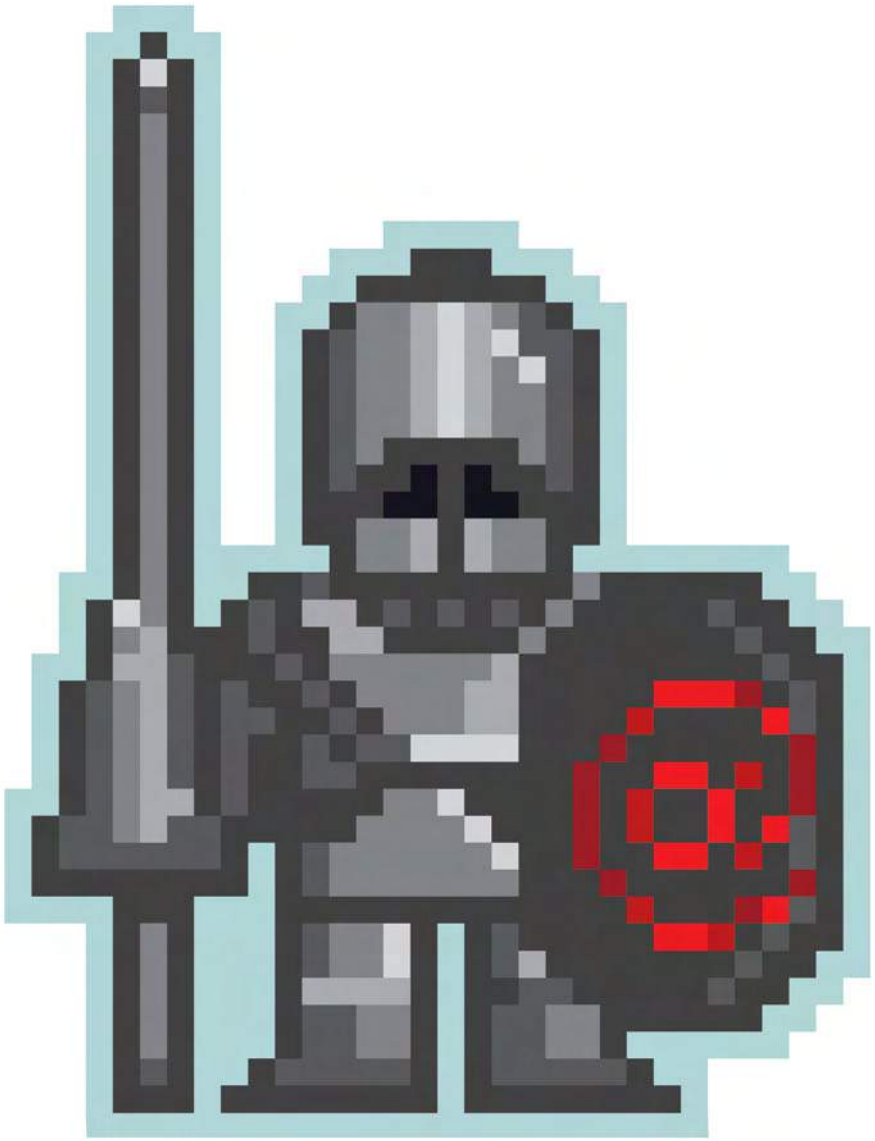
Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ
ΣΤΟ ΔΙΑΔΙΚΤΥΟ
ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ



2ο Συνέδριο
για την Ασφαλή Πλοήγηση στο Διαδίκτυο
2013

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΕΚΔΟΤΙΚΟΣ ΟΙΚΟΣ Α.Α. ΛΙΒΑΝΗ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Συμβουλές για τους γονείς!

- Προτιμήστε να τοποθετήσετε τον υπολογιστή σας σε χώρους όπως είναι το σαλόνι, και όχι στο υπνοδωμάτιο του παιδιού. Έτσι, θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται.
- Κάντε την πλοήγηση στο Διαδίκτυο οικογενειακή δραστηριότητα. Χρησιμοποιήστε τον υπολογιστή μαζί με τα παιδιά σας.
- Ενημερώστε τα παιδιά σας για τους κινδύνους που ελλοχεύουν όταν συνομιλούν με αγνώστους μέσω chatrooms.
- Συζητήστε με τα παιδιά σας για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο Διαδίκτυο.
- Διδάξτε τα να μη δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας (επίθετο, όνομα, ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οικογενειακό εισόδημα, ωράρια σχολείου, ονόματα φίλων κ.λπ.).
- Μη δίνετε στα παιδιά την πιστωτική σας κάρτα για να τη χρησιμοποιήσουν σε διαδικτυακές συναλλαγές.
- Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου. Διδάξτε τα να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. Εξηγήστε τους ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν μπορεί, να είναι επικίνδυνοι.
- Χρησιμοποιήστε τα λεγόμενα «φίλτρα», που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητά sites (βία, πορνογραφία).
- Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.ά., που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίλους τους.
- Μείνετε κοντά στα παιδιά σας και εμπλακείτε σε κάθε δική τους διαδικτυακή δραστηριότητα, με τον ίδιο τρόπο που κάνετε για τις δραστηριότητες του σχολείου.
- Μιλήστε με το παιδί σας και κάντε το να συνειδητοποιήσει ότι, αν προκύψει κάτι ξαφνικό ή ενοχλητικό στο Διαδίκτυο, πρέπει να κλείσει την ηλεκτρονική σελίδα.

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

2ο Συνέδριο
για την Ασφαλή Πλοήγηση στο Διαδίκτυο
2013

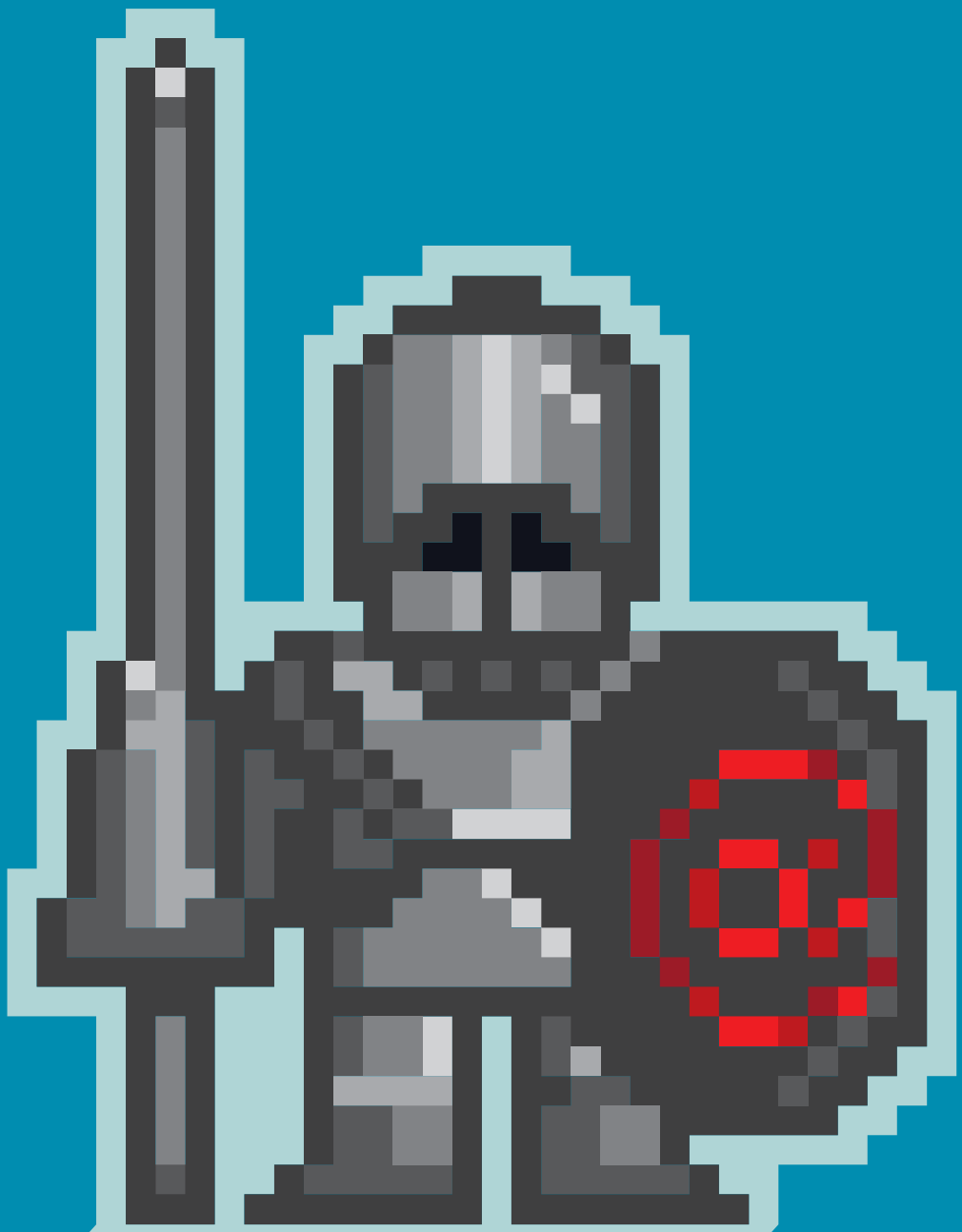
«Το Αρχηγείο της Ελληνικής Αστυνομίας
και η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
συνιστά ΝΑΙ στο διαδίκτυο και τις νέες τεχνολογίες.»

ISBN: 978-960-14-2660-0

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

07/02/2013

2ο Συνέδριο για την Ασφαλή Πλοήγηση στο Διαδίκτυο



Bold Ogilvy & Mather

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT

Χορηγός Φιλοξενίας ATHENAEUM INTERCONTINENTAL ATHENS

Χορηγός Επικοινωνίας BHMAFM 99,5

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Πρόσκληση

Το Αρχηγείο της Ελληνικής Αστυνομίας, με αφορμή
την ***«Παγκόσμια ημέρα ασφαλούς πλοήγησης στο διαδίκτυο»****,*
σας προσκαλεί στο συνέδριο το οποίο διοργανώνεται
από την ΥΠ.Ο.Α.Δ.Η.Ε./Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
και θα πραγματοποιηθεί την ***Πέμπτη 7 Φεβρουαρίου 2013*** *στο ξενοδοχείο*
Athenaeum Intercontinental Athens*, Λ. Συγγρού 89-93.*

Ώρα *έναρξης:* ***09:30****.*

Πέρας *προσέλευσης:* ***09:00****.*

Η πρόσκληση είναι προσωπική και θα διευκόλυνε τη διαπίστευση εισόδου
η προσκόμιση του δελτίου ταυτότητας.

AEGEAN · Bold Ogilvy & Mather · Εκπαιδευτήρια ΓΕΙΤΟΝΑ · cyta · Eurobank · FORTHNET nova · Hertz · hol hellas online · OLYMPIC · ΟΤΕ · COSMOTE · VISA · vodafone · WIND

Χορηγός Φιλοξενίας ATHENAEUM INTERCONTINENTAL ATHENS

Χορηγός Επικοινωνίας ΒΗΜΑFM 99,5

ΠΡΟΓΡΑΜΜΑ ΣΥΝΕΔΡΙΟΥ

ΑΙΘΟΥΣΑ 01

Ασφάλεια Ηλεκτρονικών Πληροφοριών – Βιομηχανική Κατασκοπεία			
	Ενότητα 1η		Ενότητα 2η
10:00–11:15	**Συντονιστής: Καθηγητής Ιάκωβος Στ. Βενιέρης, Εθνικό Μετσόβιο Πολυτεχνείο** **«Τι μέλλει γενέσθαι»** Αστυνομικός Διευθυντής Εμμανουήλ Σφακιανάκης, Προϊστάμενος Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος Αστυνόμος Β' Αναστάσιος Παπαθανασίου, Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Υπαστυνόμος Α' Λαλάς Ευθύμιος, Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος **«Ο μορφότυπος του Ειδικού Ασφάλειας στις ΤΠΕ»** Καθηγητής Δημήτρης Γκρίτζαλης, Τμήμα Πληροφορικής Οικονομικό Πανεπιστήμιο Αθηνών **«Τεχνικές Βιομηχανικής Κατασκοπείας»** Δρ. Ιωσήφ Ανδρουλιδάκης, Πανεπιστήμιο Ιωαννίνων **«Ασφάλεια και προστασία στο Διαδίκτυο»** κ. Διονύσης Κολοκοτσάς, Public Policy manager Google **«Η ανάγκη της Ασφάλειας Ηλεκτρονικών Πληροφοριών Μύθος ή Πραγματικότητα»** κ. Απόστολος Πανδρούλας, Country Leader Symantec Hellas κ. Πάρις Κάσκας, Principal Presales Consultant, Symantec Hellas	12:00–13:15	**Συντονιστής: Καθηγητής Δημήτρης Γκρίτζαλης, Τμήμα Πληροφορικής Οικονομικό Πανεπιστήμιο Αθηνών** **«Information Protection "by Design": Σχεδίαση Συστημάτων με Ενσωματωμένη Δυνατότητα Προστασίας και Ακεραιότητας της Πληροφορίας»** Καθηγητής Ιάκωβος Στ. Βενιέρης, Εθνικό Μετσόβιο Πολυτεχνείο **«Και μετά την παραβίαση ασφάλειας, τι;»** Καθηγητής Σωκράτης Κάτσικας Τμήμα Ψηφιακών Συστημάτων Πανεπιστήμιο Πειραιώς **«Μπορώ να προστατεύσω αποτελεσματικά τα κρίσιμα επιχειρησιακά δεδομένα μου;»** Επίκουρος Καθηγητής Κων/νος Λαμπρινουδάκης, Τμήμα Ψηφιακών Συστημάτων Πανεπιστήμιο Πειραιώς **«Το Κόστος της Ανασφάλειας»** κ. Σωτήρης Ιωαννίδης, Ερευνητής στο Ίδρυμα της Επιστήμης της πληροφορικής **«European Cybercrime Unit»** Mr. Massimiliano Michenzi, Europol EC3
		13:15–13:30	Ερωτήσεις
11:15–11:30	Ερωτήσεις	13:30–13:45	Μουσικό διάλειμμα
11:30–12:00	Διάλειμμα για καφέ	13:45–14.30	Ελαφρύ γεύμα

ΑΙΘΟΥΣΑ 02

Κυβερνοέγκλημα και νομοθεσία – «Κραυγές απόγνωσης» – Πρόληψη αυτοκτονιών			
	Ενότητα 1η		Ενότητα 2η
10:00–11:15	**Συντονιστής: κ. Γεώργιος Σανιδάς, Επίτιμος Εισαγγελέας Αρείου Πάγου** **«Ασφάλεια στο Διαδίκτυο – Από το νόμο στην πραγματικότητα»** κ. Ιωάννης Αγγελής, Εισαγγελέας Εφετών Αθηνών **«Προαναγγελίες αυτοκτονιών στο Διαδίκτυο. Διαστάσεις του φαινομένου και νομική προσέγγιση»** κ. Δημήτριος Κιούπης, Επίκουρος Καθηγητής Ποινικού Δικαίου και Ποινικής Δικονομίας, Τμήμα Νομικής, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών **«Η πρόληψη της αυτοκτονίας ανηλίκου κι ένα νομικό παράδοξο»** κ. Δημήτριος Ι. Γκύζης, Ε.Σ.Δ., LL.M, Εισαγγελέας Πρωτοδικών Αθηνών, Προϊστάμενος Τμήματος Β΄ Ποινικής Δίωξης Εισαγγελίας Πρωτοδικών Αθηνών **«Κραυγές απόγνωσης μέσω Διαδικτύου»** κ. Εμμανουήλ Σφακιανάκης, Αστυνομικός Διευθυντής, Προϊστάμενος Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος	12:00–13:15	**Συντονιστής: κ. Λεωνίδας Κοτσαλής, Καθηγητής Ποινικού Δικαίου Πανεπιστημίου Αθηνών, Μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.)** **«Ερμηνευτικές προσεγγίσεις ως προς την έκταση του υπό του άρθρου 19 του Συντάγματος θεσπιζομένου απορρήτου και η σχέση της Δικαιοσύνης και των οργάνων της προς την Α.Δ.Α.Ε. κατά την εφαρμογή του»** κ. Γεώργιος Σανιδάς, Επίτιμος Εισαγγελέας Αρείου Πάγου **«Οι γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου και η νομοθεσία του Διαδικτύου για την άρση του απορρήτου»** κ. Κωνσταντίνος Παρασκευαΐδης, Αντεισαγγελέας Αρείου Πάγου, ΜΔΕ Ποινικών Επιστημών Νομικής Σχολής Πανεπιστημίου Αθηνών **«Μέτρα ασφαλείας και αντιμετώπιση περιστατικών παραβίασης προσωπικών δεδομένων: Προβλήματα και σκέψεις με αφορμή την πρόσφατη νομολογία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα»** κ. Γρηγόρης Λαζαράκος, Δικηγόρος, Δ.Ν., Αναπληρωματικό Μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) **«Profiling στα κοινωνικά δίκτυα»** κ. Λίλιαν Μήτρου, Αναπληρώτρια Καθηγήτρια, Πανεπιστήμιο Αιγαίου
11:15–11:30	Ερωτήσεις		
11:30–12:00	Διάλειμμα για καφέ		
		13:15–13:30	Ερωτήσεις
		13:30–13:45	Μουσικό διάλειμμα
		13:45–14.30	Ελαφρύ γεύμα

ΑΙΘΟΥΣΑ 03

Διαδικτυακός Εκφοβισμός – CYBERBULLYING			
	Ενότητα 1η		Ενότητα 2η
10:00–11:15	**Συντονιστής: κ. Γεώργιος Κουμουτσάκος, Μέλος του Ευρωπαϊκού Κοινοβουλίου** **«Το Χαμόγελο του Παιδιού: Δράσεις ενάντια στον εκφοβισμό»** κ. Κωνσταντίνος Γιαννόπουλος, Πρόεδρος του Δ.Σ. του οργανισμού «Το Χαμόγελο του Παιδιού» Ομάδα παιδιών «YouSmilers» **«Digital και cyber bullying και αθέμιτη χρήση ηλεκτρονικών πληροφοριών ως το "bullying του μέλλοντος" – Γνώση και πρόληψη»** κ. Φώτης Σπυρόπουλος, Δικηγόρος – οικονομολόγος, ποινικολόγος (ΜΔΕ), εγκληματολόγος (ΜΔΕ), υπ. Δρ. Ποινικού Δικαίου – Εγκληματολογίας Νομικής Αθηνών, αριστούχος υπότροφος προγράμματος «ΗΡΑΚΛΕΙΤΟΣ ΙΙ» **«Η προστασία των δικαιωμάτων των παιδιών στο διαδίκτυο: Προτάσεις για δράσεις στο σχολείο»** κ. Γεώργιος Μόσχος, Νομικός–Εγκληματολόγος, Βοηθός Συνήγορος του Πολίτη για τα Δικαιώματα του Παιδιού **«Ο φόβος στα παραμύθια και στο διαδίκτυο (από την Κοκκινοσκουφίτσα στο facebook)»** κ. Ελευθέριος Γείτονας, Εκπαιδευτικός – Πρόεδρος και Διευθύνων Σύμβουλος στα Εκπαιδευτήρια ΓΕΙΤΟΝΑ **«Recorded Message»** Facebook Team	12:00–13:15	**Συντονιστής: κ. Ελευθέριος Γείτονας, Εκπαιδευτικός – Πρόεδρος και Διευθύνων Σύμβουλος στα Εκπαιδευτήρια ΓΕΙΤΟΝΑ** **«Οι συνέπειες του κυβερνοεκφοβισμού στην ψυχική υγεία των παιδιών και των εφήβων: Τρόποι αντιμετώπισης του φαινομένου»** Δρ. Κωνσταντίνος Στώμος, Ψυχίατρος παιδιών και εφήβων – Πρόεδρος της Ελληνικής Εταιρείας Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο **«Διαδικτυακός εκφοβισμός: σύγχρονα ερευνητικά δεδομένα, πρόληψη και αντιμετώπιση του φαινομένου»** κ. Βάντα Φισούν, Κλινική Ψυχολόγος M.Sc, Υπ. Διδάκτωρ Παν/μίου Αθηνών, Γ.Ν.Α. «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ», Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο **«Η απειλή του διαδικτυακού εκφοβισμού: Η Ευρώπη αφυπνίζεται»** κ. Γεώργιος Κουμουτσάκος, Μέλος του Ευρωπαϊκού Κοινοβουλίου **«Διαδίκτυο και Εφηβεία: αποτελέσματα της Ευρωπαϊκής μελέτης EU NET ADB»** Δρ. Άρτεμις Τσίτσικα, Λέκτορας Εφηβικής Ιατρικής Πανεπιστημίου Αθηνών, Επιστημονική Υπεύθυνος Μονάδα Εφηβικής Υγείας (ΜΕΥ),Β Παιδιατρική Κλινική, Νοσοκομείο Παίδων «Π.& Α. Κυριάκου» κ. Βασιλική Δημητρακοπούλου, Ψυχολόγος, Επιστημονική Συνεργάτης Μονάδα Εφηβικής Υγείας (ΜΕΥ), Β Παιδιατρική Κλινική, Νοσοκομείο Παίδων «Π. & Α. Κυριάκου» **«Διαδικτυακός εκφοβισμός: Μύθος και πραγματικότητα»** κ. Εμμανουήλ Σφακιανάκης, Αστυνομικός Διευθυντής, Προϊστάμενος Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος Υπαστυνόμος Α' Γαλάνη Όλγα, Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Υπαστυνόμος Α' Κώνστα Λαμπρινή, Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος
11:15–11:30	Ερωτήσεις		
11:30–12:00	Διάλειμμα για καφέ		
		13:15–13:30	Ερωτήσεις
		13:30–13:45	Μουσικό διάλειμμα
		13:45–14.30	Ελαφρύ γεύμα

«Τα πρακτικά του συνεδρίου έχουν αναρτηθεί σε ψηφιακή μορφή στο www.astynomia.gr, ενώ οι ομιλίες βρίσκονται στο κανάλι της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος στο youtube (www.youtube.com/ccugreece).»

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΓΡΑΜΜΑ ΣΥΝΕΔΡΙΟΥ

Ασφάλεια Ηλεκτρονικών Πληροφοριών Βιομηχανική Κατασκοπεία

Διαδικτυακός Εκφοβισμός Cyberbullying

Κυβερνοέγκλημα και νομοθεσία «Κραυγές απόγνωσης» Πρόληψη αυτοκτονιών

ΦΥΛΛΑΔΙΑ

Ασφάλεια Ηλεκτρονικών Πληροφοριών
Βιομηχανική Κατασκοπεία

«Τι μέλλει γενέσθαι»

Ταξίαρχος **Εμμανουήλ ΣΦΑΚΙΑΝΑΚΗΣ**
Αστυνόμος **Β' Αναστάσιος ΠΑΠΑΘΑΝΑΣΙΟΥ**
Υπαστυνόμος **Α' Ευθύμιος ΛΑΛΑΣ**

Πρόλογος

Το διαδίκτυο είναι το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο και μπορεί να χαρακτηριστεί ένα από τα σημαντικότερα – αν όχι το σημαντικότερο – από τα σύγχρονα επιτεύγματα της ανθρωπότητας. Παρ' όλα αυτά, η ευρεία διάδοση του διαδικτύου δεν είναι χωρίς συνέπειες καθώς μία πληθώρα αδικημάτων αυξανόμενης συχνότητας λαμβάνουν χώρα σε αυτό ή με τη χρήση αυτού. Η παρούσα παρουσίαση τιτλοφορείται «Τι μέλλει γενέσθαι» ακριβώς γιατί έχει σκοπό να αποτυπώσει την υπάρχουσα κατάσταση και να διαγράψει το μέλλον του διαδικτύου και τα μέτρα που πρέπει να λαμβάνονται από όλους ώστε η πλοήγηση σε αυτό να είναι πραγματικά ασφαλής.

Εισαγωγή

Ο Παγκόσμιος Ιστός είναι σαν μία κοινωνία – διαθέτει μία πληθώρα πληροφοριών, ευκαιριών και υπηρεσιών που είναι προσβάσιμες σε όλους. Η διείσδυση του διαδικτύου στη ζωή μας είναι πάρα πολύ μεγάλη. Ενδεικτικά πάνω από το 50% των νοικοκυριών διαθέτει ευρυζωνική σύνδεση στο διαδίκτυο ενώ επίσης πάνω από τους μισούς ανθρώπους (και σχεδόν όλα τα άτομα νεαρής ηλικίας) κάνουν χρήση υπολογιστών και διαδικτύου, όπως φαίνεται στα παρακάτω γραφήματα.

Αρνητικά του διαδικτύου

Πέρα από τη θετική επίπτωση του διαδικτύου στη ζωή μας, η παρούσα ομιλία έχει σκοπό να καταδείξει την αρνητική πλευρά αυτού και των τρόπων που κάποιος μπορεί να το χρησιμοποιεί και να είναι ασφαλής.

Όπως προαναφέρθηκε, μέσω διαδικτύου ή με τη χρήση αυτού λαμβάνει χώρα καθημερινά μία πληθώρα αδικημάτων ή άλλων αντικοινωνικών συμπεριφορών όπως:

- Διακίνηση παιδικής πορνογραφίας
- Κυβερνοεκφοβισμός (cyber bullying)
- Εθισμός – αυτοκτονίες
- Παραβίαση προσωπικών δεδομένων
- Απάτες
- Βιομηχανική κατασκοπεία

Επίσης, λόγω ευρείας χρήσης του διαδικτύου, ένα πλήθος από άλλα αδικήματα του κοινού Ποινικού Κώδικα μεταφέρονται συνεχώς σε αυτό. Παραδείγματα είναι η εμπορία ανθρώπων, η τρομοκρατία, η διακίνηση ναρκωτικών κλπ.

Στις επόμενες ενότητες θα παρουσιάσουμε τα σημαντικότερα από τα προαναφερθέντα αδικήματα, που είναι αυτά που διαπράττονται μέσω κοινωνικών δικτύων (social networks), οι απάτες, και ασφαλώς η βιομηχανική κατασκοπεία, που αποτελεί και το κύριο θέμα του συνεδρίου.

Αδικήματα στα μέσα κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης (social networking sites ή εν συντομία social networks) είναι πλατφόρμες/ιστοσελίδες στις οποίες κάθε εγγεγραμμένο μέλος δημιουργεί εικονικές φιλίες, ανταλλάσσει απόψεις, κοινωνικοποιείται ψηφιακά, αναζητά εργασία και γενικά περνάει ένα μεγάλο μέρος του χρόνου του. Ενδεικτικά στην Ελλάδα υπάρχουν σχεδόν 4 εκατομμύρια χρήστες του facebook (παγκόσμια φτάνουν το 1 δισεκατομμύριο), περίπου 165.000 χρήστες στο Twitter και χιλιάδες άλλοι στις υπόλοιπες πλατφόρμες (Youtube, LinkedIn κλπ).

Τελευταία μέσω των κοινωνικών δικτύων και λόγω της εξάπλωσης αυτών παρατηρούνται πολύ συχνά φαινόμενα όπως:

- Κλοπή/ανάρτηση προσωπικών δεδομένων
- Εκβιασμοί
- Διακίνηση υλικού παιδικής πορνογραφίας
- Εκφοβισμοί κλπ.

Επίσης τα κοινωνικά δίκτυα και ειδικά το facebook χρησιμοποιούνται συχνά για αλλότριους σκοπούς, όπως για παράδειγμα από τις εισπρακτικές εταιρίες προκειμένου να δουν αν οι οφειλέτες τους, μέσα από τα posts/comments και τις αναρτήσεις που κάνουν, έχουν όντως οικονομικό πρόβλημα ή όχι! Δεν είναι λίγες οι φορές επίσης που τα δεδομένα αυτά παρουσιάζονται στο δικαστήριο ως αποδείξεις για να ισχυροποιήσουν τη θέση κάποιου από τους αντιδίκους! Μία άλλη επίσης συχνή περίπτωση είναι αυτή όπου διαρρήκτες παρακολουθούν μέσω facebook τα θύματά τους και «επισκέπτονται» το σπίτι τους όταν αυτά έχουν δημοσιοποιήσει μέσω posts/comments την απουσίας τους σε διακοπές ή για άλλους λόγους!

Απάτες μέσω διαδικτύου

Ένα άλλο συχνό φαινόμενο που παρατηρείται, και επηρεάζει σε μεγάλο βάθμό τους χρήστες, είναι η πραγματοποίηση απατών μέσω διαδικτύου. Οι απάτες χωρίζονται στις εξής:

- Phisihng/pharming
- Scam mails
- Νιγηριανή απάτη/ισπανικό λόττο
- Διαδικτυακές παγίδες
- Απατηλές αγγελίες

Από αυτές, η πρώτη κατηγορία αφορά κυρίως τους χρήστες τραπεζών, όπου τους υποκλέπτονται στοιχεία (όνομα χρήστη/κωδικός) με σκοπό την πραγματοποίηση συναλλαγών εν αγνοία τους, με κέρδη παγκοσμίως πάνω από 1 δισεκατομμύριο ευρώ.

Τα scam mails αφορούν ψεύτικα (απατηλά) μηνύματα που μοιάζουν με αληθινά, κυρίως για ψεύτικες αγγελίες θέσεων εργασίας, και σκοπό έχουν να παραπλανήσουν ανυποψίαστους που αναζητούν εργασία για να τους πείσουν να αποστείλουν τα προσωπικά τους στοιχεία ή/και κάποια χρήματα για τη διεκπεραίωση κάποιων «απαραίτητων εγγράφων».

Οι διαδικτυακές παγίδες και οι απατηλές αγγελίες έχουν επίσης σκοπό την εξαπάτηση των χρηστών, παρουσιάζοντάς τους ψεύτικα γεγονότα ως αληθινά με σκοπό να τους αποσπάσουν χρηματικά ποσά.

Ιδιαίτερα θα σταθούμε στο φαινόμενο των νιγηριανών απατών/ισπανικού λόττο. Στο είδος αυτό των απατών, τα θύματα ενημερώνονται ότι κέρδισαν κάποιο μεγάλο χρηματικό ποσό σε λοταρία ή ότι κάποιος τους έχει αφήσει μία μεγάλη κληρονομία. Προκειμένου να «αποδεσμεύσουν» αυτό το χρηματικό ποσό, τους ζητείται συνήθως να καταβάλλουν χρήματα, κάτι που τα πιο ανυποψίαστα θύματα κάνουν.

Μερικές φορές μάλιστα, με σκοπό να φανεί όσο το δυνατόν πιο πιστευτή η ιστορία, οι δράστες στήνουν μέχρι και σκηνικά τραπεζών ή συμβολαιογράφων, ώστε το θύμα να πειστεί ότι υπάρχει όντως η κληρονομιά ή το χρηματικό ποσό. Χαρακτηριστική είναι η περίπτωση θύματος για το οποίο έστησαν αερομεταφορά σε χώρα του εξωτερικού, προκειμένου να του δείξουν το χρηματικό ποσό σε «πλαστό» τραπεζικό οργανισμό.

Τελευταία, σε πολλές ευρωπαϊκές χώρες είναι σε έξαρση μία άλλη μορφή απάτης, ο ιός «ransomware» ή αλλιώς ιός των 100 ευρώ. Στην περίπτωση αυτή, ένας ιός προσβάλει τον υπολογιστή και εμφανίζει μήνυμα στον χρήστη ότι δήθεν η Ελληνική Αστυνομία έχει κλειδώσει τον υπολογιστή και ότι πρέπει να καταβάλει το ποσό των 100 ευρώ για πρόστιμο έναντι των αδικημάτων που έχει διαπράξει. Τα θύματα πανευρωπαϊκά είναι εκατοντάδες χιλιάδες ενώ η λεία των συγκεκριμένων δραστών ανέρχεται σε πολλά εκατομμύρια ευρώ.

Βιομηχανική κατασκοπεία

Με τον όρο κατασκοπεία εννοούμε την πρόσβαση σε πληροφορίες, χωρίς την έγκριση των κατόχων τους, από άτομα, εταιρίες, ανταγωνιστές, κράτη, με σκοπό την απόκτηση συγκριτικού πλεονεκτήματος. Αντίστοιχα, κυβερνοκατασκοπεία (cyber spying ή cyber espionage) είναι η κατασκοπεία που διαπράττεται μέσω διαδικτύου ή με τη χρήση υπολογιστών, με μεθόδους cracking και με ιομορφικό λογισμικό όπως trojan horses και spyware (stuxnet, flame, red october etc.).

Η κατασκοπεία είναι ένα φαινόμενο που έχει μεγάλη εξάπλωση τα τελευταία χρόνια, καθώς λίγοι είναι εκείνοι που μπορούν να υποψιαστούν ότι η απώλεια των εταιρικών ή άλλων εμπιστευτικών δεδομένων μπορεί να προκαλέσει τεράστιες οικονομικές απώλειες αλλά και πραγματική καταστροφή μίας επιχείρησης ή ακόμα και ενός κράτους!

Χαρακτηριστική είναι η περίπτωση μεγάλης ναυτιλιακής εταιρίας που έπεσε θύμα βιομηχανικής κατασκοπείας με την υποκλοπή όλων των ηλεκτρονικών συνομιλιών κατόπιν επίθεσης στον mail server. Το λογισμικό που υπέκλεπτε ήχο και εικόνα, και τα έστελνε διαδικτυακά στη Ρωσία, ήταν εγκατεστημένο στο laptop του Προέδρου, ενώ οι πράξεις αυτές οδήγησαν την εταιρία σχεδόν στην καταστροφή.

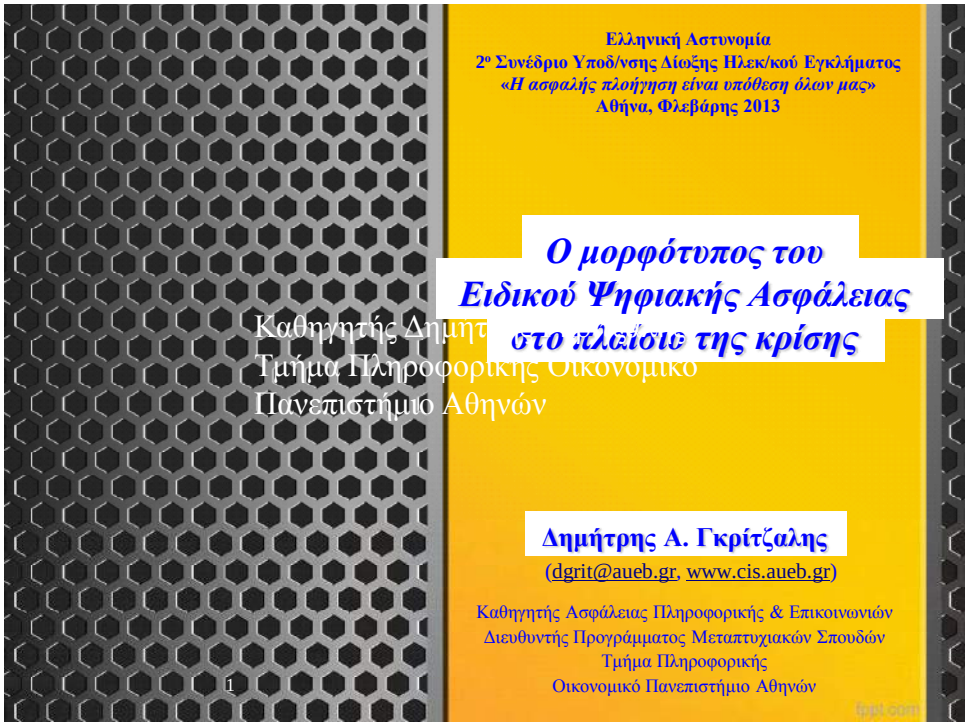
Παρόμοια περίπτωση είναι αυτή με την κωδική ονομασία «Κάτια», όπου πραγματοποιήθηκε υποκλοπή λογισμικού από εταιρία πολεμικής βιομηχανίας. Το κύκλωμα στη συνέχεια διέθετε το λογισμικό παράνομα στην παγκόσμια αγορά, προκαλώντας ζημιά άνω των 360.000.000 δολαρίων στην εταιρία.

Λίγα λόγια για την Υπηρεσία μας

- Διακρίθηκε και τιμήθηκε από τον Πρόεδρο της Δημοκρατίας ως μια από τις καλύτερες υπηρεσίες της ΕΛ-ΑΣ.
- Διακρίθηκε και τιμήθηκε τρεις φορές από το FBI για την προσφορά της στην καταπολέμηση του cyber crime και της παιδικής πορνογραφίας.
- Διακρίθηκε και τιμήθηκε από τον Υπουργό Παιδείας για την πρόληψη μιας Αυτοκτονίας μέσω INTERNET.
- Διακρίθηκε και τιμήθηκε από τον Υπουργό Εθνικής Οικονομίας για την σημαντική προσφορά της στον τομέα της καταπολέμησης του κυβερνοεγκλήματος
- Είναι πιστοποιημένη κατά ISO9001:2008.

«Ο μορφότυπος του Ειδικού Ασφάλειας στις ΤΠΕ»

Καθηγητής **Δημήτρης Γκρίτζαλης**
Τμήμα Πληροφορικής Οικονομικό Πανεπιστήμιο Αθηνών



Το *puzzle* και η "διανομή των ρόλων"

Ε.Ε., Δ.Ν.Τ., Π.Δ.Ε., Επιχειρήσεις (*Χρηματοδότες*)

Κυβέρνηση, Οργανισμοί (*Διαχειριστές*)

Εταιρείες ΤΠΕ κ.ά. (*Προμηθευτές*)

Χρήστες (*Δημόσια Διοίκηση, Οργανισμοί κ.ά.)*

Πολίτες (*Πελάτες, Χρήστες*)

Ειδικοί Ψηφιακής Ασφάλειας (*εσ/μείς*)

2

Η κυρίαρχη (;) αντίληψη κάθε ρόλου

Εταιρείες ΤΠΕ κ.ά. (*Προμηθευτές*)

⇒ "Είναι ευέλικτο το εργασιακό καθεστώς;"

⇒ "Είναι ρεαλιστικό το πλαίσιο προμηθειών;"

⇒ "Τα περιθώρια, στο έργο αυτό, είναι πολύ μικρά"

⇒ "Ε, όχι! Θα ζητήσω ασφαλιστικά μέτρα!"

⇒ Ειδικός Ψηφιακής Ασφάλειας;
"Είναι απαραίτητος; Τι λέει η σύμβαση;"

3

Η κυρίαρχη (;) αντίληψη κάθε ρόλου

Χρήστες (Δημόσια Διοίκηση, Οργανισμοί κ.ά.)

- ⇒ "Ποια κίνητρα προβλέπονται;"
- ⇒ "Αυτά μας τα 'παν κι άλλοι!"
- ⇒ "Δεν μπορώ να τα κάνω όλα μόνος μου!"
- ⇒ "Βγαίνω στη σύνταξη/εφεδρεία"
- ⇒ "Χρειάζομαι - επιπλέον αυτών - και…"
- ⇒ "Υπάρχουν άλλες προτεραιότητες"
- ⇒ Ειδικός Ψηφιακής Ασφάλειας;
  "Για ασφάλεια θα φροντίσει ο προμηθευτής!"

4

Εμείς, οι Πληροφορικοί

Αυτοκριτικά

Ως χρήστες (ή ως πελάτες):

- ⇒ Γενικά, "έχουμε άποψη"!
- ⇒ Συνήθως, δεν αμοιβόμαστε "αρκετά"...
- ⇒ "Ο manager μου ευνοήθηκε, αλλοιώς εγώ..."
- ⇒ "Εγώ απλώς εισηγούμαι"
- ⇒ "Δεν παραλαμβάνω!"

5

Εμείς, οι Πληροφορικοί

Όποιοι κι αν είμαστε:

⇒ Δεν συμμεριζόμαστε το ίδιο όραμα (*γιατί άλλωστε;*)

⇒ Λειτουργούμε αποσπασματικά ή μοναχικά (*ξέρουμε πού οφείλεται;*)

⇒ Μπορούμε - και πρέπει - να κρίνουμε (*όπως και να κρινόμαστε!*)

⇒ Κανένας μας δεν περισσεύει (*αλλά και όλοι μαζί ίσως δεν αρκούμε…*)

fppt.com

6

Ερωτήματα του Πολίτη - Ειδικού Ασφάλειας

Το όραμά μας δεν (μπορεί να) είναι ανάπτυξη χωρίς κοινωνικά αντίβαρα. **Ποιά είναι αυτά;**

Το ΕΣΠΑ είναι ένας ακόμη (μείζον) κρίκος σε μια αναπτυξιακή αλυσίδα. **Ποιός τη διαμορφώνει;**

(Συν)Ευθυνόμαστε για τη μορφή που έχει πάρει η Κοινωνία της Πληροφορίας. **Ποιά μορφή θέλουμε;**

Έχουμε "άποψη", αλλά δεν έχουμε "φωνή". **Γιατί;**

Ψηφιακή ανάπτυξη χωρίς ασφάλεια και ιδωτικότητα είναι "ρότα δίχως πυξίδα". **Πώς να παρέμβουμε;**

fppt.com

7

Ειδικοί Ψηφιακής Ασφάλειας

⇒ Η ψηφιακή ασφάλεια είναι **ολιστικό ζήτημα** - δεν είναι, ούτε πρωτίστως, ούτε αμιγώς, τεχνικό ζήτημα.

⇒ Η ψηφιακή ασφάλεια είναι επιτεύξιμη με **μεθοδικές προσεγγίσεις** - όχι με αποσπασματικές παρεμβάσεις.

⇒ Η ψηφιακή ασφάλεια απαιτεί **Ειδικούς Ψηφιακής Ασφάλειας** - όχι (τυχάρπαστους) εμπειροτέχνες.

⇒ Η ψηφιακή ασφάλεια απαιτεί **ειδικές επιστημονικές γνώσεις/δεξιότητες** - δεν αρκούν (μόνον) πιστοποιήσεις.

⇒ Ο ρόλος του **ανθρώπινου παράγοντα** - των αξιών, του ήθους, της προσωπικότητας - παραμένει θεμελιώδης.

⇒ "**Too much security is bad security**!"

fppt.com

8

Ψηφιακή Ασφάλεια: Με ποια πυξίδα; (1/2)

1. Σε κάθε πολίτη πρέπει να παρέχονται επαρκώς **ασφαλείς ψηφιακές υπηρεσίες.**

2. Η ψηφιακή ασφάλεια προϋποθέτει **γνώση, ευαισθητοποίηση** και **υπευθυνότητα**.

3. Η ψηφιακή ασφάλεια είναι **ολιστικό** ζήτημα, με κύρια συνιστώσα τον **ανθρώπινο παράγοντα.**

fppt.com

9

Ψηφιακή Ασφάλεια: Με ποια πυξίδα; (2/2)

4. Η ψηφιακή ασφάλεια προϋποθέτει
επιστημονική και κοινωνική υπευθυνότητα
και διευκολύνεται από τη **συλλογική δράση.**

5. Η ψηφιακή ασφάλεια
είναι, πρωτίστως, έργο **ειδικών επιστημόνων.**

6. Η ψηφιακή ασφάλεια διασφαλίζεται πληρέστερα
όταν σχεδιάζεται με **διεπιστημονική συνεργασία.**

7. Η ψηφιακή ασφάλεια πρέπει να αποβλέπει, πρωτίστως,
στην **προστασία ευαίσθητων κοινωνικών ομάδων**.

fppt.com

10

«Τεχνικές Μέθοδοι Βιομηχανικής Κατασκοπείας»

Δρ. **Ιωσήφ Ι. Ανδρουλιδάκης**

Περίληψη

Στις μέρες μας, η προστασία της πνευματικής ιδιοκτησίας και των εμπιστευτικών δεδομένων είναι ζωτικής σημασίας. Όχι μόνο για τις εταιρείες και τους επαγγελματίες αλλά και για τους ιδιώτες που αντιμετωπίζουν καθημερινά πλέον πληθώρα επιθέσεων στα προσωπικά τους δεδομένα. Αντίθετα με την «κλασσική» κατασκοπεία που γίνεται για εθνικούς σκοπούς, η πρακτική της συγκέντρωσης εμπιστευτικών πληροφοριών χωρίς την άδεια του κατόχου τους για εμπορικούς και οικονομικούς σκοπούς καλείται βιομηχανική, εταιρική, εμπορική ή οικονομική κατασκοπεία. Παρά το γεγονός ότι οι τεχνικές που χρησιμοποιούν οι «κατάσκοποι» πληροφοριών και τα ίδια τα περιστατικά βιομηχανικής κατασκοπείας μοιάζουν να έχουν βγει από ταινίες δράσης, η αλήθεια είναι ότι το πρόβλημα είναι υπαρκτό και περισσότερο έντονο από ποτέ, ακόμα και στη χώρα μας.

Η παρούσα δημοσίευση επικεντρώνεται σε πρακτικά ζητήματα και όχι σε θεωρητική ανάλυση, και βασίζεται στο βιβλίο του συγγραφέα «Βιομηχανική Κατασκοπεία, Υποκλοπή Πληροφοριών & Τηλεπικοινωνιών και Αντίμετρα». Τόσο η δημοσίευση όσο και το σχετικό βιβλίο επιχειρούν να ρίξουν περισσότερο φως στο ζήτημα της βιομηχανικής κατασκοπείας και των υποκλοπών και να ενημερώσουν τους αναγνώστες για τους κινδύνους που ελλοχεύουν αλλά και για το πώς μπορούν να προστατευθούν.

Εισαγωγή

Αντίθετα με την «κλασσική» κατασκοπεία που γίνεται για εθνικούς σκοπούς, η πρακτική της συγκέντρωσης εμπιστευτικών πληροφοριών χωρίς την άδεια του κατόχου τους για εμπορικούς και οικονομικούς σκοπούς καλείται βιομηχανική, εταιρική, εμπορική ή οικονομική κατασκοπεία. Φαινόμενα υποκλοπών και βιομηχανικής κατασκοπείας υπήρχαν, υπάρχουν και θα υπάρχουν τόσο στο εξωτερικό όσο και στην Ελλάδα. Αρκετές περιπτώσεις έχουν φτάσει στη δημοσιότητα, το ενδιαφέρον όμως είναι ότι πολύ περισσότερα περιστατικά δε θα αποκαλυφθούν ποτέ. Είτε γιατί όντως δεν ανακαλύφθηκαν, είτε για λόγους προστασίας της φήμης των εμπλεκόμενων.

Οι ίδιες οι προκλήσεις και τα προβλήματα που αντιμετωπίζει μια σύγχρονη επιχείρηση είναι περισσότερα από ποτέ. Το περιβάλλον είναι εντόνως ανταγωνιστικό. Τα προϊόντα πρέπει να προωθούνται στην αγορά χωρίς καθυστέρηση και οι πληροφορίες να μεταδίδονται ταχύτατα, πολλές φορές εις βάρος της ασφάλειας. Εξάλλου, όσο πιο καινοτόμο είναι ένα προϊόν, τόσο μεγαλύτερο κίνδυνο αντιγραφής αντιμετωπίζει. Την ίδια στιγμή, νέες τεχνολογίες εισάγουν και νέες τρωτότητες στα συστήματα. Αντίστοιχα, στο «παιχνίδι» δραστηριοποιούνται πολλοί «παίκτες» μεταξύ των οποίων ξένες κυβερνήσεις, ανταγωνιστές, μικρές εταιρείες οι οποίες δε διαθέτουν τους απαραίτητους πόρους για να αναπτύξουν οι ίδιες τεχνολογία αλλά και μεμονωμένοι ιδιώτες με σκοπό την εκδίκηση ή το κέρδος.

Η βιομηχανική κατασκοπεία είναι πιο συχνή στους τομείς υψηλής τεχνολογίας όπως είναι ο χώρος των Ηλεκτρονικών, της Αυτοκινητοβιομηχανίας, της Φαρμακευτικής, της Χημείας, της Βιολογίας, της Αεροναυπηγικής-Διαστημικής και της Ενέργειας. Στους τομείς αυτούς, άπαξ και η πληροφορία κλαπεί, ελάχιστα μπορούν να γίνουν για να περιορισθεί το αντίκτυπο, ενώ οι απώλειες μπορεί να είναι δυσβάσταχτες.

Εξάλλου, το πρόβλημα εντείνεται λόγω πολλών παραγόντων όπως ενδεικτικά: ελλιπούς ενημέρωσης, πληθώρας εξοπλισμού υποκλοπών, έλλειψης φυσικής ασφάλειας, παράκαμψης των μέτρων ασφάλειας για χάρη της λειτουργικότητας, σφαλμάτων-αποκαλύψεων εκ παραδρομής, περιορισμού του κόστους σε όλα τα επίπεδα, ανάγκης ανταλλαγής πληροφοριών, υπεργολαβιών-outsourcing κ.ο.κ.

Τελικά, εκτός από τις εταιρείες, ο καθένας μας κινδυνεύει από παραβιάσεις της ιδιωτικότητας, Γι' αυτό σκοπός της δημοσίευσης αυτής είναι να ενημερώσει τους αναγνώστες και να τους βοηθήσει να προστατευθούν ώστε να μην προστεθούν και αυτοί στον μακρύ κατάλογο των θυμάτων υποκλοπών.

Υποκλοπές

Η αλματώδης εξέλιξη της τεχνολογίας δίνει πλέον πρόσβαση σε πληθώρα ηλεκτρονικών συσκευών και εξαρτημάτων υποκλοπών, σε μεγέθη τόσο μικρά που καθιστούν δύσκολο τον οπτικό εντοπισμό τους. Αντίστοιχα, το κόστος για απλές διατάξεις (που όμως μπορεί να προκαλέσουν τεράστια ζημιά), είναι μόλις λίγες δεκάδες ευρώ. Με δυνατότητα on-line αγοράς, και χωρίς κανέναν περιορισμό στην πώλησή τους, δεν είναι υπερβολή να πούμε ότι ο καθένας μπορεί να μετατραπεί σε «κατάσκοπο», αρκεί να έχει το «θράσος» να τα χρησιμοποιήσει τελικά. Προφανώς, τόσο ο εξοπλισμός όσο και οι ίδιες οι τεχνικές κλιμακώνονται σε εξειδίκευση, ακρίβεια και αποτελεσματικότητα όσο ανεβαίνουν τα «συμφέροντα» και εμπλέκονται ισχυρότεροι «παίκτες».

Το πρώτο πράγμα που σκέφτεται κανείς στο άκουσμα του όρου «υποκλοπές» είναι μάλλον οι υποκλοπές τηλεπικοινωνιών και δη, των τηλεφωνικών συνδιαλέξεων. Οι διατάξεις υποκλοπής μπορεί να βρίσκονται στις συσκευές που χρησιμοποιούμε ή και στο δίκτυο και τον εξοπλισμό του παρόχου, τόσο σε μορφή υλικού όσο και λογισμικού. Οι τηλεφωνικές επικοινωνίες μπορούν να υποκλαπούν σε πραγματικό χρόνο ή να ηχογραφηθούν ώστε να ανακτηθούν και αναλυθούν αργότερα. Οι κλήσεις μπορούν να συν-ακροασθούν από εσωτερικά ή εξωτερικά σημεία παρακολούθησης, ακόμα και από άλλη χώρα. Ας μην ξεχνάμε ότι από τα σύγχρονα τηλεφωνικά δίκτυα διέρχονται και δεδομένα, τόσο τηλεομοιοτυπίας (fax) όσο και Internet. Με τον κατάλληλο εξοπλισμό λοιπόν, μπορούν να υποκλαπούν και τα δεδομένα αυτά εκτός της φωνής. Αντίστοιχα η χρήση νεότερων τεχνολογιών σταθερής τηλεφωνίας όπως το VoIP κληρονομεί τα προβλήματα ασφάλειας του Διαδικτύου και η εφαρμογή της απαιτεί την κατάλληλη προσοχή.

Όσο για τα κινητά, η καθολικότητα της χρήσης τους και η διείσδυσή τους στην καθημερινή ζωή μας είναι δεδομένες. Οι σύγχρονες συσκευές με τις εξελιγμένες λειτουργίες οι οποίες συγκλίνουν με αυτές των υπολογιστών χρησιμοποιούνται όχι μόνο για επικοινωνία αλλά και για την αποθήκευση, οργάνωση, επεξεργασία, αποστολή και λήψη πληροφοριών από τον κάτοχό τους. Με την πάροδο του χρόνου λοιπόν, από τη χρήση τους συγκεντρώνονται όλο και περισσότερα δεδομένα για τον ιδιοκτήτη τους αλλά και για την εταιρεία στην οποία εργάζεται. Τα δεδομένα αυτά μπορεί να υποκλαπούν είτε από τις συσκευές είτε από τα υπολογιστικά συστήματα των δικτύων των παρόχων με χρήση κατάλληλου λογισμικού ή υλισμικού.

Τέλος, για την παγίδευση χώρου, υπάρχει μια σειρά διαφορετικών τύπων διατάξεων υποκλοπών που σκοπό έχουν να καταγράψουν ήχο ή/και εικόνα και ενδεχομένως να εκπέμψουν την πληροφορία αυτή σε διαφορετικό χώρο (κοριοί).

Πρακτικά λοιπόν, κάθε είδος επικοινωνίας μπορεί να υποκλαπεί με πολλές φορές ανησυχητικά εύκολο τρόπο. Γι' αυτό και είναι ιδιαίτερα επιτακτική η ανάγκη της εκπαίδευσης και της ενημέρωσης του κοινού και ειδικά των υπαλλήλων των εταιρειών.

Προστασία

Η προστασία κατά της βιομηχανικής κατασκοπείας και των υποκλοπών είναι πολύ-επίπεδη διαδικασία με σκοπό πάντα τη διατήρηση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των δεδομένων. Περιλαμβάνει νομικές λεπτομέρειες (Διπλώματα Ευρεσιτεχνίας, Εμπορικά Μυστικά), Φυσική και Τεχνολογική Ασφάλεια (Εξοπλισμό, Υλισμικό, Λογισμικό), Πληροφορική Διακυβέρνηση (Πολιτικές, Ρόλους, Ευθύνες, Εφαρμογή κανονισμών, Ελεγκτικούς Μηχανισμούς), Οικονομικούς περιορισμούς (Προϋπολογισμό) και φυσικά Εκπαίδευση. Η επιλογή της βέλτιστης στρατηγικής προστασίας της πνευματικής ιδιοκτησίας εξαρτάται από μια σειρά παραγόντων: Από τις διαθέσιμες εναλλακτικές, το είδος και το βαθμό προστασίας που παρέχουν, το κόστος τους και τελικά την αξία που έχει η συγκεκριμένη πνευματική ιδιοκτησία για τον ιδιοκτήτη της.

Πρέπει να σημειωθεί ότι η ένα έργο ανίχνευσης υποκλοπών αποτελεί μια ιδιαίτερα επίπονη τεχνική εργασία και δε θα πρέπει να ανατίθεται σε μη-ειδικούς. Αντίστοιχα, ο ρόλος των Αρχών ξεκινάει από τη στιγμή που θα βρεθεί κάποια διάταξη ώστε να κινηθούν (αν είναι επιθυμητό) οι νομικές διαδικασίες. Σε κάθε περίπτωση, η προστασία και η ασφάλεια, τόσο των πληροφοριών όσο και των ίδιων των υποδομών αλλά και των προϊόντων/υπηρεσιών απαιτούν διαδικασίες ιδιαίτερα απαιτητικές σε πόρους οι οποίες ταυτόχρονα δε θα πρέπει να παρεμποδίζουν την καθημερινή λειτουργία. Προφανώς, οι πολύπλοκες λύσεις χειροτερεύουν την κατάσταση ενώ στην εποχή της «πανταχού παρούσας» πληροφορίας, οι παραδοσιακές μέθοδοι και αντιλήψεις ασφάλειας δεν αποδίδουν.

Όπως και με κάθε άλλη τεχνολογία έτσι και εδώ, η πρόληψη, με την ενημέρωση και την εκπαίδευση είναι το βασικότερα στοιχεία για να διασφαλισθεί το απόρρητο των επικοινωνιών και των προσωπικών δεδομένων μας. Φυσικά υπάρχουν και τα κατάλληλα αντίμετρα, τεχνικά και μη. Σε κάθε περίπτωση η συνεργασία με ειδικούς αποτελεί τον καλύτερο τρόπο αξιοποίησής τους. Πράγματι, η προσπάθεια ανίχνευσης με ίδιους πόρους, χωρίς τη συμβολή εξειδικευμένων εταιρειών-συμβούλων, είναι μια συνταγή αποτυχίας. Είναι πιθανό να μπορέσει κάποιος να αποκαλύψει μόνος του ερασιτεχνικές διατάξεις ή μια ερασιτεχνική τοποθέτηση, αλλά σε περιπτώσεις σοβαρής βιομηχανικής κατασκοπείας η συμβολή των ειδικών είναι μονόδρομος.

Επίλογος

Διατάξεις υποκλοπών που παρουσιάζονταν σε ταινίες κατασκοπείας και ξεπερνούσαν τη σφαίρα της φαντασίας λίγες δεκαετίες πριν αποτελούν πλέον υπαρκτή πραγματικότητα. Το πιο ανησυχητικό είναι ότι το κόστος τους είναι ιδιαίτερα μικρό (ακόμα και 20 Ευρώ είναι αρκετά για μια πλήρως λειτουργική διάταξη!) και η διάθεσή τους στην αγορά σχετικά εύκολη. Η ανίχνευση από την άλλη πλευρά, απαιτεί πολλαπλώς ακριβότερο εξοπλισμό και εξειδίκευση, ιδιαίτερα στην περίπτωση που έχουν χρησιμοποιηθεί εξελιγμένες διατάξεις.

Υλοποιώντας τις υποδείξεις αυτές και επαναλαμβάνοντας τους ελέγχους σε τακτικά χρονικά διαστήματα, σε συνδυασμό με την υιοθέτηση βέλτιστων πρακτικών, συστημάτων διαχείρισης ασφάλειας πληροφοριών (όπως το ISO 27001) και εκπαιδευτικών προγραμμάτων, η εταιρεία κάνει τα βασικά βήματα για την προστασία από τον κίνδυνο της βιομηχανικής κατασκοπίας.

Τελικά, στο σύγχρονο επιχειρηματικό περιβάλλον, η προστασία κατά της βιομηχανικής κατασκοπείας δεν αποτελεί πολυτέλεια αλλά βασική προϋπόθεση. Βασική προϋπόθεση, όχι μόνο για τη διατήρηση του ανταγωνιστικού της πλεονεκτήματος αλλά και για την ίδια τη βιωσιμότητά της!

«Ασφάλεια και προστασία στο Διαδίκτυο»

Διονύσης Κολοκοτσάς
Public Policy manager Google

Το διαδίκτυο είναι σπουδαίο εργαλείο που προσφέρει πολλές ευκαιρίες για δημιουργία, απόκτηση γνώσεων και συνεργατικότητα. Μπορούμε να αξιοποιήσουμε πλήρως αυτές τις δυνατότητες παραμένοντας ασφαλείς. Στη Google αντιμετωπίζουμε πολύ σοβαρά το θέμα της ασφάλειας και του απορρήτου σας. Καταβάλλουμε προσπάθειες για να σας προστατεύσουμε από την κλοπή στοιχείων ταυτότητας, την προσωπική εξαπάτηση και τις διαδικτυακές απάτες, για να συμβάλουμε στην προστασία του υπολογιστή σας αλλά και να να καταστήσουμε το διαδίκτυο ασφαλές. Σας παρέχουμε τα εργαλεία και τις γνώσεις που χρειάζεστε για να παραμείνετε εσείς και η οικογένειά σας ασφαλείς στο διαδίκτυο. Παράλληλα, εξακολουθούμε να επενδύουμε και να βελτιωνόμαστε συνεχώς προσλαμβάνοντας παγκοσμίως αναγνωρισμένους ειδικούς στην ασφάλεια δεδομένων, προκειμένου να διατηρήσουμε τις πληροφορίες σας ασφαλείς. Οι ειδικοί αυτοί εστιάζουν στη διατήρηση της ασφάλειάς σας και της ασφάλειας των πληροφοριών σας, παραμένοντας ένα βήμα μπροστά από τους παραβάτες του κυβερνοχώρου.

Ασφαλέστερο διαδίκτυο για όλους

Επειδή η ασφάλειά σας αποτελεί σημαντική υπόθεση για εμάς ανεξάρτητα από τις υπηρεσίες ή τα προϊόντα που χρησιμοποιείτε, μοιραζόμαστε τις πληροφορίες σχετικά με τους κακούς ιστότοπους και συνδέσμους που εντοπίζουμε με άλλες εταιρείες, έτσι ώστε να τις βοηθήσουμε να προστατεύσουν τους χρήστες τους επίσης. Με τη συνεργασία και την αλληλοβοήθεια, ολόκληρος ο ιστός είναι πολύ πιο ασφαλής.

Έχουμε αναπτύξει επίσης διάφορα δημοφιλή εργαλεία ασφάλειας, όπως το Skipfish, τα οποία παρέχουν πληροφορίες στους προγραμματιστές εφαρμογών ιστού, στους κατόχους ιστότοπων, στους διαχειριστές δικτύων, προκειμένου να τους διευκολύνουν να διατηρήσουν ασφαλείς τις πλατφόρμες τους και να εντοπίσουν προβλήματα ασφαλείας με τους ιστότοπούς τους. Παρέχουμε δωρεάν αυτά τα εργαλεία και καταβάλλουμε προσπάθειες με πολλούς συνεργάτες για να τα εξελίσσουμε και να τα βελτιώνουμε συνεχώς.

Για να βοηθήσουμε άλλους ιστότοπους να υιοθετήσουν την κρυπτογράφηση SSL και να μειώσουν το κόστος, μοιραζόμαστε τα ευρήματά μας σχετικά με τον τρόπο με τον οποίο η κρυπτογράφηση SSL μπορεί να γίνει πιο αποτελεσματική, γεγονός που διευκολύνει του ιστόττοπους να προσθέσουν αυτό το επίπεδο ασφάλειας για τους χρήστες τους.

Διατηρούμε επίσης μια ανεξάρτητη υπηρεσία που ονομάζεται VirusTotal η οποία συμβάλλει στη βελτίωση της ασφάλειας στον ιστό προσφέροντας ένα δωρεάν εργαλείο που μπορούν να χρησιμοποιήσουν ταυτόχρονα οι χρήστες για να σαρώσουν αρχεία ή διευθύνσεις URL για κακόβουλα προγράμματα και ιούς.

Καθώς καταβάλλουμε προσπάθειες να προστατεύσουμε τους χρήστες μας και τα στοιχεία τους, ορισμένες φορές ανακαλύπτουμε και εξετάζουμε ασυνήθιστα μοτίβα ενεργειών. Καθημερινά εντοπίζουμε και επισημαίνουμε περισσότερους από 10.000 επικίνδυνους ιστότοπους αυτού του είδους και εμφανίζουμε προειδοποιήσεις σε έως και 14 εκατομμύρια αποτελέσματα της Αναζήτησης Google και 300.000 λήψεις, οι οποίες ενημερώνουν τους χρήστες μας ότι ενδέχεται να συμβαίνει κάτι ύποπτο σε έναν συγκεκριμένο ιστότοπο ή σύνδεσμο.

Για παράδειγμα, τον περασμένο χρόνο εντοπίσαμε ασυνήθιστη επισκεψιμότητα αναζήτησης κατά τη διεξαγωγή της συνηθισμένης συντήρησης σε ένα από τα κέντρα δεδομένων μας. Μετά τη συνεργασία με μηχανικούς ασφάλειας σε διάφορες εταιρείες που έστελναν αυτήν την τροποποιημένη επισκεψιμότητα, καταλήξαμε στο ότι οι υπολογιστές με αυτήν τη συμπεριφορά είχαν προσβληθεί από ένα συγκεκριμένο είδος κακόβουλου προγράμματος. Θέσαμε σε εφαρμογή ένα πρόγραμμα για να ενημερώσουμε τους χρήστες που προσβλήθηκαν και να τους κατευθύνουμε σε εργαλεία που θα μπορούσαν να τους βοηθήσουν να καταργήσουν το κακόβουλο πρόγραμμα.

Δημιουργήσαμε επίσης μια τεχνολογία στο Chrome η οποία βοηθά να διασφαλιστεί ότι μια ασφαλής σύνδεση είναι όντως ασφαλής. Οι εισβολείς ενδέχεται να χρησιμοποιούν πάρα πολύ εξελιγμένες μεθόδους και μπορούν να πραγματοποιήσουν επιθέσεις για να κατασκοπεύσουν τις πληροφορίες που αποστέλλετε σε έναν ιστότοπο ακόμη και αν φαίνεται ότι η σύνδεσή σας είναι ασφαλής. Χρησιμοποιώντας την τεχνολογία μας του Chrome, εντοπίσαμε επιθέσεις όπως αυτή στο παρελθόν και επικοινωνήσαμε με τους χρήστες μας, με άλλες εταιρείες προγραμμάτων περιήγησης και με προγραμματιστές για να συμβάλουμε στην από κοινού αντιμετώπιση των εισβολέων.

Στέλνουμε επίσης καθημερινά μηνύματα σε χιλιάδες κατόχους ιστότοπων των οποίων οι ιστότοποι πιστεύουμε ότι ενδέχεται να έχουν παραβιαστεί από μια επίθεση έτσι ώστε να τους καθαρίσουν.

Προστασία από απάτη

Όπως συμβαίνει και εκτός Διαδικτύου, υπάρχουν απατεώνες και στο Διαδίκτυο. Η Google ακολουθεί μια σειρά από βήματα για να σας προστατεύσει από την απάτη.

Απαγόρευση κακών διαφημίσεων (και κακών διαφημιζόμενων)

Διαθέτουμε πολύ σαφείς πολιτικές σχετικά με το ποιος μπορεί να εμφανίσει διαφημίσεις μέσω των εργαλείων της Google. Έχουμε σχεδιάσει τις πολιτικές διαφήμισής μας λαμβάνοντας υπόψη την ασφάλεια και την εμπιστοσύνη των χρηστών. Για παράδειγμα, δεν επιτρέπουμε τις διαφημίσεις για λήψεις κακόβουλων προγραμμάτων, απομιμήσεων προϊόντων ή διαφημίσεων με ασαφείς πρακτικές χρέωσης. Σε περίπτωση που εντοπίσουμε μια απάτη διαφήμισης, δεν αποκλείουμε απλώς τη διαφήμιση – αποκλείουμε το διαφημιζόμενο από τη συνεργασία με την Google στο μέλλον.

Συμβολή στην καταπολέμηση της κλοπής στοιχείων ταυτότητας

Η Google χρησιμοποιεί διάφορες τεχνολογίες για να σας βοηθήσει να προστατευτείτε από την κλοπή στοιχείων ταυτότητας στο διαδίκτυο και να βεβαιωθείτε ότι ο Λογαριασμός σας Google παραμένει ασφαλής.

Επαλήθευση σε 2 βήματα

Για ακόμη υψηλότερα επίπεδα ασφάλειας του Λογαριασμού σας Google, προσφέρουμε στους χρήστες μας την επαλήθευση σε 2 βήματα. Αυτό το εργαλείο προσφέρει ένα επιπλέον επίπεδο ασφάλειας ζητώντας όχι απλώς έναν κωδικό πρόσβασης, αλλά επίσης έναν κωδικό επαλήθευσης για τη σύνδεση σε έναν Λογαριασμό Google. Ακόμη και σε περίπτωση που έναν εισβολέας παραβιάσει, μαντέψει ή υποκλέψει με άλλον τρόπο τον κωδικό πρόσβασής σας, δεν μπορεί να συνδεθεί στο λογαριασμό σας χωρίς να εισαγάγει τον κωδικό πρόσβασης που θα αποσταλεί στο κινητό σας τηλέφωνο. Προσφέρουμε την επαλήθευση σε 2 βήματα σε περισσότερες από 50 γλώσσες και 175 χώρες.

Κρυπτογράφηση

Η Google προβλέπει πολλά βήματα για να διατηρήσει τα προσωπικά σας στοιχεία ασφαλή από εισβολείς και παραβάτες. Από προεπιλογή, γίνεται κρυπτογράφηση της σύνδεσης στο Gmail μεταξύ του υπολογιστή και της Google – αυτό συμβάλλει στην προστασία της δραστηριότητάς σας στο Google από υποκλοπή. Αυτή η μέθοδος προστασίας, γνωστή ως κρυπτογράφηση SSL καθ'όλη τη διάρκεια της σύνδεσης, αποτελεί την προεπιλογή όταν είστε συνδεδεμένοι στο Google Drive και πολλές άλλες υπηρεσίες.

Προειδοποιήσεις ύποπτης δραστηριότητας λογαριασμού

Έχουμε ειδοποιήσει πολλούς χρήστες όταν διαπιστώσαμε ύποπτη δραστηριότητα στο Λογαριασμό τους Google – για παράδειγμα, συνδέσεις που φαίνεται να προέρχονται από μία χώρα και να σημειώνονται αμέσως μετά από μία σύνδεση σε μια άλλη χώρα. Αυτοί οι χρήστες έλαβαν ένα μήνυμα προειδοποίησης στα εισερχόμενα του Gmail σχετικά με αυτήν την ασυνήθιστη πρόσβαση. Επίσης, περιστασιακά ζητούμε από τους χρήστες να αλλάξουν τους κωδικούς πρόσβασής τους εάν έχουμε λόγο να πιστεύουμε ότι ο λογαριασμός τους ενδέχεται να έχει παραβιαστεί.

Έλεγχος ταυτότητας ηλεκτρονικού ταχυδρομείου

Προκειμένου να καταπολεμήσει την κατάχρηση και να κρατήσει τα ανεπιθύμητα μηνύματα μακριά από τα εισερχόμενά σας, το Gmail χρησιμοποιεί έλεγχο ταυτότητας ηλεκτρονικού ταχυδρομείου για να διαπιστώσει εάν ένα μήνυμα προέρχεται όντως από τη διεύθυνση από την οποία φαίνεται να έχει σταλεί. Όλοι οι ενεργοί χρήστες του Gmail –και τα άτομα που επικοινωνούν μαζί τους– λαμβάνουν αυτομάτως προστασία ενάντια στις απειλές για τα προσωπικά και τα οικονομικά τους στοιχεία.

Προστασία από ανεπιθύμητα μηνύματα

Το Gmail σάς προστατεύει από ανεπιθύμητα και επιβλαβή μηνύματα ηλεκτρονικού ταχυδρομείου. Το Gmail επεξεργάζεται δισεκατομμύρια μηνύματα καθημερινά και έχει σημειώσει εξαιρετικές επιδόσεις στην προστασία των χρηστών από ανεπιθύμητα μηνύματα – λιγότερο από το 1% του συνόλου των ανεπιθύμητων μηνυμάτων στο Gmail καταλήγει να φτάσει στα εισερχόμενα ενός χρήστη. Όταν ένας αποστολέας ανεπιθύμητου περιεχομένου αποστέλλει έναν νέο τύπο ανεπιθύμητης αλληλογραφίας, τα συστήματά μας συχνά τον εντοπίζουν και τον αποκλείουν από τους λογαριασμούς Google εντός ορισμένων λεπτών. Με αυτόν τον τρόπο τα ανεπιθύμητα μηνύματα που ενδέχεται να βλάψουν τον υπολογιστή σας ή προσπαθούν να υποκλέψουν τα προσωπικά σας στοιχεία έχουν λιγότερες πιθανότητες να το πετύχουν.

Συνεργασία με φορείς για ζητήματα ασφαλείας

Γνωρίζουμε πόσο σημαντική είναι η προστασία και η ενημέρωση ειδικά των νέων σχετικά με τη χρήση του Διαδικτύου και θέλουμε να παρέχουμε ασφαλή εμπειρία και σε αυτούς. Στόχος μας είναι να προσφέρουμε σε γονείς και δασκάλους τα εργαλεία που θα τους βοηθήσουν να επιλέξουν το περιεχόμενο που θα βλέπουν τα παιδιά τους στο Διαδίκτυο και να παράσχουμε συμβουλές στις οικογένειες σε σχέση με τον τρόπο με τον οποίο μπορούν να παραμείνουν ασφαλείς στο Διαδίκτυο.

Γι' αυτό συνεργαζόμαστε στενά με φορείς και άλλους οργανισμούς που ασχολούνται με την προστασία των νέων και θέματα που απασχολούν αυτούς και τις οικογένειές τους. Στην Ελλάδα δημιουργήσαμε την πρωτοβουλία "Κέντρο Οικογενειακής Ασφάλειας" στη οποία συμμετέχουν (1) η Ανεξάρτητη Αρχή, Συνήγορος του Πολίτη / Συνήγορος του Παιδιού (2) η Ανοιχτή Γραμμή Καταγγελιών 'Safeline.gr' – Ελληνικό Κέντρο Ασφαλούς Διαδικτύου (3) η Δράση Ενημέρωσης & Επαγρύπνησης 'Saferinternet.gr' – Ελληνικό Κέντρο Ασφαλούς Διαδικτύου (4) η Ένωση «Μαζί για το Παιδί» (5) Το Χαμόγελο του παιδιού και (6) η Unicef.

Περισσότερες πληροφορίες για την πρωτοβουλία μπορείτε να βρείτε στο http://www.google.gr/goodtoknow/familysafety.

«Η ανάγκη της Ασφάλειας Ηλεκτρονικών Πληροφοριών Μύθος ή Πραγματικότητα;»

Απόστολος Πανδρούλας
Country Leader Symantec Hellas
Πάρις Κάσκας
Principal Presales Consultant, Symantec Hellas

Εισαγωγή

Στην σημερινή εποχή της παγκόσμιας οικονομικής και όχι μόνο κρίσης, οι απειλές ασφάλειας είναι πιο δυναμικές, πιο διεισδυτικές, πιο πολύπλοκες και πιο εγκληματικές από ποτέ. Οι κακόβουλοι χρήστες επιτίθενται με αστραπιαία ταχύτητα εκμεταλλευόμενοι τα τρωτά σημεία των συστημάτων, με απώτερο οικονομικό όφελος, δημιουργώντας μια αυξανόμενη ανησυχία προς τους επαγγελματίες της ασφάλειας.

Οι κρατικοί και ιδιωτικοί οργανισμοί καθώς και οι εταιρίες προσπαθούν να παρακολουθήσουν και να εντοπίσουν αυτές τις απειλές, να συγκεντρώσουν στοιχεία από πολλαπλές πηγές και στη συνέχεια να ιεραρχήσουν τις δράσεις και τις ενέργειες που θα πρέπει να παρθούν για την αντιμετώπιση αυτών.

Η Πρόκληση

Η πρόκληση υπήρξε με την εμφάνιση ιών που χτυπούν συστήματα που δεν είχαν πρόσβαση στο Διαδίκτυο, που μέχρι πρότινος θεωρούνταν απροσπέλαστα... Ποια είναι αυτά; Τα συστήματα SCADA. Αφελές; Ίσως...

Η Πρώτη Απειλή ήρθε τον Νοέμβριο του 2009

Night Dragon, μέσω του οποίου Hackers έκλεψαν ευαίσθητα δεδομένα από έξι Αμερικάνικες και Ευρωπαϊκές εταιρίες ενέργειας, μεταξύ των οποίων η Exxon Mobil, Royal Dutch Shell και η BP. Μια εταιρία έχασε οικονομικές πληροφορίες σχετικά με οικονομικές προσφορές φυσικού αερίου και πετρελαίου και ακόμα κλάπηκαν τοπογραφικοί χάρτες με πιθανές τοποθεσίες αποθεμάτων πετρελαίου αξίας εκατομμυρίων δολαρίων.

Η Δεύτερη Απειλή ήρθε στις 13 Ιουλίου 2010 όπου ανακαλύφθηκε ότι ιός προσπαθούσε να πάρει τον έλεγχο των βιομηχανικών υποδομών στον πλανήτη...

- *Stuxnet: Μάρτιος 2010, Στόχος: Εταιρίες Ενέργειας*
- *Flame: Μάιος 2012, Στόχος: Βιομηχανία Πετρελαίου*
- *Gauss: Αύγουστος 2012: Νέος Κατασκοπευτικός Ιός*

Ειδικά ο "Gauss" είναι ένας νέος ιός που επιτέθηκε στην Μέση Ανατολή κλέβοντας οικονομικές συναλλαγές, ηλεκτρονικό ταχυδρομείο και passwords. Ο ιός αυτός είναι μετάλλαξη των Stuxnet και Flame με εξειδίκευση σε τραπεζικές συναλλαγές αντιγράφοντας κωδικούς, εισχωρώντας σε

κοινωνικά δίκτυα, emails και λογαριασμούς κοινωνικής δικτύωσης. Χτυπήθηκαν ακόμα η Citibank και το PayPal.

Εταιρικές Κυβερνοεπιθέσεις

- Οι περισσότερες Κυβερνοεπιθέσεις έδειξαν απόλυες της τάξεως του 92%
- Πιστωτικές κάρτες, Κωδικοί, Χάρτες, Τοπογραφικά, Σχέδια κ.α. ήταν τα δεδομένα που κλάπηκαν
- Στο 84% των περιπτώσεων υπήρξαν πραγματικές απόλυες σε προσωπικά και ευαίσθητα δεδομένα
- Παραγωγικότητα, εισόδημα και εταιρική φήμη τα σημεία που είχαμε τις μεγαλύτερες απόλυες
- Το 80% των εταιριών είχαν απόλυες τουλάχιστον $195,000 ως αποτέλεσμα αυτών των επιθέσεων

Προστασία των «Ευαίσθητων Δεδομένων» είναι ο απώτερος σκοπός

Σήμερα στην εποχή της ταχείας επέκτασης και ανάπτυξης του διαδικτύου σχεδόν όλοι μπορούν να μοιράζονται την πρόσβαση και τη διάδοση της πληροφορίας, απεριόριστα και χωρίς όρια. Είτε μέσω φορητών υπολογιστών (laptops, netbooks) είτε μέσω έξυπνων κινητών συσκευών (iPhone, iPad, Blackberry, Windows Mobile, κλπ).

Οι εταιρίες και οι οργανισμοί ήδη εξαρτώνται από αυτήν την πραγματικότητα και η άμεση αυτή χρηστικότητα υποδηλώνει ότι «το γραφείο» μας μπορεί να είναι οπουδήποτε. Στο σπίτι, στο γραφείο, στο δρόμο, στην καφετέρια ή στο κέντρο διασκέδασης.

Συνεπώς, έχει καταστεί πιο δύσκολο από ποτέ, για εταιρίες και οργανισμούς η πρόληψη της απώλειας "ευαίσθητων δεδομένων".

Ποια όμως είναι αυτά;

- Πιστωτικές Κάρτες,
- ΑΦΜ, ΑΜΚΑ, Αριθμοί Ταυτότητας,
- Αρχεία Υγείας,
- Πνευματικά δικαιώματα,
- Εταιρικές Στρατηγικές,
- Οικονομικοί Έλεγχοι,
- Προσωπικά Δεδομένα,
- Οικονομικά Στοιχεία.

Μέχρι πρόσφατα η προσέγγιση της ασφάλειας ήταν η θωράκιση του δικτύου. Τώρα όμως το επίκεντρο βρίσκεται στην εξασφάλιση των ίδιων των δεδομένων και ένας από τους καλύτερους τρόπους για να γίνει αυτό είναι με τις λύσεις που ονομάζονται Πρόληψη Απώλειας των Δεδομένων.

Η πρόληψη της απώλειας των δεδομένων πρέπει να απαντήσει σε τρία θεμελιώδη ερωτήματα:

- Που βρίσκονται τα εμπιστευτικά δεδομένα;
- Πως χρησιμοποιούνται και από ποιον;
- Πώς γίνετε η πρόληψη της απώλεια δεδομένων;

Αναζήτηση:

Να εντοπίζει αυτόματα τα δεδομένα, βάση κανόνων και πολιτικών, και να δημιουργεί μια λίστα με τα "ευαίσθητα δεδομένα" του οργανισμού ή εταιρίας και αυτόματα να διαχειρίζεται την ταξινόμηση τους (εάν πρέπει να βρίσκονται εκεί που εντοπίστηκαν) και εάν υπάρξει ανάγκη να κρυπτογραφούνται ανάλογα.

Παρακολούθηση:

Σε πραγματικό χρόνο να διαπιστώνεται εάν οι χρήστες που διαχειρίζονται τα "ευαίσθητα δεδομένα" θα έπρεπε να έχουν πρόσβαση σε αυτά και εάν είναι μέσα στο δίκτυο της εταιρίας ή είναι συνδεδεμένοι απομακρυσμένα μέσω της κινητής συσκευή τους (πχ. iPhone/iPad ή μέσω vpn).

Προστασία:

Σε πραγματικό χρόνο αυτόματα να προστατεύει τα "ευαίσθητα δεδομένα" από πιθανές διαρροές ή μέσω απόρριψης ή μέσω κρυπτογράφησης.

π.χ.

Αντιγραφή λίστας με τηλέφωνα, ΑΦΜ, πιστωτικές κάρτες σε USB Flash Disks.

Απόρριψη εκτύπωσης αυτών των δεδομένων είτε μέσω print είτε μέσω print screen.

Απαγόρευση αποστολής συνημμένου εγγράφου μέσω ηλεκτρονικής αλληλογραφίας σε προσωπικούς λογαριασμούς (yahoo, hotmail, gmail, MSN, κλπ) και σε περίπτωση που πρέπει να γίνει να κρυπτογραφούνται ανάλογα.

Απαγόρευση μετακίνησης "ευαίσθητων δεδομένων" σε κοινωνικούς διαδικτυακούς τόπους όπως Facebook, twitter, κα.

Διαχείριση:

Να υπάρχει κεντρική διαχείριση με αυτοματισμούς και αναφορές στα γεγονότα και να ενημερώνονται οι αντίστοιχοι εμπλεκόμενοι (είτε χρήστες που διέπραξαν το γεγονός είτε προϊστάμενοι αυτών).

Συμπέρασμα

Η Πρόληψη Απώλειας των Δεδομένων μέσω της αναζήτησης, παρακολούθησης και της προστασίας των "εμπιστευτικών δεδομένων" όπου και να βρίσκονται αποθηκευμένα ή χρησιμοποιούνται είναι το σωστό βήμα για την αύξηση της παραγωγικότητας μιας εταιρίας ή οργανισμού και παράλληλα με την σωστή εκπαίδευση των υπαλλήλων και του προσωπικού να μπορέσει ο οργανισμός να ελαχιστοποιήσει την διαρροή των ευαίσθητων δεδομένων εκτός οργανισμού στον χρόνο.

Συνεχόμενη μείωση ρίσκου

«Information Protection by Design, ήτοι Σχεδίαση Συστημάτων με Ενσωματωμένη Δυνατότητα Προστασίας και Ακεραιότητας της Πληροφορίας»

Ιάκωβος Στ. Βενιέρης Καθηγητής Ε.Μ.Π.
Διευθυντής Εργαστηρίου Ευφυών Επικοινωνιών και Δικτύων Ευρείας Ζώνης,
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών,
Εθνικό Μετσόβιο Πολυτεχνείο
www.icbnet.ntua.gr

Περίληψη

Μολονότι αποτελεί διαχρονικό φαινόμενο, η κατάχρηση εταιρικών πληροφοριών στις μέρες μας διαφέρει ως προς τον τρόπο και την έκταση της συλλογής και επεξεργασίας των δεδομένων. Στο νέο τεχνολογικό περιβάλλον, ακόμα και οι πιο ώριμοι μηχανισμοί προστασίας αποδεικνύονται ανεπαρκείς. Ως η πλέον ενδεδειγμένη λύση αναδεικνύεται η σχεδίαση συστημάτων με ενσωματωμένη δυνατότητα προστασίας και ακεραιότητας της πληροφορίας.

Εισαγωγή

Η κατάχρηση εταιρικών πληροφοριών αποτελεί διαχρονικό φαινόμενο, έχοντας ως κίνητρο και αφετηρία την απάτη, το κέρδος, την απόκτηση ανταγωνιστικού πλεονεκτήματος, την εκπλήρωση κάποιας φιλοδοξίας, ή την εκδίκηση. Μάλιστα, ενδιαφέρον παρουσιάζει το γεγονός ότι η πλειονότητα των περιστατικών κατάχρησης αφορούν «εσωτερικές επιθέσεις», δηλαδή που πραγματοποιούνται από ή πρώην υπαλλήλους και άλλα στελέχη των οργανισμών.

Η ανάπτυξη των Τεχνολογιών Πληροφορικής και Επικοινωνιών κατά τα τελευταία χρόνια έχει αλλάξει τον τρόπο με τον οποίο ευαίσθητες εταιρικές πληροφορίες συλλέγονται και υφίστανται επεξεργασία, δημιουργώντας νέες προκλήσεις και ανάγκες σε ό,τι αφορά την προστασία των εταιρικών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και αθέμιτη χρήση. Στο πλαίσιο αυτό, η βιομηχανική κατασκοπεία στις μέρες μας λαμβάνει χώρα με τη χρήση νέων μηχανισμών, όπως είναι οι Διαδικτυακές επιθέσεις και εν γένει η εκμετάλλευση κενών ασφάλειας των πληροφοριακών συστημάτων, το «ψάρεμα» (phishing) μέσω, π.χ., παραπλανητικών μηνυμάτων ηλεκτρονικού ταχυδρομείου, η «κοινωνική μηχανική» (social engineering), και η χρήση τεχνολογιών εξόρυξης δεδομένων που βασίζεται στο συνδυασμό φαινομενικά «αθώων» πληροφοριών, την εξαγωγή συμπερασμάτων και τη συνακόλουθη εκμετάλλευσή τους.

Το νέο τεχνολογικό αλλά και επιχειρησιακό περιβάλλον διέπεται από εγγενή χαρακτηριστικά που το καθιστούν ευπαθές στην κατάχρηση εταιρικών πληροφοριών. Πρωτίστως, η πληροφορία είναι πλέον τυπικά ψηφιακή, κάτι που καθιστά ευκολότερη τη συλλογή, επεξεργασία και αντιγραφή της. Επιπλέον, γίνεται ευρεία χρήση εξωγενών πόρων, τόσο για την εκτέλεση συγκεκριμένων

εργασιών, όσο ακόμα και για τη διαχείριση και διατήρηση εταιρικών συστημάτων. Η τάση αυτή, γνωστή ως *εξωπορισμός* (outsourcing), έχει ως αποτέλεσμα τη διάθεση εταιρικών δεδομένων σε τρίτους φορείς και την έκθεσή τους σε κινδύνους. Πηγαίνοντας ένα βήμα παραπέρα, οι επιχειρησιακές διαδικασίες και διεργασίες καθίστανται ολοένα πιο πολύπλοκες, βασίζονται σε πολύπλοκα, κατανεμημένα και ολοκληρωμένα συστήματα και περιλαμβάνουν ετερογενείς οργανισμούς στην αλυσίδα της εκτέλεσής τους. Η τάση αυτή εντείνεται, λαμβάνοντας υπόψη και την αυξανόμενη διείσδυση των τεχνολογιών της υπολογιστικής «σύννεφου» (cloud computing).

Ως εκ τούτου, οι ανάγκες για τεχνολογίες που θα διασφαλίζουν την προστασία και ακεραιότητα της εταιρικής πληροφορίας είναι υψηλές όσο ποτέ άλλοτε. Ωστόσο, οι υφιστάμενοι μηχανισμοί αδυνατούν να ανταποκριθούν στις υποκείμενες απαιτήσεις, σε μεγάλο βαθμό επειδή λειτουργούν *συμπληρωματικά*. Για το λόγο αυτό, ως μελλοντική τάση διαφαίνεται η προστασία *by design*, όρος που αντανακλά τη σχεδίαση συστημάτων με ενσωματωμένη δυνατότητα προστασίας και ακεραιότητας της πληροφορίας.

Προστασία εταιρικής πληροφορίας

Θα μπορούσε να λεχθεί ότι η προστασία εταιρικών πληροφοριών αποτελεί το ανάλογο της προστασίας προσωπικών δεδομένων για τα φυσικά πρόσωπα, περιγράφοντας την ανάγκη των εταιρειών και άλλων οργανισμών για *ιδιωτικότητα*. Πράγματι, όπως σημείωνε ο Καθηγητής του Πανεπιστημίου Columbia Alan Westin το 1967, η ιδιωτικότητα συνίσταται στην «*αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων*». Ως εκ τούτου, πολλοί από τους μηχανισμούς ασφάλειας και προστασίας της ιδιωτικότητας βρίσκουν εφαρμογή και στο χώρο της προστασίας της εταιρικής πληροφορίας.

Εξέχουσα θέση μεταξύ των τεχνολογιών προστασίας πληροφοριών κατέχουν οι μηχανισμοί κρυπτογράφησής τους, οι οποίοι χρησιμοποιούνται για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στα υποκείμενα δεδομένα. Στο πλαίσιο αυτό, οι εν λόγω μηχανισμοί είναι ιδιαίτερα σημαντικοί για τη διασφάλιση του απορρήτου των δικτυακών συνδέσεων, την προστασία αρχείων, καθώς και των βάσεων δεδομένων. Επιπλέον, χρησιμοποιούνται ευρέως και αποτελεσματικά για τη διασφάλιση της ακεραιότητας των πληροφοριών, την ανίχνευση παραβιάσεων, καθώς για τη δημιουργία και επαλήθευση ψηφιακών υπογραφών.

Σημαντικές τεχνολογίες προστασίας είναι εκείνες της ανωνυμίας (anonymity) και της ψευδωνυμίας (pseudonymity). Η πρώτη ορίζεται σαν «η κατάσταση κατά την οποία κάποιο υποκείμενο δεν είναι αναγνωρίσιμο μεταξύ των μελών ενός συνόλου υποκειμένων, του *συνόλου ανωνυμίας*», ενώ η χρήση ψευδωνύμων, συχνά με τη διαμεσολάβηση κάποιας τρίτης οντότητας, αποτελεί εναλλακτική ή και συμπληρωματική λύση η οποία επιτρέπει την προσωποποίηση χωρίς χρήση της πραγματικής ταυτότητας κάποιας οντότητας. Οι πλέον ώριμες τεχνολογίες στο χώρο αυτό βασίζονται σε ισχυρούς κρυπτογραφικούς μηχανισμούς.

Ασφαλώς, δεν πρέπει να παραγνωρίζεται ο σημαντικός ρόλος των τεχνολογιών όπως είναι τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems — IDS) και τα Συστήματα Αποτροπής Εισβολών (Intrusion Prevention Systems — IPS), καθώς και των πολύ διαδεδομένων συστημάτων firewalls. Τα προαναφερθέντα συστήματα είναι ιδιαίτερα αποτελεσματικά σε ό,τι αφορά την προστασία από εξωτερικές απειλές, δηλαδή κακόβουλες ενέργειες που έχουν ως αφετηρία τους οντότητες εκτός του οργανισμού.

Στον αντίποδα, οι οργανισμοί απειλούνται από *εκ των έσω* κινδύνους, η προστασία από τους οποίους είναι κρίσιμη, ιδιαιτέρως δε εφόσον τα καταγεγραμμένα περιστατικά αναδεικνύουν ξεκάθαρα ότι στην πλειονότητά τους αφορούν τέτοιου είδους απειλές. Στο πλαίσιο αυτό, βασικό μηχανισμό αποτελεί η χρήση τεχνολογιών ελέγχου πρόσβασης, που εφαρμόζεται σε πληροφορίες, συστήματα, αλλά και φυσικούς χώρους ενός οργανισμού. Ο έλεγχος πρόσβασης συνιστά ουσιώδες συστατικό των εταιρικών πολιτικών ασφάλειας. Οι πολιτικές αυτές, είτε είναι εκφρασμένες σε φυσική γλώσσα, είτε χρησιμοποιούν κάποια εξελιγμένη τεχνολογία που επιτρέπει την αυτόματη εφαρμογή τους μέσω ειδικών συστημάτων, στοχεύουν στον αναλυτικό προσδιορισμό και συνακόλουθη εφαρμογή κανόνων με απώτερο σκοπό την ασφάλεια.

Ωστόσο, οι ως άνω περιγραφόμενοι μηχανισμοί, μολονότι η χρήση τους είναι αναγκαία, δεν επαρκούν από μόνοι τους, ιδιαίτερα στο νέο τεχνολογικό περιβάλλον που περιλαμβάνει ευρεία ψηφιοποίηση των εταιρικών πληροφοριών, πολύπλοκες ροές εργασίας και συνεργασία με άλλους οργανισμούς, συχνά πλήρως αυτοματοποιημένη. Για το λόγο αυτό, αναπτύσσονται νέες, καινοτόμες τεχνολογίες, οι οποίες διέπονται από την έννοια της *ενσωμάτωσης* των μηχανισμών προστασίας στα ίδια τα συστήματα.

Έλεγχος πρόσβασης

Κάθε παραβίαση ασφάλειας αφορά και περιλαμβάνει αθέμιτη πρόσβαση στα αντίστοιχα δεδομένα ή/και συστήματα· ως εκ τούτου, οι τεχνολογίες ελέγχου πρόσβασης αποτελούν μηχανισμούς ιδιαίτερης σημασίας. Για το λόγο αυτό, πληθώρα μηχανισμών και τεχνολογιών έχουν αναπτυχθεί και βρίσκονται σε χρήση. Σε αυτούς περιλαμβάνονται οι «κλασικοί», όπως ο Διακριτικός Έλεγχος Πρόσβασης (Discretionary Access Control — DAC), ο Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control — MAC) και ο πιο σύγχρονος Έλεγχος Πρόσβασης Βάσει Ρόλων (Role-Based Access Control — RBAC), αλλά και πιο εξελιγμένοι, όπως είναι οι PBAC, P-RBAC, PuRBAC, PRIME, OrBAC, PRISM, μεταξύ πολλών άλλων. Το ζήτημα όμως που αναμφισβήτητα τίθεται αφορά το κατά πόσον οι μηχανισμοί αυτοί επαρκούν για την προστασία της πληροφορίας στο νέο τεχνολογικό και επιχειρησιακό περιβάλλον.

Ένας σύγχρονος μηχανισμός ελέγχου πρόσβασης πρέπει να λαμβάνει υπόψη διάφορες παραμέτρους, να συνδυάζει γεγονότα και καταστάσεις ακόμα και με μη προφανή τρόπο, και εν τέλει να είναι σε θέση να διαθέτει απαντήσεις και να συνυπολογίζει μία σειρά από ερωτήματα προτού επιτρέψει την πρόσβαση σε κάποιο πόρο, όπως: ποιος πόρος; ποιος αποκτά πρόσβαση; πρόσβαση τι είδους; πότε; (από) που; πώς; γιατί; ποιες ενέργειες έχουν προηγηθεί; ποιες ενέργειες πρέπει να έχουν προηγηθεί; ποιες ενέργειες πρέπει να ακολουθήσουν; ποιες ενέργειες δεν πρέπει να ακολουθήσουν;

Τα παραπάνω υπονοούν ιδιαίτερες ιδιότητες που θα πρέπει να χαρακτηρίζουν τους μηχανισμούς ελέγχου πρόσβασης, και τις πολιτικές ασφάλειας γενικότερα, προκειμένου να καθίστανται αποτελεσματικοί στο σύγχρονο περιβάλλον. Οι ιδιότητες αυτές, μεταξύ άλλων, περιλαμβάνουν:

- Την ύπαρξη σημασιολογικής βάσης γνώσης που θα κατευθύνει τις αποφάσεις εξουσιοδοτήσεων και παροχής δικαιώματος πρόσβασης
- Τη δυνατότητα συσχετίσεων ενεργειών, τόσο εκείνων που έχουν (ή δεν έχουν) λάβει χώρα στο παρελθόν, όσο και εκείνες που θα πρέπει να (ή να μην) ακολουθήσουν στο μέλλον
- Την αξιοποίηση πληροφοριών «ευρύτερου πλαισίου» (context) και γεγονότων πραγματικού χρόνου στη λήψη αποφάσεων

- Τη δυνατότητα εφαρμογής αρχών όπως εκείνες του διαχωρισμού των καθηκόντων, της διασύνδεσης των καθηκόντων, και των ελαχίστων προνομίων

Τέλος, οι μηχανισμοί θα πρέπει να είναι δυνατό να ενσωματώνονται στα αντίστοιχα συστήματα ως εγγενή χαρακτηριστικά, όπως περιγράφεται στην επόμενη Ενότητα.

Ενσωμάτωση δυνατοτήτων προστασίας και ακεραιότητας

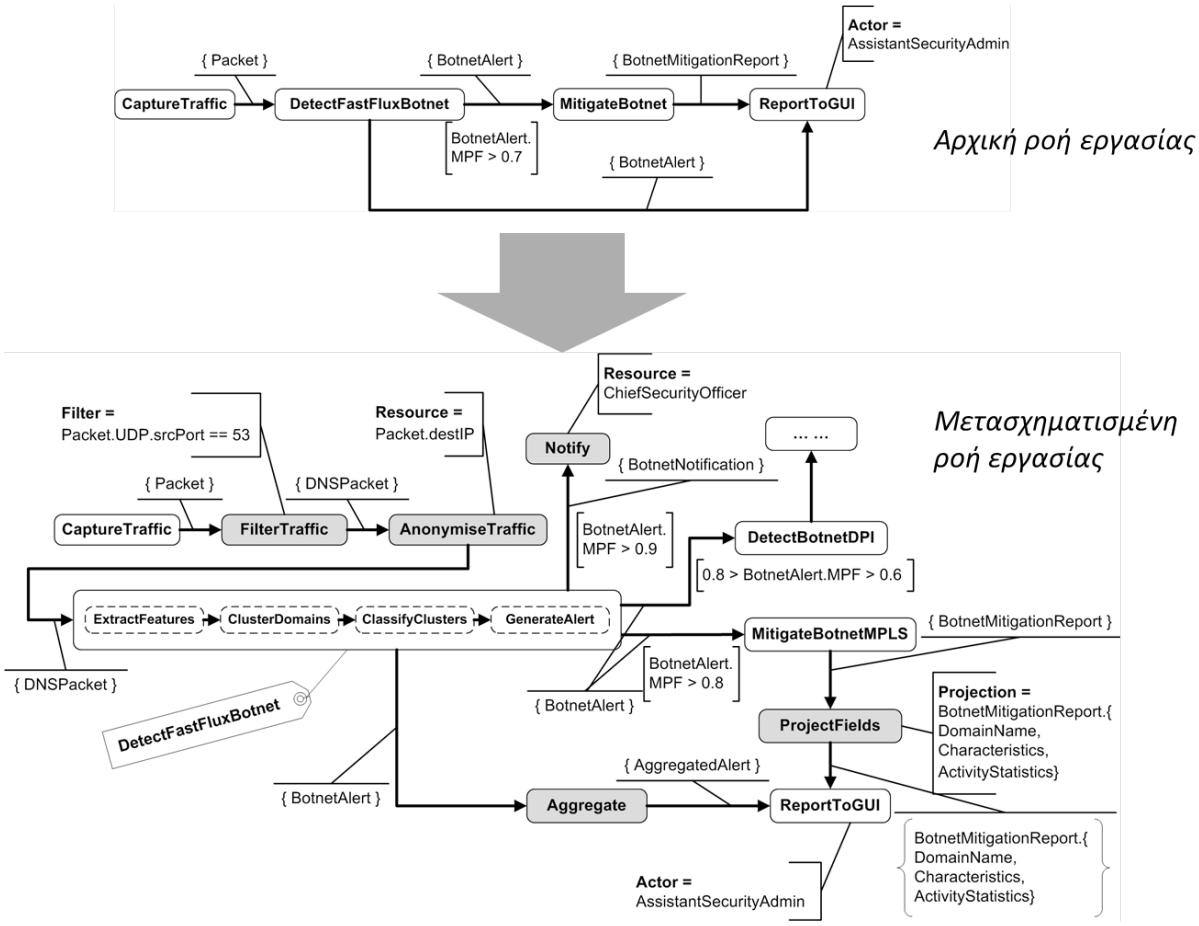
Ο όρος *by design* αφορά στην ανάπτυξη συστημάτων με εγγενώς ενσωματωμένες τις δυνατότητες προστασίας και ακεραιότητας της πληροφορίας. Στο πλαίσιο αυτό, οι υποκείμενες απαιτήσεις λειτουργούν ως οδηγός στο σχεδιασμό και ενσωμάτωση των σχετικών δυνατοτήτων στο νωρίτερο δυνατό στάδιο του κύκλου ζωής των νέων τεχνολογιών.

Σύμφωνα με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ, «[η προστασία] *απαιτεί τη λήψη κατάλληλων τεχνικών μέτρων και οργάνωση κατά τη στιγμή τόσο του σχεδιασμού των τεχνικών επεξεργασίας όσο και της εκτέλεσης της επεξεργασίας*». Η θεώρηση αυτή υπαγορεύει μία προσέγγιση η οποία θα εξασφαλίζει την τήρηση των κανόνων προστασίας της πληροφορίας σε όλα τα στάδια του κύκλου ζωής ενός συστήματος λογισμικού, δηλαδή όχι μόνο κατά την εκτέλεση αλλά και κατά τον αρχικό σχεδιασμό και την υλοποίησή του.

