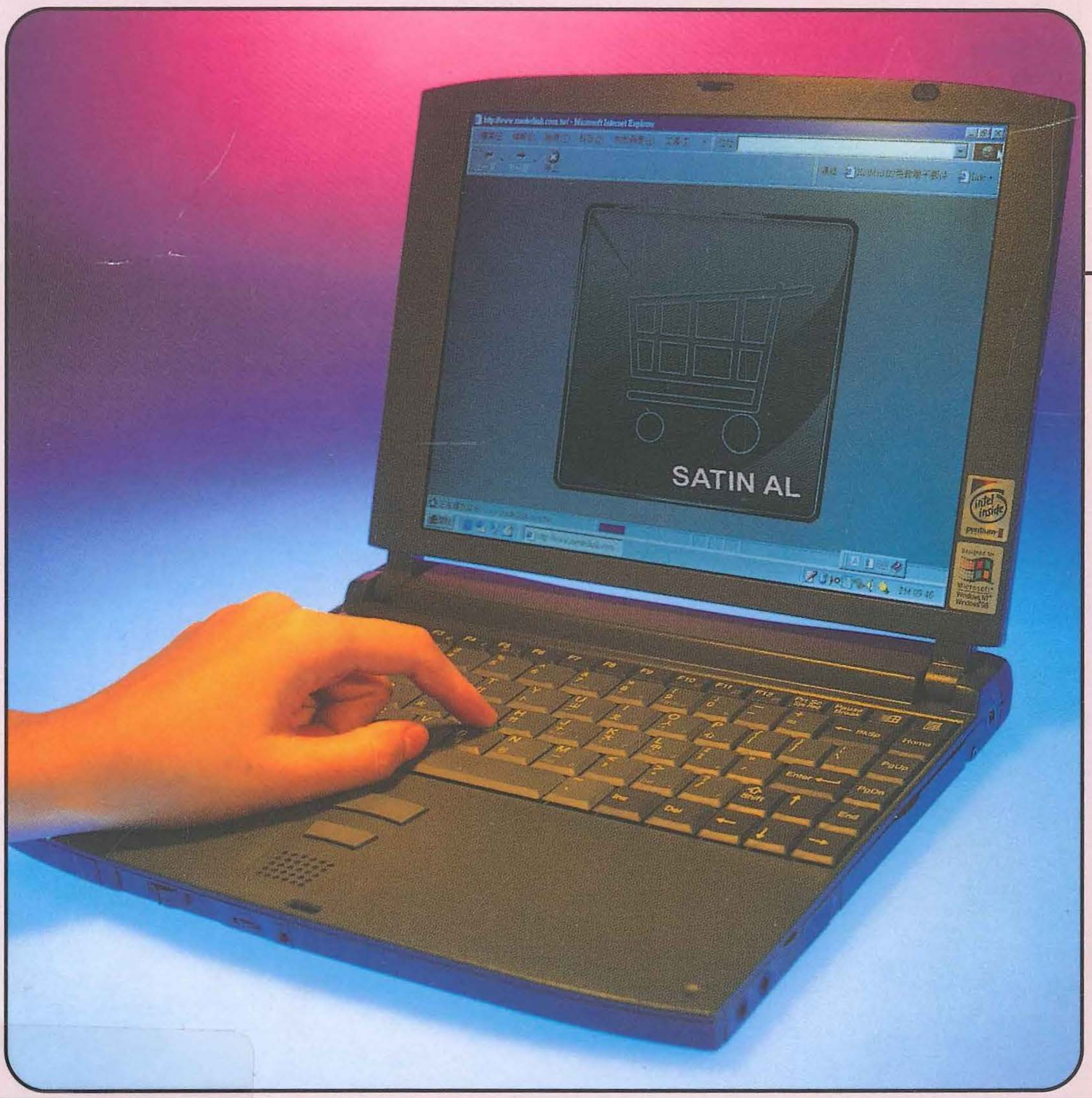
e-TİCARET GÜVENLİK REHBERİ



2. BASKI

KOBİ ARAŞTIRMALARI

YAYIN NO: 2009-9

İSTANBUL TİCARET ODASI

e-TİCARET GÜVENLİK REHBERİ

Prof. Dr. Çetin Kaya Koç
Av. Tuğrul Sevim

YAYIN NO: 2009-9
İstanbul, 2010

2.BASKI

ISBN 978-9944-60-463-5 (Basılı)
ISBN 978-9944-60-464-2 (Elektronik)

İTO ÇAĞRI MERKEZİ
Tel: (212) 444 0 486

İTO yayınları için ayrıntılı bilgi
Bilgi ve Doküman Yönetimi Şubesi
Dokümantasyon Servisi'nden alınabilir.

Tel: (212) 455 63 29
Faks: (212) 512 06 41
E-posta: ito.yayin@ito.org.tr
İnternet: www.ito.org.tr

Odamız yayınlarına tam metin ve ücretsiz olarak
internetten ulaşabilirsiniz.

YAYINA HAZIRLIK, BASKI, CİLT
G.M. Matbaacılık ve Ticaret A.Ş.
Tel: (212) 629 00 24-25 Faks: (212) 629 20 13
www.goldenmedya.com.tr

İÇİNDEKİLER

SUNUŞ

İletişim teknolojilerinde görülen hızlı gelişim ve değişim elektronik ticarette yeni pazar fırsatlarını ve iş modellerini gündeme getirmiştir. Hızla küreselleşen dünyada işletmelerin internet teknolojilerini kullanarak pazarlama faaliyetlerini sürdürmeleri, tüketicilerin ise internet kanalıyla satın alım yapmaları; giderek geleneksel ticaretin piyasadaki payının elektronik ticaret karşısında azalmasına yol açmıştır.

e-Ticaret; tüketicilerin, işletmelerin ve kamu kurumlarının internet/intranet ortamında multimedya şeklindeki sayısal bilgilerin işlenmesi, iletilmesi ve saklanması yoluyla, bilgilenme ve araştırma yapma, mal ve hizmetlerin müşteriye teslimi ile ürün ya da hizmet bedelinin ödenmesi sürecidir. Elektronik ticaretin bilişim teknolojilerine bağlı alternatif bir ticaret kanalı olarak gelişmesi ise güvenlik sorununu ön plana çıkarmış ve güvenlik konusu bilişim teknolojisi çerçevesi içinde özel bir bölüm olarak kendini göstermiştir.

Bütün bu hususlar göz önünde tutularak; konuyla ilgilenenlere bilgi sunabilmek amacıyla hazırlanan "e-Ticaret Güvenlik Rehberi" isimli çalışmayı Odamız adına hazırlayan Prof. Dr. Çetin Kaya Koç ve Av. Tuğrul Sevim'e teşekkür eder, çalışmanın tüm üyelerimize ve konuyla ilgili herkese yararlı bir kaynak oluşturmasını dilerim.

Dr. Cengiz Ersun
Genel Sekreter

Çetin Kaya KOÇ

1980 ve 1982 yıllarında İstanbul Teknik Üniversitesi Elektrik Mühendisliği bölümünden lisans ve yüksek lisans derecelerini alan Koç, 1985 ve 1988'de ise University of California (Santa Barbara) Elektrik ve Bilgisayar Mühendisliği Bölümünden yüksek lisans ve doktora derecelerini aldı. 1988-1992 arasında University of Houston'da yardımcı doçent ve 1992-2007 arasında ise Oregon State University'de doçent ve profesör olarak çalıştı. Bu üniversitede Bilgi Güvenlik Laboratuvarı'nı kuran Koç, dokuzu şu an profesör olan on dört doktora öğrencisi yetiştirmiştir. Kriptografide dünyada önde gelen uzmanlarından biridir. Springer tarafından yayınlanan iki kitabı vardır: Cryptographic Algorithms on Reconfigurable Hardware ve Cryptographic Engineering. Ayrıca IEEE Fellow en yüksek meslek ödülü almıştır.

Tuğrul SEVİM

Galatasaray Lisesi'nden sonra Marmara Üniversitesi Hukuk Fakültesi'nde lisans eğitimini, İstanbul Bilgi Üniversitesi'nde Ekonomi Hukuku Alanında yüksek lisans eğitimi tamamlayan Tuğrul Sevim özel hukuk alanında doktora çalışmalarını sürdürmektedir. Profesyonel olarak elektronik ticaret, elektronik imza, bilgi güvenliği, fikri haklar, DRM, bilgi ve iletişim teknolojileri hukuku ve stratejileri üzerine serbest danışmanlık faaliyetlerini Türkekul Hukuk Bürosu Teknoloji Hukuku Bölümü Direktörü sıfatıyla yürüten Av. Tuğrul Sevim, İstanbul Bilgi Üniversitesinde yarı zamanlı öğretim görevlisi olup; aynı üniversitenin hukuk yüksek lisans programında "Bilgi ve İletişim Teknolojileri Hukuku" dersi vermekte ve Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi Danışma Kurulu Üyesi olarak görev yapmaktadır.

ÖNSÖZ

Elektronik ticaret (e-ticaret) artık küresel bir olgu ve neredeyse bütün endüstriyel sektörleri kapsıyor. Elektronik ticaretin, gelişmiş ve gelişmekte olan ülkelerde büyümenin itici ekonomik gücü olma potensiyeline sahip olduğunu görüyoruz. Elektronik ticaret altyapılarını teşkil eden bilgi teknolojileri donanımları, yazılımları, haberleşme sistemleri ve internet, küçük ve orta büyüklükte işletmeleri dünya çapında bir pazarlama ve satış ağının parçası haline getiriyor ve onlara kendi milli sınırları dışında büyüme imkanları sunuyor.

Ancak aynı zamanda e-ticaret ortamı, üzerinde kurulmuş olduğu bilgisayar ve ağ sistemlerinin açık sistemler olması ve teknolojik atılımlar nedeniyle sürekli olarak kötü niyetli amaçlarla izlenmekte ve istismar edilmektedir. Doğal olarak, bu tip istismarların önlenmesi için gerekenleri yapmak veya yapılmasını sağlamak, ticaret sahibi kişilerin sorumluluk alanındadır. Bu rehber, İstanbul Ticaret Odası üyelerinin, güvenli bir e-ticaret ortamı sağlamak için gerekli doğru bilgilere, hızlı bir şekilde ulaşması için yazıldı. e-Ticaretin teknik ve hukuksal açılımlarını irdeleyerek, konunun uzmanı olmayan kişilerin anlayabileceği ve uygulayacağı bir seviyede açıklamaya özen gösterdik. Bize yardım sağlayan tüm meslektaş arkadaşlarımıza, özellikle, Nefin Huvaj Sevim, Yasin Beceni, Zafer Babür ve Sultan Selçuk'a teşekkürü borç biliriz.

Prof. Dr. Çetin Kaya Koç
Av. Tuğrul Sevim

KISALTMALAR

BK	Borçlar Kanunu
Bkz.	Bakınız
EC	European Commission
EİK	Elektronik İmza Kanunu
f.	Fıkra
HUMK	Hukuk Usulü Muhakemeleri Kanunu
md.	Madde
MSHY	Mesafeli Sözleşmeler Uygulama Usul Ve Esasları Hakkında Yönetmelik
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
sy.	Sayı
TCK	Türk Ceza Kanunu
TKHK	Tüketicinin Korunması Hakkında Kanun

1. e-TİCARET GÜVENLİĞİ - TEKNİK AÇILIMLAR

1.1. YENİ BİR TİCARET DÜNYASI

İnsanlık uzun zamandır bir ticaret dünyasında yaşıyor. İhtiyacımız olan şeyleri alıyor ve karşılığında verebileceğimiz şeyleri veriyoruz. Günümüzde ise ticaret yapmanın küresel değiş-tokuş aracı para. Dolayısıyla ticaret olmadan toplum işleyemez, bireyler yaşamdan tat alamaz ve hatta yaşam devam edemez.

Ancak yeni bir devrim yaklaşıyor. Nakitsiz, elektronik hesapların kullanıldığı ve internet üzerinden "online" ticaret yapılan bir dünya olma yolunda hızla ilerliyoruz. Bu değişim hareketinin hızı hakkındaki tahminler çeşitli olsa da, değişimin olması gerektiği kesin. Bu konuda şüpheciler ve iyimserler olsa da, internet bankacılık uygulamaları şu an zaten çalışıyor ve öyle görülüyor ki, geniş alana yayılmış elektronik ticaret bu yolu tamamen kaplayacak.

1.1.1. ELEKTRONİK TİCARET

Elektronik ticaret (e-ticaret) artık küresel bir olgu ve neredeyse bütün endüstriyel sektörleri kapsıyor. e-ticaretin birtakım alt kategorileri var: işletmeden-tüketiciye (business-to-consumer, B2C), işletmeden-işletmeye (business-to-business, B2B) - ki burada, özellikle üreticiler ve toptancılar arasındaki ilişkiden bahsediyoruz. Ayrıca, hükümetten-tüketiciye (government-to-consumer, G2C), hükümetten-işletmeye (government-to-business, G2B) türünden e-ticaret sayılacak etkinlikler de söz konusu, ancak burada e-devlet vatandaşlarına dönük hizmetleri internet vasıtasıyla sunmakta, örneğin vergi işlemleri, pasaport işlemleri gibi vatandaşların ve firmaların günlük hayatlarını etkileyen işlemleri yapmaktadır. Ancak prensip olarak toplam e-ticaret etkinliğinden kasıt, internet veya diğer (mobil telefon vb.) ağlar üzerinde yapılan toplam satıştır, yani değiş-tokuş edilen malların toplam değeridir.

Elektronik ticaretin, gelişmiş ve gelişmekte olan ülkelerde büyümenin itici ekonomik gücü olma potansiyeline sahip olduğunu görüyoruz. Elektronik ticaret altyapılarını teşkil eden bilgi teknolojileri donanımları, yazılımları, haberleşme sistemleri ve internet, küçük ve orta büyüklükte işletmeleri dünya çapında bir pazarlama ve satış ağının parçası haline getiriyor ve onlara kendi milli sınırları dışında büyüme imkanları sunuyor.

1.1.2. e-TİCARETİN BÜYÜME TRENDİ

Kasım 2007'de yapılan bir sayıma göre Amerika Birleşik Devletleri'nde 215 milyondan fazla kişi internet kullanıyor. Bu nüfusun %71'i demek. Bir sene öncesine göre %2 artış kaydedilmiş. Ayrıca hızlı internet kullanıcıları 100 milyonun üzerinde. Türkiye gibi hızlı büyümekte olan ülkelerde artış hızları %30'lara varıyor.

Diğer taraftan, ABD'de 2007 e-ticaret satışları 127 milyar dolar olarak hesaplanıyor. 2006 yılına göre artış hızı %17 idi. e-ticaret 2007 yılında toplan perakende satışın %3.2'sini kapsıyor; bir önceki yıl bu oran %2.8'di. Büyüme hızının 2008 ve 2009'da %20 olacağı öngörülüyor. Toplam perakende satış için e-ticaret oranının artışı, tüketicilerin ve satıcıların ortamı ve teknolojiyi benimsediklerinin güzel bir göstergesi. Ayrıca toplam perakende satış içinde %3.2'lik oran büyüme potensiyelinin çok yüksek olduğunu bize anlatıyor.

Şimdi bu rehberde bahsedeceğimiz konulara genel bir bakış olarak internet, internet güvenliği ve bunların online ticaretle olan ilişkisi konularını gözden geçirelim. İnternet üzerinden ticaret yapma, bunun faydaları, riskleri ve yasal olarak içerdiği anlam üzerinde bilgiler verelim.

1.1.3. e-TİCARETİN TARİHÇESİ

1969 yılında Amerikan Savunma Bakanlığı sponsorluğunda uzaktan kullanıcılar arasında bir araştırma yapılmıştı. Amaç bir savaş esnasında iletişimin durdurulmasını engellemekti. Böylece kontrolün dağıtıldığı bilgisayar ağları geliştirildi.

İnternet, bilgisayar ağından bağımsız olarak sabit boyutlu paketler (bilgi birimleri) iletmek için tasarlandı. Bilgisayar ağ noktaları (nodlar) oluşturulurken her mesaj bir veya daha fazla paketlere bölündü. Her paket kendi varacağı adrese yönlendirildi ve her paket, ağ boyunca kendi rotasını takip etti. Hedefe varınca, bu paketler mesaj içinde tekrar bir araya getirildi. Uzak bölgelerdeki, farklı yapıdaki bilgisayar sistemlerinin arasındaki iletişimi sağlamak için bir iletişim protokolü dizayn edildi. TCP/IP (Transmisson Control Protocol/Internet Protocol) adı verilen bu protokol şu an, bilgi transferi endüstrisi için de gerçek bir standart olmuştur. İnternet, Pentagon İleri Araştırma Projeleri Ajansı'nın bu projeye sponsor olmasından sonra ARPANET (Advanced Research Project Agency - ARPA) olarak adlandırıldı. ARPANET 1969'da dört adet nodla işe başladı. Sonra Temmuz

1971'den itibaren 15 noda genişledi. 1975 yılına kadar 57 noda ulaştı ve akabinde Amerikan Savunma Bakanlığı'na devredildi. Şimdi DARPANET ve MILNET diye iki parçaya bölünmüş olarak varlığını devam ettiriyor.

ARPANET veri ağlarının birçok alanında araştırma için bir temel sağlamıştır. TCP/IP protokolleri üzerinde çalışmalar 1970'lerin sonlarında başladı. 1980 yıllarında ise DARPA (Defence Advanced Research Project Agency), ARPANET nodlarını TCP/IP protokollerine dönüştürmeye başladığı zaman internet bağlantısı da başladı. Bu dönüşümler 1983 yılında bitirildi. TCP/IP protokolleri, TELNET ve FTP gibi bazı uygulamalar ve yüksek seviyeden sistemlerle geliştirildi. Bunlara ek olarak; paket aktarma, gönderme, akışı ve sıkışıklığı kontrol etme gibi bazı araştırmalara yönelindi.

Web, 1992'de tanıtıldı ve 1993'te gelişmeye başladı. Bundan itibaren ürün satışı veya reklamı yapan web sitelerinin sayısında sürekli bir artış meydana geldi. İnternet web sayfaları, artan çeşitli işler için bir satış noktası oldu. Gerçekten de birçok şirket internette kendi sayfalarını edinir oldu.

1.2. e-TİCARET GÜVENLİĞİ

Bilgi güvenliği konusu 1960'ların öncesine, öğrencilerin sabit zaman aralıklarıyla tüm bilgisayar sistemine girdikleri zamana dayanır. 1960'lı yılların sonlarında aynı anda birden çok kişinin erişim sağlamasına izin veren eş zamanlı bilgisayarlar tanıtıldı. Aynı zamanda, sistem programcısının diğer kullanıcılara göre daha yüksek seviyede hesaplama kaynağına ihtiyaç duyduğunun farkına varıldı.

Şu an sistem yöneticisi için "temel şifre" (root password) olarak bilinen, sistem operatörüne ait özel bir şifre belirlenerek bu ayrım sağlanmış oldu. Bununla birlikte, 1980'li yıllar boyunca, dağıtılmış erişim olarak bilinen bir ağ geliştirme devrimi tanıtıldı. Bu sistemde kullanıcılar kadar, sistem yöneticileri de bilgisayar sisteminden uzak taraflara yerleştirilebiliyordu. Yani, eski "tek noktadan sistem kaynaklarını koruma" fikri artık uygun değil. Bilgi topluluklarında yeni bir ağ güvenliği dalgası yayılıyor.

Geçen son 20 yıl, başlangıçtan beri ağ güvenliği bilgi dünyasının önemli bir parçası olmak için gelişme gösterdi. Ağ teknolojileri endüstri dünyasının bel kemiği olurken, ağ güvenliği de herhangi bir geçerli veri ağı için ön şart oldu.

Aynı zamanda internet, veri ağlarına zorla girmeyi tasarlayan sahtekarlar için elverişli bir zemin oluşturuyor. Genel kullanım için açık ve kolay bir erişim sağlayan internet, diğer herhangi bir ağa göre daha fazla saldırganın

dikkatini çeker ve bu konuda daha savunmasızdır. Ayrıca, internet ve internetin temeli olan TCP/IP protokolü, güvenlik düşünülmeden dizayn edilmiştir. Sonuç olarak, orijinal ağ dizaynı yerine, var olan ağda ek özelliklerle güvenlik tamamlanmıştır.

Ağ güvenliği üç parça halinde incelenebilir. Birinci bölüm, kullanıcı ya da program kaynağa ulaşmadan önce kimlik bilgilerinin doğrulanmasıdır. Bu işlem kimlik denetimi (authentication) olarak adlandırılır. Geleneksel olarak kimlik denetimi için parolalar kullanılır. İkinci bölüm, gizli bilgilerin yasadışı yollarla başkalarının eline geçmesini korumak için bilgi gizliliği konusunu içerir. Bilgi gizliliği genellikle şifreleme mekanizmalarıyla sağlanır. Son kısım ise bir mesajın gerçekten belli bir şahıs tarafından mı gönderildiğini ve gönderenin mesajı yolladığından beri değiştirip değiştirmediğini kontrol eden bir sistemdir. Bu fonksiyon da genellikle dijital imza projesiyle sağlanmaktadır.

Gelişmeye devam eden güvenlik servisleri birçok transfer protokolüne ve onların uygulamalarına ihtiyaç duyar. İlk olarak, internet için TCP/IP protokolünü düşünelim. Kimlik doğrulama ve gizlilik gibi güvenlik servisleri bu seviyededir. Ayrıca, TELNET, FTP ve elektronik posta gibi TCP/IP uygulamaları da kimlik doğrulama ve gizlilik servislerine ihtiyaç duyarlar. Benzer şekilde, web için protokoller yetkisiz erişimlerden korunmalıdır. Dolayısıyla benzeri birçok uygulamanın güvenlik servislerine ihtiyacı vardır.

Tüm bunların yanında çözülmeyi bekleyen birçok problem vardır. Örneğin, internet üzerinden yapılan iletişim sırasında güçlü şifreleme projelerine ihtiyaç olduğu gibi, şifremizin de korunmaya ihtiyacı vardır.

1.2.1. GÜVENLİ TİCARET

Tüm diğer konularda olduğu gibi internet üzerinde güvenli ticaret yapmak için de bazı anahtarlara ihtiyaç vardır. Bunlar; web servisi ile birlikte internet, güvenlik servisi ve ticaret uygulamalarıdır (online alışveriş merkezleri veya marketleri gibi). Bir örneği düşünelim: Ayşe internet üzerinden alışveriş yapmak istiyor. İlk yapması gereken, bilgisayarına kendi banka hesabından biraz nakit (dijital) para yüklemektir. Bundan dolayı önce hesabına ulaşır ve ihtiyacı olan kadar dijital nakit çeker. Bu işlem çok güvenli bir şekilde yapılmalıdır. Ayşe'nin kimlik bilgileri onaylanmalı, kullandığı miktar gizli tutulmalı ve hiç kimse onun yerine bu işlemi yapamamalıdır. Bu ticari alışveriş işlemi güvenli bir ödeme planı içermeli, web dosyalarına işlenmeli ve Ayşe ile banka arasındaki iletişim izlenmelidir.

İnternet protokolleri taraflar arasındaki ödeme bilgilerinin iletimini kontrol altında tutmalıdır. Sonuç olarak; gerek ticaret uygulamalarında, gerekse web protokollerinde işlemleri başarıyla tamamlayabilmek için güvenlik servislerine ihtiyaç vardır.

1.2.2. GÜVENLİK SORUNLARI

Online ticaret konusunun belki de en büyük meselesi, internet üzerinden güvenli işlem yapabilme ile ilgilidir. Güvenlik sorunu internet kullanıcıları için kolay kolay kaybolmayan bir endişe haline geldi.

Şimdi online ticaret konusunda dört temel güvenlik sorununu özetleyelim.

İlk güvenlik sorunu, tüketici kimliklerinin doğruluğunu denetlemek için yapılan elektronik bir metotla ilgilidir. Bu kimlik doğrulama işlemi, kullanıcıya şifre sormaktan fazlasını içerir. Örneğin, kullanıcı kendi kimliğini tanıtıp kabul ettirmek için belgeler ortaya koymalıdır. Bu, günümüzdeki kredi kartı veya ehliyet gibi belgelerin online versiyonudur. Bu güvenlik önlemi, online kimlik saptaması için kullanıcıların belgelerinin veya delillerinin çalınması ihtimali gibi olaylara karşı alınmıştır.

İkinci güvenlik sorunu, uzak taraflar arasında güvenli iletişim sağlayabilmekle ilişkilidir. Örneğin, bir işletme, alım satım işlemlerini yürütürken iletim işlemi boyunca veriler ve bilgiler korunmalı ve gizli tutulmalıdır. Bilgiler üzerinde herhangi bir art niyetli girişimde bulunmak, iletimin gizliliğini ve özelliğini tehlikeye atacaktır.

Üçüncü güvenlik sorunu olarak, güvenli ödeme yapma konusu karşımıza çıkar. Bu konuda en önemli önlemlerden biri; kredi kartı numarasının ve son geçerlilik tarihinin kullanıcı ve banka dışında hiç kimse tarafından ulaşılamaz olması gerektiğidir. Örneğin, bir tüccar mal satın almak için bankadan güvence alma ihtiyacı duyabilir, ama kredi kartı bilgileri tüccara mutlaka duyurulmamış olabilir. Benzer şekilde konuyla ilgili elektronik çekler ve elektronik nakit gibi daha birçok elektronik ödeme şekli bulunmaktadır.

Güvenlik servisiyle ilgili dördüncü ve son konu ise mesaj alıp gönderme konusunu içerir. Alıcı; bir mesajın gerçekten tanımlanan yaratıcı tarafından gönderildiğini, mesajın gönderici yolladığından beri değişmediğini kesinleştirmek ve ispat etmek zorundadır. Bu gereklilik alıcıyı ve göndericiyi birbirinden korur. Ağ güvenliği açısından bu servisler "nonrepudiation" ve

"data integrity" olarak adlandırılırlar. Nonrepudiation online bir işlem için şunları gerektirir; satın alan taraf gerçekten malları sipariş ettiğini ve satan taraf da gerçekten malları teslim ettiğini ispatlayacak belgeler bulundurmalıdır. Data integrity sisteminde ise, mesajın gönderici tarafından yollandığından beri değiştirilmediğini kesinleştirmek gerekir. Sonuç olarak, herhangi bir anlaşmazlığı veya mesuliyet iddialarını çözmek için uygun deliller ve gerekli prosedürler hazırda tutulmalıdır.

Bazı yazarlara göre güvenlik konusu göreceli bir kavramdır. Günlük yaşamda çekler ve kredi kartları sahtekarlık amacıyla çok fazla kullanılır hale gelmiştir. İş dünyasında firmalar kayıplarını azaltmak için tedbirler almışlardır, ama bunun için kullanışlı bir sistem yoktur. Elektronik ticaret konusunda, iş halledebilmek ve ödeme yapabilmek için güvenlik sistemlerinin geliştirilmesine önem gösterilmiştir, fakat yine de birtakım saldırılara maruz kalma ihtimali de söz konusudur.

1.3. İNTERNET ÜZERİNDEN TİCARET

İnternet üzerinden ticaret yapma işi satıcıların olduğu kadar, alıcıların da motivasyonuna bağlıdır. Öncelikle iş için internet üzerinde bir varlık oluşturmanın temel mantığını açıklayarak başlayacağız ve tüketicinin neden online alışveriş yapmak isteyeceğinin sebepleriyle devam edeceğiz. Aynı zamanda internet üzerinde ticareti yaymanın risklerinden ve bunu engelleyen durumlardan söz edeceğiz.

1.3.1. SATICILAR İÇİN FAYDALARI

1995 yılında yapılan tahminlerde; web kullanıcılarının üçte ikisinin tüketiciler, geriye kalanın üçte birlik kısmının ise şirketleşmiş ve akademik kullanıcılar olacağı iddia edilmiştir.

İnternet üzerinde iş konusunda bir varlık oluşturmak için birçok sebep vardır. Birinci ve en önemli sebep tüketicilere ulaşabilmektir. Daha önce de belirtildiği gibi, internet çok sayıda online tüketiciye erişim imkanı sunar.

İnternet üzerinde iş kurmak için ikinci bir neden olarak küreselleşmeyi söyleyebiliriz. İnternet yoluyla, bir firma hemen hemen tüm ülkelerdeki tüketicilere ulaşım kazanır. Özellikle bir dükkan açma veya birkaç ülkede reklam yapma alternatiflerini düşününce internet çok daha ucuz olacaktır.

İnternette iş kurmak için diğer bir sebep de satış maliyetinden tasarruf etmektir. Bir dükkanda veya mağazada bir işi kurup düzenlemek, fatura

ödemek, maaş veya çalışanların komisyonlarını ödemek için önemli miktarda para harcamak gerekirken; bunun yerine bu büyük giderlere nazaran küçük miktarda para ile internet üzerinde bir sayfa oluşturarak giderler azaltılabilir. Ayrıca bu tasarruflar ürünlerin maliyetini azaltabilir ve iş dünyasında onları daha rekabetçi yapabilir.

Son olarak, firmalar internet aracılığıyla kendi ticari ürünlerine ani güncellemeler sağlayabilirler. Firmalar kendi ana sayfalarına, online müşterilerin hemen ulaşabileceği şekilde güncellemeler ekleyebilirler. Bu güncellemeler özellikle ürün satışında ve kullanma süresi az kalan servislerin satışında çok kullanışlı olabilir. Örneğin, online güncellemeler Avrupa'ya gece uçağında boş kalan bir yer için bilet satışına ya da bir maç bileti satışına yarayabilir.

İnternet iş dünyasında pazarlama, hizmet ve satış işlemleri için kullanışlı olabilir. İnternet pazarlamacılığı, bir şirket hakkında bilgiye ulaşım sağladığı gibi, reklamcılığı da içerir. İnternet servisleri de şirketin durumu ve pozisyonu hakkında bilgi sağlayan veritabanına erişim sağlar. Son olarak internet - daha önce de bahsettiğimiz gibi - ticaret yapmak için çok kullanışlı bir satış noktası durumundadır.

1.3.2. TÜKETİCİLER İÇİN FAYDALARI

Firmalar internet üzerinde kendi sayfalarını kurdukça, gün geçtikçe daha da fazla tüketici çok çeşitli işler için internete bağlanacaktır. İnternet üzerinden ticaret yapmanın tüketiciler için en önemli faydası zamandan tasarruf sağlamasıdır.

Tüketiciler evlerinden kendi bilgisayarlarıyla internete bağlanarak ve firmaların ana sayfalarına girerek satıştaki ürünlere ve mağazalara kolaylıkla göz atabilirler. Buna alternatif olarak, bir tüketici gerçek dünyada mağazaları dolaşmak istese, sanal dünyada harcadığı zamandan ve enerjiden çok daha fazlasını harcamak zorunda kalacaktır

Bir tüketici için internet üzerinden alışveriş yapmanın sağladığı diğer bir yarar ise çok geniş bir ürün ve mağaza seçeneğine erişim kolaylığı sağlamasıdır. Örneğin, bir alışveriş merkezi giyim eşyası veya herhangi bir ürün üzerinde satış sağlayabilir, ama aynı zamanda araba satışı veya uçak bileti satışı hizmeti sunamayabilir.

Bir tüketici internet üzerinden herhangi biri ürünü kalite veya fiyat gibi özellikleriyle tüm mağazalardakilerle kolaylıkla kıyaslayabilir ve böylece

alışveriş yapmak bir zorunluluk değil bir zevk haline gelir. Sonuçta diyebiliriz ki; internet alışveriş yaparken karar vermeyi kolaylaştırmaya ve hızlandırmaya yardım eden bir araçtır.

1.3.3. ONLİNE BANKACILIK

Online bankacılık, kişisel bir bilgisayar kullanılarak bankacılık hizmetlerinin yapılması işlemidir. 1970'li yıllarda 7 gün 24 saat hizmet veren ATM'ler (Automatic Teller Machines) banka servislerine ucuz ve uygun bir erişim sağlama yolu olmuştur. ATM makinelerini kullanmak, banka şubelerinde veznedarla işlem yürütmekten çok daha ucuza mal olur, hızlıdır ve dolayısıyla çok daha kullanışlıdır. Ayrıca ATM sistemleri kullanan müşteriler bankada önemli bir vakti kaybetmemiş olurlar. ATM'ler müşteriler için kullanılabilirlik kazandırırken, bankalar için de işlem giderlerinin azalmasını sağlar.

Günümüzde ise bankacılık konusunda başka bir yenilik ile karşı karşıyayız.