Στο πλαίσιο αυτό, οι μηχανισμοί ελέγχου και ασφάλειας, όπως περιγράφηκαν στην παραπάνω Ενότητα, θα πρέπει να χρησιμοποιούνται ως *οδηγοί* προκειμένου τα συστήματα και οι υποστηριζόμενες από αυτά διαδικασίες να καθίστανται εγγενώς ασφαλείς. Για παράδειγμα, θεωρώντας συστήματα που διαλειτουργούν με κατανεμημένο τρόπο βάσει των αρχών των Αρχιτεκτονικών Βασισμένων σε Υπηρεσίες (Service-Oriented Architectures — SOA) συνιστώντας, τελικά, ένα πολύπλοκο σύστημα, οι φάσεις που προκύπτουν είναι οι ακόλουθες:

- Αυτόματος έλεγχος συμμόρφωσης των επιχειρησιακών διαδικασιών (ροών εργασίας — workflows) με τις πολιτικές ασφάλειας, και, σε δεύτερο στάδιο
- Αυτόματος μετασχηματισμός των ροών εργασίας σύμφωνα με τις πολιτικές ασφάλειας, συμπεριλαμβανομένων διορθωτικών αλλαγών, όπως μετατροπή εργασιών, αφαίρεση εργασιών, ή προσθήκη λειτουργιών για ρύθμιση της κυκλοφορίας των πληροφοριών

Το παρακάτω Σχήμα παρουσιάζει ένα παράδειγμα μετασχηματισμού μιας απλής επιχειρησιακής ροής εργασιών βάσει της υποκείμενης πολιτικής ασφάλειας. Μεταξύ άλλων, πραγματοποιούνται αλλαγές που αφορούν στην προσθήκη εργασιών οι οποίες φιλτράρουν, ελαττώνουν και καθιστούν ανώνυμα τα αντίστοιχα δεδομένα, αποστέλλουν κατάλληλες ειδοποιήσεις σε περιπτώσεις εμφάνισης γεγονότων, αλλά και επιβάλουν την υπό συνθήκη εκτέλεση, έχοντας ως αποτέλεσμα το μετασχηματισμό της ροής σε μία διαδικασία η οποία είναι πλήρως συμβατή με την πολιτική ασφάλειας.



Σχήμα 1: Παράδειγμα μετασχηματισμού ροής εργασιών βάσει πολιτικής ασφάλειας — πηγή: E. I. Papagiannakopoulou, M. N. Koukovini, G. V. Lioudakis, J. Garcia-Alfaro, D. I. Kaklamani, I. S. Venieris, F. Cuppens, N. Cuppens-Boulahia, "A Privacy-Aware Access Control Model for Distributed Network Monitoring", *Computers & Electrical Engineering*, 2013.

Συμπεράσματα

Αδιαμφισβήτητα, οι Τεχνολογίες Πληροφορικής και Επικοινωνιών επιφέρουν σημαντικά οφέλη στη λειτουργία των εταιρειών. Από την άλλη όμως, θέτουν σε κίνδυνο τις εταιρικές πληροφορίες και διευκολύνουν την αθέμιτη συλλογή τους και τη συνακόλουθη κατάχρηση. Δεδομένου ότι οι σύγχρονοι μηχανισμοί προστασίας αποδεικνύονται ανεπαρκείς σε ό,τι αφορά την αποτελεσματικότητά τους στο νέο τεχνολογικό περιβάλλον, νέες τεχνολογίες αναπτύσσονται. Μία σχετική τάση η οποία κατέχει εξέχουσα θέση μεταξύ αυτών, αφορά τη σχεδίαση συστημάτων με ενσωματωμένες τις δυνατότητες για την προστασία και την ακεραιότητα της πληροφορίας, θεωρώντας τις υποκείμενες απαιτήσεις σε όλα τα στάδια του κύκλου ζωής των συστημάτων.

«Και μετά την παραβίαση ασφάλειας, τι;»

Καθηγητής **Σωκράτης Κάτσικας**
Τμήμα Ψηφιακών Συστημάτων Πανεπιστήμιο Πειραιώς

Καλημέρα σας κυρίες και κύριοι.

Πριν ξεκινήσω –και δεν το λέω τυπικά– θα ήθελα να ευχαριστήσω την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, το Μανώλη Σφακιανάκη και τους συνεργάτες του για τη σημερινή πρόσκληση, αλλά και για τη δουλειά που κάνουν. Προσωπικά, αλλά –είμαι βέβαιος– και πολλοί άλλοι από μάς αισθανόμαστε μάλλον ασφαλέστεροι επειδή υπάρχουν αυτοί οι άνθρωποι.

Στις σημερινές παρουσιάσεις εκλεκτών συναδέλφων θα ακούσετε τρόπους πρόληψης παραβιάσεων της ασφάλειας πληροφοριακών συστημάτων. Στη δική μου ομιλία θα προσπαθήσω να καλύψω το τι πρέπει να κάνουμε στην περίπτωση που, παρά τα προληπτικά μέτρα που έχουν ληφθεί, συμβεί ένα περιστατικό παραβίασης ασφαλείας.

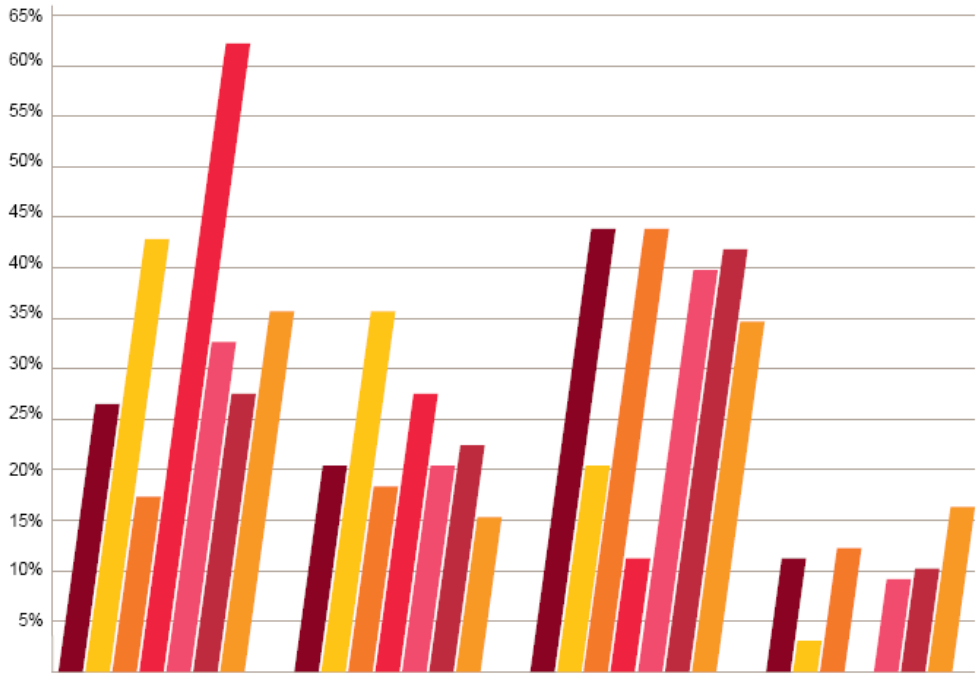
Τι είναι όμως «περιστατικό ασφαλείας» (Information Security Incident); Ο ορισμός του δίνεται περιγραφικά στο πρότυπο ISO/IEC TR 18044:2004 και στο ISO 27002, το οποίο αναφέρεται σε security management. Συγκεκριμένα, περιστατικό ασφάλειας συμβαίνει όταν συμβεί ένα ή περισσότερα απρόσμενα γεγονότα ασφάλειας. Τα γεγονότα ασφάλειας είναι μικρότερης έκτασης περιστατικά, που έχουν όμως σημαντική πιθανότητα να επηρεάσουν επιχειρησιακά τη λειτουργία του οργανισμού και να απειλήσουν την ασφάλεια των πληροφοριών.

Από τον ορισμό γίνεται φανερό ότι περιστατικό ασφάλειας μπορεί να είναι ένα περιστατικό το οποίο δεν έχει οδηγήσει ακόμα σε δυσλειτουργία, αλλά πρόκειται να οδηγήσει, με σημαντική πιθανότητα και, επομένως, χρειάζεται να αντιδράσουμε σε αυτό.

Το ακόλουθο γράφημα (Σχήμα 1) είναι από την τελευταία μελέτη της PriceWaterhouse Cooper για την Ελλάδα, που έγινε στο πλαίσιο του global information security survey και δείχνει πόσα περιστατικά ασφάλειας αναφέρθηκαν από αυτούς που συμμετέχουν στην έρευνα, τον περασμένο χρόνο.

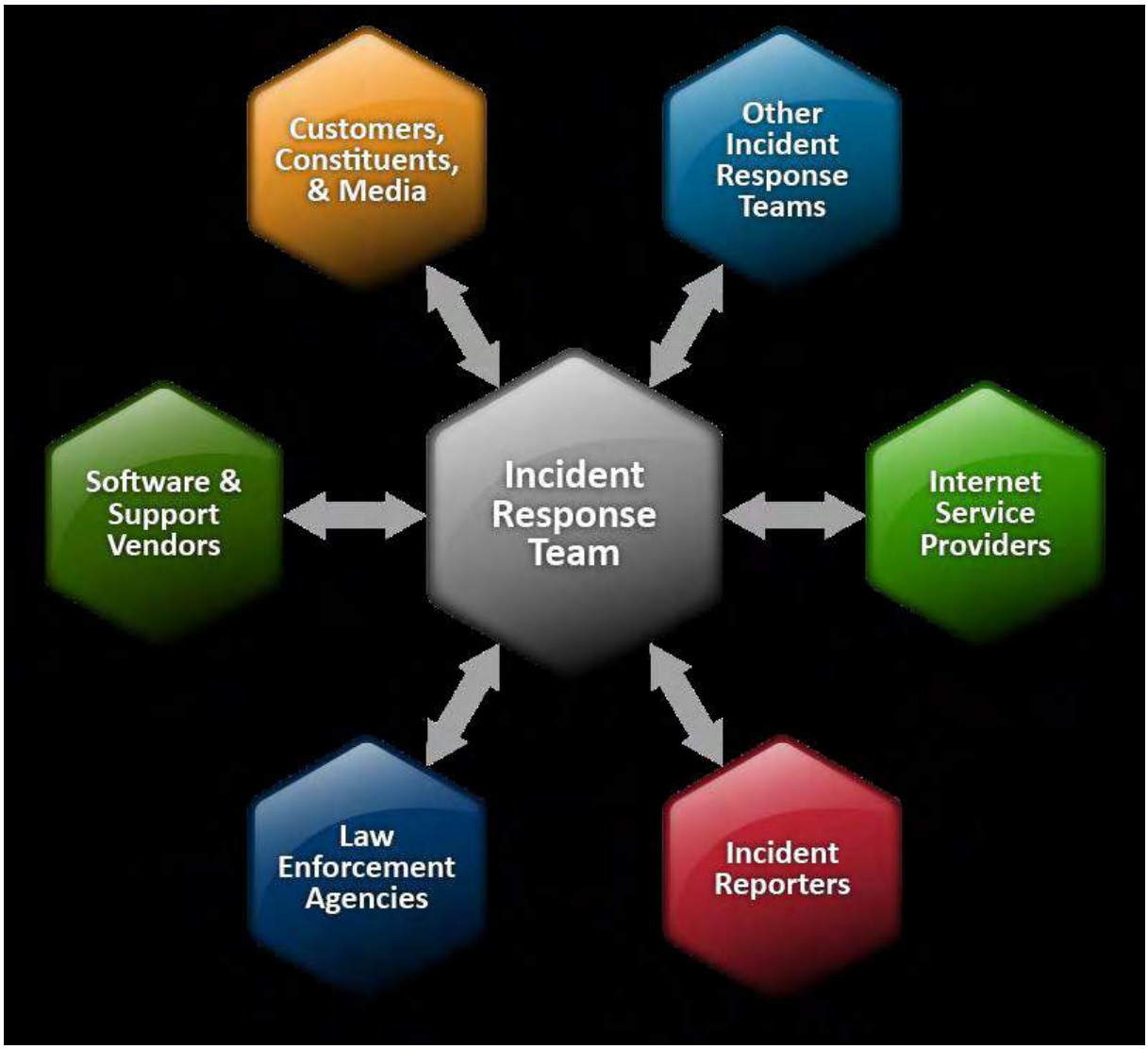
Παρατηρούμε ότι στην Ελλάδα δεν υπάρχει κανένα περιστατικό τον περασμένο χρόνο σε ποσοστό 61% , ένα έως 2 περιστατικά σε ποσοστό 27%, πάνω από 3 περιστατικά σε ποσοστό 11% και το ποσοστό του «δεν απαντώ» είναι 0. Δυστυχώς όμως, στην πραγματικότητα δεν είμαστε τόσο ασφαλείς. Δυστυχώς, το ψηλό ποσοστό επιχειρήσεων που δεν υπέστησαν περιστατικό οφείλεται –για παράδειγμα– στο ότι ένας οργανισμός δεν κατάλαβε ότι έγινε περιστατικό παραβίασης ασφαλείας και αυτό είναι ακόμα χειρότερο. Ένας δεύτερος πιθανός λόγος είναι ότι το περιστατικό εντοπίστηκε αλλά ο οργανισμός δεν θέλησε να το παραδεχτεί. Ίσως αυτό έχει μεγαλύτερη σημασία, γιατί στην ίδια σελίδα που υπάρχει αυτό το γράφημα στο report, το οποίο είναι διαθέσιμο στο διαδίκτυο, αναφέρεται ότι το 65% αυτών που υπέστησαν περιστατικά ασφαλείας στην Ελλάδα δεν τα ανέφεραν. Στον αντίποδα είναι η Κίνα όπου το 71% αυτών που υπέστησαν περιστατικό το ανέφεραν. Γιατί άραγε στην Ελλάδα σε τόσο μεγάλα ποσοστά δεν αναφέρουμε τα περι-

στατικά που παθαίνουμε; Καθένας μπορεί να δώσει πολλές απαντήσεις. Σύμφωνα με την τοποθέτηση επί του θέματος του Μανώλη Σφακιανάκη, στο ίδιο report, το φαινόμενο αποδίδεται κυρίως όχι στο ότι δεν θέλουν οι ελληνικές επιχειρήσεις να χάσουν φήμη αλλά στο ότι έχουν αναγνωρίσει την ανεπάρκεια του νομικού πλαισίου και γι' αυτό δεν αναφέρουν περιστατικά ασφάλειας.



	Κανένα	1 έως 2	πάνω από 3	Δ/Α
Ευρωζώνη	26%	20%	43%	11%
Κίνα	42%	35%	20%	3%
Γερμανία	17%	18%	43%	12%
Ελλάδα	61%	27%	11%	0%
Ιταλία	32%	20%	39%	9%
Ισπανία	27%	22%	41%	10%
Αγγλία	35%	15%	34%	16%

Σχήμα 1: Συχνότητα εμφάνισης περιστατικών ασφάλειας

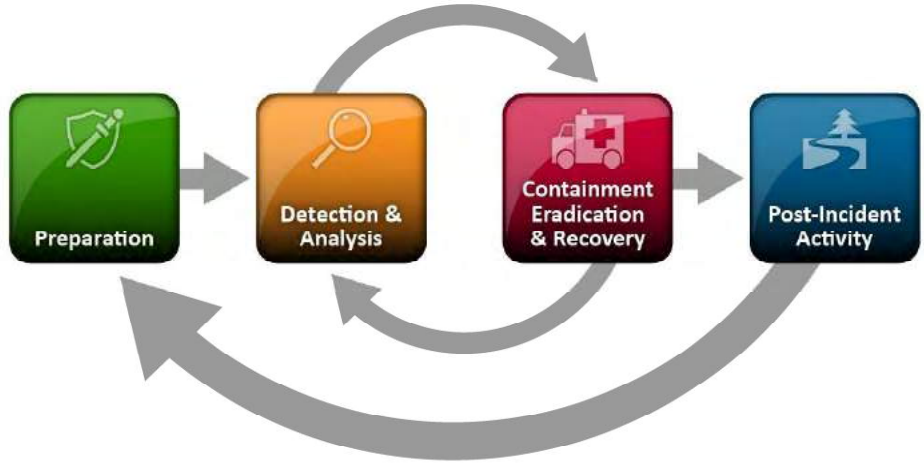


Σχήμα 2: Εμπλεκόμενα μέρη στη διαχείριση περιστατικών

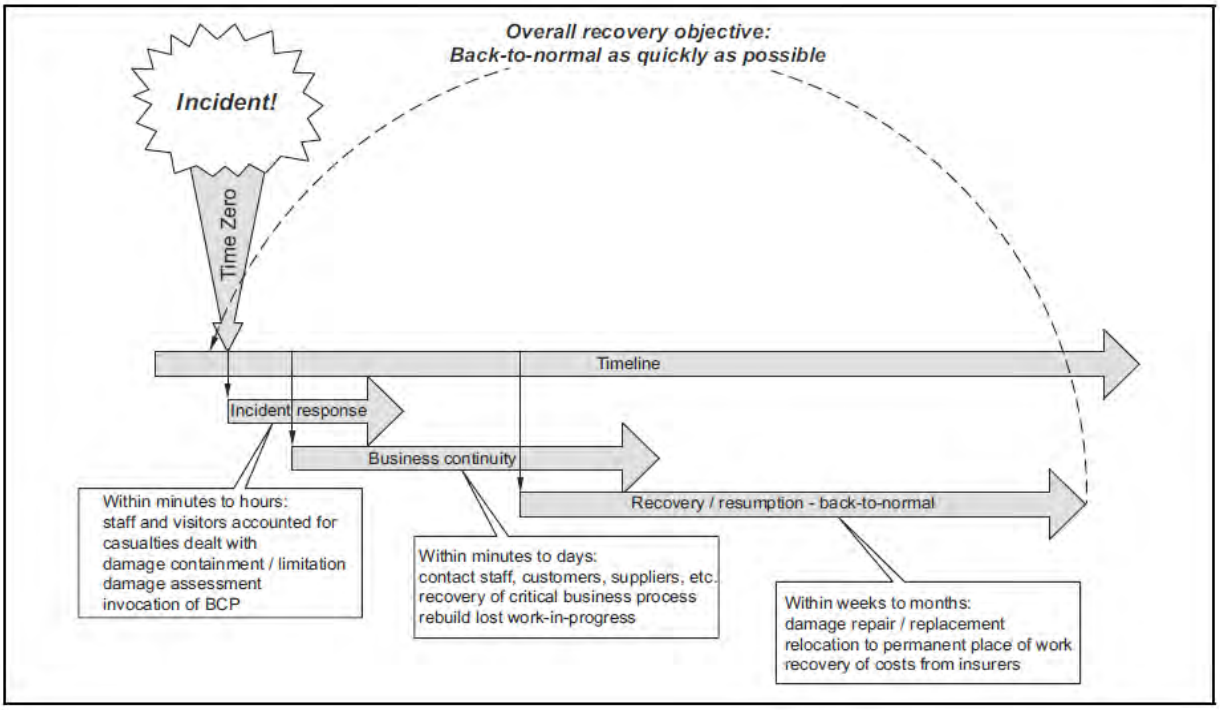
Γιατί όμως μας απασχολεί τόσο πολύ το πώς χειριζόμαστε περιστατικά; Το σχήμα 2 περιέχεται στο πρότυπο NIST SP 800-61 rev2 του αμερικανικού οργανισμού προτυποποίησης (National Institute of Standards and Technology – NIST), που αφορά το πώς χειριζόμαστε περιστατικά ασφάλειας. Σχετικό είναι και το πρότυπο ISO 27035, αλλά βρίσκεται σε διαδικασία αναθεώρησης η οποία τέλειωσε και τώρα θα ξεκινήσει να εφαρμόζεται, γι' αυτό προτίμησα να ακολουθήσω το NIST SP 800-61. Στο εν λόγω σχήμα παρουσιάζεται πόσοι εμπλέκονται στην πορεία διαχείρισης ενός περιστατικού ασφάλειας. Στο κέντρο είναι η ομάδα η οποία θα αναλάβει να χειριστεί το περιστατικό. Γύρω – γύρω όμως υπάρχουν άλλες ομάδες, οι πάροχοι της δικτυακής υπηρεσίας με τους οποίους συνεργάζεται ο οργανισμός, αυτοί οι οποίοι αναφέρουν τα περιστατικά, οι διωκτικές αρχές, οι προμηθευτές και βεβαίως οι πελάτες και τα μέσα ενημέρωσης. Όλο αυτό το τοπίο δίνει μια καλή ιδέα της πολυπλοκότητας του πράγματος, που οδηγεί στην ανάγκη να υπάρχει ένα είδος διαχείρισης των περιστατικών.

Περνώντας στον κύκλο ζωής του περιστατικού, που φαίνεται στο σχήμα 3 (πάλι από το NIST SP 800-61), εντοπίζουμε ότι ένα περιστατικό δεν ξεκινάει από τότε που συμβαίνει. Ξεκινάει από την προετοιμασία που κάνει ο οργανισμός ώστε, όταν συμβεί το περιστατικό, να μπορέσει να το αντιμετωπίσει. Στη συνέχεια περνά μια φάση ανίχνευσης και ανάλυσης. Ένα σημαντικό τμήμα της διαδικασίας είναι η επαλήθευση του περιστατικού, καθώς μερικές φορές νομίζουμε ότι έχουμε υποστεί περιστατικό παραβίασης ασφάλειας, ενώ στην πραγματικότητα συμβαίνει κάτι άλλο. Το επόμενο στάδιο είναι ο περιορισμός του περιστατικού και η άρση των συνεπειών του και βεβαίως η ανάκαμψη του οργανισμού από τις όποιες αρνητικές συνέπειες έχει ήδη υποστεί. Το τελευταίο στάδιο είναι οι διαδικασίες που πρέπει να αναπτυχθούν μετά το περιστατικό, που στην πραγματικότητα είναι το τι μάθαμε από την αντιμετώπιση ενός περιστατικού, τι πρέπει να αλλάξουμε, να κάνουμε καλύτερο ώστε την επόμενη φορά να μπορέσουμε να το αντιμετωπίσουμε καλύτερα. Κεντρική, συνεπώς, δράση είναι ο περιορισμός του περιστατικού και η άρση των συνεπειών του. Αν υποθέσουμε ότι ένα περιστατικό είναι σε εξέλιξη, είναι προφανές ότι ο οργανισμός που το υφίσταται έχει την ευθύνη να σταματήσει την ύπαρξη και την εξέλιξή του. Πως θα το κάνει όμως αυτό; Χρειάζεται μια πολύ ξεκάθαρη διαδικασία για το πώς θα αντιμετωπισθεί ένα περιστατικό, όπως επίσης και πολύ ξεκάθαρες διαδικασίες για το ποιον θα ειδοποιήσει από τις διωκτικές αρχές. Σημαντικό είναι να ειδοποιήσει τα θεσμικά όργανα που είναι επιφορτισμένα να αναλάβουν τη διαχείριση του περιστατικού, αφενός μεν την ομάδα της αστυνομίας που ξέρει πάρα πολύ καλά να κάνει τη δουλειά της, αλλά και τις ανεξάρτητες αρχές που από το νόμο καθορίζονται ως οι θεσμικοί υπεύθυνοι για να χειρίζονται τέτοια ζητήματα (τόσο η ΑΠΔΠΧ όσο και η ΑΔΑΕ).

Ξαναγυρίζοντας στον χειρισμό των περιστατικών και αναφερόμενοι στο σχήμα 4, διακρίνουμε 2 διακριτές φάσεις. Μέχρι τώρα μίλησα για την πρώτη. Στον λεγόμενο «χρόνο μηδέν», δηλαδή τον χρόνο εκδήλωσης του περιστατικού, ξεκινά η αντιμετώπισή του, φάση που μπορεί να διαρκέσει μερικά λεπτά έως κάποιες ώρες, ανάλογα με την έκταση του περιστατικού και τη δυσκολία αντιμετώπισής του. Κάπου στη μέση ξεκινά η φάση της επιχειρησιακής συνέχειας, δηλαδή της εφαρμογής του σχεδίου επιχειρησιακής συνέχειας (Business continuity). Το σχέδιο αυτό είναι προφανώς σχετιζόμενο με το σχέδιο αντιμετώπισης του περιστατικού, αλλά σαφώς διακριτό, γιατί βλέπετε και χρονικά πως διαδέχονται η μία φάση την άλλη. Και αυτό στον πραγματικό κόσμο ακολουθείται από ένα τρίτο σχέδιο, το οποίο συνήθως αναφέρεται ως σχέδιο ανάκαμψης από καταστροφή (disaster recovery plan).



Σχήμα 3: Κύκλος ζωής περιστατικού



Σχήμα 4: Φάσεις διαχείρισης περιστατικού

Επικεντρώνοντας στην επιχειρησιακή συνέχειαν, ας δούμε τον ορισμό της με βάση το ISO 22300, μια ομάδα προτύπων που αναφέρονται στην επιχειρησιακή συνέχεια: Επιχειρησιακή συνέχεια είναι η ικανότητα του οργανισμού να συνεχίζει να λειτουργεί, να παραδίδει προϊόντα ή υπηρεσίες σε κάποιο αποδεκτό προκαθορισμένο επίπεδο μετά από ένα αποδιοργανωτικό συμβάν. Το πρότυπο δεν αναφέρεται μόνο σε επεισόδια παραβίασης ασφάλειας, αλλά σε οποιοδήποτε επεισόδιο που διαταράσσει τη λειτουργία του οργανισμού. Άρα, πριν συμβεί ο,τιδήποτε θα πρέπει ο οργανισμός να έχει μελετήσει ποιο είναι το minimum αποδεκτό επίπεδο παράδοσης προϊόντων η υπηρεσιών που παράγει ή παρέχει και να φτιάξει ένα σχέδιο το οποίο θα του διασφαλίζει μετά τη ζημιά ότι αυτό το επίπεδο θα μπορεί να συνεχίσει να το παρέχει, μέχρις ότου ενεργοποιηθεί το σχέδιο ανάκαμψης από την καταστροφή που θα τον επαναφέρει στο επίπεδο λειτουργίας του όπως ήταν πριν την καταστροφή. Τι μπορεί να συμβεί αν τέτοιο σχέδιο δεν υπάρχει; Τα στατιστικά είναι αμείλικτα:

- 43% των οργανισμών που αντιμετώπισαν μεγάλες καταστροφές δεν ξαναλειτούργησαν μετά το γεγονός.
- 80% των οργανισμών μετά από εκτεταμένη καταστροφή διακόπτουν τη λειτουργία τους μέσα σε πέντε έτη.
- 29% κλείνουν μέσα σε τρία έτη.
- 75% των οργανισμών που υφίστανται διακοπή των υπηρεσιών πληροφορικής και επικοινωνιών διακόπτουν τη λειτουργία τους μέσα σε 14 ημέρες.
- Το μέσο κόστος ανά ώρα διακοπής λειτουργίας, σε όλους τους κλάδους, είναι 1.000.000 USD.

Το πλήθος των εταιρειών που στεγάζονταν στους δίδυμους πύργους στη Νέα Υόρκη και που έκλεισαν μετά από κάποια χρόνια επειδή δεν είχαν σχέδιο επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή, ή –πράγμα που είναι τραγικότερο– το είχαν αλλά ήταν φυλαγμένο μέσα στον ίδιο χώρο, μέσα στους δίδυμους πύργους, είναι δυστυχώς μεγάλο.

Για να εφαρμόσουμε σχέδιο ανάκαμψης από καταστροφή, πρέπει πρώτα να το διαμορφώσουμε και για να το διαμορφώσουμε χρειάζονται τρία βασικά συστατικά: Το σχέδιο επιχειρησιακής συνέχειας, το οποίο παίρνει και πληροφορίες από το σχέδιο διαχείρισης επικινδυνότητας και τα μέτρα ασφάλειας. Υπάρχει κάτι άλλο εδώ το οποίο λέγεται ανάλυση επιχειρησιακών επιπτώσεων (business impact analysis) και στην πραγματικότητα δεν είναι τίποτα άλλο από την καταγραφή των κρίσιμων λειτουργιών του οργανισμού και την ανάλυση του πώς αυτές συνδέονται με τους πληροφορικούς πόρους.

Ένας τέτοιος σχεδιασμός ανάκαμψης από καταστροφή

- Εξασφαλίζει την επιβίωση της επιχείρησης
- Ελαχιστοποιεί την απώλεια πληροφοριών
- Ελαττώνει το κόστος ανάκαμψης
- Ελαχιστοποιεί τον χρόνο μη λειτουργίας
- Δίνει τη δυνατότητα αποφυγής διαφυγόντων κερδών
- Διατηρεί τους σημαντικούς πελάτες
- Δίνει τη δυνατότητα αποφυγής επιβολής ποινικών ρητρών
- Στέλνει ένα ισχυρό μήνυμα στον ανταγωνισμό
- Διαφυλάσσει τη φήμη εταιρείας
- Αποτελεί προπομπό πιστοποίησης κατά BS 7799-2 : 2007

Προφανώς υπάρχει ένα κόστος για τα παραπάνω. Είναι ασφαλώς επιχειρηματική απόφαση το αν κάποιος θα εμπλακεί σε αυτή την ιστορία ή απλώς θα πάρει το ρίσκο του να υποστεί ένα περιστατικό και να μην μπορεί να το αντιμετωπίσει. Μάλιστα τελευταία στην Ελλάδα υπάρχει τουλάχιστον μία ασφαλιστική εταιρεία η οποία καλύπτει πληροφοριακά συστήματα. Είναι πρόσφατη εξέλιξη, νομίζω τους τελευταίους μήνες. Το πρόβλημα είναι ότι τα αντίστοιχα κόστη συνήθως δεν γίνονται αποδεκτά από τις ασφαλιστικές εταιρείες και θέλει πάρα πολύ μεγάλη προσοχή για το τι γίνεται αποδεκτό και το τι δεν γίνεται.

Ο κύκλος ζωής ενός σχεδίου επιχειρησιακής συνέχειας περιλαμβάνει τις εξής φάσεις:

- Διαμόρφωση δήλωσης πολιτικής
- Διεξαγωγή ανάλυσης επιχειρησιακών επιπτώσεων (Business Impact Analysis – BIA)
- Αναγνώριση προληπτικών μέτρων
- Επιλογή στρατηγικών ανάκαμψης
- Ανάπτυξη σχεδίου επιχειρησιακής συνέχειας
- Δοκιμή σχεδίου, εκπαίδευση και ασκήσεις
- Συντήρηση σχεδίου

Κλείνοντας, θα ήθελα να επαναλάβω μερικές διαπιστώσεις:

- Η επιχειρησιακή συνέχεια είναι ένα από τα τρία σημαντικότερα θέματα στην ατζέντα των Διευθυντών Πληροφορικής (CIO)
- Λιγότερο από το 50% των οργανισμών διαθέτουν επιχειρησιακά προγράμματα (πλάνα) ανάκτησης της ομαλής λειτουργίας και τουλάχιστον το 90% δεν τα έχει θέσει σε εφαρμογή.
- Ο χρόνος ανάκτησης λειτουργίας σχεδόν πάντα υποτιμάται.
- Τα κόστη ανάκτησης δεν καλύπτονται πάντα από τους ασφαλιστικούς Οργανισμούς

Σας ευχαριστώ.

«Μπορώ να προστατεύσω αποτελεσματικά τα κρίσιμα επιχειρησιακά δεδομένα μου;»

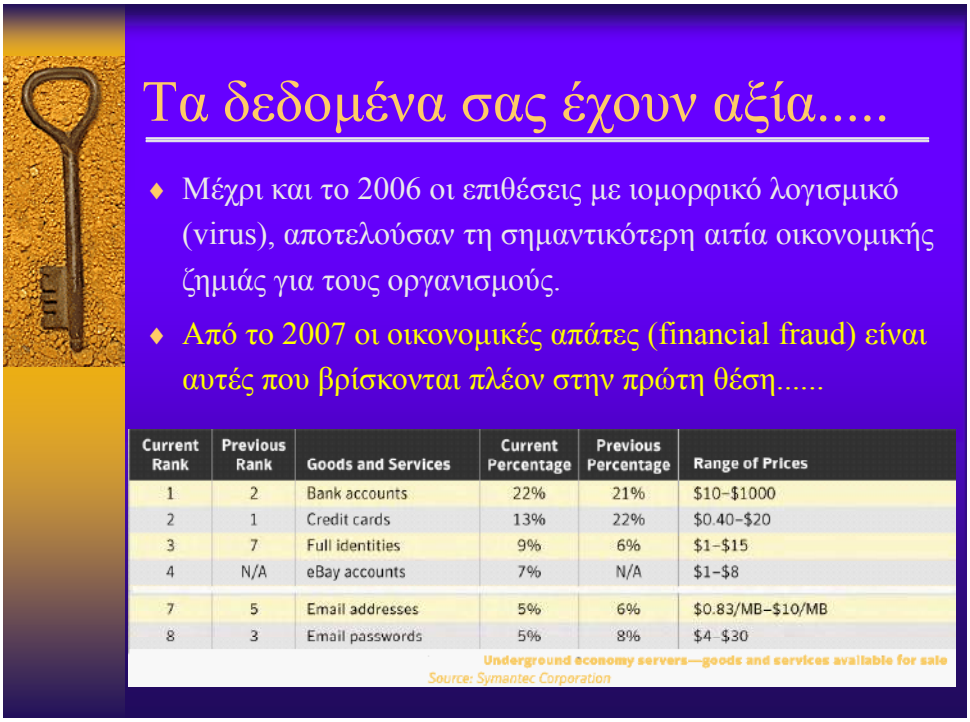
Επίκουρος Καθηγητής **Κων/νος Λαμπρινουδάκης**
Τμήμα Ψηφιακών Συστημάτων Πανεπιστήμιο Πειραιώς

Θα ήθελα και εγώ με την σειρά μου να ευχαριστήσω τον κ. Σφακιανάκη προσωπικά και την Υπηρεσία για την πρόσκληση αυτή η οποία ήταν μεγάλη τιμή για μένα.

Να ξεκινήσω μένοντας στην πρώτη διαφάνεια. As προσπαθήσουμε να ερμηνεύσουμε λίγο τον τίτλο: :"Μπορώ να **προστατεύσω αποτελεσματικά** τα **κρίσιμα επιχειρησιακά δεδομένα** μου;»

As μείνω πρώτα στη λέξη « προστατεύσω «. Φαντάζομαι ότι το πρώτο πράγμα το οποίο έρχεται στο μυαλό κάποιου όταν σκέφτεται εάν μπορεί να προστατεύσει το πληροφοριακό του σύστημα είναι αν επαρκούν τα τεχνικά μέτρα ασφάλειας. Όμως, η ασφάλεια δεν είναι, σε καμία περίπτωση , αποκλειστικά και μόνο τεχνικό θέμα. Συνεπώς, η υλοποίηση – αγορά εγκατάσταση κάποιων τεχνικών αντιμέτρων και μόνο, δεν μπορεί να εξασφαλίσει την αποτελεσματική προστασία του συστήματος μας. Στη συνέχεια, στο τίτλο φαίνεται η λέξη «αποτελεσματικά» . Η λέξη αυτή επίσης μπορεί να οδηγήσει στη σκέψη του κατά πόσο είμαστε 100 % ασφαλής. Κάποιοι θεωρούν ότι εί-

μαστε ασφαλείς μόνο αν έχουμε βγάλει τον ηλεκτρονικό υπολογιστή από την παροχή του ρεύματος. Εγώ υποστηρίζω ότι ούτε τότε είμαστε ασφαλείς. Ακόμα και όταν ο υπολογιστής δεν λειτουργεί μπορεί να πάρει φωτιά το κτίριο και να καταστραφεί ο υπολογιστής ή μπορείς κάποιος να τον κλέψει. Επομένως, 100% ασφάλεια είναι κάτι ανέφικτο. Ο στόχος είναι να προσπαθούμε να είμαστε όσο γίνεται καλύτερα προστατευμένοι. Επίσης υπάρχει η έννοια της προστασίας ανάλογα με την κρισιμότητα των δεδομένων μου. Είναι σαφές ότι η πολυπλοκότητα – βαρύτητα των μέτρων ασφάλειας που θα υιοθετηθούν εξαρτάται από την κρισιμότητα της προσφερόμενης υπηρεσίας και των σχετικών δεδομένων. Τέλος, στο τίτλο αναφέρεται «να προστατεύσω αποτελεσματικά τα κρίσιμα επιχειρησιακά δεδομένα μου». Φοβάμαι ότι δεν είμαστε πάντα σε θέση να προσδιορίσουμε επακριβώς ποια είναι αυτά τα επιχειρησιακά δεδομένα που πραγματικά είναι κρίσιμα για τη λειτουργία της επιχείρησης μας. Είναι και αυτό ένα θέμα μεγάλης συζήτησης και είναι κάτι που απαιτεί την υιοθέτηση συγκεκριμένων επιστημονικών μεθοδολογιών που μας βοηθούν να εντοπίσουμε και να αποτιμήσουμε την κρισιμότητα των επιχειρησιακών μας δεδομένων.

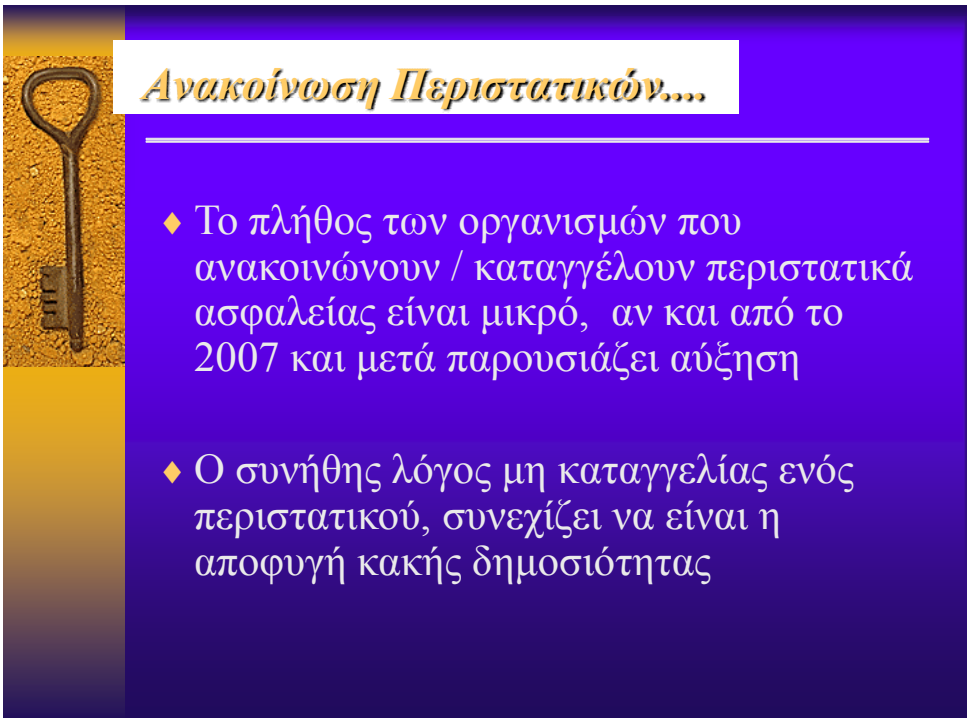


Current Rank	Previous Rank	Goods and Services	Current Percentage	Previous Percentage	Range of Prices
1	2	Bank accounts	22%	21%	$10–$1000
2	1	Credit cards	13%	22%	$0.40–$20
3	7	Full identities	9%	6%	$1–$15
4	N/A	eBay accounts	7%	N/A	$1–$8
7	5	Email addresses	5%	6%	$0.83/MB–$10/MB
8	3	Email passwords	5%	8%	$4–$30

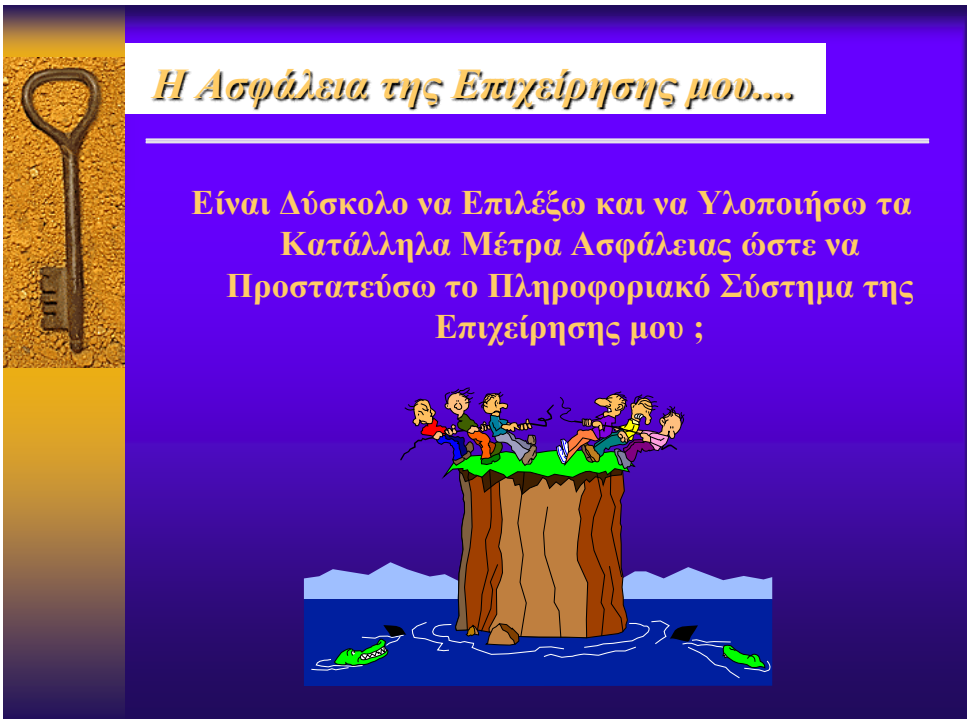
Ξεκινώντας από κάποια στατιστικά στοιχεία, παρατηρούμε ότι περίπου μέχρι το 2006 οι επιθέσεις που γίνονταν γνωστές ήταν ότι κάποιος 'κόλλησε' κάποιον ιό που του έσβησε κάποια αρχεία ή του άλλαξε κάποια εικόνα στον ιστοχώρο της επιχείρησης κτλ. Ήταν, λοιπόν, επιθέσεις που είχαν ως στόχο την ικανοποίηση του επιτιθέμενου. Δεν αποσκοπούσαν στο οικονομικά όφελος του επιτιθέμενου. Αν δείτε από το 2007 και μετά στην πρώτη θέση βρίσκεται πλέον η οικονομική απάτη. Ο λόγος είναι ότι τα δεδομένα σας στο διαδίκτυο έχουν πλέον συγκεκριμένη αξία και μπορούν να πουληθούν. Αν κάποιος λοιπόν βρει τον αριθμό της πιστωτικής κάρτας σας, θα λάβει ένα συγκεκριμένο ποσό ως αντίτιμο. Επομένως, υπάρχει πλέον αξία στα προσωπικά, στα ευαίσθητά και στα επιχειρησιακά σας δεδομένα.

Σχετικά με το οικονομικό κόστος που έχουν προκαλέσει διάφορα περιστατικά ασφάλειας είναι κάτι που δεν παραμένει σταθερό. Βλέπετε ότι στις Ηνωμένες Πολιτείες παρουσιάστηκε κάποια σχετική μείωση του οικονομικού κόστους που προκλήθηκε από επιθέσεις, ενώ στην Αγγλία, Γερμανία, Γαλλία και Αυστραλία υπήρχαν αυξητικές τάσεις.

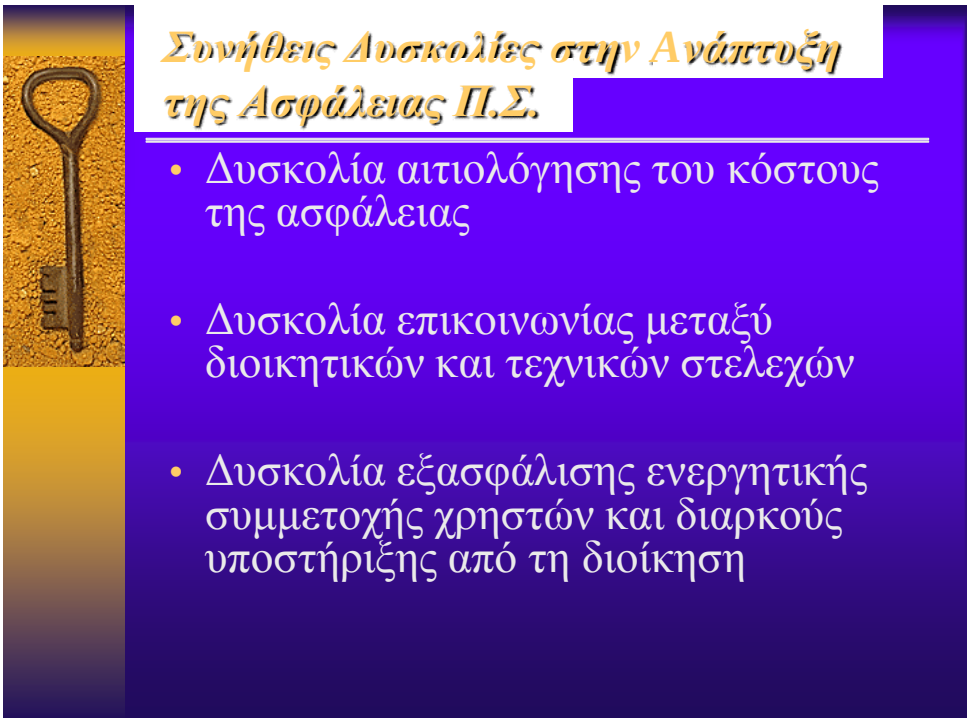
Επίσης, κάτι άλλο που παρατηρούμε είναι ότι αλλάζει ο τρόπος της επίθεσης. Από κάποια στατιστικά δεδομένα του 2011 φαίνεται ότι πλέον η πλειοψηφία των επιθέσεων γίνεται είτε με κακόβουλο λογισμικό (malware) είτε με hacking, κάτι που δεν ίσχυε παλιότερα. Ο λόγος αυτής της διαφοροποίησης στις τεχνικές που αξιοποιούν οι επιτιθέμενοι έχει προκληθεί από το γεγονός ότι πλέον έχει καλλιεργηθεί η κουλτούρα ασφάλειας. Δεν είναι πια εύκολο κάποιος να 'κολλήσει' ένα ιό ή να έχει τόσο 'απροστάτευτο' το σύστημα του. Επομένως ακόμα και η επίθεση χρειάζεται επιστημονική προσέγγιση.



Επίσης, έχει διαπιστωθεί ότι οι οργανισμοί ή οι επιχειρήσεις που έχουν υποστεί κάποιο περιστατικό ασφαλείας προσπαθούν με κάθε τρόπο να αποφύγουν τη δημοσιοποίηση του. Ο λόγος είναι πολύ απλός: η δυσφήμηση της επιχείρησης. Αν κάποιο σοβαρό περιστατικό ασφάλειας δημοσιοποιηθεί τότε αυτό σίγουρα έχει επιρροή είτε στην εμπορική δραστηριότητα της επιχείρησης είτε στο πελατολόγιο της. Η συγκεκριμένη 'συμπεριφορά' των επιχειρήσεων παραμένει η ίδια αν και βαίνει μειούμενη.



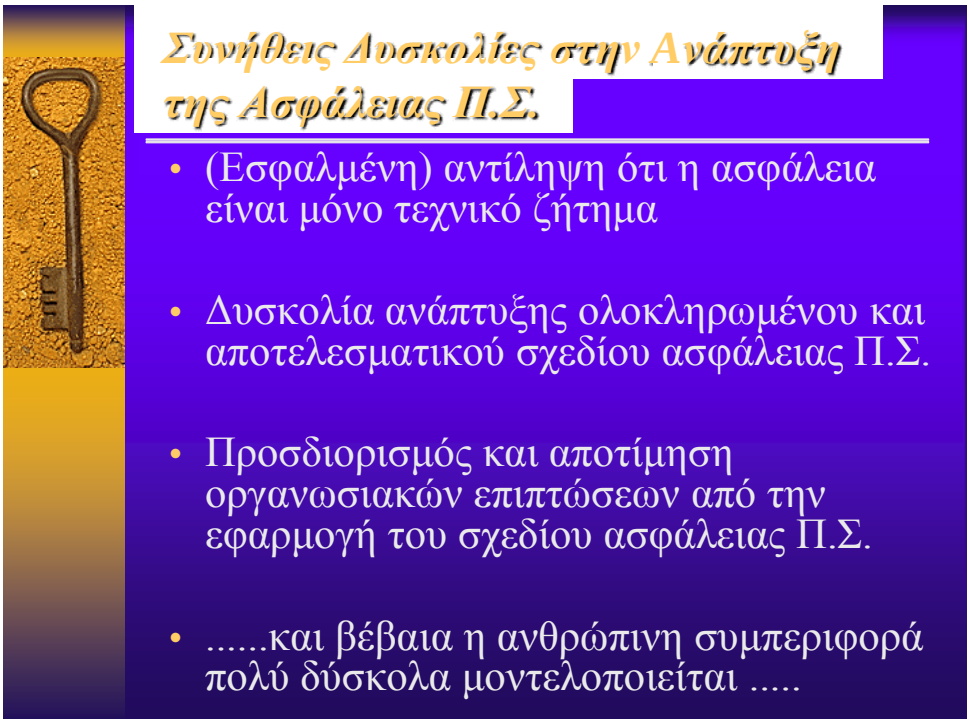
Ας συνεχίσω με αυτό που ξεκίνησα. Ο στόχος μας είναι να προστατεύσουμε το πληροφοριακό σύστημα μας. Τελικά είναι δύσκολο; Μπορούμε να το κάνουμε ; Μπορούμε να επιλέξουμε και να υλοποιήσουμε τα κατάλληλα μέτρα ασφαλείας; Πριν απαντήσουμε ας δούμε τις συνηθέστερες δυσκολίες που θα αντιμετωπίσουμε.



Το πρώτο θέμα είναι η δυσκολία στην αιτιολόγηση του κόστους της ασφάλειας. Όταν θα πάω ως τεχνικός διευθυντής ή ως υπεύθυνος ασφάλειας ενός δημόσιου οργανισμού ή μιας επιχείρησης και απευθυνθώ στη διοίκηση ζητώντας 100 χιλιάδες ευρώ για την υλοποίηση των απαραίτητων μέτρων ασφάλειας, τότε νομίζω ότι καταλαβαίνετε τι θα συμβεί. Η απάντηση της διοίκησης θα είναι: «Ποιο είναι το πρόβλημα; Η επιχείρηση λειτουργεί χωρίς κανένα απολύτως πρόβλημα. Ποτέ δεν μας προβλημάτισε κάποιο περιστατικό ασφάλειας. Γιατί χρειάζεται να επενδύσουμε τόσα χρήματα; «. Η σωστή απάντηση σε αυτό είναι ότι εφόσον δεν έχει συμβεί κάτι μέχρι σήμερα, οι πιθανότητες να συμβεί αυξάνουν και τείνουν προς το ένα, δηλαδή είναι σχεδόν σίγουρο ότι πολύ σύντομα κάποιο περιστατικό ασφάλειας θα απασχολήσει την επιχείρηση.

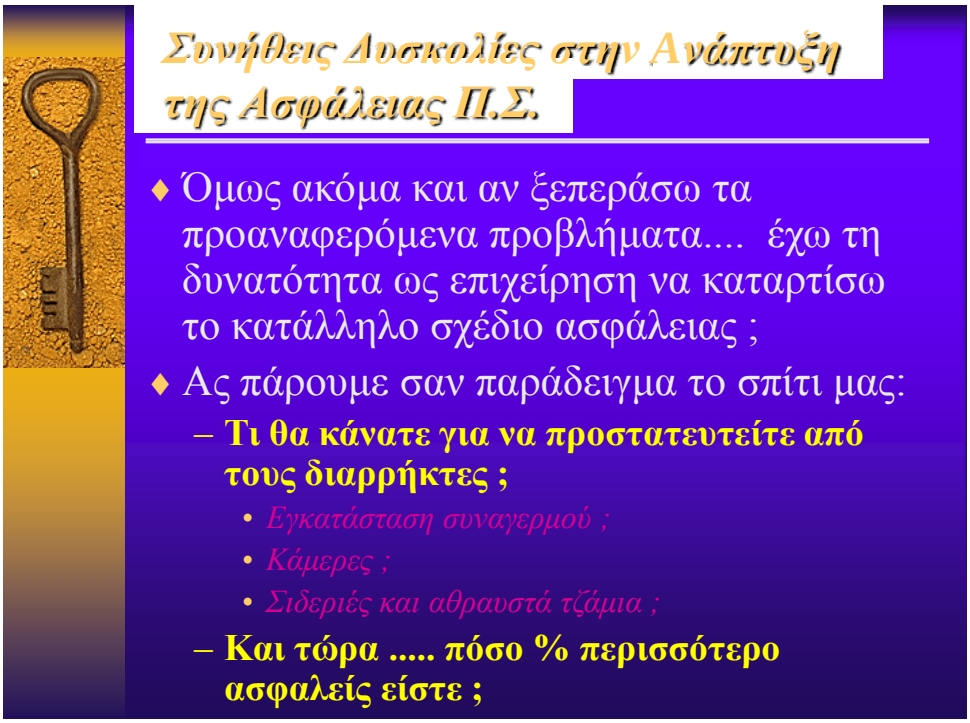
Μια άλλη δυσκολία είναι το πρόβλημα επικοινωνίας μεταξύ διοικητικών και τεχνικών στελεχών. Οι τεχνικοί προσπαθούν να τεκμηριώσουν τις ανάγκες προστασίας των συστημάτων της επιχείρησης με τεχνικούς όρους κάτι που τις περισσότερες φορές δε γίνεται κατανοητό από τη διοίκηση, δημιουργώντας ένα σημαντικό χάσμα επικοινωνίας.

Υπάρχει δυσκολία να εξασφαλιστεί η ενεργητική συμμετοχή των χρηστών του πληροφοριακού συστήματος. Σε οποιοδήποτε πληροφοριακό σύστημα αν οι χρήστες δε θέλουν να συμμετέχουν και να βοηθήσουν οι πιθανότητες επιτυχίας είναι εξαιρετικά μικρές. Ένα απλό παράδειγμα: σε πολλές περιπτώσεις θα διαπιστώσετε ότι οι υπάλληλοι έχουν το Password γραμμένο σε κίτρινο χαρτάκι κολλημένο στην οθόνη, αν και σήμερα υπάρχουν και πιο εξελιγμένες λύσεις αφού πλέον το γράφουν με διορθωτικό κάτω από το πληκτρολόγιο!! Υπό αυτές τις συνθήκες δεν είναι δυνατόν να υπάρξει πραγματική ασφάλεια στο σύστημα. Η συμμετοχή λοιπόν των χρηστών είναι κάτι που πρέπει να εξασφαλιστεί τόσο με την υποστήριξη της διοίκησης αλλά και με την ενημέρωση των χρηστών (security awareness). Πρέπει να είναι ενήμεροι από τι κινδυνεύουν και πώς μπορούν να προστατευθούν.

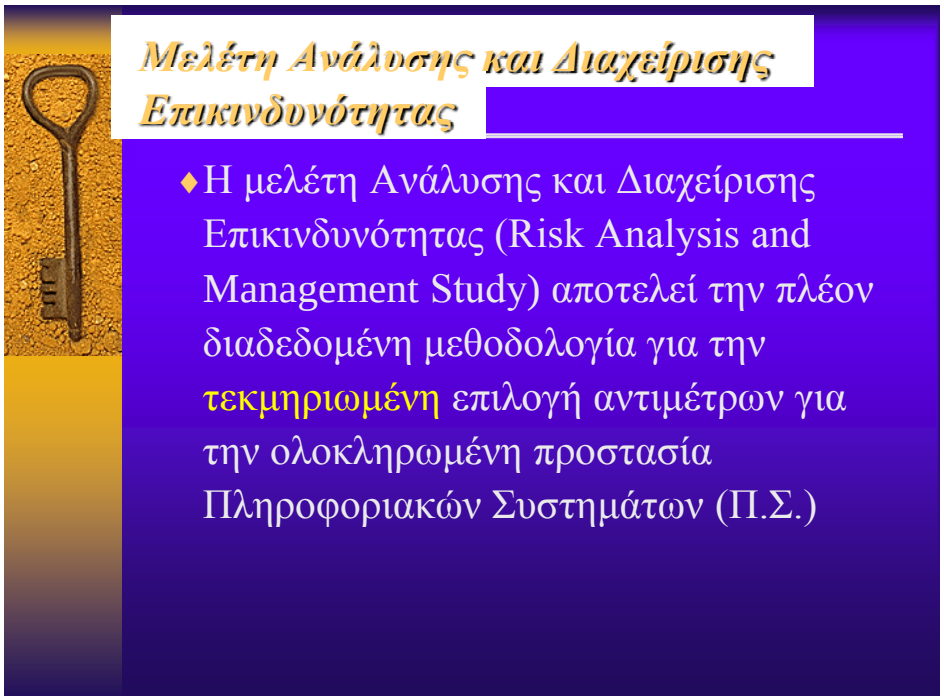


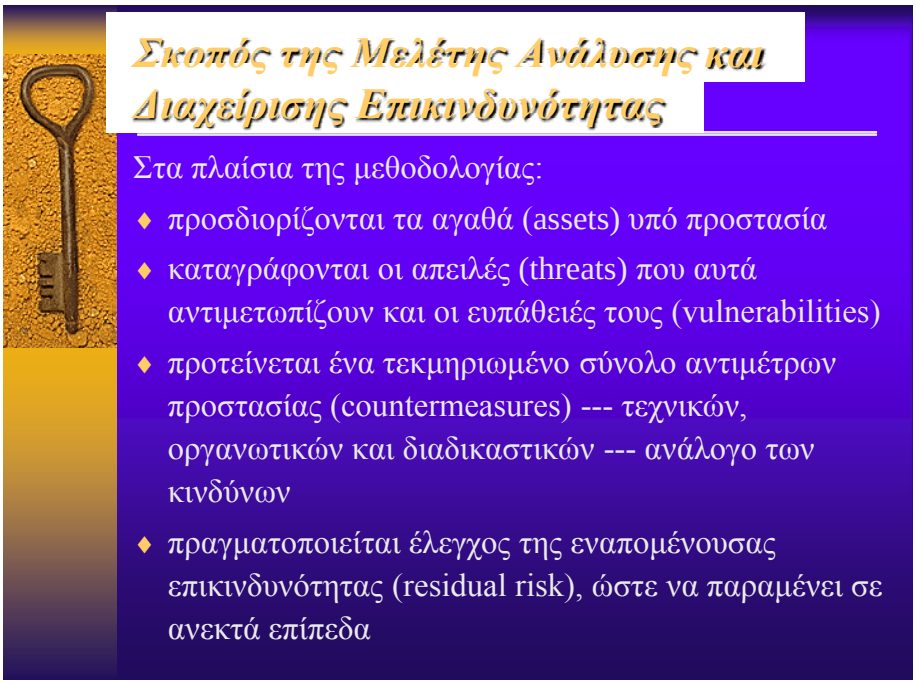
Όπως προανέφερα, η αντίληψη ότι η ασφάλεια είναι μόνο τεχνικό θέμα, είναι εσφαλμένη. Είναι σίγουρα και τεχνικό θέμα, αλλά πρωτίστως απαιτεί και οργανωτικές παρεμβάσεις και υιοθέτηση συγκεκριμένων διαδικασιών. Δεν είναι κάτι που είναι απλό αλλά ούτε εύκολο. Δε είναι δυνατόν απλά να δω ένα πληροφοριακό σύστημα και να αποφασίσω τι μέτρα απαιτούνται για την προστασία του. Χρειάζεται μελέτη βάση συγκεκριμένης μεθοδολογίας για να καταλήξω στα κατάλληλα μέτρα ασφαλείας. Μια δυσκολία είναι ο τρόπος που θα αποτιμήσω τις επιπτώσεις σε περίπτωση που συμβεί κάποιο περιστατικό ασφάλειας. Για παράδειγμα αν εσείς χάσετε τον φορητό υπολογιστή σας μπορείτε άμεσα να καταλάβετε ποιο είναι το κόστος που υφίστασθε; Είμαι σχεδόν σίγουρος ότι δε μπορείτε. Ακόμα και αν αγνοήσουμε το θέμα αντικατάστασης του υπολογιστή, δηλαδή το κόστος να αγοράσετε έναν καινούργιο, η εκτίμηση της αξίας των δεδομένων που απωλέσατε, που μπορεί να είναι δεδομένα που έχουν προκύψει από εργασία 10 ή και 20 χρόνων, είναι εξαιρετικά δύσκολη.

Τέλος, πολύ σημαντική είναι η ανθρώπινη συμπεριφορά. Είναι αρκετά δύσκολο να μοντελοποιήσουμε και να προβλέψουμε την ανθρώπινη συμπεριφορά στα μέτρα ασφάλειας. Υπάρχει πάντα η περίπτωση κάποιος να προκαλέσει ζημιά στα συστήματα της επιχείρησης μας χωρίς να έχει πρόθεση. Ένα χαρακτηριστικό πραγματικό παράδειγμα είναι το εξής: Σ' ένα μεγάλο οργανισμό είχε παρατηρηθεί ότι κάθε απόγευμα, σε συγκεκριμένη ώρα, διεκόπτετο η λειτουργία του εξυπηρετητή χωρίς όμως να διαπιστώνεται κάποια διακοπή ρεύματος ή κάποιο άλλο πρόβλημα. Οπότε παρακολούθησαν να δουν τι συμβαίνει και με έκπληξη διαπίστωσαν ότι το πρόβλημα οφειλόταν στο συνεργείο καθαρισμού που έμπαινε στο computer room και έβγαζε από τη πρίζα τον εξυπηρετητή για να βάλει την ηλεκτρική σκούπα. Είναι λοιπόν ξεκάθαρο ότι κάποια πράγματα δεν μπορείς να τα προβλέψεις εύκολα. Απαιτείται λοιπόν κάποιος τρόπος για να ξεπεράσουμε αυτά τα προβλήματα.



Προχωράμε στην υλοποίηση του κατάλληλου σχεδίου ασφάλειας. Ας πάρουμε ως παράδειγμα το σπίτι μας. Αν προσπαθούσαμε να προστατεύσουμε το σπίτι μας τι θα επιλέγατε για να θωρακίσετε το σπίτι σας από τους διαρρήκτες; Θα βάζατε συναγερμό, κάμερες ή σιδεριές και άθραυστα τζάμια; Η απάντηση δεν είναι δυνατή αν δεν εκτιμήσετε πρώτα την αξία των πραγμάτων που βρίσκονται μέσα στο σπίτι και θέλετε να προστατεύσετε. Εάν το σπίτι είναι άδειο δε χρειάζομαι κανένα από τα μέτρα που περιγράφονται παραπάνω. Εάν η αξία των πραγμάτων που βρίσκονται μέσα στο σπίτι είναι 200 ευρώ τότε η επιλογή τοποθέτησης σιδεριάς και άθραυστων τζαμιών δεν είναι συμφέρουσα καθώς θα κοστίσει περισσότερα από τη πιθανή ζημιά που θα υποστώ από μια κλοπή.





Συνεπώς, γίνεται εύκολα κατανοητή η ανάγκη μιας μεθοδολογικής προσέγγισης ανάλυσης και διαχείρισης επικινδυνότητας του πληροφοριακού μου συστήματος. Στα πλαίσια της μεθοδολογίας αυτής, μπορώ να προσδιορίσω τα αγαθά του συστήματος που θέλω να προστατεύσω (assets), μπορώ να καταγράψω τις απειλές που αντιμετωπίζω και μπορώ να εντοπίσω τις ευπάθειες του συστήματος. Λαμβάνοντας υπόψη τα στοιχεί αυτά μπορώ να καταλήξω σε μία συγκεκριμένη ομάδα κατάλληλων μέτρων ασφάλειας που είναι ανάλογα της αξίας των αγαθών μου καθώς και της σοβαρότητας των απειλών και των ευπαθειών που αντιμετωπίζει το πληροφοριακό σύστημα μου.

Τελειώνοντας, θα ήθελα να τονίσω ότι η ουσιαστική δυσκολία σε όλη αυτή τη μεθοδολογία είναι η αποτίμηση της αξίας των δεδομένων. Η αποτίμηση του υλικό και του λογισμικό είναι εύκολη καθώς υπάρχει μόνο το κόστος αντικατάστασης. Για τα δεδομένα όμως κάτι τέτοιο δεν ισχύει . Η αποτίμηση τους εξαρτάται από τον τύπο της ζημιάς και από την επίπτωση που η συγκεκριμένη ζημιά προκαλεί. Για παράδειγμα, υπήρξε διαρροή των δεδομένων ή μήπως υπήρξε μη εξουσιοδοτημένη τροποποίηση των; Μήπως τα δεδομένα καταστράφηκαν ή δεν είναι διαθέσιμα (denial of service);

Για καθεμία από τις παραπάνω περιπτώσεις είναι απαραίτητο να εκτιμηθούν οι παρακάτω παράμετροι:

- Κατά πόσο υπάρχει οικονομική απώλεια για την επιχείρηση μου
- Κατά πόσο παραβιάζεται η προσωπική ζωή κάποιων πελατών μου. Για παράδειγμα αν σ' ένα νοσοκομείο διαρρεύσει ο ιατρικός μου φάκελος αυτό συνιστά παραβίαση της προσωπικής μου ζωής
- Εάν υπάρχει αδυναμία συμμόρφωσης με νομικές υποχρεώσεις , όπως για παράδειγμα με το Νόμο 2472 για την προστασία των προσωπικών δεδομένων
- Εάν υπάρχει απώλεια της εμπορικής μου θέσης λόγω, για παράδειγμα, απώλειας του πελατολογίου μου.
- Εάν το περιστατικό ασφάλειας μπορεί να προκαλέσει διακοπή λειτουργίας του οργανισμού
- Εάν το περιστατικό μπορεί να προκαλέσει απώλεια καλής φήμης εξαιτίας κάποιου περιστατικού
- Εαν παρεμποδίζεται η εφαρμογή του Νόμου
- Εάν τίθεται σε κίνδυνο η ασφάλεια του Προσωπικού (safety) όπως, για παράδειγμα, στην περίπτωση που δεν λειτουργεί το πληροφοριακό σύστημα ενός Νοσοκομείου με αποτέλεσμα να κινδυνεύει η ζωή των ασθενών

Συνοψίζοντας, μέσω μίας τέτοιας μεθοδολογικής προσέγγισης έχουμε πλέον τη δυνατότητα τεκμηριωμένα να καταλήξουμε στα κατάλληλα μέτρα ασφάλειας για την προστασία του πληροφοριακού μας συστήματος. Ταυτόχρονα, μέσω της διαδικασία ανάλυσης και διαχείρισης της επικινδυνότητας ενός πληροφοριακού συστήματος αναιρούνται κάποια από τις δυσκολίες – προβλήματα που είχα αναφέρει στην αρχή. Είναι δυνατή πλέον η τεκμηρίωση του κόστους των μέτρων ασφάλειας αλλά και η συμμόρφωση με τις τρέχουσες νομικές και κανονιστικές υποχρεώσεις για την προστασία των προσωπικών δεδομένων των πελατών τους.

Διαδικτυακός Εκφοβισμός
Cyberbullying

«Το Χαμόγελο του Παιδιού: Δράσεις ενάντια στον εκφοβισμό»

Κωνσταντίνος Γιαννόπουλος
Πρόεδρος του Δ.Σ. του οργανισμού «Το Χαμόγελο του Παιδιού»
Ομάδα παιδιών «YouSmilers»

Καλησπέρα σε όλους. Είστε σήμερα πολύ σημαντικοί σ' αυτήν την προσπάθεια. Το Χαμόγελο του Παιδιού δε θα μπορούσε να μην είναι εδώ για τα παιδιά, αλλά και μαζί με τα παιδιά. Θα ήθελα να καλέσω στο βήμα, για να συμπαρουσιάσουμε, τη Ράνια και το Νόα, δύο παιδιά που εκπροσωπούν τα χιλιάδες παιδιά που είναι μαζί μας. Θα ήθελα ξεκινώντας με την ευκαιρία να πω κάτι που δεν είναι τόσο ευχάριστο. Θα ήθελα να τιμήσουμε έναν φίλο μας, έναν εθελοντή μας που έφυγε από τη ζωή άδοξα, τον Θανάση Μακρή, τον λιμενικό, εκείνον ο οποίος, εκτός από τη σπουδαία δουλειά που έκανε στις ειδικές δυνάμεις του Λιμενικού, ήταν στην ομάδα διάσωσης στο Χαμόγελο του Παιδιού στην επιχειρησιακή ομάδα που δημιουργήσαμε μαζί με το Λιμενικό, την Πυροσβεστική, την Αστυνομία και όλους τους φορείς για να σώζουμε παιδάκια. Ήτανε μαζί με το σκυλάκο του, τον οποίο τον είχε εκπαιδεύσει να βρίσκει παιδάκια και δυστυχώς έχασε τη ζωή του. Τιμούμε το θανάση, τιμούμε τους εθελοντές μέσα από το θανάση που δυστυχώς έφυγε και θα μας λείψει και τον αποχαιρετούμε στην τελευταία του κατοικία.

Μέσα στα λίγα λεπτά που έχω θα πρέπει να ξεδιπλώσω όχι τόσο για να δείξω τι κάνει το Χαμόγελο του Παιδιού όσο για να καταλάβουμε κάποια πράγματα σαν κοινωνία. Αν ενωθούμε όλοι θα τα καταφέρουμε, όπως έλεγε ο μικρός 10χρονος Ανδρέας, ο γιος μου, πριν από 18 χρόνια. Έλεγε "ελάτε λοιπόν να ενωθούμε, να βοηθήσουμε, αν ενωθούμε όλοι θα τα καταφέρουμε". Αυτή η αγωνία ενός παιδιού είναι αγωνία όλων των παιδιών και θα δείτε μετά τι έκαναν προκειμένου να μας δείξουν ένα δρόμο.

Το Χαμόγελο του Παιδιού είναι ένας οργανισμός με πανελλήνια δράση 24 ώρες το 24ωρο 365 μέρες το χρόνο στη διάθεσή σας, στους εκπαιδευτικούς που νοιάζεστε και είστε σήμερα εδώ προσπαθώντας να ρουφήξετε πράγματα για να προσπαθήσετε να βοηθήσετε μέσα στη σχολική κοινότητα που πρέπει να λειτουργήσει μόνη της και εμείς οι υπόλοιποι οι ειδικοί ή μη ειδικοί να τη στηρίξουμε. Σήμερα το Χαμόγελο του Παιδιού απασχολεί 320 επαγγελματίες ειδικούς και 1800 ενεργούς πολίτες Μπείτε στο www.hamogelo.gr για να ενημερωθείτε. Ειπώθηκε από τον κ. Κουμουτσάκο για το προσβλητικό σχόλιο, την προσβλητική φωτογραφία, τη διάδοση φήμης, όλα αυτά τα οποία γνωρίζουμε αλλά δεν τα έχουμε νοιώσει κάποιοι από εμάς. Και μπορεί να είναι ανυπολόγιστες οι ζημιές, όπως η απομόνωση, η μελαγχολία, η μείωση απόδοσης στο σχολείο και όλα αυτά μπορεί να οδηγήσουν ακόμα και σε αυτοκτονικό ιδεασμό. Με τον κ. Σφακιανάκη, το μαέστρο αυτής της προσπάθειας, έναν άνθρωπο ο οποίος ένωσε δυνάμεις και όχι μόνο δυνάμεις της κοινωνίας αλλά και δυνάμεις της επιχειρηματικότητας, γιατί αν δεν ήταν σήμερα οι χορηγοί δε θα ήταν δυνατό όλα αυτά να γίνουν, άρα θα πρέπει να δίνουμε τιμή σ' αυτούς που βάζουν όχι μόνο την ψυχή τους αλλά και τον οβολό τους για να γίνει αυτό που γίνεται. Φτάνουμε λοιπόν σε

σημείο να έχουμε ανοιχτή γραμμή στο 1056 με τη Δίωξη Ηλεκτρονικού Εγκλήματος ώστε να σώζουμε παιδιά που βρίσκονται σε κίνδυνο.

Έχουμε δημιουργήσει ένα επιχειρησιακό κέντρο το οποίο είναι το καλύτερο στην Ευρώπη, μπορώ να σας το πω με όλη την άνεση πλέον, γιατί κάποτε προσπαθούσαμε να κρατάμε χαμηλούς τόνους και τελικά αφηνόμαστε στο τι σκέπτεται ο καθένας γι΄ αυτό. Άμεση ενεργοποίηση όλων των κοινωνικών φορέων στηρίζοντας τους θεσμούς και δίνοντας τη δυνατότητα στους θεσμούς να λειτουργήσουν καλύτερα και όχι υποκαθιστώντας τους και κινητοποίηση με κέντρα άμεσης κοινωνικής επέμβασης σε όλη την Ελλάδα. Χάρη στις χορηγίες μας, χάρη στις εταιρείες που μας έχουν δώσει τη δυνατότητα, αυτή τη στιγμή λειτουργούν σε όλη την Ελλάδα κέντρα.

Όταν τηλεφωνήσετε στο 1056 στη γραμμή έκτακτης ανάγκης, στη γραμμή που θα χρειαστείτε μια βοήθεια, μια στήριξη, μια συμβουλή, παιδιά, γονείς ή εκπαιδευτικοί εκεί θα βρείτε τους ανθρώπους, τους ειδικούς οι οποίοι θα σας απαντήσουν πάντα με ευγένεια και με καλή διάθεση. Σε διάφορους χώρους στην Αθήνα, την Πάτρα και τη Θεσσαλονίκη, όπως θα δείτε, υπάρχουν εξελιγμένες διαδικασίες μέσα από το χώρο της Πληροφορικής. Όλα αυτά είναι διαδικασίες και δυνατότητες, ακόμη και σε κάποια μεγάλη κρίση το Χαμόγελο του Παιδιού έχει τη δυνατότητα να λειτουργήσει, ακόμα και στο αεροδρόμιο χωρίς να επηρεάζεται από δύσκολες καταστάσεις (disaster recovery area).

Επίσης θα ήθελα να τιμήσουμε τον γυμνασιάρχη του 6ου Γυμνασίου Ιλίου, γυμνασιάρχη ο οποίος κόντρα στις γραφειοκρατίες βοήθησε και έγινε αυτό το γύρισμα και έτσι στην Ευρώπη να έχουμε ένα spot το οποίο είναι πάρα πολύ σημαντικό και δείχνει το πραγματικό πρόβλημα του cyberbullying.

Είναι πολύ σημαντικό να πούμε ότι όλα αυτά τα χρόνια το Χαμόγελο του Παιδιού είναι κοντά στη σχολική κοινότητα στηρίζοντας τους εκπαιδευτικούς και τα παιδιά με έναν διαδραστικό τρόπο, με ενημέρωση για την ενδοσχολική βία, για τη χρήση της τεχνολογίας, παιδική κακοποίηση και δίνουμε φωνή στα παιδιά μέσω του YouSmile. Το YouSmile είναι μια πλατφόρμα που δημιουργήσαμε για τους έφηβους για τα παιδιά και θα μας πουν τα ίδια τι είναι και τι κάνουν τα παιδιά σ' αυτήν την πλατφόρμα.

Νόα: Καλημέρα και από μένα με λένε Νόα, είμαι YouSmiler και είμαι μέλος της ομάδας των δικαιωμάτων του παιδιού. Εγώ θα ήθελα απλά να τονίσω σχετικά με το cyberbullying, ένα φαινόμενο που γιγαντώνεται κυρίως εξαιτίας του Ιντερνετ που είναι πυρήνας όσων θέλουν να προκαλέσουν κακό, με την έννοια ότι τα νέα διαδίδονται πιο γρήγορα και σε ακόμα περισσότερους μέσω αυτού. Θα τονίσω μερικά περιστατικά μόνο και μόνο επειδή θέλω να πω ότι αυτό δεν είναι μακριά, δεν είναι στο εξωτερικό, γίνεται και εδώ κοντά μας. Μία συμμαθήτριά μου κατέληξε αιμόφυρτη σε ένα χώρο στάθμευσης αυτοκινήτων λόγω μιας παρεξήγησης σε ιστοσελίδα κοινωνικής δικτύωσης, ενώ μια άλλη κοπέλα χαρακωνόταν για να νιώθει σωματικά τον πόνο που της προκαλούσαν τα σχόλια για την κοινωνική της ζωή. Θέλω να τελειώσω εδώ και να δώσω το λόγο στη Ράνια λέγοντας σε όσους μπορούν να με ακούσουν ότι υπάρχει καταφύγιο για όσους δέχονται σχόλια, επικρίσεις, υπάρχει ένα μέρος όπου μπορεί να επικοινωνήσει με παιδιά συνομήλικά του και ανθρώπους που γνωρίζουν για το φαινόμενο αυτό μέσω του YouSmile ή και της γραμμής 1056.

Ράνια: Καλημέρα κι από εμένα, είμαι η Ράνια και είμαι YouSmiler, είμαι δηλαδή μέλος της μεγάλης παρέας του YouSmile. Τί είναι όμως το YouSmile; Είναι το βήμα που μας προσέφερε το Χαμόγελο του Παιδιού μέσα από το οποίο μπορούμε να εκφραζόμαστε, να μοιραζόμαστε σκέψεις και

εμπειρίες με άλλα παιδιά. Πρόκειται για μια διαδικτυακή πλατφόρμα στην οποία στόχος μας είναι να περνάμε καλά. Προσπαθούμε από τον Οκτώβρη που τη δημιουργήσαμε να φτιάξουμε μια μεγάλη παρέα. Ήδη έχουμε φίλους από όλη την Ελλάδα, από τη Θράκη μέχρι την Κρήτη, αλλά και από το εξωτερικό. Το YouSmile βρίσκεται σε όλα τα μέσα, ή τουλάχιστον προσπαθούμε να είναι σε όλα τα μέσα, μπορείτε να μας βρείτε τόσο στο facebook όσο και twitter πληκτρολογώντας www.yousmile.gr και να μπείτε και 'σεις στην παρέα μας και να ενημερωθείτε για τις δράσεις μας.

Στο YouSmile όπως ανέφερα εκφραζόμαστε για θέματα που μας αφορούν είτε αυτά έχουν να κάνουν με την ψυχαγωγία και τον αθλητισμό είτε για πιο σοβαρά ζητήματα όπως η παιδική κακοποίηση και η ασφάλεια στο διαδίκτυο. Ουσιαστικά ενημερωνόμαστε και μιλάμε για ότι αφορά τον σύγχρονο νέο. Στόχος μας είναι εμείς τα παιδιά να εξοικειωθούμε με την παιδική γραμμή 1056, στην οποία μπορούμε να μιλήσουμε, να πούμε τους προβληματισμούς μας και να βρούμε λύσεις από ειδικευμένο προσωπικό του Χαμόγελου του Παιδιού, ψυχολόγους, κοινωνικούς λειτουργούς. Πάρα πολλά παιδιά έχουμε έρθει σε δύσκολη θέση θέλοντας να μιλήσουμε κάπου αλλά μη μπορώντας να μιλήσουμε ούτε στους γονείς μας ούτε στους φίλους μας. Το 1056 είναι εκεί είναι δωρεάν και είναι 7 μέρες την εβδομάδα 24 ώρες το 24ωρο.

Το YouSmile είναι ένα εφηβικό site σε ασφαλές διαδικτυακό περιβάλλον στο οποίο αναρτώνται άρθρα από παιδιά και ειδικευμένους ψυχολόγους από το Χαμόγελο του Παιδιού που άλλες φορές αφορούν ψυχαγωγικά θέματα και άλλες φορές μέσα από τα άρθρα δίνονται συμβουλές που αφορούν τα παιδιά και είναι σχετικές με αυτοτραυματισμούς ή με το cyberbullying.

Το YouSmile διατηρώντας τη μορφή του ως ιστοσελίδα χωρίζεται σε 3 επίπεδα, στο YouSmile tv, YouSmile radio και στο YouSmile learn. Το πιο ζωντανό κομμάτι του YouSmile, και το πιο ελκυστικό αν θέλετε, είναι οι διαδικτυακές εκπομπές είτε στη διαδικτυακή τηλεόραση είτε στο διαδικτυακό ραδιόφωνο. Αυτές γίνονται από εμάς τα παιδιά, είμαστε οι κύριοι πρωταγωνιστές και έχουν ψυχαγωγικό και ενημερωτικό περιεχόμενο.

Νόα: Είχα την τιμή να παρουσιάσω μια εκπομπή μέσω της οποίας ενημερώσαμε σχετικά με την παιδική κακοποίηση και ονειρευόμασταν την ημέρα που θα μπορούσαμε να απευθυνόμασταν σε περισσότερο κόσμο, όπως αυτή τη στιγμή, και να ενημερώσουμε και να προβληματίσουμε όλους τους φορείς σχετικά με τα φαινόμενα αυτά και το πώς να αντιμετωπιστούν.

Ράνια: Όπως είπα νωρίτερα πρωταγωνιστές σ' αυτές τις εκπομπές είμαστε εμείς τα παιδιά έχουμε όμως την έμπρακτη στήριξη τόσο των εργαζομένων του συλλόγου όσο και επαγγελματιών από διάφορους τομείς και δημόσιων προσώπων. Για παράδειγμα, πριν λίγες μέρες είχαμε κοντά μας σε μια διαδικτυακή ραδιοφωνική εκπομπή τον κ. Καραμέρο ο οποίος συζήτησε με παιδιά από σχολείο του Ηρακλείου και παλιότερα είχαμε κοντά μας σε μία διαδικτυακή τηλεοπτική εκπομπή τον κ. Γιώργο Παπαδάκη και καταφέραμε μάλιστα να του πάρουμε και τον λόγο πράγμα πολύ δύσκολο.

Στις φωτογραφίες βλέπουμε το studio μας και ίσως μερικοί σκεφτείτε: μα καλά σε καιρό οικονομικής κρίσης φτιάχνουνε studio; Κι όμως το studio είναι σημαντικό, να επισημάνουμε ότι έγινε με την πολύτιμη βοήθεια χορηγών και εθελοντών του συλλόγου Χαμόγελο του Παιδιού στους οποίους και χρωστάμε το γεγονός ότι αυτή τη στιγμή έχουμε ένα βήμα να εκφραστούμε και να έρθουμε σε επαφή με άλλα παιδιά που το έχουν και ανάγκη πιθανότατα. Στο YouSmile περνάμε υπέροχα, αξίζει να μπείτε στο www.yousmile.gr να δείτε τις δράσεις μας και γιατί όχι να έρθετε στην παρέα μας.

Αυτό δε θέλουν όλα τα παιδιά ένα μέσο να εκφραστούν;

Να ακουστούν; Σας περιμένουμε! Σας ευχαριστούμε πολύ!

«Digital και cyber bullying και αθέμιτη χρήση ηλεκτρονικών πληροφοριών ως το "bullying του μέλλοντος" Γνώση και πρόληψη»

Φώτης Σπυρόπουλος
Δικηγόρος – οικονομολόγος, ποινικολόγος (ΜΔΕ), εγκληματολόγος (ΜΔΕ),
υπ. Δρ Ποινικού Δικαίου-Εγκληματολογίας Νομικής Αθηνών,
αριστούχος υπότροφος προγράμματος «ΗΡΑΚΛΕΙΤΟΣ ΙΙ»[1]

Θέλω να δώσω συγχαρητήρια στην Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος για τα πολύ σημαντικά συνέδρια που διοργανώνει και το σημαντικότερο όλων ότι καταφέρνει και διοργανώνει αυτά τα συνέδρια με τους καλύτερους. Έχουν κληθεί πραγματικά ειδικοί επιστήμονες με γνώση με εμπειρία όπως είναι ο κ. Μόσχος, ο κ. Στώμος, η κ. Φισούν, οι οποίοι έχουν ασχοληθεί ιδιαίτερα με το θέμα. Από 'κει και πέρα, πιστεύω όλοι θα βάλουμε το δικό μας λιθαράκι για να προσεγγίσουμε κάποιες και δυσνόητες ίσως έννοιες με απλό και όχι απλοϊκό τρόπο. Λίγο πριν ξεκινήσω να πω το εξής, γιατί μιλάμε τόσο πολύ για το **bullying για το cyberbullying; Προφανώς γι**ατί το θύμα βιώνει μια κατάσταση η οποία είναι δυσβάσταχτη γι' αυτό.

Όταν πρωτοασχολήθηκα με το bullying, το 2005, όταν ακόμα το θέμα αυτό δεν είχε κεντρίσει ιδιαίτερα το επιστημονικό ενδιαφέρον, ήταν γιατί είχα βρει τότε κάποιες έρευνες του Dan Olweus που μου έκαναν εντύπωση στην ενασχόληση μου με τα νομικά, οι οποίες έλεγαν ότι όσοι διέπρατταν bullying στο γυμνάσιο το 60% αυτών είχε τουλάχιστον μια καταδίκη ως ενήλικας, αποτέλεσαν δηλαδή εισροές στο σύστημα ποινικής δικαιοσύνης και από αυτό το 60% το 35-40% είχαν από την πλικία των 24 και μετά τουλάχιστον 3 καταδίκες. Δηλαδή η πρόληψη του bullying έχει αφενός τα βραχυπρόθεσμα αποτελέσματα, αφετέρου μπορεί να μειώσει τις εισροές στο σύστημα της ποινικής μας δικαιοσύνης.

Η εισήγηση μου θα διαρθρωθεί σε 3 μέρη. Στην αρχή θα θίξουμε κάποια θεωρητικά ζητήματα, στο 2ο μέρος θα αναφέρω τη δική μου προσέγγιση αναφορικά με τις αλλαγές που έχουν επέλθει όταν πλέον μιλάμε για **cyberbullying και στο 3ο μέρος θα μιλήσουμε για πράξη, για πρακτι**κές που έχουν ήδη εφαρμοστεί σε ότι αφορά το πώς μπορούμε να είμαστε δημιουργικοί στο διαδίκτυο αναφορικά με την πρόληψη του bullying.

Είναι προφανές ότι η εισβολή της τεχνολογίας στην καθημερινή ζωή έχει επηρεάσει και τους τρόπους εκδήλωσης συμπεριφορών bullying[2]. Συσκευές ψηφιακής (digital) επικοινωνίας όπως τα κινητά τηλέφωνα [ιδίως με υποστήριξη πολυμέσων (**multimedia) και δυνατότητες λήψης φωτο-**

1. Η παρούσα έρευνα έχει συγχρηματοδοτηθεί από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο – ΕΚΤ) και από εθνικούς πόρους μέσω του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» του Εθνικού Στρατηγικού Πλαισίου Αναφοράς (ΕΣΠΑ) – Ερευνητικό Χρηματοδοτούμενο Έργο: Ηράκλειτος ΙΙ. Επένδυση στην κοινωνία της γνώσης μέσω του Ευρωπαϊκού Κοινωνικού Ταμείου.

2. Για το φαινόμενο του bullying πρβλ. την αναλυτική μελέτη του γράφοντος, Σχολικός τραμπουκισμός, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα – Κομοτηνή, 2011.

γραφιών και βίντεο και σύνδεσης σε δίκτυο (smart phones)] και η χρήση της πληροφορικής και, δη, του διαδικτύου και του κυβερνοχώρου (ιδίως σε περιπτώσεις επισκέψεων σε ιστοσελίδες κοινωνικής δικτύωσης – social networking websites[3]), έχουν αναπτύξει νέες μορφές άσκησης του bullying οι οποίες καλούνται **digital bullying**[4] και **cyber bullying**[5] αντίστοιχα.

Έννοια του bullying

Η ελληνική επιστημονική βιβλιογραφία ήρθε πολύ πρόσφατα σε επαφή με την έννοια του bullying[6], η οποία αποδίδεται από τον Κουράκη στην ελληνική γλώσσα με τη λέξη «τραμπουκισμός»[7], και η οποία περιγράφει[8] το φαινόμενο **τέλεσης πράξεων παραβατικού χαρακτήρα** (απειλητική ή αυταρχική συμπεριφορά με πρόθεση την πρόκληση βλάβης ή τρόμου[9]) χωρίς συνήθως να έχει προκληθεί ο θύτης από ένα άτομο ή ομάδα ατόμων (ακόμα και κράτος στην περίπτωση του political bullying) εναντίον άλλου ή άλλων **με επαναλαμβανόμενο ρυθμό εμφάνισης** (δεν θεω-

3. Πρβλ. Γιώτας Γ. Κυριάκη, Ιστοσελίδες κοινωνικής δικτύωσης και διαπροσωπικές σχέσεις, εις: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 63 επ.

4. Για το digital bullying και το cyber bullying βλ. τη στήλη «Ψηφιακός τραμπουκισμός (digital bullying)" στο (αξιόλογο) δημοσίευμα των Κωνσταντίνας Γαρνέλη, Μαρίας Παπαδημητρίου και Αρετής Νταραδήμου, «Φάκελος bullying» στην εφημερίδα «Ελεύθερος Τύπος» της 14ης Οκτωβρίου 2007, σελ. 62–65.

5. Για περαιτέρω βιβλιογραφία αναφορικά με το θέμα βλ. A. Burgess-Proctor, J. W. Patchin, & S. Hinduja, Cyberbullying and online harassment: Reconceptualizing the victimization of adolescent girls. In V. Garcia and J. Clifford [Eds.]. Female crime victims: Reality reconsidered. Upper Saddle River, NJ: Prentice Hall. In Print, 2009, S. Keith, & M. E. Martin, Cyber-bullying: Creating a Culture of Respect in a Cyber World. Reclaiming Children & Youth, 13(4), 2005, pp. 224–228., S. Hinduja & J. W. Patchin, Offline Consequences of Online Victimization: School Violence and Delinquency, Journal of School Violence, 6(3), 2007, pp. 89–112. S. Hinduja, & J. W. Patchin, Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization. Deviant Behavior, 29(2), 2008, pp. 129–156. S. Hinduja & J. W. Patchin, Bullying beyond the Schoolyard: Preventing and Responding to Cyberbullying. Thousand Oaks, CA: Sage Publications, 2009, J. W. Patchin, & S. Hinduja, Bullies Move beyond the Schoolyard: A Preliminary Look at Cyberbullying. Youth Violence and Juvenile Justice, 4(2), 2006, pp. 148–169. S. Y. Tettegah, D. Betout & K. R. Taylor, Cyber-bullying and schools in an electronic era, in S. Tettegah & R. Hunter (Eds.) Technology and Education: Issues in administration, policy and applications in k12 school. pp. 17–28. London: Elsevier, 2006, J. Wolak, K. J. Mitchell & D. Finkelhor, Online victimization of youth: 5 years later. Alexandria, VA: National Center for Missing & Exploited Children, 2006. url: http://www.unh.edu/ccrc.

6. Ένας από τους πρωτεργάτες της μελέτης του φαινομένου του bullying είναι ο Καθηγητής στο Πανεπιστήμιο του Bergen της Νορβηγίας Dan Olweus. Για τις θέσεις του πρβλ. D. Olweus, A Research Definition of Bullying, url: http://www.cobb.k12.ga.us/~preventionintervention /Bully/Definition%20of%20Bullying.pdf καθώς και το «μνημειώδες» έργο του για το ζήτημα Dan Olweus, Bullying at School – What we Know & What we Can Do, Blackwell Press, 1993. (στα ελληνικά Dan Olweus, Εκφοβισμός και Βία στο σχολείο – Τι γνωρίζουμε και τι μπορούμε να κάνουμε, εκδ. της ΕΨΥΠΕ, 2009). Η πρωτοπορία του Olweus αναγνωρίζεται και από τον Ken Rigby, Bullying in schools and what to do about it, ACER (Australian Council for Educational Research Ltd) Press, Victoria Australia 2007, p. 12 (url: http://books.google.gr/books?id=KEUeLn09668C&pg=PA121&lpg=PA121&dq=Rigby+2006+bullying&source=bl&ots=NkVGkVGo2B&sig=lDRzjZDml6cg9qMJJy7vLwyBQfE&hl=el&ei=Bgh_SqPbNoqknQPjkY2DAg&sa=X&oi=book_result&ct=result&resnum=4#v=onepage&q=Rigby%202006%20bullying&f=false

7. Ν. Κουράκης, Μορφές σχολικής βίας και δυνατότητες αντιμετώπισής της, ηλεκτρονικό περιοδικό Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών www.theartofcrime.gr (τεύχος 11)

(url: http://www.theartofcrime.gr/index.php?pgtp=1&aid=1247152434) και ΠοινΧρ ΝΘ/2009, σελ. 865–871.

8. Για τον ορισμό του bullying βλ. ενδεικτικώς D. Olweus, Sweden, in P. K. Smith, Y. Morita, J. Junger-Tas, D. Olweus, R. Catalano, & P. Slee (Eds.), The Nature of School Bullying: A Cross-National Perspective (pp. 7–48). London and New York: Routledge, 1999, K. Stassen Berger, Update on bullying at school: science forgotten? Developmental Review, 2006, p. 5, P.K. Smith & S. Sharp, School bullying: insights and perspectives, Routledge ed., London 1994, ED 387223, p. 2 και στο googlebooks (url: http://www.google.com/books?hl=el&lr=&id=K4nh6ZggMF8C&oi=fnd&pg=PA1&dq="Smith"+"The+problem+of+school+bullying"+&ots=e_HWBrEvfG&sig=lmAuTjMhv9hbu93bnETjnH6RZRM#v=onepage&q=%22Smith%22%20%22The%20problem%20of%20school%20bullying%22&f=false) και F. Clark Power, Ronald J. Nuzzi, Darcia Narvaez, Daniel K. Lapsley & Thomas C. Hunt, Moral Education, a Handbook, στο google books (url: http://books.google.gr/books?id=qIMQzDGvQZIC&pg=PA52&lpg=PA52&dq=R.+S.+griffin+A.+M.+Gross&source=bl&ots=S143ra18Va&sig=AP0lzGoYgsRExJE1BHrEJAnbcko&hl=el&ei=VuzAStHABY78_AanjpyCAQ&sa=X&oi=book_result&ct=result&resnum=6#v=onepage&q=R.%20S.%20griffin%20A.%20M.%20Gross&f=false), pp. 51, James Alan Fox, D. S. Elliott, R. G. Kerlikowske, S. A. Newman & W. Christeson, Bullying Prevention is Crime Prevention, url: http://www.pluk.org/Pubs/Bullying2.pdf, σελ. 7 (Το τελευταίο αυτό άρθρο υπέδειξε σ'εμένα η εξαίρετη συνάδελφος υπ. Δρ. Εγκληματολογίας Μάρθα Λεμπέση την οποία ευχαριστώ και από αυτή τη θέση).

9. Delwyn Tattum & Graham Herbert, Bullying: A positive response, Cardiff Institute of Higher Education, 1990.

ρείται πάντοτε απαραίτητος[10]). Συστατικό και κυριότερο στοιχείο αυτής της συμπεριφοράς είναι η **ανισορροπία δύναμης μεταξύ θύτη και θύματος (imbalance of power)**[11] και συνεπώς η χρήση από κάποιον ή από μια ομάδα της δύναμης ή της υπερέχουσας κατάστασης στην οποία βρίσκεται (σε ψυχολογικό, συναισθηματικό, σωματικό, γνωστικό επίπεδο) προκειμένου να εκφοβίσει, να βλάψει ή να ταπεινώσει κάποιον άλλο ή άλλους.

Ο θύτης, επομένως, υπερέχει του θύματος σε σωματική ή / και ψυχική δύναμη[12] [13], ανάλογα και με τη μορφή και φύση της προσβολής· η, δε, διαφορά δύναμης είναι τέτοια ώστε το θύμα να αδυνατεί να αμυνθεί και να αντιδράσει. Επομένως, εναλλακτικά το bullying ορίζεται ως μια **«συστηματική κατάχρηση δύναμης»**[14] ή «κατάχρηση εξουσίας» και όχι ως απλή παρενόχληση[15]

10. Υπάρχουν στην διεθνή βιβλιογραφία αρκετοί ορισμοί για το bullying οι οποίοι είναι παρεμφερείς με τον ορισμό που υιοθετείται εδώ. Σκόπιμο να αναφερθεί ότι κάποιοι εξ αυτών κρίνουν ότι το bullying δυνητικά μπορεί να συνίσταται σε επαναλαμβανόμενες πράξεις (έτσι Delwyn Tattum & Graham Herbert, Bullying: A positive response, όπ. π.).

11. ...ευδιάκριτη στις σωματικές εκδηλώσεις bullying, δυσδιάκριτη όμως στις κοινωνικές εκδηλώσεις του φαινομένου (Έτσι Ken Rigby, Bullying in schools and what to do about it, ACER (Australian Council for Educational Research Ltd) Press, Victoria Australia 2007, p. 15, όπ. π.).

12. Βλ. C. F. Garandeau & A. H. N. Cillessen, From indirect aggression to invisible aggression : A conceptual view on bullying and peer group manipulation, Aggression and Violent Behaviour, 2005 και M. B. Greene, Bullying and harassment in schools, in R. S. Moser, & C. E., Franz (Eds.), Shocking Violence: Youth Perpetrators and Victims– a Multidisciplinary Perspective, 2000 (pp. 72–101). Βλ. επίσης, Ν. Κουράκης, Μορφές σχολικής βίας και δυνατότητες αντιμετώπισής της, όπ. π.

13. Έχουν καταγραφεί ενδεικτικά διαφορετικοί τρόποι με τους οποίους η δύναμη μπορεί να χρησιμοποιηθεί για την επιβολή σε ένα περιβάλλον:

1. Η δύναμη να κυριαρχείς στους άλλους σωματικά – μπορεί να σχετίζεται με το παράστημα, τη σωματική ικανότητα και τις ικανότητες πάλης.
2. Οξύτητα της γλώσσας – Σχετίζεται με τις λεκτικές ικανότητες και ιδιαίτερα με την ταχύτητα του πνεύματος. Αυτές οι ικανότητες χρησιμοποιούνται περισσότερο για την άσκηση bullying καθώς οι ανήλικοι μεγαλώνουν.
3. Ικανότητα να καλείς άλλους για υποστήριξη – Σχετίζεται με την δημοτικότητα, την ικανότητα ανάπτυξης κοινωνικών επαφών και δεξιοτήτων, κ.λπ.
4. Θέση στην ομάδα – Σχετίζεται με προσωπικές επιτυχίες π.χ. σε αθλήματα, καθώς και με το να είναι κάποιος ελκυστικός, να είναι μέλος μιας κυρίαρχης ομάδας της πλειοψηφίας σε αντίθεση, για παράδειγμα, με το να έχει κάποια αναπηρία ή να ανήκει σε μια ομάδα μειοψηφίας (π.χ. μετανάστης), ή να ανήκει σε ομάδα LGBT (λεσβία, gay, bisexual ή transexual).
5. Θεσμοθετημένη ή αποδοθείσα εξουσία – Σχετίζεται με θέση διοίκησης στην ομάδα, π.χ. παλαιότερος μαθητής, πρόεδρος τμήματος ή υπεύθυνος υπηρεσίας
6. Δύναμη του ειδικού – Όταν ο ειδικός χρησιμοποιεί την υπεροχή της γνώσης του για να κυριαρχήσει ή να παραπλανήσει
7. Νόμιμη – θεσμοθετημένη δύναμη – Όταν ένα άτομο σε εξουσία, όπως νέος λειτουργός ή δάσκαλος, μπορεί να επιβληθεί αδίκως σε κάποιον λόγω της θέσης του
8. Δύναμη της πληροφορίας – Όταν κάποιος στερείται πρόσβασης σε ό,τι κάποιος έχει το δικαίωμα να γνωρίζει, π.χ. πληροφορία για μια διαδικασία υποβολής παραπόνου

[Από τις απαντήσεις της Πρεσβείας της Ιρλανδίας στο αίτημα υπόδειξης καλών πρακτικών για την αντιμετώπιση της σχολικής βίας της ad hoc «Ειδικής Επιτροπής Μελέτης των Ομάδων Ενδοσχολικής Βίας» (ΕΕΜΟΕΒ). Η επιτροπή αυτή ιδρύθηκε και λειτούργησε στο πλαίσιο της Εθνικής Επιτροπής για τα Δικαιώματα του Ανθρώπου από τον Ιούνιο του 2006 έως τον Μάιο του 2010, υπό την προεδρία της Καθηγήτριας κ. Αλίκης Γιωτοπούλου – Μαραγκοπούλου. Στην εν λόγω επιτροπή κλήθηκαν και συμμετείχαν όλοι οι επιστημονικοί και κοινωνικοί φορείς τους οποίους αφορά άμεσα το θέμα καθώς και ειδικοί επιστήμονες: ενδεικτικά συμμετείχαν ο επ. Αντιπρόεδρος του ΑΠ Πέτρος Κακκαλής, ο συνήγορος του παιδιού κ. Γ. Μόσχος, νομικοί, εγκληματολόγοι, εκπρόσωποι των συλλόγων γονέων, εκπρόσωποι της ΟΛΜΕ, εκπαιδευτικοί κ.α. – μέλος της επιτροπής και ο γράφων. Τα πορίσματα των εργασιών της Επιτροπής δημοσιεύθηκαν στον συλλογικό τόμο «Ομαδική βία και επιθετικότητα στα σχολεία», εκδ. Νομική Βιβλιοθήκη, Αθήνα 2010 σε διεύθυνση έκδοσης της Προέδρου της Επιτροπής Καθηγήτριας Αλίκης Γιωτοπούλου–Μαραγκοπούλου].