Online bankacılık sistemleri bugün ATM sistemlerinden daha fazla bankacılık hizmeti vermeyi sağlamaktadır. Online bankacılık yoluyla müşteriler birikimlerine kolayca ulaşabilir ve hesaplarını veya kredi limitlerini kontrol edebilirler. Online bankacılığın kullanıcıya faydalarını şöyle sıralayabiliriz:

- Banka işlemini online yapmak zaman tasarrufu sağlar.
- Online bankacılık 7 gün 24 saat hizmet sunar.
- Belge ve kayıt saklamak için güvenli bir yoldur.

Online bankacılığın bankalar açısından faydaları ise şunlardır:

- Veznedarın bilgisayar üzerinden işlem yürütmesi giderlerin çok küçük bir parçasını içerir.
- Bankalara borsa işlemleri veya sigortacılık işlemleri gibi ek servisler sunmayı sağlar.
- Bankalara; müşteriler online olarak ürün satın alırken, onlara fon transferi sağlayarak online ticaretin bir parçası olma imkanı sunar.

Dört çeşit online ödeme modeli bulunmaktadır: Güvenilir üçüncü taraf sistemi, nakit fişi, elektronik çekler ve kredi kartları. Güvenilir üçüncü taraf sistemi, müşterinin hesap açtığı bir hizmet şirketini kullanır. Bu sistem müşterinin kredi kartı numarasına veya banka hesap numarasına ihtiyaç duyar. Böylece müşteri bir alışveriş yaptığı zaman, hizmet şirketi müşterinin

banka hesabından veya kredi kartından parayı transfer eder. Nakit fişi ise aynen nakit ödeme gibidir. Müşteri nakit ödeme ile nakit fişi edinir. Aynı zamanda bu fişi online ödeme yapmak için de kullanabilir. Elektronik çekler kağıt üzerindeki çeklere benzer şekilde kullanılır, fakat online sonuçlar vermesi ve sadece kullanıcı tarafından bilinen gizli şifreler kullanılması açısından farklılık gösterir. Kredi kartı ve son kullanma tarihi kullanılarak online alışveriş yapılabilir.

Online bankacılık; fatura ödeme işlemlerinde, fon transferinde ve hesap bilançosu bilgilerine ulaşmada çok elverişli yöntemler sağlar. Bunların yanında borsa işlemleri, ev veya araba mortgage kredileri ve konutsal öz sermaye kredisi gibi daha kompleks hizmetler de sunar.

Dijital ekonomiye giden yolda bazı engellerle de karşılaşabiliriz. Online bankacılık sistemi mevcut bankacılık sistemiyle beraberce çalışmak zorundadır. Federal bankacılık yönetmeliği online bankacılık projelerini değiştirmek zorundadır. Bunlara ek olarak bankacılık ve ticaret işlemlerinin hızlı bir şekilde gelişmesini bekleriz. Bankacılık sistemi de bu beklentileri karşılayabilmek için gerekli kapasiteye sahip olmalıdır.

1.3.4. e-TİCARET KONUSUNDA RİSKLER ve ENGELLEYİCİ FAKTÖRLER

Başarılı bir elektronik ticaret yapabilmek için iki tip risk veya engelleyici vardır. Bunlardan birincisi satışın ve karın olmaması, ikincisi ise bazı legal ve ağ güvenliği ile ilgili konulardır.

Ortalama bir Amerikan ailesinin yıllık geliri 42,400 dolar iken, internet erişimine sahip bir ailenin yıllık geliri 66,700 dolar civarındadır. Daha önce de belirtildiği gibi web kullanıcılarının üçte ikisi tüketiciler iken, üçte biri de akademik ve şirketleşmiş kullanıcılardır. Zaman geçtikçe bu istatistikler değişebilecek olmasına rağmen, iş dünyası internet aracılığıyla ulaşabileceği tüketicileri hedef almalıdır.

Online ticaretin azlığının ikinci bir nedeni ise bazı iş alanlarında internet üzerinden satış yapmanın, gerçek hayattaki kadar başarılı ve etkili olamaması olabilir. Online satış yapmak yerine gerçek mağazalarda satış yapmak daha kolay ve kazançlı olabilir. Bunun yanında ise internette reklam verilebilir.

İnternet üzerinden reklam vermek hem daha ucuz ve kolay hem de daha ilgi çekicidir. Ayrıca online satışta para transferi yaparken birçok güvenlik

sorunuyla karşı karşıya kalabiliriz. Bazen bir tüccar için ürünlerini en uygun ve etkili şekilde satabilme yolunu bulmak ve sürekli müşterilerinin devamlılığını sağlayabilmek birkaç yıl alabilir. Perakende satış yapan bayiler müşterilerine ürünlerin aktüelliğini, uygunluğunu, kullanım kolaylığını ve olabilecek düşük fiyatları göstermek zorundadır.

Son zamanlardaki göstergeler sadece tahmin olsa da eğilimler çok enteresan değişimler gösteriyor. Online ticaret yavaş olsa da, online bankacılık büyük sıçrayışlar yapıyor.

1.3.5. TEKNOLOJİ TRENDLERİ

İnternet ağ işletmesi ve bilgisayar kullanırlığı alanında en iyi yeniliklerin ilgisini çekiyor. İnternet tarayıcıları ve servisleri internet erişimine yenilikçi yollar kadar var olan bilgi kaynaklarına erişimi de içermenin peşinden koşmaya devam ediyor.

İlk yenilik dalgası, rehberlik ve güvenlik servisleri gibi lokal internet sistemleri için hazırlıkları içeriyor. Web rehberleri ve sunucularına güvenlik sağlamak için yeni protokoller geliştirildi. Bu gelişimler web üzerinden dokümanlara ulaşmak, doküman yayınlamak ve web dokümanlarına bağlantı yapmak gibi temel araçları da içermektedir. Diğer bir gelişme internet üzerinde yeni araştırma araçları, video akışı gibi yayıncılık araçlarını içeriyor. Her geçen gün yeni teknolojiler tanıtılıyor. Bazı enteresan internet teknolojileri şunları kapsar:

- İnteraktif Sarı Sayfalar
- Sanal Postane
- Elektronik Taciz
- İnternet Üzerinden Politika
- Sanal Gerçeklik
- Yeni Yayın Yaklaşımları
- Eş Zamanlı Haberler
- Televizyon Yayını
- 3 Boyutlu Resimler
- 3 Boyutlu Aktifler

İnternetin gelişmesinde bazı zor sosyal sorunlarla karşı karşıya kalınabilir. İnternet ahlakı ve pornografi sorunları acilen adreslenmelidir.

Bu yenilik trendi sürekli devam edecektir. Şimdiki sınırlar, geniş ölçekli öneriler ve elektronik ticaretin kullanımıdır. Yeni güvenlik teknolojilerinin

sürekliliği internet üzerinden yapılan birçok işlemi daha da çok yaygınlaştıracaktır (şu an internet üzerinde şifreli çok az mesaj vardır). Java gibi web üzerindeki uygulamalar için getirilen yeni programlama teknikleri devam edecektir.

İnternet üzerinde bizim için özelleştirilmiş paketler olacaktır. Bankacılık toplulukları evden bankacılık işlemlerini yapabilmek için önceden yüklenmiş bilgisayar yazılımlarıyla kendi ana terminallerini dağıtabilirler. Büyük bir bilgi devriminin tam ortasında bulunuyoruz.

1.3.6. GÜVENLİK İHLALLERİ

Bu bölümde, internet üzerinde güvenli ticareti sağlamak için gerekli, ağ ve internet güvenliğinin temelini oluşturan esasları tartışacağız.

Birçok örnekte görülüyor ki, internet özel ağlara illegal yollarla erişim sağlamak için bir ortam haline geliyor. Bir hacker, internette binlerce özel firma ile bilgi alışverişi yapabilme özelliğinden faydalanarak, özel bir ağa erişmenin gayri resmi yollarını bulabilir. Bundan başka, izni olmadan başkasının ağına giren kişi, internet üzerinden şifre çözebilir, bilgilerin üzerinde oynayarak verileri değiştirebilir, hatta veri akışına engel olup, durdurabilir.

İnternet güvenliği ihlalleri konusu çeşitli ve karmaşık bir konudur. Özel bir ağa izinsiz girmeye çalışan bir kişinin, bunu yapmak için çeşitli amaçları olabilir. Bu amaçlar finansal kazançlar sağlamak veya endüstriyel casusluk gibi çeşitlilik gösterebilir. Bir kere erişimi sağladıktan sonra, kullanıcıya çok çeşitli zararlar verilebilir ve bilgi, kaynak veya para çalınabilir. Bir ihlalin söz konusu olduğunu fark etmenin çeşitli yöntemleri ve belirtileri vardır. İnternet ağınızın saldırı altında olduğunu fark ettiğinizde, kötü etkiyi en aza indirmek için alınacak bazı tedbirler vardır. Güvenlik ihlaline karşı korunmasızlığı en aza indirmek ve yazılımınızı test edip korumak için çeşitli araçlar ve stratejiler bulunmaktadır. Bundan sonraki bölümlerde bu konular üzerinde konuşacağız.

1.3.7. GÜVENLİK İHLALİNDE AMAÇLAR

Ağ güvenliği ihlalinde en yaygın üç amaç şunlardır: Endüstriyel casusluk yapmak, finansal kazançlar sağlamak ve intikam almak veya propaganda yapmak.

1. Endüstriyel Casusluk

Endüstriyel casusluk; rekabetsel avantajları elde etmek için, endüstri alanındaki önemli sırları çalmak gibi konularla ilgilidir. Saldırgan, bir şirketin özel dosyalarına girer, şirket sırlarını araştırır ve bunları şirketin bir rakibine satar. Bununla beraber güvenliğin tehlike altında olduğunun fark edilmesini önlemek saldırgan için önemli bir amaçtır.

İnternet üzerinden iş ve ticaret yapma yaygınlaştıkça, endüstriyel casusluk konusu büyüyen bir sorun haline gelmiştir. Federal Bureau of Investigation (FBI - Federal Araştırma Bürosu), Amerikan şirketlerinin endüstriyel casusluk yüzünden yıllık 100 milyar dolar kaybettiğini kaydetmiştir.

Son araştırmalar gösteriyor ki, iş dünyası kendi bünyesindeki dürüst ve uyumlu olmayan çalışanları yüzünden önemli tehlikelerle karşı karşıya geliyor. Büyük şirketler için, anlayış ve etki testi oluşturan bir çalışmanın özeti yayınlandı. Hedef, bir endüstriyel casusluk saldırısı sonucu, parasal kaynaklara sınırlama getirilmesini taklit etmekti. Bununla birlikte, bu saldırı halk tarafından elde edilebilir bilgileri toplamak, şirkette geçici bir pozisyon elde ederek bunu kötüye kullanmak ve pozisyonu kötü temsil etmek, erişime zarar vermek, içsel ve dışsal bilgisayar korsanlığı yapmak gibi konuları da içeriyordu. Çıkan rapora göre bir gün içinde bir milyar doların üzerinde bilgi çalınmıştı.

Aynı zamanda Michigan Üniversitesi tarafından yapılan bir çalışmaya göre şirketlerdeki büyük kayıpların kaynağı büyük ölçüde içeride çalışanlardan biri.

Yine Trident Data Systems tarafından yayınlanan bir veriye göre sistem ağı kırma sorunlarının çoğu, iş yeri içinde oluşuyor.

Endüstriyel casusluk hakkında başka bir durum ise, hassas bilgileri edinmek için devletin ağlarına yapılan saldırılardır. Pentagon'un Bilgi Sistemleri Güvenliği Merkezi (Center for Information Systems Security - CISS) savunma ağlarına sızmak için yaptığı çalışmalara göre, hackerlar izinsiz erişim elde etmede %95 oranında başarılı olurken, bunların sadece %5'i saptanabilmekte ve %5'ten daha azı ihbar edilmektedir.

2. Finansal Kazançlar

Finansal kazanç sağlamak, ağ güvenliği ihlali konusunda diğer bir yaygın amaçtır. Saldırgan izinsiz bir erişim edinir ve para veya para sağlayacak

kaynaklar çalmaya başlar. Örneğin, dürüst olmayan bir çalışan, şirketin parasını kendi hesabına kolaylıkla transfer edebilir. Ya da işten çıkarılan bir işçi intikam almak amacıyla şirketten çıkmadan önce para çalabilir. Bir hacker, bir banka sistemine internet üzerinden izinsiz bir erişim sağlayabilir ve fon transferinde bulunabilir.

3. İntikam Alma veya Propaganda Yapma

Ağ güvenliği intikam alma veya hesaplaşma, reklam veya propaganda yapma isteğiyle delinebilir. Örneğin, işten atılmış bir işçi, arkasında bir saatli bomba bırakabilir. Ya da şirketin internet ağına zarar vermek için Trojan horse (Truva atı) denilen bir virüs bırakabilir. Bazen hackerlar yeteneklerini sergilemek ve kendi reklamlarını yapmak için ağlara zorla girerler. Bazı şirket veya acenteler, kendi ağ güvenliği ürünlerini kırmayı başaranlara ödüller veya iş teklif etmektedirler.

4. Tehlikeler

İnternet üzerinde oluşabilecek tehlikeler, izinsiz erişim, bilgi veya tüketimlerin ortaya çıkartılması, kaynakların yok edilmesi veya çalınması olarak tanımlanabilir. İnternet üzerinde olası tehlikelerin bazıları şunlarıdır:

- Yönetici Hataları
- Telefonları Gizlice Dinleme Olayları
- Virüsler
- Hackerler
- Ticari Rakipler
- Dürüst Olmayan Çalışanlar

1.3.8. SALDIRILARIN ÇEŞİTLERİ

İnternet güvenliği ihlalleri, aşağıdaki saldırı çeşitleri şeklinde bölümlere ayrılabilir.

1. Hizmet Engelleme

Hizmet engelleme (denial of service), ağ üzerindeki belirli amaçlar için tasarlanmış faaliyetlerin kaynaklarına erişimini engellemek anlamındadır. Hizmet engelleme, yetki dışı tahribatlara, değişimlere veya hizmetin gecikmesine sebep olma şeklinde olabilir. Bunlar kullanılabilir hafıza yetersizliğinden veya ağ üzerindeki kısmi kapanmalardan kaynaklanabilir. Hizmet engelleme saldırısı genellikle, kullanıcılara bir veya daha fazla iş

görmeyen bilgisayar bırakır. Bazı durumlarda ise, bütün ağ performansı şiddetli şekilde etkilenir. Hizmet engelleme saldırılarının ayrıntıları bilgisayar güvenliği teknik içerikli kitaplarda bulunabilir.

2. Dolandırıcılık

Dolandırıcılık amaçlı bir saldırıda, saldırgan illegal yollar kullanarak para çalar ve bir hesaptan başka bir hesaba para transfer eder. Bazen böyle bir saldırı, kullanıcı şifreleri tehlikeye atılarak başlatılır.

3. Mahremiyetin İhlali

Gizlilik (confidentiality), bilgilerimizin illegal yollarla açığa çıkarılmasını engelleyen bir korumadır. Mahremiyetin ihlali denilince gizli bilgilerin yetkisi olmayan şahıslar tarafından ortaya çıkarılması anlaşılır. Bu ihlal, bilgilerin şifrelenmesi ve şifre çözülmesi için kullanılan kriptografik şifreleri tahmin etme veya çalma yoluyla gerçekleştirilir. Bu şifreleri tahmin etmenin en yaygın yolu bir bütün-anahtarları-deneme (brute-force) saldırısı denilen bir metottur. Böyle bir saldırı da doğru şifre bulunana kadar muhtemel bütün anahtar kombinasyonlar denenir.

4. Kaynak Hırsızlığı

Kaynak hırsızlığı, yasa dışı kişilerin diğer şahısların bilgilerini transfer etmeleri veya bilgi kaynaklarına erişim sağlamaları şeklinde olur. Bu tür saldırılar, mahremiyetin ihlali veya kullanıcı şifrelerinin çalınmasıyla sonuçlanabilir. Çoğu endüstriyel casusluk faaliyetleri, yasa dışı yollarla kaynak hırsızlığı yapma amaçlıdır.