14. Έτσι K. Stassen Berger, Update on bullying at school: science forgotten? Developmental Review, 2006, p. 5, P.K. Smith & S. Sharp, School bullying: insights and perspectives, Routledge ed., London 1994, ED 387223, p. 2 και στο googlebooks (url: http://www.google.com/books?hl=el&lr=&id=K4nh6ZggMF8C&oi=fnd&pg=PA1&dq="Smith"+"The+problem+of+school+bullying"+&ots=e_HWBrEvfG&sig=lmAuTjMhv9hbu93bnETjnH6RZRM#v=onepage&q=%22Smith%22%20%22The%20problem%20of%20school%20bullying%22&f=false) και F. Clark Power, Ronald J. Nuzzi, Darcia Narvaez, Daniel K. Lapsley & Thomas C. Hunt, Moral Education, a Handbook, στο google books (url: http://books.google.gr/books?id=qIMQzDGvQZIC&pg=PA52&lpg=PA52&dq=R.+S.+griffin+A.+M.+Gross&source=bl&ots=S143ra18Va&sig=AP0lzGoYgsRExJE1BHrEJAnbcko&hl=el&ei=VuzAStHABY78_AanjpyCAQ&sa=X&oi=book_result&ct=result&resnum=6#v=onepage&q=R.%20S.%20griffin%20A.%20M.%20Gross&f=false), pp. 51.

15. Ο Rigby υποστηρίζει ότι ο όρος **bullying** χρησιμοποιείται περισσότερο στο Ηνωμένο Βασίλειο ενώ ο όρος **harassment** στις Η.Π.Α. Επί-

(εφόσον στην δεύτερη φαίνεται να ελλείπει το κριτήριο της μεγαλύτερης ισχύος του παρενοχλούντος) και της θέλησης επιβολής του θύτη. Δηλαδή, ο τραμπουκισμός (bullying) συνίσταται σε σκόπιμες αρνητικές ενέργειες με στόχο την πρόκληση σωματικών ή / και ψυχολογικών βλαβών σε έναν ή περισσότερους ανήλικους, οι οποίοι είναι αδύναμοι και δεν μπορούν να υπερασπιστούν τον εαυτό τους, με **σκοπό και την επιβολή και την εγκαθίδρυση / επίδειξη / διατήρηση της ισχύος του θύτη στα υπόλοιπα μέλη του κοινωνικού περιβάλλοντος.**

Ο Olweus συνοψίζει τον ορισμό του bullying σε τρεις βασικές παραμέτρους:

α) (χωρίς πρόκληση) επιθετική/ παραβατική συμπεριφορά ατόμου ή ομάδας ατόμων

β) επαναλαμβανόμενος ρυθμός εμφάνισης (ωστόσο υπό περιστάσεις ακόμα και μεμονωμένη συμπεριφορά μπορεί να αποτελεί bullying)

γ) διαπροσωπική σχέση η οποία χαρακτηρίζεται από ανισορροπία δύναμης[16]

Τέλος, οι εν λόγω συμπεριφορές διενεργούνται ως αυτοσκοπός και όχι ως μέσο επίτευξης κάποιου άλλου στόχου από τον θύτη ή ως εκδίκηση για κάποιο λόγο. Ως μόνος λόγος για την άσκηση τραμπουκισμού προβάλλει η ικανοποίηση του θύτη όταν βλέπει το θύμα του να υποφέρει και να τρομοκρατείται[17].

Digital και cyber bullying

Το digital και cyber bullying αποτελεί ειδική μορφή του bullying και ορίζεται ως επιθετική συμπεριφορά, η οποία λαμβάνει χώρα εναντίον άλλου από πρόθεση με τη χρήση ηλεκτρονικών μέσων ή μορφών επικοινωνίας, επαναληπτικά και πάνω από μια φορά κατά ενός θύματος που δε μπορεί εύκολα να υπερασπιστεί τον εαυτό του.[18]

Στην προκειμένη περίπτωση μπορεί, με μια πρώτη ματιά, να υποστηριχθεί ότι ουσιαστικά πρόκειται για εκδήλωση συμπεριφορών της μορφής του ήδη αναλυθέντος τραμπουκισμού με τη βοήθεια της τεχνολογίας. Ο τίτλος σχετικού πονήματος του *Q. Li* "New bottle but old wine"[19] («καινούριο μπουκάλι αλλά παλιό κρασί») αναφορικά με το **cyber bullying υποδηλώνει με τον καλύτερο τρόπο ότι οι συμπεριφορές τις οποίες καλούμαστε να μελετήσουμε και να αντιμετωπίσουμε είναι παρόμοιες με τις «παραδοσιακές».**

Ωστόσο, είναι γεγονός ότι οι εκδηλώσεις του φαινομένου υπό αυτές τις συνθήκες και ο τρόπος δράσης των θυτών (*modus operandi*) έχουν τροποποιηθεί σε σχέση με τις («παραδοσιακές») μορφές που παρουσιάστηκαν παραπάνω:[20] χαρακτηριστικά, οι «ηλεκτρονικοί bullies» συνήθως και

σης, προβαίνει σε μια εκτενή ανάπτυξη των διαφορών που εντοπίζει μεταξύ των όρων harassment και bullying (Ken Rigby, Bullying in schools and what to do about it, ACER (Australian Council for Educational Research Ltd) Press, Victoria Australia 2007, p. 21, όπ. π.)

16. D. Olweus, Sweden, in P. K. Smith, Y. Morita, J. Junger-Tas, D. Olweus, R. Catalano, & P. Slee (Eds.), The Nature of School Bullying: A Cross-National Perspective (pp. 7-48). London and New York: Routledge, 1999.

17. C. F. Garandeau & A. H. N. Cillessen, όπ. π. και M. B. Greene, όπ. π.

18. Το γεγονός ότι το cyber bullying χρήζει ξεχωριστής και ιδιαίτερης αντιμετώπισης αποτελεί κεντρικό θέμα σύγχρονων επιστημονικών συζητήσεων και δράσεων. Βλ. ενδεικτικά Διονυσίας Μουζάκη, Διεθνής επιστημονική ημερίδα με θέμα: *"Η αντιμετώπιση του cyberbullying από νομική σκοπιά"*, ηλεκτρονικό περιοδικό του Εργαστηρίου Ποινικών και Εγκληματολογικών Ερευνών www.theartofcrime.gr, τεύχος 15 (url: http://www.theartofcrime.gr/?_pgtp=1&aid=1277745364) όπου παρουσιάζεται διεθνής επιστημονική ημερίδα με θέμα την **αντιμετώπιση του Cyberbullying από νομική σκοπιά**. Η εν λόγω ημερίδα απετέλεσε δραστηριότητα ενταγμένη στη δράση για το cyberbullying, η οποία λαμβάνει χώρα σύμφωνα με το πρόγραμμα Ευρωπαϊκής Συνεργασίας «COST ISCH domain». Η ως άνω δράση αναφορικά με θέματα cybebullying έχει ξεκινήσει ήδη από τον Οκτώβριο του 2008 και προεδρεύων της κίνησης αυτής είναι ο Peter Smith, Καθηγητής Ψυχολογίας στο Πανεπιστήμιο Goldsmiths του Λονδίνου.

Ο ως άνω ορισμός είναι αυτός ο οποίος χρησιμοποιείται στις εργασίες του εν λόγω προγράμματος.

19. Q. Li, New bottle but old wine: A research of cyberbullying in schools, 2005, url: http://www.ucalgary.ca/~qinli/publication/cyber_chb2005.pdf

20. π.χ. αποστολή sms ή e-mail με υβριστικό / απειλητικό περιεχόμενο, φωτογράφηση-κινηματογράφηση του ανηλίκου για την απειλή και

ενδεικτικώς (δύνανται να) δρουν ανώνυμα χρησιμοποιώντας ενδεχομένως κάποιο ψευδώνυμο (nickname) σε σελίδες συνομιλίας (chat rooms) και η προσβολή ή επιθετική τους πράξη (να) συνίσταται σε πρακτικές hacking[21] (μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή) και cracking (ηλεκτρονικός βανδαλισμός)[22] –οι οποίες διαφοροποιούνται άμεσα από τις παραδοσιακές πρακτικές–, όπως αποστολή ιών που μπορεί να βλάψουν πρόγραμμα ή αρχεία υπολογιστή, αθέμιτη και χωρίς δικαίωμα πρόσβαση σε ηλεκτρονικά δεδομένα άλλου, αποστολή μεγάλου αριθμού μηνυμάτων προκειμένου να υπερφορτωθεί ο υπολογιστής ή το κινητό τηλέφωνο άλλου (sms ή mail bombing), καθώς και κατασκευή ψεύτικου προφίλ με το όνομα άλλου και διενέργεια πράξεων που τον προσβάλλουν, αποκλεισμός κάποιου από μια online ομάδα (σε περιπτώσεις συζήτησης ή παιχνιδιών στο διαδίκτυο – online gaming environment[23]– κ.λπ.), λήψη και διάδοση προσβλητικών για το θύμα φωτογραφιών και βίντεο κ.λπ.

Η αθέμιτη χρήση πληροφοριών ως «συστηματική κατάχρηση δύναμης»

Οι αθέμιτες πρακτικές μέσω της χρήσης του διαδικτύου ήδη έχουν κερδίσει και θα κερδίσουν στο μέλλον χώρο, παράλληλα με την επέκταση της χρήση του διαδικτύου.[24] Η κοινωνικοποίηση στο διαδίκτυο είναι επόμενο να μεταφέρει εκεί και τις κοινωνικές παθογένειες, οι οποίες πλέον θα ασκούνται με τρόπους άμεσα συνυφασμένους με τις τεχνολογικές δυνατότητες και την κατάχρηση αυτών.[25]

Επομένως, είναι προφανές ότι η «συστηματική κατάχρηση δύναμης» όπως αναφέρθηκε ανωτέρω, έχει πλέον άμεση σχέση με την χρήση–κάταχρηση της τεχνολογίας. Οι περισσότερες από τις παραπάνω πράξεις, ειδικές εκφάνσεις του διαδικτυακού τραμπουκισμού, απαιτούν από τον θύτη αφενός πρόσβαση σε προηγμένες μορφές της τεχνολογίας και αφετέρου ειδική γνώση της χρήσης της τεχνολογίας. Πρέπει, δε, να ληφθεί υπόψιν ότι αυτή η πρόσβαση στην τεχνολογία –τουλάχιστον για κάποιες από τις ως άνω πράξεις– καθώς και η ειδική γνώση για τον χειρισμό της– αποτελούν στο σύγχρονο συνεχώς εξελισσόμενο τεχνολογικό περιβάλλον, παράγοντες ισχύος. Και σε «μάκρο» επίπεδο, μπορούμε κάλλιστα να ισχυριστούμε πως όποιος ελέγχει την τεχνολογική παραγωγή και την παραγωγή λογισμικών καθώς και κάθε τεχνολογικής μεθόδου έχει σίγουρα

τον εξευτελισμό του και δημοσιοποίηση του υλικού αυτού, αρνητικά σχόλια σε ιστοσελίδες κοινωνικής δικτύωσης και forums ειδικού ενδιαφέροντος κ.λπ. [πρβλ. Β. Πρεκατέ και Ορ. Γιωτάκου, Πρόληψη και αντιμετώπιση του σχολικού εκφοβισμού (bullying) στη Μεγάλη Βρετανία και στις ΗΠΑ, www.obrela.gr]

21. Η συμπεριφορά του hacking αρχικώς σήμαινε τις «καινοτόμες ιδέες αναδιάταξης δεδομένων για την εκτόνωση θεωρητικά και πρακτικά της σύγχυσης που προκαλούσε η αύξηση της γνώσης με τις καθιερωμένες μεθόδους». Η έννοια, βεβαίως, μαζί με τις αντίστοιχες συμπεριφορές εξελίχθηκε σε τέτοιο βαθμό που έχει πλέον αποκτήσει έντονο νομικό ενδιαφέρον και τιμωρείται σε πολλές χώρες (Βλ. πιο αναλυτικά Γ. Λάζου, Πληροφορική και έγκλημα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2001, σελ. 95).

Αναφορικά με το hacking βλ. αναλυτικά Richard Mansfield, Οι χάκερ επιτίθενται, εκδ. Μ. Γκιούρδα, 2001.

22. Βλ. ενδεικτικά Γ. Λάζου, Πληροφορική και έγκλημα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2001, σελ. 109 επ.

23. Πρβλ. Ιωάννης Κατερέλος, Χαρ. Τσέκερης, Μιχ. Λάβδας & Κατερίνα Δημητρίου, Μια ψυχοκοινωνιολογική προσέγγιση της χρήσης του Διαδικτύου και των μαζικών online παιχνιδιών ρόλων (MMORPGs), εις: Κ. Στιλιόπουλου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 69 επ.

24. Αναφορικά με παραβατικές συμπεριφορές στο διαδίκτυο πρβλ. ιδίως και ενδεικτικώς Ν. Κουράκη, Εγκληματολογικοί ορίζοντες, τ. Β': Πραγματολογική προσέγγιση και επιμέρους ζητήματα, 2η εκδ., εκδ. Αντ. Ν. Σάκκουλα, Αθήνα– Κομοτηνή, 2005, σελ. 182 επ. (ενότητα με τίτλο «Το ηλεκτρονικό έγκλημα και το έγκλημα στο Διαδίκτυο» στο κεφάλαιο «Το οικονομικό έγκλημα στην Ελλάδα»), Γ. Λάζου, Πληροφορική και έγκλημα, εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2001, Steven Furnell, Κυβερνοέγκλημα, εκδ. Παπαζήση, Αθήνα, 2006, Χ. Τσουραμάνη, Ψηφιακή εγκληματικότητα – Η (αν)ασφαλής όψη του διαδικτύου, εκδ. Β. Κατσαρού, Αθήνα, 2005 και Αν. Ζάννη, Το διαδικτυακό έγκλημα, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα–Κομοτηνή, 2005.

25. Βλ. χαρακτηριστικά του γράφοντος, Οι εκδηλώσεις παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο – Σκέψεις για τις ανάγκες εκσυγχρονισμού της ελληνικής ποινικής νομοθεσίας, εις: Κ. Στιλιόπουλου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 137 επ.

προβάδισμα έναντι του θύματος – π.χ. στις περιπτώσεις political bullying[26] και κυβερνοτρομοκρατίας[27] και «πολέμου της πληροφορίας» μεταξύ κρατών[28]. Είναι, βέβαια, γεγονός ότι ανά τους αιώνες όποιος είχε τον έλεγχο της τεχνολογίας, κατείχε μια υπεροχή σε επίπεδο ισχύος – χαρακτηριστικό παράδειγμα ο τεχνολογικός ανταγωνισμός κατά τη διάρκεια του ψυχρού πολέμου. Εντούτοις, σήμερα ο ανταγωνισμός έχει γίνει μάλλον πιο «γήινος»!– από το διάστημα έχει περάσει στη διαχείριση δεδομένων και πληροφοριών.[29]

Στο **modus operandi, όπως αναλύθηκε παραπάνω, βλέπουμε ότι οι πράξεις bullying του διαδικτύου** έχουν να κάνουν με την αθέμιτη χρήση ή τον επηρεασμό αυτών των πληροφοριών (η καταστροφή τους, η αλλοίωσή τους, το μπλοκάρισμα της χρήσης τους, η διάδοσή τους, η πρόσβαση σε αυτές χωρίς δικαίωμα). Άρα, μπορεί να υποστηριχθεί ότι **το "bullying του μέλλοντος" στην κοινωνία της πληροφορίας είναι ουσιαστικά το bullying της αθέμιτης χρήσης της πληροφορίας.**

Συνεπώς, είναι γεγονός ότι αυτή **η δυνατότητα πρόσβασης και γνώσης της τεχνολογίας και συνάμα της διαχείρισης των πληροφοριών μετατρέπεται ουσιαστικά σε ισχύ**, αφού για να προβεί κάποιος σε πράξεις, όπως για παράδειγμα η κατασκευή και αποστολή ιών, απαιτεί ειδική γνώση της χρήσης της σχετικής τεχνολογίας. **Επομένως, η ανισορροπία δύναμης, συστατικό στοιχείο των συμπεριφορών τραμπουκισμού (bullying), είναι ουσιαστικά ανισορροπία ισχύος, η οποία είναι άμεσα συνυφασμένη με την πρόσβαση και τη γνώση της τεχνολογίας.** Παραδείγματος χάριν, υπάρχει το δίχως άλλο ανισορροπία δύναμης και ισχύος μεταξύ κάποιου ο οποίος έχει τη γνώση και τη δυνατότητα να αλλοιώνει το περιεχόμενο ιστοσελίδων και κάποιου που δεν έχει αντίστοιχη γνώση να πράξει τα ίδια ή να αμυνθεί.

Επεκτείνοντας τη σκέψη μας, μπορούμε, σύμφωνα με τα παραπάνω, να συνδυάσουμε την εν λόγω διαπίστωση με τη **θεωρία της «διαφορικής παράνομης ευκαιρίας» / «διαφοροποιούσας ευκαρίας»** των **Cloward και Ohlin** σύμφωνα με την οποία ***«ενώ όλα τα μέλη της κατώτερης κοινωνικής τάξης έχουν την ίδια έλλειψη ευκαιρίας για ανάμιξη σε νόμιμες και συμβατικές δραστηριότητες, δεν έχουν την ίδια ευκαιρία συμμετοχής σε παράνομες και παρεκκλίνουσες δραστηριότητες»***[30] καθώς ο έχων μεγαλύτερη πρόσβαση στην τεχνολογία και ειδικότερες γνώσεις έχει αδιαμφισβήτητα περισσότερες ευκαιρίες για αθέμιτη χρήση της πληροφορίας στο διαδίκτυο και γενικότερα της τεχνολογίας. Επίσης, σχετικό είναι σύμφωνα με τα παραπάνω και το **κοινωνικό status των εγκλημάτιών**, κατά τη **θεωρία των εγκλημάτων του λευκού περιλαιμίου** (white-collar crime),[31] το οποίο δύναται να

26. Βλ. Ενδεικτικώς D.L. McCracken, Stephen Harper – The Classic Political Bully, url: http://www.halifaxlive.com/content/view/976/32/

27. Βλ. Αν. Ζαννή, Το διαδικτυακό έγκλημα, εκδ. Αντ. Ν. Σάκκουλα, Αθήνα–Κομοτηνή 2005, σελ. 80 επ. αναφορικά με τους λόγους για τους οποίους χρησιμοποιούν οι «τρομοκράτες πληροφοριών» το διαδίκτυο.

28. Βλ. ενδεικτικά το κεφάλαιο «Ηλεκτρονική Τρομοκρατία και Εγκλήματα Υψηλής Τεχνολογίας» εις Μ. Μπόση, Ζητήματα Ασφάλειας στη Νέα Τάξη Πραγμάτων, εκδ. Παπαζήση, Αθήνα, 1999, σελ. 229 επ. όπου και αναφέρεται: **«Η μεταψυχροπολεμική εποχή βασίζεται και στηρίζεται στην Πληροφορική και στη δυνατότητα αξιοποίησης των νέων μορφών τεχνολογίας προς όφελός της. Ενδιαφέρον παρουσιάζουν τα σενάρια πολέμου, ενός ιδιότυπου ανορθόδοξου πολέμου, που ... αφορά τη χρήση της Πληροφορικής. ... οι Mollander, Riddile and Wilson, σε μελέτη τους για το θέμα, αναφέρονται στη "στρατηγική χρήση του πολέμου της πληροφορικής"»**.

29. Δεδομένη πληροφορία είναι αυτή που έχει ήδη παρασχεθεί (γι' αυτό και η χρήση της μετοχής παρακειμένου) και μάλιστα έχει καταγραφεί με την μορφή καταχώρησής της σε ένα αρχείο. Σήμερα, ο υπολογιστής και γενικότερα οι συσκευές με δυνατότητα σύνδεσης σε δίκτυο είναι αυτές μέσω των οποίων πραγματοποιείται αυτή η (κάποιες φορές) αθέμιτη χρήση των πληροφοριών.

30. Βλ. Alex Thio, Παρεκκλίνουσα συμπεριφορά (επιμ. Χρήστος Τσουραμάνης), ίων, εκδ. έλλην, 2008, σελ. 52, Ν. Κουράκη, Δίκαιο παραβατικών ανηλίκων, εκδ. Σάκκουλα, Αθήνα – Κομοτηνή, 2004, σελ. 103 επ. καθώς και Κ.Δ. Σπινέλλη, Εγκληματολογία – Σύγχρονες και παλαιότερες κατευθύνσεις, 2η εκδ., εκδ. Αντ. Ν. Σάκκουλα, Αθήνα–Κομοτηνή 2005, σελ. 256 επ.

31. Ενδιαφέρουσα στο σημείο αυτό η ανάπτυξη του Λάζου στο κεφάλαιο «Πληροφορικό έγκλημα και εγκλήματα λευκού περιλαιμίου» (Γ. Λάζος, Πληροφορική και έγκλημα, οπ. π., σελ. 55 επ.), όπου αναλύεται η ανάπτυξη του **Sutherland** για τα **εγκλήματα λευκού περιλαιμίου** ("white-

προσφέρει αυτή την ιδιαίτερη πρόσβαση ή γνώση που μετατρέπεται σε ανισορροπία δύναμης, ως ανωτέρω.

Εξάλλου, τούτο ενδυναμώνεται και εκ του ότι, με δεδομένη την «πλαστικότητα» του εγκεφάλου, σύμφωνα με τη νευροβιολόγο Susan Greenfield, «*η συνεχής επαφή με το ίντερνετ μπορεί να επιφέρει κάποιες θετικές αλλαγές, **όπως ένα υψηλότερο IQ και τη δυνατότητα επεξεργασίας πολύπλοκων πληροφοριών σε γρήγορο χρόνο,** αλλά οδηγεί το άτομο στο να συμπεριφέρεται σαν ένα κομπιούτερ και να αναπτύσσει μια ποικιλία αντιδράσεων απέναντι στην ποικιλία ερεθισμάτων που δέχεται. Έτσι, όμως, το άτομο κάνει αυτό που κάνει και ο υπολογιστής: δεν καταλαβαίνει τί συμβαίνει*»[32]. Άρα διαπιστώνεται ότι από τη μια η επαφή με το διαδίκτυο (η δυνατότητα, δηλαδή, πρόσβασης και η γνώση της τεχνολογίας) «δημιουργεί» μάλλον πιο έξυπνους εγκεφάλους[33] (των θυτών δηλαδή) οι οποίοι υπερέχουν σχετικά και έτσι δημιουργείται ανισορροπία σε σχέση με τα υποψήφια θύματα (ιδού η ανισορροπία δύναμης), οι οποίοι όμως από την άλλη στερούνται ενσυναίσθησης (empathy)[34,35] σχετικά και με την ανάπτυξη της κοινωνικής συνοχής ακόμη και σε διαδραστικό επίπεδο. Τούτο είναι εξάλλου λογικό και από την ίδια τη φύση της ηλεκτρονικής επικοινωνίας, η οποία δεν προσφέρει τη δυνατότητα ανάλυσης της ματιάς, του τόνου της φωνής ή ακόμη και της γλώσσας του σώματός του συνομιλητή.[36] Αυτή η «έλλειψη κοινωνικοποίησης» επιτείνει το δίχως άλλο το πρόβλημα της κατάχρησης της τεχνολογίας[37].

Μια επιπλέον σύνδεση της υπερβολικής χρήσης της τεχνολογίας για την κατάχρηση δύναμης στο **cyber bullying μπορεί να βασιστεί στο γεγονός ότι υποστηρίζεται πως σε παιδιά και εφήβους** που καταφεύγουν σε υπερβολική χρήση του διαδικτύου εντοπίζονται, μεταξύ άλλων βιοψυχολογικών επιπτώσεων, μεταβολές στα επίπεδα της κορτιζόλης.[38] Σύμφωνα, δε, με πορίσματα των βρετανών επιστημόνων *Graeme Fairchild* και *Ian Goodyer* προέκυψε ότι στους δράστες πράξε-

collar crime") στην οποία τονίζεται ως ανωτέρω και το κοινωνικό status των εγκληματιών, υπόθεση η οποία είναι το δίχως άλλο αξιοποιήσιμη επιστημονικά και πέραν του στενού πλαισίου επιχείρησης στο οποίο αναφέρευαι κατά κύριο λόγο η ως άνω ανάλυση.

Επίσης, βλ. Αγγ. Κίτσιου & Χρ. Κουρούτζα, Μελετώντας το ηλεκτρονικό έγκλημα στο πλαίσιο της κοινωνίας της πληροφορίας. Πιλοτική έρευνα αναπαραστάσεων σε φορείς του νομού Λέσβου, εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τ. Ι, σελ. 322.

32. Βλ. τη συνέντευξη της Susan Greenfield στο περιοδικό «Ε (έψιλον)» της εφημερίδας «Κυριακάτικη Ελευθεροτυπία», τ. 1037, 27.02.2011 στο δημοσιογράφο Σπύρο Χατζηγιάννη.

33. Βλ. χαρακτηριστικά Γενοβέφας Χρίστου, Οι θετικές επιδράσεις των MMORPGs, εις: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 82 επ., όπου και ως θετικές επιδράσεις στους χρήστες – «παίκτες» αναφέρονται και αναλύονται η ανάπτυξη των αισθήσεων και των οπτικοκινητικών λειτουργιών, η ανάπτυξη ψυχοκοινωνικών δεξιοτήτων (σε επίπεδο βέβαια κοινωνικοποίησης μέσα από τα παιχνίδια και όχι ανάπτυξης απομονωτικής διάθεσης) καθώς και η χρήση των παιχνιδιών αυτών ως υποστηρικτικό και ψυχοθεραπευτικό μέσο.

34. Η ελλείπουσα «ενσυναίσθηση» αποτελεί άλλο ένα χαρακτηριστικό συμπεριφορών των θυτών bullying (βλ. του γράφοντος, Σχολικός τραμπουκισμός, όπ.π. σελ. 87).

35. Βλ. χαρακτηριστικά Ηλία Κορομηλά, Sensibilis modus operandi (?) – Οπτικός πολιτισμός και σύγχρονη εγκληματικότητα, εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τ. Ι, σελ. 362, υποσ. 9 όπου και αναλύεται η έκφραση των συναισθηματικών καταστάσεων σε σχέση με την νευροφυσιολογία του εγκεφάλου.

36. Βλ. ενδεικτικά την ενότητα «Η επίπτωση της προβληματικής χρήσης του Διαδικτύου στις σταθερές σχέσεις» στο πόνημα του Γ. Φλώρου, Η σκοτεινή πλευρά του διαδικτύου – ο ρόλος της πρόληψης, εις: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 104.

37. Εξάλλου, όπως χαρακτηριστικά αναφέρει ο Λάζος για το hacking **«...το hacking φαίνεται να περιλαμβάνει μιαν ισχυρή κοινωνικοσυναισθηματική συνιστώσα, χωρίς την οποία οι υπόλοιπες συνιστώσες του θα παρέμεναν ανενεργές ή θα οδηγούνταν προς άλλες εμφάσεις και εστιάσεις. Πρόκειται για μία μόνιμη δυσφορία του ατόμου απέναντι στον τρόπο που ο γνωστός του κοινωνικός κόσμος είναι οργανωμένος και λειτουργεί.»** (Γρ. Λάζος, Πληροφορική και Έγκλημα, όπ. π., σελ. 98).

38. Έτσι Γιάννης Α. Δελημάρης & Στ. Πηπεράκης, Βιολογική θεώρηση της υπερβολικής χρήσης του Διαδικτύου σε παιδιά και εφήβους, εις: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 220.

ων bullying παρατηρείται χαμηλό επίπεδο της κορτιζόλης και, άρα, γι' αυτό το λόγο εμφανίζουν επιθετικές συμπεριφορές.[39] Συνεπώς, ο Κουράκης επισημαίνει ότι ίσως η μειωμένη παρουσία της ορμόνης αυτής ευθύνεται για την «συναισθηματική ψυχρότητα» που χαρακτηρίζει τους δράστες αυτών των πράξεων, έχοντας προκαλέσει σε αυτούς ένα είδος νοητικής διαταραχής που ευνοεί την (συχνότερη) καταφυγή σε πράξεις βίας.[40]

Εξορθολογισμός της χρήσης των πληροφοριών και πρόληψη

Με αυτά τα δεδομένα, η πρόληψη είναι άμεσα συνυφασμένη με τον εξορθολογισμό της χρήσης της τεχνολογίας[41] και όχι με τη δαιμονοποίησή της, λαμβάνοντας, βέβαια, ως δεδομένο ότι η σύγχρονη επιστημονική οπτική και οι θυματολογικές προσεγγίσεις επιτάσσουν να προβαίνουμε σε θέαση των ως άνω συμπεριφορών και από την πλευρά του θύματος.

Πέραν αυτών, το δίχως άλλο, το δικαίωμα στην πρόσβαση στην τεχνολογία είναι και συνταγματικώς κατοχυρωμένο, ενταγμένο στο δικαίωμα ελεύθερης ανάπτυξης της προσωπικότητας κατ' ά. 5 του Συντάγματος. Επίσης, με το ά. 9Α του Συντάγματος «*Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει*»[42]. Περαιτέρω, **κάθε πρακτική πρόληψης δεν μπορεί να συνίσταται σε πρακτικές μακιαβελικής εμπνεύσεως και «ενοχοποίησης της γνώσης» αλλά να προωθείται κατ' ουσίαν η ίση πρόσβαση στις τεχνολογικές εξελίξεις και η «συμφιλίωση» με την τεχνολογία**.

Προς αυτές τις κατευθύνσεις κινούνται πολλά προγράμματα πρόληψης τα οποία εφαρμόζονται στην Ευρώπη, απευθυνόμενα ιδίως σε ανηλίκους[43]. Χαρακτηριστικά, στην Ιρλανδία[44] έχει οργανωθεί ***εκστρατεία ενημέρωσης και παροχής πρακτικών συμβουλών*** για την αντιμετώπιση του φαινομένου του ψηφιακού τραμπουκισμού σε μια **διαδραστική online υπηρεσία σε διαδικτυακό τόπο,** ήδη από το 2007. Συγκεκριμένα, την 1η Φεβρουάριου 2007 το Υπουργείο Παιδείας και Επιστήμης της Ιρλανδίας (Υπουργός η Hanafin T.D.) άρχισε μια νέα εκστρατεία στο διαδίκτυο με

39. Η κορτιζόλη είναι στεροειδής ορμόνη, της οποίας η αυξημένη παρουσία στον οργανισμό συντελεί στον έλεγχο των συναισθημάτων και καταστέλλει την εκδήλωση βίαιων παρορμήσεων.

40. Έτσι Ν. Κουράκης, Μορφές σχολικής βίας και δυνατότητες αντιμετώπισής της, όπ. π. – ιδίως υποσ. 10. Βλ. σχετικά και το άρθρο του Σπύρου Μανουσέλη με τίτλο «Ορμόνη υπεύθυνη για το bullying» στην εφημερίδα «*ΕΛΕΥΘΕΡΟΤΥΠΙΑ*», 18/10/2009 (url: http://archive.enet.gr/online/online_text/ c=113,dt=18.10.2008,id=69243600).

41. Μια αξιόλογη ανάπτυξη «θετικής» χρήσης του διαδικτύου περιλαμβάνεται στην ανάλυση των Χρήστου Τσουραμάνη & Μαρίνας – Ευγενίας Κορολή, Ο ρόλος του διαδικτύου στην εξάπλωση, αλλά κυρίως στην αντιμετώπιση της σεξουαλικής εκμετάλλευσης των μεταναστών και της καταπάτησης των ανθρωπίνων δικαιωμάτων τους, εις: Τιμητικός τόμος για τον Καθηγητή Ιάκωβο Φαρσεδάκη «Η σύγχρονη εγκληματικότητα, η αντιμετώπισή της και η Επιστήμη της Εγκληματολογίας», εκδ. Νομική Βιβλιοθήκη, Αθήνα, 2011, τ. Ι, σελ. 661 επ. στην ενότητα με τίτλο «Η θετική όψη του διαδικτύου» όπου προτείνονται απλές και εφικτές δράσεις μέσω του κυβερνοχώρου αναφορικά με την προάσπιση των δικαιωμάτων των μεταναστών και την αντιμετώπιση της σεξουαλικής τους εκμετάλλευσης.

42. Βλ. χαρακτηριστικά Ευγενίας Αλεξανδροπούλου – Αιγυπτιάδου, Η νομική προστασία των προσωπικών δεδομένων κατά την πλοήγηση των ανηλίκων στο Διαδίκτυο, εις: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 141. Αναλυτικά για τα προσωπικά δεδομένα και την ανάλυση του ν. 2472/1997 ο οποίος έχει ψηφιστεί δυνάμει της ως άνω αναφερθείσας συνταγματικής επιταγής πρβλ. Π. Αρμαμέντου & Β. Σωτηρόπουλου, Προσωπικά Δεδομένα, εκδ. Σάκκουλα, Αθήνα–Θεσσαλονίκη, 2005. Για τη σύνδεση των προσωπικών δεδομένων με το δικαίωμα στην ιδιωτική ζωή (ά. 8 ΕΣΔΑ) πρβλ. και του γράφοντος, Τα δεδομένα προσωπικού χαρακτήρα στη νομολογία του Ε.Δ.Δ.Α. – Χαρακτηριστικές αποφάσεις αναφορικά με νέες τεχνολογίες, ανακριτικές πράξεις, ελευθερία του τύπου και άσκηση του δικηγορικού επαγγέλματος, Αρχείο Νομολογίας, Ιούλιος–Αύγουστος 2009, σελ. 401 επ. όπου και παρουσιάζονται σχετικές αποφάσεις του Ε.Δ.Δ.Α.

43. Στα καθ' ημάς βλ. χαρακτηριστικά Ηλ. Παρασκευόπουλου, Το Διαδίκτυο ως χρήσιμο εργαλείο και μέσο βοήθειας για την ψυχοκοινωνική υποστήριξη εφήβων, εις: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 27 επ.

44. Βλ. αναλυτικά του γράφοντος, Καλές πρακτικές ευρωπαϊκών χωρών για την αντιμετώπιση της σχολικής βίας, εις: Αλ. Γιωτοπούλου–Μαραγκοπούλου (εκδ. επιμ.), Ομαδική βία και επιθετικότητα στα σχολεία, εκδ. Νομική Βιβλιοθήκη, Αθήνα 2010, σελ. 293 επ.

τίτλο «ΠΡΟΣΕΧΕ ΤΟ ΧΩΡΟ ΣΟΥ – WATCH YOUR SPACE»[45] με στόχο την ενημέρωση και την προαγωγή ασφαλών πρακτικών στους νέους όταν χρησιμοποιούν το Διαδίκτυο προκειμένου να μην πέσουν θύματα πράξεων cyber bullying[46] και βασικό μήνυμα: «*Να είσαι δημιουργικός – Να είσαι ο εαυτός σου – Αλλά να έχεις τον έλεγχο*». Ο ιστότοπος www.watchyourspace.ie προσφέρει πρακτικές συμβουλές και υποστηρίζει τους εφήβους που χρησιμοποιούν το διαδίκτυο. Βασικό χαρακτηριστικό της είναι ότι συμβουλές δίνονται από εφήβους σε εφήβους (peer mentoring).

Η συνδρομή βοήθειας προς την κατεύθυνση της πρόληψης του bullying μπορεί να συνίσταται σε:

- Παροχή βοήθειας τους δράστες προκειμένου να αναπτύξουν άλλες συμπεριφορές οι οποίες να εμφορούνται από πνεύμα δημιουργικότητας στο διαδίκτυο
- Παροχή υποστήριξης σε όσους έχουν αντιληφθεί συμπεριφορές ψηφιακού τραμπουκισμού προκειμένου αυτοί να βρουν τη δύναμη να αντισταθούν και να εναντιωθούν στις εκδηλώσεις bullying

Στο www.watchyourspace.ie μπορεί κανείς να αναζητήσει παρουσιάσεις των βασικών ευρημάτων από μελέτες για τη χρήση του διαδικτύου από εφήβους. Το site είναι, επίσης, συνδεδεμένο με μία online **υπηρεσία γραμμής βοήθειας από την Childline, η οποία είναι μια τηλεφωνική γραμμή υπο**στήριξης και παροχής συμβουλών σε ανηλίκους. Η εκστρατεία προώθησης του site περιλαμβάνει την καμπάνια με αφίσες στα σχολεία. Επίσης, ένα εκπαιδευτικό και ενημερωτικό πακέτο για το πρόγραμμα αποστέλλεται σε όλα τα σχολεία. Τέλος, για την προώθηση χρησιμοποιούνται ενημερωτικά δελτία, posters, e-mails, videos και γενικότερα ο, τιδήποτε μπορεί να τραβήξει την προσοχή μέσω της χρήσης εικόνας και ήχου, όπως visual arts[47] και performace arts[48] κ.λπ.

Το παράδειγμα της Ιρλανδίας έχει ακολουθηθεί σε θεσμικό επίπεδο και από άλλες χώρες της Ευρώπης (π.χ. η Ολλανδία[49]), οι οποίες έχουν αναπτύξει στο διαδίκτυο Οδηγούς Κοινωνικών Δεξιοτήτων απευθυνόμενους σε ανηλίκους.

Τέλος, η τεχνολογία έχει χρησιμοποιηθεί ουσιαστικά για την πρόληψη του bullying. Στη Δανία[50], το Υπουργείο Παιδείας έχει χρηματοδοτήσει την ανάπτυξη ενός ηλεκτρονικού «εργαλείου» το οποίο ονομάζεται *Mobblenøglen (το κλειδί του bullying).* Το ηλεκτρονικό αυτό εργαλείο απευθύνεται σε όλα τα σχολεία και περιλαμβάνει ερωτηματολόγια για παιδιά της 5ης ως και 10ης τάξης (5η Δημοτικού έως 3η Λυκείου) τα οποία συμπληρώνονται μέσω διαδικτύου. Βάσει των απο-

45. Η εν λόγω καμπάνια πραγματώνεται μέσω μιας διαδραστικής online υπηρεσία στον ιστότοπο www.watchyourspace.ie που αναπτύχθηκε από το Εθνικό Κέντρο Τεχνολογίας στη Παιδεία (NCTE).

46. Η Υπουργός Hanafin έθεσε τους στόχους της καμπάνιας στην παρουσίαση αυτής: «οι έφηβοι ενεργά δημιουργούν προσωπικά τους προφίλ, γράφοντας κριτικές στο Amazon, καταγράφοντας κάρτες, φλυαρώντας για τα χόμπι τους και ηχογραφώντας τραγούδια για τις εμπειρίες τους. Βιντεοσκοπούν τα σημαντικότερα γεγονότα στη ζωή τους και τα μοιράζονται με τους φίλους και την οικογένειά τους χρησιμοποιώντας το δίκτυο. Αυτό είναι θαυμάσιο με την προϋπόθεση ότι γίνεται με λογικό, υπεύθυνο και ασφαλή τρόπο ... Όταν οι νέοι είναι online πρέπει να εξασφαλίσουν το ότι οι αυτοί είναι δημιουργικοί, είναι ο εαυτός τους αλλά πάνω από όλα έχουν τον έλεγχο. Το να αποκαλύπτουν υπερβολικά πολλές προσωπικές πληροφορίες μπορεί να θέσει τους νέους σε αυξανόμενο κίνδυνο ... εκμετάλλευσης, εκφοβισμού και παρενόχλησης. Μερικά από τα περιεχόμενα αυτών των sites ποικίλουν από απρόσεκτα έως σοκαριστικά και μπορεί να περιλαμβάνουν άσεμνες σκηνές και εκφοβισμό. ...«εάν δώσεις μια εικόνα στο διαδίκτυο έχασες τον έλεγχο αυτής. Μπορεί να αντιγράφει, αλλαχτεί και εκτεθεί σε διάφορους χώρους χωρίς τη συγκατάθεση σου. Έχε τον έλεγχο δίνοντας μόνο εικόνες για τις οποίες είσαι χαρούμενος να τις δουν όλοι».

47. χρήση εικόνων, γλυπτών και οπτικών μέσων, μέσα από την οποία διευκολύνεται η αποσαφήνιση της έννοιας του bullying

48. δραστηριότητες όπως μουσική, θέατρο, αναπαράσταση ρόλων, δημιουργία σεναρίου σε μια προσπάθεια αναπτέρωσης της συνείδησης των νέων για τα ζητήματα του bullying.

49. Βλ. αναλυτικά του γράφοντος, *Καλές πρακτικές ευρωπαϊκών χωρών για την αντιμετώπιση της σχολικής βίας*, εις: Αλ. Γιωτοπούλου-Μαραγκοπούλου (εκδ. επιμ.), Ομαδική βία και επιθετικότητα στα σχολεία, όπ. π., σελ. 291 επ.

50. Βλ. αναλυτικά του γράφοντος, *Καλές πρακτικές ευρωπαϊκών χωρών για την αντιμετώπιση της σχολικής βίας*, εις: Αλ. Γιωτοπούλου-Μαραγκοπούλου (εκδ. επιμ.), Ομαδική βία και επιθετικότητα στα σχολεία, όπ. π., σελ. 306 επ.

τελεσμάτων, κατασκευάζεται αυτόματα το προφίλ της τάξης ή του σχολείου, από το οποίο μπορούν στη συνέχεια να εξαχθούν πορίσματα για προτάσεις για δράση. Οι προτάσεις αυτές απευθύνονται στους καθηγητές των σχολείων και λαμβάνουν υπόψη τους τα διαφορετικά επίπεδα του προβλήματος όπως «χαρτογραφούνται» ανά σχολείο, τάξη κ.λπ. – εστιάζουν, δε, στην προληπτική δράση δια της ανάπτυξης της κοινωνικής επάρκειας και της ανεύρεσης τρόπων επίλυσης των συγκρούσεων.

Επιμύθιον

Επομένως, πέρα από τις ίσες δυνατότητες πρόσβασης και γνώσης της τεχνολογίας, είναι απαραίτητη, πέρα από τη θωράκισή της με τεχνικά μέσα[51], η ανάπτυξή της με τέτοιο τρόπο ώστε να εμπεδώνεται η αίσθηση της αυτοεκπλήρωσης κάθε ανθρώπου και της ανάπτυξης της προσωπικότητάς του[52], διά της έκφρασης της δημιουργικότητας του χρήστη της τεχνολογίας.

Είναι σημαντικό, δηλαδή, η χρήση και η εκμάθηση της τεχνολογίας να κινείται γύρω από τους άξονες δημιουργίας ατομικής–προσωπικής και κοινωνικής ταυτότητας, δηλαδή της δημιουργίας αντίληψης για τον εαυτό μας και για τη σχέση μας με τους άλλους, και συνεπώς της ένταξης των τεχνολογικών επιτευγμάτων και εξελίξεων στην υπηρεσία του κοινωνικού συνόλου και της κοινωνικής συνοχής, με σκοπό την πρόληψη αντικοινωνικών συμπεριφορών στο διαδίκτυο.

Η **συνειδητοποίηση της αξίας της πληροφορίας στην «κοινωνία της πληροφορίας»**[53] θα είναι φυσικό επακόλουθο των ανωτέρω αντιλήψεων. Η σύμφωνη με αυτές τις επιταγές ανάπτυξη της υπό διαμόρφωση ακόμη «διαδικτυακής ηθικής»[54] θα προλάβει κάθε κατάχρηση του νοήματος της σοφής ρήσης του Francis Bacon «***Η γνώση είναι δύναμη!***»

51. Βλ. Γ. Λάζου, *Πληροφορική και Έγκλημα*, όπ. π., σελ. 174 επ. όπου και αναφέρονται ενδεικτικώς «εργαλειακές κατασκευές για την πληροφορική ασφάλεια».

52. Βλ. και Δημ. Γερούκαλη, Η ανάδειξη του προσώπου ως πρόταση εξόδου από την κρίση της νεωτερικότητας, στο: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 257 επ.

53. Βλ. την ανάπτυξη του Τσουραμάνη για την «ψηφιακή κοινωνία» [Χρ. Τσουραμάνης, Ψηφιακή εγκληματικότητα – Η (αν)ασφαλής όψη του διαδικτύου, όπ. π., σελ. 1, κεφάλαιο «1. Ψηφιακή κοινωνία, Διαδίκτυο (Internet) και ασφάλεια πληροφοριακών συστημάτων»].

54. Βλ. του γράφοντος, Οι εκδηλώσεις παρεκκλίνουσας συμπεριφοράς στο διαδίκτυο – Σκέψεις για τις ανάγκες εκσυγχρονισμού της ελληνικής ποινικής νομοθεσίας, στο: Κ. Σιώμου και Γ. Φλώρου (εκδ. επιμ.), Έρευνα, πρόληψη, αντιμετώπιση των κινδύνων στη χρήση του διαδικτύου, Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο, Λάρισα, 2011, σελ. 137 επ. Επίσης, βλ. αντίστοιχα για τις διαφορετικές προσεγγίσεις –οι οποίες αταλάντευτα συνδέονται με τα (υπό διαμόρφωση) διαδικτυακά ήθη– αναφορικά με τη νομική αντιμετώπιση του πληροφορικού εγκλήματος Γ. Λάζου, Πληροφορική και Έγκλημα, όπ. π., σελ. 83 επ.

«Η προστασία των δικαιωμάτων των παιδιών στο διαδίκτυο. Προτάσεις για δράσεις στο σχολείο»

Γιώργος Μόσχος
Βοηθός Συνήγορος του Πολίτη για τα Δικαιώματα του Παιδιού

Γεια σας. Είμαστε χαρούμενοι που σας βλέπουμε σήμερα και ελπίζουμε κάποια μηνύματα να τα μεταφέρετε στα σχολεία σας, στις οικογένειες σας, κυρίως μηνύματα να περάσουν από τη σημερινή εκδήλωση και βέβαια εμείς οι ενήλικες πρέπει να μελετήσουμε τα μέτρα που χρειάζεται να ληφθούν. Διάλεξα σα θέμα σήμερα «Δράση στο σχολείο» που μας αφορά άμεσα όλους εμάς που ασχολούμαστε με το σχολείο. Τί μπορούμε να κάνουμε γι' αυτήν την τεράστια υπόθεση. Και όχι ότι δεν έχουν υπάρξει κάποιες πρωτοβουλίες, αλλά θεωρούμε ότι υπάρχει πολύ μεγάλο πεδίο να διορθώσουμε και να βελτιώσουμε την καθημερινή πραγματικότητα των παιδιών. Ήταν πάρα πολύ ωραία αυτά που ακούσαμε από την ομάδα των παιδιών YouSmile. Πόσοι θα θέλαμε να είχαμε στο δικό μας το σχολείο μια ομάδα που κάνει τέτοιου είδους δραστηριότητες, ενεργοποιείται, που περνάει καλά, όχι που περνάει το χρόνο της περιμένοντας πότε θα σχολάσει, πότε θα φύγει από ένα βασανιστικό ωράριο.

Ο Συνήγορος του Πολίτη ανέλαβε την αρμοδιότητα του Συνηγόρου του Παιδιού το 2003, κοντεύει τα 10 χρόνια, είναι ο επίσημος θεσμικός φορέας για την προάσπιση των δικαιωμάτων του παιδιού. Είχαμε την ευκαιρία όλα αυτά τα χρόνια να έρθουμε σε επαφή και επικοινωνία με χιλιάδες παιδιά, γονείς, εκπαιδευτικούς.

Ένα περιστατικό θα πω από αυτά που πολύ συχνά συμβαίνουν. Πήγαμε σε μια επαρχιακή πόλη και κουβεντιάζαμε με τα παιδιά σχετικά με την επιθετικότητα, με προβλήματα, διάφορες εμπειρίες και εκεί μου ανέφεραν τα παιδιά για μια μαθήτρια Γυμνασίου που αναγκάστηκε να αλλάξει σχολείο επειδή προηγουμένως είχε γίνει θύμα cyberbullying, αφού της είχαν φτιάξει ένα ψεύτικο προφίλ. Το κορίτσι ζήτησε και άλλαξε σχολείο και εκ των υστέρων ανακάλυψαν το θέμα οι καθηγητές. Τα παιδιά στο σχολείο το ήξεραν, ενώ οι καθηγητές το μάθανε μετά. Αυτό είναι ένα από τα μεγάλα ελλείμματα, ότι εμείς οι μεγάλοι αργούμε να καταλάβουμε, γιατί έχουμε λάθος προτεραιότητες. Οι γονείς που έρχονται σε επαφή μαζί μας είναι πανικόβλητοι "τι να κάνω με το παιδί μου;", "δε ξέρω πού μπαίνει, πού τριγυρνάει στο site", "δε μπορώ να του περιορίσω τις ώρες", "φοβάμαι", "έχω ακούσει για κάτι ειδικά προγράμματα που μπορώ να το παρακολουθώ μυστικά, είναι αποδοτικά;". Κοιτάνε δηλαδή την αγωνία τους και το φόβο τους να τον αντικαταστήσουν με προγράμματα παρακολούθησης.

Τα παιδιά δεν χρειάζονται αστυνόμευση ούτε μυστική παρακολούθηση στο διαδίκτυο, όπως άλλωστε και σε ολόκληρη τη ζωή τους. Χρειάζονται σαφή προσδιορισμό, κατανόηση, συμφωνία και τήρηση των όρων και των ορίων χρήσης του διαδικτύου, με γνώμονα την ηλικία και την ωριμότητά τους, να μάθουν να προστατεύουν τα δικαιώματά τους και να σέβονται τα δικαιώματα των άλλων, χρειάζονται ενημέρωση και επικοινωνία, **ζωντανές σχέσεις** ειλικρίνειας και εμπιστοσύ-

νης με τα υπεύθυνα ενήλικα πρόσωπα της ζωής τους (γονείς, συγγενείς, εκπαιδευτικούς και κάθε είδους φροντιστές τους).

Τα παιδιά δεν κινδυνεύουν τόσο από τη βία και την επιθετικότητα των άλλων, όσο **από την δική τους αδυναμία**, ευαλωτότητα και επιπολαιότητα.

Ένα παιδί που έχει ενημερωθεί και ενδυναμωθεί και που μπορεί να μιλά και να ακούγεται για ό,τι το απασχολεί, δεν γίνεται εύκολα θύμα προσώπων και καταστάσεων.

Ο Συνήγορος του Παιδιού, έχοντας ως αποστολή την προάσπιση και προαγωγή των δικαιωμάτων των παιδιών, γνωρίζει καλά, τόσο από τα ίδια τα παιδιά όσο και από ενήλικες που έχουν ευθύνες στη ζωή τους, ότι αυτά που λείπουν κατ' εξοχήν στη ζωή των παιδιών δεν είναι τόσο τα μέτρα καταστολής όσο η **επικοινωνία, η κατανόηση, η εμπιστοσύνη, η προσεκτική ακρόαση των απόψεων και των συναισθημάτων τους, η βιωματική μάθηση και η καθοδήγησή τους μέσα από το θετικό παράδειγμα των ενηλίκων.**

Η οικογένεια και το σχολείο έχουν πρωτεύοντα ρόλο στο να εκπαιδεύσουν τα παιδιά για όλες τις κοινωνικές τους σχέσεις και ειδικότερα, όσο αφορά τη χρήση του διαδικτύου, για το πώς με ασφάλεια θα ασκούν τα δικαιώματά τους μέσα από αυτό, χωρίς να εκτίθενται ή παγιδεύονται, χωρίς να παραβιάζουν τα δικαιώματα άλλων ή να ανέχονται και να συμμετέχουν σε κάθε είδους παραβιάσεις.

Επειδή οι γονείς συχνά υπολείπονται σε γνώσεις αλλά και σε τεχνικές που θα βοηθήσουν τα παιδιά σε μια ορθολογική και υπεύθυνη χρήση του διαδικτύου, το σχολείο χρειάζεται να αναπτύξει ισχυρότερο ρόλο, κάνοντας ελκυστική τη μάθηση, και προσφέροντας δυνατότητες διαλόγου, επεξεργασίας των βιωμάτων των παιδιών και επίλυσης των ερωτημάτων που διαρκώς γεννώνται σε αυτά.

Προτείνουμε συνεχείς **συμμετοχικές παιδαγωγικές δράσεις** στο σχολείο, από τις πρώτες ηλικίες που ένα παιδί μπορεί να κατανοήσει και να χρησιμοποιήσει το διαδίκτυο, έτσι ώστε να το παρακινήσει στη σωστή χρήση και αυτοπροστασία του. Την ευθύνη των δράσεων αυτών θα πρέπει να αναλάβει η κάθε σχολική μονάδα, με την κατάλληλη υποστήριξη και καθοδήγηση από τις εκπαιδευτικές αρχές.

Με τον όρο συμμετοχικές παιδαγωγικές δράσεις εννοούμε:

- **Διαδραστικές περιηγήσεις** σε εκπαιδευτικούς, ενημερωτικούς και άλλους χρήσιμους ιστοχώρους, ανάλογα με την ηλικία των παιδιών, με έμφαση στα θετικά αλλά και τα αρνητικά στοιχεία του κάθε περιβάλλοντος.
- **Παρουσίαση, με παραδείγματα και παιχνίδια ρόλων**, όλου του πλέγματος **των δικαιωμάτων** των παιδιών, τους τρόπους άσκησης, παραβίασης, αλλά και επίλυσης σε περιπτώσεις σύγκρουσης και ανάγκης στάθμισης τους, με γνώμονα το συμφέρον του παιδιού. Ιδιαίτερη έμφαση να δίνεται στην κατανόηση του περιεχομένου και των ορίων των δικαιωμάτων στην προσωπικότητα, τα προσωπικά δεδομένα, την ιδιωτικότητα, την πρόσβαση σε κατάλληλο για την κάθε ηλικία υλικό, την προστασία από άσκηση βίας, παραπλάνηση, εκμετάλλευση και προκαλυμμένη πληροφόρηση – παρακίνηση, όπως είναι η διαφήμιση.
- **Διάδοση χρηστικών πληροφοριών για τους φορείς προστασίας** από κάθε είδους παραβιάσεις και τους τρόπους προτεινόμενης προσφυγής σε αυτούς.
- **Αναθέσεις στα ίδια τα παιδιά,** για παρουσιάσεις και βιωματική επεξεργασία, παραδειγμάτων, με άξονα και πρίσμα την άσκηση, τον σεβασμό και την προστασία των δικαιωμάτων.
- **Συζητήσεις, σχετικά με τα ειδικότερα προβλήματα,** που μπορεί να αντιμετωπίσει ένα παιδί, είτε κατά την ίδια του την πλοήγηση και την χρήση του διαδικτύου, είτε σε σχέση με

τους γονείς του και το περιεχόμενο της γονικής ευθύνης, που είναι απαραίτητο να γίνει κατανοητό στα παιδιά. Οι συζητήσεις μπορεί να τροφοδοτούνται από σχετικό εκπαιδευτικό υλικό, όπως παρουσιάσεις, μικρά βίντεο ή σχολιασμένες ειδήσεις.

- **Διαθεσιμότητα των εκπαιδευτικών για ατομικές συναντήσεις** με μαθητές τους που ενδεχομένως αντιμετωπίζουν ειδικά προβλήματα που δεν θέλουν να συζητήσουν δημόσια.
- **Ενέργειες διαμεσολάβησης** σε περιπτώσεις που εκδηλώνονται προβλήματα στις σχέσεις μεταξύ των μαθητών, όπως επιθετικότητα και εκφοβισμός, που εκτείνονται και στη διαδικτυακή τους επικοινωνία.
- **Πρωτοβουλίες παραγωγής και διάδοσης μηνυμάτων** από τα ίδια τα παιδιά προς τους συνομηλίκους τους, στο σχολείο ή τους φίλους τους και γνωστούς τους μέσω διαδικτύου.
- **Προτάσεις στα παιδιά για συζητήσεις με τους γονείς** και σαφή συμφωνία για τους όρους χρήσης του διαδικτύου από τα παιδιά στο σπίτι ή σε ίντερνετ καφέ.
- **Ενημερωτικές συζητήσεις των εκπαιδευτικών με τους γονείς,** σχετικά με το περιεχόμενο της γονικής ευθύνης και με την ίδια τη χρήση του διαδικτύου από τα παιδιά τους. Προτροπή στους γονείς να μάθουν καλύτερα το περιεχόμενο, τα μέσα και τους κινδύνους της πλοήγησης στο διαδίκτυο και να επικοινωνούν με τα παιδιά τους, ανταλλάσσοντας πληροφορίες και εξηγώντας τους τις δικές τους ευθύνες.
- **Εκδηλώσεις στη σχολική κοινότητα** για την διάδοση των μηνυμάτων θετικής χρήσης του διαδικτύου και την αντιμετώπιση κινδύνων ή συμπεριφορών που παραβιάζουν δικαιώματα.
- Ο Συνήγορος του Πολίτη, ενεργώντας με την ιδιότητά του ως Συνήγορος του Παιδιού, ακούσει συστηματικά τις απόψεις και τους προβληματισμούς παιδιών, γονέων και εκπαιδευτικών και απαντά σε ερωτήματα ή αιτήματά τους.

Στον ιστοχώρο του υπάρχει ειδικό τμήμα με στόχο την ευαισθητοποίηση σε θέματα χρήσης διαδικτύου (www.0-18.gr/gia-megaloys/internet) ενώ τα ίδια τα παιδιά μπορούν να απευθύνουν ερωτήματα σχετικά με τις παραβιάσεις δικαιωμάτων τους μέσω της σελίδας: Ρωτάω το Συνήγορο (www.0-18.gr/rotao).

«Ο Φόβος στα παραμύθια και το διαδίκτυο. Από την κοκκινοσκουφίτσα στο facebook»

Ελευθέριος Γείτονας Εκπαιδευτικός
Πρόεδρος και Διευθύνων Σύμβουλος στα Εκπαιδευτήρια ΓΕΙΤΟΝΑ

Θέλω πρώτα πριν απευθυνθώ στους μεγάλους να ευχαριστήσω και να καταθέσω το θαυμασμό μου στα παιδιά για την ωραία εικόνα που παρουσιάζουν.

Θα μου επιτρέψετε να συγχαρώ την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος και προσωπικά τον κ. Μανώλη Σφακιανάκη για την διοργάνωση αυτού του Συνεδρίου με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Πλοήγησης στο Διαδίκτυο. Εκτιμώ ότι η προσφορά της Υπηρεσίας αυτής στα Ελληνόπουλα είναι μοναδική και αναγκαία.

Η εισήγησή μου περιλαμβάνει ένα γενικό προβληματισμό για τη «φενάκη της κοσμόπολης», γιατί έτσι νιώθω εγώ σαν δάσκαλος τον κυβερνοχώρο, ή την προβληματική της παγκοσμιοποίησης. Και την προβληματική αυτή θα τη δανειστώ από το πεδίον του στοχασμού του John P. Anton.

Και τολμώ να μοιραστώ μαζί σας τους στοχασμούς του John Anton, διότι η έννοια του κυβερνοχώρου προσεγγίζει και ταυτίζεται, προϊόντος του χρόνου, με την έννοια της παγκοσμιοποίησης και της παγκόσμιας αυτοκρατορίας.

Γράφει λοιπόν στο βιβλίο του «Έρως Πολιτικός» ο John Anton: «Όλες οι αυτοκρατορίες, παλιές και νεότερες, τελικά κατέρρευσαν. Όλες είχαν νόμους, αλλά όχι και δικαιοσύνη. Όλες υιοθετούσαν κάθε μια τη δική της ιδέα για το τι σημαίνει «άνθρωπος», αλλά υστερούσαν σε ανθρωπιά ή γιατί η ιδέα ήταν λειψή, ή γιατί δεν μπορούσε στην πράξη να δώσει το προβάδισμα στο κοινό αγαθό και να υπηρετεί την ισονομία. Θα μπορέσει άραγε το «παγκόσμιο κράτος» να αποφύγει όλους αυτούς τους σκοπέλους; Τολμώ να φτάσω στο συμπέρασμα ότι από μόνη της η τεχνολογία ή και σε συνδυασμό με την πολιτική του κράτους, του όποιου προηγμένου κράτους, όσο κι αν πετύχει να παγκοσμιοποιήσει τις αξίες της και τα αγαθά της, ούτε την παγκόσμια πόλη μπορεί να στηρίξει, ούτε το κοινό αγαθό να προωθήσει. Έχει σωστά τονιστεί ότι «η τεχνολογία από μόνη της δεν είναι ούτε καλή ούτε κακή».

Γίνεται καλή ή κακή σε συνάρτηση με τη δύναμη που την καθοδηγεί και την ελέγχει. Η βασική αυτή διάγνωση μάς ξαναφέρνει στο διαχρονικό ζήτημα της έννοιας του ορθού πολιτικού βίου, του αγαθού βίου και του κοινού αγαθού».

Χρησιμοποιώντας λοιπόν ως υπόβαθρο τους βαθυστόχαστους αυτούς προβληματισμούς περνάμε στην αντίστιξη της διαχείρισης των κινδύνων που αναφύονται από την προσπάθεια των σημερινών ενηλίκων να δημιουργήσουν πεδία αυτονόμησης και ελευθερίας στους πολίτες του μέλλοντος, στα παιδιά μας.

Η «Κοκκινοσκουφίτσα», και χρησιμοποιώ το παραμύθι σα δάσκαλος και παππούς, παίρνει τις βασικές οδηγίες ασφαλούς πορείας: «Κάνε γρήγορα, πριν αρχίσει η μεγάλη ζέστη και πήγαινε σαν καλό κορίτσι, χωρίς να βγεις καθόλου από το δρόμο».

Η οδηγία που έδωσε η μητέρα στην κοκκινοσκουφίτσα είναι γενικού περιεχομένου. Μη βγεις από το δρόμο σου. Δεν της μίλησε καθόλου για το ποιους πειρασμούς και ποιες προκλήσεις θα μπορούσε ενδεχομένως να συναντήσει καθ' οδόν. Δεν της δόθηκαν περιγραφές και βαθύτερη γνώση για το λύκο. Έτσι η Κοκκινοσκουφίτσα επορεύετο αγνοώντας την αγριότητα και τη σαρκοβόρο δυναμική του λύκου. Και όχι μόνο αυτό. Αγνοούσε παντελώς τον δείκτη πονηρίας και ικανότητας αυτού. Ευρισκομένη λοιπόν σε πλήρη άγνοια παρέδωσε τα προσωπικά της δεδομένα, χωρίς καμία επιφύλαξη. Και το χειρότερο παρεξέκλινε η ίδια της πορείας της και παρασύρθηκε από την ευωδία, τα χρώματα και την ποικιλία των ανθέων.

Και ο ανώνυμος αυτός κύριος αξιοποίησε την παρέκκλιση της κοκκινοσκουφίτσας δεόντως. Έτσι καταβρόχθισε την γιαγιά της και την ίδια. Κι ευτυχώς που πέρασε τυχαία ένας κυνηγός κι άκουσε το ροχαλητό του γέρου-αλήτη. Στη συνάντηση αξιολογούνται θετικά δύο γνωρίσματα του κυνηγού. Πρώτον, ότι βρισκόταν σε συνεχή αναζήτηση του λύκου και δεύτερον, ότι είχε την προνοητικότητα πριν ενεργήσει να σκεφτεί τη γιαγιά.

Έτσι δημιουργήθηκαν συνθήκες «κάθαρσης», όπως θα λέγαμε στην περίπτωση της τραγωδίας και όχι μόνο. Αφού το τέλος ήταν καλό, όπως συμβαίνει σε κάθε παραμύθι, η κοκκινοσκουφίτσα είχε την ευκαιρία να συνειδητοποιήσει και να ενστερνιστεί μια σωτήρια για το μέλλον αξιακή γραμμή.

«Ποτέ πια δεν θα ξανατρέξω μόνη μου στο δάσος μακριά από το δρόμο, όταν η μαμά μού το έχει απαγορεύσει».

Ας έρθουμε τώρα στην αντίστιξη των εικόνων του παραμυθιού με όσους συνδέονται με τους κινδύνους του κυβερνοχώρου.

Εικόνες του παραμυθιού	Κομπάρσοι του κυβερνοχώρου
Μαμά της Κοκκινοσκουφίτσας	Οικογένεια – Σχολείο
Δάσος	Διαδίκτυο
Λύκος	Ο άγνωστος που καραδοκεί να παρασύρει τα παιδιά μας στο δρόμο του και να τους αποσπάσει προσωπικά δεδομένα. Να χλευάσει, διασύρει, προσβάλλει και γενικά να συμπεριφερθεί με τρόπο που παραβιάζει βασικά ανθρώπινα δικαιώματα
Κυνηγός	Το θεσμικό πλαίσιο το οποίο πρέπει να επαγρυπνεί και να περιφέρεται για να συναντήσει τον κακό λύκο

Αν πάμε τώρα από το παραμύθι στην παιδαγωγική φιλοσοφία και πρακτική, οδηγούμαστε αβίαστα στην παραδοχή ότι η μύηση των παιδιών μας να μην παρασύρονται στο διαδίκτυο από τους άγνωστους και να μην οδηγούνται στη συγκομιδή ανθέων, όσο εύοσμα και πολύχρωμα κι αν είναι, πρέπει να γίνεται με τρόπο αναλυτικό και όσο γίνεται περισσότερο παραστατικό, χωρίς εκφοβισμούς και απαγορευτικούς αφορισμούς.

Στο σημείο αυτό διατυπώνω την πρόταση να δημιουργηθούν οι παιδαγωγικές και τεχνολογικές προϋποθέσεις προκειμένου να ερευνηθεί ο τρόπος με τον οποίον από το Νηπιαγωγείο θα μπορούσαμε να διαπαιδαγωγήσουμε ή καλύτερα να οπλίσουμε σιγά σιγά τα παιδιά με δεξιότητες για ασφαλή πλοήγηση στον κυβερνοχώρο. Με άλλα λόγια, προτρέπω πτυχιούχους του Παιδαγωγικού Προσχολικής Αγωγής να μπουν στην διαδικασία αναζήτησης μεταπτυχιακών σπουδών

που θα αφορούν στις νέες τεχνολογίες στην προσχολική αγωγή. Επίσης, παρακαλώ τα Πανεπιστήμιά μας να εκπονήσουν μεταπτυχιακά προγράμματα για μύηση των παιδιών από το Νήπιο στη χρήση του διαδικτύου. Πιστεύω πως με την ίδια έννοια που κάνουμε μύηση των παιδιών στην πρώτη ανάγνωση, γραφή και αρίθμηση πρέπει από το Νηπιαγωγείο να διαπαιδαγωγήσουμε τα παιδιά να κάνουν τα πρώτα ασφαλή βήματα στο διαδίκτυο. Μόνο έτσι θα μάθουν να πορεύονται σ' αυτό και να προστατεύονται.

Και διατυπώνω την πρόταση αυτή συνεπικουρούμενος από τις παρακάτω απλές επισημάνσεις:

- Όταν ένα παιδί συνειδητοποιεί την επικινδυνότητα, είναι γεγονός ότι λυτρώνεται και γίνεται πιο προσεκτικό. Η πρόληψη όμως είναι πάντα καλύτερη.
- Όχι απαγόρευση (απόρριψη) και δαιμονοποίηση της χρήσης διαδικτύου. Το διαδίκτυο για τα παιδιά είναι πολύ γοητευτικό. Τους δίνει την πρόσβαση σε έναν κόσμο με πολλά ερεθίσματα και ελευθερίες που στον πραγματικό κόσμο «γεύονται» κυρίως οι ενήλικες. Είναι στημένο με τέτοιο τρόπο, ώστε να είσαι εκεί χωρίς αίσθηση του χρόνου και των περιορισμών/ορίων. Μπορείς να είσαι παντού, οποιαδήποτε στιγμή, ταυτόχρονα!
- Αυτό που πρέπει να συνειδητοποιήσουμε γονείς και δάσκαλοι είναι το εξής: Όπως μαθαίνουμε στα παιδιά πώς να φέρονται και να κυκλοφορούν στην πραγματικό κόσμο, έτσι οφείλουμε να τα εκπαιδεύσουμε πώς να «κυκλοφορούν» και να φέρονται στον εικονικό κόσμο. Ακόμη να τους δίνουμε τόση ελευθερία όσοι μπορούν να διαχειριστούν (ή αλλιώς να θέτουμε τα απαραίτητα για την ηλικία τους όρια – φίλτρα).
- Η οριοθέτηση γονιών και σχολείου προσαρμόζεται στις ηλικιακές και ψυχοσυναισθηματικές ανάγκες των παιδιών. Δηλαδή σε ό,τι αφορά στο διαδίκτυο τα μικρότερα παιδιά θα πρέπει να εκτίθενται σε ένα ελεγχόμενο από τους γονείς περιβάλλον, μέσα από τη χρήση φίλτρων (που περιορίζουν την πρόσβαση σε υλικό που ο γονέας κρίνει ακατάλληλο για το παιδί του). Παράλληλα και καθώς το παιδί μεγαλώνει το νουθετούμε για το πώς οφείλει να φέρεται στις διαδικτυακές του επισκέψεις (τι είναι ασφαλές και ηθικά σωστό να κάνει, ποιοι είναι οι κίνδυνοι και ποιες οι παγίδες). Με άλλα λόγια κάνουμε αυτό που θα κάναμε αν επρόκειτο να επισκεφθεί το παιδί μας ένα δημόσιο, αλλά άγνωστο σ' αυτό χώρο.

Ο προσανατολισμός των παιδιών μας να γίνουν πολίτες του κυβερνοχώρου «καλοί κ' αγαθοί» επιβάλλεται ν' αρχίσει έγκαιρα. Δεν αφήνουμε αυτή τη διαπαιδαγώγηση σε τιμωρητικές αντιλήψεις για την παραβατικότητα στον κυβερνοχώρο. Διότι ναι, μπορεί να τιμωρηθεί ο θύτης, αλλά να μην επουλωθεί ποτέ το ψυχικό τραύμα του θύματος.

Διάβασα στις 27.01.2013 στην Καθημερινή: «Η βία στα Σχολεία και η σιωπή που τη θρέφει» το εξής: « Η πρώτη μαθήτρια ενός Σχολείου έλαβε mail, όπου εμφανιζόταν σε γυμνές φωτογραφίες. Στο κεφάλι της είχε προσαρμοστεί το σώμα μιας άλλης. Το κορίτσι άρχισε να υποφέρει, να χάνει την όρεξή της, να υστερεί στα μαθήματα. Οι γονείς της απευθύνθηκαν στην υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος. Αποκαλύφθηκε ότι ο εκβιάζων ήταν ο δεύτερος «τη τάξει» μαθητής ο οποίος συνέλαβε αυτόν τον τρόπο για να εξουδετερώσει τον αντίπαλο». ΚΑΘ. 27.1.2013 (Η βία στα Σχολεία και η σιωπή που τη θρέφει) Μ. Κατουνάκη.

Αλήθεια ποιος μπορεί να επουλώσει το τραύμα του θύματος ακόμη κι αν τιμωρηθεί αυστηρά ο θύτης; Γι' αυτό, κυρίες και κύριοι, εκείνο το οποίο προέχει στην καταιγίδα που κυοφορείται στα σπλάχνα του κυβερνοχώρου είναι το χτίσιμο «χρηστών πολιτών». Είναι η οικοδόμηση μιας κοινωνίας που τα άτομα που τη συναπαρτίζουν θα εγκολπωθούν τα ίδια αξιακά συστήματα, την ίδια πίστη στον άνθρωπο. Μέσα σ' αυτό το καμίνι του κυβερνοχώρου, ποια είναι η θέση του Σχολείου και της οικογένειας;

Η καλύτερη αντιμετώπιση είναι η πρόληψη.

- **Κύκλοι γονέων** (ενημέρωση γύρω από τους κινδύνους που υπάρχουν για ένα παιδί και για έναν έφηβο) (τμήμα συμβουλευτικής και ψυχολογίας)
- **Ομιλίες σε γονείς** (ευαισθητοποίηση των γονέων σε θέματα γύρω από την πρόληψη και την αντιμετώπιση) (από ειδήμονες)
- **Ενημέρωση παιδιών** (σε ομάδες) (ευαισθητοποίηση παιδιών εφήβων για το τι πρέπει να προσέχουν ή να αποφεύγουν) (από ειδήμονες.)
- **Ενημέρωση εκπαιδευτικών** (ευαισθητοποίηση εκπαιδευτικών γύρω από τους κινδύνους και τις πιθανές δυσκολίες που μπορεί να συμβούν στους μαθητές τους) (τμήμα πληροφορικής και τμήμα συμβουλευτικής και ψυχολογίας)
- **Ενεργοποίηση των εκπαιδευτικών** (με πρωτοβουλίες και δράσεις με τη βοήθεια των οποίων θα οδηγήσουν τα παιδιά στην κατανόηση του φαινομένου της βίας, τόσο στην καθημερινότητα, όσο και στον κυβερνοχώρο)
- **Προληπτικά προγράμματα από το τμήμα συμβουλευτικής και ψυχολογίας μέσα στην τάξη σε όλα τα επίπεδα με στόχο**:
  - το σεβασμό των δικαιωμάτων των παιδιών
  - τον ορισμό των υποχρεώσεων των παιδιών
  - την καλλιέργεια της ενσυναίσθησης
  - τη δημιουργία ενός θετικού κλίματος μέσα και έξω από την τάξη
  - την εκπαίδευση των μαθητών στην επίλυση συγκρούσεων
  - την ενδυνάμωση των σχέσεων μεταξύ των παιδιών

Δημιουργία προγραμμάτων από το Υπουργείο Παιδείας και Δια Βίου Μάθησης με σκοπό το σύνολο των Ελλήνων Εκπαιδευτικών να ενταχθεί στις ίδιες αξιακές γραμμές για την πρόληψη, αντιμετώπιση και θεραπεία του φαινομένου του εκφοβισμού στον κυβερνοχώρο.

Εμπλουτισμός του Αναλυτικού Προγράμματος των Σχολείων Πρωτοβάθμιας και Δευτεροβάθμιας Εκπαίδευσης με δράσεις που θα αναπτύσσουν την άμιλλα, τον αλληλοσεβασμό, την ανθρωπιά, την αγάπη για τη φύση και το δέσιμο και την αλληλοτροφοδότηση των μελών της οικογένειας με κοινούς στόχους και κοινές αξίες.

Αναπλήρωση των χαμένων κοινωνικών λειτουργιών της γειτονιάς λόγω «σκλήρυνσης του κοινωνικού ιστού» από δράσεις του Σχολείου. Οι μεταμορφώσεις που έχουν συμβεί στον κοινωνικό ιστό, όχι μόνο σε επίπεδο πόλεως αλλά και σε επίπεδο γειτονιάς και πολυκατοικίας ακόμη, είναι αισθητές και ορατές από τον καθένα μας. Το κενό αυτό μπορούν να το αναπληρώσουν μόνο τα Σχολεία εκείνα που από κέντρα κατάκτησης της στείρας γνώσης έχουν μεταμορφωθεί σε χώρους Παιδείας και Πολιτισμού.

Θα διατυπώσω μερικές προτάσεις προγραμμάτων που μπορεί να υλοποιηθούν πέρα από την πιστή εφαρμογή και τήρηση του Αναλυτικού Προγράμματος που αποτελεί νόμο του κράτους.

Τα προγράμματα αυτά πραγματοποιούνται στα Εκπαιδευτήρια ΓΕΙΤΟΝΑ εδώ και πολλά χρόνια και είναι ενταγμένα στην δυναμική των επιλεκτικών, προαιρετικών προγραμμάτων. Υποτροφίες που προκηρύσσονται κάθε χρόνο και απονέμονται σε μαθητές/τριες με συγκεκριμένα κριτήρια:

- Πρόγραμμα Απόκτησης Εργασιακής Εμπειρίας για παιδιά Γ' Γυμνασίου κ αι Α' Λυκείου
- Πρόγραμμα παρακολούθησης μαθημάτων Επιχειρηματικής Ηθικής
- Προγράμματα Βιωματικής Μάθησης
- «Γονείς και παιδία παίζει...και μαθαίνει»

- Οικοδεσμός
- Λογοτεχνικές Παραπλανήσεις
- Ταξίδι στο χώρο και το χρόνο
- Γιορτή της ανάγνωσης (Α' Δημοτικού)
- Διαβάζω, επιλέγω, παρουσιάζω (Β' και Γ' Δημοτικού)
- Αθλούμαι – ψυχαγωγούμαι – δημιουργώ (Δημοτικό – Γυμνάσιο) – Προγράμματα του Σαββάτου
- Βιβλιοδρομίες
- Αριθμοδρομίες
- Ευκλείδης – Θαλής – Εύδοξος
- Πιστοποιήσεις Ηλεκτρονικών Υπολογιστών / Ξένων Γλωσσών
- Αθλητισμός
- Τέχνες
- Ελληνικό Πανηγύρι
- Ζούμε σε σκηνές – Γνωρίζουμε τη φύση
- Σπήλαια της Ελλάδος
- Εμπειρίες συγκομιδής καρπών
- Κοινωνική προσφορά
- Ομάδα αιμοδοσίας

Λεπτομέρειες για την Εκπαιδευτική πολιτική και φιλοσοφία όλων των δράσεων που ανέφερα επιγραμματικά μπορείτε να βρείτε στο Web Site: geitonas.edu.gr.

Αφού σας ευχαριστήσω που με ακούσατε θα κλείσω με 4 επισημάνσεις για το τι πρέπει να προσπαθούν να επιτύχουν όλα τα Σχολεία στην Ελλάδα με δράσεις που υπερβαίνουν το επίσημο αναλυτικό πρόγραμμα.

Να μεταδώσουν στα παιδιά το μήνυμα ότι η ζωή θέλει όνειρο, στοχασμό, ευθύνη, δράση, αποφασιστικότητα, προνοητικότητα, σκληρή ατομική προσπάθεια και ικανότητα για συνεργασία.

Να εξασφαλίσουν ένα ακόμη όχημα επικοινωνίας με το χώρο των γραμμάτων, των τεχνών, των επιστημών της τεχνολογίας και της άθλησης.

Να ενσταλάξουν στα παιδιά αρχές και αξίες με τη βοήθεια των οποίων θα μπορέσουν να αναδείξουν τα εν δυνάμει στοιχεία τους και να διακριθούν στο στίβο της ζωής.

Να ενεργοποιήσουν το δυναμικό των παιδιών και να απελευθερώσουν τις δημιουργικές τους δυνάμεις.

Με την Παιδεία και τον Πολιτισμό πιστεύουμε ότι μπορούν να θωρακιστούν τα άτομα και τα κοινωνικά σύνολα από το Λύκο που παραμονεύει στον κοινωνικό περίγυρο και στον κυβερνοχώρο.

«Policy & Privacy Manager Facebook»

Melina Violari

Το Facebook είναι το διαδικτυακό σπίτι εκατοντάδων εκατομμυρίων ανθρώπων. Τίποτα δεν είναι πιο σημαντικό για εμάς από την ασφάλεια όσων χρησιμοποιούν την υπηρεσία μας. Στόχος μας είναι η καινοτομία στην ασφάλεια, γι' αυτό και δημιουργούμε λειτουργίες που αξιοποιούν την κοινωνική φύση της υπηρεσίας μας. Ενδυναμώνουμε και εκπαιδεύουμε τους χρήστες μας, με στόχο τη διεξαγωγή μιας παγκόσμιας συζήτησης τόσο με τους χρήστες όσο και όλους τους άλλους ενδιαφερόμενους.

Για εμάς η ασφάλεια είναι κοινή ευθύνη όλων μας. Στόχος μας είναι να παρέχουμε πάντοτε στους χρήστες απλές πληροφορίες και εύχρηστα εργαλεία, ώστε να απολαμβάνουν με ασφάλεια την πλατφόρμα μας:

- Ένα από τα σημαντικότερα εργαλεία που χρησιμοποιούμε για τη διαδικτυακή ασφάλεια είναι η προώθηση της χρήσης του πραγματικού ονόματος κάθε χρήστη στο Διαδίκτυο. Πιστεύουμε ότι οι χρήστες του Διαδικτύου είναι πιθανότερο να τηρούν τους κανόνες της κοινότητας και να απέχουν από αρνητικές, επικίνδυνες ή εγκληματικές συμπεριφορές, όταν περιβάλλονται από τους φίλους και τους συγγενείς τους. Ζητάμε από όλους να χρησιμοποιούν το πραγματικό τους όνομα, ώστε οι χρήστες μας να γνωρίζουν πάντα με ποιον αλληλεπιδρούν. Με αυτόν τον τρόπο, δημιουργείται ένα ασφαλές περιβάλλον για όλους.
- Το **Κέντρο οικογενειακής ασφάλειας** του Facebook προσφέρει χρήσιμες συμβουλές και πηγές ενημέρωσης σε γονείς και εκπαιδευτικούς, προκειμένου να ενημερώσουν και να δραστηριοποιήσουν τους νέους όσον αφορά το θέμα της ασφάλειας.
- Το Facebook διέπεται από τη Δήλωση δικαιωμάτων και υποχρεώσεων, βάσει της οποίας απαγορεύεται η δημοσίευση περιεχομένου το οποίο παρενοχλεί ή απειλεί οποιοδήποτε άτομο, ή το οποίο περιλαμβάνει εχθρική φρασεολογία ή υποκινεί τη βία.
- Το σύστημα αναφοράς που έχουμε δημιουργήσει και είναι ενσωματωμένο σε σχεδόν κάθε σελίδα και περιεχόμενο που υπάρχει στον ιστότοπο, επιτρέπει στους 1 δισεκατομμύριο χρήστες του Facebook να αναφέρουν οποιοδήποτε περιεχόμενο ή συμπεριφορά που ενδεχομένως παραβιάζει τους όρους της κοινότητάς μας. Η ομάδα των εκπαιδευμένων αναλυτών μας δίνει προτεραιότητα στις πιο σοβαρές αναφορές (π.χ. όσες αφορούν σεξουαλική κακοποίηση ή παρενόχληση) και ανταποκρίνεται σε αυτές, ενώ, ανάλογα με την περίσταση, τις προωθεί στις αστυνομικές αρχές, σε ΜΚΟ ή γραμμές βοήθειας.
- Εκτός από το σύστημα αναφοράς, το Facebook έχει δημιουργήσει ένα νέου είδους εργαλείο το οποίο αξιοποιεί τη δύναμη της κοινότητας. Σε ορισμένες περιπτώσεις, για να κρίνουμε αν κάποιο περιεχόμενο που έχει αναφερθεί παραβιάζει όντως τις πολιτικές του Facebook, χρειάζεται να γνωρίζουμε το ευρύτερο πλαίσιο, αλλά αυτό δεν συμβαίνει συχνά. Επιπλέον, πολλές φορές το πρόβλημα μπορεί να λυθεί με μια απλή συζήτηση μεταξύ των ενδιαφερομέ-

νων. Το νέο πρωτοποριακό εργαλείο που έχουμε δημιουργήσει – το οποίο ονομάζεται «αναφορά κοινωνικού περιεχομένου» – επιτρέπει στους ανηλίκους και σε άλλους χρήστες να ειδοποιούν απευθείας κάποιον άλλο σε περίπτωση που ένας φίλος δημοσιεύσει μια ντροπιαστική ή μη κολακευτική φωτογραφία ή άλλο ενοχλητικό περιεχόμενο. Έτσι, σε περίπτωση που κάποιος νιώθει ότι απειλείται από το δημοσιευμένο περιεχόμενο, έχει την επιλογή, μέσω της αναφοράς κοινωνικού περιεχόμενου, να αναφέρει το περιεχόμενο στο Facebook, να στείλει αντίγραφο του περιεχομένου σε έναν ενήλικο ή φίλο που εμπιστεύεται, ή να μπλοκάρει το άτομο που δημοσίευσε το περιεχόμενο. Χάρη στην πληθώρα των επιλογών που προσφέρουμε για την αντιμετώπιση ανεπιθύμητων συμπεριφορών, οι ανήλικοι μπορούν πλέον να λύνουν τυχόν προβλήματα με αποτελεσματικότερο τρόπο απ' ότι στο παρελθόν.

- Πιστεύουμε ότι κάθε χρήστης πρέπει να έχει τον έλεγχο του περιεχομένου που κοινοποιεί και να επιλέγει το κοινό στο οποίο θέλει να το κοινοποιήσει. Χάρη στις ενσωματωμένες ρυθμίσεις που εμφανίζονται την ώρα που δημοσιεύετε το περιεχόμενο, μπορείτε εύκολα να καταλάβετε ποιος μπορεί να δει κάθε φωτογραφία, ετικέτα, δημοσίευση τοίχου ή άλλο περιεχόμενο που δημοσιεύετε.
- Το **αρχείο δραστηριοτήτων** είναι ένα από τα πιο πρωτοποριακά εργαλεία στο χώρο των μέσων κοινωνικής δικτύωσης. Αποδεικνύει ξεκάθαρα τη δέσμευση του Facebook για την ενσωμάτωση της διαφάνειας και τη δυνατότητα ελέγχου των δεδομένων από μέρους των χρηστών κατά τη χρήση του ιστοτόπου.
- Το αρχείο δραστηριοτήτων παρουσιάζει αναλυτικά και με λεπτομέρειες όλες τις δραστηριότητες κάθε χρήστη στο Facebook από τη μέρα που δημιούργησε το λογαριασμό του. Του δίνει επίσης τη δυνατότητα να αλλάξει την ορατότητα κάθε δραστηριότητας, καθώς και να την αφαιρέσει από το Χρονολόγιό του ή να τη διαγράψει εντελώς.
- Επίσης, το Facebook πιστεύει στην **ενδυνάμωση των χρηστών με αξιόπιστες πληροφορίες**. Έτσι, προσφέρει συμβουλές για τη χρήση των εργαλείων, περιηγήσεις και παράθυρα διαλόγου επιβεβαίωσης τόσο κατά την εγγραφή όσο και την πρώτη φορά που οι χρήστες κοινοποιούν κάτι, ώστε αφενός να κοινοποιούν το περιεχόμενο στα άτομα που θέλουν και αφετέρου να γνωρίζουν πώς να αλλάζουν τις αντίστοιχες ρυθμίσεις στο μέλλον.
- Για παράδειγμα, όταν κάποιος ενημερώνει για πρώτη φορά την κατάστασή του, παρουσιάζονται όλες οι σχετικές ρυθμίσεις και λειτουργίες, καθώς και τα εικονίδια με τις επιλογές απορρήτου («Δημόσια», «Φίλοι φίλων», «Φίλοι», «Μόνο εγώ» και «Προσαρμογή»).
- Πιστεύουμε ότι η ασφάλεια στο Διαδίκτυο είναι ευθύνη όλων μας. Γι' αυτό και συνεργαζόμαστε με οργανισμούς από όλον τον κόσμο, με σκοπό να δημιουργήσουμε ένα άκρως αξιόπιστο, ασφαλές και αποτελεσματικό περιβάλλον. Κατά τη γνώμη μας, η συνεργασία με εξειδικευμένους οργανισμούς είναι απαραίτητη για την προώθηση θεμάτων ασφάλειας. Έτσι δημιουργήσαμε μια παγκόσμια Συμβουλευτική επιτροπή ασφάλειας, η οποία απαρτίζεται από πέντε κορυφαίους οργανισμούς που ειδικεύονται σε θέματα οικογενειακής ασφάλειας (Childnet International, ConnectSafely.org, Family Online Safety Institute, National Network to End Domestic Violence και WiredSafety) και η οποία μας συμβουλεύει όσον αφορά τις καλύτερες πρακτικές. Είμαστε επίσης περήφανοι για τη συνεργασία μας με κυβερνητικούς αξιωματούχους και άλλους ειδικούς (όπως μεταξύ άλλων την ομάδα δράσης Internet Safety Technical Task Force, το πρόγραμμα «Ασφαλέστερο Διαδίκτυο» της ΕΕ, την Klimaka και την National Cyber Security Alliance), για την προώθηση της ασφάλειας στο Διαδίκτυο.

«Οι συνέπειες του κυβερνοεκφοβισμού στην ψυχική υγεία των παιδιών και των εφήβων: Τρόποι αντιμετώπισης του φαινομένου»

Δρ. **Κωνσταντίνος Ε. Σιώμος**
Ψυχίατρος παιδιών και εφήβων
Πρόεδρος της Ελληνικής Εταιρείας Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο

Περίληψη

Περιγράφεται το φαινόμενο του κυβερνοεκφοβισμού, ως η τεχνολογική προέκταση του παραδοσιακού εκφοβισμού και τα βασικά χαρακτηριστικά του. Παρουσιάζονται τα αποτελέσματα ερευνών για τον κυβερνοεκφοβισμό καθώς και οι προτάσεις της Ε.Ε.Μ.Δ.Ε.Δ για την αντιμετώπιση του φαινομένου.

Ραγδαίες εξελίξεις

Η χρήση των κινητών τηλεφώνων και του διαδικτύου θεωρούνταν μέχρι πρόσφατα ότι έχει μόνο πλεονεκτήματα (π.χ., εύκολη και γρήγορη επικοινωνία, πρόσβαση σε απεριόριστο αριθμό πληροφοριών κ.λπ.). Ωστόσο, σταδιακά άρχισε να διαφαίνεται ότι η αλόγιστη, ανεύθυνη και καταναλωτική χρήση των μέσων αυτών μπορεί να προκαλέσει αρνητικές συνέπειες, όπως ο εθισμός στο διαδίκτυο, τα φαινόμενα του ηλεκτρονικού εγκλήματος, οι ηλεκτρονικές απάτες και ο κυβερνοεκφοβισμός. Η δυναμική και το εύρος των αλλαγών από το Διαδίκτυο είναι τέτοια που καμία μεμονωμένη επιστημονική προσέγγιση, ερευνητής ή πόσο μάλλον μεμονωμένος χρήστης δεν μπορεί να την παρακολουθήσει. Χαρακτηριστικό παράδειγμα αποτελούν οι περυσινοί οδηγοί για το Facebook ή τον εκφοβισμό στο Διαδίκτυο οι οποίοι είναι ήδη μέρος της ιστορίας, καθώς το πρώτο άλλαξε τις ρυθμίσεις χρήσης και ο δεύτερος μετανάστευσε από τα chat στα κοινωνικά δίκτυα (Τσορμπατζούδης και συν. 2012).

Εκφοβισμός – Σχολικός εκφοβισμός – Κυβερνοεκφοβισμός

Ο εκφοβισμός είναι ένα παγκόσμιο, διαχρονικό φαινόμενο βίας που εκδηλώνεται σε διάφορους κοινωνικούς χώρους π.χ. σχολείο, χώρος εργασίας, διαδίκτυο.

Ο Σχολικός Εκφοβισμός περικλείει διάφορα φαινόμενα βίας που συμβαίνουν στο σχολικό χώρο κυρίως μεταξύ των μαθητών, έχουν επαναλαμβανόμενο χαρακτήρα και ποικίλη διάρκεια, υπάρχει ανισότητα δυνάμεως μεταξύ δράστη και θύματος ενώ ο δράστης συνειδητά θέλει να προκαλέσει φόβο, άγχος ή ζημιά στο παιδί – στόχο. Συνήθως ο σχολικός εκφοβισμός είναι φανερός, γίνεται πρόσωπο με πρόσωπο σε συγκεκριμένη ώρα και τόπο, διαδίδεται σιγά και σε μικρή έκταση, συντηρείται δύσκολα, ενώ μάρτυρες είναι ως επί το πλείστον μαθητές του εκάστοτε σχολικού περιβάλλοντος.

Ο Κυβερνοκφοβισμός θεωρείται η τεχνολογική προέκταση του παραδοσιακού εκφοβισμού. Είναι συνήθως ανώνυμος, μπορεί να πραγματοποιηθεί με χρήση ηλεκτρονικών μέσων, κάθε ώρα και

σε κάθε μέρος, διαδίδεται γρήγορα και σε μεγάλη έκταση, συντηρείται εύκολα, ενώ μάρτυρες μπορεί να είναι διάφορα άτομα και όχι απαραίτητα άτομα εντός του σχολικού περιβάλλοντος. Βασικές αιτίες του εκφοβισμού είναι η έλλειψη ενημέρωσης – ευαισθητοποίησης, παράμετροι οικογένειας (διαζύγιο – κακοποίηση – παραμέληση – ενδοοικογενειακές συγκρούσεις), εφηβεία, ακαδημαϊκή αποτυχία, φύλο και εθνικότητα.

Έρευνες για τη έκταση του παραδοσιακού εκφοβισμού και του κυβερνοεκφοβισμού

Το 2009 πραγματοποιήθηκε από την HSBC (Health Behavior in School Aged Children) μια έρευνα μεγάλης κλίμακας για τον παραδοσιακό εκφοβισμό, η οποία περιελάμβανε 203.000 εφήβους από σαράντα χώρες (Graig et al. 2009). Τα αποτελέσματα της έρευνας έδειξαν πως τα ποσοστά εκφοβισμού κυμαίνονται από 8,6% στη Σουηδία μέχρι 45,2% στη Λιθουανία. Είναι δηλαδή πολύ υψηλά στις χώρες της Βαλτικής, ενώ οι χώρες της βόρειας Ευρώπης παρουσιάζουν τα χαμηλότερα ποσοστά. Επίσης, διαπιστώθηκε ότι τα αγόρια υπερισχύουν στις εκφοβιστικές πράξεις σε όλες τις χώρες, ενώ σε είκοσι εννέα από τις σαράντα χώρες τα κορίτσια είναι κυρίως τα θύματα. Στην ίδια έρευνα η Ελλάδα εμφανίζει από τα υψηλότερα ποσοστά εκφοβισμού 41,3% σε δείγμα 1713 εφήβων.

Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί την τελευταία πενταετία σε διάφορες χώρες με διαφορετικές μεθοδολογικές προσεγγίσεις, προέκυψε πως η συχνότητα του εκφοβισμού στο Διαδίκτυο εμφανίζεται ως εξής: ΗΠΑ 13,6%, Μ. Βρετανία 22,2%, Βέλγιο 34,6%, Πολωνία 52%, Γερμανία 14,1%, Ισπανία 25–29%, Ιαπωνία 10%, Αυστραλία 4,9–7,6%.

Στην έρευνα EU Kids Online που πραγματοποιήθηκε σε 25 χώρες το 2010 και περιελάμβανε δείγμα 25,142 παιδιών στην Ευρώπη ηλικίας 9–16 ετών, διαπιστώθηκε πως το 6% των παιδιών αναφέρουν πως έπεσαν θύματα του κυβερνοεκφοβισμού, ενώ 19% αναφέρουν πως έχουν εκφοβιστεί εκτός και εντός διαδικτύου (Livingstone et al. 2011).

Απάντηση στο ερώτημα για το ποιά είναι η έκταση του κυβερνοεκφοβισμού σε σχέση με τον παραδοσιακό εκφοβισμό επιχείρησε να δώσει διαχρονική έρευνα μεγάλης κλίμακας που πραγματοποιήθηκε στις ΗΠΑ το χρονικό διάστημα 2007–2010 σε δείγμα 450.490 μαθητών 6–18 ετών και στη Νορβηγία το χρονικό διάστημα 2006–2010 σε δείγμα 9.000 μαθητών 10–16 ετών. Διαπιστώθηκε πως ο κυβερνοεκφοβισμός εντοπίζεται στο 30% του παραδοσιακού εκφοβισμού και στις δύο χώρες, ενώ το 90% των παιδιών που δέχθηκε κυβερνοεκφοβισμό έχει δεχθεί παράλληλα και παραδοσιακό εκφοβισμό. Συνεπώς σύμφωνα με την έρευνα ο κυβερνοεκφοβισμός όταν δεν εξετάζεται μόνος του αλλά στα πλαίσια του ευρύτερου όρου του παραδοσιακού εκφοβισμού είναι ένα φαινόμενο χαμηλής επικράτησης (Olweus 2012).

Ψυχική υγεία και κυβερνοεκφοβισμός

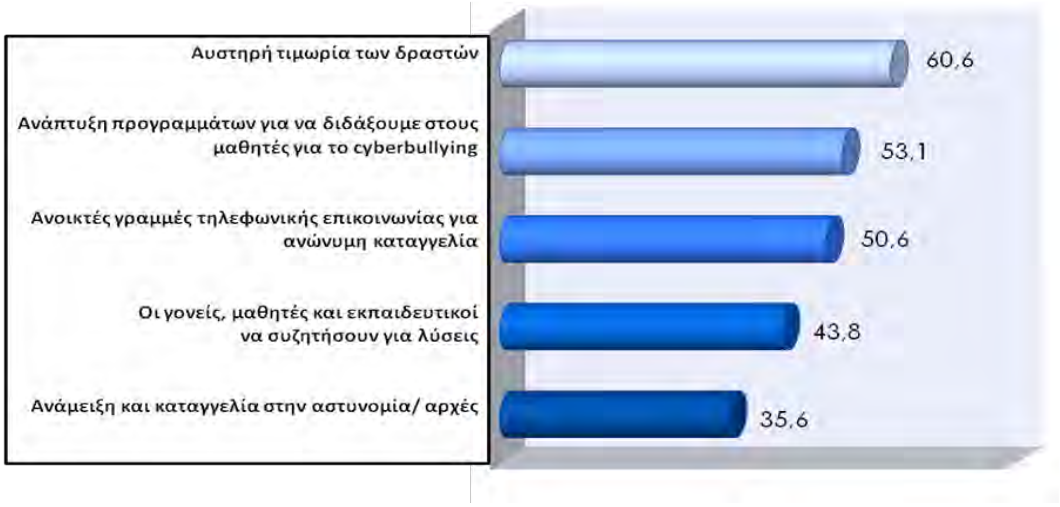
Βάσει ερευνών που έχουν πραγματοποιηθεί, έχει προκύψει πως τα παιδιά και οι έφηβοι που έχουν εκφοβιστεί διαδικτυακά έχουν στατιστικά αυξημένες πιθανότητες να παρουσιάσουν μείζον καταθλιπτικό επεισόδιο σε σχέση με άτομα που δεν έχουν υποστεί εκφοβισμό (Ybarra 2004). Επιπρόσθετα, έχει διαπιστωθεί πως ένα σημαντικό ποσοστό ατόμων που έχουν εκφοβιστεί μέσω διαδικτύου 34% (έχουν δεχτεί σεξουαλικές προσβολές) παρουσιάζουν συμπτώματα διαταραχής μετατραυματικού άγχους (PTSD) είναι ανήσυχα, αγχωμένα και δεν μπορούν να σταματήσουν να σκέφτονται το περιστατικό (Wolak et al. 2006). Τα παιδιά και οι έφηβοι που υφίστανται σεξουαλικό ηλεκτρονικό εκφοβισμό έχουν διπλάσιες πιθανότητες να παρουσιάσουν κατάθλιψη ή να καταφύ-

γουν σε χρήση εξαρτησιογόνων ουσιών από τα άτομα που δέχονται παραδοσιακού τύπου σεξουαλική παρενόχληση. Ακόμη, τα θύματα εμφανίζουν διπλάσια πιθανότητα δήλωσης απόπειρας αυτοκτονίας (Hinduja et al. 2010), ενώ ο συνδυασμός σχολικού εκφοβισμού και κυβερνοεκφοβισμού αυξάνει τα συμπτώματα κατάθλιψης, τους αυτοτραυματισμούς και τις απόπειρες αυτοκτονίας (Schneider et al. 2012). Έχει διαπιστωθεί, τέλος, πως υπάρχει ισχυρή συσχέτιση εκφοβισμού και μελλοντικής παραβατικής συμπεριφοράς (Ttofi et al. 2011).

Συνέδριο E-LIFE (Θεσσαλονίκη 2011)

Το 2011 πραγματοποιήθηκε στη Θεσσαλονίκη το συνέδριο E-LIFE της Ελληνικής Εταιρείας Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο, όπου παρουσιάστηκαν αποτελέσματα ερευνών αναφορικά με τη στάση των εκπαιδευτικών στο φαινόμενο του κυβερνοεκφοβισμού (Μαλαμά 2011). Ειδικότερα, διαπιστώθηκε πως το 44% των εκπαιδευτικών δευτεροβάθμιας εκπαίδευσης δηλώνει πλήρη ή μερική αδυναμία να αναγνωρίσει και να αντιμετωπίσει το φαινόμενο, ενώ το 80% των εκπαιδευτικών της πρωτοβάθμιας εκπαίδευσης και το 81% των εκπαιδευτικών δευτεροβάθμιας εκπαίδευσης θεωρούν ότι δεν έχουν λάβει σχετική εκπαίδευση. Μόνον το 31% των εκπαιδευτικών πρωτοβάθμιας και το 22% της δευτεροβάθμιας εκπαίδευσης θεωρεί την απαγόρευση των κινητών στα σχολεία ως αποτελεσματικό μέτρο.

Επίσης, στο παραπάνω συνέδριο παρουσιάστηκαν οι απόψεις για την αντιμετώπιση του ηλεκτρονικού εκφοβισμού, σε δείγμα δοκίμων αστυφυλάκων (Αδαμοπούλου & Θεολόγη 2011).