5. Her Anahtarı Deneme Saldırısı

Bütün-anahtarları-deneme saldırısında bütün olası şifreleri deneyebilen bir bilgisayar kullanılır. Bölüm 2'de anlatılan Data Encryption Standard (DES) şifreleme algoritması gibi bir algoritma düşünelim. DES bilgi şifreleme ve şifre çözme işlemi için 56-bit anahtarlar kullanır. Buna karşılık saldırganlar muhtemel 56-bit şifreleri deneyen bir program yazarlar. Program, sonuçta ortaya çıkan metin, orijinal metin ile eşleşene kadar 56-bit anahtarların her birine bunu uygular. Bu durumda bu saldırı programı en fazla 256 değerine karşılık gelen sayıda şifre deneyecektir.

Bütün-anahtarları-deneme saldırısı her zaman mümkündür. Bununla birlikte böyle bir saldırıya yakalanma ihtimalini azaltmak için alınabilecek tedbirler

vardır. Bütün-anahtarları-deneme saldırısı para ve zaman açısından çok pahalıya mal olabilir; bu da çok az kişinin bu saldırıyı gerçekleştirebileceği anlamına gelir. Ancak ileri bilgisayar teknikleri kullanılarak, böyle saldırıları yapmak gün geçtikçe daha kolay ve ucuz olmaktadır. Bu konuyu ayrıntılarıyla ele alan ve çeşitli plan ve projelere karşı başarılı bir bütün-anahtarları-deneme saldırısı gerçekleştirmenin ne kadar zaman alacağını hesaplayan teknik makaleler vardır.

6. Kripto Analiz

Kripto analiz, şifrelenmiş metinlerin şifreleri çözme ilmidir. Bu aynı zamanda, şifrelenmiş bir mesajdan bir anahtar kullanmadan şifresiz orijinal metni elde etme işlemidir. Kriptanalist ise kripto analizi yapan kişiye denir. Şifreleme ile ilgili beş çeşit saldırı vardır. Bunları etkili olma potansiyellerine göre şöyle sıralayabiliriz:

1. ***Sadece Şifreli Mesaj Saldırısı:*** Bu saldırıda kriptanalistin elinde birkaç şifreli metin vardır. Saldırının amacı olabildiğince çok şifresi çözülmüş metin ortaya çıkarmaktır. Bunun yanında, kriptanalist, aynı şifre ile şifrelenen diğer mesajların şifresini çözmek için bir şifreleme anahtarı belirlemelidir.
2. ***Bilinen Açık Mesaj Saldırısı:*** Kriptanalist, şifrelenmiş mesaja karşılık gelen çeşitli şifresiz mesajlara ulaşabilir. Burada kriptanalistin işi, aynı anahtar veya anahtarlarla şifrelenmiş mesajların şifresini çözmek için anahtar veya anahtarlar belirlemektir.
3. ***Seçilen Açık Mesaj Saldırısı:*** Bu saldırıda kriptanalist, seçilmiş bir şifresiz mesaj için şifreli bir metin elde edebilir. Bunun yanında, kriptanalist diğer şifresiz metinlere ve bunlara karşılık gelen şifreli mesajlara ulaşır. Bu saldırı bir öncekine göre çok daha güçlüdür. Çünkü kriptanalist kendi seçimiyle bir şifresiz metin oluşturur. Bu da anahtarı belirlemede daha çok bilgi edinmeyi sağlar.
4. ***Özel Seçilen Açık Mesaj Saldırısı:*** Bu saldırı bir öncekinden çok daha güçlü ve etkilidir. Burada kriptanalist, şifresiz metni her seferinde değiştirerek defalarca şifrelenmiş mesajı elde edebilir.
5. ***Seçilen Şifreli Mesaj Saldırısı:*** Bu saldırıda, kriptanalist çeşitli şifrelenmiş metinlerin şifrelerini çözebilir ve buna karşılık gelen metine ulaşabilir.

Kriptografinin temel ders kitaplarında kriptoloji sistemlerindeki zamanlama saldırılarının kullanılışını açıklanmıştır. Bu konunun temelinde kriptografik çalışmaların kullanılışı vardır.

7. Temel İhlaller

İnternet, kullanıcılar için kolay ve hemen hemen her yerde geniş alana yayılmış bağlanabilirlik sağladığı için hackerlar ve davetsiz misafirler için gözde hedeflerdir. Güvenlik ihlallerinin sayısı hızlı bir şekilde artmaktadır. Carnegie Mellon Üniversitesi Bilgisayar Olaylarına Müdahale Ekibi (CERTB, 1995) her gün yaklaşık 3 yeni bilgisayar güvenliği vakasıyla karşılaştıklarını belirtiyor. Birçok güvenlik ihlali duyurulmuştur ve ağ ilgililerinin dikkatini çekmiştir. Bunun yanında gözden kaçanlar da olmuştur. Devam eden süreçte geçen birkaç yıl içinde gerçekleşen önemli güvenlik ihlallerini anlatacağız. Aşağıda da belirtildiği gibi, son birkaç yılda temel internet güvenliği saldırılarının sayısı artmıştır.

1. Yıl, Konu: 1988, Internet Solucanı
   Açıklama: Çok sayıda internet sunucusunu etkiledi.

2. Yıl, Konu: 1989, Hacker in "Cuckoo's Egg"
   Açıklama: Doğu Alman ajanları ABD savunma alanına girdiler ve Cliff Stoll tarafından yakalandılar.

3. Yıl, Konu: 1993, New York City İhlali
   Açıklama: Bilgisayar korsanları oturum açma aktivitelerini engellediler ve kullanıcı bilgilerini çaldılar.

4. Yıl, Konu: 1995, Kaynak Adres Saldırısı
   Açıklama: Hizmet engelleme atağı kaynak adresini yanıltmak için Spoofing kullanıldı.

5. Yıl, Konu: 1995, Banka Dolandırıcılığı
   Açıklama: Citibank'tan 10 milyar dolar çalındı ve çalınan paranın büyük kısmı geri alındı.

6. Yıl, Konu: 1996, ABD Hükümetine Saldırı
   Açıklama: ABD hükümeti tarafından, internet üzerinden konuşma hükümet ağ dinleme aleti saptandı.

7. Yıl, Konu: 1996, Word Macro Virus
   Açıklama: Hizmet engelleme atağıyla çeşitli virüsler yayıldı.

8. Yıl, Konu: 1998, Internet Solucanı
   Açıklama: 2 Kasım 1998'de internet en kötü saldırılardan biriyle karşılaştı. İnternet solucanı (İnternet Worm) olarak adlandırılan bu saldırı sonucu, internet aracılığıyla birkaç saat içinde kendi kendini kopya eden bir virüs

yayıldı. Kimilerine göre bu virüsten 7000'den fazla sunucu etkilendi. Birçok sunucu kapandı ve birçoğu da büyük zarara uğradı. Bu solucan Robert T. Morris tarafından oluşturuldu. Morris şu üç uygulamadaki zayıf noktaları kullandı: Fingerd, Rhost ve Sendmail. Ocak 1990'daki denemesinde, amacının kötü niyetli bir şey olmadığını ve internetteki zayıf noktaları göstermek olduğunu kanıtladı. İnternet solucanı gün geçtikçe ün kazandı ve internet güvenliği konusundaki bilincin artmasına sebep oldu.

9. Yıl, Konu: 1989, Hacker in "Cuckoo's Egg"
Açıklama: Aslında bir astronot olan Cliff Stoll sistem yöneticisi olarak çalışıyordu ve 75 centlerdeki hatanın izini sürüyordu. Bu süreçte, Doğu Almanya'dan bir davetsiz misafirin ABD hükümet bilgisayarlarına girmeye teşebbüs ettiğini saptadı. Stoll bir süre onu takip etti. 10 ay gibi bir süre boyunca, bilgisayar korsanı yaklaşık 450 bilgisayara saldırdı bunlardan 35 tanesine girmeyi başardı.

   Saldırgan, saldırıyı saklamak için çeşitli giriş noktaları kullandığından neredeyse bir uzman gibi görünüyordu. Aynı zamanda saldırgan kullanıcı şifreleri gibi ince bilgilerle de ilgileniyordu. Stoll bu saldırıyı, "The Cuckoo's Egg" adlı kendi kitabında ayrıntılı bir şekilde açıklamıştır. Onun bu hackerı ortaya çıkarması, hem birçok hükümetin hem de birçok ajansın soruşturması ile sonuçlanmıştır.

10. Yıl, Konu: 1993, New York Şehri Saldırısı
Açıklama: Ocak 1993'de, genel bir internet erişim sistemi, birinin kullanıcı kimliklerini ve şifrelerini çaldığını bildirdi. Bu yüzden birçok sitenin güvenliği de tehlikeye düşmüş oldu. Hacker, SENDMAIL programındaki zayıf noktaları kullanarak kullanıcı kimliklerini ve şifrelerini kaydetmiştir. Bu saldırı, SENDMAIL programının internet worm saldırısında faydalanılan zayıf noktalarından farklı bir zayıf noktasından yararlanılmıştır. Bu saldırı, bir hata sonucu hackerın dosyasına girilmesi sonucu ortaya çıkmıştır.

11. Yıl, Konu: 1995, Kaynak Adres Yanıltma Adresi
Açıklama: Bu saldırı 23 Ocak 1995 yılında CERT tarafından yapılan bir uyarı sonucu ortaya çıktı. Bu saldırı TCP/IP sunucusunda oluşan bir hatadan faydalanılarak yapılmıştır. Böyle saldırılar, kullanıcıların IP adreslerini doğrulama için kullanılan programları etkiler. Bu saldırı engelleyici güvenlik duvarını aşmıştır. Bu saldırıdan, San Diego Center for Supercomputing ve Standford Linear Accelerator Computing Center da dahil olmak üzere en az 50 sunucu etkilenmiştir.

Böyle saldırılardan korunmak için bazı önlemler vardır. Açıkçası, her sunucudan yazılım programlarını değiştirmelerini istemek çok zordur. Bununla birlikte, güvenlik duvarı yapılandırması bu tip saldırılara karşı dirençli bir şekilde ayarlanmalıdır, çünkü bu gibi durumların çoğunda, saldırgan özel ağın içinden birinin, örneğin ağ yöneticisinin yerine geçer. Zaten genellikle ağ kaynaklarının ağ yöneticisi veya bir çalışan tarafından kontrol edildiğini unutmayalım.

12. Yıl, Konu: 1995, Banka Dolandırıcılığı
Açıklama: 17 Ağustos 1995'de Vladimir Levin adlı şahıs, Amerikan savcıları tarafından, Citibank'tan 40'tan fazla kere para sızdırmak ve 10 milyon dolardan fazla parayı başka banka hesaplarına aktarmak suçundan soruşturmaya alındı. Amerikan savcıları Londra mahkemelerinden suçluyu ülkesine iade edilmesini istedi. Bu durumda hedef, Citibank'ın Manhatten'daki fon transfer sistemiydi. Diğer dört şüpheli suç ortağı da tutuklandı. Hemen hemen 400 bin dolar tazmin edildi. Bu saldırı ayrıntılarıyla Caldwell (1995)'de anlatılmıştır.

13. Yıl, Konu: 1996, ABD Ordu Bilgisayarlarına Girme
Açıklama: 30 Mart 1996'da, Amerikan gazeteleri, federal ajansın internet üzerinden bir wiretap aracılığıyla bir bilgisayar korsanın izlerini takip ederek yakaladığını yazdı. Julio Cesar Ardita adındaki hacker 22 yaşında, Arjantin'de yaşayan bir bilgisayar bilimleri öğrencisiydi. Arjantin'de de yasadışı bilgisayar girişimlerinde bulunduğu ortaya çıkmıştı. Gazete haberine göre, Ardita önce Harvard Üniversitesi, Fen-Edebiyat Fakültesi bilgisayarlarına girdi. Bu kaçak girişler, 12 Temmuz-28 Aralık 1995 tarihleri arasında gerçekleşti. Ardita, 16500 yasal kullanıcılardan bazılarının şifrelerini çalmış ve ABD ordu bilgisayarlarına girmek için Harvard bilgisayarlarını bir ortam olarak kullanmıştır. Böylece, önemli gizli devlet bilgilerine erişim sağlamıştır, fakat milli güvenlik dosyalarına dokunmamıştır. 1995 yılı Kasım/Aralık ayları boyunca, Harvard bilgisayarlarına mahkeme emriyle bir wiretap yerleştirilmiştir. Bu olay bilgisayarla ilgili suç işleyen birinin izini sürüp yakalamak için mahkeme emriyle wiretap kullanılmasının ilk örneğidir.

14. Yıl, Konu: 1996, Word Macro Virüsü
Açıklama: Word Macro virüsü, hem MAC hem de Windows'un tüm versiyonlarındaki Microsoft WordBasic'te yazılan "auto-executing macros" yoluyla yayılmıştır. Consept virüs (winword.consept) çıktı alma ve büyük Word dosyalarını kaydetme fonksiyonlarını etkilemiştir. Diğer bir Word Macro virüsü olan hot virus, Word dokümanları açıldığı anda onları siliyordu. Colors virus denilen virüs Windows'taki rasgele seçilen

renklerin renk ayarlarını değiştiriyordu. Format C virus, hard drives üzerindeki dosyaları siliyordu ve atom virüs ise 13 Aralık'taki güncel rehberin dosyalarını siliyordu. Bu virüsler, Microsoft Word 2.0 veya Windows 3.1, Windows 95, Windows NT de çalışan dokümanlara ve MAC işletim sistemlerine bulaşmıştır. Antivirüs firmaları Word Macro virüsü temizlemek için ürünler tasarlamıştır.

Ulusal Bilgisayar Güvenliği Birliği (NCSA), Kuzey Amerika'daki 300 büyük firmanın katıldığı bir araştırma yapmıştır. Bu firmaların %50'si macro virüs saldırısında zarar görmüş olduğunu beyan etmiştir.

15. Banka Soygunu
1984 yılında bir bankanın şube müdürü, hesap kontrolünü engelleyen bir bilgisayar sistemi kurarak 25 milyon dolar para transferi yapmıştır.

16. Onüçüncü Cuma Virüsü (Friday the 13th Virus)
1988 yılında Kudüs'deki Hebrew Üniversitesi'nin binlerce öğrencisinin 13. Cuma Virüsü adı verilen bir virüsten etkilendiği ortaya çıktı. 13 Mayıs 1988'de ortaya çıkan bu virüs, finans, araştırma ve yönetim bilgisayarlarının harddisklerini silmek için programlanmıştır. Bu virüs İngiltere'de tekrar ortaya çıktı ve aylarca yapılan çalışmaları sildi. Daha sonra Amerika'da görüldü.

17. Beyaz Saray Bilgisayarları
Bir araştırmacı İran karşıtı ilişkiler konusu üzerinde çalışırken Oliver North tarafından kullanılan bir bilgisayar keşfetti. Bununla birlikte Beyaz Saray bilgisayarlarından silinen bazı önemli notlar ve bilgiler buldu. Sonuçta bu bilgi ana bilgisayar kullanıcıları tarafından erişilebilirdir. Bu olay 1988 yılında meydana gelmiştir ve Beyaz Saray bilgisayar sisteminin güvenliği konusunda şüpheleri artırmıştır.

18. Havayolu Sistemi
Büyük bir seyahat acentesi, rezervasyon ve bilet kesme sistemine gizlice girildiğini fark etti ve birilerinin illegal bir şekilde uçak biletlerini basmış olduğunu gördüler. Bu olay 1988 yılında gerçekleşti. Bir terörist organizasyon tarafından rezervasyon sistemine girildiği ve saldırı planlamak için kullanıcı bilgilerinin elde edildiği düşüncesi belirdi.

19. Uydu Konumlandırma Sistemi
1989 yılında bir Kansas Üniversitesi öğrencisi hava kuvvetleri uydusunun konumlandırma sistemine gizlice girdi. 14 yaşındaki öğrenci bir Apple bilgisayar kullanarak, Hava Kuvvetleri Sistemi'ne giriş yapmak

için, yasadışı uzun mesafeli ulaşım kodlarını çevirmiştir. Öğrenci erişim sağladıktan sonra 200den fazla işle ilgili gizli dosyaya giriş yapmıştır.

20. 20. NASA Bilgisayarları
1990 yılında, Norfolk Virginia da bir NASA bilgisayarı 24 saat boyunca kapatıldı. Bunu kendine Phoenix diyen Avusturyalı bir öğrenci yaptı. Görünüşe göre bu öğrenci birçok Avusturya ve Amerika bilgisayarına sızmış ve California'daki Lawrence Livermore Laboratuvarı bilgisayarlarında bilgileri değiştirmiştir.