Προγράμματα παρέμβασης στα σχολεία

Μια σειρά προγραμμάτων προγράμματα παρέμβασης στα σχολεία για την αντιμετώπιση του φαινομένου του διαδικτυακού εκφοβισμού έχουν εφαρμοστεί σε αρκετές χώρες σε παγκόσμια κλίμακα.

Στη Νορβηγία, στη Σουηδία και στις Η.Π.Α. εφαρμόστηκε το πρόγραμμα παρέμβασης στα σχολεία με την ονομασία «Olweus Bullying Prevention», που περιελάμβανε την εμπλοκή όλων των ενδιαφερομένων (μαθητών- γονέων – εκπαιδευτικών), την ενημέρωση για το πρόβλημα, τη βελτίωση των σχέσεων, την εφαρμογή κανόνων κατά του εκφοβισμού, την εκμάθηση τρόπων άμυνας των θυμάτων και την καλλιέργεια ενσυναίσθησης στους θύτες. Μετά την εφαρμογή του προγράμματος διαπιστώθηκε ότι ο εκφοβισμός μειώθηκε κατά 50% σε διάρκεια είκοσι μηνών.

Στην Αγγλία εφαρμόστηκε το «Πρόγραμμα ολικής απάντησης από το σχολείο» που περιελάμβανε τρία στάδια: το στάδιο διαχείρισης κρίσης, το στάδιο παρέμβασης (εκπαίδευση στην ανάπτυξη διαπροσωπικών δεξιοτήτων), και το στάδιο της πρόληψης (ανάπτυξη ενσυναίσθησης, ανάληψη ευθυνών, δημιουργία θετικού κλίματος, ανταμοιβή καλής συμπεριφοράς κ.α).

Επιπρόσθετα, το 2011 οι Ttofi and Farrington μελέτησαν την αποτελεσματικότητα των παρεμβάσεων για τον εκφοβισμό. Αξιολογήθηκαν συνολικά 44 προγράμματα που κάλυπταν 25 έτη παρεμβάσεων και διαπιστώθηκε πως υπήρξε μείωση του εκφοβισμού κατά 20–23% και μείωση της θυματοποίησης κατά 17–20%. Διαπιστώθηκε επίσης ότι επιτυχία κατά της θυματοποίησης είχαν η προβολή βίντεο, οι πειθαρχικές μέθοδοι, η εργασία με μαθητές, η εκπαίδευση γονέων και η συνεργατική ομαδική εργασία, ενώ επιτυχία στη μείωση του εκφοβισμού είχαν τα προγράμματα κατάρτισης γονέων, η βελτίωση της εποπτείας στο προαύλιο του σχολείου, οι πειθαρχικές μέθοδοι, τα σχολικά σεμινάρια, οι οδηγίες για γονείς, η διατήρηση σχολικών κανόνων και η αποτελεσματική ενδοσχολική διαχείριση του φαινομένου.

Προτάσεις της Ε.Ε.Μ.Δ.Ε.Δ.

Παρουσιάζονται στη συνέχεια οι προτάσεις της Ελληνικής Εταιρίας Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο (Ε.Ε.Μ.Δ.Ε.Δ.) αναφορικά με τη διαχείριση του φαινομένου του διαδικτυακού εκφοβισμού:

Το πρώτο επίπεδο παρέμβασης αφορά στην πρόληψη. Προτείνεται η αξιολόγηση αναγκών μέσα από τεκμηριωμένη έρευνα στην Ελλάδα, με αξιοποίηση εξειδικευμένων επιστημονικών φορέων, η επιμόρφωση εκπαιδευτικών που αναλαμβάνουν προγράμματα αγωγής υγείας, η χρήση κατάλληλων επιμορφωτικών συγγραμμάτων, η δημιουργία διεπιστημονικού κρατικού συμβουλευτικού οργάνου, ο εκσυγχρονισμός των παιδαγωγικών τμημάτων των πανεπιστημίων με την προσθήκη μαθημάτων σε ειδικά θέματα χρήσης των νέων τεχνολογιών και αναπτυσσόμενων συμπεριφορών από τα παιδιά και τους εφήβους (προετοιμασία εκπαιδευτικών στο ταχύτατα αναπτυσσόμενο επιστημονικό πεδίο).

Το δεύτερο επίπεδο παρέμβασης αφορά στη διαχείριση εντός του σχολικού πλαισίου. Προτείνεται η σύνταξη ενός Σχολικού Κανονισμού Λειτουργίας για όλα τα σχολεία σχετικά με τη διαχείριση φαινομένων εκφοβισμού, που θα επικουρείται από το Υπουργείο Παιδείας, την Ανεξάρτητη Αρχή του Συνηγόρου του παιδιού και θα εφαρμόζεται από το σχολείο, η δημιουργία ειδικής φόρμας καταγραφής των περιπτώσεων εκφοβισμού στο σχολείο, η πρόσληψη ενός σχολικού ψυχολόγου ανά πέντε σχολεία και η συνεργασία των σχολείων με εξειδικευμένους επιστημονικούς φορείς μέσα από προγράμματα συνεργασίας.

Συμπεράσματα

Ο διαδικτυακός εκφοβισμός παρουσιάζει παγκόσμια έξαρση, ενώ τα τελευταία χρόνια έχει διαπιστωθεί αρκετά μεγάλος αριθμός περιστατικών και στη χώρα μας. Η κατάλληλη ενημέρωση και επιμόρφωση των παιδιών, των γονέων και των εκπαιδευτικών αποτελεί πλέον μονόδρομο, ώστε να μπορέσει να επιτευχθεί η καλύτερη δυνατή αντιμετώπιση του φαινομένου.

Βιβλιογραφία

1. Craig, Wendy, et al. A cross-national profile of bullying and victimization among adolescents in 40 countries.International journal of public health 54 (2009): 216–224.

2. Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.
3. Dan Olweus (2012): Cyberbullying: An overrated phenomenon? European Journal of Developmental Psychology, 9:5, 520–538.
4. Olweus, D., & Limber, S. P. (2010). The Olweus Bullying Prevention Program: Implementation and evaluation over two decades. In S. R. Jimerson, S.M. Swearer, & D. L. Espelage (Eds.), Handbook of bullying in schools: An international perspective (pp. 377–402). New York, NY: Routledge.
5. Ybarra ML. Linkages between depressive symptomatology and Internet harassment among young regular Internet users. Cyber psychol Behav 2004;7:247–57
6. Wolak, J., Mitchell, K., & Finkelhor, D. (2006). Online victimization: 5 years later. Alexandria, VA: National Center for Missing & Exploited Children
7. Sameer Hinduja & Justin W. Patchin (2010): Bullying, Cyberbullying, and Suicide,
8. Archives of Suicide Research, 14:3, 206–221.
9. Schneider et al. (2012). Cyberbullying, School Bullying, and Psychological Distress: A Regional Census of High School Students. American Journal of Public Health: Vol. 102, No. 1, pp. 171–177.
10. MM. Ttofi et al. (2011). The predictive efficiency of school bullying versus later offending: A systematic/meta-analytic review of longitudinal studies. Criminal Behaviour and Mental Health, 21: 80–89
11. Maria M. Ttofi & David P. Farrington. Effectiveness of school-based programs to reduce bullying: a systematic and meta-analytic review. J Exp Criminol (2011) 7:27–56.
12. Χ. Τσορμπατζούδης, Λ. Λαζούρας, Β. Μπαρκούκης. Κυβερνοεκφοβισμός στην Ελλάδα : Μια διεπιστημονική προσέγγιση. ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ, ΕΥΡΩΠΑΪΚΟ ΠΡΟΓΡΑΜΜΑ DAPHNE III (2012).
13. Σφακιανάκης Ε – Σιώμος Κ – Φλώρος Γ. (2012). Εθισμός στο Διαδίκτυο και άλλες διαδικτυακές συμπεριφορές υψηλού κινδύνου. Εκδόσεις Λιβάνη.
14. Σιώμος Κ– Φλώρος Γ. (2013). E-LIFE. Εκδόσεις Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο, (συλλογικό έργο υπό έκδοση).

«Διαδικτυακός εκφοβισμός, σύγχρονα ερευνητικά δεδομένα, πρόληψη και αντιμετώπιση του φαινομένου»

Βάνια Φισούν Κλινική Ψυχολόγος MSc
Υπ. Διδάκτωρ Παν/μίου Αθηνών, Γ.Ν.Α. «Ο ΕΥΑΓΓΕΛΙΣΜΟΣ»
Ελληνική Εταιρεία Μελέτης της Διαταραχής του Εθισμού στο Διαδίκτυο

Περίληψη

Ο διαδικτυακός εκφοβισμός παρουσιάζει έξαρση τα τελευταία χρόνια, κυρίως μέσω της χρήσης ηλεκτρονικών και ψηφιακών συσκευών. Παρουσιάζονται τα βασικά χαρακτηριστικά των θυμάτων και των θυτών, καθώς και τα αποτελέσματα απογραφικών ερευνών στην Κω τα έτη 2008 και 2010.

1. Διαδικτυακός εκφοβισμός – Cyberbullying

Ο διαδικτυακός εκφοβισμός είναι οποιαδήποτε επαναλαμβανόμενη πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που θεσπίζεται και πραγματοποιείται μέσω της χρήσης των ψηφιακών συσκευών, συγκεκριμένα του Διαδικτύου και των κινητών τηλεφώνων. Περιλαμβάνει πειράγματα με στόχο τη διασκέδαση σε βάρους του θύματος, τη διάδοση προσβλητικών φημών on line, τη δυσφήμηση σε τρίτους μέσω e-mail, SMS, φωτογραφίες-βίντεο στο διαδίκτυο, ιστοσελίδες, blogs, chat rooms και την αποστολή ανεπιθύμητων μηνυμάτων με υβριστικό-προσβλητικό ή σεξουαλικό περιεχόμενο.

Προφίλ θυμάτων

Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί τόσο στο εξωτερικό όσο και στη Ελλάδα, τα θύματα διαδικτυακού εκφοβισμού είναι συνήθως ήσυχα, προσεκτικά και ευαίσθητα παιδιά, ανασφαλή με μειωμένη αυτοπεποίθηση, κοινωνικά απομονωμένα, με αγχώδη ή καταθλιπτική προσωπικότητα, που πιθανόν να παρουσιάζουν κάποιες σωματικές αδυναμίες, επιδιώκουν συνήθως τις επαφές με ενηλίκους και ενδεχομένως να έχουν κάποιο σωματικό πρόβλημα.

Προφίλ θύτη

Τα παιδιά που διαπράττουν διαδικτυακό εκφοβισμό είναι συνήθως σκληρά και χωρίς ενσυναίσθηση, εμφανίζουν ηγετική προσωπικότητα, παρουσιάζουν συχνά επιθετικές συμπεριφορές, ενώ υπακούουν δύσκολα σε κανόνες.

Είναι πιθανόν ένας έφηβος να εκφοβίζει διαδικτυακά κάποιον άλλο έφηβο για να τον εκδικηθεί καθώς μπορεί να έχει πέσει και ο ίδιος θύμα εκφοβισμού στο παρελθόν, ή επειδή πιστεύει ότι έτσι δείχνει δύναμη και εξυπνάδα, ή ακόμη και για να διασκεδάσει.

Οδηγίες προς τους γονείς

Μια σειρά συμπεριφορών μπορεί να προβληματίσει τους γονείς καθώς είναι αρκετά πιθανόν να

συνδέονται με το διαδικτυακό εκφοβισμό. Για παράδειγμα, όταν το παιδί αλλάζει γρήγορα την οθόνη του ή κλείνει προγράμματα όταν πλησιάζει κάποιος τον ηλεκτρονικό υπολογιστή, ή χρησιμοποιεί τον ηλεκτρονικό υπολογιστή οποιαδήποτε ώρα τη νύχτα. Επίσης ο γονέας θα πρέπει να προβληματιστεί όταν το παιδί γίνεται απροσδόκητα αρνητικό εφόσον δεν μπορεί να χρησιμοποιήσει τον ηλεκτρονικό υπολογιστή ή το κινητό του τηλέφωνο ή όταν γελάει υπερβολικά ενώ τα χρησιμοποιεί. Επίσης, ενέργειες όπως η χρήση από το παιδί πολλαπλών λογαριασμών χρήστη ή ενός λογαριασμού που δεν είναι δικός του, και η έκφραση υποτιμητικών σχολίων για συμμαθητές του, είναι πολύ πιθανόν να συνδέονται με το διαδικτυακό εκφοβισμό. Ωστόσο θα πρέπει να είναι κανείς ιδιαίτερα προσεχτικός, καθώς τέτοιου είδους συμπεριφορές μπορεί να συνδέονται με άλλου είδους δυσκολίες της εφηβικής ηλικίας. Καλό θα είναι εφόσον τα προβλήματα έχουν διάρκεια να γίνεται εκτίμηση του παιδιού από έναν ειδικό εξειδικευμένο σε τέτοιου είδους θέματα.

2. Απογραφικές έρευνες στην Κω

Θα παρουσιαστούν στη συνέχεια τα αποτελέσματα δύο απογραφικών ερευνών που πραγματοποιήθηκαν στην Κω. Η πρώτη αφορά δείγμα 121 εφήβων ηλικίας 14–19 ετών και πραγματοποιήθηκε το 2008, ενώ η δεύτερη αφορά δείγμα 2017 εφήβων ηλικίας 12–19 ετών και πραγματοποιήθηκε το 2010.

Στην έρευνα του 2008 διαπιστώθηκε πως το 14,7% των εφήβων βίωσε διαδικτυακό εκφοβισμό, ενώ δεν προέκυψε σημαντική διαφορά ανάμεσα στα δύο φύλα, κάτι το οποίο διαφοροποιείται από τον παραδοσιακό εκφοβισμό, όπου εκεί τα θύματα είναι συχνότερα αγόρια. Εξίσου σημαντικό με βάση τα αποτελέσματα της έρευνας του 2008 ήταν το γεγονός ότι η διαδικτυακή παρενόχληση ήταν συχνότερη σε εφήβους που είχαν προσωπικό ηλεκτρονικό υπολογιστή. Αξίζει όμως να σημειωθεί ότι και ανάμεσα στους έφηβους που δεν είχαν προσωπικό υπολογιστή υπήρχε ένα σημαντικό ποσοστό που είχαν υποστεί παρενόχληση μέσω του διαδικτύου (12.3%). Συμπεραίνεται λοιπόν ότι οι γονείς που είναι εφησυχασμένοι πως ο διαδικτυακός εκφοβισμός δεν αφορά τα δικά τους παιδιά επειδή έχουν υπό έλεγχο τη χρήση του ηλεκτρονικού υπολογιστή στο σπίτι, πρέπει να συνειδητοποιήσουν ότι είναι πιθανό το παιδί τους να υποστεί αυτού του είδους την παρενόχληση. Επιπρόσθετα, διερευνώντας τη σχέση παρενόχλησης και εμπειρίας χρήσης ηλεκτρονικού υπολογιστή διαπιστώθηκε ότι πρακτικά δεν υπάρχει καμία διαφορά ως προς την πιθανότητα κάποιος να είναι θύμα διαδικτυακού εκφοβισμού ανάλογα με το πόση εμπειρία έχει στη χρήση Η/Υ. Η εμπειρία χρήσης δεν συνεπάγεται και προστασία από τη κακόβουλη συμπεριφορά.

Στην έρευνα του 2010 διαπιστώθηκε πως το 30,4% των εφήβων είχε δεχθεί παρενόχληση μέσω διαδικτύου, διπλάσιο ποσοστό σε σύγκριση με τα αποτελέσματα της έρευνας του 2008. Στην έρευνα του 2010 μελετήθηκε ο διαδικτυακός εκφοβισμός και από την πλευρά του θύτη. Ειδικότερα και όπως έδειξε η έρευνα, το 17,1% των εφήβων παραδέχτηκε ότι έχει παρενοχλήσει διαδικτυακά είτε μέσω προσβλητικών μηνυμάτων είτε μέσω μηνυμάτων σεξουαλικού περιεχομένου. Σε αντίθεση με την έρευνα του 2008, η έρευνα που διεξήχθη το 2012 έδειξε ότι τα περιστατικά του διαδικτυακού εκφοβισμού ήταν πολύ συχνότερα στα κορίτσια από ότι στα αγόρια, ενώ προέκυψε ότι είναι πιο πιθανό τα αγόρια να εμπλέκονται σε περιστατικά διαδικτυακού εκφοβισμού από την πλευρά του θύτη σε σχέση με τα κορίτσια. Επίσης, μελετήθηκε η υποκειμενική αίσθηση ευτυχίας σε συνάφεια με τον διαδικτυακό εκφοβισμό, και διαπιστώθηκε ότι οι έφηβοι που έχουν βιώσει τέτοιου είδους εμπειρίες τείνουν να αναφέρουν ότι είναι λιγότερο ευτυχισμένοι σε σχέση με όσους δεν τις έχουν βιώσει. Διαπιστώθηκε ακόμη πως η βίωση εμπειριών διαδικτυακού

εκφοβισμού καθώς και η εμπλοκή σε διαδικτυακό εκφοβισμό έναντι τρίτων συσχετίζονται αρνητικά με τη πορεία της σχολικής επίδοσης. Τέλος, διαπιστώθηκε πως οι καλύτεροι μαθητές τείνουν να αναφέρουν λιγότερες εμπειρίες διαδικτυακού εκφοβισμού, αντιστρέφοντας την εικόνα του παραδοσιακού εκφοβισμού, ενώ ο εκφοβισμός μέσω του διαδικτύου δεν μπορεί να θεωρηθεί ως απλή μετεξέλιξη του παραδοσιακού με τη χρήση νέων μέσων.

Συμπερασματικά, θα πρέπει να τονίσουμε ότι το ποσοστό διαδικτυακού εκφοβισμού διπλασιάστηκε από το έτος 2008 έως το 2010, τα θύματα διαδικτυακού εκφοβισμού είναι συχνότερα κορίτσια ενώ οι θύτες είναι συχνότερα αγόρια, η εμπειρία χρήσης ηλεκτρονικού υπολογιστή δεν αποτελεί και μέτρο προστασίας, ο διαδικτυακός εκφοβισμός επηρεάζει την υποκειμενική αίσθηση ευτυχίας του ατόμου, τόσο για τα θύματα όσο και για τους θύτες προκύπτει μείωση της σχολικής επίδοσης, ενώ ο εκφοβισμός μέσω του διαδικτύου διαφοροποιείται από τον παραδοσιακό εκφοβισμό.

3. Συμβουλές προς τα παιδιά, τους γονείς και τους εκπαιδευτικούς

Όταν ένα παιδί πέσει θύμα διαδικτυακού εκφοβισμού, δεν θα πρέπει να νιώσει φόβο ή ντροπή. Δεν θα πρέπει να απομονώνεται στο σπίτι του αλλά να συνεχίζει τη ζωή του και τις δραστηριότητές του όπως και πριν, και να ενημερώνει άμεσα τους γονείς του ή κάποιον εκπαιδευτικό που εμπιστεύεται ή να ζητήσει βοήθεια από τον ψυχολόγο του σχολείου του.

Οι γονείς μπορούν να προβούν σε μια σειρά ενεργειών προκειμένου να προφυλάξουν τα παιδιά τους από τον διαδικτυακό εκφοβισμό, όπως εγκατάσταση συστήματος φιλτραρίσματος και η διαμόρφωση κώδικα συμπεριφοράς στο διαδίκτυο. Είναι σημαντικό να συμβουλεύουν τα παιδιά τους να προφυλάσσουν τα προσωπικά τους δεδομένα και να σέβονται τους συνανθρώπους τους. Αυτό που θα πρέπει να γίνει αντιληπτό είναι πως η σωστή επικοινωνία γονέα-παιδιών και η ορθή ενημέρωση είναι απαραίτητες. Το παιδί θα πρέπει να μάθει πως θα πρέπει να συμπεριφέρεται στο διαδίκτυο όπως και στην κανονική του ζωή.

Οι εκπαιδευτικοί από την πλευρά τους μπορούν να ερευνήσουν εάν υπάρχουν φαινόμενα διαδικτυακού εκφοβισμού στο σχολείο τους, χορηγώντας απλά και ανώνυμα ερωτηματολόγια προς επίτευξη του σκοπού αυτού. Ιδιαίτερα σημαντική είναι η σωστή κατάρτιση των εκπαιδευτικών ώστε να είναι σε θέση να αντιμετωπίσουν τέτοιου είδους φαινόμενα που παρουσιάζονται στη σχολική κοινότητα, ενημερώνοντας καταλλήλως και τους γονείς των μαθητών τους.

4. Συμπεράσματα

Με την έλευση του διαδικτύου και την ευρεία χρήση των μέσων κοινωνικής δικτύωσης από τους εφήβους έχει παρατηρηθεί έξαρση του φαινομένου του διαδικτυακού εκφοβισμού. Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί, το ποσοστό των εφήβων που έχουν πέσει θύματα διαδικτυακού εκφοβισμού διπλασιάστηκε μέσα σε δύο χρόνια, ενώ τα θύματα είναι συνήθως κορίτσια και οι θύτες αγόρια. Τέλος, τόσο οι γονείς όσο και οι εκπαιδευτικοί οφείλουν να συμβάλλουν στην ορθή ενημέρωση των εφήβων γύρω από το θέμα του διαδικτυακού εκφοβισμού.

5. Βιβλιογραφία

1. Aftab, P. (2006). http://www.wiredsafety.net
2. i-SAFE (2006-2007) National Assessment Center database: Query of pre-assessment question for 5th through 8th grades nationwide for 6-7 academic year

3. Fisoun, V., Floros, G., Siomos, K., Geroukalis, D. (2010) Internet addiction in the island of Hippokrates: impact of gender and age in teenage use and abuse of the internet. 18th European Congress of Psychiatry, Munich, 27/2 – 2/3/2010.
4. Floros, G., Fisoun, V., Siomos, K., Geroukalis, D. (2012) Adolescent online cyberbullying in Greece – the impact of parental online security practices, bonding and online impulsiveness. Journal of School Health
5. Kowalski, R., Limbez, S., Agatston, P. (2008). Cyber Bullying: Bullying in the digital age. Blackwell Publishing
6. King, L. (2006) No hiding from online bullies. Retrieved September 16, 2006, from http://www.news-leader.com/apps/pbcs.dll/article
7. Li, Q. (2006). Cyber bullying in schools: A research of gender differences. *School Psychology International, 27, 157-170.*
8. Olweus, D. (1994). Annotation: Bullying at school: Basic facts and effects of a school-based intervention program. Journal of Child Psychology and Psychiatry, 35, 1171-1190
9. Siomos, K., Dafouli E., Braimiotis D., Mouzas O., Agelopoulos N. Internet Addiction among Greek Adolescent Students. *Cyber Psychology & Behavior*. Vol 11 N 6. 2008.
10. Σιώμος, Κ. (2008) Εθισμός των εφήβων στους Ηλεκτρονικούς Υπολογιστές και το Διαδίκτυο: Ψυχιατρικά συμπτώματα και διαταραχές ύπνου. Διδακτορική Διατριβή, Παν/μιο Θεσσαλίας, Σχολή Επιστημών Υγείας, Τμήμα Ιατρικής.
11. Shariff, S., (2008). Cyber-Bullying. Issues and solutions for the school, the classroom and the home. Routledge
12. Smith, P., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). An investigation into cyber bulling, its forms, awareness and impact, and the relationship between age and gender in cyber bullying. A report to the Anti-Bulling Alliance. Retrieved December 16, 2006, from http://www.dfes.gov.uk/research/data/uploadfiles/RBX03-06.pdf
13. Willard N., (2008) Educator's Guide to Cyberbullying Addressing the Harm Caused by Online Social Cruelty. URL: http://cyberbully.org or http://csriu.org
14. Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining characteristics and associate distress related to Internet harassment: Findings from the second youth internet safety syrvey. Pediatrics, 118, 1169-1177.

«Η απειλή του διαδικτυακού εκφοβισμού: Η Ευρώπη αφυπνίζεται»

Γιώργος Κουμουτσάκος, Ευρωβουλευτής ΝΔ

Κυρίες και κύριοι,

Σας καλωσορίζουμε στην ενότητα του διαδικτυακού ή ηλεκτρονικού εκφοβισμού ως μέρος της ευρύτερης συζήτησης για την ασφαλή πλοήγηση στο Διαδίκτυο.

Πιστεύω ότι αυτή η θεματική συζήτηση είναι εξαιρετικά κρίσιμη, καθώς αφορά το παρόν και το μέλλον της πιο δυναμικής και πιο ευαίσθητης κοινωνικής ομάδας της χώρας και της κοινωνίας μας. Αφορά στα παιδιά μας, στους μαθητές μας, που είναι η βάση του μέλλοντός μας.

Ευχαριστώ ιδιαιτέρως τους διοργανωτές της σημερινής ημερίδας γιατί συμπεριέλαβαν το κρίσιμο ζήτημα του διαδικτυακού εκφοβισμού –ή αλλιώς cyberbullying– στη σημερινή συζήτηση. Είμαι πολύ χαρούμενος που θα μοιραστούμε σκέψεις, προβληματισμούς, τρόπους και λύσεις για μια καλύτερη, πιο υγιή και πιο ασφαλή σχέση χρήστη– μαθητή με το Διαδίκτυο.

Την Τρίτη, 5 Φεβρουαρίου γιορτάσαμε για δέκατη χρονιά την Ημέρα Ασφαλούς Διαδικτύου. Από Ευρωπαϊκής πλευράς, την οποία κατά κάποιο τρόπο εκπροσωπώ σήμερα εδώ, το μήνυμα είναι πολύ σαφές: "Συνδέσου με σεβασμό!– Connect with respect!".

Θα αναφερθώ σύντομα σε κάποια στατιστικά στοιχεία. Είναι γνωστό ότι το διαδίκτυο δε δημιουργήθηκε για παιδιά, τουλάχιστον όχι αποκλειστικά για παιδιά. Ωστόσο, το 75% των παιδιών από 6–17 χρονών στην Ευρώπη το χρησιμοποιούν, ενώ η πλειοψηφία των παιδιών 9–10 χρόνων δηλώνουν ότι άρχισαν να το χρησιμοποιούν ήδη από την ηλικία των 7 ετών. Η εκτεταμένη χρήση του Διαδικτύου από ανηλίκους αναδεικνύει νέες, σοβαρές και πρωτόγνωρες προκλήσεις στη διαχείρισή του.

Πέραν όμως του ευρέος φάσματος ευκαιριών, δυνατοτήτων, ψυχαγωγίας, κλπ, υπάρχουν πολλοί κίνδυνοι. Θα αναφερθώ επιγραμματικά σε κάποιους από αυτούς τους κινδύνους. Σύμφωνα με έρευνα που πραγματοποιήθηκε σε ευρωπαϊκό επίπεδο, 4 στα 10 παιδιά στην Ευρώπη αντιμετώπισαν έναν από τους ακόλουθους κινδύνους:

α) διαδικτυακή επικοινωνία με άτομα που δεν είχαν ποτέ συναντήσει κατά πρόσωπο,
β) έκθεση σε περιεχόμενο που εξωθεί σε ανορεξία, αυτοτραυματισμό, χρήση ναρκωτικών ουσιών ή ακόμα και αυτοκτονία,
γ) διαδικτυακή έκθεση σε εικόνες σεξουαλικού περιεχομένου και κατάχρηση προσωπικών δεδομένων,
δ) διά ζώσης συνάντηση με άτομα που τα παιδιά ήρθαν σε επαφή πρώτη φορά στο Διαδίκτυο, και τέλος
ε) διαδικτυακό εκφοβισμό, που αποτελεί μεγάλο κίνδυνο για την ψυχική υγεία και πολλές φορές την ίδια τη ζωή των παιδιών.

Η εκμετάλλευση των δυνατοτήτων και της ανωνυμίας του διαδικτύου δίνει μια καινούρια, πιο δηλητηριώδη διάσταση σε ένα ήδη επικίνδυνο φαινόμενο – το φαινόμενο του εκφοβισμού και της βίας στο σχολείο ή αλλιώς bullying, που δυστυχώς παρουσιάζει έξαρση τα τελευταία χρόνια.

Στην παραδοσιακή του μορφή, υπήρχε κατά βάση ένας εύσωμος θύτης που είχε διαθέσεις βίαιης συμπεριφοράς ή μια ομάδα που συντονισμένα ασκούσε βία, ψυχολογική ή σωματική, σε ένα μαθητή 'διαφορετικό'. Αυτό προαπαιτούσε επαφή, δύναμη, ή και έναν αριθμό ατόμων, που διαμόρφωναν την ομάδα. Ο θύτης έπρεπε λοιπόν να έχει κάποια χαρακτηριστικά, ορισμένες "προδιαγραφές", ενώ το θύμα συνήθως δύσκολα μπορούσε να αντιδράσει. Όμως, στο διαδίκτυο η κατάσταση είναι διαφορετική. Οι ρόλοι μπορούν να αντιστραφούν ανά πάσα στιγμή. Δεν είναι απαραίτητο ο θύτης να είναι πιο δυνατός, ενώ το θύμα του παραδοσιακού bullying, στην αυλή του σχολείου, μπορεί "εύκολα" να μετατραπεί σε θύτη στον ανώνυμο και πολυδαίδαλο κόσμο του διαδικτύου.

Επομένως, το διαδίκτυο δίνει νέα διάσταση, βάθος και ένταση σε αυτό το νοσηρό φαινόμενο, καθιστώντας το ακόμη πιο πολύπλοκο.

Είναι πεποίθησή μου ότι η διάκριση, επιπόλαιη και βιαστική, θύτη- θύματος είναι σε μεγάλο βαθμό εσφαλμένη. Μιλάμε για παιδιά που είναι μπλεγμένα στα δίχτυα της ίδιας νοσηρής κατάστασης. Όση φροντίδα και προσοχή χρειάζεται το θύμα, άλλη τόση χρειάζεται και ο θύτης. Στην πρώτη περίπτωση, αυτή του θύματος, η κατάληξη μπορεί να είναι πολύ τραγική. Στην περίπτωση του θύτη, η κατάληξη μπορεί να είναι οι φυλακές ανηλίκων. Βεβαίως και είναι διαφορετική η βαρύτητα της ίδιας της πράξης και των επιπτώσεών της. Επειδή λοιπόν μιλάμε για νέα παιδιά, θα πρέπει να δούμε θύτη και θύμα σαν τις όψεις του ίδιου νομίσματος.

Συμπερασματικά, τονίζω ότι: δεν πρέπει να προβούμε σε δαιμονοποίηση του μέσου, δηλαδή του διαδικτύου. Όχι στην τιμωριτική στάση γονέων και εκπαιδευτικών, ναι στη χρήση του Διαδικτύου αλλά με μέτρο. Φροντίδα από εκπαιδευτικούς, φροντίδα από γονείς. Πάνω από όλα όμως, είναι απαραίτητο να σπάσει η ιδιότυπη σιωπή που περιβάλλει το φαινόμενο του εκφοβισμού. Μόνον έτσι μπορούν να διαγνωστούν και να αντιμετωπιστούν αποτελεσματικότερα φαινόμενα διαδικτυακού –αλλά και ενδοσχολικού– εκφοβισμού.

Κλείνοντας, απευθύνω μια παράκληση, μια ενθάρρυνση για τα παιδιά που μας ακούν: Αν ποτέ τύχει, είτε εσείς είτε κάποιος συμμαθητής σας να εμπλακεί σε φαινόμενα διαδικτυακού εκφοβισμού, μη διστάσετε να το κοινοποιήσετε όσο το δυνατό γρηγορότερα. Να ζητήσετε βοήθεια. Υπάρχουν ασφαλή σημεία καταφυγής: το σπίτι, η οικογένεια, και το σχολείο, η "εκπαιδευτική οικογένεια".

Σας ευχαριστώ πολύ!

«Διαδίκτυο και Εφηβεία: αποτελέσματα της Ευρωπαϊκής μελέτης EU-NET ADB»

Δρ. **Άρτεμις Τσίτσικα**,
Λέκτορας Εφηβικής Παιδιατρικής
Επιστημονική Υπεύθυνος
Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.)
Β΄ Παιδιατρική Κλινική Πανεπιστημίου Αθηνών,
Νοσοκομείο Παίδων «Π. & Α. Κυριακού»

Βασιλική Δημητρακοπούλου,
Ψυχολόγος,
Επιστημονική Συνεργάτης
Μονάδας Εφηβικής Υγείας (Μ.Ε.Υ.)
Β΄ Παιδιατρική Κλινική Πανεπιστημίου Αθηνών,
Νοσοκομείο Παίδων «Π. & Α. Κυριακού»

Περίληψη

Ο διαδικτυακός εκφοβισμός αποτελεί ένα φαινόμενο με τεράστια έξαρση που απασχολεί πλέον ολοένα και μεγαλύτερο ποσοστό παιδιών και εφήβων σε πανευρωπαϊκό επίπεδο. Παρουσιάζονται τα αποτελέσματα της έρευνας EU-NET ADB.

Εισαγωγή

Σύμφωνα με μελέτες, το 92% των εφήβων είναι μέλη σε κοινωνικά δίκτυα. Ειδικότερα, το 39.4% των εφήβων κάνει χρήση των μέσων κοινωνικής δικτύωσης πάνω από δύο ώρες καθημερινά ενώ το 60.2% κάνει χρήση πάνω από δύο ώρες το Σαββατοκύριακο. Πολλές από τις συμπεριφορές των σημερινών εφήβων είναι παρόμοιες με εκείνες των άλλων γενεών. Τα δίκτυα κοινωνικής δικτύωσης θα μπορούσαν να συγκριθούν με τα «στέκια» των προηγούμενων γενεών, όπου οι έφηβοι συναθροίζονται και επικοινωνούν.

Το φαινόμενο του «εκφοβισμού» γνωστό και ως «bullying» που εκδηλώνεται στο χώρο του σχολείου ή σε άλλα περιβάλλοντα συνάθροισης των νέων, έχει μεταφερθεί πλέον και στο διαδικτυακό κόσμο. Για την περιγραφή του φαινομένου αυτού δημιουργήθηκε ο όρος «διαδικτυακός εκφοβισμός» ή αλλιώς «cyberbullying».

Διαδικτυακός εκφοβισμός

Διαδικτυακός εκφοβισμός είναι κάθε συμπεριφορά που συμβαίνει ηλεκτρονικά ή ψηφιακά από άτομα ή ομάδες, τα οποία επαναλαμβανόμενα στέλνουν εχθρικά ή επιθετικά μηνύματα, με πρόθεση να βλάψουν ή να προκαλέσουν δυσφορία στους άλλους.

Έρευνα EU-NET ADB

Η Έρευνα EU-NET ADB πραγματοποιήθηκε σε επτά ευρωπαϊκές χώρες με συντονίστρια χώρα την Ελλάδα (Ελλάδα, Γερμανία, Ισπανία, Πολωνία, Ισλανδία, Ολλανδία, Ρουμανία) και ολοκληρώθηκε το 2012.

Σκοπός της έρευνας ήταν να αξιολογήσει τη σχέση μεταξύ των εφήβων που είχαν υποστεί «διαδικτυακό εκφοβισμό» και των τωρινών ψυχοκοινωνικών τους δυσκολιών καθώς και να αξιολογήσει το συναίσθημα «πρόκλησης βλάβης» εξαιτίας αυτού του εκφοβισμού στους εφήβους και

τη σχέση αυτού του συναισθήματος με διάφορους ψυχοκοινωνικούς παράγοντες.

Πρόκειται για μια ποσοτική έρευνα που περιελάμβανε τη δημιουργία Ερωτηματολογίου-Εργαλείου σχετικά με τη διαδικτυακή χρήση και την ψυχοκοινωνική κατάσταση των παιδιών. Επιλέχθη αντιπροσωπευτικό δείγμα εφήβων 15-16 ετών, με 2000 ερωτηματολόγια από κάθε χώρα (συνολικά 14000 ερωτηματολόγια).

Τα αποτελέσματα της έρευνας έδειξαν ότι περισσότερο από ένας στους πέντε εφήβους έχουν πέσει θύματα «διαδικτυακού εκφοβισμού» (21.9%). Τα κορίτσια παρουσίαζαν μεγαλύτερα ποσοστά έκθεσης σε διαδικτυακό εκφοβισμό, ενώ οι χώρες με τα μεγαλύτερα ποσοστά ήταν οι Ρουμανία και Ελλάδα και τα μικρότερα οι Ισλανδία και Ισπανία. Η ηλικία των εφήβων, αλλά και το χαμηλό ή μέτριο μορφωτικό επίπεδο των γονέων φάνηκε ότι σχετίζεται με το φαινόμενο του «διαδικτυακού εκφοβισμού». Οι ψυχοκοινωνικοί παράγοντες σχετίζονται επίσης, στενά με το φαινόμενο του «διαδικτυακού εκφοβισμού» και με το συναίσθημα ότι έχουν υποστεί «βλάβη» από αυτόν. 53.5% από τους εφήβους που δέχθηκαν διαδικτυακό εκφοβισμό δηλώνουν ότι είχε αρνητικό αντίκτυπο στον ψυχικό τους κόσμο το γεγονός ότι είχαν υποστεί το φαινόμενο αυτό. Παρατηρείται μεγάλη διαφοροποίηση ανά χώρα σχετικά με το ποσοστό των εφήβων που «νιώθουν αναστατωμένοι» επειδή έχουν υποστεί «διαδικτυακό εκφοβισμό».

Κίνδυνος *vs* βλαπτικής επίδρασης

Μεγάλος αριθμός εφήβων μπορεί να εκτεθεί σε διαδικτυακό κίνδυνο, ωστόσο ένα πολύ μικρότερο ποσοστό βλάπτεται από αυτή την έκθεση. Η εκπαίδευση των παιδιών και των εφήβων στη διαχείριση κινδύνου αποτελεί την καλύτερη λύση. Πολύ σημαντικό ρόλο στην επίπτωση του διαδικτυακού εκφοβισμού σε ένα παιδί παίζει η ευαισθησία της προσωπικότητας του, η κληρονομικότητα, το οικογενειακό, το σχολικό και το κοινωνικό περιβάλλον. Μάλιστα, όπως έχει διαπιστωθεί, η διαφορετικότητα στην εμφάνιση, στην εθνικότητα, στη σχολική επίδοση και στη συμπεριφορά μπορεί να οδηγήσει ένα παιδί στο να υποστεί διαδικτυακό εκφοβισμό. Ένα δημοφιλές και κοινωνικό παιδί στα δίκτυα κοινωνικής δικτύωσης μπορεί να πέσει θύμα εκφοβισμού λόγω φθόνου. Αρκετές φορές μάλιστα είναι πιθανό ο θύτης να υπήρξε και ο ίδιος θύμα, ενώ συχνά ο θύτης ελπίζει ότι τα θύματα του δεν θα τον μαρτυρήσουν, συνεχίζοντας έτσι ανενόχλητος τα πειράγματα.

Συμβουλές για γονείς και εκπαιδευτικούς

Κάποια σημάδια που μπορεί να οδηγήσουν έναν γονέα να αντιχνεύσει ότι το παιδί του έχει πέσει θύμα διαδικτυακού εκφοβισμού ενδέχεται να είναι τα εξής: διατροφική διαταραχή, διαταραχές ύπνου, πτώση σχολικής επίδοσης, απομόνωση (αδιαφορία για φίλους, φλέρτ κ.λπ.), αδιαφορία για την εμφάνιση και τη σωματική υγιεινή. Σε κάθε περίπτωση, οι γονείς θα πρέπει να παρέχουν συναισθηματική κάλυψη στα παιδιά τους, να σέβονται την προσωπικότητα τους, να παρέχουν εμπειρία ζωής στα μικρότερα παιδιά για όσα χρειάζεται να προσέχουν στο διαδικτυακό κόσμο και να συμφωνούν μαζί με τους εφήβους τα όρια και τους κανόνες κατά την πλοήγηση τους στο Διαδίκτυο.

Ο ρόλος του σχολείου είναι εξίσου σημαντικός, διότι μερικές φορές είναι πιο εύκολο να παρατηρήσει ο εκπαιδευτικός μια ανορθόδοξη συμπεριφορά του παιδιού. Οι εκπαιδευτικοί είναι σε θέση-κλειδί για την πρόληψη και την πρώιμη αντιμετώπιση και για το λόγο αυτό χρειάζεται να υπάρχει ενημέρωση και κατάρτιση. Η Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) στο πλαίσιο του Προγράμματος ΑΡΙΑΔΝΗ έχει ήδη ενημερώσει 1000 ειδικούς επιστήμονες, μεγάλο ποσοστό εκ των οποί-

ων είναι εκπαιδευτικοί, προκειμένου να βοηθούν σε θέματα ασφάλειας και υπερβολικής χρήσης του διαδικτύου.

Συμβουλές για παιδιά και εφήβους

Τα παιδιά και οι έφηβοι θα πρέπει να γνωρίζουν ότι κανένας δεν έχει δικαίωμα να τους κάνει πλάκα και να τους στενοχωρεί στο διαδίκτυο και στην περίπτωση που κάποιος τους παρενοχλεί διαδικτυακά δεν θα πρέπει να μπαίνουν στη διαδικασία να απαντούν. Δεν χρειάζεται να υπομένουν τον καθένα, πρέπει να προστατέψουν τον εαυτό τους. Για το λόγο αυτό χρειάζεται να συζητούν τέτοια περιστατικά με τους γονείς τους ή κάποιον καθηγητή/δάσκαλο και να κάνουν καταγγελία στο www.safeline.gr ή να τηλεφωνούν χωρίς χρέωση στη Γραμμή ΥΠΟΣΤΗΡΙΖΩ 8001180015 της Μονάδα Εφηβικής Υγείας (Μ.Ε.Υ.) για συμβουλές.

Είναι σημαντικό επίσης, τα παιδιά και οι έφηβοι να εκπαιδεύονται να μην αποκαλύπτουν τα προσωπικά τους στοιχεία στο Διαδίκτυο, να μη συναντούν άγνωστους «φίλους» που έχουν επικοινωνήσει μαζί τους διαδικτυακά, να μη δέχονται οποιαδήποτε διαδικτυακή πληροφορία χωρίς να την ελέγχουν για την αξιοπιστία της και να συζητούν την έκθεσή τους σε πορνογραφικό, ρατσιστικό, βίαιο και γενικά ακατάλληλο περιεχόμενο με γονείς ή δασκάλους τους.

Συμπεράσματα

Τα παιδιά και οι έφηβοι πρέπει να ενημερώνονται σωστά για τις δυνατότητες που παρέχει η χρήση του Διαδικτύου, αλλά και τους κινδύνους που ενδέχεται να αντιμετωπίσουν προκειμένου να μπορούν να τους περιορίσουν.

«Διαδικτυακός εκφοβισμός: Μύθος και Πραγματικότητα»

Εμμανουήλ Σφακιανάκης,
Αστυνομικός Διευθυντής,
Προϊστάμενος Υποδιεύθυνσης
Δίωξης Ηλεκτρονικού
Εγκλήματος

ΓΑΛΑΝΗ Όλγα
Υ/Α΄ της Υποδιεύθυνσης
Δίωξης Ηλεκτρονικού
Εγκλήματος

ΚΩΝΣΤΑ Λαμπρινή
Υ/Α΄ της Υποδιεύθυνσης
Δίωξης Ηλεκτρονικού
Εγκλήματος

Θα ήθελα να σας ευχαριστήσω από καρδιάς γιατί είναι μεγάλη τιμή για την Ελληνική Αστυνομία και τη Δίωξη Ηλεκτρονικού Εγκλήματος η παρουσία σας στο σημερινό συνέδριο. Θα πρέπει όμως να γνωρίζετε κάποιες αλήθειες. Η πρώτη μεγάλη αλήθεια είναι ότι η Ελληνική Αστυνομία και η Δίωξη Ηλεκτρονικού Εγκλήματος έχει κάνει πολλά για εσάς, και κάνει κάθε μέρα πολλά για εσάς, τα οποία πρέπει να τα μάθετε. Όταν παρέλαβα την Υπηρεσία οι παιδόφιλοι δεν τιμωρούνταν. Έπρεπε να αποδείξουμε κερδοσκοπία για να τιμωρηθεί ο παιδόφιλος. Το 2007 άλλαξε η νομοθεσία στη χώρα μας, και έτσι το ελληνικό κράτος έχει φτιάξει μια πολύ καλή νομοθεσία πάνω στην παιδοφιλία και τιμωρείται πλέον και ο Έλληνας παιδόφιλος.

Δεύτερον, θα πρέπει να γνωρίζετε ότι η Ελληνική Αστυνομία έχει εξοπλιστεί με προγράμματα και συστήματα ώστε να εντοπίζει εικοσιτέσσερις ώρες το εικοσιτετράωρο αυτούς που θέλουν να σας κάνουν κακό, τους παιδόφιλους. Άρα, ότι κινείται στο Διαδίκτυο όλο το εικοσιτετράωρο εντοπίζεται με ειδικά προγράμματα, με αποτέλεσμα να έχουμε εντοπίσει, συλλάβει και στείλει στη Δικαιοσύνη περίπου οκτακόσιους παιδόφιλους.

Τρίτον, θα πρέπει να γνωρίζετε ότι έχουμε αναπτύξει ειδικούς μηχανισμούς και πυρήνα Αξιωματικών οι οποίοι όλο το εικοσιτετράωρο εντοπίζουν και ελέγχουν παιδιά που έχουν βγάλει στο Διαδίκτυο μηνύματα απόγνωσης – θέλουν να φύγουν από τη ζωή. Πάνω στο θυμό τους, και λόγω της εφηβείας , γράφουν «Δεν αντέχω άλλο, θέλω να φύγω». Μάλιστα, μέχρι σήμερα έχουμε εντοπίσει και σώσει περί τα επτακόσια άτομα που εξεδήλωσαν την πρόθεση τους να αυτοκτονήσουν, η πλειοψηφία των οποίων ήταν παιδιά. Μπορεί μέσα από έναν απλό διαπληκτισμό με τους γονείς σας να πάρετε μια λάθος απόφαση. Δεν θα ξεχάσω ποτέ την υπόθεση μιας κοπέλας δεκαοκτώ χρονών, που όταν τη σώσαμε και ήρθε στο γραφείο μου ο πατέρας της να με ευχαριστήσει, η κοπέλα ενώπιον του πατέρα της, του κ. Γιαννόπουλου από το «Χαμόγελο του Παιδιού» και μιας ψυχολόγου, είπε το εξής: «Πατέρα, αν δεν υπήρχε ο κ. Σφακιανάκης και οι Αξιωματικοί του, εγώ σήμερα δεν θα ήμουν εδώ!». Θυμάμαι πολύ έντονα αυτή την υπόθεση, έχει χαράξει τη μνήμη και την πορεία μου. Γιατί δίνουμε καθημερινά τη ζωή μας, κάνουμε αγώνα δρόμου και εμείς και οι Εισαγγελείς όλης της χώρας τους οποίους θα ήθελα να ευχαριστήσω, γιατί είναι κοντά μας καθημερινά. Θα ήθελα να ευχαριστήσω ιδιαιτέρως τον κ. Τέντε, την κ. Φάκου, τον κ. Μαρκογιαννάκη, τον κ. Δραγάτση και τον κ. Παναγόπουλο, που είναι κοντά μας εικοσιτέσσερις ώρες το εικοσιτετράωρο.

Σήμερα ήρθαμε να μοιραστούμε εμπειρίες μαζί σας που προκύπτουν από την καθημερινή επαφή μας με παιδιά που αντιμετωπίζουν προβλήματα. Η Υπηρεσία μας δεν θα πει ποτέ «Δε μου δί-

νουν τα ίχνη». Θα σηκώσω το τηλέφωνο, θα πάρω τον Εισαγγελέα και ο Εισαγγελέας θα μου δώσει την εντολή. Και όποιος δεν υπακούσει στην εντολή του Εισαγγελέα θα βρεθεί ενώπιον των Αρχών. Δε χαριζόμαστε σε κανέναν. Αυτό πιστέψτε το. Και αυτοί που μας ακούνε θα πρέπει καλά να πιστέψουν ότι δεν παίζουμε με τα παιδιά. Με τα παιδιά δεν παίζει κανείς, το λέω και το εννοώ.

Η Δίωξη Ηλεκτρονικού Εγκλήματος και η Ελληνική Αστυνομία έχει ένα σύνθημα: **«Ναι στο χαμόγελο, ναι στο Διαδίκτυο, ναι στις νέες τεχνολογίες»**. Είναι για εμάς αδιανόητο να διαπραγματευόμαστε αν θα μας δώσουν ή όχι τα ηλεκτρονικά ίχνη για να σώσουμε ένα παιδί. Εμείς θα τα πάρουμε τα ίχνη! Κλείνοντας, θέλω να σας γνωρίσω ότι έχουμε φτάσει σε ακραίες περιπτώσεις, και έχουμε συλλάβει ακόμη και διαχειριστές, για να πάρουμε ένα ίχνος που αντιστοιχεί σε παιδί.

Σας ευχαριστώ πολύ!

Κυβερνοέγκλημα και νομοθεσία
«Κραυγές απόγνωσης»
Πρόληψη αυτοκτονιών

«Ασφάλεια στο διαδίκτυο – από το νόμο στην πραγματικότητα»

Ιωάννης Αγγελής
Εισαγγελέας Εφετών Αθηνών

ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ

Η ραγδαία εξέλιξη της τεχνολογίας στο χώρο του διαδικτύου έχει δημιουργήσει πλείστα όσα νομικά προβλήματα στο σύγχρονο νομικό και νομοθέτη ειδικότερα. Καλείται δε αυτός «να ρυθμίσει νομικώς την νέα κατάσταση», με την έννοια ότι πρέπει να άρει τις συγκρούσεις μεταξύ των εννόμων αγαθών που βλάπτονται στη νέα κοινωνία του διαδικτύου, όπως π.χ. τη σύγκρουση μεταξύ της ελεύθερης επικοινωνίας και της καταστολής της εγκληματικότητας στον συγκεκριμένο χώρο. Στο πλαίσιο δε αυτό σημαίνοντα ρόλο έχει η ασφαλής πλοήγηση και η δημιουργία κλίματος ασφαλείας στον πολίτη.

Η προσέγγιση των νομικών θεμάτων που αφορούν το διαδίκτυο ενέχει την δυσκολία ότι, προϋποθέτει όχι μόνο νομικές, αλλά μέχρι ένα βαθμό τουλάχιστον και τεχνικές γνώσεις σε θέματα ηλεκτρονικών υπολογιστών (computers) και διαδικτύου (internet) ειδικότερα . Οι τεχνικές όμως γνώσεις δεν επαρκούν για την κατανόηση της νομικής διάστασης του θέματος. Αυτό σε πρακτικό επίπεδο σημαίνει ότι, ο νομικός πρέπει να διαθέτει γενικές τεχνικές γνώσεις, ο δε τεχνικός πρέπει να κατέχει τουλάχιστον βασικές νομικές γνώσεις, προκειμένου ο καθένας απ΄ αυτούς (νομικοί και τεχνικοί) να αντιληφθεί τις εξελίξεις στον αντίστοιχο νομικοτεχνικό χώρο (on line κόσμος). Ο συνδυασμός των δύο βασικών, αλλά και διαφορετικών τρόπων σκέψεως αποτελεί "τον σταυρό του μαρτυρίου" για την κατανόηση του θέματος, δηλαδή του εγκλήματος στο διαδίκτυο και στη συγκεκριμένη περίπτωση του επιμέρους θέματος της ασφάλειας στο διαδίκτυο και της αντιμετώπισής της εγκληματικότητας που παρουσιάζεται από την παραβίαση των κανόνων της ασφαλούς πλοήγησης.

2. Γενικές παρατηρήσεις για την ασφάλεια στο διαδίκτυο.

Στην καθομιλουμένη γλώσσα ασφάλεια είναι η κατάσταση εκείνη, στην οποία δεν υπάρχει κίνδυνος, όπου αισθάνεται κάποιος ότι, δεν απειλείται. Είναι επίσης η αποτροπή κινδύνου ή απειλής, ή εξασφάλιση σιγουριάς και βεβαιότητας[1]. Στην καθημερινή πρακτική, ο καθένας δίνει στον όρο ασφάλεια, το περιεχόμενο εκείνο, που καθορίζουν οι συνθήκες ασκήσεως του επαγγέλματός του και η γενικότερη κοσμοθεωρία του. Έτσι π.χ. για τον στρατιωτικό η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο απ΄ ότι για τον εκπαιδευτικό (δάσκαλο ή καθηγητή), ο οποίος επίσης αντιλαμβάνεται την ίδια έννοια εντελώς διαφορετικά απ΄ ότι ο εργαζόμενος σε οικοδομικές εργασίες κλπ.

Αλλά και στον ίδιο ευρύτερο επαγγελματικό κλάδο η έννοια ασφάλεια έχει διαφορετικό περιεχόμενο, ανάλογα με την επιμέρους ενασχόληση του κάθε προσώπου. Έτσι π.χ. για τον στρατιωτικό που ασχολείται με τα όπλα η έννοια της ασφάλειας, δεν ταυτίζεται με αυτή που αντιλαμβάνεται ο ασχολούμενος με τους ηλεκτρονικούς υπολογιστές του ίδιου κλάδου. Ακόμα όμως και στον ίδιο στενότερο – επιμέρους κλάδο, η οπτική γωνία θεωρήσεως του όρου ασφάλεια είναι εντελώς διαφορετική. Έτσι, π.χ. διαφορετικά αντιλαμβάνεται τον όρο "ασφάλεια" ο τεχνικός ασφαλείας δικτύων υπολογιστικών συστημάτων και διαφορετικά ο τεχνικός ασφάλειας τραπεζικών πληροφοριακών συστημάτων.

Σε κάθε περίπτωση όμως όλοι, όσοι ασχολούνται με θέματα ασφαλείας "συναντώνται" στην κατάσταση εκείνη, όπου δεν υπάρχει κίνδυνος, όπου αισθάνονται ασφαλείς, όπου δεν απειλούνται, όπου πρέπει να αποτρέψουν τον κίνδυνο ή την απειλή και όπου πρέπει να εξασφαλίσουν την σιγουριά και την βεβαιότητα κατά την ενάσκηση του έργου των. Είναι ευνόητο βέβαια ότι, η ασφάλεια στο διαδίκτυο είναι ένα θέμα που αφορά όλους, δηλαδή τόσο τα μεμονωμένα άτομα, τις επιχειρήσεις, αλλά ακόμα και αυτές τις οργανωμένες πολιτείες[2].

Πρακτικό παράδειγμα για την διαφορετική αντίληψη της έννοιας της ασφάλειας στο διαδίκτυο αποτελεί αυτή καθ' εαυτή η σημερινή συνάντηση. Δηλαδή στην 1η ενότητα με θέμα «Ασφάλεια Ηλεκτρονικών Πληροφοριών – Βιομηχανική Κατασκοπεία» το ακροατήριο θα απαρτίζουν εκπρόσωποι επιχειρήσεων, επιχειρηματίες, διευθύνοντες σύμβουλοι. Στη 2η ενότητα με θέμα «Κυβερνοέγκλημα και νομοθεσία» – «Κραυγές απόγνωσης – πρόληψη αυτοκτονιών» το ακροατήριο θα απαρτίζουν Δικαστές, Εισαγγελείς, Καθηγητές συναφών Επιστημών, Δικηγόροι, Φοιτητές Νομικής και Δόκιμοι Αξιωματικοί των Παραγωγικών Σχολών των Ε.Δ. και Σωμάτων Ασφαλείας. Στη 3η ενότητα με θέμα «Cyber bullying» το ακροατήριο θα απαρτίζουν μαθητές από δημόσια και ιδιωτικά Σχολεία της Αττικής. Είναι ευνόητο ότι, σε περίπτωση που όλοι οι παραπάνω βρισκόταν στην ίδια αίθουσα, παρότι (όλοι) θα άκουγαν για το ίδιο θέμα (ασφαλής πλοήγηση στο διαδίκτυο), δεν θα υπήρχε ομοιόμορφη κατανόηση του θέματος, λόγω της διαφορετικής αντίληψης που έχει η κάθε ομάδα για την έννοια της ασφάλειας.

3. Η νομική έννοια της ασφάλειας στο διαδίκτυο

Για τον νομικό, κάθε έννοια έχει το περιεχόμενο εκείνο, που με ακρίβεια καθορίζει ο νόμος για το συγκεκριμένο θέμα. Το ίδιο συμβαίνει βέβαια και με την έννοια της ασφάλειας. Άρα για το νομικό ασφάλεια στο διαδίκτυο σημαίνει αυτό που ο νόμος ορίζει ως ασφάλεια στο διαδίκτυο. Ο νόμος επίσης καθορίζει και το περιεχόμενο όλων εκείνων των επιμέρους εννοιών που αναφέρο-

1. Βλέπ. Γ. Μπαμπινιώτη, "*Λεξικό της Νέας Ελληνικής Γλώσσας*", έκδ. 1998, σελ. 310.
2. Βλέπ. Παναγ. Αναστασιάδης "*Στον αιώνα της Πληροφορίας*", σελ. 222, εκδόσεις: Νέα Σύνορα – Λιβάνης, 2000.

νται στον βασικό ορισμό της ασφάλειας. Έτσι αν π.χ. ο νομοθέτης ορίσει ως ασφάλεια στο διαδίκτυο «τον κίνδυνο να επέλθει κάποια βλάβη», θα πρέπει να ορίσει ταυτόχρονα και τους όρους «κίνδυνο» και «βλάβη».

Για το συγκεκριμένο θέμα, της ασφάλειας του διαδικτύου, ή της ασφάλειας στο διαδίκτυο η Ελληνική νομοθεσία δεν έχει δώσει ακόμα ορισμό. Θα έλεγα, χωρίς επιφύλαξη ότι, ουδόλως έχει ασχοληθεί με το θέμα. Αυτό σημαίνει πρακτικώς ότι, ο ποινικός νομοθέτης δεν έχει (ακόμα) θεωρήσει την ασφάλεια στον κυβερνοχώρο ως έννομο αγαθό.[3]

Βέβαια, η έννοια της ασφάλειας δεν είναι άγνωστη στο ποινικό δίκαιο. ΄Έτσι, στο 14ο κεφάλαιο του ποινικού Κώδικα και στα άρθρα 290 επόμενα, ο ποινικός νομοθέτης με συγκεκριμένες διατάξεις προσδιορίζει τα εγκλήματα κατά της ασφάλειας των συγκοινωνιών και κατά των κοινωφελών εγκαταστάσεων. Επίσης στο άρθρο 388 Π.Κ. που ρυθμίζει την απάτη την σχετική με τις ασφάλειες, η έννοια της ασφάλειας λαμβάνεται από το ασφαλιστικό δίκαιο, ενώ στα άρθρα 69 επόμ. Π.Κ. που αναφέρονται στα μέτρα ασφαλείας, ως μέρος της επιβολής ή εκτέλεσης των ποινών, η έννοια της ασφάλειας λαμβάνεται από το δημόσιο δίκαιο (δημόσια ασφάλεια). Συμπερασματικώς μπορεί να λεχθεί ότι, η έννοια της ασφάλειας στο διαδίκτυο δεν έχει καθοριστεί ακόμα από το νομοθέτη. Κατά τον καθορισμό της όμως, πρέπει να ληφθούν υπόψη οι βασικές Αρχές του Δικαίου, όπως αυτές προσδιορίζονται στο Ελληνικό Σύνταγμα και στους ισχύοντες Διεθνείς Κανόνες.

4. Βασικές Αρχές του όρου «ασφάλεια» στο Διαδίκτυο

Στο διαδίκτυο "διακινούνται" πληροφορίες – δεδομένα (data) που έχουν σχέση με την προσωπική και ιδιωτική σφαίρα του ατόμου (χρήστη ή μη χρήστη του διαδικτύου). Κάθε άτομο έχει το δικαίωμα να απαιτήσει την μη διαρροή των στοιχείων αυτών σε τρίτα "αδιάκριτα βλέμματα". Κατά συνέπεια απαιτεί τα στοιχεία αυτά να κινούνται με ασφάλεια και μυστικότητα. Η ελεύθερη διακίνηση των ιδεών, ο σεβασμός της αξίας και η προστασία του ατόμου, η ελεύθερη ανάπτυξη της προσωπικότητας, το απόρρητο και το απαραβίαστο της επικοινωνίας, αποτελούν μερικές από τις βασικότερες Αρχές του δικαίου. Είναι ευνόητον ότι, οι θεμελιώδεις αυτές Αρχές πρέπει να εφαρμόζονται και στον κυβερνοχώρο. Ο υπερβολικός αστυνομικός έλεγχος (αστυνόμευση) του κυβερνοχώρου, δηλαδή η ευρεία διατύπωση του όρου ασφάλεια έρχεται ή ενδεχομένως να έρχεται σε αντίθεση με τις παραπάνω Αρχές. Δεν μπορούμε να ομιλούμε για κρατικό έλεγχο, καθότι η έννοια του κράτους και της κρατικής κυριαρχίας είναι έννοιες άγνωστες στο διαδίκτυο.

Η εφαρμογή όμως των Αρχών αυτών στο διαδίκτυο είναι ένα από τα πλέον δύσκολα και περίπλοκα θέματα, τόσο από τεχνικής, όσο και από νομικής απόψεως. Από τεχνική άποψη διότι, κάθε τεχνικός τρόπος που αποβλέπει στην ασφάλεια του διαδικτύου, μπορεί να εξουδετερωθεί και συνήθως εξουδετερώνεται) από ένα άλλο τρόπο "αντιασφάλειας". Από νομική άποψη διότι, ο νομοθέτης δεν "προφταίνει" να παρακολουθεί τις τεχνολογικές εξελίξεις και τις κοινωνικές επιπτώσεις και συνέπειες των, ώστε να μπορέσει να τις ρυθμίσει. Με άλλα λόγια οι αλλαγές στην τεχνική δομή του κυβερνοχώρου και κατά συνέπεια στη νομική αντιμετώπισή του, είναι τόσο ραγδαίες, που, εάν το θέμα δεν "σταθεροποιηθεί" κάπου από τεχνολογικής απόψεως, ο νομοθέτης δεν θα καταφέρει να λάβει οποιοδήποτε μέτρο, σε ουσιαστικό ή δικονομικό επίπεδο.

3. ως έννομο αγαθό είναι θεωρείται κάθε βιοτικό αγαθό το οποίο, το δίκαιο περιβάλλει με προστασία. Βλέπ. Ν. Χωραφάς "*Ποινικό Δίκαιο*", σελ. 5, εκδ. Σάκκουλας, 1978.

5. Η τεχνική διάσταση του όρου ασφάλεια στο διαδίκτυο.

Από τεχνική άποψη, ασφάλεια (security) είναι η προστασία ενός συστήματος υπολογιστών και των δεδομένων του από απώλεια ή ζημιά. Αυτή επιτυγχάνεται με την πρόληψη της πρόσβασης μη εξουσιοδοτημένων ατόμων στο σύστημα. Κλασσικό παράδειγμα ασφαλείας αποτελεί η συναλλαγή (αγοραπωλησία) που γίνεται στο διαδίκτυο με την χρήση πιστωτικής κάρτας. Σ΄ αυτήν την περίπτωση πρέπει να εξασφαλιστεί ότι, δεν είναι δυνατόν να "συλλάβει" (υποκλέψει) κάποιος τον αριθμό της πιστωτικής κάρτας ή να τον αντιγράψει από τον διακομιστή, που είναι αποθηκευμένος. Επίσης πρέπει να επαληθευτεί ότι, ο αριθμός της πιστωτικής κάρτας αποστέλλεται πράγματι, από το πρόσωπο, που ισχυρίζεται ότι τον στέλνει.

Η ασφάλεια δηλαδή των δεδομένων που διακινούνται στο διαδίκτυο πρέπει να ικανοποιεί την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των δεδομένων.

Εμπιστευτικότητα (confidentiality) των δεδομένων είναι η ιδιότητά τους να καθίστανται προσπελάσιμα μόνο από εξουσιοδοτημένους χρήστες του συστήματος.

Ακεραιότητα (integrity) των δεδομένων είναι η ιδιότητά των στοιχείων να είναι ακριβή και να αντιπροσωπεύουν την πραγματικότητα, κάθε δε αλλαγή των να είναι αποτέλεσμα εξουσιοδοτημένης ενέργειας.

Διαθεσιμότητα (availability) των πόρων ενός πληροφοριακού συστήματος είναι η ιδιότητά τους να καθίστανται άμεσα προσπελάσιμοι σε κάθε εξουσιοδοτημένο χρήστη του συστήματος.

Ως παράδειγμα στη νομική πρακτική μπορεί να αναφερθεί η ηλεκτρονική κατάθεση αγωγής:

Α) το περιεχόμενό της να είναι προσβάσιμο μόνον στους εξουσιοδοτημένους από το σύστημα χρήστες (δικαστές – δικηγόροι), – Εμπιστευτικότητα,

Β) να υφίσταται βεβαιότητα ότι, τα δεδομένα που «έφθασαν» στον παραλήπτη (π.χ. Πρωτοδικείο), είναι αυτά που «έφυγαν» από τον αποστολέα (π. χ. δικηγορικό γραφείο), – Ακεραιότητα

Γ) να εξασφαλίζεται ότι, τα δεδομένα – πόροι (ηλεκτρονικό περιεχόμενο αγωγής) είναι άμεσα προσπελάσιμα σε κάθε εξουσιοδοτημένο χρήστη (π.χ. δυνατότητα του δικαστή να επεξεργάζεται την δικογραφία από το σπίτι του (Διαθεσιμότητα).

6. Θέματα σχετικά με την ασφάλεια στο διαδίκτυο

Η ασφαλής πλοήγηση στο διαδίκτυο εξαρτάται από πλείστους όσους παράγοντες μεταξύ των οποίων ενδεικτικώς θα αναπτυχθούν παρακάτω η ύπαρξη αποτελεσματικής προς τούτο νομοθεσίας και η αστυνόμευση στο διαδίκτυο.

Α) η ύπαρξη αποτελεσματικής νομοθεσίας

Είναι γνωστό ότι για να "μπει" κάποιος στον κυβερνοχώρο (internet) απαραίτητη προϋπόθεση αποτελεί η χρήση του «χώρου των τηλεπικοινωνιών» (σταθερού ή κινητού τηλεφώνου). Η χρήση αυτή επιτυγχάνεται με την σύνδεση του χρήστη με μια εταιρεία παροχής υπηρεσιών διαδικτύου. Απαραίτητο βέβαια είναι να διαθέτει ο χρήστης τον κατάλληλο τεχνολογικό εξοπλισμό. Κατά συνέπεια οι σχετικοί με τις τηλεπικοινωνίες νόμοι έχουν άμεση ή έμμεση σχέση με την χρήση της τηλεπικοινωνιακής τεχνικής υποδομής. Βασικοί νόμοι («ελάχιστο ποσοστό γνώσεως») που πρέπει να γνωρίζει ένας νομικός προκειμένου να αντιληφθεί τα σχετικά με την ασφαλή πλοήγηση στο διαδίκτυο είναι:

- Ν. 2225/1994 για την προστασία της ελευθερίας και ανταπόκρισης και επικοινωνίας και άλλες διατάξεις,

- Ν. 2251/1994 (ειδικότερα το άρθρο 4) περί προστασίας καταναλωτών.
- Ν. 2532/1997 που αναφέρεται στην κύρωση της Σύμβασης των Ηνωμένων Εθνών για τις διεθνείς πωλήσεις κινητών πραγμάτων.
- Ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των τηλεπικοινωνιών, Οδηγία 97/7/ΕΚ Προστασία των καταναλωτών κατά τις εξ αποστάσεως συμβάσεις,
- Ν. 2672/1998 (ειδικότερα το άρθρο 14), που αφορά την διακίνηση εγγράφων με ηλεκτρονικά μέσα τηλεομοιοτυπία – ηλεκτρονικό ταχυδρομείο),
  Ο Ν.2774/22.12.99 για την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, σε συνδυασμό με το Ν.2472 /10.4.97 «προστασία ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα».
- Ν. 2867/2000, που αναφέρεται στην οργάνωση και λειτουργία των τηλεπικοινωνιών,
- Π. Δ. 342/2002 που αναφέρεται στην διακίνηση εγγράφων με ηλεκτρονικό ταχυδρομείο μεταξύ των δημοσίων υπηρεσιών, Ν.Π.Δ.Δ. και Ο.Τ.Α. ή μεταξύ αυτών και των φυσικών ή νομικών προσώπων ιδιωτικού δικαίου και ενώσεων φυσικών προσώπων.
- Ν. 3115/2003 για την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών,
- Π. Δ. 150/2001 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές,
- Π.Δ. 131/2003 που αφορά την προσαρμογή στην Οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. (Οδηγία για το ηλεκτρονικό εμπόριο).
- Π. Δ. 47/2005 που αφορά τις διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του.

Σ' όλα τα παραπάνω πρέπει να προστεθεί η (λογική) διαπίστωση ότι: Η τεχνολογία εξελίσσεται με τόσο γρήγορο ρυθμό, που είναι πολύ δύσκολο (σχεδόν αδύνατο), ακόμα και στον ειδικό να την παρακολουθήσει. Ταυτόχρονα, η ταχεία αυτή εξέλιξη της τεχνολογίας οδηγεί στη διαμόρφωση νέων κοινωνικών δεδομένων και καταστάσεων και κατά συνέπεια σε νέες μορφές αστικών συμπεριφορών, ποινικών αδικημάτων και εγκληματικότητας γενικότερα. Ειδικότερα δε οι νέες μορφές εγκληματικότητας είτε είναι δύσκολο να διαπιστωθούν αμέσως, είτε δεν μπορούν να διερευνηθούν ανακριτικώς, με την έννοια, ακόμα και εάν προσδιοριστεί ο τρόπος τελέσεως, δεν μπορεί να εντοπιστεί (ανακαλυφθεί) ο δράστης της πράξεως, ο οποίος τελικώς παραμένει άγνωστος. Και αυτό, όχι λόγω τεχνικών προβλημάτων, αλλά λόγω νομικών κωλυμάτων, που συνίστανται στην αδυναμία άρσης απορρήτου των επικοινωνιών ή λόγω δυσχερειών σε θέματα αστυνομικής και δικαστικής συνεργασίας, που απαιτείται κατά την διερεύνηση των εγκλημάτων στο διαδίκτυο.

Η ταχεία αυτή εξέλιξη της τεχνολογίας έχει ως συνέπεια την ψήφιση όλων και περισσότερων σχετικών με την τεχνολογία νόμων, τόσο σε ποινικό, όσο και αστικό, αλλά και σε διοικητικό επίπεδο. Κατά κανόνα η νέα αυτή νομοθεσία θεσπίζεται αρχικώς (υπό διάφορες νομικές μορφές) στα πλαίσια Διεθνών Οργανισμών (Ε.Ε. Συμβούλιο της Ευρώπης, ΟΗΕ κλπ) και στη συνέχεια ενσωματώνεται στην Ελληνική έννομη τάξη.

Είναι απαραίτητο πάντως να λεχθεί ότι: Η ίδια η τεχνολογία, ανεξάρτητα από τα προβλήματα (νομικά ή μη) που δημιουργεί αυτή καθ΄ εαυτή, δίνει στη συνέχεια λύση σ' αυτά (δηλαδή στα προβλήματα, που η ίδια δημιουργεί). Έτσι π.χ. η πρακτική εφαρμογή του "e-banking" έχει δημιουργήσει την διάπραξη πλείστων όσων οικονομικών ποινικών αδικημάτων (ενδεικτικώς αναφέ-

ρεται το "fishing"). Την σχετική γνώση όμως για την έννοια (νομική και μη) του "e-banking" και του "fishing" μας την δίνει η ίδια η τεχνολογία, «ψάχνοντας τον ίδιο τον τόπο του εγκλήματος» (δηλαδή το διαδίκτυο) με την χρήση μιας κατάλληλης μηχανής αναζήτησης. Όσον αφορά δε τους σχετικούς με το διαδίκτυο και την τεχνολογία (νέους) νόμους η πρόσβαση (και κατά συνέπεια γνώση) σ΄ αυτούς είναι δυνατή, είτε με την επίσκεψη σε μια από τις πολλές βάσεις νομικών δεδομένων, είτε με την αναγραφή του αριθμού του νόμου (ή του αντικειμένου που αφορά) σε μια κατάλληλη μηχανή αναζήτησης.

Ειδικότερα για τα θέματα αστυνομικής και δικαστικής συνεργασία στο διαδίκτυο πρέπει να λεχθεί ότι:

Οι δικαστικές-Αστυνομικές έρευνες που γίνονται προς διακρίβωση εγκλημάτων του κυβερνοχώρου, ουδεμία σχέση έχει με τις έρευνες , που μέχρι τώρα γνωρίζουμε . Στις μέχρι τώρα «παραδοσιακές» έρευνες ο ερευνών έψαχνε σε συγκεκριμένο χώρο π.χ. δωμάτια, συρτάρια κλπ. για να εντοπίσει το αναζητούμενο αντικείμενο. Σήμερα έχει να ψάξει files , note pads , botes, dada, κρυπτογραφημένα στοιχεία κλπ. Μπορεί το προς έρευνα αντικείμενο να βρίσκεται μπροστά στα μάτια του ερευνητή και να μην μπορεί να το εντοπίσει , εάν δεν έχει τις απαραίτητες τεχνικές γνώσεις . Ερωτάται λοιπόν, πως θα διεξαχθεί σε μια τέτοια περίπτωση η αστυνομική έρευνα; Ο «παραδοσιακός Εισαγγελέας » και η «παραδοσιακή αστυνομία» δεν επαρκούν πλέον για την εξιχνίαση των σχετικών εγκλημάτων. Ένα άλλο πρόβλημα είναι ότι στην κοινή έρευνα το αντικείμενο βρίσκεται σ΄ ένα σημείο . Αντίθετα στο έγκλημα του κυβερνοχώρου το αντικείμενο μπορεί να βρίσκεται σε πολλούς υπολογιστές οι οποίοι μάλιστα μπορεί να βρίσκονται σε διάφορες χώρες. Το πρόβλημα του τόπου τελέσεως είναι ένα από τα σημαντικότερα προβλήματα που αντιμετωπίζεται κατά την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο, δεδομένου ότι, η ίδια αξιόποινη πράξη μπορεί να διαπράττεται ταυτόχρονα σε εκατοντάδες ή και χιλιάδες τόπους τελέσεως. Γενικώς ο αριθμός των τόπων τελέσεως εξαρτάται από την συγκεκριμένη λειτουργία του διαδικτύου (αποστολή e-mails, new groups, internet relay chat, κλπ). Ακόμα και σε δορυφόρους (Satellite-technology) είναι δυνατό να βρίσκονται τα αποδεικτικά στοιχεία , δεδομένου ότι , οι επικοινωνίες (κινητά τηλέφωνα κλπ.) γίνονται πλέον δορυφορικώς. Σε κάθε περίπτωση όμως δημιουργείται πρόβλημα όχι μόνο σε θέματα Δικαστικής και Αστυνομικής συνεργασίας, αλλά και σε θέματα κατά τόπον αρμοδιότητος ως προς την εκδίκαση της πράξεως. Η έννοια επίσης των γεωγραφικών συνόρων είναι άγνωστη στα εγκλήματα του κυβερνοχώρου. Ειδικότερα, όταν οι υπολογιστές (computers) είναι συνδεδεμένοι μεταξύ των ολόκληρος ο πλανήτης αποτελεί « μία χώρα». Κατά συνέπεια οι «κλασσικές» Διεθνείς Συμβάσεις περί αμοιβαίας Δικαστικής Συνδρομής και Συνεργασίας, είναι «παραχωρημένες» στο πεδίο του εγκλήματος στον κυβερνοχώρο. Η Δικαστική συνεργασία στα συγκεκριμένα θέματα του κυβερνοχώρου, για να είναι αποτελεσματική, πρέπει να είναι ταχύτατη. Είναι δε ευνόητον ότι, χωρίς την ύπαρξη σχετικής ειδικής νομοθετικής πρόβλεψης δεν μπορεί να νοηθεί αστυνομική ή δικαστική συνεργασία.

Β) η αστυνόμευση του διαδικτύου.

Το θέμα της αστυνόμευσης του διαδικτύου αποτελεί μέρος των ευρύτερων ερωτημάτων: μπορεί να ελεγχθεί το διαδίκτυο και εάν ναι ποιος το ελέγχει; (από άποψη περιεχομένου -από άποψη θεσπίσεως νομοθεσίας – από άποψη εφαρμογής της νομοθεσίας). Είναι ευνόητον ότι, κάθε οργανωμένο κράτος έχει εξειδικευμένη υπηρεσία για την αστυνόμευση του διαδικτύου.

Στην Ελλάδα η αστυνόμευση του διαδικτύου γίνεται από την υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος, που διέπεται από ειδικό θεσμικό πλαίσιο και έχει στελεχωθεί από εξειδικευμένο προσωπικό (Βλέπ. σχετικό site της Ελληνικής αστυνομίας). Σημειωτέον δε ότι, το θέμα της αστυνόμευσης το διαδικτύου δεν πρέπει να συγχέεται με το θέμα του νομικού ελέγχου αυτού που γίνεται στον Ελληνικό χώρο από τις ανεξάρτητες αρχές, δηλαδή την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)

7. Συμπεράσματα – προτάσεις

Η έννοια της ασφάλειας, όπως αναπτύχτηκε παραπάνω είναι έννοια σχετική. Συμπερασματικώς μπορεί να λεχθεί ότι, απόλυτη ασφάλεια στο Διαδίκτυο δεν υπάρχει. Ασφαλής υπολογιστής είναι μόνο ο κλειστός υπολογιστής. Κάθε υπολογιστής που συνδέεται με το διαδίκτυο αποτελεί «εν δυνάμει» θύμα επιθέσεως (σε hackers, crackers κλπ). Με αυτή την έννοια στο διαδίκτυο δεν υπάρχει «ιδιωτικός χώρος». Αν ληφθεί μάλιστα υπόψη ότι, «στο διαδίκτυο δεν μπορεί να χρησιμοποιηθεί μπλάνκο και ότι γράφει δεν ξεγράφει», είναι βέβαιον ότι, πρακτικώς δεν υπάρχει ιδιωτικότητα. Η ύπαρξης κωδικών πρόσβασης ελάχιστα μπορούν να βοηθήσουν. Αυτό που βοηθάει για την ασφάλειας είναι η ύπαρξη γνώσεων στο χρήστη.

Δεν υπάρχουν τεχνικώς αξεπέραστες δυσκολίες κατά τον έλεγχο του διαδικτύου. Υπάρχουν μόνο νομικοί περιορισμοί. Επομένως απαιτείται να τεθούν κοινοί (νομικοί) κανόνες παγκόσμιας ισχύος (όπως π.χ. έχουν τεθεί για τα ναρκωτικά, την διαφθορά, το διεθνιστικό οργανωμένο έγκλημα κλπ). Δεν επαρκεί η αυτορρύθμιση. Απαιτείται έλεγχος και αστυνόμευση του διαδικτύου, κατ΄ αναλογία του off line χώρου.

Απαιτείται Δικαστική και Αστυνομική (διεθνής) συνεργασία. Απαιτείται εκπαίδευση και εξειδίκευση των ασχολουμένων με τον έλεγχο του διαδικτύου Αρχών (Δικαστικών – Αστυνομικών).

Προς επίλυση όλων των παραπάνω αναγκαία καθίσταται η ψήφιση Διεθνούς Συμβάσεως στα πλαίσια του ΟΗΕ για τον έλεγχο και την ασφάλεια του διαδικτύου, η οποία να δεσμεύει νομικώς ολόκληρο το «παγκόσμιο χωριό» (δηλαδή ολόκληρη την διεθνή κοινότητα).

Προαναγγελίες αυτοκτονιών στο Διαδίκτυο[1]
Διαστάσεις του φαινομένου και νομική προσέγγιση

Δημήτριος Κιούπης
Επίκουρος Καθηγητής Ποινικού Δικαίου και Ποινικής Δικονομίας
Νομικής Σχολής Πανεπιστημίου Αθηνών

1. Εισαγωγή – Η σημασία του Διαδικτύου στην σύγχρονη κοινωνία

Το Γερμανικό Ακυρωτικό Δικαστήριο με πρόσφατη απόφαση του[2] είχε την ευκαιρία να τονίσει τον κεντρικό ρόλο που διαδραματίζει το Διαδίκτυο στην σύγχρονη κοινωνία.

Τα πραγματικά περιστατικά της υπόθεσης ήταν, συνοπτικά, τα ακόλουθα:

Λόγω σφάλματος του τηλεπικοινωνιακού παρόχου διακόπηκε η σύνδεση του ενάγοντος, μέσω της οποίας αυτός πραγματοποιούσε τηλεφωνικές κλήσεις, έστελνε και λάμβανε φαξ και είχε πρόσβαση στο Διαδίκτυο.

Ο ενάγων ζήτησε, πέρα από την αποκατάσταση της υλικής ζημίας που υπέστη, επιπλέον αυτοτελή αποζημίωση για τον αποκλεισμό της "χρήσης ενός σημαντικού οικονομικού αγαθού", όπως προβλέπεται κατά το γερμανικό δίκαιο.

Το αίτημά του αυτό απορρίφθηκε αναφορικά με την υπηρεσία αποστολής και λήψης φαξ, διότι το δικαστήριο έκρινε ότι αυτή η χρήση δεν είναι τόσο σημαντική, ενόψει της δυνατότητας αποστολής του περιεχομένου ενός φαξ με ηλεκτρονικό τρόπο.

Επίσης, το αίτημα πρόσθετης αποζημίωσης απορρίφθηκε και σχετικά με την χρήση του τηλεφώνου, που θεωρήθηκε μεν σημαντική, αλλά κρίθηκε ότι καλύφθηκε με την αποζημίωση της δαπάνης που κατέβαλε ο ενάγων για την χρήση κινητής τηλεφωνίας, ως υποκατάστατου της σταθερής τηλεφωνικής επικοινωνίας.

Αντιθέτως, το αίτημα έγινε δεκτό για την διακοπή της πρόσβασης στο Διαδίκτυο.

Συγκεκριμένα το Δικαστήριο δέχθηκε τα εξής:

Η δυνατότητα χρήσης του Διαδικτύου είναι οικονομικό αγαθό καθοριστικής σημασίας για την αυτοτελή οικονομική δραστηριότητα και του ιδιώτη. Το Διαδίκτυο παρέχει σε παγκόσμια κλίμακα εκτεταμένες πληροφορίες με την μορφή δεδομένων κειμένου, ήχου, εικόνας και βίντεο. Έτσι καλύπτονται σχεδόν όλες οι θεματικές περιοχές ανθρώπινου ενδιαφέροντος και ικανοποιούνται απαιτήσεις διαφορετικής ποιότητας και αξίας. Μπορεί κανείς να βρει δεδομένα ελαφρού ψυχαγωγικού περιεχομένου, πληροφορίες για θέματα της καθημερινότητας μέχρι πολύπλοκα επιστημονικά θέματα. Με τον τρόπο αυτό το Διαδίκτυο, χάρις στην εύκολη πρόσβαση σε πληροφορίες αντικαθιστά άλλα μέσα, όπως π.χ. λεξικά, περιοδικά ή την τηλεόραση και επιπλέον διευκολύνει την επικοινωνία των χρηστών (π.χ. ηλεκτρονικό ταχυδρομείο, ιστολόγια, σελίδες κοινωνικής δικτύωσης, χώροι

1. Κείμενο της εισήγησης με προσθήκη ορισμένων ενημερωτικών υποσημειώσεων.
2. Απόφαση III ZR 98/12 της 24/1/2013

συζητήσεων). Επιπλέον, χρησιμοποιείται όλο και περισσότερο για την σύναψη συμβάσεων, την κατάρτιση δικαιοπραξιών, αλλά και την εκπλήρωση υποχρεώσεων δημοσίου δικαίου. Λόγω της εκτεταμένης χρήσης του έχει αναδειχθεί σε βασικό μέσο διαμόρφωσης της ζωής των περισσοτέρων.[3]

Έτσι, αποτυπώνεται χαρακτηριστικά η κεντρική σημασία της χρήσης του Διαδικτύου όχι απλώς σε θεωρητικό επίπεδο, αλλά και σε απόφαση ανωτάτου Δικαστηρίου.

Από την άλλη πλευρά, η μεταφορά ενός μεγάλου τμήματος της κοινωνικής δραστηριότητας στο ψηφιακό περιβάλλον έχει μεταφέρει και ένα αντίστοιχης έκτασης τμήμα εγκληματικότητας στο Διαδίκτυο.

Κυριότερες μορφές αυτού του διαδικτυακού εγκλήματος είναι η αθέμιτη παρέμβαση σε δεδομένα (hacking), απάτες και απάτες με υπολογιστή, παραβάσεις της νομοθεσίας περί πνευματικής ιδιοκτησίας και προσωπικών δεδομένων, αλλοίωση δεδομένων μέσω ιών, επιθέσεις σε συστήματα πληροφοριών, πλαστογραφίες, παιδική πορνογραφία κ.λπ.

Κεντρικό χαρακτηριστικό του διαδικτυακού εγκλήματος είναι ο διασυνοριακός του χαρακτήρας, καθώς από την φύση και την λειτουργία του το Διαδίκτυο αποτελεί ένα παγκόσμιο ψηφιακό περιβάλλον που υπερβαίνει τα κρατικά σύνορα του φυσικού κόσμου.

Μέσα σε αυτό το πλαίσιο, ιδιαίτερη θέση έχει το ζήτημα των προαναγγελιών αυτοκτονιών στο Διαδίκτυο, των αυτοκτονιών που μεταδίδονται μέσω Διαδικτύου, αλλά και το γενικότερο ζήτημα της επικοινωνίας των χρηστών και ανταλλαγής δεδομένων σχετικά με την τέλεση αυτοκτονιών.

2. Η αυτοκτονία

Το ζήτημα της αυτοκτονίας, ως το κατ' εξοχήν κρίσιμο και οριακό ζήτημα της ανθρώπινης ύπαρξης, έχει απασχολήσει άλλωστε τόσο την λογοτεχνία[4] όσο και την φιλοσοφία.[5]

Σύμφωνα με το δίκαιό μας, η απόπειρα αυτοκτονίας[6] δεν αποτελεί αξιόποινη πράξη.

Η νομοθετική επιλογή θεμελιώνεται με δύο διαφορετικά επιχειρήματα: Κατά την πρώτη άποψη, πρόκειται για επιλογή σκοπιμότητας, αφού τυχόν επιβολή ποινής δεν έχει κάποια προληπτική λειτουργία στον δράστη, αφού αυτός που επιχειρεί να θέσει τέρμα στην ίδια την ζωή του δεν μπορεί να αποτραπεί με την απειλή μιας χρηματικής ποινής η μιας στερητικής ποινής της ελευθερίας του, ενώ οδηγεί και στο παράδοξο να τιμωρείται κάποιος, επειδή απέτυχε να ολοκληρώσει την πράξη του, ενώ φυσικά θα ήταν ατιμώρητος αν είχε ολοκληρώσει την αυτοκτονία.

Κατά την δεύτερη άποψη, ο λόγος του μη αξιοποίνου της απόπειρας δεν είναι η σκοπιμότητα μιας τέτοιας διάταξης, αλλά η αναγνώριση από το νομοθέτη της αρχής ότι δεν μπορεί να παρέμβει στην διάθεση των εννόμων αγαθών του ατόμου από το ίδιο.[7]

Ωστόσο, ο νομοθέτης προβλέπει ποινική ευθύνη για τρίτους που εμπλέκονται στην αυτοκτονία μέσω της διάταξης του άρθρου 301 Π.Κ. (συμμετοχή σε αυτοκτονία)[8].

3. Το σχετικό, αναλυτικό σκεπτικό της απόφασης στον αριθμ. 17 του κειμένου της απόφασης του Δικαστηρίου, όπως δημοσιεύθηκε στον δικτυακό τόπο του Δικαστηρίου www.bundesgerichtshod.de

4. Χαρακτηριστική είναι η περίπτωση του έργου του Γκαίτε « Τα πάθη του νεαρού Βέρθερου», που θεωρήθηκε υπεύθυνο για κύμα αυτοκτονιών που ακολούθησαν την δημοσίευσή του.

5. Βλ. ενδεικτικά τις μελέτες των Albert Camus, An absurd reasoning και David Hume, On suicide.

6. Για αξιόποινο της αυτοκτονίας δεν μπορεί καν να γίνει λόγος, αφού, στην περίπτωση ολοκληρωμένης αυτοκτονίας, ο θάνατος του αυτόχειρα καθιστά την συζήτηση περί ενδεχόμενης ποινικής ευθύνης του είναι άνευ αντικειμένου.

7. Αναλυτικά για το θέμα αυτό βλ. την παρουσίαση των διάφορων απόψεων σε Δ. Κιούπη, Συμμετοχή σε αυτοκτονία, Ερμηνεία μιας αμφιλεγόμενης διάταξης, ΠοινΧρον 1995, σελ 549 επ.

8. Αξίζει να σημειωθεί ότι κατά το γερμανικό δίκαιο, που είναι συγγενές προς το ελληνικό, η συμμετοχή σε αυτοκτονία δεν τιμωρείται. Επίσης, στην αγγλική έννομη τάξη που τιμωρεί την συμμετοχή σε αυτοκτονία και μάλιστα αυστηρά, συνήθως οι εισαγγελικές αρχές δεν προχωρούν σε άσκηση ποινικής δίωξης.

«Όποιος με πρόθεση κατέπεισε άλλον να αυτοκτονήσει, αν τελέστηκε η αυτοκτονία ή έγινε απόπειρά της, καθώς και όποιος έδωσε βοήθεια κατ' αυτήν, τιμωρείται με φυλάκιση.»

3. Ερμηνευτική προσέγγιση του άρθρου 301Π.Κ.

Η διάταξη του άρθρου 301 προβλέπει δύο μορφές παρέμβασης τρίτου προσώπου στην αυτοκτονία: την κατάπειση και την βοήθεια κατά την αυτοκτονία ή την απόπειρά της. Η χρήση διαφορετικής ορολογίας από την αντίστοιχη της συμμετοχής (άρθρα 45 επ.) δείχνει την ποιοτική διαφορά της παρέμβασης των τρίτων στην αυτοκτονία, αλλά και την πρόθεση του νομοθέτη να ποινικοποιήσει μόνο ορισμένες μορφές παρέμβασης.

Ως κατάπειση νοείται η δημιουργία σε άλλον της απόφασης να αυτοκτονήσει. Χαρακτηριστικό της είναι δηλαδή ότι έναυσμα και αφετηρία της απόφασης είναι η ενέργεια του τρίτου. Αντίθετα, δεν υπάγεται στην έννοια της καταπείσεως η ισχυροποίηση ή ενθάρρυνση μιας ήδη ειλημμένης απόφασης του αυτόχειρα. Αυτό προκύπτει τόσο από το γλωσσικό περιεχόμενο της λέξης καταπείθω, όσο και από το σκοπό του νομοθέτη που θέλει με την χάραξη των ορίων της τιμωρητής παρέμβασης να ρυθμίσει τις περιπτώσεις εξωτερικής δράσης που έχουν αυτοδύναμο παρεμβατικό χαρακτήρα. Κατά την ορθότερη άποψη, απαιτείται γλωσσική επικοινωνία μέσω της οποίας ο τρίτος δημιουργεί στον αυτόχειρα την διάθεση να αυτοκτονήσει. Ακόμη η κατάπειση απευθύνεται σε ορισμένο πρόσωπο με το οποίο να βρίσκεται σε επικοινωνία ο δράστης.

Αντίθετα, δεν εμπίπτουν στην έννοια της καταπείσεως οι απαισιόδοξες ή μελαγχολικές αφηγήσεις που δημιουργούν το κατάλληλο υπέδαφος για την αυτοκτονία, ούτε βέβαια η οσοδήποτε μελοδραματική παρουσίαση των αδιεξόδων της ζωής.

Δεύτερη μορφή παρέμβασης των τρίτων θεωρεί ο νομοθέτης την βοήθεια που παρέχουν κατά την αυτοκτονία ή την απόπειρά της. Αποφασιστικό είναι εδώ το στοιχείο της χρονικής σύμπτωσης της βοήθειας και της πράξεως. Δεν τιμωρείται λοιπόν η βοήθεια που μπορεί να παρέχει κάποιος πριν από την πράξη και η οποία μπορεί να συνίσταται στην παροχή και προμήθεια των κατάλληλων μέσων, στην υπόδειξη μεθόδου, στην τεχνική υποστήριξη ή στην απλή παροχή συμβουλών.

Αναφορικά με την τιμωρητή βοήθεια κατά την πράξη θα πρέπει να σημειωθεί ότι αυτή μπορεί να είναι μόνο θετική ενέργεια, αφού η απλή, απαθής και αμέτοχη παρουσία του τρίτου κατά την αυτοκτονία δεν ενέχει οποιασδήποτε μορφής παρεμβατικό στοιχείο. (εκτός αν τίθεται θέμα ψυχικής συνέργειας).

4. Εξαιρετικές περιπτώσεις: ανθρωποκτονία με πρόθεση κατ' έμμεση αυτουργία

Διαφορετική είναι η μεταχείριση των περιπτώσεων εκείνων όπου ο αυτός που αυτοκτονεί ή αποπειράται να αυτοκτονήσει είναι α) ανήλικος, β) άτομο ανίκανο για καταλογισμό ή ευρισκόμενο σε κατάσταση που επηρεάζει ουσιαστικά την ικανότητα σκέψης γ) άτομο που εξωθείται από τρίτον στην αυτοκτονία με άσκηση βίας, έντονης ψυχολογικής πίεσης, πλύσης εγκεφάλου, ιεραρχικού «ελέγχου» ως μέλος θρησκευτικής, ή πολιτικής ομάδας κ.λπ.

Κοινό χαρακτηριστικό των πιο πάνω περιπτώσεων είναι ότι η αυτοκτονία δεν προέρχεται από μια ώριμη απόφαση ενός αυτόνομου προσώπου, αλλά είναι το αποτέλεσμα της εξωτερικής πίεσης ενός τρίτου που χρησιμοποιεί τον αυτόχειρα ως όργανο κατά του ίδιου του εαυτού του. Έτσι, εδώ πρόκειται για ανθρωποκτονία με πρόθεση που τελείται κατ' έμμεση αυτουργία και όργανο τον ίδιο τον αυτόχειρα.

5. Το ειδικότερο ζήτημα: Αυτοκτονία στο διαδίκτυο

Σύμφωνα με σχετικό δελτίο τύπου της Ελληνικής Αστυνομίας[9] κατά τα έτη 2006-2012 474 άτομα εκδήλωσαν μέσω Διαδικτύου την πρόθεσή τους να αυτοκτονήσουν και εντοπίστηκαν από στελέχη της Δίωξης Ηλεκτρονικού Εγκλήματος.

Οι σχετικές συμπεριφορές εμφανίζονται συνήθως με τις ακόλουθες μορφές:

Α) Προαναγγελία αυτοκτονίας με αποστολή **e-mail, δημοσίευση σε ιστοσελίδα σελίδα σε δί-**κτυο κοινωνικής δικτύωσης, ανάρτηση σε ιστολόγιο κ.λπ

Β) Τέλεση της αυτοκτονίας και μετάδοση σε ζωντανή σύνδεση μέσω web κάμερας ή με άλλες τεχνικές μετάδοσης βίντεο.

Γ) Αναζήτηση δεδομένων που περιέχουν οδηγίες για μεθόδους τέλεσης αυτοκτονίας

Δ) Συμμετοχή σε σχετικές συζητήσεις

Οι παραπάνω μορφές συμπεριφοράς μπορούν να έχουν τα ακόλουθα ποιοτικά χαρακτηριστικά:

1. Σοβαρή εκδήλωση της βούλησης του ατόμου, όταν αυτό π,χ αναγγέλλει και αμέσως μετά τελεί την πράξη.

2. Έκκληση για βοήθεια ή έκφραση εκδήλωσης προσωπικού και κοινωνικού αδιεξόδου. Τέτοιες είναι οι περιπτώσεις που το άτομο δεν έχει επιχειρήσει να αυτοκτονήσει, ούτε καν έχει σχεδιάσει τον τρόπο τέλεσης, αλλά εκδηλώνει μια γενική και αόριστη επιθυμία, της οποίας η πραγμάτωση εντοπίζεται στο εγγύς ή και στο απώτερο μέλλον.

3. Αστεϊσμοί και υπερβολές , απλή εκδήλωση απογοήτευσης στο πλαίσιο γενικών συζητήσεων στο Διαδίκτυο , καθώς αρκετοί χρήστες νεότερης ιδίως ηλικίας χρησιμοποιούν το διαδίκτυο ως ένα τεχνητό κοινωνικό περιβάλλον χωρίς άμεση σύνδεση με την πραγματική κοινωνική ζωή.

Αν και, όπως τονίσθηκε ήδη, η αυτοκτονία δεν τιμωρείται, δεν είναι κοινωνικά αποδεκτή.[10] Αυτή η αμφισημία μεταξύ νομικού δικαιώματος και έλλειψης κοινωνικής αποδοχής ανοίγει το πεδίο για την ύπαρξη στο διαδίκτυο ομάδων **(groups) που υποστηρίζουν όσους θέλουν να αυτοκτο-**νήσουν , ενώ παράλληλα, υπάρχουν πολλοί ιστότοποι ψυχολογικής υποστήριξης και παροχής συμβουλών που σκοπεύουν να αποτρέψουν από την αυτοκτονία.

6. Ο εντοπισμός των ψηφιακών ιχνών σε περίπτωση προαναγγελίας αυτοκτονίας. Η έγκαιρη αποτροπή της αυτοκτονίας.

Στην περίπτωση της διαδικτυακής προαναγγελίας αυτοκτονίας, το επόμενο πρακτικό ζήτημα που ανακύπτει είναι, εφόσον εντοπισθεί έγκαιρα η διαδικτυακή προαναγγελία, ποια διαδικασία μπορεί να ακολουθηθεί κατά το δίκαιό μας, ώστε να ταυτοποιηθούν τα δεδομένα με συγκεκριμένο χρήστη του διαδικτύου και να υπάρξει έγκαιρη αποτροπή της αυτοκτονίας.[11]

Στις εξαιρετικές περιπτώσεις απόπειρας ανθρωποκτονίας κατ' έμμεση αυτουργία (κακούργημα), η άρση του απορρήτου της επικοινωνίας καλύπτεται οπωσδήποτε από τις διατάξεις του Ν. 2225/1994.

---

9. Ημερομηνία δημοσίευσης 3/7/2012

10. Χαρακτηριστικό είναι και ότι και σε νομικό επίπεδο σύμφωνα με το άρθρο 12 Ν. 3418/2005 (Κώδικας Ιατρικής Δεοντολογίας) σε περίπτωση απόπειρας αυτοκτονίας ο ιατρός μπορεί να προχωρήσει κατ' εξαίρεση στην εκτέλεση ιατρικής πράξης και χωρίς την συναίνεση του ασθενούς.

11. Για λόγους συντομίας δεν θα αναφερθούμε εδώ στο κεντρικό και εξαιρετικά αμφιλεγόμενο ζήτημα των ορίων επέμβασης σε σχέση με μια ώριμη απόφαση ενός ενήλικου και υγιούς ατόμου, αλλά θα επικεντρωθούμε στις περιπτώσεις εκείνες, όπου η αποτροπή της αυτοκτονίας γίνεται καθολικά αποδεκτή (ανήλικοι, ακαταλόγιστοι, ψυχικά ασθενείς, άτομα σε καθεστώς βίας και πίεσης)

Οι ίδιες διατάξεις δεν μπορούν να εφαρμοσθούν στην περίπτωση του πλημμελήματος της συμμετοχής σε αυτοκτονία (άρθρο 301 Π.Κ.), στις περιπτώσεις δηλ. που τρίτος καταπείθει ή δίνει βοήθεια στην αυτοκτονία.[12]

Στο συμπέρασμα αυτό, ότι δηλ. τα λεγόμενα εξωτερικά ή συνδετικά στοιχεία της επικοινωνίας καλύπτονται από το απόρρητο του άρθρου 19 του Συντάγματος και υπάγονται στην σχετική νομοθεσία περί άρσης απορρήτου οδηγούν οι σχετικές διατάξεις του άρθρου 4 παρ.1 Ν. 3471/2006 (προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών) και του άρθρου 4 Ν. 3917/2011 (διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών) που ενσωματώνουν μάλιστα αντίστοιχες οδηγίες της ΕΕ.

Αντιθέτως, αλλεπάλληλες γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου (ΓνωμΕισΑΠ 9/2009 ΠοινΔικ 2009, 923 επ., ΓνωμΕισΑΠ 12/2009, ΠοινΔικ 2009, 1089 επ. και ΓνωμΕισΑΠ 9/2011, ΠοινΧρον 2011, 714) καταλήγουν στο συμπέρασμα ότι το απόρρητο της επικοινωνίας δεν καλύπτει και τα εξωτερικά-συνδετικά δεδομένα κίνησης σε επιμέρους *περιπτώσεις αξιόποινης συμπεριφοράς*.[13]

Το περίπλοκο αυτό ζήτημα ενόψει και της αυστηρής διατύπωσης του άρθρου 19 του Συντάγματος αποτελεί αντικείμενο άλλων εισηγήσεων της ημερίδας και έτσι δεν θα αναλυθεί εδώ. Πάντως, ακόμη και υπό την εκδοχή ότι στις περιπτώσεις του πλημελήμματος της συμμετοχής σε αυτοκτονία είναι επιτρεπτή η ταυτοποίηση των εξωτερικών δεδομένων των χρηστών (ταυτότητα, κίνηση και θέση) το πρόβλημα παραμένει για τις περιπτώσεις, όπου δεν μπορεί να γίνει λόγος για οποιαδήποτε αξιόποινη συμπεριφορά λόγω μη εμπλοκής στην πράξη κάποιου τρίτου προσώπου εκτός του ατόμου που προαναγγέλλει ότι θα αυτοκτονήσει.