Tüm bunların dışında, burada anlatılmayan birçok güvenlik ihlali olayı yaşanmıştır.

1.3.9. BİLGİSAYAR GÜVENLİĞİ

1. Bilgisayar Güvenliği Nedir?

Bilgisayar güvenliği, bilgisayarınıza yapılabilecek izinsiz girişleri ortaya çıkarma ve bilgisayarınızı koruma işlemleridir. Bu işlemler, "intruder-davetsiz misafir" olarak bilinen yetkisiz kullanıcıların bilgisayar sisteminizin bir parçasına ulaşmalarını engellemeye yardımcı olur. Ayrıca, birisinin sisteminize girip girmediğini, eğer zorla girilmişse neler yaptığını ortaya çıkartır.

2. Bilgisayar Güvenliği Konusunda Niçin Dikkatli Olmalıyız?

Bilgisayarı hemen hemen her şey için kullanıyoruz. Örneğin, bankacılık işlemleri için, alışveriş yapmak için, e-posta veya chat programları ile iletişim kurmak için. E-postalarınızın çok gizli olduğunu düşünmeseniz de büyük ihtimalle onların yabancılar tarafından okunmasını istemezsiniz. Ya da sizin bilgisayarınız kullanılarak diğer insanların bilgisayarlarına saldırılmasını, onlara bilgisayarınızdan sahte e-postalar yollanmasını, bilgisayarınızda saklı olan kişisel bilgilerinizin incelenmesini istemezsiniz.

3. Bilgisayarımıza Kim Zorla Girmek İsteyebilir?

Intruders-işgalciler, hackerler, sistem kırıcılar veya saldırganlar olarak tanımlanan bilgisayarınıza zorla giren kişiler sizin kimliğinizle ilgilenmeyebilirler. Genellikle sizin bilgisayarınızın kontrolünü ele geçirerek diğer bilgisayar sistemlerine saldırılarını yaymayı amaçlarlar. Bilgisayarınızın kontrolünü ele geçirmek, devlet sistemi veya finansal sistemler gibi yüksek profilli bilgisayar sistemlerine saldırılarını yayarken onların gerçek konumlarını saklama avantajı sağlar. Örneğin, internete bağlı bir bilgisayarla

oyun oynuyor olsanız veya bir arkadaşınıza e-posta gönderiyor olsanız bile bilgisayarınız hedefte olabilir. Sistem kırıcılar sizin bilgisayardaki tüm hareketlerinizi izliyor olabilirler. Veya bilgilerinizi değiştirerek veya bilgisayarınızı tekrar formatlayarak sisteminize zarar veriyor olabilirler.

4. Bilgisayarımıza Zorla Girilmesi Ne Kadar Kolaydır?

Maalesef hackerler bilgisayar sistemine girmek için her geçen gün yeni savunmasız noktalar boşluklar ve yeni yöntemler buluyorlar. Yazılımın karmaşıklığı bilgisayar sisteminin güvenliğini tamamen test etmeyi daha da zorlaştırıyor.

Sistemdeki bu boşluklar keşfedildiğinde, bilgisayar satıcıları bu problemlere yönelik çözümler üretirler. Aslında yeni güvenlik ve onarım programları elde edip yüklemek yada yazılımın daha güvenli bir şekilde çalışmasını sağlamak için yeni yapılandırmalar yapmak daha çok kullanıcıya bağlıdır. Ayrıca bazı yazılım uygulamalarında, siz daha güvenli olması için ayarlarınızı değiştirmeseniz de diğer kullanıcıların sizin bilgisayarınıza ulaşmasını sağlayan ayarlar vardır. Örneğin, yabancıların sizin bilgisayarınız üzerinden yorum yapmasına izin veren chat programları aracılığıyla üzerine tıkladığınız zaman sisteminize zarar verecek programlar koyabilirler.

1.3.10. TEKNOLOJİ

Bu bölümde internetin temelini oluşturan teknolojiler hakkında bazı tanıtımlar yapılacaktır.

1. Geniş Bant Nedir?

Geniş Bant (Broadband), yüksek hızlı ağ bağlantısını tanımlamak için kullanılan genel bir terimdir. Bu bağlamda kablolu modem veya DSL (Digital Subscriber Line) yoluyla olan internet bağlantıları, genellikle broadband (geniş bantlı) internet bağlantılarını ima etmektedir. Örneğin, birçok çevirmeli modemler saniyede 56 bin bit bant genişliğini destekleyebilir.

2. Kablolu Modem Bağlantısı Nedir?

Kablolu bir modem, tek bir bilgisayarı ya da bilgisayar ağını kablolu TV ağıyla internete bağlamaya yarayan bir araçtır. Kablolu bir modem bilgisayara genellikle bir Ethernet LAN (Local Area Network - Yakın Bölge Ağı) bağlantısına sahiptir ve saniyede 5 milyon bit hızına ulaşabilir.

3. DSL Bağlantısı Nedir?

DSL internet bağlantısı, kablolu modem tabanlı servislerin aksine sadece bir müşteri için ayrılmış bant genişliği ile hizmet sunar, ama DSL kullanıcıları için kullanılabilir maksimum bant uzunluğu, kullanıcıların kişisel ağ teknolojilerindeki farklılıklardan dolayı kablolu modemlerin maksimum oranından daha azdır. Aynı zamanda, sadece bir müşteri için ayrılmış bant genişliği (dedicated bandwith) sadece evinizle DSL sunucunuzun merkez ofisi arasında hizmet verir. Bununla birlikte DSL sunucu, bilgisayarlar arasında veri paketlerinin dinlenmesi konusunda kablolu modem kadar hassas değildir.

4. Geniş Bant Servisi Geleneksel Çevirmeli Ağlardan Nasıl Farklılık Gösterir?

Geleneksel çevirmeli internet servisleri (dial-up) bazen sadece ihtiyaç duyulduğunda kullanılan (dial-on-demand) servisler olarak adlandırılır. Bu, bilgisayarınızın sadece bir e-posta göndermek istediğinizde ya da bir web sayfasını yüklemek için istek gönderdiğinizde internete bağlandığı anlamına gelir. Bu durumda gönderilecek bir veri yoksa ya da bir müddet bilgisayarda çalışılmamışsa bilgisayar bağlantıyı keser.

Geniş bant servisi ise her zaman açık ve kullanımda olan anlamında kullanılır, çünkü bilgisayardan bir şey göndermek istediğimizde herhangi bir çağrı oluşturmamıza gerek yoktur. Bilgisayar her zaman ağa bağlıdır ve ağ arabirim kartı (NIC) aracılığı ile her zaman veri göndermek ve almak için hazırdır. Bağlantınız her zaman var olduğundan IP adresiniz çok sık değişmeyecektir ve bu da onu saldırılar için sabit bir nokta haline getirecektir.

Bunlara ek olarak, birçok geniş bant sistemi bireysel kullanımlar için belirli IP adresleri kullanımı sağlar. Bu durumda, bir saldırgan size ait olan belirli bir bilgisayarı seçmiş olmadığı halde sizin geniş bant servis kullanıcılarından biri olduğunuzu ve belli bir IP adresini kullandığınızı bilir. Bu sebeple bu durum sizin bilgisayarınızı diğerlerinden daha belirgin bir hedef haline getirir.

Aşağıdaki tablo geleneksel çevirmeli sistemlerle geniş bant sisteminin karşılaştırmasını göstermektedir.

	Çevirmeli	Genişbant
Bağlantı tipi	İsteğe bağlı bağlantı	Her zaman bağlı
IP adresi	Her çağrı da değişir	Sabit veya nadiren değişir
Rölatif bağlantı hızı	Düşük	Yüksek
Uzaktan kontrol potansiyeli	Uzaktan kontrol için bilgisayar bağı olmalı	Bilgisayar her zaman bağlı olduğundan uzaktan kontrol her zaman yapılabilir.
Sağlanan güvenlik	Çok az ya da hiç yok	Çok az ya da hiç yok

5. Geniş Bant Sistemi İşte Kullandığımız Ağdan Nasıl bir Farklılık Gösterir?

Şirket ve hükümete ait ağlar genellikle ağ güvenli duvarları veya şifreleme gibi birçok tipik güvenlik işlemleriyle korunurlar. Ayrıca ağ bağlantısının her zaman kullanılabilirliği ve güvenliğini sağlamak için bir destek kadrosu bulundururlar.

Her ne kadar internet servisi sağlayıcınız servisinizin muhafaza edilmesini sağlamakla görevli olsa da büyük ihtimalle evinizde bu işle görevli çalışanlarınız bulunmamaktadır. Eninde sonunda siz kendi bilgisayarınızdan sorumlusunuz. Sonuçta bilgisayarınızı kötü kullanımlardan veya her türlü kazadan korumak için makul önlemler almak tamamen size bağlıdır.

6. Protokol Nedir?

Protokol, bilgisayarların ağ içinde iletişim kurmasını sağlayan iyi tanımlanmış bir şartnamedir. Bir bakıma, protokoller bilgisayarların birbiriyle konuşabilmesi için gerekli gramer olarak tanımlanabilir.

7. IP Nedir?

"IP" internet protokolü anlamına gelmektedir. IP internet kullanılan bilgisayarların en yaygın dili olarak bilinir. IP'nin birçok yerde birkaç detaylı açıklaması vardır. IP'nin bilgisayarınızı nasıl koruduğunu anlamak için IP hakkında birkaç şey bilmek önemlidir. Şimdi IP adresi, statik ve dinamik adresleme, NAT, TCP ve UDP portlarından bahsedelim.

8. IP Adresi nedir?

IP adresleri telefon numaralarına benzer. Nasıl ki bir kişiyi aramak için öncelikle kişinin telefon numarasını bilmek gerekirse, benzer şekilde bir bilgisayardan diğerine veri göndermek için onun IP adresi bilinmelidir. IP adresleri nokta ile birbirinden ayrılmış dört sayıdan oluşur. Örneğin, 10.24.254.3 ve 192.168.62.231 IP adresleridir.

Eğer bir kişiyi aramak istiyorsanız ve elinizde sadece kişinin ismi var ise, kişinin ismiyle telefon numarasını telefon rehberinden bulabilirsiniz. İnternette bu rehber Alan İsimlendirme Sistemi olarak isimlendirilen DNS (Domain Name System) olarak bilinir. Eğer internet kullanıcısının adını biliyorsanız, örneğin web tarayıcınıza, www.cert.org yazarsanız bilgisayarınız bu isimle ilişkili nümerik IP adresini bulmak için DNS servisine yönlenecektir.

İnternete bağlı her bilgisayar kendisiyle özdeşleşen bir IP adresine sahiptir, ama bu adres zamanla değişebilir, özellikle bilgisayar:

- İnternet servisi sağlayıcısına (ISP) bağlanıyorsa
- Bir güvenli duvarı arkasından bağlantı yapılıyorsa,
- Dinamik IP adresleme kullanılarak geniş bant servisi ile bağlantı yapılıyorsa.

9. Statik ve Dinamik Adresleme Nedir?

Statik adresleme, internet servisi sağlayıcısının her kullanıcı için bir veya daha fazla kalıcı IP adresi belirlemesiyle meydana gelir. Bu adresler zaman içinde değişmez, ama belirlenmiş bir IP adresi kullanılmıyorsa bu adres kullanılmış sayılır.

Dinamik adresleme kullanıldığında bireysel kullanıcı bilgisayarlarının IP adresleri zamanla değişebilir. Bir dinamik adres kullanılmıyorsa, bu adres otomatik olarak ihtiyacı olan başka bir bilgisayara atanır.

1.3.11. KULLANICILAR İÇİN BİLGİSAYAR GÜVENLİĞİ RİSKLERİ

1. Risk Nedir?

Bilgi güvenliği 3 temel alanla ilgilenir:

- Gizlilik - Bilgi sadece yasal olarak hak sahibi olanlar tarafından ulaşılabilir olmalıdır.

- Güvenilirlik - Bilgi sadece yasal olarak yetkili olanlar tarafından değiştirilebilir olmalıdır.
- Kullanılırlık - Bilgi ihtiyacı olanların ihtiyacı olduğu zaman ulaşılabilir olmalıdır.

Büyük ihtimalle hiç kimse önemli dokümanlarına yabancıların bakmasına izin vermek istemez. Benzer şekilde hazırlamış olduğumuz ödev ve işleri güvenli bir şekilde saklı tutmak isteriz. Aynı zamanda, bilgisayarımıza sakladığımız bilgilerin el sürülmemiş bir şekilde tutulmasını ve istediğimiz zaman kolaylıkla ulaşılabilmenin garanti altına alınmasını isteriz.

Bazı güvenlik riskleri, saldırganların internet yoluyla bilgisayarınızı kasti olarak kötüye kullanma ihtimalinden ortaya çıkar. Diğer bazı riskler ise siz internete bağlı olmasanız bile karşılaşabileceğiniz durumlar olabilir (hard disk bozuklukları, hırsızlık veya güç kesilmeleri vb.). Burada kötü olan muhtemel her risk için önlem almanın neredeyse imkansız oluşu. İyi olan ise, karşılaşabileceğiniz en yaygın tehlikelerin etkilerini azaltmak için bazı aşamalar vardır ve bu aşamalar size karşılaşabileceğiniz olası kasıtlı veya kazara olan risklerden koruyacaktır.

Bilgisayarınızı ve internet ağınızı korumak için alınabilecek bazı tedbirlerle ilgili tavsiyeler şunlardır:

- Eğer evden çalışıyorsanız, sistem destek çalışanlarınıza güvenlik için danışın.
- Virüs koruma programları kullanın.
- Firewall (güvenlik duvarı) kullanın.
- Bilmediğiniz e-posta eklentilerini açmayın.
- Kaynağını bilmediğiniz programları çalıştırmayın.
- İsmi gizli dosya uzantılarını devre dışı bırakın.
- İşletim sisteminiz de dahil olmak üzere tüm uygulamalarınızın yamalarını (patch) yükleyin.
- Kullanmadığınız zaman bilgisayarınızı ve internet bağlantınızı kapatın.
- Mümkünse Java, JavaScript ve ActiveX programlarını devre dışı bırakın.
- E-posta programları içindeki komut dizisi oluşturma özelliğini devre dışı bırakın.
- Önemli verilerin yedek kopyasını bulundurun.
- Bilgisayarınızın tehlikeye düşme durumunda işletim sistemini yeniden yüklemek için bir disk bulundurun.

1.4. ELEKTRONİK TİCARETE BAŞLAMAK İSTİYORSANIZ

Bilindiği gibi "ticaret" ifadesi kavramsal olarak "mal veya hizmetin satın alınması ve satılması" işlemlerini kapsamaktadır. Bu sürecin elektronik ortamda, internet üzerinde yapılması e-ticaret kavramını ortaya çıkarmıştır.

e-Ticaretin tanımı konusunda farklı ülkelerin kuruluşları tarafından farklı tanımlar ortaya konmaktadır. Ancak e-ticaret konusunda en yaygın genel kabul görmüş tanım OECD tarafından 1997'de yapılan tanımdır. Bu çerçevede e-ticaret aşağıdaki eylemleri kapsayan bir süreç olarak tanımlanmaktadır:

Ticaret öncesi firmaların elektronik ortamda bilgilenmesi ve araştırma yürütmesi, firmaların elektronik ortamda buluşması, ödeme sürecinin yerine getirilmesi, taahhüdün yerine getirilmesi, mal veya hizmetin müşteriye teslimi, satış sonrası bakım, destek, vb. hizmetlerin temin edilmesi.

İlk olarak elektronik ticarete başlamak için gerekli olan en basit ve ana ihtiyaçlardan bahsedersek: internet erişimi bu işlemin olmazsa olmazıdır. Diğer bir basit ihtiyaç ise satışa sunulacak ürünleri web üzerinden müşteriye tanıtmak için kaliteli bir fotoğraf makinesi olmalıdır. Bunların dışında ise web sitesi, güvenlik, bankalarla anlaşma, kargo ile anlaşma, hukuki maddeler vs. gibi teferruatlı işlemleri vardır.