Πράγματι, η άμεση παρέμβαση για αποτροπή του ατόμου που εκδηλώνει πρόθεση να αυτοκτονήσει έχει πρωτίστως τον χαρακτήρα έγκαιρης παροχής ψυχολογικής και κοινωνικής στήριξης σε ευάλωτα άτομα (ανήλικους, ψυχικά πάσχοντες, άτομα που αντιμετωπίζουν καταστάσεις αδιεξόδου) και σπανιότατα την μορφή αστυνομικής επέμβασης για την αποτροπή ή την διακρίβωση εγκλήματος.

Αυτό σημαίνει ότι ο εντοπισμός των ψηφιακών ιχνών του υποψήφιου αυτόχειρα θα πρέπει να αποσυνδεθεί από τις σπάνιες και εντελώς διαφορετικές περιπτώσεις της ανθρωποκτονίας κατ' έμμεση αυτουργία ή της συμμετοχής σε αυτοκτονία και να εντοπισθεί στην αληθινή κοινωνική του διάσταση.[14]

Στην κατεύθυνση αυτή κινείται και πρόσφατο σχέδιο νόμου της γερμανικής κυβέρνησης,[15] που μετά από σχετική απόφαση του γερμανικού συνταγματικού δικαστηρίου προχωρεί σε τροποποιήσεις του νόμου περί τηλεπικοινωνιών αλλά και άλλων διατάξεων. Στο πλαίσιο αυτό επέρχονται και τροποποιήσεις του νόμου για την ομοσπονδιακή υπηρεσία αντιμετώπισης του εγκλήματος και την

12. Αξίζει πάντως να σημειωθεί ότι η ανίχνευση οποιασδήποτε ποινικής ευθύνης στο πλαίσιο του άρθρου 301 Π.Κ. προϋποθέτει τέλεση τουλάχιστον απόπειρας αυτοκτονίας, άλλως δεν υπάρχει καν αξιόποινη πράξη

13. Οι ανωτέρω γνωμοδοτήσεις αντιμετωπίζουν διαφορετικές περιπτώσεις (κακόβουλες κλήσεις, εξυβριστικά-δυσφημιστικά μηνύματα κ.λπ) και προβαίνουν, μεταξύ άλλων, σε ερμηνεία της έννοιας του απορρήτου ενόψει του άρθρου 19 Σ, αλλά και της κείμενης νομοθεσίας περί τηλεπικοινωνιών σε σχέση με την έννοια της «αρχής».

14. Στην πράξη, οι ποινικές διώξεις για ανθρωποκτονία κατ' έμμεση αυτουργία λειτουργούν απλώς ως νομική βάση για την άρση του επικοινωνιακού απορρήτου και εντοπισμό του υποψήφιου αυτόχειρα και ουδέποτε οδηγούν σε εντοπισμό ή σύλληψη του (ανύπαρκτου) δράστη της απόπειρας ανθρωποκτονίας κατ' έμμεση αυτουργία ή, έστω, συμμετοχής σε αυτοκτονία.

15. Βλ. σχετικά http://dip21.bundestag.de/dip21/btd/17/120/1712034.pdf

ομοσπονδιακή αστυνομία, ώστε οι υπηρεσίες αυτές να μπορούν να αποκτούν πρόσβαση σε συνδετικά δεδομένα σε περιπτώσεις αντιμετώπισης κινδύνων, όπως η προαναγγελία αυτοκτονίας.

Μια αντίστοιχη λύση στην ελληνικά νομοθεσία, που θα επέλυε τα προβλήματα που ήδη επισημάνθηκαν, θα αποτελούσε νομοθετική παρέμβαση στην κατεύθυνση ειδικής ρύθμισης άρσης του απορρήτου σε περιπτώσεις αναγγελίας αυτοκτονίας αλλά και σαφέστερης ρύθμισης-οριοθέτησης των όρων και των διαδικασιών άρσης του απορρήτου των δεδομένων περιεχομένου και των εξωτερικών-συνδετικών δεδομένων.

«Η πρόληψη της αυτοκτονίας ανηλίκου και ένα νομικό παράδοξο»

Δημήτριος Ι. Γκύζης
Εισαγγελέας Πρωτοδικών

Ευχαριστίες...

Όπως θα έχετε ήδη παρατηρήσει, βλέποντας το πρόγραμμα των σημερινών εισηγήσεων, σε αυτή αλλά και στην επόμενη ενότητα αναπτύσσονται, από σοφότερους εμού, νομικούς, συναδέλφους και θεωρητικούς του Δικαίου, θέματα ασφάλειας των επικοινωνιών μέσω του Διαδικτύου, θέματα που αφορούν στην άρση του απορρήτου και ειδικά τις αντικρουόμενες απόψεις για τα λεγόμενα εξωτερικά στοιχεία της επικοινωνίας. Από την πλευρά μου θα ήθελα να προσπαθήσω να σας περιγράψω, στα λίγα λεπτά που έχω στη διάθεσή μου και μέσα από μια πραγματική υπόθεση, που χειρίσθηκα, πως και από ποιους αντιμετωπίζεται σήμερα μια προαναγγελία αυτοκτονίας στο Διαδίκτυο και ίσως να βοηθήσω να καταλήξουμε πως *αλλιώς* και από ποιους *άλλους* θα έπρεπε να αντιμετωπίζεται.

Ιδού, λοιπόν, τα πραγματικά περιστατικά[1]: την 6.5.2009 περιήλθε στην Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος η πληροφορία ότι χρήστης με το ψευδώνυμο «dimitrios» ανάρτησε στην ιστοσελίδα http://www.lifo.gr/blogs/dimitrios/16503#comment, σκέψεις, οι οποίες οδηγούσαν στο συμπέρασμα ότι προτίθεται να θέσει τέλος στη ζωή του.

Έτσι όπως εισέρχονται τα δεδομένα δεν προκύπτει *prima facie* το ενδεχόμενο τέλεσης αξιόποινης πράξης ώστε να γεννάται, σύμφωνα με τους κανόνες της ποινικής δικονομίας, καθήκον αυτεπάγγελτης επέμβασης της Αστυνομίας και ειδικότερα της Δίωξης Ηλεκτρονικού Εγκλήματος πόσω μάλλον του Εισαγγελέα καθόσον η προαναγγελία αυτοκτονίας δεν είναι αξιόποινη πράξη και μάλιστα από αυτές που ανήκουν στο «ηλεκτρονικό» λεγόμενο έγκλημα. Η έλλειψη, όμως, άλλων κρατικών υποδομών, όπως για παράδειγμα κάποιας κοινωνικής υπηρεσίας, αποτελούμενης από κοινωνικούς λειτουργούς ή ψυχολόγους, εκπαιδευμένους στην ανίχνευση εντός του διαδικτύου τέτοιων προαναγγελιών, με αποστολή τον εντοπισμό του αποστολέα και την ψυχολογική υποστήριξή του ώστε σε πρώτη φάση, άμεσα, να μην αποπειραθεί να θέσει τέλος στη ζωή-του και σε δεύτερη, μακροπρόθεσμα, να αποτραπεί από παρόμοιες σκέψεις, δημιούργησε το «ηθικό», περισσότερο, καθήκον τόσο της Δίωξης Ηλεκτρονικού Εγκλήματος, λόγω εξειδικευμένων γνώσεων όσο και του Εισαγγελέα να παρέμβουν, ο καθένας με τον τρόπο-του, ώστε να προληφθεί η καταστροφή μιας ανθρώπινης ζωής.

Το μόνο έγκλημα που θα μπορούσε, ενδεχομένως, να τελείται κατά το χρόνο αποστολής της προαναγγελίας είναι αυτό της συμμετοχής σε αυτοκτονία, που προβλέπεται και τιμωρείται από τις διατάξεις του άρθρ. 301 ΠΚ. Σύμφωνα με τις τελευταίες τιμωρείται με φυλάκιση, δηλαδή σε βαθμό πλημμελήματος, όποιος με πρόθεση καταπείθει άλλον να αυτοκτονήσει, αν τελέστηκε η αυτοκτονία ή έγινε απόπειρά της καθώς και όποιος δίνει βοήθεια κατ' αυτήν. Με την «αρωγή»

1. Στο ιστορικό είναι πραγματικό έχουν, όμως, αλλαχθεί τα ονόματα.

της ανωτέρω ποινικής διάταξης η Δίωξη Ηλεκτρονικού Εγκλήματος συνέτασσε άμεσα, μόλις αντιλαμβανόταν την ύπαρξη τέτοιας προαναγγελίας, σχετική αναφορά, που υπέβαλε στον οικείο Εισαγγελέα Πρωτοδικών, ο οποίος, με τη σειρά-του, της απεύθυνε παραγγελία προκαταρκτικής εξέτασης προκειμένου να διακριβωθεί το ενδεχόμενο τέλεσης της ανωτέρω πράξης και ιδίως να αποκαλυφθεί η διεύθυνση IP και ο κάτοχός της. Στην πραγματικότητα λοιπόν γινόταν έρευνα για την αποκάλυψη των στοιχείων όχι δράστη αξιόποινης πράξης που χρησιμοποιεί ως μέσο τέλεσης το διαδίκτυο αλλά του χρήστη του διαδικτύου που προαναγγέλλει την αυτοκτονία-του προκειμένου, αν αυτή (η προαναγγελία) είναι σοβαρή, να αποτραπεί η αυτοκτονία και σε δεύτερο στάδιο, αν παρ' ελπίδα αυτή ή απόπειρά της είχε ήδη τελεστεί να διερευνηθεί αν κάποιος τον κατέπεισε να αυτοκτονήσει ή του έδωσε βοήθεια.

Για λόγους, που όπως είπαμε θα αναπτυχθούν από άλλος εισηγητές σήμερα, οι πάροχοι υπηρεσιών διαδικτύου αρνούντο να χορηγήσουν στη Δίωξη Ηλεκτρονικού Εγκλήματος τα αιτούμενα, αναγκαία δεδομένα για την ανίχνευση και τον προσδιορισμό της πηγής της επικοινωνίας και πιο συγκεκριμένα το ονοματεπώνυμο και τη διεύθυνση του συνδρομητή ή εγγεγραμμένου χρήστη στον οποίο είχε αποδοθεί κατά το χρόνο επικοινωνίας διεύθυνση IP (πρωτοκόλλου διαδικτύου), απαιτώντας την προηγούμενη έκδοση Διάταξης και Βουλεύματος περί άρσεως του απορρήτου της σχετικής επικοινωνίας, σύμφωνα τις προϋποθέσεις και τη διαδικασία που προβλέπουν οι διατάξεις του άρθρ. 4 Ν. 2225/1994. Οι διατάξεις αυτές προβλέπουν ότι η άρση του απορρήτου (των επικοινωνιών) είναι επιτρεπτή μόνο για τη διακρίβωση συγκεκριμένων *κακουργημάτων*. Ποιο κακούργημα τελείται, όμως, σε περίπτωση προαναγγελίας αυτοκτονίας; Η ελληνική εφευρετικότητα επιστρατεύθηκε και πράγματι στάθηκε στο ύψος-της. Επινοήθηκε η απόπειρα ανθρωποκτονίας με παράλειψη, κατά συναυτουργία (άρθρ. 15, 42 παρ. 1, 45, 83, 299 παρ. 1 ΠΚ), που φέρεται ότι τελούν οι γονείς σε βάρος του ανήλικου τέκνου-τους, κατά την ώρα που προαναγγέλλει την αυτοκτονία του.

Με την «αρωγή» της ανωτέρω ελληνοπρεπέστατης «πατέντας», η οποία, ας σημειωθεί, πέραν του ότι η εφαρμογή-της στα συγκεκριμένα πραγματικά περιστατικά είναι δογματικά εσφαλμένη δεν καλύπτει, ούτως ή άλλως, ενήλικους, υποψήφιους αυτόχειρες, ο αρμόδιος Εισαγγελέας Πρωτοδικών εκών άκων εκδίδει Διάταξη, την οποία επικύρωσε το οικείο Συμβούλιο, περί άρσης του απορρήτου της ανωτέρω επικοινωνίας, από την εκτέλεση της οποίας προέκυψε ότι οι επίμαχες σκέψεις αναρτήθηκαν την 5.5.2009 και ώρα 21:09 (GMT + 0300) από τον ενήλικο Δημήτριο Παπαδόπουλο μέσω της με IP address: 77.49.157.48/FORTHNET, που ανήκει στη μητέρα-του Δέσποινα Γεωργίου. Για το τι ακολουθεί αρμοδιότερος να απαντήσει είναι ο κος Διευθυντής.

Ήδη θα έχετε αντιληφθεί ότι το νομικό παράδοξο του τίτλου της εισήγησής μου δεν εντοπίζεται τόσο στο ότι απαιτείται, λόγω, θέλω να πιστεύω, δογματικού εγκλωβισμού (βλ. εξωτερικά στοιχεία επικοινωνίας), άρση απορρήτου για να αποκαλυφθούν τα στοιχεία κάποιου, που δημοσιοποιεί σε blog την πρόθεσή του να αυτοκτονήσει και να βοηθηθεί έστω προσωρινά. Δεν είναι νομικό παράδοξο η εσφαλμένη ερμηνεία του Νόμου. Όλοι οι εφαρμοστές έχουμε υποπέσει στο συγκεκριμένο «αδίκημα». Εντοπίζεται κυρίως σε αυτή την ίδια την εμπλοκή της ποινικής δικαιοσύνης σε ένα θέμα που δεν φαίνεται εξαρχής να την αφορά. Ας σκεφθούμε: πρέπει να επιστρατευθεί ολόκληρος ο μηχανισμός ποινικής καταστολής για να σωθεί ένας καταθλιπτικός άνθρωπος; Πρέπει κάποιος να τελεί πλημ/μα ή κακούργημα σε βάρος-του; Πρέπει να διενεργήσει προκαταρκτική εξέταση η Δίωξη Ηλεκτρονικού Εγκλήματος; Πρέπει και εδώ να επέμβει ο Εισαγγελέας;

Πιστεύω ότι η προαναγγελία αυτοκτονίας πρέπει να αντιμετωπισθεί όπως ταιριάζει σε αυτό που πράγματι είναι: μια επείγουσα κλήση για βοήθεια. Δεν διαφοροποιείται σε κανένα ουσιώδες σημείο από μια κλήση για βοήθεια σωματικά ασθενούς, που δεν ξέρουμε που βρίσκεται, μια κλήση έκτακτης ανάγκης, μια κλήση που πρέπει να απαντάται από ανθρώπους που ξέρουν και μπορούν πραγματικά να βοηθήσουν.

Ευχαριστώ για την υπομονή σας.

Δημήτριος Ι. Γκύζης

Εισαγγελέας Πρωτοδικών Αθηνών

«Κραυγές απόγνωσης μέσω Διαδικτύου»

κ. **Εμμανουήλ Σφακιανάκης**, Αστυνομικός Διευθυντής,
Προϊστάμενος Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος

Σας ευχαριστώ κι εγώ με τη σειρά μου που μου κάνετε την τιμή να είστε εδώ στο συνέδριο μας, ένα συνέδριο που σκοπό έχει να δείξει ότι το διαδίκτυο είναι το άλφα και το ωμέγα. Η Δίωξη Ηλεκτρονικού Εγκλήματος λέει ναι στο Διαδίκτυο και ναι στις νέες τεχνολογίες. Καθημερινά δεχόμαστε τους προβληματισμούς του κόσμου και ακούμε τα προβλήματά του. Πρέπει λοιπόν να δώσουμε λύσεις. Ευτυχώς που έχουμε δίπλα μας τους Εισαγγελείς και τους δικαστές. Χωρίς τους Εισαγγελείς δε θα είχαμε κάνει τίποτα. Ευχαριστούμε την Προϊσταμένη της Εισαγγελίας Πρωτοδικών, την κυρία Φάκου, η οποία μας έχει διαθέσει δύο Εισαγγελείς που τους έχουμε όποτε τους χρειαστούμε. Καθημερινά έχουμε καταργήσει το ταχυδρομείο και πάμε τις υποθέσεις χέρι με χέρι, λόγω του κατεπείγοντος των υποθέσεων. Όταν βλέπουμε έναν άνθρωπο που κινδυνεύει, τα δίνουμε όλα. Ευχαριστώ μέσα από την καρδιά μου τον Εισαγγελέα του Αρείου Πάγου, την Πρόεδρο του Αρείου Πάγου, τους Εισαγγελείς και τους Δικαστές. Οι άνθρωποι αυτοί είναι μαζί μου και λύνουμε τα προβλήματα. Μόνος μου δε θα είχα κάνει τίποτα και αυτή είναι μια εξομολόγηση από καρδιάς. Οφείλω να πω πως και με τον κο Σανιδά είχαμε άψογη συνεργασία.

Το διαδίκτυο έχει μπει για τα καλά στη ζωή μας και τα παιδιά μας αντιμετωπίζουν κινδύνους μπροστά τους. Εμείς λέμε ναι στο διαδίκτυο και προστατεύουμε τα παιδιά κάνοντας συνέδρια και ημερίδες. Κάθε Παρασκευή 12-2 είμαστε κοντά στα παιδιά μέσω τηλεδιασκέψεων. Έχουμε χιλιάδες αιτήματα από σχολεία να πάμε να μιλήσουμε. Καθημερινά δεχόμαστε αιτήματα από περίπου 50 σχολεία. Επειδή όμως είναι ανέφικτο να τα επισκεφτούμε όλα αυτά, η Vodafone μας έχει χορηγήσει το Microsoft Link 365. Μέσω του συστήματος αυτού, συνδεόμαστε ταυτόχρονα με 20-30 σχολεία και γλιτώνουμε τις μετακινήσεις. Έτσι, κάνουμε παρουσιάσεις στα παιδιά, στο τέλος των οποίων δεχόμαστε ερωτήσεις από τα παιδιά. Μέσω του συστήματος αυτού, έχουμε σωθεί, καθώς καλύπτουμε όλη την Ελλάδα. Μιλάμε σε 5000-6000 παιδιά ταυτόχρονα και μεταλαμπαδεύουμε σε αυτά τις γνώσεις και τις εμπειρίες μας για το διαδίκτυο.

Αν έχει μπει κόφτης στα εγκλήματα εκφοβισμού μέσα από το διαδίκτυο, είναι γιατί η Υπηρεσία μας προέβλεψε το είδος αυτών των εγκλημάτων εδώ και 5 χρόνια. Δεν μπορώ να ξεχάσω τις ημερίδες που έχω πάει στα βουνά και στα λαγκάδια με τους αξιωματικούς. Πρέπει να υπάρχει γνώση και πρόληψη κι εμείς αυτό το πιστεύουμε. Μέσα από αυτό το συνέδριο, θα μεταλαμπαδευτεί η γνώση και έτσι θα έχουμε αποτέλεσμα. Όταν μιλάμε σε παιδιά, βλέπουμε ότι αυτά απορροφούν όλον τον προβληματισμό μας. Τα παιδιά είναι σκεπτόμενα, έχουμε καλό υλικό, αλλά πρέπει να τους δώσουμε γνώση. Για αυτό, κάνω όλον αυτό τον αγώνα, για να μεταλαμπαδεύσουμε τη γνώση που χρειάζονται τόσο οι γονείς όσο και τα παιδιά. Ξέρετε πόσα παιδιά έχουμε σώσει από κρυφά ραντεβού, που γνωρίζουμε μέσω chat και πηγαίνουν; Όταν λέμε τις εμπειρίες μας στα παιδιά, αυτά προβληματίζονται και κόβουν κάθε δίοδο προς το έγκλημα; Καθημερινά δεχόμαστε πο-

λίτες στην Υπηρεσία μας. Έχουμε όμως καταφέρει και ελέγχουμε το έγκλημα μέσα από το διαδίκτυο, καθώς έχουμε καλή δικαιοσύνη και καλή αστυνομία. Παλιά ήταν αναρχία, τώρα όμως με τους αξιωματικούς που έχουμε, με το προσωπικό που έχουμε και τους δικαστές, υπάρχει ιδιαίτερα αποδοτικός έλεγχος.

Ας περάσουμε στην παρουσίασή μας, όπου εκθέτουμε τους προβληματισμούς μας για το διαδίκτυο, τα εμπόδια και τις εμπειρίες μας και πάνω από όλα τι κάνουμε εμείς όταν βλέπουμε αυτές τις κραυγές απόγνωσης από διάφορα μέρη, είτε είναι απειλή είτε είναι αυτοκτονία. Θα πω τους προβληματισμούς μου στους νομικούς επιστήμονες, προκειμένου να μου δώσουν λύσεις.

Το διαδίκτυο είναι το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο. Έχεις πρόσβαση από παντού και η πρόσβαση γίνεται ακόμα και με κινητό τηλέφωνο.

Οι πληροφορίες όμως που παίρνεις μέσα από αυτό, δεν είναι πάντα έγκυρες. Και αυτό συμβαίνει γιατί τις πληροφορίες τις γράφει ο άνθρωπος και όπου μπαίνει χέρι ανθρώπινο, αν γράφει από του πονηρού, υπάρχει πρόβλημα. Κάποιος γράφει μέσα από ένα Blog ένα ψέμα, μια συκοφαντία, η οποία στη συνέχεια γίνεται εκβίαση και ζητάει λεφτά από το θιγόμενο για να το κατεβάσει. Επομένως, ό,τι γράφουμε στο διαδίκτυο το διυλίζουμε και προσπαθούμε να δούμε το σκοπό για τον οποίο έχει γραφτεί. Δε βάζουμε στην πυρά τον άνθρωπο για τον οποίο έχει γραφτεί ένα αρνητικό δημοσίευμα. Ξέρετε πόσοι άνθρωποι αυτή τη στιγμή παίρνουν ψυχοφάρμακα και αιτία είναι τα αρνητικά σχόλια στο διαδίκτυο; Προσωπικά, δέχομαι καθημερινά 40 καταγγελίες για ανώνυμα σχόλια. Αυτό είναι θέμα και η πολιτεία πρέπει να το λύσει. Ευχαριστώ δημόσια τον κο Σανιδά και τον κο Τέντε που με τις γνωμοδοτήσεις τους έχουν δώσει λύσεις. Αν δεν υπήρχαν οι γνωμοδοτήσεις του Αρείου Πάγου, αυτήν τη στιγμή θα είμαστε όλοι με ψυχοφάρμακα.

Φαντάζεστε στο διαδίκτυο να μπορεί ο καθένας να λέει αρνητικά πράγματα για τον άλλον; Να λέει ότι θέλει και να μην τιμωρείται; Εάν δεν υπήρχαν οι γνωμοδοτήσεις του Αρείου Πάγου θα είχαμε μέγα θέμα. Οι γνωμοδοτήσεις των Εισαγγελέων είναι αυτές που έλυσαν το θέμα σε πολύ μεγάλο βαθμό.

Περνάμε σε ένα άλλο θέμα, όποιο αρχείο δημοσιεύεται στο διαδίκτυο, μένει εκεί για πάντα. Πρέπει να προσέχουμε ποιό αρχείο δημοσιοποιούμε στο διαδίκτυο, γιατί υπάρχουν και κακόβουλοι που παίρνουν τα αρχεία και τα αρχεία αυτά συνοδεύουν μετά από χρόνια το βιογραφικό μας. Πρέπει λοιπόν αυτό που γράφουμε, να προσέξουμε πριν το γράψουμε. Για παράδειγμα, το facebook δε διαγράφει ποτέ το λογαριασμό μας και όσα έχουμε γράψει διατηρούνται. Με απλά λόγια, τα παιδιά μας όταν μεγαλώσουν και ψάξουν για δουλειά, μπορεί να βρουν μπροστά τους πράγματα που έχουν γράψει στο facebook όταν ήταν 16.

Και προχωράμε στα στατιστικά: το 96% των συνδέσεων είναι ευρυζωνικές, ενώ το 53,2 των νοικοκυριών έχουν πρόσβαση στο διαδίκτυο. Το 55% έχουν ηλεκτρονικούς υπολογιστές. Το 94% των νέων ανθρώπων χρησιμοποιούν τις νέες τεχνολογίες.

Ποιες είναι οι μορφές εγκληματικότητας που γνωρίζουν έξαρση σήμερα;

- Παιδική πορνογραφία
- Cyber bullying
- Τυχερά παιχνίδια-Τζόγος
- Προσωπικά Δεδομένα
- Απάτες μέσω διαδικτύου
- Παράνομη διείσδυση σε υπολ. συστήματα (cracking)

- Διακίνηση πειρατεία λογισμικού
- Διακίνηση ναρκωτικών
- Εγκλήματα κυβερνο-εμπορίου

Τώρα μπαίνουμε σε ένα μεγάλο αγώνα δρόμου που κάνουμε καθημερινά, τις αυτοκτονίες. Οι αυτοκτονίες είναι μεγάλο στοίχημα για την Υπηρεσία μας, πώς θα εντοπίσουμε το άτομο που έχει πρόβλημα και κινδυνεύει. Σε περίπτωση που κάποιος απειλεί μέσα από το διαδίκτυο σε κάποιο site ότι θα αυτοκτονήσει, κάνουμε αίτημα στη χώρα όπου φιλοξενείται το site. Περιμένουμε λοιπόν να μας στείλουν το ηλεκτρονικό ίχνος και μόλις μας το στείλουν, κατόπιν εισαγγελικής εντολής, ζητάμε στοιχεία από την εταιρεία που παρέχει υπηρεσίες διαδικτύου, οι οποίες μας δίνουν που ανήκει το ίχνος. Εδώ θα ήθελα να αναφερθώ σε μια γνωμοδότηση και να ζητήσω τη γνώμη των ειδικών. Μέσα από τη γνωμοδότηση αυτή, ανάγεται η αυτοκτονία σε ανθρωποκτονία και έτσι παίρνουμε τα ηλεκτρονικά ίχνη. Η γνωμοδότηση αυτή είναι η 68/2008 από την ΑΔΑΕ. Θα ήθελα να μου πουν οι ειδικοί κατά πόσο αυτό μπορεί να στοιχειοθετηθεί και να είναι το άλφα και το ωμέγα για να κάνουμε μια έρευνα.

Στη συνέχεια, έχουμε τις εξής γνωμοδοτήσεις του Αρείου Πάγου: Υπ' αριθ. 9/2011, υπ' αριθ. 12/2009 και υπ' αριθ. 9/2009.

Σύμφωνα με την απάντηση που έδωσε ο Άρειος Πάγος (07-12-2012) σε εταιρεία παροχής υπηρεσιών Ίντερνετ προς Παρόχους Υπηρεσιών Ίντερνετ: Οι παραγγελίες των Εισαγγελικών και δικαστικών Αρχών πρέπει να εκτελούνται άμεσα για άρση του απορρήτου ή Χορήγηση στοιχείων από τους Παρόχους Υπηρεσιών Ίντερνετ. Η συμμόρφωση αυτή δεν συνεπάγεται καμία κύρωση οποιασδήποτε μορφής αφού σε κάθε περίπτωση οι εταιρείες δεν έχουν υποχρέωση να ελέγχουν την νομιμότητα των παραγγελιών. Ο πάροχος λοιπόν δεν έχει δικαίωμα να ελέγχει τον Εισαγγελέα.

Η Συνθήκη της Βουδαπέστης:

- Στη Συνθήκη αυτή τονίζεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγεται το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά.
- Στη Συνθήκη αυτή, την οποία υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας, υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα.
- Η Συνθήκη αυτή έχει υπογραφεί μεν από την Ελλάδα, πλην όμως δεν έχει ενταχθεί, με την ψήφιση σχετικού νόμου, στο ελληνικό δίκαιο μέχρι σήμερα.

Η συνθήκη αυτή ελπίζουμε να γίνει σύντομα νόμος του κράτους.

Τέλος, έχουμε συνεργασία με Μ.Κ.Ο., Εισαγγελικές Αρχές, Ιντερπόλ και Europol.

«Η Λερναία Ύδρα διαμοιρασμού προστατευομένων αρχείων»

Θεμιστοκλής Ι. Σοφός
Δ.Ν. – Δικηγόρος

Η Λερναία Ύδρα, καρπός της Έχιδνας και του Τυφώνα, δρούσε στην περιοχή Λέρνη – βαλτότοπος που βρίσκεται νότια του Άργους – απ' όπου πήρε και το όνομά της. Όταν ο Ηρακλής έκοβε ένα κεφάλι, έβγαιναν δύο. Μόνο καίγοντάς το με φωτιά κατάφερε να σταματήσει τον πολλαπλασιασμό και αυτό το κατάφερε με την βοήθεια του ανιψιού του Ιολάου. Το τελευταίο κεφάλι, που ήταν και το κεντρικό κι αθάνατο, το έκοψε και το έθαψε στη γη για να μην ξαναζωντανέψει. Από το αίμα της ο Ηρακλής έκανε τα βέλη του δηλητηριώδη.

22 κράτη μέλη της Ευρωπαικής Ένωσης –ανάμεσα τους και η χώρα μας– υπέγραψαν τον Ιανουάριο του 2012 στο Τόκυο τη συμφωνία κατά της πειρατείας ACTA (Anti-Coutnerfeiting Trade Agreement). Στην πράξη, η ACTA αφορά τη θέσπιση διεθνών προτύπων σε ζητήματα που σχετίζονται με την προστασία και την επιβολή των πνευματικών δικαιωμάτων και την καταπολέμηση της πειρατείας. Μεταξύ άλλων, η συμφωνία προτείνει σοβαρότατες κυρώσεις –όπως απαγόρευση πρόσβασης στο διαδίκτυο, πρόστιμα ή ακόμα και φυλάκιση– για όσους επιχειρήσουν να χρησιμοποιήσουν ή να μοιραστούν αρχεία προστατευμένα με copyrights. Η υπογραφή της συμφωνίας προκάλεσε έντονες αντιδράσεις, με κυριότερο επιχείρημα την απόπειρα κατάργησης της ελευθερίας της έκφρασης στο διαδίκτυο. Ο λεγόμενος "*homo hactivist*" δείχνει να έχει χάσει τον έλεγχο, αφού ακτιβιστές hackάρουν κυβερνητικές ιστοσελίδες, όπως αυτές του Πρωθυπουργού και του Κοινουβουλίου της Πολωνίας. Από την 1η Οκτωβρίου 2011 τη συμφωνία υπέγραψαν οι ΗΠΑ, Αυστραλία, Καναδάς, Νότια Κορέα, Σιγκαπούρη, Νέα Ζηλανδία και Μαρόκο. Οι πέντε ευρωπαϊκές χώρες που δεν υπέγραψαν είναι οι Γερμανία, Ολλανδία, Εσθονία, Σλοβακία και Κύπρος. *Το Ευρωπαϊκό Κοινοβούλιο καταψήφισε την συμφωνία ACTA με πλειοψηφία 478 –39*. «Hello Democracy, Goodbye ACTA» φώναξαν κάποιοι νομικοί μετά την ανακοίνωση του αποτελέσματος την 5 Ιουλίου 2012.

Σύμφωνα με το άρθρο 27 παρ. 4 της ACTA, την οποία έχει συνυπογράψει και η χώρα μας, ένα συμβαλλόμενο μέρος μπορεί, σύμφωνα με τους νόμους και τους κανονισμούς του, να εξασφαλίζει στις αρμόδιες αρχές του την εξουσία να διατάσσουν έναν πάροχο υπηρεσιών διαδικτύου **να αποκαλύπτει**, χωρίς χρονοτριβή, στον κάτοχο δικαιώματος πληροφορίες επαρκείς για τον εντοπισμό συνδρομητή του οποίου ο λογαριασμός φέρεται ότι χρησιμοποιήθηκε για παρανομία, **όταν ο εν λόγω κάτοχος δικαιώματος έχει καταθέσει νομικά επαρκή ισχυρισμό παραβίασης εμπορικού σήματος ή δικαιώματος πνευματικής ιδιοκτησίας ή σχετικών δικαιωμάτων και όταν οι πληροφορίες αυτές ζητούνται με σκοπό την προστασία ή την επιβολή αυτών των δικαιωμάτων**. Οι διαδικασίες αυτές εφαρμόζονται κατά τρόπο που να αποφεύγεται η δημιουργία εμποδίων για νόμιμες δραστηριότητες, συμπεριλαμβανομένου του ηλεκτρονικού εμπορίου, και, σύμφωνα με τη νομοθεσία του συμβαλλόμενου μέρους, να τηρούνται θεμελιώδεις αρχές, όπως η

ελευθερία της έκφρασης, η διεξαγωγή δίκαιης δίκης και η ιδιωτικότητα. Ενώ, στο άρθρο 39 παρ. 2 της ACTA προβλέπεται, ότι για να καταπολεμηθεί η παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας, ιδίως η απομίμηση ή παραποίηση εμπορικών σημάτων ή η παράνομη εκμετάλλευσης δικαιώματος πνευματικής ιδιοκτησίας ή σχετικών δικαιωμάτων, τα συμβαλλόμενα μέρη **προωθούν τη συνεργασία, κατά περίπτωση, μεταξύ των αρμόδιων αρχών τους που είναι υπεύθυνες για την επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας. Η συνεργασία αυτή μπορεί να περιλαμβάνει τη συνεργασία για την επιβολή του νόμου όσον αφορά τις ποινικές κυρώσεις και τα συνοριακά μέτρα που προβλέπει η παρούσα συμφωνία**.

Την ίδια ώρα, μεγάλα sites διαμοιρασμού αρχείων και μηχανών αναζήτησης torrents κλείνουν το ένα μετά το άλλο μπροστά στο ενδεχόμενο να καταλήξουν στη φυλακή οι διαχειριστές τους. Εύλογα τα ερωτήματα που προκύπτουν: Θα υποχρεωθούν οι πάροχοι υπηρεσιών INTERNET (ISP) να κατασκοπεύουν τις πληροφορίες που περνάμε μέσα από τα δίκτυα μας; Θα ελέγχονται στα αεροδρόμια οι φορητοί υπολογιστές για παράνομες ταινίες και τραγούδια; Τι γίνεται αν ποστάρεις ένα video clip στο FACEBOOK ή το twitter; Θα βρίσκονται και οι καλλιτέχνες υπόλογοι επειδή διακίνησαν με «παράνομο» τρόπο την ίδια τους τη δουλειά; Τελικά, μπορεί κάποιος να βάλει σύνορα εκεί που δεν πρέπει να υπάρχουν; Είναι όντως σενάριο επιστημονικής φαντασίας ή μία ζοφερή πραγματικότητα; Η οθόνη του υπολογιστή θα δείξει.

Ένα παράδειγμα που αποτυπώνει γλαφυρά το ζήτημα είναι η ιστορία ενός ζαχαροπλαστείου στις Η.Π.Α., το COLLEGE BAKERY. Εκεί προσφέρονταν πλάκες ζάχαρης, πάνω στις οποίες τα παιδιά θα ζωγράφιζαν τον ήρωά τους. Άλλα ζωγράφισαν μυθικούς ή φανταστικούς ήρωες, άλλα τους γονείς τους, και άλλα το Mickey Mouse. Όσο αστείο και αν ακούγεται το παράδειγμα, ανέκυψε πρόβλημα ως προς τη δυνατότητα πώλησης της συγκεκριμένης τούρτας, αφού παραβίαζε συγκεκριμένα πνευματικά δικαιώματα.

Με τα νομοσχέδια **SOPA** (Stop On-line Piracy Act – Νόμος «Σταματήστε την πειρατεία στο INTERNET) και **PIPA** (Protect Intellectual Property Act – Νόμος για την προστασία της πνευματικής ιδιοκτησίας) έγινε προσπάθεια περιορισμού της ελευθερίας αναπαραγωγής προστατευομένων αρχείων, αλλά χωρίς επιτυχία μέχρι τώρα.

«Η ελευθερία δεν παραχωρείται ποτέ εθελοντικά από τον καταπιεστή. Πρέπει να κατακτηθεί από τον καταπιεζόμενο». Αυτήν τη ρήση του Μάρτιν Λούθερ Κινγκ έκανε tweet ο Τζίμι Γουέιλς, ιδρυτής τη Wikipedia, του έκτου δημοφιλέστερου site του κυβερνοχώρου, την ημέρα που το blackout στο Internet έγραψε Ιστορία.

Το αγαθό της ελευθερίας όμως ανήκει και στον πνευματικό δημιουργό, και όχι μόνον στο χρήστη που θέλει να κάνει share στο έργο του πνευματικού δημιουργού, να το διαμοιράσει. Για 48 ώρες, την Τετάρτη 18 Ιανουαρίου, το Διαδίκτυο «σκοτείνιασε», με εκατομμύρια εξοργισμένους χρήστες, μπλόγκερ και επαγγελματίες να διαμαρτύρονται ενάντια στα νομοσχέδια SOPA και PIPA που προχωρούσαν στο Κογκρέσο των ΗΠΑ. Ανάμεσα τους η αγγλική Wikipedia με απόφαση, μάλιστα, του ίδιου του Γουέιλς, αλλά και η Google που χαρακτηριστικά έγραψε «End piracy not liberty».

Με μία από τις πιο ενδιαφέρουσες δικαστικές αποφάσεις της τελευταίας δεκαετίας, την υπ΄ αριθμ. 4658/2012 απόφαση του Μονομελούς Πρωτοδικείου Αθηνών (ΝοΒ 2012, 1204, με σχόλιο *Μιχ. Μαργαρίτη*) κρίθηκε αίτηση ασφαλιστικών μέτρων αστικής μη κερδοσκοπικής εταιρίας συλλογικής διαχείρισης και προστασίας των συγγενικών δικαιωμάτων, που έχει συσταθεί νόμιμα κατά το άρθρο 54 παρ. 4 του νόμου 2121/1993 από τις δισκογραφικές επιχειρήσεις-παραγωγούς

υλικών φορέων ήχου. Όπως ορθά επισημαίνει ο διακεκριμένος δικαστής *Μ. Μαργαρίτης*, Αρεοπαγίτης ε.τ., στο σχόλιό του επί της ως άνω δημοσιευομένης αποφάσεως, «*ευελπιστούμε ότι η απόφαση θα αποτελέσει μία καλή αρχή προς περιστολή της διαδικτυακής ασυδοσίας στην πειρατεία των έργων πνευματικών δημιουργών*».

Σύμφωνα με την αίτηση, μέσω ιστοσελίδας εδρεύουσας στις Η.Π.Α. που δεν ανήκει ούτε φιλοξενείται από τις καθών εταιρίες, που είναι φορείς παροχής υπηρεσιών της κοινωνίας της πληροφορίας, αφενός έχουν παρανόμως αναπαραχθεί (ανέβει) και καθίστανται διαρκώς προσιτά στο κοινό και αφετέρου καταφορτώνονται παράνομα μουσικά έργα, ταινίες, βιβλία και άλλα έργα επί των οποίων υπάρχουν δικαιώματα πνευματικής ιδιοκτησίας και συγγενικά δικαιώματα· ότι η εν λόγω ιστοσελίδα κατατάσσεται στη θέση με αριθμό 293 της ελληνικής επισκεψιμότητας· ότι οι ιδιοκτήτες εκμεταλλευτές, αλλά και οι συνδρομητές μέλη της εν λόγω ιστοσελίδας προβαίνουν σε ψηφιοποίηση ελληνικού και ξένου ρεπερτορίου, ακολούθως δε στη διαδικασία του φορτώματος των εν λόγω ψηφιοποιημένων έργων – αντιγράφων σε κεντρικούς servers γνωστών διαδικτυακών τόπων παράνομης αποθήκευσης φωνογραφημάτων, που αναφέρονται ειδικά στην αίτηση, δημιουργούμενου σταθερού ψηφιακού αντιγράφου εκάστου φωνογραφήματος· ότι τα εν λόγω φωνογραφήματα είναι ανοικτά προς ψηφιακή κλήση με τη δημιουργία υπερσυνδέσμων ή συνδέσμων· ότι έτσι παρέχουν τη δυνατότητα σε οποιονδήποτε επισκέπτη της εν λόγω ιστοσελίδας να αποκτήσει πρόσβαση σε αποθηκευμένα φωνογραφήματα ενεργοποιώντας το σύνδεσμο, η ύπαρξη του οποίου καθιστά το έργο προσιτό στο χρήστη, όταν και από όπου ο ίδιος το επιθυμεί· ότι το σύνολο των φωνογραφημάτων που ψηφιοποιήθηκαν, φορτώθηκαν και κατέστησαν ανοικτά προς ψηφιακή κλήση, έχουν ψηφιοποιηθεί άνευ αδείας των αποκλειστικών για την Ελλάδα δικαιούχων των συγγενικών δικαιωμάτων επ' αυτών· ότι τα περιεχόμενα στην ως άνω ιστοσελίδα φωνογραφήματα έγιναν πράγματι αντικείμενο εκμετάλλευσης από Έλληνες διαδικτυακούς χρήστες, οι οποίοι είναι συνδρομητές σε κάποια από τις καθών, οι οποίες είναι οι μοναδικές που παρέχουν πρόσβαση στο διαδίκτυο σε Έλληνες χρήστες, εγκατεστημένους στην Ελλάδα· ότι ο χρήστης πληκτρολογώντας το domain name της ένδικης ιστοσελίδας σε λογισμικό πρόγραμμα περιήγησης, αποκτά πρόσβαση στην ιστοσελίδα και μπορεί να πλοηγηθεί σ' αυτή και να επιλέξει το φωνογράφημα που επιθυμεί, το οποίο σημαίνεται με συγκεκριμένο σύνδεσμο, που ενεργοποιεί ο χρήστης και ο οποίος ανακατευθύνει τη σύνδεση σε διακομιστή, όπου το έργο είναι προαποθηκευμένο· ότι κατόπιν αυτού το έργο αποθηκεύεται ως αρχείο στο σκληρό δίσκο του ηλεκτρονικού υπολογιστή του χρήστη–μέλους της ιστοσελίδας· ότι οι καθών εταιρίες, οι οποίες διατηρούν δίκτυο επικοινωνιών, παρέχουν στους συνδρομητές τους χρήστες του διαδικτύου τις υπηρεσίες της πρόσβασης στο διαδίκτυο και της μετάδοσης πληροφοριών με τη διαδικασία του caching εντός τους δικτύου τους· ότι αυτοί (χρήστες) καθίστανται αποδέκτες των εν λόγω υπηρεσιών· ότι και οι ιδιοκτήτες/εκμεταλλευτές της ένδικης ιστοσελίδας είναι επίσης αποδέκτες, καθώς παρέχουν στους συνδρομητές των καθών πρόσβαση στα παραπάνω φωνογραφήματα· ότι χωρίς την υπηρεσία πρόσβασης που παρέχεται από τις καθών στους συνδρομητές τους οι ιδιοκτήτες/εκμεταλλευτές της ένδικης ιστοσελίδας θα αδυνατούσαν να παράσχουν τα φωνογραφήματα «ανοικτά» προς κλήση στην Ελλάδα και να προβούν στις ως άνω εκτεθείσες προσβολές των συγγενικών δικαιωμάτων· ότι μέλη της ίδιας (αιτούσας) είναι οι λεπτομερώς αναφερόμενοι στην αίτηση παραγωγοί υλικών φορέων ήχου.

Με βάση αυτό το ιστορικό, η αιτούσα, επικαλούμενη επείγουσα περίπτωση προσωρινής ρύθμισης της κατάστασης, καθώς και ότι ο κίνδυνος προσβολής είναι όχι μόνον επικείμενος, αλλά

ότι έχει επέλθει ήδη αυτή (προσβολή) λόγω των συνεχώς επαναλαμβανόμενων και πυκνών προσβολών, εκ των οποίων υπολογίζεται ότι απόλλυνται καθημερινά εισπράξεις που αντιστοιχούν σε πωλήσεις δεκάδων χιλιάδων δίσκων, όπως τούτο προκύπτει από τον αντίστοιχο αριθμό των συνδρομητών των καθών, που καθημερινά προβαίνουν σε πράξεις καταφόρτωσης φωνογραφημάτων από την παραπάνω ιστοσελίδα, η απώλεια δε εισπράξεων ανέρχεται σε ποσόν εκατοντάδων χιλιάδων ευρώ ημερησίως. Η αίτηση, σύμφωνα και με όσα αναφέρονται στις παραπάνω νομικές σκέψεις της παρούσας, παραδεκτά και αρμόδια φέρεται προς συζήτηση ενώπιον αυτού του Δικαστηρίου κατά τη διαδικασία των ασφαλιστικών μέτρων, εφαρμοζόμενου σύμφωνα με τα ανωτέρω εκτιθέμενα στην οικεία μείζονα σκέψη του ελληνικού δικαίου, αφού αφενός στην κρινόμενη αίτηση και κατ' εκτίμηση αυτής εκτίθεται ότι οι καθών είναι εταιρίες παροχής υπηρεσιών πρόσβασης στο διαδίκτυο με έδρα και άσκηση της οικονομικής τους δραστηριότητας στην ελληνική επικράτεια, αφετέρου δε υφίσταται προσβολή συγγενικών δικαιωμάτων, μέσω ενεργειών των συνδρομητών των καθών για καταφόρτωση φωνογραφημάτων που εκπροσωπούνται από την αιτούσα, ο αποδέκτης των οποίων – ιδιοκτήτης/εκμεταλλευτής της ανωτέρω ιστοσελίδας– εδρεύει στο εξωτερικό (Η.Π.Α.), η δε επικαλούμενη ζημία επήλθε στην Ελλάδα. Περαιτέρω, είναι νόμιμη, στηριζόμενη στις διατάξεις των άρθρων που διαλαμβάνονται ανωτέρω στις οικείες μείζονες σκέψεις, καθώς και σ' αυτές των άρθρων 1, 2 παρ.1, 46, 47, 54, 55, 63Α, 64, 64Α, 65 παρ. ί του Ν.2121/93, 11, 12, 17 Π.Δ. 131/2003, 682 επ., 450 επ, 731, 732, 176, 947 παρ. 1 ΚΠολΔ, 901 επ., 914 ΑΚ.

Κατά τη συζήτηση της υπόθεσης, η εκ των ανωτέρω Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), με προφορική δήλωση στο ακροατήριο άσκησε πρόσθετη παρέμβαση υπέρ των καθών οι αιτήσεις, ως έχουσα έννομο συμφέρον, ισχυριζόμενη ότι η ίδια ως Ανεξάρτητη Αρχή είναι αρμόδια για την επίβλεψη της αγοράς ηλεκτρονικών υπηρεσιών και τα αιτούμενα ασφαλιστικά μέτρα άπτονται της ελεγχόμενης από την ίδια υποχρέωσης των καθών να εξασφαλίζουν την ασφάλεια, ακεραιότητα και διατήρηση της σύνδεσης στο διαδίκτυο. Επίσης, υπέρ των αιτούντων παρενέβησαν με δήλωση στο ακροατήριο οργανισμοί προστασίας πνευματικής ιδιοκτησίας κ.α.

Με την εν λόγω απόφαση του Μονομελούς Πρωτοδικείου Αθηνών πιθανολογήθηκε ότι οι καθών είναι ανώνυμες εταιρίες παροχής υπηρεσιών πρόσβασης στο διαδίκτυο (internet service providers), η δε προσθέτως υπέρ αυτών παρεμβαίνουσα «Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων» (Ε.Ε.Τ.Τ.), η οποία είναι Ανεξάρτητη Αρχή και ως εκ του Ν. 3431/2006 αποτελεί την εθνική κανονιστική αρχή που ελέγχει, ρυθμίζει και εποπτεύει μεταξύ άλλων, την αγορά ηλεκτρονικών επικοινωνιών στην οποία δραστηριοποιούνται επιχειρηματικά. Οι καθών εταιρίες, οι οποίες διατηρούν δίκτυο επικοινωνιών, παρέχουν στους συνδρομητές τους χρήστες του διαδικτύου εγκατεστημένους στην Ελλάδα τις υπηρεσίες της πρόσβασης στο διαδίκτυο και της μετάδοσης πληροφοριών με τη διαδικασία του caching, εντός του δικτύου τους, οι δε συνδρομητές/χρήστες καθίστανται αποδέκτες των εν λόγω υπηρεσιών. Περαιτέρω πιθανολογήθηκε ότι μέσω της ιστοσελίδας με domain name www....., η οποία εδρεύει στις Η.Π.Α. στην πολιτεία του Αρκάνσας με διεύθυνση στο διαδίκτυο IP:....., δεν φιλοξενείται δε από τις ως άνω καθών εταιρίες, τουλάχιστον από το έτος 2010, οπότε και ήλθε σε γνώση των αιτούντων η ύπαρξη, η δραστηριότητα και η λειτουργία της εν λόγω ιστοσελίδας και μέχρι τη συζήτηση των κρινόμενων αιτήσεων, αφενός παρανόμως αναπαράγονταν (ανέβαιναν) και καθίσταντο διαρκώς προσιτά στο κοινό και αφετέρου καταφορτώνονταν σε καθημερινή βάση και από συνδρομητές των καθών – χρήστες του διαδικτύου, μουσικά έργα, ταινίες, βιβλία και άλλα έργα επί των οποίων υπάρχουν δικαιώματα πνευματικής ιδιοκτησίας και συγγενικά δικαιώματα δικαιούχων που

εκπροσωπούνται από τους αιτούντες και τον προσθέτως παρεμβαίνοντα αστικό μη κερδοσκοπικό συνεταιρισμό περιορισμένης ευθύνης.

Το σύνολο των έργων που ψηφιοποιήθηκαν, φορτώθηκαν και κατέστησαν ανοικτά προς ψηφιακή κλήση, από έρευνα που διενήργησε η αιτούσα ανερχόταν σε 381.618 μουσικά έργα, 239 ελληνικές ταινίες, 6.400 αλλοδαπές ταινίες, 1.247 βιβλία, 376 ελληνικές τηλεοπτικές σειρές, 2.442 ξένες τηλεοπτικές σειρές και 820 ντοκιμαντέρ, τα έργα δε αυτά έχουν ψηφιοποιηθεί άνευ αδείας των αποκλειστικών για την Ελλάδα δικαιούχων των δικαιωμάτων πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων επ' αυτών. Η ένδικη ιστοσελίδα λειτουργεί με τη μορφή διαδικτυακού forum όπου η θεματολογία του είναι προσβάσιμη μόνο σε εγγεγραμμένα μέλη, η διαδικασία δε που ακολουθείται για την φόρτωση/ανέβασμα (uploading) και την καταφόρτωση/ κατέβασμα (downloading) των εν λόγω έργων έχει ως ακολούθως: οι ιδιοκτήτες/εκμεταλλευτές, αλλά και οι συνδρομητές/μέλη της εν λόγω ιστοσελίδας προβαίνουν σε παράνομη ψηφιοποίηση ελληνικών και αλλοδαπών έργων, που ήδη είχαν το πρώτον νόμιμα ψηφιοποιηθεί από τους δικαιούχους αυτών, όπως αυτοί εκπροσωπούνται στην Ελλάδα από τους αιτούντες και τον προσθέτως παρεμβαίνοντα, ακολούθως δε (προβαίνουν) στη διαδικασία του φορτώματος των εν λόγω ψηφιοποιημένων έργων – αντιγράφων σε κεντρικούς servers γνωστών διαδικτυακών τόπων αποθήκευσης ψηφιοποιημένων έργων με την έννοια του Ν. 2121/1993 (www....., www..... κλπ), δημιουργούμενου εκεί σταθερού ψηφιακού αντιγράφου εκάστου έργου. Τα εν λόγω έργα είναι ανοικτά προς ψηφιακή κλήση από την ένδικη ιστοσελίδα με τη δημιουργία υπερσυνδέσμων ή συνδέσμων, παρέχοντας έτσι τη δυνατότητα σε οποιονδήποτε επισκέπτη της εν λόγω ιστοσελίδας, που θα καταστεί μέλος αυτής κατά τα ανωτέρω, να αποκτήσει πρόσβαση σε αποθηκευμένα έργα ενεργοποιώντας το σύνδεσμο, η ύπαρξη του οποίου καθιστά το έργο προσιτό στο χρήστη κατ' αίτηση του (on demand) – όπως η έννοια αυτή περιγράφεται ανωτέρω στην οικεία μείζονα σκέψη –, όταν και από όπου ο ίδιος το επιθυμεί. Τα περιεχόμενα στην ένδικη ιστοσελίδα έργα έχουν γίνει αντικείμενο εκμετάλλευσης από διαδικτυακούς χρήστες εγκατεστημένους στην Ελλάδα, οι οποίοι είναι συνδρομητές και σε κάποια από τις καθών εταιρίες. Συγκεκριμένα ο χρήστης, που επιθυμεί να προβεί σε καταφόρτωση κάποιου έργου, πληκτρολογώντας το domain name της ένδικης ιστοσελίδας σε λογισμικό πρόγραμμα περιήγησης (browser), αποκτά πρόσβαση στην ιστοσελίδα, μπορεί να πλοηγηθεί σ΄ αυτή και να επιλέξει το έργο που επιθυμεί, το οποίο σημαίνεται με συγκεκριμένο σύνδεσμο που ενεργοποιεί αυτός και ο οποίος (σύνδεσμος) ανακατευθύνει τη σύνδεση στο διακομιστή (server) όπου το έργο είναι προ αποθηκευμένο. Κατόπιν αυτού το έργο μέσω φευγαλέων αναπαραγωγών (caching) καταφορτώνεται και αποθηκεύεται ως αρχείο σε ψηφιακό μέσο αποθήκευσης (σκληρό δίσκο του ηλεκτρονικού υπολογιστή ή άλλο, ψηφιακό δίσκο, κλπ) του χρήστη του διαδικτύου – μέλους της ιστοσελίδας, ενώ χωρίς την υπηρεσία πρόσβασης που παρέχεται από τις καθών εταιρίες στους συνδρομητές τους (μέλη της ένδικης ιστοσελίδας) οι εκμεταλλευτές αυτής θα αδυνατούσαν να παράσχουν τα έργα «ανοικτά» προς κλήση στην Ελλάδα και να προβούν στις ως άνω εκτεθείσες προσβολές των δικαιωμάτων πνευματικής ιδιοκτησίας και των συγγενικών δικαιωμάτων. Οι χρήστες του διαδικτύου που είναι εγκατεστημένοι στην Ελλάδα και εισέρχονταν, στην εν λόγω ιστοσελίδα ανέρχονταν σε 20.456 άτομα ημερησίως βάσει στατιστικών στοιχείων που συγκέντρωσε η αιτούσα από σχετική ιστοσελίδα του διαδικτύου.

Με την εν λόγω απόφαση του Μονομελούς Πρωτοδικείου Αθηνών πιθανολογήθηκε περαιτέρω αφενός ότι η ζημία από τις προσβολές δικαιωμάτων πνευματικής ιδιοκτησίας και συγγενικών δι-

καιωμάτων μέσω των παράνομων ενεργειών των μελών/συνδρομητών ή εισερχομένων χρηστών του διαδικτύου στις ένδικες ιστοσελίδες ανέρχεται στο ποσό που θα πωλείτο στην ελληνική αγορά έκαστο φωνογράφημα ή μουσικό έργο ή οπτικοακουστικό έργο ή βιβλίο, το οποίο καταφορτώνεται από τις ως άνω ιστοσελίδες από τους εισερχόμενους σ' αυτές ανωτέρω χρήστες – συνδρομητές των καθών εγκατεστημένους στην Ελλάδα, καθώς και ότι οι αιτούντες προέβησαν στις αναγκαίες και κατάλληλες ενέργειες για την ανακάλυψη των εκμεταλλευτών των ένδικων ιστοσελίδων, που εδρεύουν κατά τα ανωτέρω στις Η.Π.Α. και τη Ρωσία αντίστοιχα και την παύση των ανωτέρω παράνομων προσβολών, με την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου προς τους διαχειριστές των εν λόγω ιστοτόπων, πλην όμως χωρίς κάποιο αποτέλεσμα, ακολούθως δε αμέσως μόλις αποκτήθηκε από τους ίδιους (αιτούντες) επαρκής γνώση σχετικά με τις προεκτεθείσες προσβολές των συγγενικών δικαιωμάτων, αυτοί κοινοποίησαν στις καθών, εξώδικες γνωστοποιήσεις – δηλώσεις, όπως τούτο συνομολογείται από τις τελευταίες. Με την εν λόγω απόφαση του Μονομελούς Πρωτοδικείου Αθηνών κρίθηκε αναγκαία η λήψη ασφαλιστικών μέτρων, συνιστάμενων σε προσωρινή ρύθμιση κατάστασης, κατά την έννοια του άρθρου 64Α του Ν. 2121/1993, που αφορά τη διακοπή της πρόσβασης στους χρήστες του διαδικτύου που είναι εγκατεστημένοι στην Ελλάδα, από τις καθών εταιρίες προς τις ένδικες ιστοσελίδες.

Η δικαστική απόφαση εισέρχεται και στην συγκεκριμένη τεχνική διακοπής πρόσβασης τόσο σε συγκεκριμένη διεύθυνση διαδικτύου όσο και σε συγκεκριμένο όνομα δικτυακού τόπου. Ειδικότερα, τα αιτήματα των χρηστών/πελατών του ISP διαβιβάζονται στις διατάξεις δρομολόγησης του ISP για περαιτέρω μεταβίβαση με βάση τη διεύθυνση διαδικτύου του αποδέκτη. Οι διατάξεις δρομολόγησης (δρομολογητές – routers) διαθέτουν τεχνική δυνατότητα λήψης ρητών οδηγιών σε σχέση με συγκεκριμένες διευθύνσεις και μπλοκ διευθύνσεων διαδικτύου. Συγκεκριμένα, οι εν λόγω οδηγίες καθορίζουν το είδος των αιτημάτων και των απαντήσεων σε αιτήματα («κίνηση») που επιτρέπεται ή απαγορεύεται να δέχονται οι δρομολογητές σε συγκεκριμένες λίστες διευθύνσεων που ονομάζονται «λίστες πρόσβασης» (access lists.) Οι διευθύνσεις εμφανίζονται σε μια λίστα πρόσβασης μαζί με οδηγίες για το επιτρεπτό ή ανεπίτρεπτο της κίνησης από ή προς την καθεμία διεύθυνση. Η συμπερίληψη μιας διεύθυνσης και των σχετικών με αυτή οδηγιών σε λίστα πρόσβασης γίνεται με προσθήκη λίγων (λιγότερο)ν των δέκα, συνήθως) γραμμών κώδικα σε ένα αρχείο ρυθμίσεων του δρομολογητή. Πρόσβαση στο αρχείο αυτό έχει μόνο το προσωπικό διαχείρισης του δικτύου του ISP. Οι ρυθμίσεις αυτές αναλόγως της αρχιτεκτονικής δικτύου του ISP μπορεί να πρέπει να γίνουν σε άνω του ενός δρομολογητή. Ωστόσο για δίκτυα του μεγέθους των ελληνικών ISP ο αριθμός των δρομολογητών που εξασφαλίζουν πρόσβαση των χρηστών του κάθε ISP στο ευρύτερο διαδίκτυο είναι εν γένει μικρός. Με την προσθήκη της διεύθυνσης που θέλουμε να διακοπεί η πρόσβαση και της κατάλληλης οδηγίας (απαγόρευση πάσης εξερχόμενης από το δίκτυο του ISP κίνησης προς τη συγκεκριμένη διεύθυνση, ήτοι διακοπή κάθε αιτήματος χρήστη στην «πηγή», αλλά δυνητικά απαγόρευση και πάσης εισερχόμενης προς το δίκτυο του ISP κίνησης προερχομένης από τη συγκεκριμένη διεύθυνση, επικουρικά) επιτυγχάνεται η διακοπή πρόσβασης με βάση τη διεύθυνση διαδικτύου του δικτυακού τόπου των χρηστών του ISP. Εναλλακτική μέθοδος επίτευξης του ίδιου αποτελέσματος αποτελεί η με κατάλληλο τρόπο ενημέρωση του/των δρομολογητή/ων του ISP για την ανακατεύθυνση (αντί για την απόρριψη ως ανωτέρω) των αιτημάτων με προορισμό την εν λόγω διεύθυνση. Ειδικότερα, ο δρομολογητής περιλαμβάνει «πίνακα διαδρομών» όπου με βάση την διεύθυνση αποστολής ενός αιτήματος, επιλέγεται η αποστολή του προς επόμενη, «εγγύτερη» προς τον τελικό προορισμό διάταξη δρομολόγησης. Με χρή-

ση κατάλληλων οδηγιών που μπορούν να εισαχθούν στο δρομολογητή του ISP είναι δυνατό να ενημερωθεί αυτός να αποστέλλει αιτήματα με διεύθυνση αποστολής την υπό διακοπή πρόσβασης προς συγκεκριμένη, επιλεγμένη από τον ISP, ιδιωτική διεύθυνση, εμποδίζοντας έτσι την παράδοση τους. Η ενημέρωση του δρομολογητή για μια τέτοια διαδρομή γίνεται με προσθήκη λίγων γραμμών κώδικα από το προσωπικό διαχείρισης του δικτύου του ISP. Η ενημέρωση αυτή, αναλόγως του ακριβούς τρόπου υλοποίησης της και της αρχιτεκτονικής δικτύου του ISP, μπορεί να πρέπει να γίνει σε άνω του ενός δρομολογητή. Ωστόσο για δίκτυα του μεγέθους των ελληνικών ISP ο αριθμός των δρομολογητών που εξασφαλίζουν πρόσβαση των χρηστών του κάθε ISP στο ευρύτερο διαδίκτυο είναι εν γένει μικρός.

Σχετικά με την Τεχνική διακοπής πρόσβασης σε συγκεκριμένο όνομα δικτυακού τόπου, η βασική τεχνική αφορά στην παρεμβολή στη διαδικασία στην κατανεμημένη Υπηρεσία Ονομάτων Δικτυακών Τόπων (Domain Name Service–DNS) που χρησιμοποιείται από τον υπολογιστή του χρήστη προκειμένου να ενημερωθεί για τη διεύθυνση (ή τις διευθύνσεις) διαδικτύου που αντιστοιχεί(ουν) στο συγκεκριμένο όνομα δικτυακού πόρου που αναφέρεται στο αίτημα του χρήστη. Ειδικότερα, το αίτημα γίνεται από τις διατάξεις του υπολογιστή του χρήστη προς συγκεκριμένο εξυπηρετητή Ονομάτων Δικτυακών Τόπων (Domain Name Server) που διαθέτει ο πάροχος υπηρεσιών διαδικτύου (ISP) του χρήστη. Ο κάθε τέτοιος εξυπηρετητής διαθέτει λίστα αντιστοιχίσεων ονομάτων δικτυακών τόπων με διευθύνσεις διαδικτύου, ενώ για ονόματα που δεν «γνωρίζει» μπορεί να απευθύνει ερώτημα σε άλλους παρόμοιους εξυπηρετητές. Η τεχνική διακοπής πρόσβασης συνίσταται στην τοποθέτηση στον (στους) εξυπηρετητή(ες) Ονομάτων Δικτυακών Τόπων που διαθέτει και διαχειρίζεται ο ISP της αντιστοίχισης από το όνομα δικτυακού τόπου που θέλουμε να διακόψουμε την πρόσβαση (π.χ. www....) προς μια από τον ISP επιλεγμένη διεύθυνση (όχι την πραγματική για τον εν λόγω τόπο) όπου και θα μεταφέρεται κάθε αίτημα προς το αποκλεισμένο όνομα δικτυακού τόπου. Στην εν λόγω επιλεγμένη διεύθυνση είναι δυνατόν να αναρτηθεί ενημερωτικό μήνυμα για τους λόγους αποκλεισμού πρόσβασης στο ζητούμενο δικτυακό τόπο. Με τον τρόπο αυτό διακόπτεται η πρόσβαση προς τον δικτυακό τόπο μέσω αιτημάτων που ζητούν πρόσβαση μέσω ονόματος. Σε συνδυασμό με τις μεθόδους που αναφέρονται ανωτέρω, επιτυγχάνεται η συνολική διακοπή πρόσβασης των αιτημάτων σε κάποιο δικτυακό τόπο με χρήση διατάξεων που βρίσκονται υπό τον πλήρη έλεγχο του παρόχου υπηρεσιών διαδικτύου (ISP).

Σύμφωνα με τα συμπεράσματα της δικαστικής απόφασης, οι ως άνω περιγραφόμενες τεχνικές επιτρέπουν τη διακοπή πρόσβασης χρηστών σε συγκεκριμένες διευθύνσεις διαδικτύου ή/και σε δικτυακούς τόπους με συγκεκριμένα ονόματα. Οι τεχνικές της πρώτης ενότητας αποτελούν τις αποτελεσματικότερες για τη διακοπή πρόσβασης. Σε συνδυασμό με την τεχνική της δεύτερης ενότητας, εξασφαλίζουν στο μέγιστο βαθμό τη διακοπή πρόσβασης στο δικτυακό τόπο στην πλειονότητα των δυνητικών χρηστών. Για την εφαρμογή των τεχνικών αυτών δεν απαιτείται καθόλου νέο υλικό/νέο λογισμικό και εν γένει νέος εξοπλισμός, καθώς η λειτουργικότητα που χρησιμοποιείται ενυπάρχει στον εξοπλισμό που ήδη χρησιμοποιεί ο ISP (δρομολογητές/routers και λογισμικό για τη διαχείριση της Υπηρεσίας Ονομάτων Δικτύου – Domain Name Service). Η εφαρμογή των τεχνικών μέσω της υλοποίησης των απαραίτητων εντολών προς τους δρομολογητές και τους εξυπηρετητές Ονομάτων Δικτύου (Domain Name Servers) απαιτεί πολύ μικρή προσπάθεια: Ειδικότερα απαιτείται η ενσωμάτωση λίγων (εν γένει, και αναλόγως του μοντέλου του υπάρχοντος εξοπλισμού, λιγότερων των 50) γραμμών κώδικα υπό μορφή οδηγιών. Η συγγραφή, έλεγχος και εγκατάσταση των εν λόγω οδηγιών στις σχετικές διατάξεις μπορεί να πραγματοποιηθεί εύ-

κολα από ένα εξειδικευμένο άτομο και ειδικότερα από το διαχειριστή των εν λόγω διατάξεων, εντός σύντομου χρονικού διαστήματος. Η εγκατάσταση συγκεκριμένα γίνεται εντός λίγων λεπτών. Η χρήση των ανωτέρω περιγραφόμενων τεχνικών για τη διακοπή πρόσβασης σε μια διεύθυνση διαδικτύου δεν προβλέπεται να έχει αρνητικές επιπτώσεις στην επίδοση των υπηρεσιών πρόσβασης στο διαδίκτυο (π.χ. ταχύτητα πρόσβασης, καθυστέρηση απόκρισης, διαθέσιμο εύρος ζώνης). Ειδικότερα, οι υπάρχουσες διατάξεις ενσωματώνουν τα μέσα για την υλοποίηση των περιγραφόμενων μεθόδων διακοπής με τρόπο συμβατό με την πραγματοποίηση των κύριων λειτουργιών τους, που είναι η δρομολόγηση και η αντιστοίχηση ονομάτων δικτυακών τόπων με διευθύνσεις. Έτσι, η ενσωμάτωση και υπό των διατάξεων εκτέλεση των οδηγιών διακοπής, όπως περιγράφονται ανωτέρω δεν καθυστερούν ή άλλως αρνητικά επηρεάζουν τις κύριες λειτουργίες των διατάξεων. Η χρήση όλων των αναφερόμενων τεχνικών οδηγεί σε παθητικό έλεγχο της κίνησης στο διαδίκτυο: οι εν λόγω διατάξεις εφαρμόζουν με τρόπο ομοιόμορφο τις οδηγίες διακοπής πρόσβασης επί όλων των αιτημάτων σύνδεσης στο διαδίκτυο που διακινούνται μέσω του εξοπλισμού των ISP. Η εφαρμογή αυτή δεν απαιτεί από τα συστήματα δρομολόγησης καμιά περαιτέρω γνώση των χαρακτηριστικών των αιτημάτων πέραν της γνώσης που απαιτείται για καθαυτή τη λειτουργία της δρομολόγησης. Ως εκ τούτου, κανείς δεν αποκτά οποιαδήποτε πρόσθετη γνώση για τους αποστολείς, τους αποδέκτες ή το περιεχόμενο των ηλεκτρονικών επικοινωνιών που διακινούνται μέσω του ISP, ενώ δεν ασκείται καμιά επέμβαση επί οποιασδήποτε ενέργειας των χρηστών διαδικτύου–πελατών του ISP πέραν της συγκεκριμένης διακοπής πρόσβασης στο/στους συγκεκριμένο/ους δικτυακό τόπο/ους, ούτε οποιαδήποτε μεταβολή ή τροποποίηση των μεταδιδόμενων πληροφοριών.

Τα προτεινόμενα τεχνολογικά μέσα είναι σύμφωνα με τη δικαστική απόφαση αποτελεσματικά και ευκόλως υλοποιήσιμα, αμελητέας όχλησης και χωρίς επιπτώσεις στα απολαμβανόμενα από τους χρήστες αγαθά και υπηρεσίες στο διαδίκτυο (εκτός των πολύ περιορισμένων δυνητικών τοιαύτων που αναφέρονται ακριβώς ανωτέρω), καθώς και χωρίς αρνητικές επιπτώσεις στη λειτουργία του διαδικτύου γενικώς και του εξοπλισμού των ISP ειδικότερα». Από τα παραπάνω πιθανολογηθέντα κρίνεται ότι οι διαλαμβανόμενες στην ως άνω τεχνική έκθεση, τεχνολογικές μέθοδοι για τη διακοπή πρόσβασης των συνδρομητών των καθών, χρηστών του διαδικτύου, προς τις ένδικες ιστοσελίδες, αποτελούν κατάλληλες, αναλογικές και πρόσφορες μεθόδους, όπως οι έννοιες αυτές ερμηνεύονται από το Δικαστήριο σύμφωνα με τα ανωτέρω στην οικεία μείζονα σκέψη, για το συγκεκριμένο σκοπό, καθώς όσον αφορά: α) το στοιχείο της καταλληλότητας, η εγκατάσταση των συγκεκριμένων τεχνικών διακοπής πρόσβασης γίνεται εντός λίγων λεπτών, η δε χρήση των ανωτέρω περιγραφόμενων τεχνικών για τη διακοπή πρόσβασης σε μια διεύθυνση διαδικτύου δεν προβλέπεται να έχει αρνητικές επιπτώσεις στην επίδοση των υπηρεσιών των καθών για πρόσβαση στο διαδίκτυο (π.χ. ταχύτητα πρόσβασης, καθυστέρηση απόκρισης, διαθέσιμο εύρος ζώνης) ενώ το κόστος είναι αμελητέο, β) όσον αφορά το στοιχείο της με στενή έννοια αναλογικότητας, είναι καταρχήν αναγκαίες σύμφωνα με τα ανωτέρω πιθανολογηθέντα, ενώ τελούν και σε εύλογη σχέση με τον επιδιωκόμενο σκοπό, διότι επιτρέπουν τη διακοπή πρόσβασης χρηστών – συνδρομητών των καθών εγκατεστημένων στην Ελλάδα σε συγκεκριμένες διευθύνσεις διαδικτύου ή/και σε δικτυακούς τόπους με συγκεκριμένα ονόματα και γ) όσον αφορά το στοιχείο της προσφορότητας, εμποδίζεται η πρόσβαση σε όλο το περιεχόμενο και τις υπηρεσίες του δικτυακού τόπου με αυτή τη διεύθυνση για την οποία ζητείται η διακοπή πρόσβασης, ενώ η τεχνική διαδικασία της παράκαμψης των συγκεκριμένων τεχνικών διακοπής πρόσβασης είναι άγνωστη στο μέσο χρήστη δι-

αδικτύου και γενικότερα άγνωστη στη μεγάλη πλειονότητα των συνδρομητών των καθών, που είναι οι δυνητικοί επισκέπτες των ιστοτόπων, στους οποίους θα διακοπεί η πρόσβαση.

Με την ανωτέρω δικαστική απόφαση διατάσσεται προσωρινά, ως τεχνολογικό μέτρο, προκειμένου να καταστεί αδύνατη στους συνδρομητές των καθών, οι οποίες είναι εταιρίες παροχής υπηρεσιών πρόσβασης στο διαδίκτυο, η ψηφιακή καταφόρτωση στους υπολογιστές των συνδρομητών τους, των έργων επί των οποίων υπάρχουν δικαιώματα πνευματικής ιδιοκτησίας και συγγενικά δικαιώματα δικαιούχων, που εκπροσωπούνται στην Ελλάδα από τους αιτούντες, τα οποία περιέχονται στις ιστοσελίδες με διευθύνσεις στο διαδίκτυο (domain names) www.....com και www..... και διευθύνσεις IP (IP addresses) IP: ..... και IP: ....., αντίστοιχα, την επιβολή της περιγραφόμενης «Βασικής Τεχνικής Διακοπής Πρόσβασης σε συγκεκριμένη διεύθυνση του διαδικτύου», που αφορά τις ως άνω ιστοσελίδες με τις παραπάνω διευθύνσεις, μέσω της εγκατάστασης από το προσωπικό διαχείρισης του δικτύου των καθών, των σχετικών ρητών οδηγιών στους δρομολογητές – routers του εν λόγω δικτύου. Απειλεί σε βάρος έκαστης των καθών οι αιτήσεις, χρηματική ποινή πέντε χιλιάδων (5.000) ευρώ για κάθε παράβαση του διατακτικού της παρούσας.

Μπορεί οι χρήστες και οι μπλόγκερ ανά τον κόσμο να μη SOPAίνουν, τι γίνεται, με τα sites διαμοιρασμού αρχείων και torrents που επιτρέπουν την ανταλλαγή αρχείων μεταξύ χρηστών (peer – to peer); Την επόμενη ακριβώς ημέρα μετά το απίστευτο blackout στο Internet, το FBI με εντολή του υπουργείου Δικαιοσύνης έθεσε τέλος στη λειτουργία του Megaupload, ενός από τα μεγαλύτερα sites διαμοιρασμού αρχείων, και αυτό δεν ήταν καθόλου τυχαίο. Τις τελευταίες εβδομάδες ο πανικός έχει επεκταθεί και σε άλλα sites που φιλοξενούν αρχεία (μουσικά mp3 ή ταινίες) ή απλώς κάνουν απευθείας streaming των ταινιών, Ήδη το FileSonic και το FileServe σταμάτησαν να παρέχουν υπηρεσίες, το upload σταμάτησε να δίνει πρόσβαση στους χρήστες που βρίσκονται στις ΗΠΑ, ενώ το MediaFire διαγράφει όλα τα αρχεία που φιλοξενεί, χωρίς καμία προειδοποίηση στους χρήστες, κι ας έχουν πληρώσει ετήσια συνδρομή άνω των 100 δολαρίων.

Από την πλευρά τους οι χρήστες δεν είναι και τόσο ανήσυχοι, αφού, όπως υποστηρίζουν, sites με παρόμοιες υπηρεσίες μοιάζουν σαν τη Λερναία Ύδρα: κόβεις το ένα, πετάγονται χιλιάδες.

Θεμιστοκλής Ι. Σοφός
Δ.Ν. Δικηγόρος παρ' Αρείω Πάγω

«Ερμηνευτικές προσεγγίσεις ως προς την έκταση του υπό του άρθρου 19 του Συντάγματος θεσπιζομένου απορρήτου και η σχέση της Δικαιοσύνης και των οργάνων της προς την Α.Δ.Α.Ε. κατά την εφαρμογή του»

κ. **Γεώργιος Σανιδάς**, Επίτιμος Εισαγγελέας Αρείου Πάγου

Κυρίες και Κύριοι

Δύο είναι τα ζητήματα με τα οποία θα ασχοληθεί ο ομιλών.

Το πρώτο είναι εάν το υπό του άρθρου 19 του Συντάγματος θεσπιζόμενο απόρρητο της επικοινωνίας καλύπτει:

α) μόνο το περιεχόμενο της επικοινωνίας ή και τα εξωτερικά στοιχεία αυτής (αριθμό κλήσεως κ.λ.π.) και

β) και την επικοινωνία μέσω του διαδικτύου.

Το δεύτερο είναι ποία η σχέση της Δικαιοσύνης με την ΑΔΑΕ.

Α. Ως προς το πρώτο ζήτημα:

Θα επισημάνω ευθύς εξ αρχής ότι ως προς το πρώτο ζήτημα έχουν διατυπωθεί εκ διαμέτρου αντίθετες θέσεις από την Εισαγγελία του Α.Π. και την ΑΔΑΕ.

Αα. Η Εισαγγελία του Α.Π. με τρεις γνωμοδοτήσεις έχει δεχθεί ότι το απόρρητο του άρθρου 19 του Συντάγματος δεν καταλαμβάνει τα εξωτερικά στοιχεία της επικοινωνίας και την επικοινωνία μέσω διαδικτύου για τους πιο κάτω συνοπτικά λόγους:

Ι. Ως προς τα εξωτερικά στοιχεία:

Από το γράμμα και το σκοπό της διατάξεως του άρθρου 19 παρ. 1 του Συντάγματος προκύπτει ότι το απόρρητο αφορά στο περιεχόμενο της επικοινωνίας δηλ. στον πυρήνα αυτής και όχι στα εξωτερικά στοιχεία της. Εξ άλλου ούτε στον εκτελεστικό Ν. 2225/1994 ούτε στο Ν. 3115/2003 με τον οποίο συνεστήθη η ΑΔΑΕ υπάρχει διάταξη από την οποία να προκύπτει ότι το απόρρητο του άρθρου 19 καλύπτει και τα εξωτερικά στοιχεία της επικοινωνίας. Αντιθέτως μάλιστα από τη διάταξη του άρθρου 5 παρ. 1, 2 και 6 του Ν. 2225/1994 η οποία προβλέπει ότι η διάταξη που επιβάλλει την άρση του απορρήτου θα πρέπει να ορίζει και τη χρονική διάρκεια της άρσης, που μάλιστα κατ΄ αρχάς δεν μπορεί να υπερβαίνει τους δύο μήνες, συνάγεται αβιάστως ότι η άρση του απορρήτου σκοπό έχει να αποκαλυφθεί το περιεχόμενο της επικοινωνίας και όχι τα εξωτερικά στοιχεία, για τη λήψη των οποίων δεν είναι αναγκαία η χρονική διάρκεια της άρσης.-

Την θέση αυτή δέχεται το σύνολο της επιστήμης (πλην του Δαγτόγλου) με πρώτο τον αείμνηστο και μεγάλο καθηγητή του Συνταγματικού Δικαίου Αριστόβουλο Μάνεση (Ατομικές Ελευθερίες σελ. 167). Την δέχθηκε ο ΄Αρειος Πάγος με την 570/2006 απόφασή του, αλλά η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με τις υπ΄ αριθμ. 79/2002 και 37/2004 αποφάσεις της. Χαρακτηριστικά στην υπ΄ αριθμ. 37/2004 απόφασή της με την οποία αντιμετώπισε θετικά

θέμα γνωστοποιήσεως στοιχείων καλούσας γραμμής διαλαμβάνει: «Είναι αυτονόητο ότι τα ανωτέρω δεν ισχύουν ως προς το εσωτερικό περιεχόμενο της τηλεφωνικής συνομιλίας για την οποία εφαρμογή έχει το άρθρο 19 του Συντάγματος και ο Ν. 2225/1994».

Παγίως εξάλλου η πιο πάνω Αρχή δίδει εντολές στους παρόχους επικοινωνιών να χορηγούν τα εξωτερικά στοιχεία της επικοινωνίας, όταν πρόκειται να γίνει χρήση ενώπιον Δικαστηρίων και ιδίως προκειμένου να αποκαλυφθεί η τέλεση εγκλήματος.

Τούτο διότι στην περίπτωση κατά την οποία με τη χρήση ενός μέσου επικοινωνίας π.χ. του τηλεφώνου τελούνται υπό του ενός εκ των χρηστών εγκλήματα π.χ. υβριστικό, απειλητικό, απατηλό, εκβιαστικό κ.λ.π. τηλεφώνημα, δεν δύναται να υπάρξει προστασία ούτε με την επίκληση του άρθρου 19 του Συντάγματος, αφού δεν υπάρχει επικοινωνία σε οικειότητα, ώστε να υπάρχει βούληση των επικοινωνούντων να παραμείνει η επικοινωνία μυστική, ούτε με την επίκληση του άρθρου 9Α του Συντάγματος και του Ν. 2472/1997 καθ΄ όσον η εγκληματική συμπεριφορά του ατόμου ούτε εμπίπτει ούτε είναι δυνατόν να εμπίπτει στην έννοια των προσωπικών δεδομένων και ούτε καλύπτεται από αυτήν. Τόσο η διάταξη του άρθρου 9Α του Συντάγματος όσο και πολύ περισσότερο οι διατάξεις του Ν. 2472/1997 δεν εκτείνονται στο πεδίο της ποινικής διαδικασίας και στο πλαίσιο απονομής της ποινικής δικαιοσύνης, όπως άλλως τε αυτό προκύπτει και από τη διάταξη του άρθρου 7Α παρ. 1 περιπτ. στ του άνω νόμου που προστέθηκε με το άρθρο 10 του Ν. 3090/2002.

Μέλη της ανωτέρω Αρχής ήταν, μεταξύ των άλλων, ο Κ. Δαφέρμος επίτιμος αντιπρόεδρος του Α.Π. και ο Ν. Αλιβιζάτος καθηγητής του Συνταγματικού Δικαίου. Η μη αποδοχή της ανωτέρω θέσεως οδηγεί: α) Στην παραβίαση της διατάξεως του άρθρου 20 του Συντάγματος, αφού οι πολίτες οι οποίοι δέχονται π.χ. υβριστικά, απειλητικά ή εκβιαστικά τηλεφωνήματα ή έχουν εξαπατηθεί μέσω τηλεφωνημάτων, θα εστερούντο του δικαιώματος παροχής εννόμου προστασίας από τα δικαστήρια, αφού δεν θα ήταν εφικτή η αποκάλυψη των δραστών και β) στο ανέφικτο της διώξεως εγκληματιών, που έχουν τελέσει εγκληματικές πράξεις, άλλες εκτός από εκείνες για τις οποίες είναι επιτρεπτή η άρση του απορρήτου σύμφωνα με το Ν. 2225/1994, εντεύθεν στη συγκάλυψη και υπόθαλψη εγκληματικών πράξεων και εγκληματιών, οι οποίοι θα ήταν δυνατόν να αποκαλυφθούν ευχερώς μέσω των εξωτερικών στοιχείων της επικοινωνίας και στη στέρηση του δικαιώματος παροχής εννόμου προστασίας για τους παθόντες και εν τέλει στην μη εφαρμογή της αρχής του κράτους δικαίου.

ΙΙ. Ως προς την επικοινωνία μέσω διαδικτύου:

΄Οπως προκύπτει από τη διατύπωση του άρθρου 19 του Συντάγματος το απόρρητο αφορά σε κάθε μέσο επικοινωνίας, υπαρκτό ή μελλοντικό, εφ' όσον το μέσον αυτό είναι από τη φύση του κατάλληλο για τη διεξαγωγή της επικοινωνίας μέσα σε οικειότητα και όχι σε δημοσιότητα. Εκ τούτου παρέπεται ότι στην επικοινωνία μέσω Internet δεν υπάρχει απόρρητο, αφού αυτή είναι εξ ορισμού επικοινωνία σε δημοσιότητα. Το διαδίκτυο είναι εξ ορισμού χώρος ελεύθερης έκφρασης και η δημιουργία ή άλλως η κατασκευή ιστοσελίδας σ΄ αυτό είναι ελεύθερη σε οποιονδήποτε.

Τούτο προκύπτει και από τη διάταξη του άρθρου 5Α παρ. 2 του Συντάγματος με την οποία θεσπίζεται το ατομικό δικαίωμα συμμετοχής στην κοινωνία της πληροφορίας.

Είναι αυτονόητο ότι μπορεί να υπάρξει απόρρητο και στην επικοινωνία μέσω Internet, εάν έχει χρησιμοποιηθεί ειδική διαδικασία διαφύλαξης του απόρρητου. Τούτο ισχύει π.χ. όταν μέσω της ιστοσελίδας έχει δημιουργήσει κάποιος ένα απόρρητο προφίλ στο οποίο θα έχει το δι-

καίωμα πρόσβασης και κάποιο ή κάποια πρόσωπα που έχει επιλέξει και έχουν τα απαραίτητα «κλειδιά».

Πέραν των ανωτέρω επιβάλλεται να σημειωθεί ότι ούτε στο Ν. 2225/1994 ούτε στο Ν. 3115/2003 υφίσταται διάταξη ορίζουσα ότι η μέσω διαδικτύου επικοινωνία καλύπτεται από το απόρρητο του άρθρου 19 του Συντάγματος.

Την πιο πάνω θέση δέχονται οι καθηγητές Χρυσόγονος του Συνταγματικού Δικαίου και Χαραλαμπάκης του Ποινικού Δικαίου. Ο τελευταίος σε άρθρο του με τίτλο «Μ.Μ.Ε. και προσβολή της προσωπικότητας–Ποινικές Διαστάσεις» επιδοκιμάζοντας τις τρεις γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου σημειώνει χαρακτηριστικά: «...Η σειρά αυτή των εισαγγελικών γνωμοδοτήσεων θέτει κατά την άποψή μου αποφασιστικό φραγμό σ΄ ένα φαινόμενο που γνώρισε τελευταία ιδιαίτερη όξυνση και το οποίο συντελούσε, όχι μόνον στην ατιμώρητη βάναυση προσβολή της προσωπικότητας μη εμπλεκομένων πολιτών αλλά και στην ειρωνική αμφισβήτηση της αποτελεσματικότητας του κράτους δικαίου».

Είναι λοιπόν προφανές ότι αντίθετη εκδοχή θα οδηγεί στην συγκάλυψη εγκλημάτων και εγκλημάτων τα οποία τελούνται μέσω του διαδικτύου και εντεύθεν αφ΄ ενός σε παραβίαση του άρθρου 20 του Συντάγματος και αφ΄ ετέρου στη μη εφαρμογή της αρχής του κράτους δικαίου».

Αβ. Ας δούμε τώρα τα ερείσματα των αντιθέτων θέσεων της ΑΔΑΕ.

Η ΑΔΑΕ επικαλείται:

Ι. Την υπ΄ αριθμ. 1/3-2-2005 γνωμοδότησή της στην οποία, εν τέλει διαλαμβάνει ότι: 1) στην προστατευτική σφαίρα του απορρήτου εμπίπτουν και τα εξωτερικά στοιχεία της επικοινωνίας, 2) δεν είναι παραδεκτό σε περιπτώσεις που γίνεται έρευνα για τη διακρίβωση κακουργημάτων που αναφέρονται στο άρθρο 4 του Ν. 2225/1994 οι αρμόδιες δικαστικές ή προανακριτικές αρχές που ενεργούν κατ΄ άρθρο 243 Κ.Ποιν.Δ. να ζητούν από τους τηλεπικοινωνιακούς φορείς τη χορήγηση εξωτερικών στοιχείων επικοινωνίας των συνδρομητών τους, χωρίς να τηρείται η προβλεπόμενη στο Ν. 2225/1994 διαδικασία και 3) στις περιπτώσεις αξιοποίνων πράξεων που δεν αναφέρονται στο Ν. 2225/1994 ή το άρθρο 253 Α του Κ.Ποιν.Δ. δεν δικαιολογείται η απαίτηση των αρμοδίων αρχών να χορηγούνται από τους φορείς εξωτερικά στοιχεία επικοινωνίας των συνδρομητών τους.

Η γνωμοδότηση αυτή είναι ανίσχυρη αφού δεν προβλέπεται από κάποια διάταξη του Ν. 3115/2003 η δυνατότητα εκδόσεως γνωμοδοτήσεως από την ΑΔΑΕ με το πιο πάνω περιεχόμενο, θα έλεγα δε και γενικότερα επί νομικών ζητημάτων. Ειδικότερα με το άρθρο 6 παρ. 1 περ. 1 του Ν. 3115/2003, στο οποίο στηρίζεται η έκδοσή της ορίζεται ότι η ΑΔΑΕ «γνωμοδοτεί και απευθύνει συστάσεις και υποδείξεις για τη λήψη μέτρων διασφάλισης του απορρήτου των επικοινωνιών καθώς και για τη διαδικασία άρσης» άρα για τεχνικά ζητήματα.

Είναι λοιπόν πρόδηλο ότι η ανωτέρω διάταξη του Ν. 3115/2003 δεν νομιμοποιεί την ΑΔΑΕ να γνωμοδοτήσει για την έκταση του υπό του άρθρου 19 του Συντάγματος θεσπιζόμενου απορρήτου και για το τί πρέπει να κάνουν ή να μην κάνουν οι δικαστικές αρχές αλλά και γενικότερα για νομικά ζητήματα. Τούτο άλλως τε είναι εύλογο αφού τα εξ από τα επτά μέλη της ΑΔΑΕ είναι τεχνικοί.

Μία πρόσθετη παρατήρηση.

Όπως προκύπτει από τα διαλαμβανόμενα στην αρχή της γνωμοδοτήσεως, την έκδοσή της προκάλεσαν πάροχοι επικοινωνιών. Γιατί άραγε και τί συμφέρον είχαν;

Μήπως τελικώς οι πάροχοι είναι εκείνοι που αντιδρούν στα αιτήματα των δικαστικών αρχών;

II. Το εκδοθέν ένα μήνα μετά υπ΄αριθμ. 47/2005 Π.Δ. με τίτλο «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του», στο οποίο, παρά τον τίτλο του, διαλαμβάνεται, μεταξύ των άλλων, ότι στο απόρρητο του άρθρου 19 του Συντάγματος εμπίπτουν τόσο οι επικοινωνίες μέσω του διαδικτύου όσο και τα εξωτερικά στοιχεία της επικοινωνίας. Το πιο πάνω Διάταγμα, το οποίο συντάχθηκε μετά από εισήγηση της ΑΔΑΕ, ως προς τις ρηθείσες ρυθμίσεις του είναι ανίσχυρο, ως εκδοθέν καθ΄υπέρβαση νομοθετικής εξουσιοδοτήσεως, αφού ούτε από τις διατάξεις του Ν. 2225/1994, ούτε από τις διατάξεις του Ν. 3115/2003, παρέχεται εξουσιοδότηση να προσδιορισθεί με Π.Δ. η έκταση του απορρήτου της επικοινωνίας και τί αυτό καλύπτει, ενώ εξ άλλου με τις διατάξεις των ανωτέρω νόμων δεν ορίζεται ότι το απόρρητο της επικοινωνίας καλύπτει τα εξωτερικά στοιχεία αυτής και την επικοινωνία μέσω Internet. Ούτε τέλος καθιστά σύμφωνο προς το Σύνταγμα το ανωτέρω Π.Δ. το γεγονός ότι έτυχε επεξεργασίας από το Στ.Ε.

Ειδικότερα τούτο προκύπτει αβιάστως από το περιεχόμενο του άρθρου 9 του Ν. 3115/2003, βάσει του οποίου εκδόθηκε το ως άνω Π.Δ. και το οποίο έχει ως ακολούθως:

«Με προεδρικά διατάγματα προσυπογραφόμενα..... και γνώμη της ΑΔΑΕ, ρυθμίζονται οι διαδικασίες καθώς και οι τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών, όταν αυτή διατάσσεται από τις αρμόδιες δικαστικές και Εισαγγελικές αρχές και ειδικότερα ο καθορισμός των στοιχείων στα οποία επιτρέπεται η πρόσβαση, η τεχνική μέθοδος πρόσβασης στα στοιχεία και το είδος του χρησιμοποιουμένου τεχνικού εξοπλισμού, οι υποχρεώσεις των παρόχων υπηρεσιών επικοινωνίας, η τεχνική μέθοδος λήψης αναπαραγωγής και μεταβίβασης των στοιχείων, όπως και οι εγγυήσεις για τη χρήση και καταστροφή τους, η διασφάλιση του απορρήτου των επικοινωνιών από άποψη τεχνική και από άποψη αρμοδίων εξουσιοδοτημένων προσώπων, ο καταμερισμός του κόστους, αφ΄ενός του εξοπλισμού και αφ΄ετέρου της διαδικασίας μεταξύ των παρόχων υπηρεσιών επικοινωνίας και των αρμοδίων αρχών καθώς και κάθε άλλο θέμα τεχνικού ή λεπτομερειακού χαρακτήρα, το οποίο άπτεται της εγγύησης και διασφάλισης της άρσης του απορρήτου των επικοινωνιών».

III. Το άρθρο 4 του Ν. 3471/2006 με τον οποίο ενσωματώθηκε η οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα ηλεκτρονικών επικοινωνιών. ΄Ομως η πιο πάνω διάταξη, (καθώς και η παραπέμπουσα σε αυτήν διάταξη του άρθρου 5 παρ. 2 του Ν. 3783/2009, αλλά και οι ομοίου περιεχομένου διατάξεις του Ν. 3917/2011) καθ΄ό μέρος φαίνεται να εντάσσει στο απόρρητο των επικοινωνιών και τα δεδομένα κίνησης, στα οποία περιλαμβάνονται και τα εξωτερικά στοιχεία της επικοινωνίας, είναι ανίσχυρη ως ερχόμενη σε αντίθεση με το άρθρο 19 του Συντάγματος, στο οποίο μάλιστα η ίδια στη συνέχεια παραπέμπει, ορίζοντας ότι «η άρση του απορρήτου είναι επιτρεπτή μόνο υπό τις προϋποθέσεις και τις διαδικασίες που προβλέπονται από το άρθρο 19 του Συντάγματος». ΄Ερχεται δε σε αντίθεση με το άρθρο 19 του Συντάγματος διότι με το τελευταίο δεν προστατεύονται τα εξωτερικά στοιχεία της επικοινωνίας, αλλά μόνον το περιεχόμενο της επικοινωνίας. Είναι εξ άλλου περιττό να σημειωθεί, ότι η διάταξη του άρθρου 19 του Συντάγματος υπερισχύει του άρθρου 4 του έχοντος απλώς αυξημένη τυπική ισχύ Ν. 3741/2006 με τον οποίο ενσωματώθηκε η οδηγία 2002/58/ΕΚ.

Ανεξαρτήτως όμως και πέραν τούτων από τη διάταξη του άρθρου 8 παρ. 7 του ίδιου νόμου 3471/2006 προκύπτει ακριβώς το αντίθετο και δη ότι τα εξωτερικά στοιχεία της επικοινωνίας δεν εμπίπτουν στο απόρρητο του άρθρου 19. Ειδικότερα με τη διάταξη αυτή παρέ-

χεται το δικαίωμα σε ιδιώτη που δέχεται κακόβουλες ή ενοχλητικές κλήσεις από μη καταγραφόμενο συνδρομητή, να ζητήσει από τον φορέα παροχής δημοσίου δικτύου επικοινωνιών ή διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών, την εξουδετέρωση της δυνατότητας μη αναγραφής της καλούσας γραμμής και στη συνέχεια την ανακοίνωση σ΄ αυτόν της ταυτότητας του καλούντος.

Είναι λοιπόν προφανές ότι το περιεχόμενο της διάταξης αυτής επιβεβαιώνει ότι τα εξωτερικά στοιχεία της επικοινωνίας δεν καλύπτονται από το θεσπιζόμενο απόρρητο του άρθρου 19. Εάν εκαλύπτοντο δεν θα ήταν δυνατή η αποκάλυψη των στοιχείων της καλούσας γραμμής εκτός της υπό του Ν. 2225/1994 διαδικασίας. Ούτε όμως και με τη διαδικασία του Ν. 2225/1994 θα ήταν εφικτή η αποκάλυψη, αφού οι κακόβουλες ή ενοχλητικές κλήσεις δεν θεμελιώνουν κάποιο από τα αδικήματα του Ν. 2225/1994 για τα οποία είναι επιτρεπτή η άρση του απορρήτου. Για να είναι όμως δυνατή, και μάλιστα μετά εξουδετέρωση της δυνατότητας μη αναγραφής της καλούσας γραμμής, η αποκάλυψη της ταυτότητας του καλούντος, ο οποίος προβαίνει σε κακόβουλες και ενοχλητικές κλήσεις και η παράδοση μάλιστα των στοιχείων του σε αιτησάμενο ιδιώτη σημαίνει αναγκαίως ότι τα εξωτερικά στοιχεία της επικοινωνίας δεν προστατεύονται από το άρθρο 19 του Συντάγματος. Ούτε θα μπορούσε να γίνει δεκτό ότι επιτρέπεται μόνο στην πιο πάνω περίπτωση η αποκάλυψη και παράδοση των εξωτερικών στοιχείων της επικοινωνίας, όχι όμως και σε άλλες περιπτώσεις. Τα εξωτερικά στοιχεία ή προστατεύονται από το άρθρο 19 του Συντάγματος και απαγορεύεται η αποκάλυψή τους σε κάθε περίπτωση χωρίς την τήρηση της διαδικασίας του Ν. 2225/1994 (και συνεπώς διάταξη η οποία επιτρέπει τούτο σε κάποιες περιπτώσεις είναι αντισυνταγματική) ή δεν προστατεύονται οπότε είναι ανακοινώσιμα, προεχόντως στις δικαστικές αρχές, χωρίς να τηρείται η διαδικασία του Ν. 2225/1994. Στην τελευταία αυτή περίπτωση προστατεύονται απλώς ως προσωπικά δεδομένα. Εκτός εάν φθάσουμε στο παράλογο να μπορεί να λαμβάνει από τους παρόχους στοιχεία ο ιδιώτης όχι όμως και οι δικαστικές αρχές.–

Δεν θα ήταν περιττό τέλος να επισημάνω ότι στο άρθρο 1 παρ. 3 της οδηγίας 2002/58/ΕΚ αναγράφεται ότι «η παρούσα οδηγία δεν εφαρμόζεται..... στις δραστηριότητες που αφορούν τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου» με ό,τι αυτό μπορεί να σημαίνει.–

Θα μου επιτραπεί εν τέλει μια παρατήρηση σε σχέση προς το Ν. 3917/2911 με τον οποίο ενσωματώθηκε η οδηγία 2006/24/ΕΚ. ΄Οπως προκύπτει από το προοίμιο αλλά και το σώμα της οδηγίας αυτής με την οποία θεσπίσθηκε η υποχρέωση για τη διατήρηση επί ικανό χρόνο των δεδομένων κίνησης και θέσης, στα οποία περιλαμβάνονται και τα εξωτερικά στοιχεία της επικοινωνίας, σκοπό είχε τη δυνατότητα διερεύνησης, διαπίστωσης και δίωξης ποινικών αδικημάτων και της τρομοκρατίας. Εμείς στον πιο πάνω νόμο επιχειρούμε να προσθέσουμε ρήτρες, που, εφόσον θεωρηθούν ισχυρές, δυσχεραίνουν το στόχο και σκοπό αυτό.

IV. Τέλος κάποιοι επικαλούνται τις διατάξεις των άρθρων 5 παρ. 10 του Ν. 2225/1994 και 8 παρ. 7 του Ν. 3471/2006 προκειμένου να ενισχύσουν τη θέση της ΑΔΑΕ ότι το απόρρητο των επικοινωνιών του άρθρου 19 του Συντάγματος καλύπτει και τα εξωτερικά στοιχεία της επικοινωνίας. Οι πιο πάνω όμως διατάξεις οδηγούν στο ακριβώς αντίθετο συμπέρασμα, για λόγους τους οποίους έχουμε εκθέσει σε άλλο συνέδριο και ελλείψει χρόνου δεν θα εκθέσουμε εδώ.–

V.Συγκριτικό Δίκαιο

Στην Ιταλία τα εξωτερικά στοιχεία της επικοινωνίας δίδονται από τις εταιρίες κινητής ή σταθερής τηλεφωνίας με εντολή του αρμοδίου Εισαγγελέα δια της δικαστικής αστυνομίας.

Στη Γερμανία δίδονται στους αρμόδιους Εισαγγελείς, μετά από παραγγελία τους, ανεξαρτήτως του είδους του ποινικού αδικήματος.

VI. ΕΔΔΑ

Υπόθεση K.U. εναντίον Φινλανδίας

Δωδεκάχρονος αιτών εκτέθηκε σε διαφήμιση σεξουαλικού περιεχομένου σε διαδικτυακό τόπο. Η ταυτότητα του προσώπου που είχε τοποθετήσει τη διαφήμιση δεν ήταν δυνατόν να γίνει γνωστή από τον παροχέα υπηρεσιών Internet λόγω της Φινλανδικής νομοθεσίας που ίσχυε το συγκεκριμένο χρόνο. Το ΕΔΔΑ έκρινε ότι για την πρακτική και αποτελεσματική προστασία του αιτούντος ήταν αναγκαίο να ληφθούν ουσιαστικά μέτρα για τον εντοπισμό και δίωξη του δράστη που τοποθέτησε την αγγελία, λόγος για τον οποίο καταδίκασε τη Φινλανδία.

Από την απόφαση αυτή προκύπτει σαφώς ότι το δημόσιο συμφέρον αλλά και το συμφέρον των θυμάτων επιβάλλει οι δράστες εγκληματικών πράξεων να αποκαλύπτονται και να τιμωρούνται και ότι οποιοσδήποτε φραγμός (ακόμη και έλλειψη νομοθετικής ρυθμίσεως) στην επιδίωξη αυτού του σκοπού είναι ανεπίτρεπτος.

Αγ. Εν όψει λοιπόν των μέχρι τώρα εκτεθέντων είναι πρόδηλη η ορθότητα των θέσεων των γνωμοδοτήσεων της Εισαγγελίας του Αρείου Πάγου περί του ότι το υπό του άρθρου 19 του Συντάγματος θεσπιζόμενο απόρρητο δεν προστατεύει τα εξωτερικά στοιχεία της επικοινωνίας και την επικοινωνία μέσω του διαδικτύου.

Εκ τούτων παρέπεται ότι:

α) θέμα άρσεως του απορρήτου μιάς επικοινωνίας είτε ως προς τα εξωτερικά στοιχεία αυτής είτε όταν αυτή γίνεται μέσω του διαδικτύου με την υπό του Ν. 2225/1994 προβλεπόμενη διαδικασία δεν δύναται να τεθεί και β) Οι εισαγγελικές, ανακριτικές, προανακριτικές αρχές, τα Δικαστήρια και τα Δικαστικά Συμβούλια δικαιούνται να ζητούν από τους παρόχους των υπηρεσιών επικοινωνίας, μέσω του διαδικτύου (Internet) τα ηλεκτρονικά ίχνη μιάς εγκληματικής πράξεως, την ημεροχρονολογία και τα στοιχεία του προσώπου στο οποίο αντιστοιχεί το ηλεκτρονικό ίχνος, από τους λοιπούς δε παρόχους των υπηρεσιών επικοινωνίας τα «εξωτερικά στοιχεία» της επικοινωνίας και οι πάροχοι υποχρεούνται να τα παραδίδουν χωρίς να είναι αναγκαίο να προηγηθεί άδεια κάποιος αρχής και ιδίως της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών.

Β. Ως προς το δεύτερο ζήτημα:

Τη σχέση της Δικαιοσύνης με την ΑΔΑΕ και γενικότερα με τις ανεξάρτητες αρχές την καθορίζει το Σύνταγμα και η συνταγματική τάξη.

Η δικαστική λειτουργία είναι η μία από τις τρεις συντεταγμένες λειτουργίες (εξουσίες) και επομένως ανήκει και αυτή στον σκληρό πυρήνα της κρατικής εξουσίας. Δεν υπόκειται ούτε στις άλλες δύο λειτουργίες (εξουσίες) βάσει της αρχής της διακρίσεως των εξουσιών (άρθρο 26 του Συντάγματος) ούτε πολύ περισσότερο σε οποιαδήποτε από τις ανεξάρτητες Αρχές. Αντιθέτως οι ανεξάρτητες αρχές υπόκεινται στη δικαστική εξουσία αφού οι αποφάσεις τους ελέγχονται από αυτήν. Η Εισαγγελική Αρχή μετά το 1975 και το ψηφισθέν τότε Σύνταγμα είναι αυτοτελής δικαστική αρχή απολύτως ισότιμη με τα δικαστήρια και ανεξάρτητη από αυτά και αποτελεί όργανο της δικαστικής λειτουργίας.

Τα ανωτέρω ήταν απότοκα και του γεγονότος ότι οι Εισαγγελείς κατέστησαν και αυτοί ισόβιοι δικαστικοί λειτουργοί. Οι Εισαγγελείς έχουν, μεταξύ των άλλων, την αρμοδιότητα να γνωμοδοτούν επί νομικών ζητημάτων σύμφωνα με το άρθρον 25 του Κ.Ο.Δ.Κ.Δ.Λ.

Οι γνωμοδοτήσεις που εκδίδουν οι Εισαγγελείς, ως προερχόμενες από όργανο της Δικαστικής εξουσίας, δεσμεύουν τους πάντες εκτός από τα Δικαστήρια τα οποία θα αποφανθούν οριστικά επί του νομικού ζητήματος εφ' όσον αχθεί ενώπιόν τους. Όπως είναι αυτονόητο από τη δέσμευση αυτή δεν εξαιρούνται οι ανεξάρτητες αρχές, οι οποίες ευρίσκονται εκτός του σκληρού πυρήνα της κρατικής εξουσίας. Τούτο σημαίνει ότι εφ όσον ο Εισαγγελεύς του Αρείου Πάγου γνωμοδότησε επί ενός νομικού ζητήματος, απτομένου και των ανεξάρτητων αρχών, οι τελευταίες έχουν υποχρέωση να σεβασθούν και να συμμορφωθούν προς τη λύση που δόθηκε με τη γνωμοδότηση. Υποχρέωση όμως συμμορφώσεως έχουν και εκείνοι τη δραστηριότητα των οποίων ελέγχουν οι Ανεξάρτητες Αρχές, εφ όσον το επιλυθέν νομικό ζήτημα έχει σχέση με τη δραστηριότητα αυτών.

Αυτά σημαίνουν σε σχέση προς το συγκεκριμένο ζήτημα ότι τόσον η ΑΔΑΕ όσο και οι πάροχοι των επικοινωνιών θα έπρεπε να έχουν συμμορφωθεί απολύτως προς τις γνωμοδοτήσεις, οι οποίες, άλλως τε, έχουν έρεισμα, εκτός των άλλων και την υπ αριθμ. 570/2006 απόφαση του Αρείου Πάγου.

Δυστυχώς η ΑΔΑΕ αρνείται να συμμορφωθεί προς τις τρεις γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου, η δεύτερη μάλιστα των οποίων (αυτή του κ. Τέντε) εκδόθηκε μετά από ερώτημά της, ενώ οι πάροχοι των επικοινωνιών δεν συμμορφώνονται προς τις γνωμοδοτήσεις και δεν ικανοποιούν τα αιτήματα των δικαστικών αρχών επειδή όπως λέγουν, απειλούνται από την ΑΔΑΕ με πρόστιμα.

Έτσι όμως πράττοντες οι μεν πάροχοι τελούν τα αδικήματα της απειθείας και υποθάλψεως εγκληματιών, τα δε μέλη της ΑΔΑΕ τα αδικήματα της παραβάσεως καθήκοντος και παρανόμου βίας, αφού με τη ρηθείσα απειλή (εφ όσον αυτό ήθελε θεωρηθεί βάσιμο) εξαναγκάζουν τους παρόχους σε παράλειψη για την οποία δεν υφίσταται υποχρέωσή τους.

Είναι λοιπόν προφανές ότι τη λύση στο πρόβλημα που έχει γεννηθεί θα πρέπει να δώσουν κατ αρχάς οι Εισαγγελείς με την άσκηση διώξεων κατά των παρανομούντων και στη συνέχεια τα δικαστήρια με τις δικαστικές αποφάσεις. Έτσι θα περισώσουν και το κύρος της Δικαιοσύνης το οποίο πλήττεται από την άρνηση των παρόχων επικοινωνιών να ικανοποιούν τα αιτήματα των ανακριτικών και προανακριτικών αρχών αλλά και την άρνηση των ανωτέρω αλλά και της ΑΔΑΕ να συμμορφωθούν προς τις γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου αλλά και προς την απόφαση του Αρείου Πάγου.

Κυρίες και Κύριοι

Η χώρα μας τείνει να γίνει, αν δεν έχει γίνει ο παράδεισος εγκληματικής δράσεως και το καταφύγιο εγκληματιών. Σε τούτο έχει συντελέσει κατά πρώτο λόγο η απονεύρωση και ο ευτελισμός της ποινικής νομοθεσίας, όμως μερίδιο ευθύνης έχουν και κάποιες ανεξάρτητες αρχές, οι οποίες για λόγους που αυτές γνωρίζουν, δημιουργούν προσκόμματα στη δικαιοσύνη και κυρίως στις ανακριτικές και προανακριτικές αρχές στην προσπάθειά τους για την εξιχνίαση των εγκλημάτων και τιμωρία των εγκληματιών και την επικράτηση έτσι της αρχής του κράτους δικαίου. Θα ήθελα εδώ να υπενθυμίσω εκείνα που είχαν λάβει χώραν από το τέλος του 2007 και επί ικανό χρονικό διάστημα, με αφορμή τη χρήση ή μη των καμερών. Με γνωμοδότησή του ο ομιλών είχε ταχθεί υπέρ της χρήσεως των καμερών προκειμένου να επιτυγχάνεται η εξιχνίαση εγκλημάτων και η αποκάλυψη εγκληματιών. Είχα υποστεί τότε των παθών μου τον τάραχο υβριζόμενος από τα κόμματα της τότε αντιπολιτεύσεως, πολιτικούς, ΜΜΕ ακόμη και από δικαστικούς λειτουργούς επειδή δήθεν με τη λειτουργία των καμερών ετίθετο σε κίνδυνο το δημοκρατικό πολίτευμα. Και

όμως είχα γνωμοδοτήσει για κάτι που ίσχυε και ισχύει σε όλα τα κράτη της Δυτικής Ευρώπης χωρίς ποτέ να τεθεί θέμα κινδύνου λειτουργίας του δημοκρατικού πολιτεύματος. Οι πόλεις της Μεγάλης Βρεττανίας και ιδιαίτερα το Λονδίνο, της Γερμανίας και της Γαλλίας είναι γεμάτες με κάμερες. Επειδή στάθηκα αταλάντευτος στη θέση μου ως προς την εφαρμογή της γνωμοδοτήσεως παρητήθησαν, ως προσβληθέντα πέντε μέλη της Αρχής Προστασίας Προσωπικών δεδομένων και δέχθηκα και γι΄ αυτό άλλες επιθέσεις.

Μετά τέσσερα χρόνια εκείνοι που με καθύβριζαν και ζητούσαν την κατάργηση της γνωμοδοτήσεως θέσπισαν με νόμο (που δεν ήταν κατά την άποψή μου αναγκαίος), με πρόταση μάλιστα της Αρχής Προστασίας Προσωπικών δεδομένων, τη δυνατότητα λειτουργίας των καμερών. Τα ΜΜΕ ενώ το 2007 έκαναν λόγο για «χαφιεδοκάμερες» το 2011 επικροτούσαν τη χρήση των καμερών, αναγράφοντας «κάμερες παντού». Και δεν βρήκε κανείς τη δύναμη να ζητήσει συγνώμη για την αναστάτωση και τη δηλητηρίαση που είχε προκληθεί επί δύο και πλέον χρόνια σ΄ αυτό το δύσμοιρο τον τόπο. Είμαι βέβαιος ότι αργά ή γρήγορα και στο ζήτημα της εκτάσεως της προστασίας του άρθρου 19 του Συντάγματος θα πρυτανεύσει η σύνεση και η λογική και η ΑΔΑΕ θα παύσει τη μη σύννομη συμπεριφορά της. Τούτο επιβάλλει όχι μόνο η συνταγματική τάξη αλλά και η ανάγκη επιβιώσεως της χώρας μας, που κινδυνεύει από τη λαίλαπα της εγκληματικότητας. Όμως με τέτοιες νοοτροπίες και συμπεριφορές δεν προάγονται τα κράτη και οι κοινωνίες. Τα τόσα χρήματα που ξοδεύονται για τη λειτουργία των ανεξάρτητων αρχών θα πρέπει να έχουν αντίκρυσμα στους πολίτες, που σήμερα μάλιστα δοκιμάζονται σκληρά και υποφέρουν από την οικονομική δυσπραγία. Διαφορετικά δεν έχουν λόγο υπάρξεως και λειτουργίας.

Εν όσω λοιπόν υπάρχουν και λειτουργούν θα πρέπει τουλάχιστον να μη δημιουργούν προβλήματα και προσκόμματα στη λειτουργία της Δικαιοσύνης και να μην στερούν τους πολίτες από την έννομη προστασία αλλά και ολόκληρη την κοινωνία να ζει σ΄ ένα κράτος Δικαίου.

«Οι γνωμοδοτήσεις της Εισαγγελίας του Αρείου Πάγου και η νομοθεσία του Διαδικτύου για την άρση του απορρήτου»

κ. **Κωνσταντίνος Παρασκευαΐδης**, Αντεισαγγελέας Αρείου Πάγου,
ΜΔΕ Ποινικών Επιστημών Νομικής Σχολής Πανεπιστημίου Αθηνών

Με την εισήγησή μας επιχειρούμε να αντιμετωπίσουμε τα θεωρητικά και πρακτικά νομικά προβλήματα σε σχέση με την άρση του απορρήτου στο διαδίκτυο αποκλειστικά για ποινικές περιπτώσεις, για την διερεύνηση εγκλημάτων που τελούνται σε «περιβάλλον internet».

Οι σχετικές γνωμοδοτήσεις του Εισαγγελέα του Αρείου Πάγου σχετικά με την άρση του απορρήτου στο διαδίκτυο είναι οι 9/10 -5-2011, 12/29-9-2009 και η 9/29-6-2009 που εκδόθηκαν σύμφωνα με το άρθρο 25§2 Ν 1756/1988 του Κώδικα Οργανισμού Δικαστηρίων, με τις οποίες διατυπώνεται η άποψη ότι σε περίπτωση που διενεργείται προκαταρκτική εξέταση ή προανάκριση ή κύρια ανάκριση μετά από παραγγελία του εισαγγελέα, τότε η αρμόδια, κατά περίπτωση δικαστική αρχή, για τον εντοπισμό της ταυτότητας του προσώπου που αποστέλλει μηνύματα εξυβριστικού, δυσφημιστικού, απειλητικού, εκβιαστικού περιεχομένου, μέσω διαδικτύου, μπορεί να ζητήσει από τους παρόχους των υπηρεσιών internet, την ανακοίνωση στοιχείων σχετικών με την ταυτότητα ή την θέση του χρήστη, της ip address του δράστη, δίχως την τήρηση της διαδικασίας άρσης του απορρήτου του άρθρου 4 Ν 2225/1994, εφόσον, βάσει των στοιχείων που μέχρι εκείνη την στιγμή διαθέτει, είναι δυνατόν να υποτεθεί ότι μόνο με αυτό το μέσο θα γίνει δυνατή η ανακάλυψη του δράστη, επειδή τα «εξωτερικά στοιχεία της επικοινωνίας» δηλαδή τα δεδομένα της ταυτότητας και της θέσης του χρήστη εκφεύγουν του προστατευτικού πεδίου της διάταξης του άρθρου 19§1 του Συντάγματος, αφού στις προαναφερόμενες περιπτώσεις δεν πρόκειται για επικοινωνία ή ανταπόκριση κατά την έννοια της συνταγματικής διάταξης αλλά οι επαφές αυτές έχουν έγκλημα τικό περιεχόμενο, δεν συνιστούν ανταλλαγή απόψεων, διανοημάτων κλπ και δεν γίνονται στο πλαίσιο οικειότητας και εμπιστευτικότητας και επομένως ότι δεν συντρέχει δικαιολογητικός λόγος προστασίας του απορρήτου και κατ' ακολουθία η επικοινωνία αυτού του είδους δεν προστατεύεται από το άρθρο 19§1 του Συντάγματος και από την διάταξη του άρθρου 4§1 Ν 3471/2006.

Με λίγα λόγια ο Εισαγγελέας του Αρείου Πάγου δέχτηκε ότι από το απόρρητο της επικοινωνίας καλύπτεται μόνο το περιεχόμενο της και όχι τα «εξωτερικά στοιχεία της επικοινωνίας» και δεν απαιτείται άρση απορρήτου για την γνωστοποίηση των στοιχείων του δράστη στις δικαστικές αρχές.

Μετά την ισχύ του Ν 3917/2011 με τον οποίο ενσωματώθηκε σ' αυτόν η οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15 Μαρτίου και τροποποιήθηκε η παλαιότερη οδηγία 2002/58/ ΕΚ εκδόθηκε η τελευταία γνωμοδότηση (η 9/2011) του Εισαγγελέα ΑΠ με την οποία εκείνος εμμένει στην προηγούμενη θέση του, με την αιτιολογία ότι με τη ρύθμιση των άρθρων 4 και 5 του Ν. 3917/2011 ο νομοθέτης δεν θέλησε να εισαγάγει νέο περιοριστικό

καθεστώς για την χορήγηση των εξωτερικών στοιχείων της επικοινωνίας, σύμφωνα με την αιτιολογική έκθεση, στην οποία αναφέρεται σχετικά με το άρθρο 4 ότι «Δεν εισάγονται νέες ρυθμίσεις σε σχέση με την υφιστάμενη νομοθεσία» που είχε ληφθεί υπόψη για την έκδοση των δύο προηγούμενων γνωμοδοτήσεων και ότι οι γνωμοδοτήσεις αφορούσαν αιτήματα ανακριτικών αρχών που ενεργούσαν για την παροχή έννομης προστασίας και τιμώρησης των εγκλημάτων (άρθρων 20, 96§1 και 87§1 ΠΚ Συντάγματος), τα οποία αιτήματα αναφέρονται σε περιπτώσεις στις οποίες δεν πρόκειται για απόρρητο κατά την έννοια του άρθρου 19§1 Συντάγματος. Και πριν αλλά και μετά την ισχύ του Ν 3917/2011 εκφράστηκε απο μεγάλη μερίδα της επιστήμης και θεωρίας και την ΑΔΑΕ που ασκεί διοικητική εποπτεία και έλεγχο στους παρόχους υπηρεσιών στο διαδίκτυο (Ν 3115/2003 και Ν 3917/2011) η αντίθετη άποψη περί του ότι το απόρρητο της επικοινωνίας καλύπτει όχι μόνο το περιεχόμενο αλλά και τα εξωτερικά στοιχεία της επικοινωνίας, της ip address του δράστη, ότι απαιτείται να συντρέχουν οι όροι και προϋποθέσεις των άρθρων 4 και 5 Ν 2225/1994, δηλαδή βούλευμα για την γνωστοποίησή της, ακόμα και στην περίπτωση που διενεργείται δικαστική έρευνα για την διακρίβωση εγκλημάτων που δεν αναφέρονται στο άρθρο 4 Ν 2225/1994 ή το άρθρο 253 Α ΚΠΔ και δεν δικαιολογείται η απαίτηση των αρμοδίων δικαστικών αρχών για την χορήγηση των εξωτερικών στοιχείων της επικοινωνίας από τους φορείς παροχής. Υπήρξε μια αρνητική κριτική των προαναφερομένων εισαγγελικών γνωμοδοτήσεων περί του αν έρχονται σε αντίθεση με το άρθρο 19 και 25§1 Συντάγματος, του άρθρου 4 Ν 2225/1994, Ν 2774/1999 που όμως ήδη καταργήθηκε με άρθρο 17 Ν 3471/2006, Ν 3115/2003, ΠΔ 47/2005, Ν 3471/2006, Ν 3783/2009, άρθρο 370 Α ΠΚ και άρθρο 4 και 5 Ν 3917/2011 ως και με τις αποφάσεις του ΕΔΔΑ Malone και Copland κατά Ηνωμένου Βασιλείου. Ο συντάκτης της πρώτης γνωμοδότησης, επίτιμος Εισαγγελέας του ΑΠ κ Γ. Σανιδάς, απάντησε στην αρνητική κριτική σε επιστημονικό συνέδριο για το διαδίκτυο που οργανώθηκε στην Αράχωβα και δημοσιεύθηκαν οι νομικές απόψεις του στο περιοδικό Δίκαιο Μέσων Ενημέρωσης Επικοινωνίας 2010. Όμως οι εισαγγελικές γνωμοδοτήσεις, προς τις οποίες συμφωνούμε, δεν έρχονται σε αντίθεση με τις προαναφερόμενες δύο αποφάσεις του ΕΔΔΑ αφού με αυτές δεν κρίθηκε παρέμβαση δικαστικής αρχής για την άρση του απορρήτου των εξωτερικών στοιχείων επικοινωνίας, αλλά η μεν υπόθεση Malone αφορούσε την άρση του τηλεφωνικού απορρήτου κάποιου κατηγορουμένου για αποδοχή προϊόντων εγκλήματος, μετά από εντολή της Αστυνομίας και κατόπιν αδείας του αρμόδιου Υπουργού, η δεν υπόθεση Copland αφορούσε την παρακολούθηση του email και της επίσκεψης στο διαδίκτυο μιας υπαλλήλου ενός δημόσιου Κολλεγίου από τον αναπληρωτή διευθυντή του Κολλεγίου.

Το Ευρωπαϊκό Δικαστήριο (ΕΔΔΑ) εξετάζει την συνδρομή ή όχι μιας επιτακτικής κοινωνικής ανάγκης στις υποθέσεις που έρχονται ενώπιον του για την άρση του απορρήτου, στο δε κείμενο της ΕΣΔΑ δεν γίνεται λόγος για αναλογικότητα (proportionality), αλλά για μέτρο αναγκαίο σε μια δημοκρατική κοινωνία (άρθρο 8). Έτσι η παρέμβαση της δικαστικής αρχής για την άρση του απορρήτου στο διαδίκτυο πρέπει να είναι: 1) αναγκαίο μέτρο σε μια δημοκρατική κοινωνία. 2) να γίνεται χάριν της εξυπηρέτησης κάποιου υπέρτερου σκοπού όπως είναι η εθνική και δημόσια ασφάλεια, η πρόληψη της διάπραξης εγκλημάτων, η προστασία των δικαιωμάτων των τρίτων και η διασφάλιση του κύρους και της αμεροληψίας της δικαιοσύνης. 3) να υπάρχει πρόβλεψη, της παρέμβασης, από το νόμο, ώστε ο πολίτης να γνωρίζει το ενδεχόμενο περιορισμού των ελευθεριών του, έτσι ώστε να μπορεί να προσαρμόζει την συμπεριφορά του και να προβλέπει τις συνέπειες των ενεργειών του. Πρέπει να υπάρχει ασφάλεια δικαίου.

Το αντικείμενο του άρθρου 8 της ΕΣΔΑ είναι ουσιαστικά για την προστασία του ατόμου από αυθαίρετη επέμβαση των δημοσίων αρχών. Όμως το κράτος, εκτός από αυτή την αρνητική υποχρέωση μπορεί να έχει και θετικές υποχρεώσεις που είναι συνυφασμένες με τον πραγματικό σεβασμό της ιδιωτικής ή οικογενειακής ζωής (απόφαση ΕΣΔΑ K.U. κατά Φινλανδίας). Σύμφωνα με την ίδια απόφαση τα κράτη έχουν μια θετική υποχρέωση, με βάση το άρθρο 8 για την ποινικοποίηση των εγκλημάτων κατά προσώπων και να έχουν ως στόχο την αποτελεσματική διερεύνηση και δίωξη εγκλημάτων και επιβάλλεται από λόγους δημόσιου συμφέροντος η ύπαρξη μέτρων που να επιτρέπουν τον εντοπισμό του πραγματικού δράστη και την παραπομπή του στη δικαιοσύνη.

Πιστεύω ότι πληρούνται οι προαναφερόμενες προϋποθέσεις για την γνωστοποίηση των στοιχείων της ip address του δράστη, όπως εκτίθενται στις εισαγγελικές γνωμοδοτήσεις, σύμφωνα με το άρθρο 20§1 του Συντάγματος, αλλά και το άρθρο 6§1 της ΕΣΔΑ (Δικαίωμα στη χρήση και απονομή δικαιοσύνης),ως και το άρθρο 8 της ΕΣΔΑ, γιατί αλλιώς, με το απόρρητο των στοιχείων του δράστη, θα στερηθεί ο παθών του δικαιώματός του στην παροχή έννομης προστασίας από τα δικαστήρια και δεν θα μπορεί να αναπτύξει σωστά τις απόψεις του για τα δικαιώματά του, ενώ αντίθετα ο ανώνυμος δράστης θα επιτίθεται εναντίον του στο διαδίκτυο. Έχει άραγε την έννοια της επικοινωνίας στο διαδίκτυο ή την έννοια της επίθεσης και την έννοια του εγκλήματος η συμπεριφορά του ανώνυμου που στέλνει mail απειλητικά, εκβιαστικά και δυσφημιστικά κατά τρίτων ως και του ανώνυμου ο οποίος αναρτά στο διαδίκτυο μια κατασκευασμένη ψευδή συνέντευξη μεταξύ ενός δημοσιογράφου και ενός επιστήμονα, με την οποία τους προσβάλει βάναυσα και τους δυσφημεί. Πιστεύω ότι έτσι αναιρείται η έννοια της επικοινωνίας ή της επικοινωνίας σε οικειότητα και αυτός είναι ένας πρόσθετος λόγος που ενισχύει τις απόψεις των εισαγγελικών γνωμοδοτήσεων για την χορήγηση των στοιχείων της ip address του δράστη στις δικαστικές αρχές, δίχως άλλη διαδικασία. Τα αιτήματα των δικαστικών αρχών για την χορήγηση των στοιχείων της ip address του δράστη δεν διέρχονται προς έγκριση από την ΑΔΑΕ ή από άλλη διοικητική αρχή, γιατί αυτό θα αποτελούσε παρέμβαση στο έργο της απονομής της δικαιοσύνης, επειδή τα σχετικά αιτήματα των δικαστικών αρχών υποβάλλονται σύμφωνα με τις διατάξεις των άρθρων 243 §§1, 2, 251 και 275§1 ΚΠΔ. Επομένως προβλέπεται η παρέμβαση των δικαστικών αρχών από τις διατάξεις του ΚΠΔ, οι δε διατάξεις του ΠΚ και άλλων ποινικών νόμων προβλέπουν την αντικειμενική και υποκειμενική υπόσταση των εγκλημάτων που τελεί ο ανώνυμος δράστης σε περιβάλλον internet. Η εγκληματική συμπεριφορά δεν εμπίπτει στην έννοια των προσωπικών δεδομένων ώστε να καλύπτεται από αυτή, η δε αποκάλυψη της ip address του δράστη στις δικαστικές αρχές δεν θεωρείται προσβολή της προσωπικότητας του και παραβίαση των προσωπικών δεδομένων. Με τους όρους και προϋποθέσεις των άρθρων 3,4,5 Ν. 2225/1994 και μόνο για τα διαλαμβανόμενα σ' αυτά εγκλήματα μπορεί να γίνει άρση του απορρήτου των επικοινωνιών στο διαδίκτυο και για τα εξωτερικά στοιχεία της επικοινωνίας και για το περιεχόμενό της προς διακρίβωση των εγκλημάτων αυτών. Για τα υπόλοιπα εγκλήματα δεν μπορεί να γίνει άρση του απορρήτου του περιεχομένου της επικοινωνίας αλλά μόνο των εξωτερικών στοιχείων αυτής, σύμφωνα με τις προαναφερόμενες εισαγγελικές γνωμοδοτήσεις.

Ο χώρος του διαδικτύου δεν πρέπει να είναι νομικά ανεξέλεγκτος, η δε ποινική δικαιοσύνη δεν μπορεί να μείνει αδιάφορη μπροστά σε αυτήν την αξιόποινη ανθρώπινη συμπεριφορά.

Κωνσταντίνος Παρασκευαΐδης
Αντεισαγγελέας Αρείου Πάγου

«Μέτρα ασφαλείας και αντιμετώπιση περιστατικών παραβίασηςπροσωπικών δεδομένων: Προβλήματα και σκέψεις με αφορμή την πρόσφατη νομολογία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα»

κ. **Γρηγόρης Λαζαράκος**, Δικηγόρος, Δ.Ν.,
Αναπληρωματικό Μέλος της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.)

Ι. Εισαγωγικές παρατηρήσεις

Είναι γνωστό ότι η πληροφορία αποτελεί διαχρονικά πολύτιμο αγαθό για εκείνον που την κατέχει. Στο επίκεντρο των σύγχρονων συναλλαγών τοποθετείται πλέον η προσωπική πληροφορία για το άτομο, η οποία αποκτά οικονομική αξία και καθίσταται, κατ' αυτόν τον τρόπο, αντικείμενο συναλλαγής, νόμιμης αλλά και παράνομης συναλλαγής.

Όλοι θυμόμαστε την πρόσφατη περίπτωση εταιρίας, που εμπορευόταν παράνομα προσωπικά δεδομένα και την οποία η Αρχή Προστασίας Προσωπικών Δεδομένων είχε εντοπίσει μετά από πολύ προσεκτική έρευνα, που διεξήγαγε το εξειδικευμένο προσωπικό της. Θυμίζω ότι τότε ζητήθηκε από την Αρχή η συνδρομή της Δίωξης Ηλεκτρονικού Εγκλήματος, διενεργήθηκε αιφνίδια έρευνα στα ηλεκτρονικά αρχεία του φυσικού προσώπου, στο σπίτι του, με αποτέλεσμα να προκύψουν σοβαρές ενδείξεις εμπλοκής του στην ερευνώμενη παράνομη δραστηριότητα και να προφυλακιστεί. Από τους σκληρούς δίσκους δε που κατασχέθηκαν προέκυψαν πολύ χρήσιμα στοιχεία τόσο για την προέλευση των δεδομένων όσο και για την χρήση τους μέχρι εκείνη τη στιγμή. Τα στοιχεία αυτά μας οδήγησαν (και μας οδηγούν) σε νέους ελέγχους και σε νέα ενδιαφέροντα ευρήματα.

Και σε αυτή την περίπτωση όπως και σε πολλές άλλες αντίστοιχες, τα προσωπικά δεδομένα κατέληξαν στα χέρια μη εξουσιοδοτημένων προσώπων, διότι δεν ελήφθησαν από τον υπεύθυνο επεξεργασίας των εκάστοτε βάσεων δεδομένων τα αναγκαία οργανωτικά και τεχνικά μέτρα ασφαλείας, καθώς και τα μέτρα φυσικής ασφάλειας, που όφειλε και μπορούσε να έχει λάβει η επιχείρηση ή φορέας του Δημοσίου, καθότι υπάρχουν σοβαρές ενδείξεις ότι διαρροή μπορεί να έχει γίνει και από δημόσιες υπηρεσίες που τηρούν μεγάλες βάσεις δεδομένων.

Όσο πιο αδύναμη παρουσιάζεται όμως η οργανωτική, τεχνική και φυσική προστασία των πληροφοριακών συστημάτων και των βάσεων δεδομένων, τόσο πιο πολύ αυξάνεται ο κίνδυνος παραβίασής τους. Όπως, μάλιστα, δέχεται η Οδηγία 2009/136/ΕΚ στην αιτιολογική σκέψη 61, «*η παραβίαση που αφορά δεδομένα προσωπικού χαρακτήρα μπορεί να επιφέρει, εάν δεν αντιμετωπιστεί κατάλληλα και εγκαίρως, σημαντική οικονομική απώλεια και κοινωνική ζημία στο συνδρομητή ή στο μεμονωμένο άτομο*».

Κατά την επεξεργασία του θέματος ενόψει της σημερινής ημερίδας, αντιμετώπισα πολλές δυσκολίες, διότι η προσέγγιση και η ανάλυση του συγκεκριμένου θέματος για έναν νομικό, όπως ο ομιλών, είναι εξαιρετικά δύσκολη, λόγω των πολλών και σύνθετων τεχνικών ζητημάτων, αποτε-

λεί όμως συγχρόνως και μία μεγάλη πρόκληση, η οποία τις τελευταίες μέρες έγινε ακόμη μεγαλύτερη, όταν διαβάζοντας τον ελληνικό και ξένο τύπο, περιήλθαν σε γνώση μου αλλεπάλληλα γεγονότα παραβίασης προσωπικών δεδομένων. Κάθε μέρα διάβαζα και κάτι καινούργιο:

1. Στις 30.1.2013 η αμερικάνικη εφημερίδα New York Times ανακοίνωσε ότι τους τελευταίους 4 μήνες η εφημερίδα είχε γίνει στόχος κυβερνο-επιθέσεων από χάκερς, οι οποίοι κατόρθωσαν, σύμφωνα με τα δημοσιεύματα, να εισβάλουν στα συστήματα υπολογιστών της εφημερίδας και να αποκτήσουν τους κωδικούς δημοσιογράφων και άλλων υπαλλήλων, αποκτώντας έτσι πρόσβαση στους υπολογιστές 53 εργαζομένων στην εφημερίδα.
2. Στις 31.1.2013 παρόμοια ανακοίνωση εξέδωσε μία άλλη γνωστή αμερικάνικη εφημερίδα, η Wall Street Journall.
3. Μία ημέρα αργότερα, την 1.2.2013, ο Brian Krebs, πρώην ρεπόρτερ μίας άλλης γνωστής αμερικάνικης εφημερίδας, της Washington Post, αποκάλυψε ότι παρόμοιες επιθέσεις είχε δεχθεί και η δική του εφημερίδα.

   Όλες οι εφημερίδες επέρριψαν την ευθύνη των κυβερνο-επιθέσεων σε κινέζους χάκερς.
4. Μία μέρα αργότερα, στις 2.2.2013, ο διευθυντής ασφαλείας του Twitter παραδέχθηκε ότι θύματα επιθέσεων χάκερ έχουν πέσει περίπου 250.000 χρήστες του Twitter. Οι χάκερ κατάφεραν να πάρουν τα ονόματα, τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, τους κωδικούς πρόσβασης και άλλα δεδομένα.

Υπό την πίεση των γεγονότων αυτών, το γνωστό γερμανικό περιοδικό "Der Spiegel" δημοσίευσε στη διαδικτυακή του έκδοση στις 2/2 ότι σύμφωνα με πληροφορίες του πρακτορείου Reuters, η Ευρωπαϊκή Επιτροπή επεξεργάζεται, τη θέσπιση υποχρέωσης γνωστοποίησης επιθέσεων χάκερς κατά της ασφάλειας των πληροφοριακών συστημάτων επιχειρήσεων, που δραστηριοποιούνται σε διάφορους κλάδους της οικονομίας, όπως στον τραπεζικό, τον χρηματιστηριακό, τον ενεργειακό κλάδο, επίσης τον κλάδο της υγείας και των συγκοινωνιών, καθώς επίσης και στη δημόσια διοίκηση. Οι επιχειρήσεις ξεπερνούν στο σύνολό τους τις 44.000, γεγονός που προκάλεσε μεγάλες ανησυχίες κυρίως σε εισηγμένες στο χρηματιστήριο εταιρείες, οι οποίες φοβούνται την ανασφάλεια, που μπορεί να δημιουργηθεί στους επενδυτές, σε περίπτωση που γίνει γνωστή μία κυβερνο-επίθεση στην εταιρεία.

Τέτοια υποχρέωση γνωστοποίησης υπάρχει ήδη στην Ελλάδα, αλλά και σε ευρωπαϊκό επίπεδο, μόνο για φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, υπάρχει όμως η σκέψη η υποχρέωση αυτή να επεκταθεί και σε άλλους υπεύθυνους επεξεργασίας.

Επισημαίνεται ότι τη θέσπιση τέτοιας υποχρέωσης επεχείρησε, χωρίς όμως επιτυχία, και ο αμερικανός Πρόεδρος Barack Obama, κατά την πρώτη προεδρική του θητεία, ενώ τα δημοσιεύματα αναφέρουν ότι θα προσπαθήσει ξανά στη διάρκεια της δεύτερης θητείας του. Αλλά και στη Γερμανία υπάρχει, σύμφωνα με το περιοδικό "Spiegel", παρόμοιο σχέδιο νόμου, το οποίο πρόκειται να ψηφιστεί από το Κοινοβούλιο τον ερχόμενο Μάρτιο.

Το θέμα της πολιτικής ασφαλείας και των μέτρων ασφαλείας, που πρέπει να λαμβάνονται ώστε να αποφεύγονται παραβιάσεις προσωπικών δεδομένων όσο κρίσιμο και επίκαιρο κι αν είναι, υποεκτιμάται από τους υπεύθυνους επεξεργασίας, οι οποίοι μέσα στη δίνη της σκληρής καθημερινότητας και των οικονομικών προβλημάτων που αντιμετωπίζουν οι επιχειρήσεις τους, ιδίως στις μέρες μας, αμελούν και δεν δίδουν τη δέουσα προσοχή στην πολιτική ασφαλείας των πληροφοριακών τους συστημάτων.

Επιτρέψτε μου, λοιπόν, να αναφερθώ εν συντομία, στα μέτρα ασφαλείας, που θα πρέπει να λαμβάνονται από τον υπεύθυνος επεξεργασίας, προκειμένου να προστατεύσει αφενός τα προσωπικά δεδομένα που τηρεί και αφετέρου τη δική του εμπορική φήμη.

II. Χρήσιμοι ορισμοί

Παραβίαση προσωπικών δεδομένων: Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση προσωπικών δεδομένων που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία, σε συνδυασμό με την παροχή διαθέσιμης στο κοινό ηλεκτρονικής υπηρεσίας επικοινωνιών στην Κοινότητα.

(άρθρο 2 στοιχ. (η) της Οδηγίας 2002/58/ΕΚ, το προσετέθη ως άνω βάσει της Οδηγίας 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Νοεμβρίου 2009).

Δεδομένα προσωπικού χαρακτήρα: Κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί <το πρόσωπο στο οποίο αναφέρονται τα δεδομένα>– ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη.
(άρθρο 2 στοιχ. (α) της Οδηγίας 95/46/ΕΚ).

Πολιτική ασφαλείας: Έγγραφο του υπευθύνου επεξεργασίας στο οποίο περιγράφονται οι στόχοι της ασφάλειας και οι αντίστοιχες διαδικασίες που πρέπει να ακολουθούνται ώστε να επιτευχθούν αυτοί οι στόχοι. Πολύ σημαντικότερο βεβαίως από την Πολιτική Ασφαλείας είναι το Σχέδιο Ασφαλείας, στο οποίο θα πρέπει να εξειδικεύονται οι αρχές αυτές.

Η πολιτική ασφαλείας πρέπει να θέτει τις βασικές αρχές για α) τα οργανωτικά μέτρα ασφαλείας αναφορικά με τους ρόλους και τις αρμοδιότητες του προσωπικού και των εξωτερικών συνεργατών–εκτελούντων την επεξεργασία, τον καθορισμό και τις αρμοδιότητες του υπευθύνου ασφαλείας, την εκπαίδευση του προσωπικού, τη διαχείριση περιστατικών ασφαλείας, καθώς και την καταστροφή των προσωπικών δεδομένων, β) τα τεχνικά μέτρα ασφάλειας αναφορικά με τη διαχείριση των χρηστών του πληροφοριακού συστήματος, την αναγνώριση και αυθεντικοποίηση των χρηστών, την ασφάλεια των επικοινωνιών, τη λειτουργία των αρχείων καταγραφής του πληροφοριακού συστήματος, την εξαγωγή αντιγράφων ασφαλείας και γ) τα μέτρα φυσικής ασφάλειας.

IV. Νομικό πλαίσιο στην ευρωπαϊκή έννομη τάξη

Όπως αναφέρθηκε ήδη, ο ορισμός του όρου «παραβίαση προσωπικών δεδομένων συναντάται στην Οδηγία 2009/136/ΕΚ, που τροποποίησε την Οδηγία 2002/58/ΕΚ (για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών).

Επισημαίνεται ότι εισάγεται για πρώτη φορά η υποχρέωση του παρόχου διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών να γνωστοποιεί άμεσα, δηλαδή χωρίς αδικαιολόγητη καθυστέρηση, την παραβίαση προσωπικών δεδομένων α) στην αρμόδια εθνική αρχή και β) στον ενδιαφερόμενο συνδρομητή ή στο ενδιαφερόμενο πρόσωπο.

V. Νομικό πλαίσιο στην ελληνική έννομη τάξη

Οι σχετικές διατάξεις της Οδηγίας 2009/136/ΕΚ ενσωματώθηκαν στην ελληνική έννομη τάξη με το άρθρο 173 του ν. 4070/2012, που τροποποίησε το άρθρο 12 του ν. 3471/2006 (για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών).

Οι βασικές διατάξεις του άρθρου 12 του ν. 3471/2006 προβλέπουν τα εξής:

α) Σε περίπτωση παραβίασης προσωπικών δεδομένων ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών γνωστοποιεί αμελλητί την παραβίαση στην Α.Π.Δ.Π.Χ. και στην Α.Δ.Α.Ε. **(παρ. 5).** Θυμίζω ότι η Οδηγία έλεγε ότι η γνωστοποίηση θα πρέπει να γίνεται στην αρμόδια εθνική αρχή. Εδώ ο νομοθέτης όρισε και τις 2 Αρχές συναρμόδιες για τον χειρισμό τέτοιου είδους θεμάτων. Ευτυχώς δεν έχει προκύψει ακόμη η ανάγκη εφαρμογής της συγκεκριμένης διάταξης. Φαντάζομαι ότι το πρόβλημα θα λυθεί στην πράξη, όταν προκύψει.

β) Όταν η παραβίαση προσωπικών δεδομένων ενδέχεται να έχει δυσμενείς επιπτώσεις στα δεδομένα προσωπικού χαρακτήρα ή την ιδιωτική ζωή του συνδρομητή ή άλλου ατόμου, ο φορέας ενημερώνει αμελλητί για την παραβίαση αυτή και τον θιγόμενο συνδρομητή ή το θιγόμενο άτομο **(παρ. 6).**

γ) Οι φορείς που παρέχουν διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών τηρούν αρχείο παραβιάσεων δεδομένων προσωπικού χαρακτήρα (που περιλαμβάνει την περιγραφή των σχετικών περιστατικών, τα αποτελέσματα τους και τις διορθωτικές ενέργειες στις οποίες προέβησαν **(παρ. 9).**

Επισημαίνεται ότι οι διατάξεις του άρθρου 10 παρ. 3 του ν. 2472/1997, που παρέχουν το γενικό κανόνα, εξακολουθούν να ισχύουν και να εφαρμόζονται για όλες τις περιπτώσεις παραβίασης προσωπικών δεδομένων, πλην φυσικά εκείνων που αφορούν παραβίαση προσωπικών δεδομένων σε φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών. Σύμφωνα με το άρθρο 10 παρ. 3 του νόμου «ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας».

VI. Μέτρα ασφαλείας

Η Αρχή έχει αποτυπώσει εγγράφως τις βασικές αρχές που πρέπει να διέπουν την πολιτική ασφαλείας του υπεύθυνου επεξεργασίας κι έχει εξειδικεύσει τα μέτρα ασφαλείας που θα πρέπει να λαμβάνονται από έναν οργανισμό ή μία επιχείρηση. Τα μέτρα ασφαλείας εντάσσονται στις παρακάτω τρεις κύριες κατηγορίες:

Α) Οργανωτικά μέτρα ασφαλείας

Β) Τεχνικά μέτρα ασφαλείας

Γ) Μέτρα φυσικής ασφαλείας

Για λόγους οικονομίας χρόνου, θα αναφερθώ εν συντομία μόνο στα βασικότερα στοιχεία που συνιστούν το κάθε επιμέρους μέτρο.[2]

Α) Οργανωτικά Μέτρα Ασφαλείας

Υπεύθυνος Ασφαλείας

Πρέπει να οριστεί θέση υπεύθυνου ασφαλείας, ο οποίος θα έχει, τουλάχιστον, την επίβλεψη και τον έλεγχο της εφαρμογής της πολιτικής ασφαλείας και των μέτρων ασφαλείας.

Οργάνωση / Διαχείριση προσωπικού

Σε κάθε εργαζόμενο θα πρέπει να έχουν ανατεθεί (και μάλιστα εγγράφως) συγκεκριμένα καθήκοντα, βάσει δε αυτών να έχουν δικαίωμα πρόσβασης μόνο στα απολύτως απαραίτητα δεδομένα προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Επίσης κατά την αποχώρηση του εργαζομένου από την επιχείρηση πρέπει να εφαρμόζονται συγκεκριμένα μέτρα ασφαλείας, όπως π.χ. i) κατάργηση όλων των λογαριασμών πρόσβασης, των εξουσιοδοτήσεων και των κωδικών-συνθηματικών πρόσβασης, ii) κατάργηση των λογαριασμών ηλεκτρονικού ταχυδρομείου και μη ανάθεσή τους σε άλλον ή άλλους υπαλλήλους (μη επαναχρησιμοποίηση τους), iii) Επιστροφή οποιουδήποτε εξοπλισμού έχει παρασχεθεί στον υπάλληλο και ανήκει στον υπεύθυνο επεξεργασίας, (συμπεριλαμβανομένων υπολογιστών, κλειδιών, ηλεκτρονικών καρτών εισόδου/εξόδου, κ. λπ).

Διαχείριση πληροφοριακών αγαθών

Θα πρέπει να τηρείται επικαιροποιημένος κατάλογος των πληροφοριακών και επικοινωνιακών υποδομών και συστημάτων, του λογισμικού καθώς και των κατηγοριών αρχείων και δεδομένων που χρησιμοποιούνται ή τηρούνται από τον υπεύθυνο επεξεργασίας. Επίσης, τα δεδομένα πρέπει να διαβαθμίζονται βάσει του είδους και της κρισιμότητάς τους, ενώ σε περίπτωση που εξοπλισμός (π.χ. υπολογιστής ή USB) με προσωπικά δεδομένα μεταφέρεται εκτός των εγκαταστάσεων του υπευθύνου επεξεργασίας, η ενέργεια αυτή πρέπει να καταγράφεται (ημερομηνία και ώρα εξόδου, πρόσωπο που χρησιμοποιεί τον εξοπλισμό, επιστροφή του εξοπλισμού) και να τελεί υπό την έγκριση είτε του υπευθύνου επεξεργασίας είτε του υπευθύνου ασφαλείας.

Εκτελούντες την επεξεργασία

Στην περίπτωση που ο υπεύθυνος επεξεργασίας αναθέτει την επεξεργασία δεδομένων σε εκτελούντα, κατά την έννοια του στοιχ. η) του άρθρου 2 ν.2472/1997, η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως και προβλέπει ότι ο εκτελών την επεξεργασία την διεξάγει μόνο κατ' εντολή του υπευθύνου και ότι οι λοιπές υποχρεώσεις του άρθρου 10 ως προς την ασφάλεια βαρύνουν αναλόγως και αυτόν (τον εκτελούντα). Οι έγγραφες αναθέσεις-συμβάσεις πρέπει να περιέχουν κατ' ελάχιστο περιγραφή των προσωπικών δεδομένων, το σκοπό, τον τόπο και τον τρόπο/διαδικασία της επεξεργασίας, καθώς και τα επίπεδα των υπηρεσιών που πρέπει να επι-

2. Αναλυτικά τα μέτρα ασφαλείας αναφέρονται στην Ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα www.dpa.gr.

τυγχάνει ο εκτελών την επεξεργασία (σε επίπεδο ασφαλείας και ποιότητας δεδομένων). Όταν η επεξεργασία γίνεται εκτός των εγκαταστάσεων του υπευθύνου επεξεργασίας, ο υπεύθυνος θα πρέπει να εξασφαλίζει ότι ο εκτελών παρέχει επίπεδο ασφαλείας τουλάχιστον ανάλογο με αυτό που ορίζεται στην πολιτική ασφαλείας του υπευθύνου. Περαιτέρω, οι υπάλληλοι του εκτελούντος που επεξεργάζονται, κατά το χρονικό διάστημα της σύμβασης, προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας πρέπει να δεσμεύονται εγγράφως με κατάλληλη δήλωση εμπιστευτικότητας.

Καταστροφή δεδομένων και αποθηκευτικών μέσων

Θα πρέπει να ακολουθούνται κατ' ελάχιστον όσα προβλέπονται στην Οδηγία 1/2005 της Αρχής για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας.

Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων

Ο υπεύθυνος επεξεργασίας οφείλει να διαθέτει διαδικασίες για την αναγνώριση, αναφορά και άμεση αντιμετώπιση των περιστατικών παραβίασης της ασφάλειας των προσωπικών δεδομένων. Θα πρέπει να υπάρχει καταγραφή του κάθε συμβάντος σε σχετικό αρχείο, που θα περιλαμβάνει τη χρονική στιγμή που έλαβε χώρα, το πρόσωπο που το ανέφερε και σε ποιον το ανέφερε, εκτίμηση των συνεπειών και της κρισιμότητας του περιστατικού, διαδικασίες ανάκαμψης/διόρθωσης που ακολουθήθηκαν, καθώς και ενδεχόμενη διαδικασία ενημέρωσης των θιγομένων ατόμων (υποκειμένα των δεδομένα) ανάλογα με την έκταση του περιστατικού, κ.ο.κ.

Εκπαίδευση προσωπικού

Η εκπαίδευση του προσωπικού θα πρέπει να γίνεται σε θέματα προστασίας προσωπικών δεδομένων, καθώς και σε ειδικές σχετικές με ασφάλεια λειτουργίες του πληροφοριακού συστήματος (π.χ. χρήση μη προβλέψιμων κωδικών πρόσβασης και συνθηματικών, τρόπο εντοπισμού και αναφοράς των περιστατικών παραβίασης της ασφαλείας, σωστή χρήση των e-mail και των αποσπώμενων μέσων αποθήκευσης).

Έλεγχος

Πρέπει να πραγματοποιούνται προγραμματισμένοι έλεγχοι (είτε εσωτερικοί είτε εξωτερικοί, σε ετήσια βάση), όπου να αποτυπώνεται και να ελέγχεται η τήρηση των μέτρων ασφαλείας και η αποτελεσματικότητά τους. Έτσι μπορεί να τροποποιούνται ορισμένα μέτρα και να προστίθενται νέα.

Β) Τεχνικά Μέτρα Ασφαλείας

Έλεγχος πρόσβασης

α) Πρέπει να αναπτυχθούν μηχανισμοί που να μην επιτρέπουν προσβάσεις σε πόρους/εφαρμογές/αρχεία από μη εξουσιοδοτημένους χρήστες

β) Ο υπεύθυνος επεξεργασίας οφείλει να υιοθετήσει συγκεκριμένη πολιτική διαχείρισης των συνθηματικών των χρηστών, η οποία να περιλαμβάνει τουλάχιστον κανόνες αποδοχής για το ελά-

χιστο μήκος (προτεινόμενο ελάχιστο μήκος αποτελούν οι 8 χαρακτήρες) και επιτρεπτούς χαρακτήρες των συνθηματικών (πολυπλοκότητα συνθηματικού), την ιστορικότητα του συνθηματικού και τη συχνότητα αλλαγής του.

Αντίγραφα ασφαλείας

α) Ο υπεύθυνος επεξεργασίας πρέπει να αναπτύξει συγκεκριμένη πολιτική για τη λήψη και διαχείριση των αντιγράφων ασφαλείας.

β) Το αντίγραφο ασφαλείας πρέπει να διατηρείται σε διαφορετικό χώρο/φυσική τοποθεσία από τα πρωτογενή δεδομένα, ο οποίος να διαθέτει μέτρα ασφαλείας ανάλογα με τα μέτρα που υιοθετούνται για τα πρωτογενή δεδομένα.

Διαμόρφωση υπολογιστών

α) Πρέπει να υπάρχει προστασία από κακόβουλο λογισμικό όλων των υπολογιστών (τόσο των προσωπικών υπολογιστών των υπαλλήλων όσο και των διακομιστών (servers)) που τηρούν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα. Αυτό μπορεί να επιτευχθεί (πέραν της σωστής χρήσης αυτών από τους υπαλλήλους) με αντιβιοτικά προγράμματα (antivirus), καθώς και με χρήση προγραμμάτων τειχών ασφαλείας (firewall).

β) Οι ηλεκτρονικοί υπολογιστές που χρησιμοποιούνται από τους τελικούς χρήστες δεν πρέπει να διαθέτουν δυνατότητα εξαγωγής δεδομένων με τη χρήση αποσπώμενων μέσων (π.χ. USB, CD/DVD) – εκτός αν υπάρχει έγκριση από τον Υπεύθυνο Ασφαλείας. Αυτό είναι σημαντικό ιδιαίτερα σε αρχεία με μεγάλο όγκο προσωπικών δεδομένων, ιδίως δε αν αυτό επιβάλλεται και από τη φύση των προσωπικών δεδομένων, προκειμένου να αποφεύγονται φαινόμενα εξαγωγής και χρήσης λιστών τύπου Ερβέ Φαλτσιάνι (γνωστής στην Ελλάδα ως λίστας Λαγκάρντ).

γ) Δεν πρέπει να αποθηκεύονται δεδομένα προσωπικού χαρακτήρα σε υπολογιστές που έχουν σύνδεση με το διαδίκτυο (εκτός αν κάτι τέτοιο είναι απολύτως απαραίτητο στο πλαίσιο του ρόλου/αρμοδιοτήτων που έχουν ανατεθεί στο χρήστη του υπολογιστή). Εδώ επιτρέψτε μου να καταθέσω την προσωπική μου εμπειρία ήδη από το 1999, όταν είχα εργασθεί για ένα διάστημα στην Αρχή Προστασίας Προσωπικών Δεδομένων του Βερολίνου. Όλοι οι υπάλληλοι διέθεταν 2 Η/Υ, ένας για την υπηρεσιακή χρήση, κι ένας άλλος, ξεχωριστός Η/Υ, για να έχουν οι υπάλληλοι πρόσβαση στο Διαδίκτυο.

Αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας

Θα πρέπει να υπάρχουν διαδικασίες για την τήρηση και τον έλεγχο των αρχείων καταγραφής όλων των ενεργειών (log files) των χρηστών, συμπεριλαμβανομένων και των ενεργειών των διαχειριστών των συστημάτων, καθώς και των συμβάντων ασφαλείας.

Ασφάλεια επικοινωνιών

Ο υπεύθυνος επεξεργασίας πρέπει να υιοθετήσει συγκεκριμένη διαδικασία για τη διαχείριση της απομακρυσμένης πρόσβασης σε συστήματα (π.χ. από εταιρείες συντήρησης) μέσω ασφαλών καναλιών με δυνατή ταυτοποίηση/αυθεντικοποίηση και κρυπτογράφηση.

Αποσπώμενα μέσα αποθήκευσης

Πρέπει να υπάρχουν διαδικασίες για την αποτελεσματική κρυπτογράφηση (επιλογή σύγχρονων και ισχυρών αλγορίθμων κρυπτογράφησης, κατάλληλο μέγεθος κλειδιών και τεχνικές δια-

χείρισης αυτών, κ.λπ.) αρχείων με προσωπικά δεδομένα, ιδίως ευαίσθητα, που τηρούνται σε φορητά αποθηκευτικά μέσα (π.χ. USB δίσκους κ.ο.κ.), αφού για αυτές τις περιπτώσεις ο κίνδυνος διαρροής δεδομένων αυξάνεται.

Ασφάλεια λογισμικού

Ο σχεδιασμός των εφαρμογών που χρησιμοποιούνται για την επεξεργασία προσωπικών δεδομένων πρέπει να πραγματοποιείται λαμβάνοντας υπόψη τις βασικές αρχές της προστασίας προσωπικών δεδομένων και της ιδιωτικότητας (privacy by design).

Διαχείριση αλλαγών

Ο υπεύθυνος επεξεργασίας πρέπει να ορίσει σαφή πολιτική διαχείρισης όλων των αλλαγών που πραγματοποιούνται στα πληροφοριακά συστήματα, η οποία να περιέχει κατ' ελάχιστον: καταγραφή των αιτημάτων αλλαγής, καθορισμό των ρόλων που έχουν δικαίωμα έγκρισης των αλλαγών, καθορισμό των κριτηρίων αποδοχής της αλλαγής και χρονοδιάγραμμα υλοποίησης.

Γ) Μέτρα Φυσικής Ασφάλειας

Έλεγχος φυσικής πρόσβασης

Πρέπει να υπάρχουν τα κατάλληλα μέτρα ελέγχου φυσικής πρόσβασης στους κρίσιμους χώρους όπου βρίσκεται ο φυσικός εξοπλισμός (συμπεριλαμβανομένης τηλεπικοινωνιακής και δικτυακής καλωδίωσης) που υποστηρίζει τα πληροφοριακά συστήματα και την επεξεργασία προσωπικών δεδομένων, έτσι ώστε να επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένο προσωπικό (για παράδειγμα, κάποιοι χώροι –όπως αυτοί που βρίσκεται δικτυακός εξοπλισμός– πρέπει να είναι μόνιμα κλειδωμένοι).

Περιβαλλοντική ασφάλεια

Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για την προστασία των κτιρίων, των κρίσιμων χώρων, του computer room, των γραφείων του προσωπικού, του εξοπλισμού πληροφορικής και του χώρου τήρησης φυσικού αρχείου από ζημιές που μπορούν να προκληθούν από φυσικές καταστροφές ή κακόβουλες ενέργειες, όπως πλημμύρα, υπερθέρμανση, πυρκαγιά, σεισμός, έκρηξη, διαρροή νερού, διακοπή ρεύματος, διάρρηξη/κλοπή, βανδαλισμός, κ.λπ. Ενδεικτικά μέτρα προς αυτή την κατεύθυνση είναι τα εξής: συναγερμός, πόρτες και παράθυρα ασφαλείας, πυροπροστασία, απομάκρυνση εξοπλισμού από υδροσωληνώσεις και πηγές σκόνης, ανιχνευτές υγρασίας και πλημμύρας, αδιάλειπτη παροχή ρεύματος μέσω σταθεροποιητών/γεννητριών, κ.λπ.

Έκθεση εγγράφων

α) Οι φάκελοι που περιέχουν προσωπικά δεδομένα (φυσικό αρχείο) πρέπει να είναι τοποθετημένοι σε φωριαμούς και να μην εκτίθενται σε κοινή θέα.

β) Θα πρέπει να καταγράφεται η μεταφορά των φυσικών φακέλων σε διαφορετικά γραφεία ή οργανωτικές μονάδες. Η Αρχή επέβαλε πρόστιμο ύψους €3.000 στον «Οργανισμό Κατά των Ναρκωτικών – ΟΚΑΝΑ» για την παραβίαση της ασφάλειας προσωπικών δεδομένων. Ειδικότερα, έγγραφα με στοιχεία θεραπευομένων-μελών απορρίφθηκαν εκ παραδρομής, χωρίς προηγουμένως

να καταστραφούν, σε κάδους απορριμμάτων κατά τη διάρκεια της μετεγκατάστασης μονάδας του ΟΚΑΝΑ. Απόφαση 114/2012.

γ) Δεν θα πρέπει να αφήνονται εκτεθειμένα, χωρίς επίβλεψη, έγγραφα και φορητά μέσα αποθήκευσης πάνω σε γραφεία.

Προστασία φορητών μέσων αποθήκευσης

Πρέπει να λαμβάνονται τα κατάλληλα μέτρα για τη φυσική ασφάλεια και προστασία των φορητών αποθηκευτικών μέσων – όπως να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση και να είναι πάντα υπό επίβλεψη κατά τη διάρκεια της χρήσης τους.

Εναλλακτικές εγκαταστάσεις

Τα ανωτέρω μέτρα ελέγχου φυσικής πρόσβασης και περιβαλλοντικής ασφαλείας θα πρέπει να εφαρμόζονται και στις εναλλακτικές εγκαταστάσεις και εξοπλισμό που χρησιμοποιεί ο υπεύθυνος επεξεργασίας στο πλαίσιο του σχεδίου ανάκαμψης από καταστροφές.

VII. Ενδεικτικές αποφάσεις Αρχής προστασίας προσωπικών δεδομένων

<u>Απόφαση 59/2012</u>: Παραβίαση προσωπικών δεδομένων σε εταιρεία παραγωγής φωνογραφημάτων, φορέων ήχου και εικόνας (Sony)

Τον Μάιο του 2011 διαπιστώθηκε, κατόπιν δημοσιευμάτων στον τύπο και σχετικών αναρτήσεων στο διαδίκτυο (διαδικτυακή έκδοση του περιοδικού Pcworld, άρθρο με τίτλο «Θύμα hacking το Ελληνικό site της Sony Music», ότι υπήρξε περιστατικό παραβίασης προσωπικών δεδομένων των εγγεγραμμένων χρηστών του διαδικτυακού τόπου της εταιρείας Sony Music Entertainment Α.Ε. (εφεξής «Sony»). Στοιχεία για την παραβίαση είχαν ήδη αναρτηθεί από την προηγούμενη ημέρα σε ιστοσελίδες όπου δραστηριοποιούνται ομάδες "hacker" ή δημοσιεύονται στοιχεία για αυτούς. Ο αριθμός των χρηστών, των οποίων τα δεδομένα διέρρευσαν, ανέρχεται σε 8.385. Τα δεδομένα που διέρρευσαν αφορούν σε όνομα χρήστη (user name), κωδικούς πρόσβασης (password) για την είσοδο στην συγκεκριμένη ιστοσελίδα, διευθύνσεις e-mail και τηλεφωνικούς αριθμούς.

Από τον επιτόπιο έλεγχο διαπιστώθηκαν κενά στην πολιτική ασφαλείας και ιδίως στην εφαρμογή των μέτρων ασφαλείας, που επέτρεψαν την παραβίαση. Ειδικότερα, διαπιστώθηκε ότι α) τα αρχεία καταγραφής δεν παρακολουθούνταν από την Sony με αποτέλεσμα να μη γίνουν αντιληπτές επιθέσεις και παραβιάσεις ασφάλειας σε διάστημα 3 ετών, β) η πολιτική ασφαλείας δεν εφαρμόστηκε στον διαδικτυακό τόπο της Sony, γ) οι κωδικοί πρόσβασης των εγγεγραμμένων χρηστών του διαδικτυακού τόπου της Sony δεν ήταν κρυπτογραφημένοι, δ) παρά την ύπαρξη διαρκούς υποστήριξης σε επίπεδο εφαρμογών η Sony δεν είχε διασφαλίσει το απαιτούμενο επίπεδο ασφάλειας των δεδομένων κατά την επεξεργασία τους από τον εκτελούντα την επεξεργασία και ειδικά κατά την ανάπτυξη του κώδικα λογισμικού του διαδικτυακού τόπου της, με αποτέλεσμα ο τελευταίος να είναι ευάλωτος σε επιθέσεις τύπου SQL Injection και Cross-site Scripting (XSS) και ε) η δυνατότητα πρόσβασης μέσω VPN δεν έχει χρησιμοποιηθεί ποτέ. Τα ανωτέρω διευκολύνουν τη μη εξουσιοδοτημένη πρόσβαση στα παραπάνω δεδομένα.

<u>Ως προς τη βαρύτητα του περιστατικού</u>, η Αρχή έκρινε ότι αυτή αυξάνεται από το γεγονός ότι α) το περιστατικό αφορά μεγάλο αριθμό ατόμων (8385 εγγεγραμμένοι χρήστες), β) τα δεδομένα που διέρρευσαν γνωστοποιήθηκαν σε μεγάλο αριθμό ατόμων (μέσω διαδικτύου) και αποτέλεσαν αντικείμενο επιτυχών προσπαθειών υποκλοπής ταυτότητας, γ) υπήρχαν προηγούμενα περιστατι-

κά ασφάλειας, τα οποία δεν έγιναν ποτέ αντιληπτά, δ) η επίθεση στη Sony ήταν η 8η παγκοσμίως κατά του ομίλου Sony, με την 1η να έχει γίνει στις 4/4/2011 και την 7η στις 21/5/20116, άρα η εταιρεία ήταν εν γνώσει της ότι υφίσταται διαδικτυακές επιθέσεις διεθνώς και ε) στα δεδομένα που διέρρευσαν περιλαμβάνονται και κωδικοί πρόσβασης χρηστών, συνοδευόμενοι τόσο από όνομα χρήστη όσο και από διεύθυνση ηλεκτρονικού ταχυδρομείου, καθιστώντας κατ' αυτόν τον τρόπο εφικτή τη μη εξουσιοδοτημένη πρόσβαση στους συγκεκριμένους αλλά και σε άλλους λογαριασμούς των χρηστών σε διάφορες ηλεκτρονικές υπηρεσίες του διαδικτύου, καθώς πολλοί χρήστες συνηθίζουν να χρησιμοποιούν κοινούς κωδικούς πρόσβασης και κοινά ονόματα χρηστών για διαφορετικές ηλεκτρονικές υπηρεσίες, στις οποίες διατηρούν λογαριασμό.

Η Αρχή τελικώς επέβαλε πρόστιμο στη Sony ύψους €10.000, αφού έλαβε υπόψη της το γεγονός ότι **α)** η Sony έλαβε αμέσως μέτρα για την αντιμετώπιση του περιστατικού. *Ειδικότερα, μετά τη διαπίστωση του περιστατικού ο διαδικτυακός τόπος κατέστη άμεσα ανενεργός, ενώ* **β)** δόθηκε πλήρης πρόσβαση σε όλα τα αρχεία του διαδικτυακού τόπου σε εξειδικευμένο συνεργάτη (Guidance Software Inc) της μητρικής εταιρείας (Sony Music), ως πραγματογνώμονα, ο οποίος ανέλαβε να αναλύσει και να αξιολογήσει το περιστατικό. Ο διαδικτυακός τόπος της παραμένει μέχρι τη στιγμή της παρούσης ανενεργός σε αναμονή της απόφασης της Αρχής και της εκ νέου υλοποίησης του σε άλλη, πιο ασφαλή πλατφόρμα με βάση τις οδηγίες της μητρικής εταιρείας του ομίλου Sony. **γ)** Η Sony ενημέρωσε για το συμβάν μέσω ανακοίνωσης στον τύπο. **δ)** Η Sony πέτυχε, εντός δύο ημερών από την ίδια διαπίστωση του περιστατικού και εντός τριών ημερών από την ανάρτηση των διαρρευσάντων δεδομένων από τους hackers την απενεργοποίηση της ιστοσελίδας των hackers που είχε παράνομα αναρτήσει τα δεδομένα. Η Αρχή δηλαδή εφάρμοσε το άρθρο 10 του ν. 2472/1997, συνεκτιμώντας όσα ο ν. 3471/2006 προβλέπει για τους φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών υπηρεσιών.

Η Sony καταδικάστηκε και στη Μεγάλη Βρετανία για παραβίαση προσωπικών δεδομένων των χρηστών της. Συγκεκριμένα, της επιβλήθηκε πρόστιμο **250.000 λιρών,** επειδή δεν προστάτευσε επαρκώς τα προσωπικά δεδομένα των χρηστών του PlayStation Network που συνδέει τις κονσόλες του παιχνιδιού στο διαδίκτυο.

Η διαδραστική πύλη που συνδέει το PlayStation 3 με παιχνίδια και ταινίες στο Internet δέχτηκε τον Απρίλιο του 2011 επίθεση κυβερνοπειρατών που υπέκλεψαν τα προσωπικά στοιχεία εκατομμυρίων χρηστών, όπως το όνομα, τη διεύθυνση κατοικίας, τη διεύθυνση ηλεκτρονικού ταχυδρομείου, την ημερομηνία γέννησής τους και τους κωδικούς πρόσβασης. Σύμφωνα με τον Αναπληρωτή Διευθυντή του Γραφείου Επιτρόπου Πληροφοριών (ICO) της Βρετανίας «Τα μέτρα ασφαλείας που ελήφθησαν απλώς ήταν ανεπαρκή», τονίζοντας περαιτέρω ότι «πρόκειται για μια επιχείρηση που εμπορεύεται την τεχνική της εμπειρία και δεν υπάρχει καμία αμφιβολία, σύμφωνα με τη δική μου άποψη, ότι είχε την τεχνογνωσία και τις δυνατότητες να προστατεύσει τις πληροφορίες της», προσθέτοντας επίσης ότι «Η υπόθεση είναι από τις σοβαρότερες που έχουμε ποτέ χειριστεί. Έχει επηρεάσει άμεσα ένα μεγάλο αριθμό πελατών και τους δημιούργησε σοβαρά προβλήματα».

<u>Απόφαση 60/2011</u>: Παραβίαση προσωπικών δεδομένων από Οργανισμό Υγείας (Ινστιτούτο Υγείας Παιδιού)

Το Ινστιτούτο Υγείας του Παιδιού (εφεξής ΙΥΠ) ενημέρωσε την Αρχή σχετικά με παραβίαση προσωπικών δεδομένων, λόγω κλοπής, στις 8-04-2009, τεσσάρων (4) ηλεκτρονικών υπολογιστών,

στους οποίους ήταν καταχωρημένα ευαίσθητα προσωπικά δεδομένα υγείας παιδιών, όπως ονοματεπώνυμο του παιδιού, την ημερομηνία γέννησης, την εθνικότητα, τον ασφαλιστικό φορέα, αριθμούς τηλεφώνων και την αιτία επίσκεψης στο Κέντρο Υγείας. Στα παραπάνω ηλεκτρονικά αρχεία τηρούνταν προσωπικά δεδομένα 2050 παιδιών.

Το ΙΥΠ είχε λάβει ορισμένα μέτρα φυσικής ασφάλειας (συναγερμός), αλλά και τεχνικά μέτρα ασφάλειας (χρήση προσωπικών συνθηματικών ανά υπολογιστή, αντιϊκό πρόγραμμα) για την προστασία τόσο των τηρούμενων δεδομένων όσο και του πληροφοριακού εξοπλισμού του. Παρά ταύτα, ο συναγερμός δε λειτούργησε την ημέρα του περιστατικού.

Η σοβαρότητα της παραβίασης αυξάνεται από το γεγονός ότι α) τα δεδομένα που διέρρευσαν περιέχουν και δεδομένα υγείας, δηλαδή ευαίσθητα προσωπικά δεδομένα, β) το περιστατικό αφορά μεγάλο αριθμό ατόμων (2050 παιδιά που ήταν καταχωρημένα στα αρχεία του κέντρου).

Η ΑΠΔΠΧ απηύθυνε προειδοποίηση στο ΙΥΠ, με την οποία ζητούσε από το ΙΥΠ να λάβει κατ' ελάχιστο τα οργανωτικά και τεχνικά μέτρα ασφάλειας και να ενημερώσει σχετικά την Αρχή εντός τριών (3) μηνών από την κοινοποίηση της Απόφασης

VIII. Προληπτική δράση της Αρχής Προστασίας Προσωπικών Δεδομένων

1. Άδεια ίδρυσης και λειτουργίας αρχείου με ευαίσθητα δεδομένα υγείας πασχόντων από νεοπλασία ασθενών που περιλαμβάνονται στο Εθνικό Αρχείο Νεοπλασιών.

Τον Ιούλιο του 2012 η ΑΠΔΠΧ χορήγησε στο ΚΕΕΛΠΝΟ άδεια ίδρυσης και λειτουργίας αρχείου με ευαίσθητα δεδομένα για την εκπλήρωση του σκοπού της τήρησης του Εθνικού Αρχείου Νεοπλασιών.

Ο υπεύθυνος επεξεργασίας τηρεί κεντρική βάση δεδομένων, στην οποία καταχωρούνται τα στοιχεία των ασθενών που πάσχουν από νεοπλασία μέσω ειδικής διαδικτυακής εφαρμογής. Η Αρχή έδωσε γενικές αλλά και ειδικές κατευθύνσεις ως προς τα απαραίτητα μέτρα ασφαλείας, που πρέπει να ληφθούν. Στην άδεια, μεταξύ άλλων, προβλέπεται ότι:

α) Ο υπεύθυνος επεξεργασίας οφείλει να χρησιμοποιεί τους πλέον σύγχρονους και ισχυρούς αλγόριθμους κρυπτογράφησης με κλειδιά επαρκούς μήκους κατά τη διατήρηση, αποθήκευση και μετάδοση των δεδομένων των ασθενών, σύμφωνα με τα ευρέως αποδεκτά διεθνή πρότυπα.

β) Τα στοιχεία των ασθενών που οδηγούν άμεσα ή έμμεσα στην ταυτοποίησή τους πρέπει να τηρούνται κρυπτογραφημένα στη βάση δεδομένων του υπευθύνου επεξεργασίας.

γ) Οι καταγραφείς πρέπει να ορίζονται επισήμως εγγράφως από τη διοίκηση του νοσοκομείου. Έχουν δικαίωμα πρόσβασης, κατόπιν ειδικής έγγραφης εξουσιοδότησης του υπευθύνου επεξεργασίας, μόνο στα στοιχεία της βάσης δεδομένων που αφορούν ασθενείς του οικείου νοσοκομείου ή ιδιωτικής κλινικής και μπορούν να τροποποιούν μόνο τα δεδομένα των ασθενών που έχουν καταχωρίσει οι ίδιοι στη βάση δεδομένων.

δ) Ο υπεύθυνος επεξεργασίας οφείλει να αποδίδει μοναδικό ατομικό λογαριασμό πρόσβασης σε κάθε εξουσιοδοτημένο χρήστη και να καταγράφει πλήρως σε σχετικό αρχείο κάθε πρόσβαση των εξουσιοδοτημένων χρηστών στα στοιχεία των ασθενών που τηρούνται στη βάση δεδομένων.

2. Δημιουργία και τήρηση ηλεκτρονικού μητρώου προσώπων που ασκούν επάγγελμα ραδιοηλεκτρονικού και ραδιοτεχνικού.

Παρόμοιες κατευθύνσεις δόθηκαν τον Νοέμβριο του 2012 και σε ερώτημα που απηύθυνε στην Αρχή το Υπουργείο Ανάπτυξης Ανταγωνιστικότητας, Υποδομών, Μεταφορών & Δικτύων για τη δη-

μιουργία και τήρηση ηλεκτρονικού μητρώου προσώπων που ασκούν επάγγελμα ραδιοηλεκτρονικού και ραδιοτεχνικού.

3. Πληροφοριακά συστήματα e-school και e-datacenter του Υπουργείου Παιδείας αναφορικά με την προστασία και την ασφάλεια των προσωπικών δεδομένων (ΑΠΔΠΧ 187/2012).

Τέλος, η Αρχή πραγματοποίησε έλεγχο στα πληροφοριακά συστήματα e-school και e-datacenter του Υπουργείου Παιδείας αναφορικά με την προστασία και την ασφάλεια των προσωπικών δεδομένων που τηρούνται και τυγχάνουν επεξεργασίας στο πλαίσιο των παραπάνω συστημάτων.

Βασικό χαρακτηριστικό των παραπάνω συστημάτων αποτελεί η συγκέντρωση των προσωπικών δεδομένων των μαθητών, των εκπαιδευτικών και των διοικητικών υπαλλήλων σε αντίστοιχες κεντρικές βάσεις δεδομένων που φιλοξενούνται στο κέντρο υπολογιστών του Υπουργείου, στις οποίες έχουν απομακρυσμένη πρόσβαση οι αρμόδιοι εμπλεκόμενοι φορείς όπως οι σχολικές μονάδες και οι διευθύνσεις πρωτοβάθμιας και δευτεροβάθμιας εκπαίδευσης, μέσω σχετικών διαδικτυακών εφαρμογών.

Συγκεκριμένα στο **πληροφοριακό σύστημα e-school** καταχωρούνται τα στοιχεία ταυτότητας των μαθητών και των γονέων-κηδεμόνων τους, τα στοιχεία κατοικίας (διεύθυνση) και επικοινωνίας, οι βαθμολογίες, οι απουσίες, οι ποινές, οι ηθικές αμοιβές, η διαγωγή, οι μετεγγραφές, το θρήσκευμα και δεδομένα που αφορούν την υγεία των μαθητών, ειδικά αυτά που σχετίζονται με μαθησιακές δυσκολίες και αναπηρίες. Καθόσον αφορά στο **εκπαιδευτικό προσωπικό της σχολικής μονάδας**, καταχωρούνται μόνο τα στοιχεία των αρμόδιων εκπαιδευτικών που αποτελούν χρήστες του συστήματος αυτού (παρότι το σύστημα διαθέτει λειτουργικότητα για τη δημιουργία μητρώου εκπαιδευτικών της σχολικής μονάδας) επειδή λειτουργεί το σύστημα e-datacenter, το οποίο περιλαμβάνει πλήρες μητρώο των εκπαιδευτικών της χώρας. Τα στοιχεία των τοπικών βάσεων δεδομένων των σχολικών μονάδων της χώρας μεταφέρονται, με χρήση της διαδικτυακής εφαρμογής, στην κεντρική βάση δεδομένων που τηρείται στο Υπουργείο.

Στο **πληροφοριακό σύστημα e-datacenter** καταχωρούνται στοιχεία ταυτότητας και επικοινωνίας του εκπαιδευτικού ή του διοικητικού υπαλλήλου, οικογενειακής κατάστασης, σπουδών, αξιοσημείωτου έργου, ηθικών αμοιβών, ποινών, αδειών, υπηρετήσεων, μετατάξεων, μεταθέσεων, αποσπάσεων, ειδικών εκπαιδευτικών ή διοικητικών καθηκόντων. Στο υποσύστημα των μεταθέσεων καταχωρούνται στοιχεία υγείας του εργαζομένου καθώς και της συζύγου και των τέκνων του, εφόσον υπάρχουν καθώς αποτελούν κριτήρια μετάθεσης. Στο υποσύστημα της διαχείρισης των δεδομένων περιλαμβάνονται πεδία για το θρήσκευμα και την υγεία των εργαζομένων στα οποία, σύμφωνα με τις δηλώσεις των εκπροσώπων του υπευθύνου επεξεργασίας, δεν καταχωρούνται δεδομένα.

Το πόρισμα του ελέγχου των παραπάνω συστημάτων, το οποίο εγκρίθηκε με την υπ' αριθ. 187/2012 Απόφαση, παρουσιάζει τα ευρήματα της Αρχής αναφορικά με ελλιπή μέτρα ασφάλειας και προστασίας προσωπικών δεδομένων που εντοπίστηκαν, τους κινδύνους που αυτά ενδέχεται να δημιουργήσουν καθώς και τις συστάσεις για την αντιμετώπιση των κινδύνων. Τα ευρήματα που εντοπίστηκαν αφορούν κυρίως σε ελλείψεις ως προς τις διαδικασίες και την οργάνωση της ασφάλειας, την πλημμελή εφαρμογή των μέτρων ασφάλειας και τη συστηματική επίβλεψή τους καθώς και ως προς την αυθεντικοποίηση των χρηστών και την διαχείριση και υποστήριξη των συστημάτων.

Συμπερασματικά, θα πρέπει να αναφερθεί ότι αυτά είναι λίγο – πολύ τα ευρήματα, που προκύπτουν μετά από κάθε έλεγχο της Αρχής ή μετά από την αντιμετώπιση συμβάντων παραβίασης προσωπικών δεδομένων. Άλλα ευρήματα είναι το ανεπαρκές σχέδιο ασφαλείας, η πλημμελής εφαρμογή υφιστάμενου σχεδίου, το ανεκπαίδευτο προσωπικό, τα ελλιπή μέτρα ασφαλείας κατά το σχεδιασμό των εφαρμογών σε Ιστοσελίδες καθώς και η ανάπτυξη εφαρμογών σε Ιστοσελίδες, που είναι ευάλωτες σε ηλεκτρονικές επιθέσεις.

Ο προβληματισμός που τίθεται συχνά είναι κατά πόσον η διαπίστωση μιας διαρροής είναι αρκετή, προκειμένου η Αρχή να επιβάλει τις προβλεπόμενες στο νόμο κυρώσεις, ή αν υπήρξε παραβίαση εκ μέρους του υπεύθυνου επεξεργασίας της υποχρέωσής του να λαμβάνει και να τηρεί τα κατάλληλα μέτρα ασφαλείας, ανάλογα πάντοτε με τις συνθήκες και ειδικότερα ανάλογα με τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Διότι είναι αυτονόητο ότι είναι διαφορετικό το επίπεδο ασφαλείας που πρέπει να τηρείται π.χ. στην Γενική Γραμματεία Πληροφοριακών Συστημάτων ή σε ένα νοσοκομείο και διαφορετικό εκείνο που πρέπει να τηρεί μια μεσαία ελληνική επιχείρηση λ.χ. του κλάδου των κατασκευών ή της εστίασης.

Σας ευχαριστώ πολύ!

«Profiling στα κοινωνικά δίκτυα»

κ. **Λίλιαν Μήτρου,** Αναπληρώτρια Καθηγήτρια,
Πανεπιστήμιο Αιγαίου / Οικονομικό Πανεπιστήμιο Αθηνών

Περίληψη

Έννοια, εφαρμογές και τεχνικές του Profiling

Το profiling θα μπορούσε εν γένει να προσδιοριστεί ως μία διαδικασία εξεύρεσης συσχετισμών μεταξύ δεδομένων. Μέσω της διαδικασίας αυτής δημιουργούνται μορφότυποι (profiles) με τρόπο ώστε να συσχετίζονται με άλλα δεδομένα για να προσδιοριστεί ή/και να ταυτοποιηθεί ένα φυσικό πρόσωπο. Αν και έχει διαπιστωθεί και διατυπωθεί η ανάγκη προστασίας των μορφότυπων και ρύθμισης του profiling δεν υφίσταται ακόμη ένας νομικά δεσμευτικός ορισμός αυτής της διαδικασίας. Σύμφωνα με τη σχετική Σύσταση (2010) 13 του Συμβουλίου της Ευρώπης ως μορφότυπος (profile) ορίζεται ένα σύνολο δεδομένων που χαρακτηρίζει μία κατηγορία ατόμων με σκοπό την εφαρμογή του σε ένα άτομο ενώ το profiling αναφέρεται στη διαδικασία αυτοματοποιημένης επεξεργασίας δεδομένων που συνίσταται στην αντιστοίχιση ενός profile σε ένα άτομο, ιδίως με σκοπό να ληφθούν αποφάσεις που το αφορούν ή για να αναλυθούν ή να προβλεφθούν οι προτιμήσεις, συμπεριφορές και στάσεις του.

Πρακτικές profiling χρησιμοποιούνται σε μία ευρύτατη γκάμα περιπτώσεων Μορφότυποι παράγονται και χρησιμοποιούνται για τους σκοπούς της διαφήμισης εδώ και δεκαετίες αλλά και πιο πρόσφατα προς διευκόλυνση της άμεσης και στοχευμένης διαφήμισης. Οι μέθοδοι χρησιμοποιούνται περαιτέρω ευρέως για την υποστήριξη της εφαρμογής του νόμου που συμπεριλαμβάνει α) την έρευνα και την ανακάλυψη στοιχείων κι εν γένει τη διερεύνηση του εγκλήματος, β) την καταστολή, γ) τον εντοπισμό και αξιολόγηση κινδύνων ή/και επικινδύνων προσώπων και την ανάπτυξη και υιοθέτηση μέτρων πρόληψης.

Το Profiling βασίζεται κυρίως στη λεγόμενη εξόρυξη δεδομένων (data mining) που συνίσταται στην αναζήτηση /έρευνα (μέσω «έξυπνων» αλγορίθμων κλπ.) προτύπων και συσχετισμών μεταξύ δεδομένων σε μεγάλα σύνολα ή βάσεις δεδομένων. Η εξόρυξη μετατρέπει τα πρωτογενή δεδομένα (raw data) σε πληροφορία και γνώση. Θα πρέπει ωστόσο να επισημάνουμε ότι οι συσχετισμοί που προκύπτουν δηλώνουν μία σχέση, δεν εντοπίζουν αιτίες ή λόγους για αυτούς τους συσχετισμούς. Έτσι, π.χ. στο πλαίσιο της πρόληψης ή/και καταστολής του εγκλήματος μέσω και της χρήσης τεχνολογιών αναγνώρισης προτύπων (pattern recognition technologies) γίνεται εφικτή η τυποποίηση της πιθανότητας τέλεσης εγκλημάτων ή η αναζήτηση πληροφορίας για άτομα ώστε να καταταχθούν σε προυφιστάμενους μορφότυπους .

Profiling στα κοινωνικά δίκτυα και κίνδυνοι για τα δικαιώματα

Τα ψηφιακά κοινωνικά δίκτυα, όπως το facebook, συνιστούν «φλέβα χρυσού» ως προς την εξόρυξη δεδομένων και την αξιοποίηση των μεθόδων profiling. Η ιδιαίτερη προστιθέμενη αξία των

κοινωνικών δικτύων ως προς την εξόρυξη δεδομένων και την άντληση γνώσης οφείλεται σε μία σειρά από παράγοντες: α) εκθετική αύξηση χρηστών και αντίστοιχα εκθετική αύξηση διαθέσιμης πληροφορίας, β) κουλτούρα διαμοιρασμού (προσωπικών) δεδομένων, κουλτούρα που σκοπίμως και επισταμένως καλλιεργούν οι φορείς σελίδων κοινωνικής δικτύωσης και η οποία ενισχύει ακόμη περισσότερο τον διαμοιρασμό πληροφορίας. Αυτό επίσης που αναδεικνύουν μελετητές αλλά και απλοί παρατηρητές των ψηφιακών κοινωνικών δικτύων είναι η – συνειδητή, ασυνείδητη ή υποσυνείδητη αυτο-έκθεση σε βαθμό πληροφοριακής επιδειξιομανίας (exhibitionism). Τέλος, ένα βασικό, εγγενές, χαρακτηριστικό των κοινωνικών δικτύων είναι η ευχερής απόσπαση, χρήση και αξιοποίηση της πληροφορίας από το αρχικό της πλαίσιο (de-contextualisation).

Όταν χρησιμοποιούνται μέθοδοι εξόρυξης δεδομένων στα κοινωνικά δίκτυα, ώστε να καταστεί δυνατή η δημιουργία και η αξιοποίηση για σκοπούς Profiling, τότε προκύπτουν σοβαρές επιπτώσεις για τα δικαιώματα των προσώπων. Μέσω του profiling παράγονται νέα, συχνά μάλιστα ευαίσθητα υπό την προσέγγιση του νόμου, δεδομένα. Προκύπτουν δε και παράγονται εκτός του αρχικού πλαισίου επεξεργασίας (και άρα και κρίσης ως προς τη νομιμότητα) και πέραν της γνώσης/προβλεψιμότητας των θιγόμενων προσώπων ως προς τον πληροφοριακό ορίζοντα αυτού ή αυτών που αποκτά και επεξεργάζεται τη νέα πληροφορία. Επίσης η κατηγοριοποίηση, η ένταξη των προσώπων σε ομάδες ή σε μορφότυπους συμπεριφοράς θέτουν ζητήματα ως προς τον –επιβαλλόμενο από το Σύνταγμα – σεβασμό της «αξίας του ανθρώπου» καθώς ένα πρόσωπο κινδυνεύει να αντιμετωπίζεται όχι ως αυτόνομη οντότητα αλλά ως φορέας ενός μορφότυπου.

Οι σοβαρότεροι κίνδυνοι του profiling εντοπίζονται ακριβώς στον πυρήνα των ιδιοτήτων του, δηλ. στη δυνατότητα χρήσης του ως προβλεπτικού και προληπτικού εργαλείου μέσω του χαρακτηρισμού, της κατηγοριοποίησης προσώπων και του καταμερισμού τους σε ομάδες με προσδιορισμένα χαρακτηριστικά. Υπό αυτήν την έννοια το profiling ενέχει την έκθεση στον κίνδυνο δυσμενούς διακριτικής μεταχείρισης και του κοινωνικού διαχωρισμού.

Το κανονιστικό πλαίσιο του Profiling

Οι κίνδυνοι περιορισμού και βλάβης δικαιωμάτων που συνεπιφέρει η χρήση μεθόδων profiling επιβάλλουν την τήρηση των αντίστοιχων κανονιστικών επιταγών. Το profiling προϋποθέτει ή και συνεπάγεται συχνά επεξεργασία προσωπικών δεδομένων, Η συλλογή και επεξεργασία ψηφιακών ιχνών (και σε δημόσια προσιτές σελίδες/προφίλ) συνιστά, χωρίς άλλο, επεξεργασία προσωπικών δεδομένων υπό την έννοια των σχετικών κανονιστικών κειμένων. Το Profiling, όπως και αυτή καθεαυτή η εξόρυξη δεδομένων (data mining) συνιστά επεξεργασία προσωπικών δεδομένων, εφόσον γίνεται ανάλυση/αξιολόγηση δεδομένων που αναφέρονται σε προσδιορισμένα ή προσδιορίσιμα πρόσωπα ή/και από το profiling /εξόρυξη προκύπτουν δεδομένα που αναφέρονται σε προσδιορισμένα ή προσδιορίσιμα πρόσωπα.

Κρίσιμη για την αξιολόγηση του Profiling ως προς την εναρμόνιση με τις επιταγές του εθνικού και ενωσιακού κανονιστικού πλαισίου αλλά και του άρθρου 8 της ΕΣΔΑ είναι η τήρηση ορισμένων αρχών. Τέτοιες αρχές είναι :

α) η αρχή της νομιμότητας. Ως νόμιμη βάση μπορεί να προσδιοριστεί η συγκατάθεση αλλά και' εξαίρεση και το «ζωτικό συμφέρον» ενός του προσώπου. Ακραία αλλά χαρακτηριστική τέτοια περίπτωση αποτελεί το profiling χάριν της πρόληψης μίας αυτοκτονίας αλλά παραμένει εξαιρετικά ασαφές, ποιος , υπό ποιες περιστάσεις και με ποιες εγγυήσεις μπορεί να κρίνει τη ότι συντρέχει τέτοια περίπτωση. Επίσης η εκπλήρωση έργου δημοσίου συμφέροντος και η χάριν αυτού

άσκηση δημόσιας εξουσίας [πρόληψη / διερεύνηση/ καταστολή εγκλήματος] συνιστά θεσμικά επαρκή λόγο για τη διαδικασία του profiling υπό την – συνταγματικά αυτονόητη – προϋπόθεση της πρόβλεψης σχετικών εγγυήσεων.

β) η αρχή του σκοπού με βάση την οποία θα πρέπει να κριθεί η χρήση δεδομένων που προκύπτουν από το profiling δημόσια προσιτών δεδομένων για σκοπούς ασύμβατους προς τον αρχικό σκοπό δημοσιοποίησης.

γ) η αρχή της αναλογικότητας: το profiling μεγάλου και απροσδιόριστου όγκου δεδομένων θέτει ζητήματα ως προς την αρχή της αναλογικότητας. Ως μείζον ερώτημα προκύπτει κατά πόσο και σε ποια έκταση είναι αποδεκτή η χρήση τέτοιων διεισδυτικών μεθόδων όχι μόνο για τη διερεύνηση μίας συγκεκριμένης υπόθεσης αλλά στο πλαίσιο μιας γενικευμένης πρόβλεψης/πρόληψης. Στο πλαίσιο αυτό εντάσσονται η τήρηση της Αρχής της φειδούς (data minimisation), του περιορισμού δηλ. των δεδομένων που χρησιμοποιούνται στο ελάχιστο αναγκαίο μέτρο αλλά και οι δυνατότητες για ανωνυμοποίηση και ψευδωνυμοποίηση των δεδομένων.

Η εισαγωγή και η αποδοχή μεθόδων profiling συνδέεται με την υιοθέτηση εγγυήσεων, όπως η τήρηση αντίστοιχων ουσιαστικών / διαδικαστικών προϋποθέσεων, π.χ. ως προς τα ευαίσθητα δεδομένα, η εκπλήρωση υποχρεώσεων ως προς τα δικαιώματα των προσώπων αλλά και η ρητή απαγόρευση του Profiling για ορισμένους σκοπούς .

Πρακτικές όπως το Profiling καθιστούν τα πρόσωπα ευρέως ιχνηλάσιμα με επιπτώσεις στη συμπεριφορά, στην απώλεια ελέγχου επί των ιδίων πληροφοριών, στην ελευθερία της έκφρασης, στην ελευθερία της επικοινωνίας και στην ανάπτυξη της προσωπικότητας – σε όσα δικαιώματα και ελευθερίες δηλ. συνιστούν ακριβώς το οξυγόνο της δημοκρατίας Συμπερασματικά πρέπει να παρατηρήσουμε ότι η εκτεταμένη επιτήρηση, η μετάβαση στη στρατηγική της πρόληψης απαιτεί ειδική στάθμιση, το λεγόμενο democracy test κατά το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (*πόσο είναι αναγκαίο ένα μέτρο στο πλαίσιο μιας δημοκρατικής κοινωνίας*), σαφείς νομοθετικές προβλέψεις και θεσμικό έλεγχο στο πλαίσιο ενός δημοκρατικού κράτους δικαίου.

ΦΥΛΛΑΔΙΑ

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Διαδίκτυο!
Ένα παγκόσμιο θαύμα!

Το Διαδίκτυο είναι ένα παγκόσμιο δίκτυο διασύνδεσης ηλεκτρονικών υπολογιστών και αποτελεί ένα από τα σύγχρονα θαύματα του κόσμου, καθώς είναι από τα πλέον βασικά εργαλεία στην καθημερινή ζωή του ανθρώπου, και σιγά σιγά επηρεάζει κάθε ανθρώπινη δραστηριότητα. Είναι ένα παράθυρο στον κόσμο που προσφέρει άπειρες υπηρεσίες με πολύ μικρό κόστος! Ας δούμε, όμως, μαζί τα θετικά του Διαδικτύου!

- Το Διαδίκτυο έφερε την επανάσταση στην επικοινωνία, μειώνοντας στο ελάχιστο το κόστος της και αυξάνοντας την ταχύτητά της. Οι αποστάσεις εκμηδενίζονται και οι άνθρωποι μπορούν να μιλήσουν με τους φίλους και τους παλιούς τους σύμμαθητές παγκοσμίως, άμεσα και αμφίδρομα, με το πάτημα ενός κουμπιού! Επιπλέον, μπορούν να δημοσιεύσουν ελεύθερα και δωρεάν τα κείμενά τους, ανταλλάσσοντας απόψεις πάνω σε κάθε είδους θέμα!

- Η πιο εντυπωσιακή, ωστόσο, δυνατότητα που προσφέρει το Διαδίκτυο είναι η περιήγηση στον παγκόσμιο ιστό (WEB), η άντληση πληροφοριών και η ενημέρωση που προσφέρουν οι διάφοροι ιστότοποι. Έτσι, οι χρήστες μπορούν να επισκέπτονται τους ιστοτόπους αυτούς και να ενημερώνονται για θέματα που τους ενδιαφέρουν, για παρεχόμενες υπηρεσίες, για προϊόντα τα οποία θέλουν να αγοράσουν, για δραστηριότητες εκπαιδευτικών ιδρυμάτων, για νόμους και κανονισμούς κυβερνητικών υπηρεσιών, και πολλά άλλα. Επίσης, ο χρήστης μπορεί απλώς με ένα «κλικ» από την άνεση του σπιτιού του, να ανατρέξει σε κατάλληλες πηγές ή βιβλία που ίσως να μην είχε πριν άμεσα στη διάθεση του και μέσα σε λίγα δευτερόλεπτα να βρει πληροφορίες για οποιοδήποτε θέμα μπορεί να τον ενδιαφέρει!

- Πολύ σημαντικές είναι και οι δυνατότητες που προσφέρει το Διαδίκτυο για μόρφωση και επιμόρφωση. Όλο και περισσότερες βιβλιοθήκες διαθέτουν on line τους καταλόγους των βιβλίων τους. Όσοι ενδιαφέρονται, μπορούν με τη βοήθεια της μηχανής αναζήτησης να βρουν πού υπάρχει το βιβλίο που χρειάζονται. Ορισμένες μάλιστα βιβλιοθήκες επιτρέπουν ακόμα και να δανείζεται κάποιος βιβλία on line.

- Επιπλέον, το Διαδίκτυο διευκολύνει την καθημερινότητα. Πολλοί είναι εκείνοι που κάνουν αγορές μέσω του Διαδικτύου, τακτοποιούν τραπεζικά ζητήματα και γενικά διεκπεραιώνουν εργασίες που υπό διαφορετικές συνθήκες θα απαιτούσαν πολύ χρόνο.

- Οι δυνατότητες που προσφέρει το Διαδίκτυο, δεν έχουν μόνο θεωρητική αξία, αφού με το Διαδίκτυο κάποιος μπορεί να εργάζεται μακριά από τον παραδοσιακό εργασιακό χώρο με τη νέα μορφή εργασίας, την τηλεργασία. Οι επαγγελματίες που μπορούν να εκτελέσουν εργασίες μέσω του Διαδικτύου είναι πολλοί, συγγραφείς, δημοσιογράφοι, μεταφραστές κ.λπ.

Πρωτοποριακές και αποτελεσματικές μέθοδοι διδασκαλίας επιστρατεύουν το Διαδίκτυο και συντελούν στην καλύτερη δυνατή γνώση και μάθηση μέσω εξελιγμένων συστημάτων τηλεκπαίδευσης.

- Το Διαδίκτυο, επίσης, δεν είναι μόνο για τους νέους, αλλά και για άτομα της τρίτης ηλικίας. Η χρήση νέων τεχνολογιών δεν διευκολύνει μόνο την καθημερινή ζωή των ηλικιωμένων, αλλά, όπως δείχνουν τα αποτελέσματα μελετών, η περιήγηση στο Διαδίκτυο μπορεί να συμβάλει στη βελτίωση της γνωστικής λειτουργίας και να έχει θετική επίδραση στην κατάθλιψη, την αίσθηση μοναξιάς.

- Μέσα από το Διαδίκτυο μπορούμε, τέλος, να ψυχαγωγηθούμε: να παίξουμε παιχνίδια, να ακούσουμε τραγούδια, να βρούμε παραστάσεις που μας ενδιαφέρουν, να κλείσουμε εισιτήρια για τον κινηματογράφο. Κι όλα αυτά από την άνεση του σπιτιού μας!

- Χρησιμοποιώντας το Διαδίκτυο, με ένα μόνο «κλικ» μπορούμε να βρεθούμε σε οποιαδήποτε χώρα! Να δούμε ξένους πολιτισμούς, εικόνες από άλλες χώρες, να διαβάσουμε για την ιστορία ξένων λαών! Παράλληλα, μπορούμε να οργανώσουμε τα ταξίδια μας! Να κλείσουμε εισιτήρια και ξενοδοχεία σε χαμηλές τιμές, να διαβάσουμε ταξιδιωτικές εμπειρίες άλλων ανθρώπων και να γράψουμε τις δικές μας!

- Μέσα από την ψηφιοποίηση των δεδομένων, μπορούμε να αναζητήσουμε δημόσια έγγραφα που μας αφορούν, σε λίγα μόλις δευτερόλεπτα! Να υποβάλουμε αιτήσεις και να αποστείλουμε έγγραφα, γλυτώνοντας χρόνο, κόπο και χρήματα.

Η Υπηρεσία μας συστήνει:
ΝΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ αλλά ΜΕ ΠΡΟΫΠΟΘΕΣΕΙΣ!

Αρνητικά του Διαδικτύου!

Παιδική πορνογραφία
Άτομα υπεράνω πάσης υποψίας αποκτούν την εμπιστοσύνη των παιδιών, προκαλούν συζητήσεις σεξουαλικής φύσεως και στέλνουν φωτογραφίες ως κάτι το αποδεκτό και φυσιολογικό. Είναι πραγματικά όμως αυτοί που παρουσιάζονται;

Ψηφιακή παρενόχληση
Παρενόχληση, δυσφήμιση, διάδοση ψευδών φημών από άτομα που προσπαθούν να ελέγξουν ψυχολογικά τα θύματά τους.

Αυτοκτονίες
Σε 5 χρόνια πάνω από 378 άτομα έχουν εκδηλώσει πρόθεση ν' αυτοκτονήσουν.

Chat room
Η χρήση των ψευδωνύμων επιτρέπει τη διατήρηση της ανωνυμίας. Η ψευδαίσθηση της ασφάλειας, όμως, μπορεί να μετατρέψει τον τρόπο επικοινωνίας σε μία από τις μεγαλύτερες και πιο επικίνδυνες παγίδες του Διαδικτύου. Οι μόνες αληθινές φιλίες βρίσκονται στην πραγματική ζωή και δοκιμάζονται στον πραγματικό κόσμο και τον πραγματικό χρόνο.

Οικονομικές απάτες
E-mail με παραπλανητικό περιεχόμενο, υποσχόμενα τεράστιες κληρονομιές, υποκλοπές κωδικών ασφαλείας και pin πιστωτικών καρτών, υπέρογκες χρεώσεις, απατηλές αγορές! Στο Διαδίκτυο ίσως κάποιοι προσπαθήσουν να σας παραπλανήσουν!

Παραβίαση προσωπικών δεδομένων
Βομβαρδισμός διαφημιστικών μηνυμάτων μέσω Διαδικτύου, αλόγιστη χρήση καμερών παρακολούθησης, παραβίαση δεδομένων υγείας και οικονομικών, υποκλοπή κωδικών και φωτογραφιών από λογαριασμούς χρηστών σε ιστοσελίδες κοινωνικής δικτύωσης.

Ιστοσελίδες κοινωνικής δικτύωσης
Στους όρους χρήσης αναγράφεται ότι οι χρήστες αποποιούνται τα πνευματικά δικαιώματά τους για περιεχόμενο που ανεβαίνει σε ιστοσελίδες κοινωνικής δικτύωσης. Επίσης, δεν παρέχεται εγγύηση για την ασφάλεια ούτε και για τη μυστικότητα των εφαρμογών!

Εθισμός στο Διαδίκτυο
Ο εθισμός στο Διαδίκτυο αποτελεί ένα διαρκώς διογκούμενο φαινόμενο της εποχής μας, το οποίο πλήττει κυρίως τους εφήβους ή τους ενήλικες που έρχονται πρώτη φορά σε επαφή με το Διαδίκτυο και δεν έχουν αναπτύξει αντιστάσεις. Είναι μια σχετικά νέα μορφή εξάρτησης, η οποία παρασύρει ενήλικες αλλά και μικρά παιδιά σε μια άλλη πραγματικότητα, δημιουργεί αποξένωση και μονομανία. Αποτέλεσμα είναι η παραμέληση των υποχρεώσεων, η αδιαφορία για τον πραγματικό κόσμο ή, ακόμα, πονοκέφαλοι και ξηρότητα στα μάτια, που δημιουργούνται από τις πολλές ώρες μπροστά στον υπολογιστή.