1.4.1. e-TİCARET GÜVENLİĞİ

İnternet üzerinde elektronik ticaret işlemi şöyle gerçekleşir: İnternet üzerinde mal ve hizmet satın alınması sırasında, bilgisayar kullanıcıları Windows Explorer veya Netscape gibi yazılımları kullanmak suretiyle siparişlerini ve kredi kartı bilgilerini internet ortamına aktarırlar. Bu bilgiler güvenli bir şekilde Internet üzerinden satıcının bilgisayarına ulaşır. Satıcının bilgisayarı tarafından sipariş bilgileri işleme tabi tutulurken müşteriye ait kredi kartı bilgileri şifrelendikten sonra kredi kartının ait olduğu bankaya veya kuruma güvenli bir biçimde transfer edilir. Banka veya söz konusu kurum tarafından kredi kartı bilgilerinin şifresi çözülür ve sona satıcının bilgisayarına gerekli provizyon gönderilir. Aslında bu işlemler birçok yönden alışılmış olarak yapılan kredi kartlı alışverişlere çok benzemektedir.

1. Elektronik Ticaret İşlemleri

- Kredi kartı bilgileri şifre korumalı bir yazılımla bankaya aktarılır.
  Güvenli

- Bilgiler internet üzerinden gizli şekilde bankaya aktarılır.
  Güvenli
- Satıcı kredi kartı bilgileri hariç sipariş bilgilerinin şifresini çözer.
  Güvenli
- Kredi kartı bilgileri bankaya gönderilir.
  Güvenli
- Banka provizyon verir.
  Güvenli
- Satıcının bilgisayarı satış işlemini internet üzerinden sonuçlandırır.
  Güvenli

1.4.2. KREDİ KARTLARI BİLGİLERİNİN ŞİFRELENMESİ

Kredi kartına ait bilgiler İnternet Explorer veya Netscape gibi İnternet Browser'ları aracılığıyla şifrelenir ve provizyon aramak üzere satıcının bilgisayarına internet ortamında aktarılır. Satıcının bilgisayarı kredi kartı bilgilerinin şifresinin nasıl çözüleceğini bilmez; bu işlemi ancak bankalar gerçekleştirebilir. Bu durum kredi kartı sahiplerinin kredi kartlarına ait bilgilerinin güven içinde kalmasını sağlar. Bu bilgileri satıcı okuyamadığı için güvenlik sağlanmaktadır. Aslında bu haliyle internet üzerinden elektronik ticaret alışılmış yöntemde kredi kartlı alışverişlerden daha güvenlidir.

1. Şifreleme Teknolojileri

SSL (Secure Sockets Layer) (Güvenli Yuva Katmanı) bir çok internet browser (Windows Explorer, Netscape, Firefox) tarafından tamamen desteklenen bir şifreleme protokolüdür. Provizyon işlemlerinin gerçekleştirilmesinde, güçlü bir şifreleme olanağı sunması ve güvenli bir transfer gerçekleştirebilmesi sayesinde internet ortamında bilgi alışverişi güvenliğini üst düzeyde sağlanmaktadır. Birçok internet sitesi kredi kartı işlemleri için SSL protokolünü uygulamaktadır. SET, internet siteleri tarafından kullanılmaya başlanan yeni bir şifreleme protokolüdür. Visa ve Mastercard tarafından oluşturulan konsorsiyum tarafından geliştirilen bu yöntem internet üzerinde kredi kartlı işlemlerin gerçekleştirilmesinde kullanılan yeni bir standarttır. Kredi kartı kullanıcıları, satıcılar ve bankalar için tasarlanan SET elektronik ticarette, internet üzerinde güvenli bilgi aktarımını sağlamak amacıyla aralarında VISA, MasterCard ve IBM'in de olduğu kuruluşlar tarafından geliştirilen bir protokoldür. SET, özellikle on-line (gerçek zamanda) kredi kartı bilgileri iletimi için geliştirilmiş bir standarttır. SET, kredi kartı ile yapılan online ödemelerde, bilgilerin internet üzerinden

aktarımında gizlilik ve güvenlik entegrasyonunu sağlar. SET protokolü sadece müşteri (ürün siparişi veren kredi kartı sahibi) ile sanal dükkan (e-dükkan) ve kredi kartı şirketi arasındaki ödeme fazını şifreler. Bu protokol bilgisayar kullanıcılarının kimliklerini belirlemek için dijital sertifikalar kullanılmaktadır. Dijital sertifikalar bilgisayar kullanıcılarının kimlik kartları gibi işlem görür. SET ayrıca kredi kartı bilgileri ile birlikte sipariş bilgilerini de şifreler ve internet ortamına aktarır. İnternet üzerinde elektronik ticaret geliştiren birçok yazılım mevcuttur. Bu yazılımlar kredi kartı bilgilerini ve sipariş bilgilerini şifreledikten sonra bunları satıcının bilgisayarına gönderir. Satıcının bilgisayarında SSL veya SSL ve SET protokolleri kullanılmak suretiyle kredi kartı bilgileri hariç siparişlere ait bilgilerin şifreleri çözülür. Kredi kartına ait şifreli bilgiler güvenli bağlantı yoluyla ilgili bankaya aktarılır. Banka tarafından istenen provizyon verilir. Provizyon satıcıya Internet üzerinden aynı yöntemlerle geri döner. Satıcının bilgisayarı tarafından elektronik ticaret işlemi sonuçlandırılır.

2. SSL Sertifikası Alırken Dikkat Etmeliyiz

SSL sertifikası internet üzerinden yapılan işlemlerin güvenliğinin sağlanması açısından birinci derecede önem taşımaktadır. SSL sertifikasının alınması aşamasında da bazı noktalara özellikle dikkat edilmelidir.

- Sertifikanızı "Tarafsız ve Güvenilir Üçüncü Parti Sertifika Otoritesi"nden (ticari olarak tanınmış ve elektronik sertifika satışı faaliyetlerini gerçekleştiren firmalar) aldığınızdan emin olmalısınız.
- Dijital sertifikanız şifreleme standartı Dünya Standart'ı olan 128 bit'den aşağı olmamalıdır.
- Sertifikanızın geçerliliğini ilgili Sertifika Otoritesi'nin "Sertifika İptal Liste (CRL)"lerinden gerçek zamanlı kontrol edilip edilmediğini öğrenmelisiniz.
- Sertifikanızın "Sigorta Kapsam"ında olup olmadığını öğrenmelisiniz.
- Dijital Sertifikalar sanal ortamdaki dijital kimliğiniz olduğu için kimlik doğrulama evraklarının sertifika otoritesi tarafından tam olarak istendiğinden emin olmalısınız.
- Sertifika Uygulama Prosedürlerini (Evrakların kontrolü, sertifikanın yayınlanması vs.) kaç gün içerisinde yerine getirdiklerini öğrenmelisiniz.
- Sertifika otoritesinin kök sertifikalarının IE ve Netscape gibi günümüzde kullanılan popüler browser'larda yüklü olup olmadığını kontrol etmelisiniz.
- Kurulum ve ileride karşılaşabileceğiniz problemler karşısında teknik destek alabileceğinizden emin olmalısınız. (Anonim Anahtar Yaratma Süreci-CSR, Sertifikanın server'a kurulması, Sertifika yedeğini alınması, Sertifika yedeğinin kurulması vb.)

3. SSL Sertifikası Veren Bazı Firmalar

SSL sertifikasi veren yüzlerce firma vardır. Bunlardan en çok tanınan global firmalar aşağıya sıralanmıştır.

- Verisign (www.verisign.com)
- Thawte (www.thawte.com)
- Globalsign (www.globalsign.com)
- Entrust (www.entrust.net)

Türkiye'de ise SSL sertifikaları, e-Güven (www.e-guven.com.tr) ve TürkTrust (www.turktrust.com.tr) firmalarından ve Kamu Sertifikasyon Merkezinden (www.kamusm.gov.tr) temin edilmektedir.

4. Barındırma Hizmetinin e-Ticaret Sitesindeki Önemi

e-ticaret sitelerinde en çok dikkat edilmesi gereken konu barındırma (hosting) konusudur. Bir web sitesinin yayını bu servis ile yapılmaktadır. Yazılımın çeşitli modüllerini destekleyen (Database, Component) hızlı bir hosting olması gerekmektedir. Eğer e-ticaret yazılımı ASP ve ASP NET ile yazılmış ise Windows Hosting en doğru seçimdir. Yazılım PHP ise Linux bir server daha düzenli bir çalışma sağlayacaktır.

Türkiye'de barındırma hizmeti veren onlarca firma vardır. Kısa bir araştırma sonucu bizim tespit ettiklerimiz alfabetik sırayla aşağıda verilmiştir.

- Alan Adı (www.alanadi.com.tr)
- Ahoster (www.ahoster.biz)
- Ayashosting (www.ayashosting.com)
- Ege Data Center (www.egedatacenter.net)
- GlobalBilgi (www.globalbilgiteknolojilori.com)
- GoDaddy (www.godaddy.com)
- HostDesign (www.hostdesign.net)
- Hostingkayıt (www.hostingkayit.com)
- İhs Telekom (www.ihs.com.tr)
- Koc.net (www.koc.net)
- Mars (www.mars.net.tr)
- Meteksan (www.meteksan.com.tr)
- Radore (www.rh.com.tr)
- Superonline (www.superonline.net)
- Türk Ticaret (www.turkticaret.net)
- Vargonen (www.vt.com.tr)

- Vom (http://vom.com.tr)
- Webkure (www.webkure.com)
- Webiys (www.webiys.com)

5. e-Ticaret Gereği Sanal POS Yazılımı

Bilirsiniz ürünü satın alma aşamasında ödeme ekranı açılır ve kredi kartı numarası girilerek müşteri ödemesini yapar. Burda iki önemli konu devreye girer. Biri güvenlik SSL sertifikası, diğeri de sanal pos yazılımı. Çünkü e-ticaretten bahsediyorsak, ödemelerin yapıldığı sanal pos yazılımına ihtiyaç duyarsınız ve sanal pos hizmetini aldığınız bankalar, genellikle yazılımlarını güncellerler. Bankaların yazılımlarını güncellemelerinin iki nedeni vardır:

1. Yeni güvenlik katmanları oluşturmak
2. Sosyolojik olaylar sebebiyle alışveriş alışkanlıklarının değişmesi.

Bu durumda bankaların mevcut yazılımlarını takip etmek zorunluluğu ortaya çıkıyor, çünkü her ne kadar yeni yapıya geçerken bankalar eski yazılımları destekleseler de, en son teknolojiyi kullanmak hem güvenlik hem performans açısından her zaman daha iyidir.

Güvenlik sebebinin yanı sıra, tüketici alışkanlıkları ve gelen taleplere göre de bankalar yazılımlarını geliştirirler. Örneğin, artık hızla kredi kartı sistemine geçiş başlamış ve bundan bir kaç yıl sonra da taksitlendirmeye geçilmiştir. Sizin sisteminizin aynı şekilde son teknolojiyi yakalaması ürünlerinizin satışında sitenizin tercih edilmesinde çok önemli bir pay alacaktır.

6. Sanal Pos Başvurusu

Ülkemizde sanal pos hizmeti bir çok banka tarafından verilmektedir, örnek olarak, Garanti Bankası, Akbank, Finansbank, Koçbank ve Yapı Kredi Bankası söylenebilir. Yapılacak en doğru iş çalıştığınız bankaya veya size önerilen bir bankanın başvuru prosedürleri hakkında bilgi edinmek için bankaların ilgili sayfalarını ziyaret etmek olmalıdır.

7. Web Sitesi Nasıl Kurulur?

Bir web sitesi kurmak için öncelikle bir alan adı almanız gerekmektedir. Alan adı sanal dünyadaki adresinizdir. ".com" uzantılı alan adlarını herhangi bir belge gerekmeden yıllık 10 dolar gibi bir bütçeyle kolayca alabilirsiniz. Örneğin, register.com gibi alan adı alabileceğiniz bir sitede çeşitli seçenekler sunulmaktadır. Bu türden sitelerde istediğiniz alan adının sahibi olup

olmadığına bakabilir ve sahipsiz olan alan adını hemen satın alabilirsiniz. Hatta dilerseniz alan adına ek olarak web siteniz için barındırma alanı ve belirli sayıda e posta adresleri içeren paketlere de erişebilirsiniz.

Eğer ".com.tr" uzantılı alan adı almak istiyorsanız, Ticaret Sicil Gazetesi veya Marka Patent Enstitüsü tarafından onaylanmış Marka Tescil Belgesi gerekmektedir. Alan adı alım işlemini kendinizin yapması ilerde oluşabilecek olası sorunların önlenmesi için önemlidir. Dilerseniz bu işlemi web hizmetlerini aldığınız kuruluşa da yaptırabilirsiniz.

Alan adınızı aldıktan sonra sitenizi yayınlamak için bir yayınlama alanı ve size ait e-posta hesaplarına gereksinim vardır. Genellikle bu iki unsur paket olarak sunulmaktadır. Hemen bütün internet servis sağlayıcılarda firmanızın büyüklüğüne uygun alan adı, yayınlama alanı ve e-posta hesap adedi için çeşitli hizmet paketleri bulunmaktadır. Ek hizmetlerle de gelen bu paketlerden size en uygun olanı seçebilirsiniz. Özellikle internet servis sağlayıcı firma seçiminde firmanın profesyonel olmasına dikkat etmelisiniz.

Web sitesini kurmak için çeşitli yöntemler kullanabilirsiniz. Bunlardan en kolayı e-ticaret siteleri veya yazılım üreticileri tarafından sunulan şablonları kullanmaktır. Bu sayede hazır bir şablon üzerine şirketinizle ilgili ayrıntılı bilgi, ürün ve hizmetleri hızla yerleştirerek, var olan tasarım stillerinden birine karar vererek web sitenizi hızla ve kolayca oluşturabilirsiniz. Bu yöntemin tek dezavantajı diğerlerine çok benzer bir site ortaya çıkmasıdır.

Eğer biraz daha farklılaşmak isterseniz, web tasarım ve uygulama geliştirme hizmeti veren profesyonel bir kuruluşla çalışabilirsiniz. Bu kuruluşlarda hem tasarımcılar hem de teknik yeterliliğe sahip hazır ekipler size özel profesyonel bir web sitesi kurabilirler. Bu türden firmaların seçiminde firma referanslarına dikkat etmelisiniz.

Kapsamlı işlevleri olan paket e-ticaret yazılımı sayısı çok azdır. Genellikle paket yazılımlar basit sanal mağaza yazılımları düzeyindedir. Ancak paket yazılımın bedelinin özel yazılıma göre oldukça düşük olacağı da bir gerçektir. Bu durumda karar verirken öncelikle paket yazılımları inceleyerek, ihtiyacının ne kadarının karşılandığının incelenmesi ve tatminkar bir sonuca ulaşılamıyorsa özel yazılımın tercih edilmesi uygundur.

Özel yazılım tercihinde ise daha önceki bölümde de belirttiğimiz gibi mutlaka yetkin bir firma ile çalışılmalı, özellikle ticari kimliği olmayan programcılar tercih edilmemelidir. Çünkü özel yazılım sürekli olarak programcı ile işbirliği içinde çalışılmasını ve geliştirmeyi gerektirmektedir.

Diğer bir yöntem olarak şirket bünyenizde bir web tasarım ekibi oluşturmayı tercih edebilirsiniz. Eğer sürekli olarak web sitenizin güncellenmesi gerekiyorsa, bir takım internet tabanlı bilgi ve iş akışı uygulamaları kullanmak istiyorsanız, bünyenizde bir ekip kurmak daha verimli olabilir. Bu sayede sürekli değişen gereksinimlerinize daha hızlı çözümler üretebilirsiniz.

Bunun yanı sıra hosting bölümünde de belirtildiği gibi, kaliteli bir e-ticaret scripti kullanılmalıdır (ISS ve benzeri lisanslar alınmalıdır). Tercihen ASP.NET ft MsSQL kullanılmalıdır, çünkü PHP saldırılara ve açık vermeye daha yatkındır.

8. İşlemler Ne Kadar Sürecek?

Tüm bu işlemlerin tamamlanma süreleri, seçeceğiniz site tasarımına, ssl ve sanal pos anlaşmaların yapılmasına, ürünlerin yönetim konsolundan sitenize eklenme hızına bağlı olarak değişebilmektedir. Bizim öngördüğümüz süre 1 ile 4 hafta arasındadır.