Ποια είναι, όμως, η ορθή χρήση του Διαδικτύου;
Μη διακόπτετε τη χρήση, αλλά μάθετε να θέτετε όρια, και αρχίστε και πάλι την ενασχόληση με άλλες δραστηριότητες μακριά από τον υπολογιστή. Μια μέρα εκτός Διαδικτύου μπορεί να σας φανεί πιο ενδιαφέρουσα και πιο διασκεδαστική. Μια ώρα τη μέρα στο Διαδικτύο θεωρείται αρκετή για την διαδικτυακή ενημέρωση και ψυχαγωγία του χρήστη. Μην ξεχνάτε ότι το χρόνο που περνάτε μπροστά στον υπολογιστή, συνήθως τον στερείτε από κάποιον αγαπημένο σας.
Ο ρόλος των γονέων είναι πάρα πολύ σημαντικός τόσο για την πρόληψη, όσο και για την αντιμετώπιση του εθισμού των παιδιών τους στο Διαδίκτυο. Όσον αφορά την πρόληψη, το σημαντικότερο πράγμα που χρειάζεται να κάνουν οι γονείς προκειμένου να μπορούν να ελέγχουν αποτελεσματικά τη χρήση του Διαδικτύου από τα παιδιά τους, είναι να γνωρίσουν οι ίδιοι το μέσο.

Συμβουλές για τους γονείς!

- Προτιμήστε να τοποθετήσετε τον υπολογιστή σας σε χώρους όπως είναι το σαλόνι, και όχι στο υπνοδωμάτιο του παιδιού. Έτσι, θα έχετε τη δυνατότητα να επιβλέπετε το παιδί σας, χωρίς το ίδιο να αισθάνεται ότι ελέγχεται.
- Κάντε την πλοήγηση στο Διαδίκτυο οικογενειακή δραστηριότητα. Χρησιμοποιήστε τον υπολογιστή μαζί με τα παιδιά σας.
- Ενημερώστε τα παιδιά σας για τους κινδύνους που ελλοχεύουν όταν συνομιλούν με αγνώστους μέσω chatrooms.
- Συζητήστε με τα παιδιά σας για θέματα ασφάλειας (επικοινωνία με επικίνδυνα άτομα, πρόσβαση σε sites με βλαβερό περιεχόμενο) που προκύπτουν από την πλοήγηση στο Διαδίκτυο.
- Διδάξτε τα να μη δίνουν προσωπικές πληροφορίες χωρίς την άδειά σας (επίθετο, όνομα, ηλικία, διεύθυνση κατοικίας, αριθμό τηλεφώνου, οικογενειακό εισόδημα, ωράρια σχολείου, ονόματα φίλων κ.λπ.).

- Μη δίνετε στα παιδιά την πιστωτική σας κάρτα για να τη χρησιμοποιήσουν σε διαδικτυακές συναλλαγές.
- Μην επιτρέπετε ποτέ στα παιδιά σας να συναντηθούν με άτομα που γνώρισαν μέσω Διαδικτύου. Διδάξτε τα να αρνούνται από μόνα τους να συναντηθούν προσωπικά με άτομα που έχουν γνωρίσει στο Διαδίκτυο. Εξηγήστε τους ότι οι άγνωστοι με τους οποίους θέλουν να συναντηθούν μπορεί, να είναι επικίνδυνοι.
- Χρησιμοποιήστε τα λεγόμενα «φίλτρα», που είναι ειδικά προϊόντα λογισμικού με σκοπό την παρεμπόδιση της πρόσβασης σε μη επιθυμητά sites (βία, πορνογραφία).

- Ελέγξτε το περιεχόμενο οπτικοακουστικού υλικού, όπως CDs, δισκέτες κ.ά., που αγοράζουν τα παιδιά σας ή ανταλλάσσουν με τους φίλους τους.
- Μείνετε κοντά στα παιδιά σας και εμπλακείτε σε κάθε δική τους διαδικτυακή δραστηριότητα, με τον ίδιο τρόπο που κάνετε για τις δραστηριότητες του σχολείου.

Μιλήστε με το παιδί σας και κάντε το να συνειδητοποιήσει ότι, αν προκύψει κάτι ξαφνικό ή ενοχλητικό στο Διαδίκτυο, πρέπει να κλείσει την ηλεκτρονική σελίδα.

Συμβουλές για τα παιδιά!

- Το Διαδίκτυο μορφώνει και ψυχαγωγεί. Ωστόσο, μπορεί να δημιουργηθούν και προβλήματα αν υπάρξει ασυδοσία στον τρόπο που χρησιμοποιείται. Γι' αυτό:

- Μη δίνεις σε κανέναν, ακόμα και στον καλύτερό σου φίλο, τους κωδικούς πρόσβασής σου στο Διαδίκτυο. Τα μόνα άτομα που θα πρέπει να γνωρίζουν τους κωδικούς πρόσβασής σου είναι οι γονείς σου.
- Μην απαντάς σε ηλεκτρονικά μηνύματα που σε κάνουν να αισθανθείς άβολα. Σε περίπτωση που λάβεις ένα τέτοιο μήνυμα, μη διστάσεις να το πεις στους γονείς σου ή σε κάποιο πρόσωπο που εμπιστεύεσαι.
- Αν αισθανθείς άβολα την ώρα που συνομιλείς μέσω chatroom, διάκοψε αμέσως τη συνομιλία.
- Απόφυγε να στείλεις τη φωτογραφία και τα προσωπικά στοιχεία σου μέσω Διαδικτύου σε άγνωστο.
- Σιγουρέψου για τις γνωριμίες σου στο Διαδίκτυο. Να θυμάσαι ότι τα άτομα που γνωρίζεις μπορεί να μην είναι αυτά που λένε ότι είναι!
- Αν κάποιος σε παρενοχλεί, θυμήσου ότι μπορείς να βγεις από τον ιστότοπο με ένα απλό «κλικ»!
- Σκέψου πολύ καλά πριν αποφασίσεις να συναντηθείς με κάποιο άτομο που γνώρισες στο Διαδίκτυο. Ζήτησε την άποψη των γονιών σου σχετικά με αυτό το θέμα.
- Σε περίπτωση που αποφασίσεις να συναντηθείς με τον «διαδικτυακό σου φίλο», ενημέρωσε τους γονείς σου ή κάποιο άτομο που εμπιστεύεσαι, και φρόντισε αυτή η συνάντηση να γίνει σε δημόσιο χώρο.
- Μην εμπιστεύεσαι αμέσως ό,τι βλέπεις στο Διαδίκτυο.
- Μίλησε στους γονείς σου για τα όσα βλέπεις και ζεις όταν «σερφάρεις» στο Διαδίκτυο.

ΕΠΙΚΟΙΝΩΝΙΑ: Δίωξη Ηλεκτρονικού Εγκλήματος - Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, e-mail: ccu@cybercrimeunit.gov.gr, τηλ.: 11012, fax: 210 6476462

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ
ΚΑΙ ΝΟΜΟΘΕΣΙΑ

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ ΚΑΙ ΝΟΜΟΘΕΣΙΑ

1. ΑΠΟΣΤΟΛΗ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ ΚΑΙ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ (ΥΠ.Ο.Α.Δ.Η.Ε.)

Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος είναι αυτοτελής Κεντρική Υπηρεσία της Ελληνικής Αστυνομίας με αποστολή τη διερεύνηση, εξιχνίαση και δίωξη εγκλημάτων που τελέστηκαν σε βάρος των συμφερόντων του Δημοσίου και της Εθνικής Οικονομίας ή έχουν τα χαρακτηριστικά του οργανωμένου οικονομικού εγκλήματος, καθώς και οποιαδήποτε εγκλήματα διαπράττονται με τη χρήση του Διαδικτύου. Υπάγεται απευθείας στον Αρχηγό της Ελληνικής Αστυνομίας και εποπτεύεται στην προανακριτική της δράση από τον Εισαγγελέα του Οργανωμένου Εγκλήματος. Η Υπηρεσία Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΠ.Ο.Α.Δ.Η.Ε.) εδρεύει στην Αθήνα, στον 13ο και 14ο όροφο του Αστυνομικού Μεγάρου Αθηνών, στη Λεωφόρο Αλεξάνδρας 173. Η τοπική της αρμοδιότητα εκτείνεται σε όλη την Ελλάδα. Η ΥΠ.Ο.Α.Δ.Η.Ε αποτελείται από το Επιτελείο, καθώς επίσης και από τους δύο επιχειρησιακούς τομείς αστυνομικής δράσης, την Υποδιεύθυνση Οικονομικής Αστυνομίας και την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος. Προϊστάμενος της Υπηρεσίας Οικονομικής Αστυνομίας και Δίωξης Ηλεκτρονικού Εγκλήματος είναι ο Ταξίαρχος ΓΕΩΡΓΑΤΖΗΣ Δημήτριος.
Η αποστολή της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος περιλαμβάνει την πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών που διαπράττονται μέσω του Διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Διευθυντής της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος είναι ο Αστυνομικός Διευθυντής ΣΦΑΚΙΑΝΑΚΗΣ Εμμανουήλ.
Το παρόν φυλλάδιο έχει ως στόχο να παρουσιάσει συνοπτικά τις βασικές αρχές του Διαδικτύου και το νομικό πλαίσιο που εφαρμόζεται σε εγκλήματα που διαπράττονται μέσα από αυτό. Η σύνταξη του παρόντος φυλλαδίου έγινε με τη σύμφωνη γνώμη της Προϊσταμένης της Εισαγγελίας Πρωτοδικών Αθηνών, κας ΦΑΚΟΥ Παναγιώτας.

2. ΔΙΑΔΙΚΤΥΑΚΟΙ ΟΡΟΙ

ΕΙΣΑΓΩΓΙΚΑ ΣΤΟΙΧΕΙΑ-ΟΡΙΣΜΟΙ
ΔΙΑΔΙΚΤΥΟ

Το Διαδίκτυο (INTERNET-INTERconnected NETwork) είναι ένα παγκόσμιο δίκτυο στο οποίο είναι συνδεδεμένα μεταξύ τους πολλά άλλα μικρά ή μεγάλα δίκτυα υπολογιστών.

MODEM: Το modem είναι η συσκευή που επιτρέπει την πρόσβαση στο Διαδίκτυο. Το μόντεμ (ελλ. Δια/αποδιαμορφωτής, αγγλ. modem) είναι όρος που προέρχεται από τα αρχικά των αγγλικών λέξεων modulate/demodulate. Περιγράφει τη συσκευή η οποία μετατρέπει το ψηφιακό σήμα του υπολογιστή-αποστολέα σε αναλογικό, για να μπορέσει να μεταφερθεί μέσω τηλεφωνικών γραμμών στον υπολογιστή-δέκτη. Επίσης, διαθέτει τμήμα αποδιαμόρφωσης για την αντίστροφη διαδικασία, δηλαδή τη μετατροπή του αναλογικού σήματος σε ψηφιακό.

ROUTER: Ο απλούστερος ορισμός του router είναι πως πρόκειται για τη συσκευή που συνδέει δύο διαφορετικά δίκτυα μεταξύ τους: το εσωτερικό δίκτυο υπολογιστών του σπιτιού (που μπορεί να περιλαμβάνει έναν, δύο ή x υπολογιστές) με ένα εξωτερικό δίκτυο, εν προκειμένω το Internet.
Στη σημερινή εποχή και με την πρόοδο της τεχνολογίας, οι προαναφερόμενες δύο συσκευές έχουν ενοποιηθεί σε μία, γνωστή πλέον ως modem-router.

SWITCH: Το switch συνδέει διαφορετικούς υπολογιστές στο ίδιο δίκτυο. Χωρίς το switch, δύο ή περισσότεροι υπολογιστές θα μπορούσαν να επικοινωνήσουν μέσω του router με το Internet, αλλά δεν θα «έβλεπαν» ο ένας τον άλλο για να ανταλλάξουν αρχεία ή οποιαδήποτε άλλη δικτυακή εφαρμογή.

WI-FI: Η λέξη προέρχεται από τον αγγλικό όρο Wireless Fidelity (σε ελεύθερη μετάφραση «ασύρματη πιστότητα»). Η τεχνολογία Wi-Fi χρησιμοποιείται στις ασύρματες συνδέσεις με το Διαδίκτυο μέσω φορητών υπολογιστών (laptop) ή άλλων συσκευών (π.χ. «έξυπνα» κινητά τηλέφωνα-smartphones ή υπολογιστές χειρός-tablets).

INSTANT MESSAGING: Οι υπηρεσίες ανταλλαγής άμεσων μηνυμάτων (Instant Messaging-Messengers, IRC, Live Chat κ.λπ.) δίνουν τη δυνατότητα στους χρήστες που διαθέτουν κατάλληλο λογισμικό, να συνεργάζονται ηλεκτρονικά με τους εξής τρόπους:

- Δηλώνοντας την ηλεκτρονική τους παρουσία (διαθεσιμότητα για επικοινωνία) σε συνεργάτες τους οπουδήποτε στο Διαδίκτυο.
- Επικοινωνώντας μεταξύ τους μέσω σύντομων γραπτών μηνυμάτων που αποστέλλονται άμεσα, αν είναι διαθέσιμοι, ή αργότερα, μόλις γίνουν διαθέσιμοι οι παραλήπτες.
- Μεταφέροντας αρχεία μεταξύ των υπολογιστών τους.

SOCIAL NETWORKING-ΚΟΙΝΩΝΙΚΗ ΔΙΚΤΥΩΣΗ

Οι ιστοσελίδες κοινωνικής δικτύωσης προσφέρουν στους χρήστες τους τη δυνατότητα να δημιουργήσουν το προσωπικό τους προφίλ, να παρουσιάσουν τον εαυτό τους και να επικοινωνήσουν με άλλους χρήστες στο Διαδίκτυο. Οι χρήστες αυτοί μπορεί να είναι γνωστοί από την καθημερινή ζωή τους ή εντελώς άγνωστοι.
Μέσα από αυτή την επικοινωνία δημιουργούνται online κοινότητες, όπου άνθρωποι με κοινά ενδιαφέροντα μπορούν να μοιράζονται πληροφορίες και να εκφράζουν τις απόψεις τους. Δε χρειάζονται ιδιαίτερες τεχνικές γνώσεις για να δημιουργήσει κανείς το προφίλ του και να ανεβάσει περιεχόμενο (σχόλια, φωτογραφίες, βίντεο), το οποίο θα μοιραστεί αργότερα με άλλους χρήστες.
Οι διαδικτυακές κοινότητες είναι ιδιαίτερα δημοφιλείς στην Ελλάδα, με πιο γνωστές τις: Facebook, Twitter, MySpace, YouTube.

BLOG-ΙΣΤΟΛΟΓΙΟ

Τα blogs είναι εικονικά ημερολόγια που αποθηκεύονται στο Διαδίκτυο, αποτελούνται από κείμενο και εικόνες, και μπορούν να δημιουργηθούν πολύ εύκολα από οποιονδήποτε.

IP ADDRESS-ΔΙΕΥΘΥΝΣΗ IP

Μια διεύθυνση IP (IP address-Internet Protocol address) είναι ένας μοναδικός αριθμός που χρησιμοποιείται από συσκευές για τη μεταξύ τους αναγνώριση και συνεννόηση σε ένα δίκτυο υπολογιστών. Όταν ένας χρήστης αποκτά πρόσβαση στο Διαδίκτυο, η σύνδεσή του λαμβάνει έναν αριθμό διεύθυνσης IP.
Η κυρίαρχη μορφή διεύθυνσης IP είναι ένας αριθμός που αποτελείται από 4 τμήματα αριθμών, που διαχωρίζονται από τελείες και έχουν την ακόλουθη μορφή: xxx.xxx.xxx.xxx, όπου xxx είναι ένας αριθμός από 000 έως 255 (π.χ. 128.32.0.24).

ΗΛΕΚΤΡΟΝΙΚΟ ΙΧΝΟΣ

Σε κάθε διαδικτυακή έρευνα γίνεται προσπάθεια εντοπισμού του ηλεκτρονικού ίχνους του δράστη, το οποίο για κάθε χρήστη του Internet είναι μοναδικό και αποτελεί σημαντικό στοιχείο για την αποδεικτική διαδικασία στο δικαστήριο.
ΗΛΕΚΤΡΟΝΙΚΟ ΙΧΝΟΣ: ΔΙΕΥΘΥΝΣΗ IP + ΩΡΑ + ΗΜΕΡΟΜΗΝΙΑ = ΜΟΝΑΔΙΚΟ ΑΝΑΓΝΩΡΙΣΤΙΚΟ ΤΑΥΤΟΤΗΤΑΣ ΕΝΟΣ ΧΡΗΣΤΗ INTERNET

ΕΤΑΙΡΕΙΕΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ (INTERNET SERVICE PROVIDERS)

Οι ISPs (Internet Service Providers) είναι εταιρείες που προσφέρουν υπηρεσίες πρόσβασης στο Διαδίκτυο, τηλεπικοινωνιακές υπηρεσίες IP, καθώς και υπηρεσίες ηλεκτρονικού επιχειρείν (δημιουργία ιστοσελίδων-web design, φιλοξενία ιστοσελίδων-hosting, κ.λπ.). Οι υπηρεσίες τους απευθύνονται σε οικιακούς χρήστες (συνδρομητές), σε ελεύθερους επαγγελματίες, καθώς και σε μικρομεσαίες, μεγάλες επιχειρήσεις και οργανισμούς.
Οι ISPs είναι αυτοί που παρέχουν την απαραίτητη τηλεπικοινωνιακή υποδομή για να φτάνει το Internet σε κάθε σπίτι ή επιχείρηση.
ΕΤΑΙΡΕΙΕΣ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ:
OTE, COSMOTE, CYTA, FORTHNET, HOL, ON TELECOMS, VODAFONE, WIND-TELLAS.

3. ΟΡΙΣΜΟΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

α. Η ανάπτυξη της τεχνολογίας κατέστησε δυνατή τη διάπραξη ενός ευρέος φάσματος εγκληματικών πράξεων, οι οποίες απαιτούν εξειδίκευση και αυξημένη κατάρτιση. Ως «Ηλεκτρονικό Έγκλημα», λοιπόν, θεωρούνται οι αξιόποινες εγκληματικές πράξεις που τελούνται με τη χρήση ηλεκτρονικών υπολογιστών και συστημάτων επεξεργασίας δεδομένων, και τιμωρούνται με συγκεκριμένες ποινές από την ελληνική νομοθεσία.
β. Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής, καθώς και το Διαδίκτυο έχουν επιφέρει σημαντικές αλλαγές σε κάθε έκφανση της καθημερινότητας και της ανθρώπινης επαφής. Μαζί, όμως, με τις αλλαγές αυτές που διευκολύνουν και βοηθούν στην καλυτέρευση της ποιότητας ζωής, οι νέες τεχνολογίες και το Διαδίκτυο δημιούργησαν ιδανικές συνθήκες για την καλλιέργεια και ανάπτυξη νέων μορφών εγκληματικότητας, που συνοψίζονται στον όρο ηλεκτρονικό έγκλημα.

4. ΜΟΡΦΕΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Οι μορφές του ηλεκτρονικού εγκλήματος είναι ποικίλες και με τη συνεχή ανάπτυξη της τεχνολογίας και του Διαδικτύου πολλαπλασιάζονται. Μια συσκευή, όπως ο υπολογιστής ή το κινητό τηλέφωνο, μπορεί κατά περίπτωση να είναι μέσο διάπραξης ενός αδικήματος (π.χ. διακίνηση πορνογραφικού υλικού, μέσο εξύβρισης, δυσφήμησης, απειλής, εκβίασης) ή να γίνεται η ίδια στόχος της εγκληματικής επίθεσης (π.χ. υποκλοπή και αλλοίωση δεδομένων).

Κύριες μορφές Κυβερνοεγκλημάτων
Απάτες μέσω Διαδικτύου
Παιδική πορνογραφία
Cyber bullying
Τυχερά παιχνίδια-Τζόγος
Παραβίαση προσωπικών δεδομένων
Cracking και hacking
Διακίνηση-πειρατεία λογισμικού
Εγκλήματα στα chat rooms

5. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΟΥ ΕΓΚΛΗΜΑΤΟΣ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Το έγκλημα στον κυβερνοχώρο είναι γρήγορο, διαπράττεται σε χρόνο δευτερολέπτων και πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα.
Είναι εύκολο στη διάπραξή του, φυσικά για όσους το γνωρίζουν, ενώ τα ίχνη που αφήνει είναι ψηφιακά.
Για την τέλεσή του απαιτούνται άριστες και εξειδικευμένες γνώσεις.
Μπορεί να διαπραχθεί χωρίς τη μετακίνηση του δράστη, ο οποίος ενεργεί από το γραφείο ή το σπίτι του, χρησιμοποιώντας τον υπολογιστή του.
Δίνει τη δυνατότητα σε άτομα όπως οι παιδόφιλοι (child pornography) να επικοινωνούν γρήγορα ή και σε πραγματικό χρόνο, χωρίς μετακίνηση, εύκολα και ανέξοδα, ενώ μπορούν να βρίσκονται πολλοί μαζί στην ίδια ομάδα συζητήσεων (chat rooms).
Οι «εγκληματίες του κυβερνοχώρου» πολλές φορές δεν εμφανίζονται με την πραγματική τους ταυτότητα και αποστέλλουν ηλεκτρονικά μηνύματα (e-mail) με ψευδή στοιχεία.
Είναι έγκλημα «χωρίς πατρίδα» και τα αποτελέσματά του μπορεί να πραγματοποιούνται ταυτόχρονα σε πολλούς τόπους.
Η αστυνομική διερεύνησή του είναι πολύ δύσκολη, απαιτεί δε άριστη εκπαίδευση και εξειδικευμένες γνώσεις.
Η καταγραφή της εγκληματικότητας στον κυβερνοχώρο δεν ανταποκρίνεται στην πραγματικότητα, διότι ελάχιστες περιπτώσεις εγκλημάτων του κυβερνοχώρου καταγγέλλονται - όχι μόνο στον ελληνικό, αλλά και στον διεθνή χώρο. Κατά συνέπεια ο «σκοτεινός αριθμός» της εγκληματικότητας είναι «ακόμα πιο σκοτεινός» στο χώρο του Διαδικτύου από ό,τι στον «κοινό» εγκληματικό χώρο.

6. ΝΟΜΟΘΕΣΙΑ

Η ποινική νομοθεσία σχετικά με τη χρήση του Διαδικτύου στην Ελλάδα είναι σημαντική και καλύπτει αρκετές εγκληματικές πράξεις που τελούνται μέσω αυτού.

α. Ποινικος Κώδικας
Άρθρο 292Α: Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών
» 348Α: Πορνογραφία ανηλίκων
» 348Β: Προσέλκυση παιδιών για γενετήσιους λόγους
» 361: Εξύβριση
» 362: Δυσφήμηση
» 363: Συκοφαντική δυσφήμηση
» 370: Παραβίαση του απορρήτου των επιστολών
» 370Α: Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας
» 370Β: Παραβίαση στοιχείων ή προγραμμάτων υπολογιστών που θεωρούνται απόρρητα
» 370Γ: Παράνομη αντιγραφή ή χρήση προγραμμάτων υπολογιστών και παράνομη πρόσβαση σε δεδομένα υπολογιστών
» 385: Εκβίαση
» 386Α: Απάτη με υπολογιστή

β. Γνωμοδοτήσεις
Υπ' αριθμ. 9/2011: Γνωμοδότηση του Αντιεισ. Α. Π. κ. Α. Κατσιρώδη.
Υπ' αριθμ. 12/2009: Γνωμοδότηση του Εισ. Α. Π. κ. Ι. Τέντε.
Υπ' αριθμ. 9/2009: Γνωμοδότηση του Εισ. Α. Π. κ. Γ. Σανιδά.

γ. Νόμοι
Ν. 2121/1993: «Πνευματική ιδιοκτησία, συγγενικά δικαιώματα και πολιτιστικά θέματα».
Ν. 2225/1994: «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας», όπως έχει τροποποιηθεί έως σήμερα.
Ν. 2472/97 και 2774/99: «Περί προσωπικών δεδομένων στο Διαδίκτυο».
Ν. 2867/2000: «Οργάνωση και Λειτουργία του τομέα των Τηλεπικοινωνιών».
Ν. 2819/2000: «Περί νομικής προστασίας βάσεων δεδομένων».
Ν. 3471/2006: «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997».
Ν. 3431/2006: «Περί ηλεκτρονικών επικοινωνιών και άλλες διάταξεις».
Ν. 3674/2008: «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις».
Ν. 3783/2009: «Ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας και άλλες διατάξεις».
Ν. 3917/2011: «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις». Σύμφωνα με τον ανωτέρω νόμο οι εταιρείες παροχής υπηρεσιών Διαδικτύου δε διατηρούν στοιχεία συνδρομητών και δεδομένα που αντιστοιχούν σε ηλεκτρονικά ίχνη, πέραν του διαστήματος των δώδεκα (12) μηνών.
Ν. 4002/2011: όπως τροποποιήθηκε με το Ν. 4021/2011: «Ρύθμιση της αγοράς παιγνίων».

δ. Προεδρικά Διατάγματα
Π. Δ. 150/2001: «Ηλεκτρονικές Υπογραφές».
Π. Δ. 131/2003: «Ηλεκτρονικό εμπόριο κ.λπ. Υπηρεσίες της Κοινωνίας της Πληροφορίας».
Π. Δ. 47/2005: «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και τη διασφάλισή του».

ε. Συνθήκη της Βουδαπέστης

Για την αντιμετώπιση του ηλεκτρονικού εγκλήματος είναι απαραίτητη η διακρατική συνεννόηση και η εκπόνηση μιας αναλυτικής και αποτελεσματικής στρατηγικής. Ο στόχος αυτός επετεύχθη στο Συνέδριο για το Ηλεκτρονικό Έγκλημα (Convention on Cybercrime), που έγινε το 2001 στη Βουδαπέστη και όλα τα συμπεράσματα του οποίου αποκρυσταλλώνονται στη Συνθήκη που υπεγράφη μετά το πέρας των εργασιών του στις 23.11.2001. Στη Συνθήκη της Βουδαπέστης, την οποία υπέγραψαν 26 υπουργοί ευρωπαϊκών κρατών, μεταξύ των οποίων και της Ελλάδας, υπάρχουν επεξηγήσεις και ρυθμίσεις για όλα τα ηλεκτρονικά εγκλήματα. Η συνθήκη αυτή έχει υπογραφεί μεν από την Ελλάδα, πλην όμως δεν έχει ενταχθεί, με την ψήφιση σχετικού νόμου, στο ελληνικό δίκαιο μέχρι σήμερα.
Στη συνθήκη αυτή τονίζεται η αναγκαιότητα της διεθνούς συνεργασίας μεταξύ των κρατών για την καταπολέμηση του ηλεκτρονικού εγκλήματος και θίγεται το πολύ σημαντικό θέμα της αρμοδιότητας και της δικαιοδοσίας των δικαστηρίων σχετικά με τα εγκλήματα αυτά.

7. ΣΥΝΕΡΓΑΣΙΕΣ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας συνεργάζεται στενά με διεθνείς οργανισμούς και συναρμόδιους φορείς (INTERPOL, EUROPOL, EUROJUST, Εισαγγελικές Αρχές, ΜΚΟ, κ.λπ.), για ευόδωση του επιδιωκόμενου σκοπού, που δεν είναι άλλος, από την καταπολέμηση του ηλεκτρονικού εγκλήματος.

8. ΣΥΝΕΡΓΑΣΙΑ ΜΕ ΑΛΛΟΔΑΠΕΣ ΑΡΧΕΣ

Στις περισσότερες περιπτώσεις εγκλημάτων στο Διαδίκτυο, η ταυτότητα και η χώρα εγκατάστασης των δραστών είναι άγνωστη. Επίσης, ο τόπος διάπραξης του κυβερνοεγκλήματος είναι συχνά αμφισβητούμενος. Για παράδειγμα, αν η τεχνική υποδομή τέλεσης του εγκλήματος, δηλαδή ο εξυπηρετητής (server) που φιλοξενεί την απατηλή ιστοσελίδα, είναι εγκατεστημένος σε χώρα του εξωτερικού, δεν μπορούν να εφαρμοστούν οι προβλεπόμενοι ελληνικοί νόμοι, οι οποίοι τιμωρούν αποκλειστικά εγκλήματα τελούμενα στην Ελλάδα. Στην περίπτωση αυτή, ισχύει το νομικό πλαίσιο της χώρας όπου φιλοξενείται ο εξυπηρετητής.

Σύμφωνα με έως σήμερα απαντήσεις μέσω Interpol, σε τέτοιου είδους περιπτώσεις απαιτείται η υποβολή σχετικού αιτήματος δικαστικής συνδρομής, προκειμένου να εξακριβωθούν στοιχεία κατόχων ηλεκτρονικών λογαριασμών, καθώς και άλλων δεδομένων, που αφορούν εγκλήματα που τελούνται μέσω Διαδικτύου για τις παρακάτω χώρες:

Η.Π.Α.
ΓΑΛΛΙΑ
ΛΟΥΞΕΜΒΟΥΡΓΟ
ΟΛΛΑΝΔΙΑ
ΡΟΥΜΑΝΙΑ
ΙΣΠΑΝΙΑ
ΤΟΥΡΚΙΑ
ΙΣΡΑΗΛ

ΕΙΔΙΚΟΤΕΡΑ:

Η.Π.Α.

Α. FACEBOOK
Η έδρα της εταιρείας βρίσκεται στην Καλιφόρνια των Η.Π.Α. Παρόλο που το περιεχόμενο της σελίδας έχει μεταφραστεί στα Ελληνικά, δεν υπάρχει αντιπρόσωπος της εταιρείας στην Ελλάδα.
Η Facebook συνεργάζεται με τις αστυνομικές Αρχές σε όλο τον κόσμο, έπειτα από επίσημη νομική διαδικασία (αίτημα δικαστικής συνδρομής ή υπό περιπτώσεις με εισαγγελική παραγγελία). Η παροχή στοιχείων βασίζεται στις αρχές της αστυνομικής συνεργασίας και στο νομικό πλαίσιο της Καλιφόρνια.
Β. ΙΣΤΟΛΟΓΙΑ
Τα (περισσότερα) ιστολόγια αντιστοιχούν σε διακομιστές (servers) εταιρειών στις Ηνωμένες Πολιτείες Αμερικής. Επειδή τα απαραίτητα αρχεία καταγραφής δραστηριότητας των διαχειριστών και επισκεπτών τους (log files), βρίσκονται σε εξυπηρετητή (server) των Η.Π.Α., προκειμένου να πραγματοποιηθεί περαιτέρω ψηφιακή ανάλυση, απαιτείται αίτημα δικαστικής συνδρομής, όπως αναφέρθηκε παραπάνω. Για παράδειγμα, η δυσφήμηση, σύμφωνα με το υπ' αριθμ. 182-33394/06-05-2010 έγγραφο του Υπουργείου Δικαιοσύνης των Η.Π.Α., δε θεωρείται κατά κανόνα αξιόποινη σύμφωνα με το αμερικανικό δίκαιο, ως αντιβαίνουσα στις διατάξεις περί ελευθερίας του λόγου της Πρώτης Αναθεώρησης του Συντάγματος των Η.Π.Α.

ΗΝΩΜΕΝΟ ΒΑΣΙΛΕΙΟ

Στο Ηνωμένο Βασίλειο, σε περιπτώσεις απάτης στις οποίες η ζημία είναι μεγαλύτερη των 6.000 ευρώ ή υπάρχουν επαρκώς τεκμηριωμένα στοιχεία που αποδεικνύουν την ύπαρξη εγκληματικής οργάνωσης, γίνονται δεκτά τα αιτήματα για συνεργασία (αστυνομική).
Για όλες τις υπόλοιπες περιπτώσεις απαιτείται αίτημα δικαστικής συνδρομής.

ΚΑΝΑΔΑΣ

Ομοίως, στον Καναδά, σε περιπτώσεις απάτης στις οποίες η ζημία είναι μεγαλύτερη των 5.000 δολαρίων Καναδά ή υπάρχουν επαρκώς τεκμηριωμένα στοιχεία που αποδεικνύουν την ύπαρξη εγκληματικής οργάνωσης, γίνονται δεκτά τα αιτήματα για συνεργασία (αστυνομική).
Για όλες τις υπόλοιπες περιπτώσεις απαιτείται αίτημα δικαστικής συνδρομής.

ΝΙΓΗΡΙΑ

Οι Αρχές της Νιγηρίας, σε κάθε περίπτωση (μέχρι σήμερα), δεν απαντούν σε αιτήματα συνεργασίας.

9. ΔΙΚΑΣΤΙΚΗ ΣΥΝΔΡΟΜΗ

Στις περιπτώσεις όπου απαιτείται αίτημα δικαστικής συνδρομής, αυτό θα πρέπει να υποβληθεί από την επιληφθείσα Εισαγγελία στον αρμόδιο Εισαγγελέα Εφετών, ο οποίος θα το διαβιβάσει αρμοδίως στο Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων.

10. ΧΡΗΣΙΜΑ LINKS

Χρήσιμες συμβουλές από τη Δίωξη Ηλεκτρονικού Εγκλήματος:
http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=135&Itemid=128&lang=

Ανοικτή γραμμή για το παράνομο περιεχόμενο στο Διαδίκτυο:
http://www.safeline.gr

Ελληνικός κόμβος ασφαλούς δικτύου:
www.saferinternet.gr

Οργανισμός προστασίας των δικαιωμάτων των παιδιών:
http://www.hamogelo.gr

Συμβουλές ασφαλείας για online chatting:
http://www.chatdanger.com

Ιστότοπος από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος:
http://www.cyberkid.gr/

ΕΠΙΚΟΙΝΩΝΙΑ

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

Bold Ogilvy & Mather

#ηλεκτρονική_απάτη

έγκλημα μέσα από το διαδίκτυο

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

ΕΠΙΚΟΙΝΩΝΙΑ

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Μπορούν οι ΕΠΙΧΕΙΡΗΣΕΙΣ να αντιμετωπίσουν την κυβερνοαπάτη και με ποιον τρόπο;

Οι επιχειρήσεις θα πρέπει, εκτός από την εφαρμογή λογισμικών προστασίας και ασφάλειας τών πληροφοριακών τους συστημάτων, να εκπαιδεύουν το προσωπικό τους, έτσι ώστε να αποκτήσει «Κουλτούρα Ασφάλειας» (Culture of Security). Είναι αρκετά συχνό το φαινόμενο, όπου, κατά την πρόσληψη των υπαλλήλων της μια επιχείρηση τους ωθεί στην υπογραφή όρων και πολιτικών ασφαλείας που θα πρέπει να τηρούν, ώστε να προστατεύεται, τόσο το πελατολόγιό της εταιρείας όσο και τα πληροφοριακά δεδομένα αυτής. Στην προσπάθειά της αυτή, μια επιχείρηση θα πρέπει να υιοθετεί την εφαρμογή κάποιων μέτρων, τα οποία συνοψίζονται στα εξής:

1) Να εντοπίσει ποια δεδομένα είναι εκτεθειμένα σε μεγαλύτερο κίνδυνο, εφόσον τα πληροφοριακά της συστήματα έχουν πρόσβαση στο διαδίκτυο (π.χ. στοιχεία πελατών της ή λογιστικά δεδομένα και οικονομικά στοιχεία)
2) Να έχει εγκατεστημένα σε όλους τους Η/Υ με ειδικά λογισμικά (π.χ. anti-virus programs, anti-spyware programs, firewalls) και να αλλάζουν τους κωδικούς πρόσβασης και συναλλαγών κάθε 60 ή 70 μέρες.
3) Να εγκαθιστά πρόγραμμα που θα τηρεί backups (π.χ. σε εξωτερικό σκληρό δίσκο) όλων των σημαντικών δεδομένων και να το αναβαθμίζει σε τακτά χρονικά διαστήματα, έτσι ώστε να μην υπάρχει απώλεια δεδομένων σε περίπτωση φυσικής καταστροφής ή κυβερνοεπίθεσης. Καλό θα ήταν να κρυπτογραφούνται όλα τα ευαίσθητα και υψίστης σημασίας δεδομένα.
4) Να έχει ήδη σχεδιασμένο πλάνο επείγουσας επέμβασης ή εναλλακτικών ενεργειών σε περίπτωση κυβερνοεπίθεσης, το οποίο θα πρέπει να ελέγχεται ετησίως.
5) Να εκπαιδεύει το προσωπικό της για την επίδραση που θα έχει σε όλους μια κυβερνοεπίθεση με τη μορφή της απάτης. Η εκπαίδευση μπορεί να γίνει με σεμινάρια πάνω σε πρακτικές του διαδικτύου ή και τεχνολογικές λύσεις που θα πείθουν τους εργαζόμενους ότι θα πρέπει να είναι ιδιαιτέρως προσεκτικοί απέναντι σε διαδικτυακές απάτες, καθώς μπορεί να εξαπατηθούν και να ζημιωθούν στην προσωπική τους ζωή μέσα από το διαδίκτυο.

6) Να υπογράφουν συμβόλαια με τους εργαζομένούς τους, τους οποίους θα δεσμεύουν να αναφέρουν προς τις αρμόδιες αρχές τυχόν υποψία, αλλά και πραγμάτωση, διαδικτυακής απατηλής συναλλαγής εντοπίσουν.

Μερικές επιπλέον συμβουλές:

1) Συνεργαστείτε μόνο με εταιρίες που γνωρίζετε ή μπορείτε να έχετε άμεση πρόσβαση στα στοιχεία τους από επίσημες βάσεις δεδομένων.
2) Κατανοήστε όλες τις λεπτομέρειες σχετικά με τα προσφερόμενα, υπηρεσίες ή προϊόντα.
3) Ελέγξτε προσεκτικά όλα τα τιμολόγια και τους λογαριασμούς που καλείστε να πληρώσετε.
4) Διαφυλάξτε τα οικονομικά και τραπεζικά δεδομένα σας και μην τα αποκαλύπτεται σε άγνωστους τρίτους.
5) Καταστήστε το προσωπικό σας υπεύθυνο για τυχόν λανθασμένες ενέργειες, αφού πρώτα το εκπαιδεύσετε σχετικά.

Συμβουλές για Ηλεκτρονικές Δημοπρασίες (Auctions):

- Πριν δώσετε προσφορά, επικοινωνήστε με τον πωλητή και ξεκαθαρίστε αμφισβητούμενα σημεία σχετικά με το προϊόν προς πλειστηριασμό.
- Να είστε ιδιαίτερα προσεκτικοί όσον αφορά αντισυμβαλλόμενους στο εξωτερικό.
- Επιβεβαιώστε τις πολιτικές επιστροφής και εγγύησης του προϊόντος, καθώς και τα μεταφορικά έξοδα.
- Ασφαλίστε τα πλειστηριασθέντα κατά τη μεταφορά τους.

Συμβουλές για Απάτες σχετικές με Πιστωτικές Κάρτες (credit card fraud):

- Επιβεβαιώστε ότι η ιστοσελίδα που δηλώνετε τα στοιχεία της πιστωτικής σας κάρτας είναι ασφαλής και γνωστή στο ευρύ κοινό.
- Επιβεβαιώστε και το κατάστημα που προβάλλεται μέσω της ιστοσελίδας.
- Ελέγχετε συχνά τις κινήσεις της πιστωτικής σας κάρτας μέσω της τράπεζάς σας ή μέσω web-banking.

Συμβουλές για το αιτήματα Απάλλειψης Χρέους (Dept Elimination):

- Ελέγξτε το όνομα, τη διεύθυνση και τον τηλεφωνικό αριθμό της εταιρείας ή του φυσικού προσώπου που

προβάλλεται ως «σωτήρας», εάν είναι υπαρκτά.
- Ελέγξτε τους όρους της συμφωνίας πριν υπογράψετε.
- Προσέξτε εταιρείες που δηλώνουν μόνο ταχυδρομικές θυρίδες για επικοινωνία.
- Προσέξτε μήπως αυτά που υπόσχονται είναι πολύ καλά για να είναι αληθινά.

Συμβουλές για εργασιακές ευκαιρίες (Employment Opportunities):

- Προσέξτε μήπως υπόσχονται πολλά έσοδα ή κέρδη.
- Προσέξτε μήπως σας ζητήσουν να προκαταβάλλετε χρήματα για διαδικαστικά θέματα.
- Προσέξτε αγγελίες εργασίας που δε ζητούν προϋπηρεσία ως απαραίτητο προσόν.
- Επιβεβαιώστε ότι η εταιρεία-εργοδότης είναι υπαρκτή.

Συμβουλές για επιστολές «Νιγηριανής Απάτης» (Nigerian letters):

- Προσέξτε μήπως αυτά που σας υπόσχονται είναι πολύ καλά για να είναι αληθινά.
- Μην απαντάτε σε e-mail που σας ζητούν στοιχεία τραπεζικού λογαριασμού.
- Μην εξαπατάστε από άτομα που παρουσιάζονται ως κυβερνητικοί υπάλληλοι μιας ξένης χώρας.
- Προσέξτε όταν σας ζητούν να βοηθήσετε στην τοποθέτηση χρημάτων σε υπεράκτιους λογαριασμούς.
- Μην εμπιστεύεστε όσους σας υπόσχονται μεγάλα χρηματικά ποσά σε περίπτωση συνεργασίας.

Συμβουλές για phising:

- Να είστε καχύποπτοι όταν σας ζητούν μέσω απομονωμένων e-mail προσωπικές πληροφορίες.
- Μη συμπληρώνετε φόρμες με τα προσωπικά σας στοιχεία όταν σας αποστέλλονται από άγνωστες διευθύνσεις ηλεκτρονικών ταχυδρομείων.
- Πληκτρολογήστε στον browser τη διεύθυνση της ιστοσελίδας και μη μπαίνετε σε αυτή μέσω συνδέσμων.

Συμβουλές για spamming:

- Μην ανοίγετε τα spam μηνύματα.
- Μην απαντάτε στα spam μηνύματα, ώστε ο αποστολέας να μην αντιληφθεί ότι η διεύθυνσή σας είναι υπαρκτή και ενεργή.
- Διατηρείτε δύο e-mail διευθύνσεις, μία για τους οικείους σας και μία για κάθε άλλο σκοπό.
- Ποτέ μην αγοράζετε κάτι που σας αποστέλλεται μέσω ενός απομονωμένου e-mail.

Συνοψίζοντας, δε θα πρέπει να κυριεύεται κανείς από το αίσθημα του φόβου πριν προβεί σε online πληρωμές και συναλλαγές.

ΟΛΟΙ θα πρέπει να απολαμβάνουμε τα πλεονεκτήματα που μας παρέχουν αυτού του τύπου οι συναλλαγές και να πραγματοποιούμε τις αγορές μας πιο φθηνά, πιο ξεκούραστα, με μεγαλύτερη ποικιλία για εμάς να επιλέξουμε και να αγοράσουμε όποτε και οτιδήποτε επιθυμούμε. Η Υπηρεσία μας τάσσεται θετικά στις online συναλλαγές, αρκεί να διαθέτει κανείς τα «χρυσά εργαλεία» για όλων των τύπων τις συναλλαγές και να μπορείτε να τις ελέγχει πλήρως.

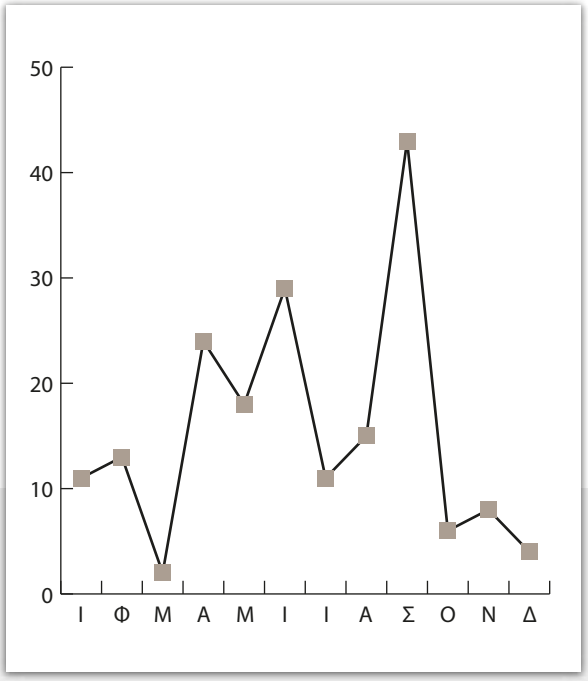
Ποια είναι αυτά τα «χρυσά εργαλεία»:

α) Μία **προπληρωμένη κάρτα** που θα έχει εκδότη ένα έγκριτο χρηματοπιστωτικό ίδρυμα.
β) Ένας **Paypal** λογαριασμός συνδεδεμένος με μια κάρτα ανάληψης.
γ) **Υπηρεσία e-banking** για την άμεση πρόσβαση στις κινήσεις των λογαριασμών και των καρτών του, αλλά και για την άμεση πραγματοποίηση πληρωμών.

ΑΠΟΛΟΓΙΣΤΙΚΑ στατιστικά στοιχεία εξιχνίασης απατών από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος για το 2012

Η Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διαχειρίστηκε με επιτυχία εκατόν ογδόντα τέσσερις (184) περιπτώσεις διαδικτυακών απατών, η μηνιαία εξέλιξη των οποίων περιγράφεται στο κατωτέρω διάγραμμα.

ΑΠΑΤΕΣ (ΜΗΝΙΑΙΑ ΕΞΕΛΙΞΗ)



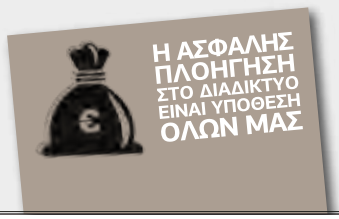
ΒΙΒΛΙΟΓΡΑΦΙΑ

"http://www.ic3.gov"
"http://www.fraud.org"
"http://www.staysafeonline.org"
"http://www.rsa.com"
"http://www.businessweek.com"
"http://www.acfe.gr"
"http://www.interpol.int"

«ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΑΛΛΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ ΣΥΜΠΕΡΙΦΟΡΕΣ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ»,
ΕΜΜΑΝΟΥΗΛ ΣΦΑΚΙΑΝΑΚΗΣ,
ΚΩΝΣΤΑΝΤΙΝΟΣ ΣΙΩΜΟΣ,
ΓΕΩΡΓΙΟΣ ΦΛΩΡΟΣ,
ΕΚΔΟΣΕΙΣ ΛΙΒΑΝΗ 2012.

ΤΟ ΔΙΚΑΙΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ,
ΑΝΑΣΤΑΣΙΑ Κ. ΜΑΛΛΕΡΟΥ,
ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2007.

ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΔΙΚΤΥΟ,
ΘΕΟΔΩΡΟΣ Ν. ΚΡΙΘΑΡΑΣ,
ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2009.



#ηλεκτρονική_απάτη
έγκλημα μέσα από το διαδίκτυο

Βασική αρχή στις απάτες που διαπράττονται μέσω διαδικτύου είναι να πείσουν το θύμα να καταβάλλει ένα μικρό, αρχικό χρηματικό ποσό, με σκοπό να εξασφαλίσει ένα πολύ μεγαλύτερο στο μέλλον (π.χ. νιγηριανές απάτες) ή γενικότερα να πείσουν το θύμα για την ασφάλεια των διαδικτυακών συναλλαγών με σκοπό στη συνέχεια να του αποσπάσουν μεγάλα χρηματικά ποσά (απάτες με πιστωτικές κάρτες κ.ά.).

Spamming- Scamming

Η λέξη "Spam" περιγράφει τη μαζική αποστολή μηνυμάτων ηλεκτρονικού υπολογιστή (e-mails), τα οποία έχουν συνήθως απρόκλητο και εμπορικό χαρακτήρα, και αποστέλλονται αδιακρίτως. Όταν ο στόχος του αποστολέα των μηνυμάτων αυτών είναι να εξαπατήσει τον αποδέκτη και να χρησιμοποιήσει με κακόβουλο τρόπο τα δεδομένα που θα υποκλέψει, τότε έχουμε να κάνουμε με τη διαδικασία του "Scamming". Πρόκειται για τον πλέον διαδεδομένο τρόπο δράσης σε πολλά είδη ηλεκτρονικών οικονομικών εγκλημάτων (ισπανικό λόττο, phishing, εικονικές θέσεις εργασίας στο εξωτερικό, διαφημίσεις για χάσιμο βάρους κ.λπ.). Επιπλέον, η μαζική αποστολή κακόβουλων μηνυμάτων γίνεται και προς κινητά τηλέφωνα, σε μια εποχή που οι χρήστες των smartphones αυξάνονται ραγδαία.

«Νιγηριανές» Απάτες

Πρόκειται για μηνύματα στο ηλεκτρονικό μας ταχυδρομείο που μας ενημερώνουν ότι κάποιος (συνήθως πρώην υψηλόβαθμο στέλεχος της νιγηριανής κυβέρνησης) χρειάζεται τη βοήθειά μας για να μεταφέρει ένα υψηλό χρηματικό ποσό (π.χ. 30 εκατ. δολάρια), έναντι υψηλής υποσχόμενης αμοιβής (ποσοστό επί του κεφαλαίου), το οποίο δεν μπορεί να διοχετευτεί εκτός της χώρας με το όνομα του δικαιούχου/αποστολέα του mail. Ζητείται δηλαδή στον παραλήπτη να βοηθήσει λειτουργώντας ως αποδέκτης του εν λόγω ποσού, αφού παράλληλα τον ενημερώσουν ότι η επιλογή του δεν έγινε τυχαία, αλλά βάσει πληροφόρησης που είχαν για τη φερεγγυότητά του (συχνά αναφέρεται κάποιο επιμελητήριο ή επαγγελματική ένωση). Παράλληλα, δίνεται ιδιαίτερη έμφαση στον εμπιστευτικό χαρακτήρα του αιτήματος, ο οποίος θα πρέπει να τηρηθεί. Σε πρώτη φάση, ζητούν από το υποψήφιο θύμα τη συγκατάθεσή του και την παροχή στοιχείων που αφορούν στους τραπεζικούς του λογαριασμούς και οποιονδήποτε πληροφοριών κρίνονται απαραίτητες για την πραγματοποίηση των συναλλαγών. Πολλές φορές και ύστερα από απαίτηση του θύματος, προσκομίζονται και έγγραφα, τα οποία δείχνουν αυθεντικά και επίσημα, εξαλείφοντας έτσι κάθε αμφιβολία του θύματος. Από τη στιγμή, λοιπόν, που το θύμα θα ανταποκριθεί, αρχίζει μια ατελείωτη διαδικασία ανταλλαγής mail, τηλεφωνημάτων και επιστολών κάνοντάς τον να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του εν λόγω ποσού. Ακριβώς όμως πριν την τελική μεταβίβαση των χρημάτων, εμφανίζεται, από πλευράς του αξιωματούχου, κάποιο προσωρινό πρόβλημα (έκτακτος φόρος, απρόβλεπτο τέλος, πληρωμή κάποιου ενδιάμεσου υπαλλήλου, κ.λπ.). Ο αξιωματούχος βέβαια προφασίζεται αδυναμία πληρωμής του ποσού λόγω του ό,τι έχει ήδη προχωρήσει σε μεταβίβαση των χρημάτων, με αποτέλεσμα τη δέσμευση αυτών, έως ότου λυθεί το πρόβλημα που προέκυψε. Στα πλαίσια συνεργασίας τους, ζητείται από το θύμα να καταβάλλει το ποσό, το οποίο φυσικά θα του επιστραφεί με την ολοκλήρωση της συναλλαγής. Αυτή βέβαια είναι η αρχή μιας σειράς «προβλημάτων» που προφασίζεται ο δράστης καταφέρνοντας να αποσπάσει χρηματικό ποσό που μπορεί να φτάσει μέχρι και τα 500.000€. Η εμπειρία έχει δείξει πως κάποια από τα θύματα πείθονται να ταξιδέψουν μέχρι την Νιγηρία για την ολοκλήρωση της συναλλαγής, κι ενώ τους έχουν διαβεβαιώσει ότι δεν απαιτείται visa, καταλήγουν να βρίσκονται παράνομα στη χώρα, γεγονός που χρησιμοποιείται εκβιαστικά από το κύκλωμα των δραστών.

Δεν είναι λίγες οι περιπτώσεις συνανθρώπων μας που το κύκλωμα των δραστών τους πείθει να ταξιδέψουν στο εξωτερικό, τους οδηγούν σε θυρίδα τράπεζας δείχνοντας τους τα λεφτά, ενώ εκείνοι έχουν ήδη καταβάλλει κάποια χρηματικά ποσά για την αποδέσμευση του κεφαλαίου. Η παραμονή τους γίνεται σε ξενοδοχείο 5 αστέρων με το κύκλωμα να τους παρακινεί να κάνουν πολυτελή ζωή για 4 ημέρες την οποία και προφασίζονται ότι θα καλύψουν, χωρίς βεβαίως να το κάνουν.

Ισπανικό Λόττο

Η εν λόγω μορφή απάτης πραγματοποιείται με τη μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου. Τα μηνύματα αυτά τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου, στην οποία όμως ποτέ δεν δήλωσαν συμμετοχή. Οι δράστες για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (πχ. Microsoft, Yahoo κ.λπ.) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά στην υποτιθέμενη ηλεκτρονική κλήρωση. Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

Phising προσωπικών στοιχείων

Το "phishing" πραγματοποιείται συνήθως με τη αποστολή μαζικών "spam e-mails", τα οποία υποτίθεται ότι αποστέλλονται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κ.λπ.), σε μία προσπάθεια να παραπλανήσει τον παραλήπτη και να του αποσπάσει απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, οι εγκέφαλοι της απάτης χρησιμοποιούν τα στοιχεία αυτά για την πραγματοποίηση αξιόποινων πράξεων. Συγκεκριμένα, ο αποστολέας απαιτεί ο παραλήπτης να ενημερώσει ή να επαληθεύσει άμεσα κάποια προσωπικά στοιχεία του για λόγους ασφαλείας, όπου στο τέλος οδηγείται μέσω συνδέσμων σε κάλπικες ιστοσελίδες, οι οποίες και μιμούνται στο μέγιστο τις επίσημες. Τα κέρδη των δραστών παγκοσμίως υπερβαίνουν το 1 δις ευρώ σε ετήσια βάση.

Pharming

Η διαδικασία "pharming" αποτελεί μια παραλλαγή του "phishing". Περιγράφει την παρέμβαση τρίτων στον DNS εξυπηρετητή (DNS server) μιας ιστοσελίδας που στόχο έχει την ανακατεύθυνση του προγράμματος περιήγησης σε άλλες ψεύτικες ιστοσελίδες. Το pharming μπορεί να πραγματοποιηθεί επιφέροντας αλλοίωση:

- του "host" file ενός Η/Υ, με αποτέλεσμα την ανακατεύθυνση ενός ονόματος χώρου σε ψευδή προορισμό.
- του "router" ενός δικτύου LAN, με την αλλοίωση των ρυθμίσεων ή ακόμη και του firmware ενός router, ο δράστης μπορεί να πετύχει την ανακατεύθυνση ενός ονόματος χώρου για όλους τους Η/Υ του δικτύου.
- ενός DNS server. Οι δράστες αποκτούν πρόσβαση σε έναν κεντρικό DNS Server, αλλοιώνοντας την κίνηση όλων των χρηστών του διαδικτύου που εξυπηρετείται από αυτούς.

Με πιο απλά λόγια, ο χρήστης του διαδικτύου πληκτρολογεί την ιστοσελίδα κάποιου διαδικτυακού καταστήματος και εν αγνοία του, μεταφέρεται σε έναν ψεύτικο ιστότοπο, ο οποίος προσομοιάζει την πραγματική ιστοσελίδα του εν λόγω καταστήματος που έχει δημιουργηθεί για να παραπλανήσει το χρήστη. Στη συνέχεια, ο δράστης υφαρπάζει τα προσωπικά στοιχεία που ο ανυποψίαστος χρήστης θα καταχωρήσει κατά τη διαδικασία της συναλλαγής (ονοματεπώνυμο, κωδικοί πιστωτικών καρτών, κ.λπ.) προκειμένου να τα χρησιμοποιήσει με κακόβουλο τρόπο.
Το φαινόμενο του pharming έχει παρουσιαστεί πρόσφατα και σε δύο τραπεζικούς οργανισμούς. Με την ανακατεύθυνση των σελίδων του web banking, μέσω μόλυνσης του προσωπικού τους Η/Υ, οι χρήστες των λογαριασμών αυτών οδηγούνταν σε ψευδείς ιστοσελίδες, όπου και υποκλέπτονταν τα προσωπικά τους δεδομένα.

Απάτες με πιστωτικές κάρτες

Τα περιστατικά απάτης με τη χρήση πιστωτικών καρτών σε online αγορές αυξάνονται με ραγδαίο ρυθμό. Υπολογίζεται ότι οι τράπεζες μετρούν απώλειες εκατομμυρίων ευρώ από ανθρώπους που κατασκευάζουν, παραχαράσσουν και υποκλέπτουν αριθμούς πιστωτικών καρτών, ή άλλων που κάνουν εικονικές αγορές μέσω Internet, χρησιμοποιώντας αριθμούς καρτών που είναι σχετικά εύκολο να βρει ο απατεώνας ή να τους κατασκευάσει με τη βοήθεια ανάλογων αλγοριθμικών προγραμμάτων με ηλεκτρονικούς υπολογιστές. Επιπλέον, η έλλειψη επαφής «πρόσωπο-με-πρόσωπο» στο διαδίκτυο, τείνει να κάνει τους απατεώνες πιο τολμηρούς. Online αγορές προϊόντων που ποτέ δεν παραδόθηκαν, υπέρογκες χρεώσεις πιστωτικών καρτών για υπηρεσίες που ποτέ δεν ζητήθηκαν ή είχαν αρχικά παρουσιαστεί ότι προσφέρονται δωρεάν, παραπλανητική πληροφόρηση για προϊόντα που αγοράζονται μέσω διαδικτύου, είναι μόνο μερικές από τις καταγγελίες πολιτών που δέχονται καθημερινά οι διωκτικές αρχές της χώρας μας.

Χαρακτηριστικά, αναφέρουμε περιπτώσεις ανθρώπων οι οποίοι, ενδιαφερόμενοι να αγοράσουν κάποιο αυτοκίνητο, τρακτέρ, μηχανή κ.λπ., αναζητούν στο διαδίκτυο την αγγελία που θα καλύψει τις ανάγκες τους. Στη συνέχεια, και αφού έχουν αναπτύξει σχετική επικοινωνία με τον κάτοχο-δράστη, καταβάλλουν κάποια προκαταβολή, συνήθως μέσω εταιρίας πληρωμών (π.χ. Western Union). Εκεί ξεκινούν τα προβλήματα, καθώς ο δράστης προφασίζεται πλέον διάφορες δικαιολογίες για να εισπράξει επιπλέον χρήματα, για να καθυστερήσει και, τελικά, να μην παραδώσει ποτέ το προϊόν.

Πυραμιδικά Συστήματα Εργασίας

Στις απάτες που διαπράττονται μέσω διαδικτύου, συμπεριλαμβάνονται και τα διαδικτυακά πυραμιδικά συστήματα εργασίας από το σπίτι. Πρόκειται για απάτες που υπόσχονται υψηλές αμοιβές και ασυνήθιστα υψηλά κέρδη από επενδύσεις που στην πραγματικότητα δεν υφίστανται. Τελικά, το σύστημα καταρρέει, αφού οι επενδυτές δεν πληρώνονται ούτε τα υποσχόμενα μερίδια ούτε τις προσυμφωνημένες αποδόσεις, με αποτέλεσμα να χάνουν και την αρχική τους επένδυση.

Θέσεις εργασίας

Η παγκόσμια οικονομική κατάσταση έχει φέρει στο προσκήνιο ένα ακόμη είδος απάτης. Πρόκειται για απατηλές διαδικτυακές αγγελίες που αναρτώνται σε ιστοσελίδες εύρεσης εργασίας ή αποστέλλονται μέσω e-mail στο θύμα και περιγράφουν ιδιαίτερα ελκυστικές θέσεις εργασίας συνήθως στο εξωτερικό, ενώ οι δράστες δεν διστάζουν να δημιουργήσουν ιστοσελίδα τής εταιρίας-εργοδότη, στην οποία αναρτούν πληροφορίες για την απατηλή αγγελία προκειμένου να γίνουν ακόμη πιο πειστικοί. Ζητείται από τους ανυποψίαστους υποψήφιους εργαζόμενους να γνωστοποιήσουν τα προσωπικά τους στοιχεία, ακόμη και να αποστείλουν αντίγραφα εγγράφων τους, όπως το δίπλωμα οδήγησης, την ταυτότητά τους και όποιο άλλο θεωρηθεί «χρήσιμο» και «απαραίτητο» για την διεκδίκηση της εν λόγω θέσης εργασίας. Στη συνέχεια, ο εργαζόμενος ενημερώνεται ότι μιας και η εργοδότρια εταιρεία δεν κατέχει τραπεζικό λογαριασμό στην δική του χώρα, ένας από τους πιστωτές της θα του χορηγήσει επιταγή για τα έξοδα και το μισθό του. Η επιταγή συνήθως υπερβαίνει κατά πολύ τα συμφωνηθέντα και ζητείται από τον υποψήφιο να αποστείλει με έμβασμα το επιπλέον ποσό στον εργοδότη. Αφού η διαδικασία ολοκληρωθεί, ο εργαζόμενος αντιλαμβάνεται ότι η επιταγή είναι πλαστή. Σε άλλες περιπτώσεις, το θύμα πείθεται να καταβάλλει ένα ποσό για να κατοχυρώσει την εν λόγω «κάλπικη» θέση εργασίας.

Απάλλειψη Χρέους (Debt Elimination)

Επιπλέον, η ισχύουσα οικονομική κατάσταση έχει οδηγήσει στην άνθηση ενός ακόμη είδους απάτης. Πρόκειται για ιστοσελίδες που υπόσχονται τη διαχείριση και εξάλειψη του χρέους των νοικοκυριών και επιχειρηματιών, διαφημίζοντας νόμιμους τρόπους για την αντιμετώπιση των στεγαστικών δανείων και του χρέους από πιστωτικές κάρτες. Συνήθως, το μόνο που ζητείται είναι η καταβολή ενός αρχικού ποσού, η αποστολή όλων των απαραίτητων πληροφοριών που αφορούν τα επίμαχα δάνεια ή τις πιστωτικές κάρτες και βέβαια, μια εξουσιοδότηση προς το άτομο που θα φέρει εις πέρας τη διαδικασία. Ο διαμεσολαβητής τότε εκδίδει ομόλογα και γραμμάτια προς τους δανειστές που φιλοδοξούν να ικανοποιήσει νόμιμα όλα τα χρέη. Σε αντάλλαγμα, το θύμα είναι υποχρεωμένο να καταβάλει ένα ποσοστό της αξίας των χρεών που θα καλύψει ο διαμεσολαβητής. Η προαναφερθείσα διαδικασία είναι ιδιαίτερα συνδεδεμένη με τα εγκλήματα που σχετίζονται με την κλοπή ταυτότητας, καθώς οι συμμετέχοντες παρέχουν όλες τις προσωπικές πληροφορίες τους προς τους διαμεσολαβητές.

Botnets

Εκατομμύρια υπολογιστές έχουν μετατραπεί σε υποχείρια οργανωμένων hackers, εν αγνοία των χρηστών τους, απειλώντας τη συνολική λειτουργία του διαδικτύου. Έως και το ένα τέταρτο των υπολογιστών που συνδέονται στο διαδίκτυο είναι μολυσμένοι με κρυφό λογισμικό που τους επιστρατεύει σε κακόβουλα δίκτυα, γνωστά ως botnets, ανέφερε ο «πατέρας του Internet» Βιντ Σερφ (επινόησε το πρωτόκολλο TCP/IP). Το φαινόμενο φαίνεται να αποκτά επιδημικές διαστάσεις, καθώς περίπου ένας στους έξι υπολογιστές με σύνδεση στο διαδίκτυο έχουν μετατραπεί σε «ζόμπι» των botnets. Ένας ηλεκτρονικός υπολογιστής θεωρείται ότι είναι υπολογιστής-zombie, όταν είναι συνδεδεμένος στο διαδίκτυο και ελέγχεται από κάποιον εξωτερικό χρήστη. Αυτός ο εξωτερικός χρήστης είναι συνήθως κάποιος hacker που, εξαπολύοντας επιτυχημένη επίθεση ενάντια στον υπολογιστή, καταφέρνει να τον μετατρέψει σε “zombie” computer. Η επίθεση αυτή περιλαμβάνει μεταξύ άλλων την μόλυνση του υπολογιστή-θύματος από κάποιον ιό ή δούρειο ίππο (trojan horse). Οι υπολογιστές-zombies χρησιμοποιούνται κυρίως για την αποστολή άχρηστων ή κακόβουλων ηλεκτρονικών μηνυμάτων (spam-scam). Με τον τρόπο αυτό, οι spammers μπορούν να αποφύγουν τον εντοπισμό τους και χρησιμοποιούν το εύρος ζώνης (bandwidth) των ιδιοκτητών των υπολογιστών zombie για τους δικούς τους σκοπούς.

Τα botnets χρησιμοποιούνται και για την εκτέλεση “DDoS Attacks”, “brute force attacks” σε πληροφοριακά συστήματα και για τη χρήση κατά τη διάρκεια pharming απάτης, με τη συνεχή δημιουργία απατηλών κλώνων σε διαφορετικά σημεία ανά τον κόσμο. Μέχρι στιγμής, τα μεγαλύτερα botnets που έχουν καταγραφεί αριθμούσαν έως και 30.000.000 Η/Υ!!!

Στην Ελλάδα, μεγάλος βιομηχανικός οργανισμός έπεσε θύμα επίθεσης botnet που εκδηλώθηκε με την υποκλοπή όλων των ηλεκτρονικών συνομιλιών κατόπιν επίθεσης στον mail server με τη χρήση botnet, ενώ τραπεζικός οργανισμός δέχθηκε ισχυρό πλήγμα, όταν οι χρήστες των υπηρεσιών διαδικτυακής εξυπηρέτησής του έπεσαν θύματα απάτης τη στιγμή που οι Η/Υ τους κατέστησαν “zombies” με τη χρήση ειδικού προγράμματος “trojan”.

Ιός ransomware

Ένα ακόμη χαρακτηριστικό παράδειγμα της μεθόδου phishing, αποτελεί και ο ιός ransomware ή όπως είναι πλέον γνωστός «ο ιός των 100€». Οι δράστες εκμεταλλευόμενοι τις αδυναμίες του Η/Υ του θύματος, του μεταφέρουν κακόβουλο λογισμικό, καθώς εκείνος περιηγείται στο διαδίκτυο. Το λογισμικό αυτό «κλειδώνει» όλες τις λειτουργίες του Η/Υ και εμφανίζει στην οθόνη του ένα μήνυμα που υποτίθεται ότι προέρχεται από τη Δίωξη Ηλεκτρονικού Εγκλήματος, ενημερώνοντας τον χρήστη ότι του καταβάλλεται το πρόστιμο των 100 € για αδικήματα του Ποινικού Κώδικα που υποτίθεται ότι διέπραξε ο ίδιος. Η καταβολή του προστίμου δύναται να πραγματοποιηθεί με τη χρήση προπληρωμένων καρτών paysafe ή ucash. Πρόκειται για έναν ιό με πανευρωπαϊκή παρουσία, που χρησιμοποιεί τα εμβλήματα της εκάστοτε αστυνομίας της χώρας από την οποία ο Η/Υ του θύματος έχει πρόσβαση στο διαδίκτυο. Χιλιάδες χρήστες έχουν πέσει θύματα αυτού, ενώ δεν είναι λίγοι κι εκείνοι που έχουν τελικά καταβάλλει το επίμαχο χρηματικό ποσό. Πρόκειται για ένα άριστα οργανωμένο κύκλωμα, το οποίο μέσα από μια πολύπλοκη διαδικασία και μέσα από μηχανισμούς ξεπλύματος μαύρου χρήματος, καταφέρνουν να διασπούν τις προπληρωμένες κάρτες των 100€ σε κάρτες αξίας 10€, τις οποίες και διανέμουν σε όλο τον κόσμο.

Κινητά τηλέφωνα και διαδικτυακές παγίδες

Η χρήση των κινητών τηλεφώνων -και δη των smart-phones- αυξάνεται συνεχώς και όλο και περισσότεροι χρήστες χρήζουν αυτά ως απαραίτητα εργαλεία για την καθημερινότητά τους. Επιτήδειοι, εκμεταλλευόμενοι την τάση αυτή, προκαλούν απάτες αρκετών εκατομμυρίων ευρώ από την αγοραπωλησία εφαρμογών software για κινητά τηλέφωνα, όπως, για παράδειγμα, ο εντοπισμός του κινητού τηλεφώνου κάποιου αγαπημένου προσώπου. Συνήθως ζητείται από τον ανυποψίαστο χρήστη, να εισάγει το κινητό του τηλέφωνο προκειμένου να αποκτήσει την εφαρμογή που έχει επιλέξει. Στη συνέχεια, ξεκινούν οι υπέρογκες χρεώσεις στον αριθμό του, τις οποίες ο ίδιος αποδέχτηκε, καθώς αυτές περιγράφονται στα ψιλά γράμματα των όρων χρήσης που η πλειοψηφία των καταναλωτών δεν διαβάζουν.

Ηλεκτρονικές Δημοπρασίες (Auctions)

Ένα είδος απάτης που είναι ιδιαίτερα διαδεδομένο σε χώρες του εξωτερικού, αφορά τις διαδικτυακές δημοπρασίες. Αυτού του είδους οι απάτες, εστιάζουν κυρίως στην διαστρεβλωμένη παρουσίαση ή στην μη παράδοση του δημοπρατούντος προϊόντος. Οι καταναλωτές θα πρέπει να είναι ιδιαίτερα προσεκτικοί όταν οι πωλητές τους ζητούν να καταβάλλουν το συμφωνημένο χρηματικό ποσό σε λογαριασμό κάποιου τρίτου ή επικαλούνται έκτακτους λόγους που τους αναγκάζουν να εγκαταλείψουν την χώρα τους. Επίσης, όταν η καταβολή του ποσού ζητείται να πραγματοποιηθεί μέσω Western Union ή MoneyGram.

Οι Νόμοι στην Πραξη

Τα στελέχη της Υποδιεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος για την αντιμετώπιση των παραβατικών πράξεων που συντελούνται μέσα από το διαδίκτυο και συνιστούν το αδίκημα της «Απάτης», έχουν ως ουραγό τη νομοθεσία και καθοδηγούνται από δύο βασικά άρθρα του κοινού Ποινικού Κώδικα (Π.Κ.): α) άρθρο 386 «Απάτη» και β) άρθρο 386Α «Απάτη με υπολογιστή», τα οποία περιληπτικά περιγράφονται ως εξής:

Άρθρο 386 «Απάτη»

1. Όποιος, με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, τιμωρείται με φυλάκιση τουλάχιστον τριών[3] μηνών και αν η ζημιά που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο (2) ετών.

3. Επιβάλλεται κάθειρξη μέχρι δέκα (10) ετών: α) αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημιά υπερβαίνουν το ποσό των δεκαπέντε χιλιάδων (15.000) ευρώ ή β) εάν το περιουσιακό όφελος ή η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσό των τριακοσίων χιλιάδων (300.000) ευρώ.

Άρθρο 386Α «Απάτη με υπολογιστή»
Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλο παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος, είτε με επέμβαση κατά την εφαρμογή του, είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων, είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του άρθρου 386. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημιάς, είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα πρόσωπα.

Πόσο άραγε κοστίσει το κυβερνοέγκλημα στις επιχειρήσεις;

Μία από τις μεγαλύτερες εταιρείες τεχνολογίες στον κόσμο, παρουσίασε περί τα τέλη του 2012 μια νέα έρευνα, η οποία αναδεικνύει ότι το κόστος και η συχνότητα του κυβερνοεγκλήματος συνέχισαν να αυξάνονται για τρίτη συνεχόμενη χρονιά. Σύμφωνα με την τρίτη ετήσια έρευνα που αφορούσε πολυεθνικές εταιρείες των Η.Π.Α., η συχνότητα των κυβερνοεπιθέσεων έχει σημειώσει ραγδαία αύξηση μέσα σε τρία χρόνια, ενώ οι οικονομικές τους επιπτώσεις αυξήθηκαν περίπου κατά 40%. Η έρευνα για το Κόστος του Κυβερνοεγκλήματος για το 2012 (Cost of Cyber Crime Study 2012), η οποία διενεργήθηκε από το **Ponemon Institute,** κατέδειξε ότι το **μέσο ετήσιο κόστος του κυβερνοεγκλήματος** για ένα ενδεικτικό δείγμα επιχειρήσεων στις Η.Π.Α. ανήλθε στα **8,9 εκατομμύρια δολάρια.** Το ποσό αυτό παρουσιάζει αύξηση 6% σε σχέση με το μέσο κόστος για το 2011 και 38% σε σχέση με το αντίστοιχο μέγεθος για το 2010. Επίσης, η φετινή έρευνα κατέγραψε μια αύξηση 42% στον αριθμό των κυβερνοεπιθέσεων, με τους οργανισμούς να αντιμετωπίζουν κατά μέσο όρο **102 ολοκληρωμένες επιθέσεις την εβδομάδα,** ενώ αντιμετώπιζαν 72 και 50 επιθέσεις την εβδομάδα, το 2011 και το 2010 αντίστοιχα.

Ανώτατο στέλεχος της εταιρείας που πραγματοποίησε την έρευνα δήλωσε:

«Οι οργανισμοί ξοδεύουν συνεχώς περισσότερο χρόνο, χρήμα και ενέργεια για να ανταποκριθούν στις κυβερνοαπειλές, φτάνοντας σε επίπεδα που σύντομα θα καταστούν μη βιώσιμα, υπάρχουν στοιχεία που ξεκάθαρα δείχνουν ότι η χρήση προηγμένων λύσεων "security intelligence" βοηθά στην ουσιαστική μείωση του κόστους, της συχνότητας και των επιπτώσεων αυτών των επιθέσεων».

Και φέτος, το **μεγαλύτερο κόστος** για τις επιχειρήσεις προήλθε από κυβερνοεγκλήματα, όπως η χρήση κακόβουλων κωδικών, οι επιθέσεις άρνησης υπηρεσίας, η χρήση κλεμμένων ή παραβιασμένων συσκευές και η κακόβουλη δραστηριότητα προσώπων που βρίσκονται μέσα σε έναν οργανισμό. **Συνδυαστικά,** το **κόστος** που προέρχεται από αυτές τις απειλές αντιστοιχεί σε **περισσότερο από το 78% του ετήσιου κόστους του κυβερνοεγκλήματος ανά οργανισμό.**

Επίσης, η έρευνα κατέληξε στα παρακάτω **βασικά ευρήματα:**

- Η κλοπή πληροφοριών και η διακοπή των εργασιών συνεχίζουν να αντιστοιχούν στο μεγαλύτερο εξωτερικό κόστος για τις επιχειρήσεις. Σε ετήσια βάση, η **υποκλοπή πληροφοριών ισοδυναμεί με το 44% του συνολικού εξωτερικού κόστους,** σημειώνοντας άνοδο 4% σε σχέση με το 2011. Η διακοπή των εργασιών ή η μείωση της παραγωγικότητας αντιστοιχεί στο 30% του εξωτερικού κόστους, σημειώνοντας άνοδο 1% από το 2011.
- Η χρήση **προηγμένων λύσεων ασφάλειας πληροφοριών και διαχείρισης περιστατικών (Security Information & Event Management–SIEM)** μπορεί να περιορίσει τις επιπτώσεις των κυβερνοαπειλών. Οι οργανισμοί που χρησιμοποίησαν τέτοιες λύσεις εξοικονόμησαν περίπου 1,6 εκατομμύρια δολάρια το χρόνο. Γι' αυτούς τους οργανισμούς, το κόστος για την ανάκτηση των συστημάτων, τον εντοπισμό και τον περιορισμό των απειλών ήταν σημαντικά μικρότερο σε σχέση με το κόστος που αντιμετώπισαν όσοι δεν αξιοποίησαν λύσεις SIEM.
- Οι κυβερνοεπιθέσεις μπορεί να κοστίσουν ακριβά, αν δεν αντιμετωπιστούν γρήγορα. Ο μέσος χρόνος αντιμετώπισης μιας κυβερνοεπίθεσης είναι 24 μέρες, αλλά μπορεί να φτάσει μέχρι και τις 50, σύμφωνα με τη φετινή μελέτη. Το μέσο κόστος που προέκυψε για την περίοδο των 24 ημερών ανερχόταν σε $591.780, καταγράφοντας

αύξηση 42% σε σχέση με το μέσο εκτιμώμενο κόστος των $415.748 για την ίδια περίοδο πέρσι.
- Η ανάκτηση δεδομένων και ο εντοπισμός των απειλών παραμένουν οι πιο δαπανηρές εσωτερικές δραστηριότητες σε σχέση με το κυβερνοέγκλημα. Σε ετήσια βάση, αυτές οι δραστηριότητες αντιστοιχούν στο μισό σχεδόν του συνολικού εσωτερικού κόστους, με τα λειτουργικά έξοδα και το κόστος εργασίας να αντιστοιχούν στο μεγαλύτερο μέρος του.

Ο Πρόεδρος και Ιδρυτής του Ponemon Institute, Dr. Larry Ponemon, δήλωσε ότι αυτοσκοπός αυτής της έρευνας είναι να ποσοτικοποιήσει τις οικονομικές επιπτώσεις των κυβερνοεπιθέσεων και να καταγράψει τις διαχρονικές τάσεις που αφορούν το σχετικό κόστος, και ότι η καλύτερη κατανόηση του κόστους του κυβερνοεγκλήματος θα βοηθήσει τους οργανισμούς να καθορίσουν τις κατάλληλες επενδύσεις και τους πόρους που χρειάζονται, ώστε να μετριάσουν τις καταστροφικές συνέπειες μιας επίθεσης.

Αντίστοιχες μελέτες για το κόστος του κυβερνοεγκλήματος έχουν πραγματοποιηθεί στην Αυστραλία, τη Γερμανία, την Ιαπωνία και το Ηνωμένο Βασίλειο με παρόμοια αποτελέσματα. Για παράδειγμα, η εταιρεία λύσεων τεχνολογίας ασφάλειας πληροφοριακών συστημάτων RSA δημοσίευσε για το 1ο εξάμηνο του 2012 έρευνα σχετικά με την αύξηση του κόστους που απέφερε το phishing σε εταιρείες του Η.Β., του Καναδά και των Η.Π.Α. Το phising υφίσταται ως φαινόμενο για τα τελευταία 16 χρόνια και εξακολουθεί να αποτελεί έναν από τους υψηλότερους κινδύνους που κρύβει το διαδίκτυο. Το κόστος του σημείωσε αύξηση κατά 19% σε σχέση με το αντίστοιχο του 1ου εξαμήνου του 2011 και απέφερε ζημιά ύψους $687 εκατ. για τις αμερικάνικες εταιρείες. Η έρευνα κατέδειξε ότι το Η.Β., οι Η.Π.Α., ο Καναδάς, η Βραζιλία και η Νότια Αφρική συγκαταλέγονται στις χώρες με τις περισσότερες επιθέσεις phising διεθνώς. Συγκεκριμένα στον Καναδά, τα φαινόμενα phising σημείωσαν αύξηση κατά 400% κατά το 1ο εξάμηνο του 2012 σε σχέση με το αντίστοιχο περσινό, γεγονός που ενδεχομένως οφείλεται στην οικονομική σταθερότητα της χώρας, αλλά και της ισοτιμίας σχεδόν 1:1 σε σχέση με το αμερικάνικο δολάριο, καθώς οι «απατεώνες» αρέσκονται να ακολουθούν το χρήμα.

Όπως και να έχει τελικά, παρά το γεγονός ότι το phising ήδη μετρά 16 χρόνια ζωής και θεωρείται «παλαιό» φαινόμενο, κανείς δε μπορεί να αγνοήσει ζημιά $687 εκατομμυρίων.

Online συναλλαγές και ασφάλεια

Με την πάροδο του χρόνου, όλο και περισσότερες επιχειρήσεις δραστηριοποιούνται μέσω του διαδικτύου, αυξάνοντας τα έσοδά τους, μειώνοντας το κόστος τους και διευκολύνοντας τους χρήστες. Με τον τρόπο αυτό, ο καθένας δύναται να έχει πρόσβαση όλο το 24ωρο στον κατάλογο μιας επιχείρησης και να αγοράσει ότι επιθυμεί. Οι περισσότερες ιστοσελίδες που πουλούν προϊόντα, χρησιμοποιούν συστήματα πληρωμών - συναλλαγών, όπως το paypal, διατραπεζικά συστήματα, κ.λπ.

Είναι όμως οι online συναλλαγές ασφαλείς;

Πως μπορούμε να είμαστε βέβαιοι ότι δεν θα πέσουμε εξαπατηθούμε και πως μπορούμε να υποψιαστούμε απάτες ώστε να τις αποφύγουμε;

Τι θα πρέπει να προσέχει κανείς όσον αφορά τις συναλλαγές του

1) Να μην κάνει τις συναλλαγές του χρησιμοποιώντας **δημόσιους υπολογιστές** (από net cafe, καφετέριες, βιβλιοθήκες, κ.λπ.). Μπορεί να έχουν keyloggers ή spywares, χωρίς να το γνωρίζει το προσωπικό του χώρου αυτού. Έτσι, μπορούν εύκολα να υποκλέψουν τα ευαίσθητα προσωπικά στοιχεία κάποιου και να προβούν σε συναλλαγές οι κακόβουλοι χρήστες αντ' αυτού.

2) Όταν πραγματοποιεί συναλλαγές από τον υπολογιστή του, θα πρέπει να είναι σίγουρος ότι έχει λάβει όλα τα **απαραίτητα μέτρα ασφαλείας πρόσφατα ενημερωμένα** (firewall, antivirus, antispyware, κ.λπ.).
3) Όταν συγκρίνει προϊόντα από διάφορες ιστοσελίδες, μπορεί να βρει σε κάποιες εξ αυτών **τα ίδια προϊόντα φθηνότερα σε σχέση με άλλες ιστοσελίδες.** Καλό θα ήταν, λοιπόν, να ψάξει μήπως οι ιστοσελίδες αυτές είναι φαντάσματα (μία αναζήτηση στο google με την επωνυμία της ιστοσελίδας με τα πολύ φθηνά προϊόντα αρκεί).
4) Πάντα να κάνει τις συναλλαγές του, **πληκτρολογώντας ο ίδιος τη διεύθυνση της ιστοσελίδας.** Να μην κλικάρει πάνω σε links από e-mail, καθώς μπορεί να είναι απατηλά.
5) Να πραγματοποιεί τις πληρωμές-συναλλαγές του μόνο μέσω ιστοσελίδων που έχουν το **εικονίδιο ασφαλείας** (μία κλειδαριά πάνω αριστερά στον browser). Το εικονίδιο αυτό μας ενδιαφέρει ουσιαστικά εκεί που πληκτρολογούμε π.χ. αριθμό κάρτας και τα υπόλοιπα ευαίσθητα προσωπικά στοιχεία και κλικάρουμε αποστολή.
6) Να επαληθεύει ότι εκεί που πληκτρολογεί τα ευαίσθητα στοιχεία του, στον browser δε γράφει http αλλά **https.**
7) Προτού πραγματοποιήσει κάποια συναλλαγή μέσω μιας ιστοσελίδας, θα πρέπει να **καλέσει** στο ηλεκτρονικό κατάστημα, προκειμένου να επιβεβαιώσει εάν θα του απαντήσουν και εάν είναι εκεί και λειτουργεί η επιχείρηση. Εάν δεν απαντήσουν, το πιθανότερο είναι να μην αποστείλουν ούτε το αγορασθέν προϊόν, ακόμη και εάν έχει πληρωθεί.
8) Πάντα να τηρεί κάπου στον υπολογιστή του ή να εκτυπώνει τις **αποδείξεις** από τις αγορές του.
9) Να είναι ιδιαίτερα προσεκτικός όσον αφορά συναλλαγές μέσω **εταιρειών μεταφοράς χρημάτων και διεθνών πληρωμών** (Western Union, MoneyGram, BidPay κ.λπ.)
10) Να είναι βέβαιος ότι οι κωδικοί του, οι αριθμοί των καρτών του (χρεωστικών-πιστωτικών) και τα άλλα ευαίσθητα προσωπικά στοιχεία του, είναι **φυλαγμένα επαρκώς,** ώστε να μη μπορεί κάποιος να τα υποκλέψει ή να τα απομνημονεύσει.
11) Να φροντίζει ώστε να **αλλάζει** τους **κωδικούς** του σε τακτά χρονικά διαστήματα, και αυτοί να αποτελούνται από μικρά και κεφαλαία γράμματα, αριθμούς και σύμβολα.

Τι θα πρέπει να προσέχει κανείς όσον αφορά τις αγορές του

1) Ποτέ να μην πληρώνει προκαταβολικά σε πωλητή, τον οποίο δε γνωρίζει, ακόμη και εάν αυτός αποκαλύπτει τα προσωπικά του στοιχεία ή τον αριθμό του τραπεζικού του λογαριασμού.
2) Να αναζητά πληροφορίες-αναρτήσεις σχετικά με το πώς το διαδικτυακό κατάστημα διαχειρίζεται τυχόν παράπονα πελατών του.
3) Να ζητά την αυθεντική απόδειξη ή γραπτή απόδειξη αγοράς.
4) Να προσέχει ιδιαιτέρως όταν η προσφορά φαίνεται πολύ καλή για να είναι αληθινή και το άλλο μέρος ασκεί συνεχώς πίεση για την ολοκλήρωση της αγοραπωλησίας.
5) Να προσέχει όταν του ζητείται η πληρωμή μεγάλων ποσών σε ανθρώπους που δε γνωρίζει, θα πρέπει να πραγματοποιείται συνάντηση σε κάποιο κατάστημα ή δημόσιο χώρο.
6) Να προσέχει εάν κατά την αγορά επώνυμων προϊόντων αυτά είναι όντως αυθεντικά.

Πως να προστατεύσει κανείς τις συναλλαγές μέσω κινητού τηλεφώνου;

1) Να διατηρεί το λογισμικό προστασίας του κινητού του τηλεφώνου επικαιροποιημένο και όλες τις συσκευές που συνδέονται με αυτό προφυλαγμένες από κακόβουλες επιθέσεις και ιούς.
2) Να χρησιμοποιεί έναν ισχυρό κωδικό προκειμένου να κλειδώνεται τη συσκευή του κινητού του τηλεφώνου.
3) Να μελετά προσεκτικά τις εφαρμογές που επιθυμεί να εγκαταστήσει, πριν το κάνει.
4) Να δίνει τον αριθμό του κινητού του τηλεφώνου μόνο σε άτομα της εμπιστοσύνης του και μη δίνει τον αριθμό τού κινητού άλλων χωρίς την έγκρισή τους.
5) Να ενεργοποιήσει την υπηρεσία «γεωεντοπισμού» του κινητού του σε περίπτωση που το χάσει.
6) Να είναι ιδιαίτερα προσεκτικοί με τα Wi-Fi Hotspot δίκτυα στα οποία συνδέεται με το κινητό του τηλέφωνο.
7) Όταν γίνεται αποδέκτης μηνυμάτων, τον αποστολέα των οποίων δε γνωρίζει, να μην ανταποκρίνεται.
8) Να μπλοκάρει τους χρήστες των οποίων τον αριθμό και το e-mail δε γνωρίζει, χρησιμοποιώντας CALLER ID.
9) Να επιβάλει σε όσους προσπαθούν να τον τραβήξουν φωτογραφία ή βίντεο να λαμβάνουν πρώτα την άδειά του.

Χρήσιμα Links

Χρήσιμες συμβουλές από τη Δίωξη Ηλεκτρονικού Εγκλήματος:
http://www.astynomia.gr/

Ανοικτή γραμμή για το παράνομο περιεχόμενο στο διαδίκτυο:
http://www.safeline.gr

Ελληνικός κόμβος ασφαλούς διαδικτύου:
www.saferinternet.gr

Οργανισμός προστασίας των δικαιωμάτων των παιδιών:
http://www.hamogelo.gr

Συμβουλές ασφαλείας για online chatting:
http://www.chatdanger.com

Ιστότοπος από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος:
www.cyberkid.gr

Πανελλήνιο σχολικό δίκτυο:
www.sch.gr

Μονάδα Εφηβικής Υγείας, Β' Παιδιατρική κλινική Πανεπιστημίου Αθηνών, Νοσοκομείο Παίδων:
www.youth-health.gr

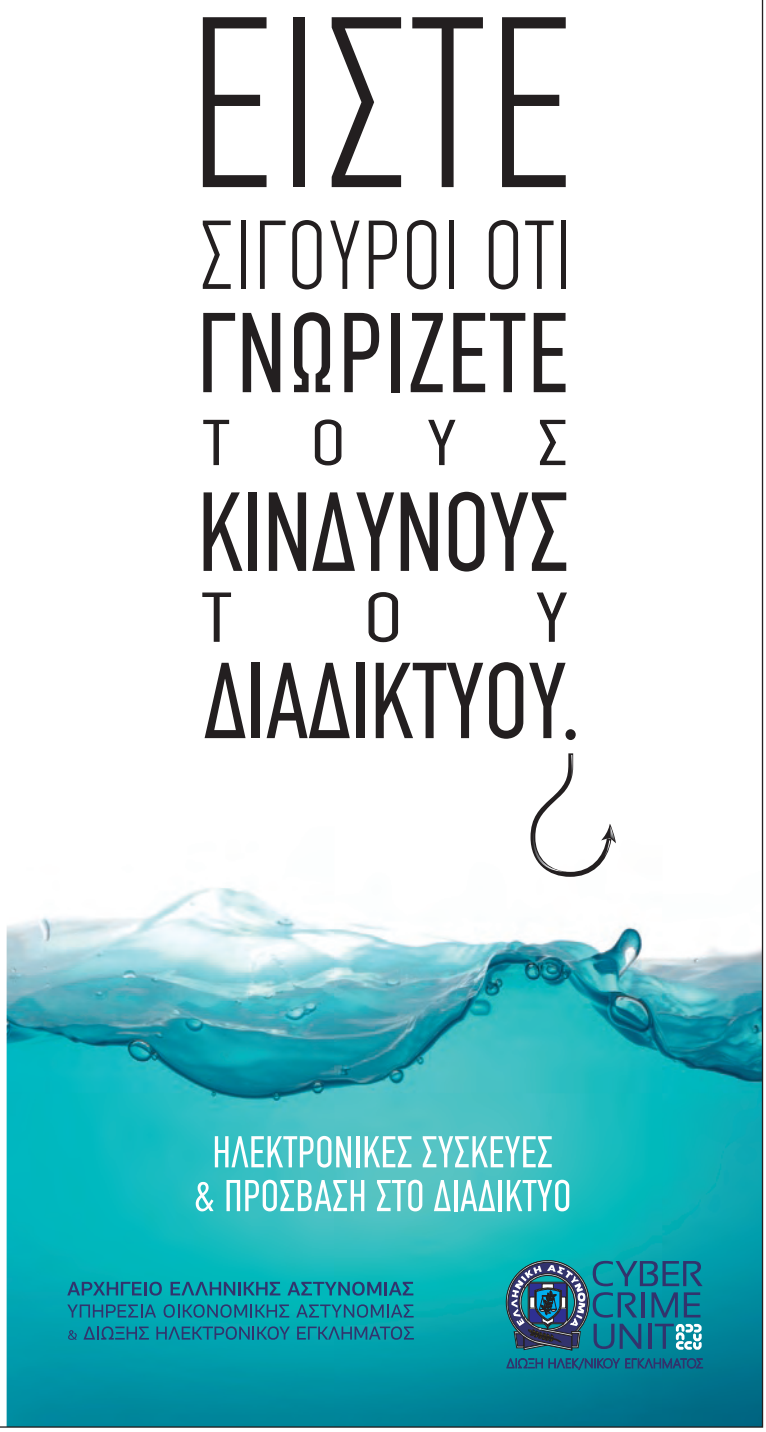
Ελληνική Εταιρεία Μελέτης της Διαταραχής Εθισμού στο Διαδίκτυο:
www.hasiad.gr

Επικοινωνία

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173,
Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

Χορηγός Φιλοξενίας

Χορηγός Επικοινωνίας



ΗΡΘΕ Η ΣΤΙΓΜΗ ΝΑ ΕΝΗΜΕΡΩΘΕΙΤΕ ΥΠΕΥΘΥΝΑ ΓΙΑ ΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΤΟΥΣ ΚΙΝΔΥΝΟΥΣ ΤΟΥ.

Σίγουρα, ο καθένας από εμάς έχει ακούσει να λέγονται πολλά για το διαδίκτυο και τους κινδύνους που μπορεί να κρύβει ανάμεσα στις χιλιάδες ιστοσελίδες και blogs, σε φαινομενικά αθώα μηνύματα στο ηλεκτρονικό μας ταχυδρομείο, αλλά και σε εφαρμογές που, εκεί που «σερφάρουμε» ανυποψίαστοι, εμφανίζονται ως διά μαγείας και ζητάνε τη συνεισφορά μας ή να πατήσουμε «ΟΚ» για να συνεχίσουμε... πού όμως;

Πολλές και διαφορετικές είναι οι καιροσκοπικές ή κακόβουλες ενέργειες κατά των χρηστών του διαδικτύου και το λιγότερο που μπορούμε να κάνουμε, είναι να μη σταματήσουμε ποτέ να ρωτάμε και να ενημερωνόμαστε για το τι μπορεί ν' αποτελέσει κίνδυνο στο διαδίκτυο τόσο για εμάς όσο και για τα παιδιά μας, τους φίλους και τους συγγενείς μας.

Ήρθε η στιγμή λοιπόν να ενημερωθούμε σε βάθος, επίσημα και υπεύθυνα, για τους κινδύνους του διαδικτύου. Στα χέρια σας κρατάτε ένα επίσημο πληροφοριακό έντυπο από την Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, το οποίο θα σας βοηθήσει να ενημερωθείτε σε βάθος και υπεύθυνα για τους κινδύνους που διατρέχετε κατά την παραμονή σας στο διαδίκτυο.

Για να μην «τσιμπάμε» τόσο εύκολα...

ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΣΚΕΥΕΣ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

ΑΣΦΑΛΗΣ ΧΡΗΣΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

I. iPhone & iPad

1. Συμβουλές Ασφαλούς Χρήσης προσωπικών iPhone & iPad

Στην παρακάτω ενότητα, θα βρείτε μερικές βασικές συμβουλές για την ασφαλή χρήση του iPhone και του iPad που χρησιμοποιούν το λειτουργικό σύστημα iOS 4. Οι οδηγίες δεν αφορούν συσκευές οι οποίες λειτουργούν σε εταιρικό περιβάλλον, αλλά μόνον συσκευές των οποίων τον έλεγχο έχει ο χρήστης. Πληροφορίες σχετικά με εταιρική σύνδεση και με θέματα όπως το VPN, μπορούν να αναζητηθούν στην ιστοσελίδα της Apple
http://www.apple.com/support/iphone/enterprise

2. Ασφάλεια της συσκευής

Πρέπει συνεχώς να προστατεύουμε τη φορητή ηλεκτρονική συσκευή από τυχόν επιτήδειους που θα θελήσουν να προσθέσουν κάποιο ύποπτο λογισμικό ή απλώς να διαβάσουν προσωπικά στοιχεία μας. Υπάρχουν αρκετοί τρόποι με τους οποίους κάποιος μπορεί να παρακάμψει τους μηχανισμούς ασφαλείας μιας συσκευής, έχοντας αποκτήσει πρόσβαση σε αυτήν. Ιδιαίτερα για τα κινητά τηλέφωνα, είναι αυξημένος ο κίνδυνος να αποκτήσει κάποιος πρόσβαση σε αυτά. Ο καλύτερος τρόπος προφύλαξης είναι να εξασφαλίσουμε ότι οι συσκευές μας με λειτουργικό iOS δεν θα βρεθούν σε χέρια ανθρώπων που θέλουν να μας βλάψουν. Αν αναλογιστούμε τον ιδιαίτερα υψηλό κίνδυνο να διαρρεύσουν ευαίσθητα δεδομένα που είναι αποθηκευμένα στη συσκευή μας, μπορούμε να αντιληφθούμε πόσο σημαντικό θέμα είναι η προστασία της. Τα δεδομένα που αποθηκεύονται μπορεί να είναι από συνθηματικές λέξεις που χρησιμοποιούνται σε κοινωνικά δίκτυα, μέχρι κωδικοί πιστωτικών καρτών. Αν το κινητό σας τηλέφωνο βρεθεί σε λάθος χέρια, σκεφτείτε σε πόσες πληροφορίες θα μπορεί κάποιος να έχει πρόσβαση!

3. Αναβάθμιση – Ενημέρωση Λογισμικού

Κάθε φορά η αναβάθμιση του κινητού τηλεφώνου θα πρέπει να γίνεται με το πιο πρόσφατο λογισμικό του iOS.
Οι αναβαθμίσεις αυτές θα πρέπει να γίνονται μέσω ενός συνδεδεμένου με το διαδίκτυο προσωπικού υπολογιστή, στον οποίο έχουμε εγκαταστήσει το πρόγραμμα iTunes. Τόσο η ενημέρωση του λογισμικού της κινητής συσκευής όσο και η εγκατάσταση του iTunes αποτελούν αποκλειστική ευθύνη του χρήστη. Προτείνεται να γίνεται ενημέρωση του λογισμικού από ηλεκτρονικό υπολογιστή τον οποίο γνωρίζουμε.

4. Μη χρησιμοποιείτε τεχνικές «Jailbreak»

Ο όρος «Jailbreak» αναφέρεται στη διαδικασία αλλαγής του λειτουργικού συστήματος μιας συσκευής iOS, κατά παράβαση της άδειας χρήσης του τελικού χρήστη. Με τη διαδικασία του «Jailbreak» μειώνεται σημαντικά η ικανότητα της συσκευής να αντιμετωπίσει επιθέσεις, γιατί αναστέλλεται η εφαρμογή των υπογραφών κώδικα, οι οποίες αποτελούν σημαντικό στοιχείο ασφαλείας. Με τη διαδικασία του «Jailbreak» είναι κατά πολύ ευκολότερο να έχει κανείς πρόσβαση σ' ένα iPhone ή iPad. Οι περισσότερες δημόσιες επιθέσεις με στόχο συσκευές iOS απαιτούν να έχει γίνει πρώτα «Jailbreak». Μια ακόμα παρεμφερής ανησυχία που εκφράζεται, αφορά την ποιότητα των εργαλείων και των εφαρμογών που προσφέρει η κοινότητα του «Jailbreak». Αυτές οι δωρεάν εφαρμογές κατασκευάζονται με ελάχιστη επίβλεψη και περιορισμένες δοκιμές. Ενδέχεται να περιλαμβάνουν ιούς ή άλλο κακόβουλο λογισμικό, και μπορεί να προκαλέσουν σοβαρές, ανεπανόρθωτες βλάβες στη συσκευή σας, καταστρέφοντας τα δεδομένα σας.

5. Ενεργοποίηση του Αυτόματου Κλειδώματος και του Κλειδώματος Συνθηματικού

Η ενεργοποίηση του Αυτόματου Κλειδώματος κλειδώνει αυτόματα την οθόνη του κινητού μετά από μια εκ των προτέρων ορισμένη περίοδο αδράνειας του κινητού τηλεφώνου. Θα πρέπει να βεβαιωθούμε ότι το Αυτόματο Κλείδωμα είναι ενεργοποιημένο. Προτεινόμενος χρόνος κλειδώματος του τηλεφώνου είναι τα 3 λεπτά, περίπου.

- Πηγαίνουμε στα Settings → General → Auto Lock.
- Ορίζουμε το χρόνο Αυτόματου Κλειδώματος στα 3 λεπτά.

Για να είναι αποτελεσματικό το Αυτόματο Κλείδωμα, **θα πρέπει να συνδυάζεται** με το Κλείδωμα Συνθηματικού. Με τη χρήση του Αυτόματου Κλειδώματος και του Κλειδώματος Συνθηματικού μπορούμε να έχουμε καλύτερη προστασία. Το συνθηματικό θα πρέπει να έχει 4 ψηφία, και θα πρέπει να δίνεται κάθε φορά που κλειδώνει η οθόνη. Για να γίνει αυτό, πρέπει να γίνουν οι παρακάτω ρυθμίσεις:

- Πηγαίνουμε στα Settings → General → Passcode Lock.
- Θέτουμε σε λειτουργία (ON) το «Passcode Lock».
- Ορίζουμε το «Require Passcode» σε Immediately.

Σημείωση: Στην ίδια οθόνη θα πρέπει να τεθεί εκτός λειτουργίας το Simple Passcode, ούτως ώστε να μπορούν να οριστούν συνθηματικά που συνδυάζουν γράμματα και αριθμούς.

Για να έχετε περισσότερη ασφάλεια, ενεργοποιήστε την Αυτόματη Διαγραφή Δεδομένων για να διαγράψετε όλα τα δεδομένα που έχουν δημιουργηθεί από το χρήστη, μετά από δέκα αποτυχημένες προσπάθειες πρόσβασης με συνθηματικό στη συσκευή.

- Πηγαίνουμε στα Settings → General → Passcode Lock.
- Θέτουμε σε λειτουργία (ON) το «Erase Data».

6. Μη συνδέεστε με ασύρματα δίκτυα που δεν εμπιστεύεστε

Όσο είναι δυνατόν, να αποφεύγετε ή να περιορίζετε τη χρήση ασύρματων δικτύων. Όταν δεν τα χρησιμοποιείτε, θα πρέπει να απενεργοποιείτε τη συσκευή για να μην είναι εκτεθειμένη.

- Πηγαίνουμε στα Settings → Wi-Fi.
- Θέτουμε εκτός λειτουργίας (OFF) τα Wi-Fi.

Αντισταθείτε στον πειρασμό να χρησιμοποιήσετε σημεία δωρεάν ασύρματης πρόσβασης στο διαδίκτυο. Τα περισσότερα από αυτά δεν προσφέρουν καμιά προστασία σε δεδομένα που μεταδίδονται ασύρματα, κάτι που σημαίνει ότι οποιοσδήποτε βρίσκεται κοντά, μπορεί να τα υποκλέψει. Αν, παρ' όλ' αυτά, είναι απολύτως απαραίτητο να χρησιμοποιήσετε ασύρματο δίκτυο, διαλέξτε κάποιο που να το ξέρετε, και φροντίστε τα δεδομένα που ανταλλάσσετε με άλλους να είναι **κρυπτογραφημένα**. Στη λίστα των διαθέσιμων δικτύων, όσα είναι προστατευμένα συνοδεύονται από το εικονίδιο κλειδαριάς δίπλα στο όνομά τους.

Για να απενεργοποιηθεί η αυτόματη σύνδεση σε ασύρματα δίκτυα, κάνουμε τις παρακάτω ενέργειες:

- Πηγαίνουμε στα Settings → Wi-Fi.
- Θέτουμε την εντολή «Ask to join Networks» στο OFF.

Σημαντική Σημείωση. Ακόμα και αν τεθεί εκτός λειτουργίας η αυτόματη σύνδεση σε ασύρματο δίκτυο, η συσκευή θα συνδεθεί αυτομάτως με δίκτυα τα οποία έχει επισκεφθεί προηγουμένως και τα οποία εξακολουθούν να υπάρχουν στη μνήμη της.

Ένα άλλο μέτρο προστασίας που μπορούμε να πάρουμε, είναι να επιλέξουμε την εντολή «Forget this Network» μετά από κάθε ασύρματη σύνδεση. Αυτό θα μειώσει τις πιθανότητες να συνδεθεί η συσκευή μας με λειτουργικό σύστημα iOS με κάποιο άλλο ασύρματο δίκτυο που έχει το ίδιο όνομα. Είναι σημαντικό να

επιλέξουμε αυτή την εκδοχή πριν βγούμε από το βεληνεκές του συγκεκριμένου δικτύου. Σε διαφορετική περίπτωση, το δίκτυο δεν θα εμφανίζεται στη λίστα των διαθέσιμων δικτύων και δεν θα είναι δυνατόν να το αφαιρέσουμε.

- Πηγαίνουμε στα Settings → Wi-Fi.
- Επιλέγουμε δίκτυο από τη λίστα.
- Επιλέγουμε την εντολή «Forget this Network».

7. Απενεργοποιήστε το Bluetooth, εκτός αν το χρειάζεστε

Το Bluetooth θα πρέπει να είναι ενεργοποιημένο μόνο όταν μας είναι απολύτως απαραίτητο. Όταν δεν το χρησιμοποιούμε, θα πρέπει να το έχουμε κλειστό, ώστε να μην μπορούν άλλες συσκευές να ανακαλύψουν την iOS συσκευή μας και να προσπαθήσουν να συνδεθούν μαζί της.

- Πηγαίνουμε στα Settings → General → Bluetooth.
- Θέτουμε το «Bluetooth» στο OFF.

8. Απενεργοποιήστε τις Υπηρεσίες Εντοπισμού, εκτός αν τις χρειάζεστε

Οι Υπηρεσίες Εντοπισμού μπορεί να χρησιμοποιηθούν από εφαρμογές στη συσκευή σας με σκοπό να ανακαλύψουν το σημείο στο οποίο είστε. Οι Υπηρεσίες Εντοπισμού θα πρέπει να είναι σε λειτουργία μόνο αν υπάρχει κάποια επείγουσα ανάγκη και οι Εφαρμογές πρέπει να γνωρίζουν πού βρίσκεστε. Διαφορετικά, απενεργοποιήστε τες ή κάντε περιορισμένη χρήση τους. Για να απενεργοποιήσουμε τις Υπηρεσίες Εντοπισμού, κάνουμε τα ακόλουθα:

- Πηγαίνουμε στα Settings (Settings → General σε iPads).
- Θέτουμε το «Location Services» στο OFF.

Οι εφαρμογές που χρησιμοποιούν την υπηρεσία «Location Services» θα ζητήσουν να κάνουν χρήση της την πρώτη φορά που θα τις θέσετε σε λειτουργία. **Σκεφτείτε προσεκτικά αυτά τα αιτήματα και επιτρέψτε τη λειτουργία των Υπηρεσιών Εντοπισμού μόνο όταν αυτό είναι απολύτως απαραίτητο.**

9. Ασφαλής Χρήση του Safari

Η δυνατότητα «Autofill» θα πρέπει να απενεργοποιηθεί στο Safari. Με αυτό τον τρόπο το Safari δεν θα μπορεί να αποθηκεύει κρίσιμες ενδεχομένως πληροφορίες που υπάρχουν στη συσκευή σας, όπως username και password.

- Πηγαίνουμε στα Settings → Safari.
- Θέτουμε το «Autofill» στο OFF.

Επιπλέον, η τεχνολογία JavaScript μπορεί να απενεργοποιηθεί, προκειμένου να εμποδίσουμε τυχόν κακόβουλο λογισμικό να βλάψει τη συσκευή μας. Ωστόσο, η απενεργοποίηση αυτή ενδέχεται να καταστήσει άχρηστες ορισμένες ιστοσελίδες, επομένως είναι αναγκαίο να εξακαλουθήσει το JavaScript να βρίσκεται σε λειτουργία. Αν θελήσουμε να το απενεργοποιήσουμε:

- Πηγαίνουμε στα Settings → Safari.
- Θέτουμε τα «JavaScripts» στο OFF.

Επιπλέον, τα «cookies» μπορεί να θέσουν σε κίνδυνο προσωπικά δεδομένα και συνήθειες πλοήγησης στο διαδίκτυο. Για να αποτρέψουμε κάτι τέτοιο, τα θέτουμε εκτός λειτουργίας, όταν αυτό είναι δυνατόν, ή ρυθμίζουμε την iOS συσκευή μας ώστε να δέχεται «cookies» μόνο από ιστοσελίδες τις οποίες έχουμε επισκεφθεί.

10. Ασφαλής Χρήση E-mail

Βεβαιωθείτε ότι όλες οι συνδέσεις e-mail που χρησιμοποιείτε είναι κρυπτογραφημένες. Προϋπόθεση για κάτι τέτοιο είναι να μπορεί ο server που χρησιμοποιείτε, να κάνει διακίνηση κρυπτογραφημένων δεδομένων: αυτό γίνεται στις περισσότερες περιπτώσεις. Αν δεν κρυπτογραφηθούν, τα μηνύματά σας θα μεταδίδονται ελεύθερα και θα είναι δυνατόν κάποιος να τα υποκλέψει και να τα διαβάσει.

- Πηγαίνουμε στα Settings → Mail, Contacts, Calendars.
- Πηγαίνουμε στο SMTP και επιλέγουμε το όνομα ενός server.
- Θέτουμε την εντολή «Use SSL» στο ON για κάθε λογαριασμό στη λίστα.
- Πηγαίνουμε στο Advanced.
- Θέτουμε την εντολή «Use SSL» στο ON για κάθε λογαριασμό στη λίστα.

Όταν ανοίγουμε το e-mail μέσω του Safari, θα πρέπει να είμαστε βέβαιοι ότι η σελίδα πιστοποίησης (login page) είναι **κρυπτογραφημένη** πριν δώσουμε τα στοιχεία μας. Αν είναι κρυπτογραφημένη, η διεύθυνση της σελίδας ξεκινάει με «https» αντί του «http» και το εικονίδιο μιας κλειδαριάς εμφανίζεται αριστερά από το URL.
Επιπλέον, η επιλογή «Remote Image Loading» θα πρέπει να είναι απενεργοποιημένη από τα e-mail. Με τον τρόπο αυτό, μπορούμε να προστατεύουμε το σύστημά μας από παραποιημένες κακόβουλες εικόνες. Επίσης, δεν θα επιτρέψει, σε όσους θέλουν να βλάψουν το σύστημά μας, να συνδέσουν τη διεύθυνσή μας στο δίκτυο με το λογαριασμό e-mail που έχουμε.

- Πηγαίνουμε στα Settings → Mail, Contacts, Calendars.
- Ρυθμίζουμε το «Load Remote Image» σε OFF.

11. Ρύθμιση του iPhone Configuration Utility

Με την έκδοση του iOS 4, κάποιες ρυθμίσεις ασφαλείας, οι οποίες μπορούσαν να τεθούν σε λειτουργία μόνο μέσω του iPhone Configuration Utility, υπάρχουν τώρα στο Settings → General → Restrictions. Στις ρυθμίσεις αυτές περιλαμβάνονται η απενεργοποίηση της κάμερας και ενσωματωμένες iOS εφαρμογές όπως το Safari και το YouTube.

12. Σημαντικές ρυθμίσεις ασφαλείας iPhone & iPad

Άλλες σημαντικές ρυθμίσεις ασφαλείας, όπως κρυπτογραφημένα αντίγραφα ασφαλείας, περισσότερο πολύπλοκα PIN και καθαρισμό δίσκου εξ αποστάσεως, θα βρείτε στο iPhone Configuration Utility, ένα δωρεάν εργαλείο το οποίο σας προσφέρει η Apple απευθείας από την ιστοσελίδα της (http://www.apple.com/support/iphone/enterprise), στην οποία θα βρείτε και όλες τις σχετικές οδηγίες χρήσεως.

II. Ασφαλής χρήση του BlackBerry

1. 10 Συμβουλές

1. Μην αποθηκεύετε ή επεξεργάζεστε απόρρητες πληροφορίες σε μια συσκευή BlackBerry.
2. Κλείστε τη συσκευή σας και αφαιρέστε την μπαταρία πριν εισέλθετε σε χώρο υψίστης ασφαλείας.
3. Διατηρήστε το BlackBerry σε απόσταση 3 μέτρων από άλλη συσκευή επεξεργασίας απορρήτων πληροφοριών.
4. Έχετε πάντα εσείς τον έλεγχο της συσκευής σας.
5. Χρησιμοποιήστε συνθηματικό που να συνδυάζει γράμματα και αριθμούς, και να έχει τουλάχιστον 8 χαρακτήρες.
6. Αν πιστεύετε ότι η συσκευή σας έχει αλλοιωθεί από τρίτους, σταματήστε να τη χρησιμοποιείτε.
7. Όταν δεν τη χρησιμοποιείτε, κλειδώστε τη συσκευή σας με το εικονίδιο «Lock Keyboard» που βρίσκεται στην οθόνη της.
8. Μην κατεβάζετε αρχεία ή επισυναπτόμενα αρχεία από το διαδίκτυο, εκτός και αν είστε βέβαιοι για το περιεχόμενό τους.
9. Μη δίνετε προσωπικά στοιχεία και κωδικούς.
10. Μη συνδέετε το BlackBerry με απόρρητα δίκτυα υπολογιστών.

2. Απόρρητα Δεδομένα

Σε περίπτωση κατά την οποία απόρρητα δεδομένα αποθηκευτούν στη συσκευή ή μεταδοθούν μέσω αυτής, θα πρέπει η συσκευή να καταστραφεί, καθώς η εντολή «Wipe» δεν εξασφαλίζει απόλυτη ασφάλεια.

3. Ταξίδια

Κατά τη διάρκεια τελωνειακών ελέγχων, θα πρέπει να αφαιρούνται η μπαταρία και η κάρτα SIM από τη συσκευή BlackBerry, η οποία καλό θα ήταν να τοποθετηθεί αλλού, λ.χ. σε μια τσάντα.

4. Ενεργοποίηση χαρακτηριστικών ασφαλείας

Υπάρχουν διάφοροι τρόποι με τους οποίους εξασφαλίζεται η ασφαλής χρήση του BlackBerry. Μεταξύ άλλων:

- Από την αρχική οθόνη επιλέγουμε «Option» και μετά «Security».
- Το πεδίο «Password» θα πρέπει να είναι ενεργοποιημένο.
- Το πεδίο «Lock Handheld Upon Holstering» θα πρέπει να είναι ρυθμισμένο στο «Yes»
- Από την αρχική οθόνη επιλέγουμε «Option» και μετά «Firewall».
- Το πεδίο «Status» θα πρέπει να είναι ενεργοποιημένο.
- Από την αρχική οθόνη επιλέγουμε το εικονίδιο «Icon» και στη συνέχεια, σκρολάροντας, επιλέγουμε «Options» και στη συνέχεια «General Options».
- Η επιλογή «Auto Answer» θα πρέπει να ρυθμιστεί σε «Never».

5. Φίλος ή εχθρός;

Η τεχνολογία BlackBerry είναι ένα πολυσύνθετο σύστημα λογισμικού και υλικού που προσφέρει στο χρήστη άπειρες δυνατότητες επικοινωνίας. Σε κάθε συσκευή θα πρέπει να γίνεται προσεκτική χρήση προκειμένου να προστατεύουμε τα προσωπικά μας δεδομένα. Επιπλέον πληροφορίες μπορείτε να βρείτε στην επίσημη ιστοσελίδα της BlackBerry (us.blackberry.com).

III. Πηγές

Το παραπάνω κείμενο προέρχεται από φυλλάδιο του Κέντρου Ανάλυσης Συστημάτων και Δικτύων (Systems and Networks Analysis Center) της Υπηρεσίας Εθνικής Ασφαλείας (National Security Agency) των Ηνωμένων Πολιτειών της Αμερικής. Επιπλέον πληροφορίες μπορούμε να βρούμε στην ιστοσελίδα www.nsa.gov/snac

Το συγκεκριμένο φυλλάδιο δεν μπορεί να αντικαταστήσει την πολιτική ασφαλείας που χρησιμοποιείται, αλλά συνεισφέρει στην προστασία των χρηστών.

ΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ
Τι να κάνετε και τι να αποφεύγετε

Η κλοπή ταυτότητας είναι σπουδαία υπόθεση. Προσωπικά και οικονομικά δεδομένα που υφαρπάζονται διαδικτυακώς, πωλούνται στην υπόγεια οικονομία και χρησιμοποιούνται για παράνομους σκοπούς από εγκληματικές οργανώσεις σε όλο τον κόσμο. Η προστασία των δεδομένων σας δεν σας γλιτώνει μόνο από τη δυσάρεστη διαδικασία τού να αλλάζετε τους κωδικούς και τις πιστωτικές κάρτες σας. Βοηθάει ταυτόχρονα και στη μάχη ενάντια στο οργανωμένο έγκλημα και την τρομοκρατία.

Τι να αποφεύγετε:

1. Να ανοίγετε συνημμένα αρχεία και συνδέσμους χωρίς να γνωρίζετε την αληθινή τους προέλευση.

Αυτό που μπορεί εκ πρώτης όψεως να μοιάζει με αθώο βίντεο ή

εικόνα, ενδέχεται στην πραγματικότητα να είναι κακόβουλο λογισμικό σχεδιασμένο να υποκλέπτει τα δεδομένα σας. Ακόμα και το να ανοίξετε μόνο ένα spam mail μπορεί να βάλει τη διεύθυνσή σας στη λίστα των spammers για μελλοντικές επιθέσεις.

2. Να δίνετε περισσότερες πληροφορίες από όσες είναι απολύτως απαραίτητες.

Η τράπεζα και ο πάροχος της πιστωτικής σας κάρτας ήδη γνωρίζουν τον κωδικό σας και τη διεύθυνσή σας. Δεν χρειάζεται να τους δώσετε αυτά τα στοιχεία μέσω e-mail, τηλεφώνου ή ιστοσελίδας.

3. Να έχετε πρόσβαση σε διαδικτυακές τραπεζικές υπηρεσίες (online banking) από υπολογιστές με πολλαπλούς χρήστες ή από δημόσια προσβάσιμους υπολογιστές.

Ποτέ δεν ξέρετε τι μπορεί να κρύβεται στον σκληρό τους δίσκο.

4. Να μοιράζεστε κωδικούς, λογαριασμούς ηλεκτρονικού ταχυδρομείου ή άλλα διαδικτυακά προσωπικά δεδομένα με άλλους ανθρώπους.

Είναι πολύ δυσκολότερο να προστατευτείτε, όταν περισσότερα από ένα άτομα έχουν πρόσβαση.

5. Να αποθηκεύετε πιστοποιητικά σε φυλλομετρητές (browsers). Θα αποθηκεύατε ποτέ τον κωδικό σας σε ένα χαρτάκι Post-it;

Το να τον αποθηκεύσετε σε ένα φυλλομετρητή είναι εξίσου επικίνδυνο.

6. Να παίρνετε οτιδήποτε ως δεδομένο.

Αν μια προσφορά σε ένα e-mail ή σε κάποιο κοινωνικό δίκτυο σας φαίνεται πολύ καλή για να είναι αληθινή, τότε μάλλον δεν είναι. Επίσης, είναι πολύ εύκολο για εγκληματίες να αντιγράψουν τα λογότυπα εταιρειών και την ταυτότητα των αποστολέων.

Τι να κάνετε:

1. Να είστε σε επιφυλακή.

Να αντιμετωπίζετε τα αυτόκλητα e-mail ή σελίδες που ζητούν προσωπικές πληροφορίες, με επιφυλακτικότητα, ιδίως εκείνα που ισχυρίζονται ότι είναι από τράπεζες και εταιρείες πιστωτικών καρτών. Μια γρήγορη έρευνα στο διαδίκτυο μπορεί να σας πει αν το e-mail που λάβατε, είναι μία από τις γνωστές απάτες. Να θυμάστε ότι πάντα μπορείτε να διασταυρώνετε με την τράπεζά σας ή την εταιρεία πιστωτικών καρτών κατά πόσο το e-mail που λάβατε, είναι πράγματι από αυτούς.

2. Να ενημερώνετε (update) συστηματικά το λογισμικό σας.

Πολλές κακόβουλες μολύνσεις προκύπτουν επειδή οι εγκληματίες εκμεταλλεύονται κενά ασφαλείας στο λογισμικό (σε διαδικτυακούς φυλλομετρητές, σε λειτουργικά συστήματα, σε διάφορα προγράμματα κ.τ.λ.). Η διαρκής ενημέρωσή τους θα σας βοηθήσει να είστε ασφαλείς.

3. Να χρησιμοποιείτε αντιικό λογισμικό (anti-virus).

Το αντιικό λογισμικό βοηθάει στο να κρατήσετε τον υπολογιστή σας καθαρό από τα πιο συνήθη κακόβουλα λογισμικά -υπάρχουν, μάλιστα, αρκετές δωρεάν επιλογές. Πάντα να ελέγχετε τα αρχεία που κατεβάζετε, με το αντιικό πρόγραμμά σας. Να μην εγκαθιστάτε προγράμματα ή εφαρμογές στον υπολογιστή σας, αν δεν ξέρετε από πού προέρχονται.

4. Να απαγορεύετε την πρόσβαση στα προσωπικά σας στοιχεία από ιστοσελίδες κοινωνικής δικτύωσης.

Όσο περισσότερες πληροφορίες έχουν οι εγκληματίες, τόσο πιο εύκολα μπορούν να σας στοχοποιήσουν. Περιορίζοντας την ποσότητα πληροφοριών που μοιράζεστε, και τα άτομα με τα οποία τις μοιράζεστε, δυσκολεύετε τη δράση τους.

5. Να χρησιμοποιείτε πάντα ισχυρούς κωδικούς.

Οι υπολογιστές μπορούν να σπάσουν τους πιο συνηθισμένους κωδικούς πολύ γρήγορα. Είναι σημαντικό να σιγουρεύετε ότι οι κωδικοί σας είναι ισχυροί (πάνω από 8 χαρακτήρες, χρησιμοποιώντας ταυτόχρονα αριθμούς, γράμματα και σύμβολα).

6. Να προβαίνετε σε καταγγελίες.

Αν πέσετε θύμα κλοπής ταυτότητας, αναφέρετέ το αμέσως στο αστυνομικό τμήμα της περιοχής σας και στην εταιρεία την οποία αφορά (τράπεζα, διαδικτυακή υπηρεσία κ.τ.λ.). Οι υπηρεσίες επιβολής του Νόμου συνεργάζονται, τόσο σε ευρωπαϊκό όσο και σε παγκόσμιο επίπεδο, για να εμποδίζουν τις δραστηριότητες όσων ασχολούνται με απάτες ταυτότητας, και να τους φέρνουν ενώπιον της Δικαιοσύνης. Όσο περισσότερες πληροφορίες δίνετε στις Αρχές, τόσο πιο αποτελεσματικά θα στοχοποιούν τις πιο επικίνδυνες εγκληματικές οργανώσεις.

#το_μέλλον_του_διαδικτύου

εκτιμήσεις και προβλέψεις

Bold Ogilvy & Mather

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

Χορηγός Φιλοξενίας

ATHENAEUM INTERCONTINENTAL ATHENS

Χορηγός Επικοινωνίας

ΒΗΜΑFM 99,5

ΕΠΙΚΟΙΝΩΝΙΑ

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#το_μέλλον_του_διαδικτύου

εκτιμήσεις και προβλέψεις

Διαδίκτυο

Το διαδίκτυο αποτελεί το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο, το οποίο επιτρέπει την επικοινωνία και την ανταλλαγή πληροφοριών μεταξύ οποιωνδήποτε σημείων στον πλανήτη. Το διαδίκτυο έχει χαρακτηριστεί ως η μεγαλύτερη «εφεύρεση» όλων των εποχών, κατακτώντας ολόκληρη την υφήλιο μέσα σε μόλις μερικές δεκαετίες ζωής και αποτελώντας πλέον τη μεγαλύτερη οργανωμένη κοινωνία παγκοσμίως.

Το διαδίκτυο αποτελεί μια παράλληλη, "εικονική" παγκόσμια κοινότητα, η οποία καταλύει όλες τις κοινωνικές και πολιτιστικές διαχωριστικές γραμμές που υπάρχουν στον πραγματικό κόσμο και που τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεράσουν. Το διαδίκτυο, σε αντίθεση με τα παραδοσιακά μέσα ενημέρωσης και επικοινωνίας, καθιστά δυνατή τη ζωντανή αμφίδρομη επικοινωνία και δίνει τη δυνατότητα της άμεσης συμμετοχής σε όλους τους χρήστες με την ελεύθερη επιλογή λήψης, παροχής και διάχυσης της πληροφορίας. Καταλύοντας τα σύνορα και εκμηδενίζοντας τις αποστάσεις, το διαδίκτυο φαίνεται να κλίνει την πλάστιγγα πλέον εμφανώς υπερ των επικοινωνιών στην αιώνια διαμάχη μεταξύ των μεταφορών και των επικοινωνιών.

Ιστορική αναδρομή

Το διαδίκτυο αριθμεί θεωρητικά μόλις λίγες δεκαετίες ζωής, στις οποίες γνώρισε εκρηκτική ανάπτυξη και αποτέλεσε το σημαντικότερο στοιχείο μετεξέλιξης της ανθρωπότητας από τη βιομηχανική εποχή στην εποχή της πληροφορίας και την ψηφιακή επανάσταση. Σημαντικοί σταθμοί στην εξέλιξη αυτή υπήρξαν οι εξής:

- **1969:** Δημιουργείται το ARPANET, ο πρόγονος του σημερινού διαδικτύου, στο οποίο συμμετείχαν 4 μίνι υπολογιστές από αντίστοιχα ακαδημαϊκά ιδρύματα των Η.Π.Α., οι οποίοι συνδέθηκαν με ταχύτητες έως 50kbps.
- **1972:** Συστήνεται στο κοινό η ιδέα του ηλεκτρονικού ταχυδρομείου, όταν το ARPANET αριθμεί πλέον 23 διασυνδεδεμένους υπολογιστές.
- **1974:** Δημοσιεύεται από τους V. Cerf και B. Kahn, η πρώτη μελέτη για το πρωτόκολλο TCP (Transmission Control Program) το οποίο επιτρέπει την επικοινωνία μεταξύ διαφορετικών δικτύων υπολογιστών.
- **1974:** Εγκαινιάζεται το Telnet, η πρώτη εμπορική εκδοχή του ARPANET.
- **1982:** Χρησιμοποιείται για πρώτη φορά ο όρος «Internet», που ορίζει ένα συνδεδεμένο σύνολο από δίκτυα τα οποία χρησιμοποιούν το πρωτόκολλο TCP/IP.
- **1986:** Δημιουργείται το Nation Science Foundation Net (NSFNET), το οποίο διασυνδέει όλα τα πανεπιστημιακά ιδρύματα των Η.Π.Α.
- **1990:** Λειτουργεί ο πρώτος πάροχος διαδικτύου με το όνομα «The World comes on-line (world.std.com)» που προσφέρει σύνδεση στο διαδίκτυο μέσω τηλεφώνου.
- **1990:** Η Ελλάδα συνδέεται στο διαδίκτυο μέσω του δικτύου NSFNET.
- **1991:** Το CERN παρουσιάζει το World Wide Web, το οποίο συστήνει στο κοινό την ιδέα της χρήσης του διαδικτύου για την παροχή πληροφορίας μέσω ιστοσελίδων υπερκειμένου (hypertext).
- **1993:** Παρουσιάζεται ο πρώτος web browser (Mosaic) από την εταιρεία National Center for Supercomputing Applications (NCSA).

- **1994:** Προσφέρονται για πρώτη φορά τραπεζικές υπηρεσίες μέσω του διαδικτύου (Stanford Federal Credit Union).
- **1996:** Διατίθεται στην αγορά το πρώτο κινητό με πρόσβαση στο διαδίκτυο (Nokia 9000 Communicator) και βάρος 397γρ.!
- **2008:** Το Google ανακοινώνει ότι ο κατάλογός του ξεπέρασε το 1 τρισεκατομμύριο URLs.

Η εικόνα σήμερα

Από τους 4 υπολογιστές που αριθμούσε αρχικά το ARPANET μπορεί κανείς να διαπιστώσει τη γιγαντιαία εξάπλωση του διαδικτύου εξετάζοντας τα αντίστοιχα σημερινά νούμερα. Το 2012, οι χρήστες του διαδικτύου ξεπερνούν τα 2 δισεκατομμύρια παγκοσμίως, ποσοστό το οποίο αντιστοιχεί στο 30,2% του παγκόσμιου πληθυσμού. Αντίστοιχα, το ποσοστό στην Ευρώπη ανέρχεται σε 58,3% και στη Β. Αμερική σε 78,3%, με την αύξηση των χρηστών παγκοσμίως τα τελευταία 10 χρόνια να ξεπερνά το 450%.

Ο παγκόσμιος ιστός (World Wide Web) αριθμεί πλέον περίπου 50 δισεκατομμύρια ιστοσελίδες. Τα κοινωνικά δίκτυα αναπτύσσονται με ταχύτατους ρυθμούς, με το Facebook να κατέχει την πρώτη θέση, ξεπερνώντας το 1 δισεκατομμύριο χρήστες, και το YouTube να φτάνει τις 1 τρισεκατομμύριο αναπαραγωγές βίντεο.

Αντίστοιχη εικόνα παρουσιάζει η ανάπτυξη του διαδικτύου και στην Ελλάδα. Οι χρήστες του διαδικτύου ξεπερνούν τα 5 εκατομμύρια (>50% του πληθυσμού)

παρουσιάζοντας αύξηση την τελευταία δεκαετία >250%. Αντίστοιχα, οι ευρυζωνικές συνδέσεις ξεπερνούν τις 2.500.000 και οι χρήστες του Facebook πλησιάζουν τα 4 εκατομμύρια. Ενδιαφέρον είναι ότι στις ηλικίες 13-24, το ποσοστό χρήσης αγγίζει το 90%, γεγονός που φανερώνει την περαιτέρω ραγδαία εξέλιξη του διαδικτύου.
Τα θετικά του διαδικτύου με τη σημερινή μορφή του είναι πολλά και ποικίλα, παρέχοντας μια πληθώρα υπηρεσιών που καλύπτει ένα μεγάλο εύρος των καθημερινών αναγκών:

- Γνώση
- Εκπαίδευση
- Πληροφορίες
- Επικοινωνία
- Ενημέρωση
- Ψυχαγωγία
- Διασκέδαση
- Αγορές
- Ταξίδια

Τι είδαμε την περασμένη δεκαετία

Την περασμένη δεκαετία, μια σειρά τεχνολογικών εξελίξεων και κοινωνικών τάσεων καθιέρωσαν τη σημερινή μορφή του διαδικτύου. Χαρακτηριστικά παραδείγματα αποτέλεσαν τα εξής:

Social Media: Σημαντικότερο σημείο στην εξέλιξη του διαδικτύου την περασμένη δεκαετία αποτέλεσε αναμφίβολα η εκρηκτική ανάπτυξη των μέσων κοινωνικής δικτύωσης.
Video sharing: Με την ευρυζωνικότητα να είναι διαθέσιμη σε κάθε σπίτι και τις ταχύτητες να αυξάνονται σημαντικά, κατέστη πρακτικά εφικτό το video sharing, το οποίο - με πρωτοστάτη το YouTube και τις υπηρεσίες του έγινε κομμάτι της καθημερινότητας.
Mobile Internet – 3G – smartphones: Πολύ σημαντική εξέλιξη αποτέλεσε τεχνολογικά και η δυνατότητα σύνδεσης στο διαδίκτυο από τις συσκευές κινητών τηλεφώνων, που επέτρεψε στους χρήστες του διαδικτύου να συνδέονται από κάθε μέρος και με κάθε συσκευή.
Online gaming: Τεράστια ανάπτυξη γνώρισαν και τα διαδικτυακά παιχνίδια, κερδίζοντας πολύ γρήγορα μεγάλο αριθμό χρηστών. Τεράστιοι εικονικοί κόσμοι προσελκύουν καθημερινά ένα μεγάλο ποσοστό χρηστών, με κάποια από τα διαδικτυακά παιχνίδια να ξεπερνούν τους 10 εκατομμύρια χρήστες.
Internet radio: Το κλασικό ραδιόφωνο μεταλλάχθηκε σε μεγάλο βαθμό σε διαδικτυακό, κερδίζοντας πολλούς θαυμαστές και καταλύοντας τα σύνορα της μετάδοσης παγκοσμίως.
Blogs: Τα ιστολόγια αποτέλεσαν ένα από τα τελευταία trends της περασμένης δεκαετίας, δίνοντας βήμα σε όλους για έκφραση και κερδίζοντας καθημερινά εκατομμύρια θαυμαστές.

Τι αναμένουμε να δούμε την επόμενη δεκαετία

Με βάση τις προηγούμενες εξελίξεις, τα δείγματα τα οποία έχουν παρουσιαστεί, και την τάση για ανάπτυξη, η επόμενη δεκαετία αναμένουμε να μας παρουσιάσει νέες καινοτόμες λύσεις και υπηρεσίες. Ας ρίξουμε μια ματιά στο μέλλον, σε ορισμένα από τα θέματα που αναμένεται να μας καταπλήξουν τα επόμενα χρόνια:

Cloud: Το cloud έχει ήδη κάνει αισθητή την παρουσία του στην παγκόσμια αγορά ανοίγοντας νέους δρόμους στην πρόσβαση σε δεδομένα και υπηρεσίες. Η πληροφορία πλέον καθίσταται προσβάσιμη από οποιοδήποτε σημείο και από οποιαδήποτε συσκευή έχει πρόσβαση στο διαδίκτυο, και οι υπηρεσίες δεν απαιτούν εγκατάσταση, με αποτέλεσμα οι απαιτήσεις για υπολογιστική ισχύ να μειώνονται τόσο για τους ιδιώτες όσο και για τις εταιρείες. Την επόμενη δεκαετία, περιμένουμε ολοένα και περισσότερες υπηρεσίες να μετακινηθούν στο «σύννεφο», και την παρουσίαση online λειτουργικών συστημάτων, κειμενογράφων και άλλων εργαλείων καθημερινής χρήσης, τα οποία θα διατίθενται αποκλειστικά ως cloud services.
3D Internet: Με τις τεχνολογίες των monitors να υποστηρίζουν ήδη 3D προβολή, αναμένεται σύντομα το διαδίκτυο να διαθέτει 3D ιστοσελίδες και εφαρμογές, και τα 3D objects να αντικαταστήσουν τα σημερινά video και φωτογραφίες, δίνοντας ένα νέο πρόσωπο στο διαδίκτυο.
IPTV: Όλες οι νέες συσκευές τηλεόρασης διαθέτουν σύνδεση στο διαδίκτυο και οι υπηρεσίες broadcasting μέσω διαδικτύου καλύπτουν πλέον πλήρως τις ανάγκες για μετάδοση εικόνας. Με βάση τα παραπάνω και ακολουθώντας το ραδιόφωνο, έχοντας ήδη τα πρώτα δείγματα στην αγορά, η τηλεόραση αναμένεται να μεταλλαχθεί ίσως και εξολοκλήρου σε Internet TV.
E-learning – τηλεεργασία: Δύο εφαρμογές του διαδικτύου που βρίσκονται πολύ καιρό σε αναμονή, αναμένεται να έλθουν στο προσκήνιο, μειώνοντας τα κόστη μετακίνησης και τα κόστη συντήρησης των εταιρειών.
Νανοτεχνολογία: Η νανοτεχνολογία ήδη βρίσκει εφαρμογή σε πάρα πολλούς τομείς και τα τελευταία πειράματα δείχνουν ότι συσκευές όπως οι μοριακοί υπολογιστές δεν αποτελούν πλέον άπιαστο όνειρο. Δεν αποκλείεται, λοιπόν, πολύ σύντομα οι χρήστες να διαθέτουν πανίσχυρους υπολογιστές σε ένα ρολόι χειρός ή ένα απλό ακουστικό.
Πλήρης διασύνδεση: Ακολουθώντας την πρόβλεψη του Bill Gates («Every device in the world will be connected») και με το IPv6 να τίθεται ήδη σε εφαρμογή σε ορισμένες χώρες της Ευρώπης, σύντομα όλες οι συσκευές θα διασυνδεθούν σε ένα υπερδίκτυο, το οποίο θα περιλαμβάνει τις οικιακές ηλεκτρικές συσκευές, τα αυτοκίνητα, τα κινητά τηλέφωνα και κάθε φορητή ή οικιακή συσκευή.
4G 5G και πέρα: Ήδη από το 2009, το 4G είναι πραγματικότητα. Με τις εξελίξεις στον τομέα mobile broadband να καλπάζουν, οι επόμενες γενιές κινητών δικτύων δεν θα αργήσουν να ακολουθήσουν.

#στατιστικά_στο_διαδίκτυο

όταν οι αριθμοί μιλάνε από μόνοι τους.

Bold Ogilvy & Mather

AEGEAN · Bold Ogilvy & Mather · Εκπαιδευτήρια ΓΕΙΤΟΝΑ · cyta · Eurobank · FORTHNETGROUP forthnet nova · Hertz · hol hellas online · OLYMPIC AIR · OTE · COSMOTE · VISA · vodafone · WIND

Χορηγός Φιλοξενίας
ATHENAEUM INTERCONTINENTAL ATHENS

Χορηγός Επικοινωνίας
ΒΗΜΑFM 99,5

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

ΕΠΙΚΟΙΝΩΝΙΑ

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#στατιστικά_στο_διαδίκτυο

όταν οι αριθμοί μιλάνε από μόνοι τους

Εξέλιξη του διαδικτύου στην Ελλάδα και την Ευρώπη

Στην εποχή της ψηφιακής επανάστασης που διανύουμε, εμφανίζονται νέες τάσεις στη χρήση του Διαδικτύου. Προοδευτικά, υιοθετούνται καινούργιοι και περισσότερο εξελιγμένοι τρόποι και υπηρεσίες για επικοινωνία, πληροφόρηση, ψυχαγωγία και αλληλεπίδραση μεταξύ επιχειρήσεων και δημόσιων φορέων. Τα ποσοστά των χρηστών του Διαδικτύου έχουν αυξηθεί κατακόρυφα τα τελευταία πέντε χρόνια, αποδεικνύοντας ότι το Διαδίκτυο όχι απλά έχει μέλλον, αλλά αποτελεί παράλληλα και το βασικότερο μέσο επικοινωνίας.

Την τελευταία πενταετία, παρατηρείται αύξηση τής πρόσβασης στο Διαδίκτυο από την κατοικία, καθώς και αύξηση του ποσοστού κατοχής ηλεκτρονικού υπολογιστή και των ευρυζωνικών συνδέσεων. Παράλληλα, υπάρχει μια άνευ προηγουμένου ανάπτυξη στην ευρυζωνική κάλυψη και, γενικότερα, αύξηση στη διείσδυση και χρήση «επιγραμμικών» (online) υπηρεσιών μέσω Διαδικτύου, τόσο στην Ευρωπαϊκή Ένωση όσο και στην Ελλάδα.

Τη μεγάλη εξέλιξη του Διαδικτύου στην Ευρώπη κατέγραψε πρόσφατη έρευνα της Eurostat για το 2010. Στην ΕΕ27, το 2010, το 70% των νοικοκυριών είχε πρόσβαση στο Διαδίκτυο, σε σύγκριση με ποσοστό 49% το 2006. Το ποσοστό των νοικοκυριών με ευρυζωνική σύνδεση διπλασιάστηκε και ανήλθε το 2010 σε 61%, σε σύγκριση με το 30% του 2006. Το επίπεδο της πρόσβασης στο Διαδίκτυο αυξήθηκε σε όλα τα κράτη-μέλη, μεταξύ 2006 και 2010, κυρίως στη Ρουμανία, όπου τριπλασιάστηκε, και στη Βουλγαρία, την Τσεχική Δημοκρατία, την Ελλάδα, την Ουγγαρία και τη Σλοβακία, όπου διπλασιάστηκε. Το 2010, τα υψηλότερα ποσοστά πρόσβασης καταγράφηκαν στις χώρες της Β. Ευρώπης που αποτελούν προπύργια στη χρήση του Διαδικτύου, παραμένοντας στις πρώτες θέσεις, με την Ολλανδία στο 91%, το Λουξεμβούργο στο 90%, τη Σουηδία στο 88% και τη Δανία στο 86%, και το χαμηλότερο στη Βουλγαρία στο 33%, τη Ρουμανία στο 42 % και την Ελλάδα στο 46%. Το ποσοστό των νοικοκυριών με ευρυζωνική σύνδεση αυξήθηκε το 2010 σε σύγκριση με το 2006. Η Σουηδία στο 83%, κατέγραψε το υψηλότερο ποσοστό, ακολουθούμενη από τη Δανία στο 80%, τη Φινλανδία στο 76% και τη Γερμανία στο 75%, ενώ η Ρουμανία στο 23%, η Βουλγαρία στο 26% και η Ελλάδα στο 41% είχαν τα χαμηλότερα ποσοστά. Ειδικά για τις ευρυζωνικές συνδέσεις, παρατηρείται μια κατακόρυφη αύξηση στην Ελλάδα, καθώς, από το 4% των νοικοκυριών το 2006, έφτασε το 2010 στο 41%. Είναι φανερό ότι εξαιρετικά μεγάλη συνεχίζει να είναι η απόσταση που χωρίζει την Ελλάδα από τις υπόλοιπες ευρωπαϊκές χώρες όσον αφορά στη χρήση του Διαδικτύου και των ευρυζωνικών συνδέσεων. Εξακολουθεί να υπολείπεται σημαντικά του μέσου ευρωπαϊκού όρου που έφτασε το 70%, αλλά είναι σαφές στα χρόνια που μεσολάβησαν ότι σημειώθηκε μια αύξηση στη χρήση τού Διαδικτύου στη χώρα μας κατά 100%.

Επιπρόσθετα, η πρόσβαση στο Διαδίκτυο παρουσιάζει αύξηση κατά περίπου 20 ποσοστιαίες μονάδες σε νοικοκυριά με παιδιά. Συγκεκριμένα, το 2010 η πρόσβαση στο Διαδίκτυο για νοικοκυριά με παιδιά, στην ΕΕ27 ήταν σημαντικά υψηλότερη (στο 84%) σε σύγκριση με τα νοικοκυριά χωρίς παιδιά (στο 65%). Καταγράφτηκε επίσης ότι ποσοστό 90% όλων των χρηστών του Διαδικτύου επικοινωνούσε μέσω e-mail. Επίσης, υπήρξε μια πολύ σημαντική διαφορά στη χρήση του Διαδικτύου για αποστολή μηνυμάτων σε chat sites, blogs και κοινωνικά δίκτυα ανάλογα με την ηλικία. Τα 4/5 των χρηστών του διαδικτύου ηλικίας 16-24, στην ΕΕ27 χρησιμοποίησαν το διαδίκτυο για το σκοπό αυτό κατά τη διάρκεια του 2010, σε σύγκριση με τα 2/5 των ατόμων ηλικίας 25-54 ετών και λιγότερο από το 1/5 των ατόμων ηλικίας 55-74. Η χρήση αυτής της μορφής

επικοινωνίας ήταν ιδιαίτερα υψηλή για όλες τις ηλικίες στην Πολωνία, την Πορτογαλία και τη Λιθουανία. Υπήρξε μια λιγότερο έντονη διαφορά μεταξύ των ηλικιακών ομάδων όσον αφορά τη χρήση του τηλεφώνου στο Διαδίκτυο και τις βιντεοκλήσεις, με το 1/3 των ατόμων ηλικίας 16-24 ετών, το 1/4 των ατόμων ηλικίας 25-54 ετών και το 1/5 των ατόμων ηλικίας 55-74. Η χρήση του Διαδικτύου μέσω τηλεφώνου και βιντεοκλήσεων, ήταν ιδιαίτερα υψηλή για όλες τις ηλικίες στη Βουλγαρία, τη Λετονία, τη Λιθουανία και τη Σλοβακία.

Σύμφωνα με την Έρευνα Χρήσης Τεχνολογιών Πληροφόρησης και Επικοινωνίας για το έτος 2010 στην Ελλάδα, η ΕΛ.ΣΤΑΤ. επισήμανε ότι με μειωμένους ρυθμούς συνεχίζεται η αύξηση κατά 2,3% στη χρήση ηλεκτρονικού υπολογιστή και κατά 4,7% στην πρόσβαση στο Διαδίκτυο, ενώ 1 στα 2 νοικοκυριά έχει πρόσβαση στο Διαδίκτυο από την κατοικία του, όπου, από το 23,1% για το 2006, έφτασε στο 46,4% για το 2010. Ο μέσος ετήσιος ρυθμός μεταβολής για το ίδιο διάστημα είναι 6,5% για τη χρήση του ηλεκτρονικού υπολογιστή και 11,4% για τη χρήση του Διαδικτύου. Η συχνότητα χρήσης του Διαδικτύου ανέρχεται στο 91,9% για καθημερινή χρήση και στο 70,1% για τακτική. Μεγάλη μείωση (περίπου 40%), σε σχέση με το 2009, παρατηρείται στην πρόσβαση από σημεία ασύρματης ευρυζωνικής πρόσβασης, γεγονός που αποδίδεται και αντισταθμίζεται με την αύξηση (περίπου 58%) που παρατηρείται στη σύνδεση στο Διαδίκτυο μέσω κινητών ή «έξυπνου κινητού τηλεφώνου» (Smartphone) κατά 68,8%. Η αναζήτηση πληροφοριών και online υπηρεσιών παραμένει στην κορυφή της λίστας των δραστηριοτήτων μέσω Διαδικτύου, με ποσοστό 93,4%. Σχετική σταθερότητα σε σχέση με το 2009 παρουσιάζει η χρήση του ηλεκτρονικού ταχυδρομείου με 72,6%, η πραγματοποίηση τραπεζικών συναλλαγών με 13%, η αναζήτηση πληροφοριών για προϊόντα, υπηρεσίες, ταξίδια και καταλύματα, η αναζήτηση ή η αποστολή αιτήσεων για εύρεση εργασίας και η αναζήτηση για υπηρεσίες εκπαίδευσης, καθώς και η συμμετοχή σε online εκπαιδευτικά προγράμματα με ποσοστό 62,6%. Αύξηση παρουσιάζουν ορισμένες από τις χρήσεις του διαδικτύου που αφορούν στο κατέβασμα λογισμικού με αύξηση 28,7%, στην ανάγνωση online ή κατέβασμα εφημερίδων και περιοδικών με αύξηση 14,4%, στην ακρόαση web ραδιοφώνου και παρακολούθηση web τηλεόρασης με αύξηση 13,7% και στην αποστολή μηνυμάτων σε chat sites, blogs και ομάδες συζήτησης, στη συμμετοχή σε fora και ανταλλαγή γραπτών μηνυμάτων σε πραγματικό χρόνο με αύξηση 11% περίπου, φτάνοντας στο 46,9%. Η τελευταία χρήση αποτελεί την κυριότερη για την ηλικιακή ομάδα 16–24 ετών με ποσοστό 39,3%. Μικρή αύξηση, κατά 4% περίπου, σημειώνεται στην ηλεκτρονική διακυβέρνηση και οι συναλλαγές με δημόσιες υπηρεσίες φτάνουν στο 29,5%.

Ποιοι και γιατί χρησιμοποιούν το Διαδίκτυο

Η αποχή από το Διαδίκτυο φαίνεται να οφείλεται τόσο σε στάση ζωής και συνειδητή άρνηση, όσο και έλλειψη δεξιοτήτων, κυρίως για τα άτομα των μεγαλύτερων ηλικιακών ομάδων, αναδεικνύοντας την ανάγκη για εξάλειψη της «τεχνοφοβίας», μέσω της εξοικείωσης και της κατάλληλης επιμόρφωσης. Οι έλληνες χρήστες φαίνεται να αξιοποιούν τις νέες δυνατότητες επικοινωνίας και ψυχαγωγίας που προσφέρει το Διαδίκτυο και να εγκαταλείπουν τις παραδοσιακές ηλεκτρονικές υπηρεσίες, όπως απλή αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες, αλλά και αποστολή και λήψη e-mail. Έτσι, το 64% των χρηστών του τελευταίου τριμήνου του 2008, δηλώνει ότι κάνει χρήση προχωρημένων υπηρεσιών, επικοινωνίας καθώς πραγματοποιεί τηλεφωνικές κλήσεις και βιντεοκλήσεις μέσω διαδικτύου, επικοινωνεί μέσω στιγμιαίων μηνυμάτων, συζητά σε ηλεκτρονικά fora, επισκέπτεται ιστολόγια (blogs), ενώ παράλληλα, 1 στους 2 «κατεβάζει» και ακούει μουσική, και 1 στους 5 παίζει διαδικτυακά παιχνίδια.

Όσον αφορά τα παιδιά και τους εφήβους, βλέπουμε ότι η συντριπτική πλειοψηφία των παιδιών 8-15 ετών χρησιμοποιούν ηλεκτρονικό υπολογιστή (85%).
Ο υπολογιστής χρησιμοποιείται τουλάχιστον 1 φορά την εβδομάδα από 9 στα 10 παιδιά (96%), ενώ τα μισά από αυτά (54%) τον χρησιμοποιούν σε καθημερινή ή σχεδόν καθημερινή βάση. Η συχνότητα χρήσης του υπολογιστή μεγαλώνει με την ηλικία. Ο υπολογιστής, όπως και για τους ενήλικες χρησιμοποιείται ουσιαστικά στο σπίτι (87%), αλλά σημαντικά και στο σχολείο, αφού όλοι είναι μαθητές (40%). Από αυτούς που χρησιμοποίησαν Η/Υ τους τελευταίους 3 μήνες, το 80% χρησιμοποίησε και το Διαδίκτυο, είτε στο σπίτι είτε στο σχολείο είτε αλλού. Από όσους χρησιμοποίησαν το Διαδίκτυο τους τελευταίους 3 μήνες, 9 στους 10 το χρησιμοποιούν τουλάχιστον 1 φορά την εβδομάδα (88%), ενώ 47% από αυτούς καθημερινά ή σχεδόν καθημερινά. Όπως η συχνότητα χρήσης υπολογιστή, έτσι και η συχνότητα χρήσης του Διαδικτύου αυξάνει με την ηλικία.

επικοινωνίας ήταν ιδιαίτερα υψηλή για όλες τις ηλικίες στην Πολωνία, την Πορτογαλία και τη Λιθουανία. Υπήρξε μια λιγότερο έντονη διαφορά μεταξύ των ηλικιακών ομάδων όσον αφορά τη χρήση του τηλεφώνου στο Διαδίκτυο και τις βιντεοκλήσεις, με το 1/3 των ατόμων ηλικίας 16-24 ετών, το 1/4 των ατόμων ηλικίας 25-54 ετών και το 1/5 των ατόμων ηλικίας 55-74. Η χρήση του Διαδικτύου μέσω τηλεφώνου και βιντεοκλήσεων, ήταν ιδιαίτερα υψηλή για όλες τις ηλικίες στη Βουλγαρία, τη Λετονία, τη Λιθουανία και τη Σλοβακία.

Σύμφωνα με την Έρευνα Χρήσης Τεχνολογιών Πληροφόρησης και Επικοινωνίας για το έτος 2010 στην Ελλάδα, η ΕΛ.ΣΤΑΤ. επισήμανε ότι με μειωμένους ρυθμούς συνεχίζεται η αύξηση κατά 2,3% στη χρήση ηλεκτρονικού υπολογιστή και κατά 4,7% στην πρόσβαση στο Διαδίκτυο, ενώ 1 στα 2 νοικοκυριά έχει πρόσβαση στο Διαδίκτυο από την κατοικία του, όπου, από το 23,1% για το 2006, έφτασε στο 46,4% για το 2010. Ο μέσος ετήσιος ρυθμός μεταβολής για το ίδιο διάστημα είναι 6,5% για τη χρήση του ηλεκτρονικού υπολογιστή και 11,4% για τη χρήση του Διαδικτύου. Η συχνότητα χρήσης του Διαδικτύου ανέρχεται στο 91,9% για καθημερινή χρήση και στο 70,1% για τακτική. Μεγάλη μείωση (περίπου 40%), σε σχέση με το 2009, παρατηρείται στην πρόσβαση από σημεία ασύρματης ευρυζωνικής πρόσβασης, γεγονός που αποδίδεται και αντισταθμίζεται με την αύξηση (περίπου 58%) που παρατηρείται στη σύνδεση στο Διαδίκτυο μέσω κινητών ή «έξυπνου κινητού τηλεφώνου» (Smartphone) κατά 68,8%. Η αναζήτηση πληροφοριών και online υπηρεσιών παραμένει στην κορυφή της λίστας των δραστηριοτήτων μέσω Διαδικτύου, με ποσοστό 93,4%. Σχετική σταθερότητα σε σχέση με το 2009 παρουσιάζει η χρήση του ηλεκτρονικού ταχυδρομείου με 72,6%, η πραγματοποίηση τραπεζικών συναλλαγών με 13%, η αναζήτηση πληροφοριών για προϊόντα, υπηρεσίες, ταξίδια και καταλύματα, η αναζήτηση ή η αποστολή αιτήσεων για εύρεση εργασίας και η αναζήτηση για υπηρεσίες εκπαίδευσης, καθώς και η συμμετοχή σε online εκπαιδευτικά προγράμματα με ποσοστό 62,6%. Αύξηση παρουσιάζουν ορισμένες από τις χρήσεις του διαδικτύου που αφορούν στο κατέβασμα λογισμικού με αύξηση 28,7%, στην ανάγνωση online ή κατέβασμα εφημερίδων και περιοδικών με αύξηση 14,4%, στην ακρόαση web ραδιοφώνου και παρακολούθηση web τηλεόρασης με αύξηση 13,7% και στην αποστολή μηνυμάτων σε chat sites, blogs και ομάδες συζήτησης, στη συμμετοχή σε fora και ανταλλαγή γραπτών μηνυμάτων σε πραγματικό χρόνο με αύξηση 11% περίπου, φτάνοντας στο 46,9%. Η τελευταία χρήση αποτελεί την κυριότερη για την ηλικιακή ομάδα 16–24 ετών με ποσοστό 39,3%. Μικρή αύξηση, κατά 4% περίπου, σημειώνεται στην ηλεκτρονική διακυβέρνηση και οι συναλλαγές με δημόσιες υπηρεσίες φτάνουν στο 29,5%.

Αν και, ομολογουμένως, όσα έχουμε αναφέρει έως τώρα μπορεί να φαντάζουν κάπως υπερβολικά, θα είχε ενδιαφέρον να δούμε τι μπορεί να γίνει σε 60" στο διαδίκτυο:

- Γίνονται **694.445 αναζητήσεις στο Google**
- Ανεβαίνουν **στο Flickr πάνω από 6.600 εικόνες**
- Ανεβαίνουν στο YouTube **600 videos συνολικής διάρκειας περίπου 25 ωρών**
- Γίνονται **695.000 status updates** και δημοσιεύονται **79,364 wall posts** και **510.040** σχόλια στο **Facebook**
- Κατοχυρώνονται **70 νέα domains**
- Στέλνονται πάνω από **168.000,000 emails**
- Δημιουργούνται **320 νέοι λογαριασμοί στο Twitter** και δημοσιεύονται **98.000 Tweets**
- Κατεβαίνουν **13,000 εφαρμογές στο iPhone**
- Δημοσιεύονται **20,000 νέα άρθρα στο tumblr**
- Ο πλοηγός **Firefox** κατέβηκε περισσότερες από **1700 φορές**
- Το **Wordpress** κατέβηκε περισσότερες από **50 φορές**
- Κατέβηκαν **περισσότερες από 125 φορές τα WordPress Plugins**
- Δημιουργούνται **100 νέοι λογαριασμοί** στο επαγγελματικό κοινωνικό δίκτυο **LinkedIn**
- Γίνονται **40 νέες ερωτήσεις** από χρήστες στο **YahooAnswers.com,** ενώ απαντώνται πάνω από **100 ερωτήσεις στο Answers.com**
- Δημοσιεύεται **1 νέο άρθρο στο Associated Content,** το μεγαλύτερο δίκτυο community-created content
- Προστίθεται **1 νέος ορισμός στο UrbanDictionary.com**
- Δημιουργούνται στο **Craigslist πάνω από 1,200 νέες διαφημίσεις**
- Γίνονται πάνω από **370,000 λεπτά κλήσεων μέσω του Skype**
- Συμπληρώνονται συνολικά πάνω από **13,000 ώρες από streaming μουσικής** μέσω του μουσικού ραδιοφώνου **Pandora**
- Και τέλος, γίνονται πάνω από **1,600 αναγνώσεις κειμένων στο Scribd,** το οποίο αποτελεί το μεγαλύτερο κοινωνικό δίκτυο δημοσίευσης εγγράφων.

Οι Έλληνες χρησιμοποιούν το διαδίκτυο κυρίως για τους παρακάτω λόγους:

Το **96%** συνδέεται για **αναζήτηση πληροφοριών**
Το **36,7%** συνδέεται για **ανάγνωση ελληνικών ειδήσεων**
Το **22,6%** συνδέεται για **ανάγνωση ξένων ειδήσεων**

Το **8,6%** συνδέεται για **εξελίξεις της οικονομίας**
Το **55,7%** συνδέεται για **ανάγνωση e-mail**
Το **32,5%** συνδέεται για **download τραγουδιών**
Το **21,4%** συνδέεται για **να παίξει παιχνίδια**
Το **20,8%** συνδέεται για **να συνομιλήσει μέσω Chat**

Περά όμως από την Ελλάδα, σε μια έρευνα που πραγματοποιήθηκε σε 16 χώρες, οι βασικότεροι λόγοι χρήσης του διαδικτύου είναι:

1) Εικονικοί φίλοι στις ιστοσελίδες κοινωνικής δικτύωσης
2) Τραπεζικές συναλλαγές
3) Η χρήση μηχανών αναζήτησης
4) Παρακολούθηση βίντεο στο διαδίκτυο
5) Site κοινωνικής δικτύωσης
6) Ραντεβού μέσω διαδικτύου

Γενικά στατιστικά

Σύμφωνα με την GoogleGreece, ενδεικτικά για την Ελλάδα:

- **Πάνω από 4 εκατ. κάτοικοι έχουν πρόσβαση στο Διαδίκτυο**
- **30 εκατ. βίντεο** προβάλλονται το μήνα από το **Youtube**
- **4 εκατ. κάτοικοι έχουν λογαριασμούς σε υπηρεσίες κοινωνικής δικτύωσης**
- **Ο μέσος εβδομαδιαίος χρόνος** που κάποιος είναι online είναι περίπου **10 ώρες**
- Πάνω από **500.000 αναζητήσεις** πραγματοποιούνται καθημερινά
- **Αυξάνεται συνεχώς η χρήση διαδικτύου μέσω κινητών**

Για την Ευρώπη:

- Με πληθυσμό περίπου **820 εκατ. να κατέχει το 25%** στην χρήση Internet σε σχέση με τις άλλες γεωγραφικές ζώνες
- Το **TOP 10 των Ευρωπαϊκών χωρών** με την μεγαλύτερη χρήση (σε εκατ. χρήστες) είναι σύμφωνα με τον ακόλουθα στοιχεία:

Γερμανία: 65,1
Ρωσία: 59,7
Ηνωμένο Βασίλειο: 51,4
Γαλλία: 44,6
Τουρκία: 35
Ιταλία: 30
Ισπανία: 29,4
Πολωνία: 22,5
Ουκρανία: 15,3
Κάτω Χώρες: 14,9

Σύμφωνα με έρευνα της Netcraft, το Διαδίκτυο έχει φτάσει να διαθέτει περίπου 150 εκατ. ιστοσελίδες. Στο διάστημα Σεπτεμβρίου-Οκτωβρίου, η αύξηση των ιστοσελίδων έφτασε στα 7,6 εκατ. Ο μηνιαίος ρυθμός ανάπτυξής του άγγιξε το 5%, το οποίο ήταν το μεγαλύτερο ποσοστό της εταιρείας που έχει καταγραφεί ποτέ.

Σχετικά με τη χρήση του Διαδικτύου στην Ελλάδα, παρατηρείται σημαντική αύξηση του αριθμού των χρηστών (από 13% το 2001 σε 31% το 2007) ηλικίας 15 έως 65 ετών που κατέχουν προσωπικό Η/Υ. Αντίστοιχα, παρατηρείται αύξηση των ωρών χρήσης του Διαδικτύου που φτάνουν κατά μέσο όρο τις 8,6 ανά εβδομάδα.

Η υπηρεσία που χρησιμοποιείται περισσότερο είναι το ηλεκτρονικό ταχυδρομείο (e-mail), αλλά και η ενημέρωση (νέα, καιρός, αθλητικά) αποτελεί από τους κυριότερους λόγους χρήσης του Διαδικτύου.

Αντίθετα, η αναζήτηση για προϊόντα και υπηρεσίες ακολουθεί πτωτική πορεία από το 2002. Ιδιαίτερα χαμηλή παραμένει η χρήση του Διαδικτύου για αγορά προϊόντων και υπηρεσιών.

Περίπου 18% των χρηστών προχώρησε σε κάποια αγορά κατά το 2006, ωστόσο το ποσοστό αυτό ανέρχεται μόλις στο 4,5% του γενικού πληθυσμού. Παρόλα αυτά, οι αγορές πραγματοποιήθηκαν κυρίως από ελληνικούς ιστοχώρους [sites] (41%) έναντι των ξένων (35%).

Οι χρήστες που αγοράζουν μέσω του Διαδικτύου, συνήθως δεν επισκέπτονται τα αντίστοιχα καταστήματα, ενώ οι κυριότεροι λόγοι αγοράς είναι η προσιτή τιμή και η καλή εξυπηρέτηση.

Τέλος, αξιοσημείωτο είναι το γεγονός ότι, σε ποσοστό πάνω από 60%, οι χρήστες θεωρούν ότι ο κίνδυνος διαρροής προσωπικών δεδομένων κατά τη χρήση πιστωτικής κάρτας στις ηλεκτρονικές αγορές είναι μεγάλος ή πολύ μεγάλος. Η παραπάνω έρευνα πραγματοποιήθηκε (για το διάστημα, 2001-2006) από την εταιρία VPRC για λογαριασμό του e-businessforum και του Εθνικού Δικτύου Έρευνας και Τεχνολογίας.

#παιδική_πορνογραφία_στο_διαδίκτυο

όταν η παιδική αξιοπρέπεια κινδυνεύει και ηλεκτρονικά

Bold Ogilvy & Mather

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

AEGEAN · Bold Ogilvy & Mather · Εκπαιδευτήρια ΓΕΙΤΟΝΑ · cyta · Eurobank · FORTHNETGROUP forthnet nova · Hertz · hol hellas online · OLYMPIC · OTE · COSMOTE · VISA · vodafone · WIND

Χορηγός Φιλοξενίας: ATHENAEUM INTERCONTINENTAL ATHENS

Χορηγός Επικοινωνίας: ΒΗΜΑ FM 99,5

ΕΠΙΚΟΙΝΩΝΙΑ

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η παιδική πορνογραφία στην Ελλάδα

Τα τελευταία χρόνια έχει υπάρξει ραγδαία αύξηση του αριθμού των χρηστών του διαδικτύου που κατεβάζουν βίντεο και φωτογραφίες με παιδικό πορνογραφικό υλικό. Πλην όμως, έως σήμερα, δεν έχει διακριβωθεί η ύπαρξη κάποιου οργανωμένου κυκλώματος που να βιντεοσκοπεί πράξεις ασέλγειας σε ανήλικους, παρά μόνο μεμονωμένες περιπτώσεις.

Πως λειτουργούν τα «αρπακτικά»

(GROOMING = αποπλάνηση ανηλίκου)

Διαδικασία κατά την οποία τα «αρπακτικά», προσποιούμενοι ότι είναι έφηβοι, χρησιμοποιούν τα δωμάτια ανοιχτής επικοινωνίας (chat rooms), τις ιστοσελίδες κοινωνικής δικτύωσης και άλλους χώρους διαδικτυακής επικοινωνίας για να προσελκύσουν παιδιά με σκοπό να τα κακοποιήσουν.
Επισημαίνεται ότι, κατά την περίοδο της εφηβείας, τα νεαρά άτομα κάνουν την «προσωπική τους επανάσταση». Αυτή η στάση ανεξαρτησίας και η αναζήτηση νέων γνωριμιών μέσω διαδικτύου, καθιστούν τους εφήβους την πιο ευαίσθητη ομάδα στο ζήτημα της πορνογραφίας, αλλά και της σεξουαλικής παρενόχλησης.

Συχνά τέτοιου είδους ιστοχώροι θεωρούνται από τα παιδιά ασφαλείς τόποι συνομιλίας στο διαδίκτυο, τόσο εξαιτίας της δημόσιας φύσης της συζήτησης, αλλά και της λανθασμένης εκτίμησης των παιδιών ότι διατηρείται η ανωνυμία τους. Τα «αρπακτικά» ξεκινούν συζητήσεις με τα πιθανά θύματα, με σκοπό να αναπτύξουν φιλική σχέση με αυτά και να αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες σχετικά με τον τόπο διαμονής τους, τα ενδιαφέροντα, τα χόμπι και τις σεξουαλικές τους εμπειρίες. Οι συζητήσεις μπορεί να διαρκέσουν ημέρες, εβδομάδες, ακόμη και μήνες, μέχρι το «αρπακτικό» να αποκτήσει την εμπιστοσύνη του παιδιού.

Στην συνέχεια, προκαλούν σιγά-σιγά συζητήσεις σεξουαλικής φύσεως και τους στέλνουν φωτογραφίες ως κάτι το αποδεκτό και φυσιολογικό.
Πρόκειται για μια τακτική που υπονομεύει την απροθυμία των παιδιών στο να λάβουν μέρος σε σεξουαλική επαφή, αλλά και που έχει σκοπό να αποτρέψει το θύμα από το να ζητήσει προστασία από τους γονείς και τους δασκάλους του, αφού καταλήγει να νιώθει ένοχο που έχει ανταλλάξει τέτοιου είδους φωτογραφίες.
Τα «αρπακτικά» συνήθως είναι άτομα υπεράνω πάσης υποψίας: μορφωμένοι, επιφανείς, οικονομικά ευκατάστατοι, οι οποίοι πιθανόν να έχουν και δική τους οικογένεια, φιλήσυχοι, ευυπόληπτοι (πχ. επιστήμονες, δάσκαλοι, επιχειρηματίες κ.ά.).

Δεν θα διστάσουν να εκμεταλλευτούν τη θέση τους, αλλά και τη σχέση τους (συγγενείς) για να ικανοποιήσουν το αρρωστημένο τους πάθος.

Πως λειτουργούν τα κυκλώματα

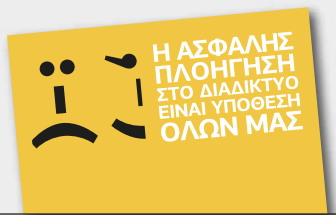
Πρόκειται για «κλειστές ομάδες», οι οποίες επικοινωνούν μέσω ομάδων συζήτησης (newsgroups), είτε μέσω δωματίων επικοινωνίας (chat rooms) είτε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail). Πάγια τακτική των κυκλωμάτων που διακινούν υλικό είναι η χρήση παραπλανητικών φωτογραφιών στην αρχική σελίδα των ιστοσελίδων.

Οι ιστοσελίδες στις οποίες «ανεβάζουν» πορνογραφικό υλικό ανηλίκων είναι «καμουφλαρισμένες», ώστε να μην εντοπίζονται (είναι αδύνατον με την χρήση μιας μηχανής αναζήτησης). Δημιουργούν videos στα οποίο αναμιγνύουν πορνογραφία ενηλίκων μαζί με ανηλίκων για να δυσκολεύουν τον εντοπισμό τους.

Μερικές από τις διεθνείς επιχειρήσεις στις οποίες έχει συμμετάσχει η Υπηρεσία μας: **CAROUSELL I & II, KOALA, STORM, PURITY, MYOSIS, TWINS, CHARLY, SPIDER WEB, ICARUS, ANGELS.**

Το υλικό πορνογραφίας ανηλίκων που έχει βρεθεί προκαλεί απδία και φρίκη. Από βρέφη λίγων μηνών έως και παιδιά 17 ετών, αυτοί είναι οι τραγικοί πρωταγωνιστές των άρρωστων σεξουαλικών βίντεο και φωτογραφιών. Ανήλικοι, οι οποίοι, με την χρήση ναρκωτικών ουσιών, υποχρεώνονται σε ερωτικές περιπτύξεις είτε μεταξύ τους είτε με ενήλικα άτομα, ακόμη και με ζώα.

Οι περισσότερες φωτογραφίες και βίντεο προέρχονται από χώρες της λατινικής Αμερικής, της νοτιοανατολικής Ασίας και της Αφρικής, όπως η Βενεζουέλα, η Βραζιλία, η Ταϊλάνδη, η Σιγκαπούρη και η Αλγερία. Το κόστος για την απόκτηση των φωτογραφιών και των βίντεο από τα «αρπακτικά» κατηγοριοποιούνται ανάλογα με την ηλικία των παιδιών ή το περιεχόμενό τους.



#παιδική_πορνογραφία_στο_διαδίκτυο

όταν η παιδική αξιοπρέπεια κινδυνεύει και ηλεκτρονικά

Η παραγωγή υλικού παιδικής πορνογραφίας είναι ένα παγκόσμιο φαινόμενο με τεράστια κέρδη. Τα κυκλώματα παιδικής πορνογραφίας δραστηριοποιούνται καθημερινά σε όλο τον κόσμο. Αυτό το νοσηρό εμπόριο θεωρείται πλέον η δεύτερη πιο προσοδοφόρα εγκληματική δραστηριότητα μετά το εμπόριο ναρκωτικών. Μόνο στις ΗΠΑ, εκτελούνται καθημερινά 700.000 συναλλαγές γύρω από την παιδική πορνογραφία και διακινούνται δύο τρισεκατομμύρια δολάρια, ενώ, σε παγκόσμιο επίπεδο, διακινούνται καθημερινά πέντε τρισεκατομμύρια δολάρια κατά μέσο όρο.

#ασφάλεια_πληροφοριών_ &_βιομηχανική_κατασκοπεία

όταν κάθε επιχείρησή βάλλεται ηλεκτρονικά

Bold Ogilvy & Mather

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

Χορηγός Φιλοξενίας
ATHENAEUM INTERCONTINENTAL ATHENS

Χορηγός Επικοινωνίας
ΒΗΜΑ FM 99,5

ΕΠΙΚΟΙΝΩΝΙΑ

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ο πολύτιμος δεκάλογος της επιχείρησής σας:

Antivirus – Antimalware

Θα πρέπει να υπάρχει πρόγραμμα προστασίας από ιούς (Antivirus) και πρόγραμμα προστασίας από κακόβουλο λογισμικό (Antimalware), τα οποία θα πρέπει να είναι ενημερωμένα για όλες τις τρέχουσες απειλές.

Firewall

Με τη χρήση του firewall, μπορείτε να παρακολουθείτε και να εντοπίζετε τυχόν ασυνήθιστη συμπεριφορά ενός επιμέρους προγράμματος. Το firewall αποτελεί την «καρδιά» της πολιτικής ασφαλείας, γιατί φιλτράρει την κίνηση του δικτύου της επιχείρησης.

Intrusion Prevention System

Το σύστημα Ελέγχου Επιθέσεων (IPS), ψάχνει για ιούς, αλλά και παρακολουθεί τα συστήματά σας για οποιαδήποτε ασυνήθιστη δραστηριότητα.

Διαχείριση Χρηστών

Πολιτική πρόσβασης χρηστών στο δίκτυο της επιχείρησης. Έλεγχος της πρόσβασης των χρηστών στο δίκτυο της επιχείρησης μέσω:
Authentication («Αυθεντικοποίηση» των χρηστών - Επιβεβαίωση της ταυτότητας των χρηστών)
Authorization Καθορισμός επιτρεπόμενων ενεργειών για κάθε χρήστη.
Accounting Δημιουργία αρχείου ενεργειών για τον κάθε χρήστη (τι ενέργειες έκανε και πότε).

Απομακρυσμένη πρόσβαση χρηστών. Οποιοσδήποτε χρήστης θα πρέπει να συνδέεται στο δίκτυό σας μέσω κατάλληλου Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network-VPN) με τα ακολουθούμενα επίπεδα ασφαλείας.

Εκπαίδευση Χρηστών, ώστε όλοι οι χρήστες να καταλαβαίνουν τη σπουδαιότητα της πιστής εφαρμογής των κανόνων ασφαλείας. Κάποιοι κανόνες ασφαλείας, ενδεικτικά, μπορεί να είναι: να σβήνουν τον υπολογιστή πριν την απομάκρυνση από το γραφείο τους και να χρησιμοποιούν ισχυρούς κωδικούς ασφαλείας (passwords). Επιπλέον, το σύστημα δε θα πρέπει να επιτρέπει σε ένα χρήστη να έχει πρόσβαση στο δίκτυο αν δεν έχει χρησιμοποιήσει ισχυρό password.
Έλεγχος των αδειών χρήσης λογισμικού. Οι χρήστες δε θα πρέπει να κατεβάζουν οποιοδήποτε λογισμικό κατά βούληση, γιατί μπορεί να θέσουν σε κίνδυνο το δίκτυο την επιχείρησή σας.
Εφαρμογή πολιτικής πρόσβασης των χρηστών και στο έντυπο υλικό της επιχείρησης.
Εφαρμογή κυρώσεων σε όποιο χρήστη δεν εφαρμόζει την πολιτική ασφαλείας της επιχείρησης.

Πολιτική ασφαλείας στις χρησιμοποιούμενες συσκευές

Διαμόρφωση κρίσιμων συσκευών, ώστε να μην υποστηρίζουν τη χρήση φορητών συσκευών μεταφοράς δεδομένων (π.χ. USB stick)
Μην επιτρέπετε σε άτομα εκτός επιχείρησης, όπως επισκέπτες να συνδέονται στο δίκτυο της επιχείρησής σας. Σε αντίθετη περίπτωση, θα πρέπει να ακολουθούν το δικό σας επίπεδο ασφαλείας. Θα πρέπει δηλαδή, να γίνετε έλεγχος της πρόσβασης στο δίκτυο από φορητές ασύρματες συσκευές όπως κινητά τηλέφωνα ή ταμπλέτες (tablets), κ.τ.λ.
Χρήση λογισμικού Data Loss Prevention (DLP) για την αποφυγή περιπτώσεων διαρροής κρίσιμων δεδομένων της επιχείρησης.

Περιορισμός της έκτασης πρόσβασης

Θα πρέπει να υπάρχουν δικλείδες ασφαλείας, ώστε αν κάποιος εισβολέας καταφέρει να εισχωρήσει σε κάποιο τμήμα του δικτύου σας, να μη μπορεί αυτομάτως να εισχωρήσει και σε όλο το δίκτυο.

Γνώση των αδυναμιών του δικτύου σας

Δεν υπάρχει το τέλειο σύστημα ασφαλείας, γι' αυτό θα πρέπει ο υπεύθυνος της επιχείρησης-ασφαλείας να γνωρίζει τα τρωτά σημεία του και τις περιοχές που παρουσιάζουν το μεγαλύτερο κίνδυνο και να απαγορεύεται η πρόσβαση σε αυτές.

Κατοχύρωση Διπλωμάτων Ευρεσιτεχνίας

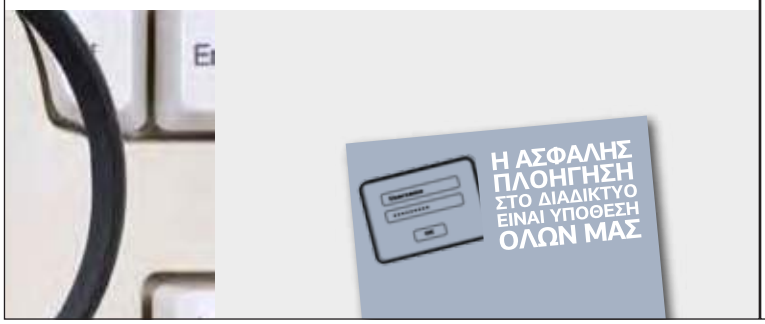
Διασφάλιση των κρίσιμων δεδομένων της επιχείρησης με Διπλώματα Ευρεσιτεχνίας, όπου είναι εφικτό.

Παρακολούθηση του φυσικού χώρου της επιχείρησής σας με χρήση καμερών ασφαλείας.

Εκτίμηση του κόστους

Θα πρέπει να δίνεται ιδιαίτερη σημασία στην εκτίμηση του κόστους για την ασφάλεια της επιχείρησης και να συνυπολογίζεται στον προϋπολογισμό της επιχείρησης, αφού είναι κρίσιμο στοιχείο για την υπόσταση της επιχείρησης.

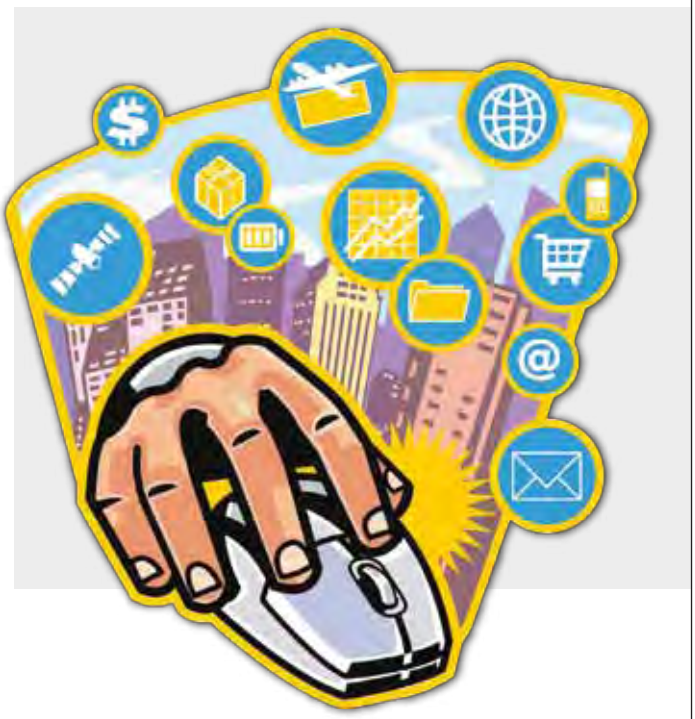
Αν πέσετε θύμα βιομηχανικής κατασκοπείας ενημερώστε άμεσα την Υπηρεσία μας, καλώντας στο τηλέφωνο 11012 ή στο τηλέφωνο 210-6476464 ή μέσω email στο **ccu@cybercrimeunit.gov.gr**



#ασφάλεια_πληροφοριών_ &_βιομηχανική_ κατασκοπεία

όταν κάθε επιχείρησή βάλλεται ηλεκτρονικά

Με τον όρο βιομηχανική κατασκοπεία, σε επίπεδο επιχειρήσεων, εννοούμε τη **συλλογή πολύτιμων δεδομένων εταιρειών, είτε από άλλες εταιρείες που αποσκοπούν στη βελτίωση των συγκριτικών πλεονεκτημάτων τους είτε από ιδιώτες-hackers.**



#cyberbullying

όταν η ψυχολογική βία στο διαδίκτυο απειλεί κάθε παιδί

Bold Ogilvy & Mather

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

Χορηγός Φιλοξενίας

ATHENAEUM INTERCONTINENTAL ATHENS

Χορηγός Επικοινωνίας

ΒΗΜΑ FM 99,5

ΕΠΙΚΟΙΝΩΝΙΑ

Δίωξη Ηλεκτρονικού Εγκλήματος
Cyber Crime Unit
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr
Τηλ.: 11012, Fax: 2106476462

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
ΥΠΗΡΕΣΙΑ ΟΙΚΟΝΟΜΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ
& ΔΙΩΞΗΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

CYBER CRIME UNIT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Τι είναι το cyberbullying

Ίσως έχει τύχει σε εσένα ή σε κάποιο φίλο σου, να δείτε μια παραλλαγμένη φωτογραφία σας στο διαδίκτυο ή να έχετε δεχθεί ένα προσβλητικό μήνυμα. Όλα τα παραπάνω είναι **περιστατικά ψηφιακής παρενόχλησης** και, όσο αστεία και αν είναι γι' αυτόν που τα έκανε ή για τα άτομα που τα είδαν, δεν φαίνονται καθόλου αστεία σε αυτούς που προσβάλλονται.

Η ψηφιακή παρενόχληση (cyberbullying) **είναι οποιαδήποτε επαναλαμβανόμενη πράξη εκφοβισμού, επιθετικότητας, παρενόχλησης, τρομοκρατικής ή αυταρχικής συμπεριφοράς που πραγματοποιείται μέσω της χρήσης ψηφιακών συσκευών (Η/Υ, κινητών τηλεφώνων).** Η ψηφιακή παρενόχληση αποτελεί απαράδεκτη συμπεριφορά. Δεν πρέπει σε καμία περίπτωση να παραβλέπεται ή να αγνοείται. Το φαινόμενο γνωρίζει έξαρση τον τελευταίο καιρό παγκοσμίως και δεν είναι λίγα τα περιστατικά και στη χώρα μας.

Το φαινόμενο του **cyberbullying** είναι περίπλοκο, καθώς μπορεί το "bullying" να έχει αντικαταστήσει, κατά μία έννοια, την παλιά «καζούρα» στα σχολεία. Παρ' όλα αυτά, έχει εντελώς διαφορετικά στοιχεία: ο ψηφιακός εκφοβισμός μοιάζει πολύ με τον απλό εκφοβισμό, αφού υπάρχει θύτης, θύμα και παρατηρητές. Έχει όμως και μερικές διαφορές, όπως:

- μπορεί να φτάσει σε πολύ λίγο χρόνο σε πολλούς παραλήπτες
- τα ηλεκτρονικά μηνύματα είναι σχεδόν αδύνατον να ελεγχθούν
- ο θύτης νιώθει ότι μπορεί να παραμείνει ανώνυμος
- Η έλλειψη προσωπικής επαφής με το θύμα κάνει το δράστη σκληρότερο
- το θύμα πλήττεται στο σπίτι και στον προσωπικό του χώρο.

Τα μέσα που χρησιμοποιούνται για την παρενόχληση μέσω διαδικτύου είναι:

- το ηλεκτρονικό ταχυδρομείο (e-mail)
- τα γραπτά μηνύματα (sms)
- μέσα κοινωνικής δικτύωσης (social media)
- δωμάτια επικοινωνίας (chat rooms)
- ιστολόγια (blogs)
- διαδικτυακά παιχνίδια (internet games)

Πως εκδηλώνεται το cyberbullying

Αυτοί που ασκούν εκφοβισμό, χρησιμοποιούν τις νέες τεχνολογίες για να παρενοχλήσουν, να απειλήσουν, να εκφοβίσουν, να δυσφημήσουν και, σε μερικές περιπτώσεις, να υποδυθούν τρίτους ή να υποκλέψουν την ταυτότητά τους. Μερικές από τις πιο κοινές μεθόδους είναι οι εξής:

- Αποστολή κειμένων, e-mail, ή άμεσων μηνυμάτων με προσβλητικό περιεχόμενο (σε instant messengers ή chatrooms)
- Η κακόβουλη δημοσίευση φωτογραφιών σε μέσα κοινωνικής δικτύωσης (social networks), ιστολόγια (blogs) ή άλλες ιστοσελίδες με μοναδικό σκοπό την παρενόχληση
- Διάδοση φημών και ψευδών γεγονότων με σκοπό την δυσφήμιση σε τρίτους σε μέσα κοινωνικής δικτύωσης, ιστολόγια, ιστοσελίδες κ.λπ.
- Ανώνυμες κλήσεις και μηνύματα με σκοπό τον φόβο και την ταραχή
- Χρήση του ονόματος ξένου χρήστη με σκοπό τη διάδοση φημών και ψεμάτων για κάποιον τρίτο (κλοπή ταυτότητας)
- Η δημιουργία ιστοσελίδων που στοχοποιούν συγκεκριμένα άτομα καλώντας άλλους να δημοσιεύσουν μηνύματα μίσους
- Η αποστολή ειδικών προγραμμάτων trojan horses (δούρειοι ίπποι) σκόπιμα για να δημιουργήσουν πρόβλημα, με την υποκλοπή κωδικών
- Εκφοβισμός στη διάρκεια ενός διαδραστικού online παιχνιδιού.

Προφίλ Θύτη-Θύματος

Ο καθένας μας μπορεί να πέσει θύμα ψηφιακής παρενόχλησης. Μπορεί να γίνει και θύτης, ή, ακόμη πιο συχνά, να γίνει παρατηρητής. Η ψηφιακή παρενόχληση ίσως ελκύει παιδιά που δεν τα έχουν παρενοχλήσει ποτέ στην πραγματική ζωή και επειδή πιστεύουν ότι είναι ανώνυμα όταν χρησιμοποιούν το διαδίκτυο ή το κινητό τους. Θα μπορούσαν να κάνουν πράγματα που δεν θα διανοούνταν να τα διαπράξουν πρόσωπο με πρόσωπο, και να χρησιμοποιήσουν τις νέες τεχνολογίες για να αναστατώσουν εσκεμμένα ένα φίλο, έναν άγνωστο, ως κι ένα δάσκαλό τους. Πολλές φορές μπορεί ακόμα και να ενδώσουν στην πίεση συνομηλίκων τους και να προωθήσουν ένα e-mail με εκφοβιστικό περιεχόμενο δίχως να αναλογιστούν τις συνέπειες.

Για ποιους λόγους μπορεί κάποιος να εκφοβίζει μέσω του Διαδικτύου;

- Η ανάγκη για επιβολή δύναμης
- Θυμός
- Ζήλια
- Διασκέδαση
- Ψυχολογική καταπίεση
- Λόγοι αντεκδίκησης
- Η ανάγκη για προσοχή

Πως αισθάνονται τα θύματα;

- Θυμό
- Αγανάκτηση
- Θλίψη
- Ντροπή
- Φόβο

Συνέπειες

Το cyberbullying φαντάζει ίσως ως αθώο αστείο, μπορεί να έχει όμως πολύ σοβαρές συνέπειες όπως:

- Αποχή από τα μαθήματα
- Απότομη πτώση στις σχολικές επιδόσεις
- Εκτέλεση πράξεων αντίθετων με τον χαρακτήρα του παιδιού ή παράνομες πράξεις λόγω εκβιασμού
- Κατάθλιψη
- Αυτοκτονία

Χαρακτηριστική είναι η περίπτωση της 13χρονης Megan από τις Η.Π.Α. που έπασχε από κατάθλιψη και η οποία αυτοκτόνησε, όταν ο διαδικτυακός της φίλος Josh την «παράτησε». Αποδείχτηκε ότι ο φίλος ήταν στην πραγματικότητα η μητέρα μιας φίλης με την οποία η Megan είχε τσακωθεί.

Τρόποι δράσης

Σε περίπτωση που έχεις πέσει θύμα εκφοβισμού μέσω διαδικτύου, είναι ανάγκη να προβείς σε μια σειρά ενεργειών:

- Απόφυγε να απαντήσεις στις απειλές του δράστη. Απαντώντας επιθετικά, φέρνουμε νέες απειλές και την ικανοποίηση στον δράστη ότι η παρενόχληση λειτουργεί.
- Άλλαξε λογαριασμό e-mail ή «κατέβασε» τη σελίδα δικτύωσής σου και, αν είναι εφικτό, δημιούργησε νέους λογαριασμούς.
- Διατήρησε αποδεικτικά της δράσης, συμπεριλαμβάνοντας όσα περισσότερα στοιχεία μπορείς, όπως ημερομηνίες και ώρες, λογαριασμούς ηλεκτρονικού ταχυδρομείου και λοιπά. Καλό θα είναι τα στοιχεία αυτά να υπάρχουν και σε εκτυπωμένη μορφή.
- Αφαίρεσε από τις λίστες των «φίλων» αυτόν που σε παρενόχλησε και ρύθμισε το προφίλ κοινωνικής δικτύωσης ώστε να είναι «απόρρητο», αν δεν είναι ήδη.
- Εάν ο θύτης είναι γνωστό σου πρόσωπο, σε αυτήν την περίπτωση ζήτησέ του να σβήσει τα μηνύματα και να αποκαταστήσει την αλήθεια σε περίπτωση διάδοσης φημών. Είναι σημαντικό να ενημερωθούν οι γονείς του παιδιού για τη συμπεριφορά του με βασικό σκοπό να περιοριστεί ο θύτης.
- Σε περίπτωση που η παρενόχληση πραγματοποιηθεί σε κάποια ιστοσελίδα κοινωνικής δικτύωσης (π.χ. Facebook, Hi5) κάνε αναφορά για το περιστατικό στους διαχειριστές της ιστοσελίδας.
- Μη κρατάς τους εκφοβισμούς για τον εαυτό σου. Δεν είσαι μόνος/μόνη! Πες το σε έναν ενήλικα που γνωρίζεις και εμπιστεύεσαι. Μπορούν να σε βοηθήσουν στην καταπολέμηση της ψηφιακής παρενόχλησης. Πρέπει οπωσδήποτε να αναφέρεις το περιστατικό σε έναν ενήλικα, είτε πρόκειται για τους γονείς σου είτε για κάποιον εκπαιδευτικό ή άλλο κοντινό και έμπιστο άτομο, και, φυσικά να το καταγγείλεις, ακόμα και μόνος σου, καλώντας στη Δίωξη Ηλεκτρονικού Εγκλήματος, στο 11012.

Σε περίπτωση που ο εκφοβισμός πραγματοποιηθεί μέσω κάποιας ιστοσελίδας κοινωνικής δικτύωσης ή chat room:

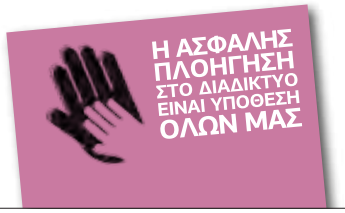
- **Facebook:** εάν κάποιος χρήστης σε ενοχλεί στο Facebook, ανάφερέ τον πατώντας την επιλογή «Αναφορά/Μπλοκάρισμα» (Report/Block) που βρίσκεται στο προφίλ του. Στο μενού ενεργειών της αναφοράς, μπορείς να δηλώσεις την αιτία της αναφοράς, π.χ. παριστάνει εσένα (κλοπή ταυτότητας), σε προσβάλει κ.ά. Μπορείς επίσης να επιλέξεις να μπλοκάρεις κάποιον χρήστη που σ' ενοχλεί, ώστε να μη λαμβάνεις μηνύματά του. Ένας καλός οδηγός ασφαλείας για παιδιά και γονείς βρίσκεται στο www.facebook.com/safety.
  Οι χρήστες κάτω των 13 ετών απαγορεύονται και μπορείς να αναφέρεις την ύπαρξή τους στο **www.facebook.com/help/contact/?id=210036389087590.**

Επίσης, στο **www.facebook.com/help /215543298568604/,** μπορείς να βρεις τη διαδικασία επαναφοράς «κλεμμένου» λογαριασμού facebook.

- **MySpace:** οδηγός ασφαλείας βρίσκεται στο www.myspace.com/safety.
- **Youtube:** εάν υπάρχει «ανεβασμένο» κάποιο κακόβουλο βίντεο, μπορείς να το αναφέρεις, πατώντας την επιλογή «Report» που βρίσκεται κάτω από το βίντεο.
- **Instant messaging** (MSN-Yahoo): επιλέγοντας το «Help tab», θα ανοίξει πολλαπλές επιλογές, μια εκ των οποίων είναι το «Report Abuse».
- **Chatrooms:** στη συντριπτική πλειοψηφία τους, υπάρχουν ρυθμιστές (moderators) που είναι συνήθως πολύ αυστηροί με περιπτώσεις κακόβουλης επίθεσης. Καλό θα ήταν να επικοινωνήσεις μαζί τους μέσω e-mail, αναφέροντας το συγκεκριμένο πρόβλημα.

Μέτρα Προστασίας

- Προστασία προσωπικών δεδομένων από ιστοσελίδες κοινωνικής δικτύωσης. Περιορίζοντας τις διαθέσιμες πληροφορίες για τον εαυτό μας η την οικογένειά μας, μειώνουμε τις πιθανότητες να πέσουμε θύματα αγνώστων δραστών.
- Δεν είναι σωστό να κάνουμε φίλους τους πάντες σε ιστοσελίδες κοινωνικής δικτύωσης.
- Να συμπεριφέρεσαι στους άλλους online, όπως θα έκανες στην πραγματική ζωή. Αν κάποιος σε αντιμετωπίζει με αγένεια ή είναι απότομος, δεν είσαι υποχρεωμένος ν' απαντήσεις. Θα δει ότι δεν έχει αποτελέσματα και θα σταματήσει τα προσβλητικά μηνύματα. Αν όχι, και τα καταχρηστικά μηνύματα συνεχιστούν, ζήτα βοήθεια από έναν έμπιστο ενήλικα.
- Ποτέ μην ανοίγεις ένα μήνυμα από κάποιον που δεν γνωρίζεις.
- Διάγραψε περίεργα μηνύματα ηλεκτρονικού ταχυδρομείου ή μηνύματα κειμένου από ανθρώπους που δεν γνωρίζεις. Σε περίπτωση αμφιβολίας, ζήτα συμβουλές από έναν έμπιστο ενήλικα.
- «Google yourself!». Χρησιμοποίησε μια μηχανή αναζήτησης ανά τακτά διαστήματα και πραγματοποίησε αναζήτηση με το όνομά σου ή το ψευδώνυμο που χρησιμοποιείς στο Διαδίκτυο. Έτσι θα μπορείς να εποπτεύεις την εικονική σου παρουσία.
- Δεν χρειάζεται να είσαι «πάντα συνδεδεμένος»! Αποσυνδέσου και κλείσε τον υπολογιστή. Δώσε στον εαυτό σου ένα διάλειμμα. Μη μένεις online για πάρα πολύ χρόνο.
- Βάλε τη φαντασία σου να δουλέψει όταν δημιουργείς κωδικούς πρόσβασης. Μη χρησιμοποιείς κωδικούς που εύκολα μπορεί κανείς να φανταστεί (ημερομηνία γέννησης κ.ά.)
- Αν δεις κάτι στο διαδίκτυο ή λάβεις ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή μήνυμα κειμένου που σε κάνει να αισθανθείς άβολα, κλείστε τον υπολογιστή ή το τηλέφωνο και ζήτα συμβουλές από έναν αξιόπιστο ενήλικα.



Τι είδαμε την περασμένη δεκαετία

Την περασμένη δεκαετία, μια σειρά τεχνολογικών εξελίξεων και κοινωνικών τάσεων καθιέρωσαν τη σημερινή μορφή του διαδικτύου. Χαρακτηριστικά παραδείγματα αποτέλεσαν τα εξής:

Social Media: Σημαντικότερο σημείο στην εξέλιξη του διαδικτύου την περασμένη δεκαετία αποτέλεσε αναμφίβολα η εκρηκτική ανάπτυξη των μέσων κοινωνικής δικτύωσης.

Video sharing: Με την ευρυζωνικότητα να είναι διαθέσιμη σε κάθε σπίτι και τις ταχύτητες να αυξάνονται σημαντικά, κατέστη πρακτικά εφικτό το video sharing, το οποίο - με πρωτοστάτη το YouTube και τις υπηρεσίες του έγινε κομμάτι της καθημερινότητας.

Mobile Internet - 3G - smartphones: Πολύ σημαντική εξέλιξη αποτέλεσε τεχνολογικά και η δυνατότητα σύνδεσης στο διαδίκτυο από τις συσκευές κινητών τηλεφώνων, που επέτρεψε στους χρήστες του διαδικτύου να συνδέονται από κάθε μέρος και με κάθε συσκευή.

Online gaming: Τεράστια ανάπτυξη γνώρισαν και τα διαδικτυακά παιχνίδια, κερδίζοντας πολύ γρήγορα μεγάλο αριθμό χρηστών. Τεράστιοι εικονικοί κόσμοι προσελκύουν καθημερινά ένα μεγάλο ποσοστό χρηστών, με κάποια από τα διαδικτυακά παιχνίδια να ξεπερνούν τους 10 εκατομμύρια χρήστες.

Internet radio: Το κλασικό ραδιόφωνο μεταλλάχθηκε σε μεγάλο βαθμό σε διαδικτυακό, κερδίζοντας πολλούς θαυμαστές και καταλύοντας τα σύνορα της μετάδοσης παγκοσμίως.

Blogs: Τα ιστολόγια αποτέλεσαν ένα από τα τελευταία trends της περασμένης δεκαετίας, δίνοντας βήμα σε όλους για έκφραση και κερδίζοντας καθημερινά εκατομμύρια θαυμαστές.

Διαδίκτυο

Το διαδίκτυο αποτελεί το μεγαλύτερο δίκτυο υπολογιστών στον κόσμο, το οποίο επιτρέπει την επικοινωνία και την ανταλλαγή πληροφοριών μεταξύ οποιωνδήποτε σημείων στον πλανήτη. Το διαδίκτυο έχει χαρακτηριστεί ως η μεγαλύτερη «εφεύρεση» όλων των εποχών, κατακτώντας ολόκληρη την υφήλιο μέσα σε μόλις μερικές δεκαετίες ζωής και αποτελώντας πλέον τη μεγαλύτερη οργανωμένη κοινωνία παγκοσμίως.

Το διαδίκτυο αποτελεί μια παράλληλη, «εικονική» παγκόσμια κοινότητα, η οποία καταλύει όλες τις κοινωνικές και πολιτιστικές διαχωριστικές γραμμές που υπάρχουν στον πραγματικό κόσμο και που τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεράσουν. Το διαδίκτυο, σε αντίθεση με τα παραδοσιακά μέσα ενημέρωσης και επικοινωνίας, καθιστά δυνατή τη ζωντανή αμφίδρομη επικοινωνία και δίνει τη δυνατότητα της άμεσης συμμετοχής σε όλους τους χρήστες με την ελεύθερη επιλογή λήψης, παροχής και διάχυσης της πληροφορίας. Καταλύοντας τα σύνορα και εκμηδενίζοντας τις αποστάσεις, το διαδίκτυο φαίνεται να κλίνει την πλάστιγγα πλέον εμφανώς υπέρ των επικοινωνιών στην αιώνια διαμάχη μεταξύ των μεταφορών και των επικοινωνιών.

Τι αναμένουμε να δούμε την επόμενη δεκαετία

Με βάση τις προηγούμενες εξελίξεις, τα δείγματα τα οποία έχουν παρουσιαστεί, και την τάση για ανάπτυξη, η επόμενη δεκαετία αναμένουμε να μας παρουσιάσει νέες καινοτόμες λύσεις και υπηρεσίες. Ας ρίξουμε μια ματιά στο μέλλον, σε ορισμένα από τα θέματα που αναμένεται να μας καταπλήξουν τα επόμενα χρόνια:

Gloud: Το cloud έχει ήδη κάνει αισθητή την παρουσία του στην παγκόσμια αγορά ανοίγοντας νέους δρόμους στην πρόσβαση σε δεδομένα και υπηρεσίες. Η πληροφορία πλέον καθίσταται προσβάσιμη από οποιοδήποτε σημείο και από οποιαδήποτε συσκευή έχει πρόσβαση στο διαδίκτυο, και οι υπηρεσίες δεν απαιτούν εγκατάσταση, με αποτέλεσμα οι απαιτήσεις για υπολογιστική ισχύ να μειώνονται τόσο για τους ιδιώτες όσο και για τις εταιρείες. Την επόμενη δεκαετία, περιμένουμε ολοένα και περισσότερες υπηρεσίες να μετακινηθούν στο «σύννεφο», και την παρουσίαση online λειτουργικών συστημάτων, κειμενογράφων και άλλων εργαλείων καθημερινής χρήσης, τα οποία θα διατίθενται αποκλειστικά ως cloud services.

3D Internet: Με τις τεχνολογίες των monitors να υποστηρίζουν ήδη 3D προβολή, αναμένεται σύντομα το διαδίκτυο να διαθέτει 3D ιστοσελίδες και εφαρμογές, και τα 3D objects να αντικαταστήσουν τα σημερινά video και φωτογραφίες, δίνοντας ένα νέο πρόσωπο στο διαδίκτυο.

IPTV: Όλες οι νέες συσκευές τηλεόρασης διαθέτουν σύνδεση στο διαδίκτυο και οι υπηρεσίες broadcasting μέσω διαδικτύου καλύπτουν πλέον πλήρως τις ανάγκες για μετάδοση εικόνας. Με βάση τα παραπάνω και ακολουθώντας το ραδιόφωνο, έχοντας ήδη τα πρώτα δείγματα στην αγορά, η τηλεόραση αναμένεται να μεταλλαχθεί ίσως και εξολοκλήρου σε Internet TV.

E-learning – τηλεεργασία: Δύο εφαρμογές του διαδικτύου που βρίσκονται πολύ καιρό σε αναμονή, αναμένεται να έλθουν στο προσκήνιο, μειώνοντας τα κόστη μετακίνησης και τα κόστη συντήρησης των εταιρειών.
Νανοτεχνολογία: Η νανοτεχνολογία ήδη βρίσκει εφαρμογή σε πάρα πολλούς τομείς και τα τελευταία πειράματα δείχνουν ότι συσκευές όπως οι μοριακοί υπολογιστές δεν αποτελούν πλέον άπιαστο όνειρο. Δεν αποκλείεται, λοιπόν, πολύ σύντομα οι χρήστες να διαθέτουν πανίσχυρους υπολογιστές σε ένα ρολόι χειρός ή ένα απλό ακουστικό.
Πλήρης διασύνδεση: Ακολουθώντας την πρόβλεψη του Bill Gates («Every device in the world will be connected») και με το IPv6 να τίθεται σε εφαρμογή σε ορισμένες χώρες της Ευρώπης, σύντομα όλες οι συσκευές θα διασυνδεθούν σε ένα υπερδίκτυο, το οποίο θα περιλαμβάνει τις οικιακές ηλεκτρικές συσκευές, τα αυτοκίνητα, τα κινητά τηλέφωνα και κάθε φορητή ή οικιακή συσκευή.

4G 5G και πέρα: Ήδη από το 2009, το 4G είναι πραγματικότητα. Με τις εξελίξεις στον τομέα mobile broadband να καλπάζουν, οι επόμενες γενιές κινητών δικτύων δεν θα αργήσουν να ακολουθήσουν.

ISBN 978-960-14-2660-0