Türkiye'de barındırma hizmeti veren onlarca firma vardır. Kısa bir araştırma sonucu bizim tespit ettiklerimiz alfabetik sırayla aşağıda verilmiştir:

- Delta Websistem (www.deltawebsistem.com)
- e-Ticaret Sistemi (www.e-ticaret-sistemi.com.tr)
- Garanti e-ticaret (http://eticaret.garanti.com.tr)
- İde Software (www.ide.com)
- Karia Soft (www.kariasoft.com)
- Kobimaster (www.kobimaster.com)
- Kolay Mağaza (www.bahacan.com.tr)
- Neticaret (www.neticaret.com)
- Odesis (www.odesis.com)
- ProjeSoft (www.projesoft.com)
- Return Group (www.return.com.tr)
- SRT Software (www.srtsoftware.com)
- TeknoArt (www.teknoart-design.com.tr)

1.4.3. İŞLETME-TÜKETİCİ e-TİCARET MODELİ

e-ticareti işletme-işletme ve işletme-tüketici arasındaki ticaret olarak ikiye ayırabiliriz. e-ticaret piyasasında gördüğümüz daha çok işletme-tüketici modelidir. İşletme-tüketici modelinin işletmecisinin yoğunlaşması gereken başlıca meseleler:

- Kişilik kazandırmaya yoğunlaşın: e-ticaret sitelerinin belirli müşterileri hedef alan benzersiz bir butik oluşturmasına yardımcı bir dizi yazılım bulunuyor. e-Ticaret sitenize bir kişilik kazandırarak belirli kesim müşteriye daha iyi hitap edebilirsiniz. Örneğin, kendi kişiselleştirme ve müşteri ilişkileri yönetimi (CRM) sistemini inşa eden Amazon, müşterilerinin kişiye has tercihlerini tanıma özelliğiyle tanınıyor.
- Kullanımı kolay bir müşteri servisi uygulaması yaratın. Sadece e-posta adresi sağlamak müşterileri sorularla yıldırmaya neden olabilir. Canlı söyleşi veya en azından bir telefon numarası yardımcı olacaktır.
- İnternet sitenizin kullanımı kolay yapmaya odaklanın.
- Taahhüt: e-ticaret giderek müşteri memnuniyeti ve teslimat gerçekleştirmeye yoğunlaştı. Taahhüt problemleri nedeniyle bazı Noel siparişlerinin teslimatını geciktirmesiyle gerçekleşen, "Toys R Us" firmasının 1999'daki fiyaskosu bu konuda uyarıcı bir hikayedir. O zamandan beri şirketler zamanında teslim garantisi için kendi lojistik sistemlerini geliştirmeye milyarlar harcadılar. Müşteriler için anında memnuniyet sağlamak hala kolay değil ama tedarik zincirindeki yatırımlar ve lojistik teknolojilere artan yoğunlaşmayla başarılı işletme- tüketici e-ticaret operasyonlarıyla taahhütten kaynaklanan problemleri bulmak kolaylaşarak, rahatlık sağlıyor.

1.4.4. e-TİCARETİN CAZİBESİ

Aşağıdaki liste e-ticaret'in cazibesinin özeti niteliğindedir.

- Düşük işlem maliyeti: eğer bir e-ticaret sitesinin gerçekleştirilmesi iyi yapılmışsa, web sayesinde sipariş alım maliyeti ve satış sonrası otomatik işlemlerle müşteri servisi maliyetlerini önemli ölçüde düşürür.
- İşlem başına daha çok alış: Amazon normal mağazaların sunmadığı bir özellik sunuyor kullanıcılara. Bir kitabın içeriğini okurken aynı zamanda "bu kitabı alan kişiler başka neler almış" seçeneğiyle insanların gerçekten aldığı ilgili kitapları görebiliyorsunuz. Bu gibi özellikler sayesinde insanlar normal bir kitapçıdan alacaklarından daha çok kitap satın almaya yöneliyorlar.
- İş devrine entegrasyon: Bir internet sitesi iş devrine iyi entegre edilmişse, müşterilere daha önce kullanılandan daha geniş bir bilgi sunabilir. Örneğin, Dell her bilgisarayın üretim ve nakliyat işlemini takip eder ve müşteriler siparişleri o an nerede görebilirler.
- İnsanlar farklı yollarla alışveriş yapabilirler: Geleneksel posta sipariş şirketleri, evden pijamalarınızla bile alışveriş yapabileceğiniz bir konsept sundular, e-ticaret de size aynı lüksü sunuyor.

- E-ticaret yapan internet sitelerinin sunduğu yeni özellikler:
  - Ürünleri yapılandırmaya ve güncel fiyatlarını görme imkanı
  - Karmaşık ısmarlama siparişlerin kolayca yapılabilme imkanı
  - Birçok satıcının fiyatlarını kolayca karşılaştırabilme imkanı
  - Geniş katalogları kolayca araştırabilme imkanı
  - Geniş kataloglar: Bir şirket normalde bir posta kutusuna sığamayacak büyüklükte geniş katalogları internette yapılandırabilir.
- Gelişmiş müşteri etkiletişimi: Otomatikleşmiş araçlarla müşterilerle neredeyse hiç maaliyet olmadan çok daha çeşitli yollarla etkileşim kurmak mümkün. Örneğin, müşteri siperişi onaylandığında, gönderildiğinde ve ulaştığında e-posta alabilir. Mutlu bir müşteri şirketten daha fazla alış yapmak isteyecektir.

Bu tür avantajlar e-ticaret'in daha çok rağbet görmesine yol açıyor. e-ticaret yapılması gerektiğine işaret eden bir nokta daha var. e-ticaret, insanlara tamamıyla yeni iş modelleri yaratma imkanı veriyor ve maliyeti düşürüyor. Örnek olarak, e-ticaret yerine katalog üzerinden postayla satış yapan bir firmanın, bu katalogları her seferinde yenileme ve düzeltme yüzünden tekrar tekrar basma maliyetleri ve postalama maliyetlerini dikkate alırsak, e-ticaret çok daha az maliyetlidir.

Bir diğer yüksek maliyetli şey de sipariş alma departmanında telefonu cevaplama personelidir. e-ticarette katalog dağıtım maliyeti ve sipariş alım maliyeti neredeyse sıfıra düşmektedir. Bu da ürünleri daha düşük fiyatlarda sunma imkanı sağlar ve ya maliyet dinamikleri nedeniyle daha önce sunulamamış ürünleri sunmaya imkan verir.

1.5. ELEKTRONİK TİCARET KISA REHBER

1.5.1. e-TİCARETİN KEŞFİ

Herhangi bir iş alanında bir hareket veya genişletme için online iş yapma düşüncesi, girişimcinin kafasını karıştıracak bazı soruların oluşmasına sebep olabilir. Bunu ortaya çıkarmak için tam olarak ne yapmak gerekir? Online varlık göstermek, işin pazarını nasıl değiştirir? Bu konuda rakipler neler yapıyor? Burada insanlar nasıl alış veriş yapacak? Nasıl güvenlik önlemlerine gerek vardır? Müşteriler ödemeyi online olarak nasıl yapacaklar?

Web sitelerinde e-ticaret olmayan veya küçük boyutlarda e-ticaret yapabilme gücüne sahip işletmeler, pazarlama sitelerini satış merkezlerine dönüştürerek müşteri tabanlarını, resimleri ve satışları tamamen değişik yollarla

genişletmeyi öğrenebilirler. Henüz online olarak iş yapmamış olan girişimciler, internetin işleri nasıl değiştirdiğini ve kendilerini pazarda nasıl tanıtacaklarını keşfedebilirler.

1.5.2. NİÇİN e-TİCARET?

e-ticaretin en şaşırtıcı ve ilgi çekici yanı, satışları ve pazarlama çalışmalarını çok hızlı bir şekilde etkileyebilme özelliğidir. Bir fırın veya bir danışmanlık servisi, online iş yaparak erişimini tüm ülkeye hatta yurtdışındaki potansiyel müşterilere kadar büyütebilir. Web üzerinde yapılan satışlarda uluslararası sınırları tanımazlar.

Online trendleri ve istatistikleri analiz eden kuruluşlar, 2008 yılında Amerika işletmeleri için online perakende satışların 230 milyar dolar olduğunu hesaplıyor. Bu rakamın tahmin edilen toplam Amerika perakende satışlarının %10'u olduğu biliniyor.

Araştırmalara göre, internet bir şirketin ulaşabileceği potansiyel müşteri sayısını artırmasının yanında, aynı zamanda karlılığın da artmasını sağlar. Bu araştırma bunun yanında, internet işlemleri ekstra gider olmaktan ziyade, işleri birçok konuda hızlandırdığını göstermiştir.

Online olsun veya olmasın yeni iş dünyasında nakit akışı önemli bir yere sahiptir. Bir çalışma, online iş yapan küçük bir işletme sahibinin online satışlar sonucunda ödemeyi daha hızlı aldığını ve işleri daha kolay yaptığını gösterdi.

Girişimciler online olarak hareket ettiği zaman, kendilerini daha büyük rakiplerin olduğu bir sahada bulurlar. İnternet üzerinde küçük-büyük her işletme, her sokak köşesinde bir mağazası olan da olmayan da aynı çekiciliğe ve aynı işlevselliğe sahiptir. Genellikle küçük mağazaların büyük dükkanlardan daha belirgin olduğunu düşünen mağaza sahipleri, müşterilerin ilgisini çekmek için butikler oluştururlar.

1.5.3. ONLİNE İŞ YAPMAK NE GETİRİR?

Girişimcilerin bir işe başlarken karşılarına çıkan zorların üstesinden gelip, bu işin meyvelerini toplamalarını sağlayan iki hususi özellik vardır. Aynen fiziksel olarak gerçek bir dükkan açar gibi, online bir alışveriş merkezi oluşturmak da çok tutku ve iyimserlik ister. Tutku girişimcinin üzerinde kariyer yapmayı istediği şeyi bulması ve bunu istemesidir. Pozitif düşünce

birlikte çalışılan insanlar, bankalar veya rakiplere karşı her zaman işe odaklı kalabilmeyi sağlar. Online yapılan işler dünyaya kapısını açtığı zaman bir "Evet, yapabilirim" ifadesi "Vay! Bu işe yarıyor" şekline dönüşebilir.

İşleri online ortama taşımak çok da zor olmak zorunda değildir. Online bir iş kurmak için girişimciler tüm tutku ve iyi niyetlerini şu üç konuya yoğunlaştırmaları gerekir:

1. ***Planlama aşaması;*** Bir girişimcinin tüm bilmesi gereken, bir e-ticaret sitesi kurmadan önce düşünmek ve karar vermek.
2. ***Pazarlama stratejisinin geliştirilmesi;*** İşlerin nasıl düzenleneceğine ve müşterilerle iyi ilişkilerin nasıl korunacağına karar vermek.
3. ***Teknoloji gereklerinin anlaşılması;*** İşi yapmak için bütün araç ve gereçleri elde etmek.

1.5.4. PLANLAMA SÜRECİ

Küçük iş sahiplerinin en önemli ve başlıca yapması gereken şey iyi düşünülmüş bir plana sahip olmaktır. İnternet bilgi toplamak, kendi konumundaki insanların tecrübelerinden faydalanmak ve bir plan oluşturmak için verimli bir şekilde kaynakları kullanmak için en iyi araçtır. Plan, yapmaya niyet edilen işi her açıdan kritik bir gözle inceleyen bir yapıda olmalıdır. Ele alınması ve üstünde durulması gereken bazı önemli sorular şunlardır.

1. Bu İşi Yapmak İçin Webi Kullanmak Mantıklı mı?

Web'in iş oluşturmak için çok büyük bir güce sahip olduğunu söylemiştik. Bunu söylemekle birlikte bazen bir ürün online satışa uygun değilmiş gibi görünebilir. Örneğin, eğlence parkları, bowling salonları veya kamu hizmetleri şirketleri gibi işler müşteriye yerinde hizmet verir. Fakat bu tip işlerde bile müşteriler online hizmet bekleyebilirler. Mesela bir şirket online bilet satışları veya indirimler uygulayabilir, tesis ve hizmetlerinin fotoğraf veya videolarını yayınlayabilir, talepleri arttırmak için online oyunlar oluşturabilir veya müşterilere internet üzerinden ödeme kolaylığı sağlayabilir.

2. Diğer Şirketler Bu Konuda Ne Yapıyor?

Sanal olmayan mağazalarda olduğu gibi online girişimcilerde eğer ayakta kalmak istiyorlarsa sektördeki yarışı anlamak zorundadırlar. Rekabetçi bir analiz yaparak online iş sahiplerine, işlerini rakip firmalardan farklılaştırmak ve promosyon yapmak için bu konuda bilgi verip donatmak gerekir.

Kapılarını internete açan bir girişimcinin atılımı, rakiplerinin satışları arttırmak için sadece fiziksel olarak neler yaptıkları değil, aynı zamanda rakiplerin sanal alemde müşterilere neler sunduklarına da bağlıdır. Örneğin, online olarak bir güzellik ürünü almak istiyorsunuz. Herhangi arama motorunda "ruj" yazarak, online alışveriş portalları, hangi rakip şirketlerin listelerde yükseldiğini görmenizi sağlar. Rakip şirketlerin ürün seçeneklerine, fiyat listelerine, sunulan promosyonlara ve hedef kitleye bakarak kendi mağaza durumunuzun nasıl konuşlanması gerektiğini belirleyebilirsiniz.

Bu çok zaman alan bir süreç olabilir ama unutmayalım ki, bu paha biçilmez araştırma para yerine zaman almaktadır. Bu durumda zaman paradır ve bir süre sonra parayı birkaç kat artıracaktır.

Eğer bir alanda zaten bir iş varsa, bu durumda önemli olan onu diğer rakip firmalardan farklılaştırmaktır. Bu, daha kapsamlı bir ürün veya hizmet sunarak, müşteri hizmetleri ya da teknoloji avantajları vererek olabilir.

3. Ne Gibi Kaynaklara İhtiyaç Vardır?

Online hizmet veren bir firmanın kapıları hiç kapanmaz. İşletmeyi online iş sahibi 7 gün 24 saat çalıştırmayarak siparişleri söz verilen zamanda yerine getiremeyebilirki bu da müşteri kaybetmenin kesin bir yoludur. Bu yüzden internet üzerinden yapılan işler full time olarak çalıştırılmaları ve girişimciler bu konuda ne kadar yardıma ihtiyaçları olduklarını gerçekçi bir şekilde karar vermeleri gerekir.

Genellikle online iş sahipleri küçük sıkıcı işlerle dolacaklarını ve işlerini yürütebilmek için birçok zorluklarla uğraşmak gerektiğini düşünüyorlar. Çoğu zaman web uzmanlarına veya her gün online görevlerin koordine edilmesini sağlayan profesyonellere dönüşürler. İyi yetişmiş bir web profesyoneli tutmak için şu ihtimaller düşünülür:

- Eğer işin yapısı ve boyutları bunu gerektiriyorsa, kendini sadece web yönetimine verecek bir kişi tut
- İşin kurulumu için ve sitede değişiklikler ve yenilikler yapmak, online kapasiteyi artırmak için çağırabileceğin geçici çalışanlar tut
- Ürün geliştirme, dizayn ve hosting için dış kaynak kullan
- Bir e-ticaret sitesi kurmak için "tek kutu içinde e-ticaret" türünden ürünleri kullan. Bu ürünler genellikle aylık bir ücretle çalışırlar.

4. Hedef Kitleniz Kimler?

Ne zaman bir firma yeni bir ürünü veya hizmeti pazara çıkaracak olsa, yönetim; tüketicilere nasıl yaklaşılacağını düşünürken coğrafi, demografik ve sosyo-ekonomik faktörleri göz önüne almalıdır.

Bazı ürünler, örneğin oyuncak, okul malzemesi veya bakıcılık hizmetleri gibi hizmetler belirli bir yaş grubuna hitap eder. Diğer ürün veya hizmetler, örneğin kar üfleyici veya yüzme havuzu araçları gibi, belirli bir coğrafi bölgeyi hedef alır. Her müşteri özeldir yani tüccarlar pazarlama ve tüketicilerle olan ilişkilerini buna uyarlamak zorundadırlar.

5. İş Sahibi Ağını Ne Kadar Uzağa Fırlatmalıdır?

Global ekonomide bir küçük işletmecinin, güne CartaSi kredi kartı ile ödeme kabul edip etmediklerini soran Milan'dan aldığı bir e-posta ile başlaması muhtemeldir. Online işletmecilerin ilk günden itibaren şunu çok iyi anlamaları gerekmektedir ki, uluslararası bir iş yaptıklarından gezegenin her köşesinde şubeleri ve vitrinleri vardır.

Bir işletme müşterilerine, sadece kuzey Amerika bölgelerine ürün gönderebildiklerini ya da sadece Amerikan doları kabul ettiklerini söyleyebilir. Ama böylelikte deniz aşırı ülkelerdeki çok iyi satış imkanlarını kaçırmış olabilirler. Bu durumda online ticaret için yabancı milletlerden müşterilerle nasıl çalışılacağına karar vermek çok önemli bir konudur. Nakliye işleri nasıl halledilecek? Para birimi değişikliğini şirket mi hazırlayacak? Farklı diller konuşan müşterilerle işletmeci nasıl ilişki kuracak?

6. Nakliyat Konusu Ne Olacak?

Online ticaret çoğu zaman nakliyat sorunları yüzünden bozulur. Şunu düşünelim: A müşterisi uzun zamandır aradığı bir ürünü çok iyi bir fiyatla bulur. Elektronik sipariş formunun bilgilerini doldurduktan sonra, fiyata nakliye için eklenen ücreti görünce şaşıp kalır. Sonuç? Müşteri bir parmak hareketiyle siteyi kapatır ve başka bir siteye yönelir. Bazı online şirketler nakliye masraflarını üstlenir, bir kısmı bu ücreti ürünün liste fiyatına ekleyerek yansıtır ve ücretsiz nakliyat işlemi sunar.

Nakliyat kolaylığı ve ücret uygunluğu en önemli rekabet aracıdır. Nakliyat masraflarından kar elde etmeye çalışılmalıdır. Çünkü buradan kazanacağınız kaybedeceğinizden çok daha fazladır.

7. Müşteri Hizmetleri Politikasının Unsurları Nelerdir?

Müşteriler işletmelerle soruları, siparişleriyle ilgi sorunları veya özel istekleri aracılığıyla kontak kurabileceklerini düşündükleri için, online ticaret yapan firmalar müşteri hizmetleri için telefon numarası ve e-posta adresi vermelidirler. Müşteri hizmetleri sadece bir bağlılık sağlama yolu değil, ayrıca değerli bir geri dönüşüm mekanizmasıdır.

Müşteri hizmetlerinin önemli bir yönü de, müşteri isteklerine veya şikayetlerine (telefon veya e-posta) ne sıklıkla cevap verileceğine karar vermektir. Bu yanıt zamanlaması gerçekçi ve tutarlı olmalıdır. Eğer anlaşmada tüm telefonlara iki dakika içinde cevap verilecek yada aynı gün içinde dönülecek deniliyorsa, bu müşteri için bir vaat anlamına gelir. Bir online müşteriyi, verilen bir e-posta adresinden saatlerce, günlerce hatta haftalarca cevap beklemek çok hayal kırıklığına uğratır. Müşterileri sitenizde tutmak için böyle şeylerden sakınmalısınız.

İyi web siteleri kurmak, kullanımı kolay iyi bir dizayn oluşturmakla başlar. Grafik dizaynı ve ana sayfanın içeriği müşterinin dikkatini çekmeli ve iç sayfaların da takibi kolay olmalıdır. Bilgiler kolaylıkla bulunmalı ve bunlar genel kullanıcıların anlayacağı dilde olmalıdır. Çok teknik ve sadece profesyonellerin anlayacağı dilden kaçınılmalıdır.

Şimdi, bir sitenin nasıl görünmesi ve müşterinin site içinde nasıl yönlendirilmesine karar vermek için 10 basit püf noktasına bakalım.

1. Firmanın ne yaptığını siteyi ziyaret edenlere hemen söyle.
2. Kullanıcıların istedikleri bilgiyi iki tuşlama sonunda bulmalarını sağla.
3. Mağazanın ismini veren ana başlıkları ve diğer linkleri içermesini ve kullanılan sayfadan ana sayfaya geçişi sağla. Kullanıcı her zaman hangi sayfada olduğunu bilsin.
4. Kullanıcının sorularına kolaylıkla cevap bulmasını sağla.
5. Büyük fonlar ve resimler düzgün bir şekilde uygulansın ve uygun olan yerlerde sesli açıklamalar içersin.
6. Bilginin kalitesine özellikle itina göster, özellikle yazım hatası olmamasına okunur olmasına dikkat et.
7. Bilgi vermeyen cümle veya sözlerden kaçının
8. Her sayfaya ana sayfanın linkini ekle ki, her durumda tek tıkla ana sayfaya ulaşılabilisin.
9. Ürünlerin fotoğraflarını içeren çok abartılı ve dikkat dağıtıcı olmayan, kullanışlı görsel efektler ekle.
10. Hangi teknolojiler faydalı, hangileri zararlı karar ver.

1.5.5. WEB SİTESİNDE ÜRÜN PAZARLAMA

Online ticaret yapmak isteyen kişinin hemen hemen her ürünü satabilmesi için atması gereken en önemli adım ürünlerin birçok resmini siteye dahil etmektir. Çünkü online alışveriş yapanlar, özellikle ürünü satın almadan tutamadıkları veya deneyemedikleri için alacakları ürünün nasıl göründüğünü görmeyi beklerler. Bu yüzden ürünlerin birçok açıdan çekilmiş resimlerini koymak gerekir. Bazı durumlarda müşterinin ürünün boyutlarını kıyaslayabileceği bir başka araçla beraber resimlerini koymak gerekir. Örneğin, bir ruj ile cep telefonu gibi.

Ürün pazarlama stratejisi oluştururken şunlar düşünülmelidir:

- Sitede, kullanıcıya sağlanamayacak öneriler sunulmamalı, yerine getirilemeyecek vaatlerde bulunulmamalıdır. Bilgiler müşteri için kullanışlı olmalı ve ürünlerin pozitif yönleri ortaya çıkartılmalıdır.
- Birbirini tamamlayan ve destekleyen ürünler sunulmalıdır.

1.5.6. YENİ ONLİNE MÜŞTERİLERİ ÇEKME

Yeni ziyaretçilere bir site açmanın çeşitli yolları vardır. Arama motorları ve e-posta bağlantıları online satıcılar için popüler yöntemler oldular.

1. Arama Motorları

Yüzlerce hatta binlerce rakip firmanın olduğu bir ortamda bir firma, arama motorunda çıkan sonuçlarda kendi ürünlerini nasıl öne çıkaracak? Arama motoru sonuçlarındaki listelerde ilk veya ikinci sayfada yer kazanmak e-ticaretin "kutsal kasesi" olarak düşünülür. Bu durumda bir işletmenin ürünlerinin ilk sayfada yer alması çok önemlidir. Bu konuyla ilgili iki yaklaşım vardır. Bunlar; doğal aramalar ve ödemeli aramalardır.

Doğal araştırmada ön sıralarda yer almak için, şirketinizin web sitesinin içeriğinde sunduğunuz ürünlerle ilgili tüketicinin arayabileceği anahtar sözcükler bulunmalıdır. Örneğin, eğer bir online mücevher mağazanız varsa tüketicilerin "elmas küpeler" şeklinde bir arama yapacağını düşünerek bunu içeren bir site oluşturmanız gerekir.

Doğal araştırmada sıralamanızı artırmak için uygulanacak çeşitli yöntemler vardır. Bu yöntemlerin çoğu yasaldır ama bazı satıcılar koyulan kurallara ve düzenlemelere uymuyorlar. Eğer siz bir doğal arama stratejisi uygulamak için üçüncü şahıslarla çalışıyorsanız, referansları kontrol ettiğinizden emin

olun, onların çalıştığı diğer firmaları gözlemleyin ve onların arama motoru servis anlaşmasına uygun şekilde çalıştıklarına emin olun.

Ödemeli aramalarda ise firmalar listelerin ön sıralarında yer almak için ödeme yaparlar. Örneğin, Overture denilen bir firma, online satış yapan şirketlerin ürünleriyle yada verdikleri hizmetlerle ilgili anahtar sözcükler alarak onlara ulaşmak istedikleri bir bölgede listelerin ön sıralarında yer verirler. Böylelikle Yahoo!, Lycos gibi arama motorlarının sonuçlarında öncelik kazanmış olurlar ve burada listedeki linklerine her tıklama olduğunda bunun için ücret öderler.

En popüler arama motorlarından biri olan Google'ın anahtar kelimeye yönelik her tıklamada ücret aldığı bir çalışması vardır. Burada sponsor linkler olarak bilinen aranan kelimeyle ilgili bazı firmaların linkleri, arama listesinin yanında, kullanıcının ilgisini çekmek için bulunur. İş sahipleri çeşitli arama motorlarını araştırarak hangi programın kendi ürünlerine en uygun olduğuna karar vermelidirler.

2. e-Posta Yolu ile Pazarlama

e-Posta yolu ile pazarlama eğer doğru bir şekilde yapılırsa müşteri ilişkilerini derinleştirir ve satış prosessine kişisel bir incelik katar. Tersine uygunsuz bir şekilde yapılmış e-posta kampanyası müşteri firmadan uzaklaştırır.

Müşteriler için hazırlanmış e-posta haber bülteni online iş yapan firmalar için mükemmel bir araçtır. Ürünler ve fiyatlar arasında mekik dokumak yerine, e-posta haber bültenleri firmanın son yaptığı işler ve ürünlerle ilgili çok kullanışlı bilgi ve haberler almamızı sağlar. Aslında e-posta haber bültenleri genellikle özel promosyon ve indirimleri duyurmak için kullanılır. Bu firma markasını oluşturmak için çok güzel ve ucuz bir yoldur. Ayrıca bunlar dijital ortamda olduğu için kağıt tüketimi ve yazım masrafları içermediğinden sınırsız sayıda e-posta haber bülteni yayınlayabilirler.

Şimdi firmanız online ticaret yapmak için bir plana ve stratejiye sahip. Peki bunu yapılandırmak içine yapmak gerekir? Aynen somut dünyada olduğu gibi öncelikle bir isim ve yer belirlemek gerekir.

Online şirketinizin adresi bir URL (Uniform Resource Locator) (Tekdüzen Kaynak Bulucu) ile gösterilir. Genellikle adres ticari bir site olduğunu gösteren (commerce) nokta com (.com) ile biter ya da organizasyon sitesi anlamı veren (organization) nokta org (.org) ile biter.

3. Sanal Alemde İlan Yayınlama

Şirketler küçük ücretler karşılığında bir web sitesi alabilir ve kayıt olabilirler. Bir web sitesi ve alan adı almak için www.nic.tr adresine gitmek yeterli. ABD menşeli alan adları için en çok kullanılan siteler www.register.com ve www.networksolutions.com'dır.

1.5.7. ONLİNE ALIŞVERİŞ KARTLARI

Verimli bir online ticaret merkezi oluşturabilmek için diğer bir gereklilik ise sanal alışveriş kartlarıdır. Aslında bu işlemin gerçekleşme sürecinde ilk adım olarak bir elektronik sipariş formu gibidir. Amacı ise şunları güvenli bir şekilde yapmaktır :

1. Müşterilerin ürünleri bakıp istediklerini seçmelerini ve hangisini alacaklarına karar vermelerini sağlamak,
2. Müşterinin seçtiği ürünlerin bir özet listesini görüntülemek,
3. Müşteriler alış işlemini onaylamadan önce, her ürün için satış politikası veya ürün ayrıntıları gibi sayfalarına geri dönebilmelerini sağlamak,
4. Müşteriler alış işlemini bitirmeden seçtikleri ürünlerden istediklerini çıkarmalarını veya ürün miktarını değiştirmelerini sağlamak,
5. Müşteriyi alış işlemini onaylayıp bitirmek için yönlendirmek ve daha fazla ürün seçmek isterse ana sayfaya gidişini kolaylaştırmak.

Bu alışveriş kartları yazılımları satıcılara web siteleri üzerinden çeşitli ürünler için sipariş kabul etme imkanı sunar. Müşteri siparişlerini, nakliyat ve vergi giderlerini de toplayarak otomatik olarak hesaplar.

Güvenli online alışveriş kartı teknolojisi sunan çeşitli servisler vardır. Örneğin, PayPal firması satıcı üyelerine ücretsiz alışveriş kartı programı verir (PayPal, online ödeme sistemi sunan bir firmadır; www.paypal.com). Alış veriş işlemlerini bitiren müşteri ödemeyi PayPal hesabından yapmak istediğini belirtince süreç otomatik bir şekilde işler.

1.5.8. GÖZ GEZDİRENLERİ ALICI YAPMAK

Online alıcılar ayrıntılarla çok uğraşan titiz insanlardır. Deneyimli olmayan müşteriler tüm alışveriş süresi boyunca ürkek davranırlar. İyi planlanmış, güvenli alışveriş kartı, hesap kontrolü sürecini kolaylıkla halleder.

Jupiter Araştırma şirketi tarafından yapılan bir çalışmada, internet müşterilerinin %54'ünün alışverişin ortasında işlemi bitirdiği tespit edilmiştir.

Bunun nedeni servis, nakliyat, teslimat ve kullanma işlemleriyle ilgili endişeleri olmasıdır. Yine müşterilerin %60 ila %90 oranında satın alma işlemini yarıda sonlandırmalarının yapma sebebi, çoğu zaman kafa karışıklığı, aradığını bulamadığı için hayal kırıklığına uğraması veya bilgi eksikliği olabilir.

Bir iş için online alışveriş kartı oluşturmak için şu yol göstermelerine dikkat edilmelidir:

- Alıcıyı oturum açma, şifre belirleme ve formları doldurma işlemleri için çok uzun bir işleme tabi tutmayın.
- Teminat, teslim garantisi, geri alış politikası ve teslimat ücreti yapılanması gibi sayfa detaylandırma müşteri servisleri için bir link ekleyin
- Sıkça sorulan sorular ve ücretsiz danışma hattı gibi tüketiciler bir problemle karşılaştığında veya bir soru sormak istediklerinde kullanabilecekleri bir "yardım" kutusu oluşturun.
- Kredi kartı bilgilerini korumak için şifreleme yöntemleriyle bir güvenlik sistemi oluşturun.
- Müşteriler işlemlerini bitirip sayfadan çıkmadan önce ürünler hakkında bilgi almak için site yöneticisine hemen ulaşılmasını sağlayın.
- Müşterilerin hesap kontrolü sayfasındayken herhangi bir ürünü ekleme, çıkarma, miktarını değiştirme veya ürünün model veya stilini değiştirme gibi işlemlerini kolaylaştırın.
- Hesap kontrolü süreci boyunca kargo masraflarını müşteriye gösterin. Bazı ürünler için bu ücretler müşterilerin online alışverişlerini ve aldıkları miktarı gösterir.
- Hesap kontrolü süreci boyunca bir sonraki adımı açık bir şekilde gösteren bir buton oluşturun ve bunu diğer linklerden daha belirgin bir şekilde gösterin.
- Kredi kartı, çek veya online ödeme servisleri gibi çeşitli ödeme seçenekleri koyun.

Bir işletmenin ilk günlerinde nakit akışı gidişatta belirleyicidir, işletmenin ilerlemesine veya batmasına sebep olabilir. Bu yüzden birçok işletme çeşitli ödeme seçenekleri sunmalarına rağmen insanları kredi kartı ödemelerine yönlendirirler. Çeşitli ödeme seçenekleri sunarak insanlara tercih ettikleri şekilde ödeme yapmalarını sağlamak online ödemeleri artırmıştır. Ayrıca para hesaba hemen girdiğinden online ödemeleri kabul etmek gelirleri ve nakit akışını artırır.

İşletmeler e-ticaret fonksiyonları oluştururken ve online ödemeleri kabul

ederken çeşitli seçeneklere sahiptirler. Bunlar aşağıdaki bölümlerde anlatıyoruz.

1. Bir İşletmecinin Hesabı Yoluyla Ödeme Yapmak

Online kredi kartı ödemelerini kabul etmek için, küçük iş sahipleri önce bir banka hesabına başvurmalı ve işlemi uygulamak için yöntemler bulmalıdır. Gerçek dünyada, kredi kardı okuyucudan geçtiği zaman bu işlem gerçekleşir. Bir online mağazada ise, müşteri kredi kartı bilgilerini girdikten ve onaylandıktan sonra işlem gerçekleşir.

Birçok online hesap kontrolü süreci boyunca, bir müşteri hangi ödeme şeklinin en çok tercih edildiğini sorabilir. Eğer bir müşteri kredi kartı ödemesi için bir form seçerse, kredi kartı bilgilerini girmek için site içinde güvenlik sayfasına yönlendirilirler. Müşteri kabul ediyorum tuşuna bastıktan sonra kredi kartı bilgileri işletmecinin hesabına gidecek ve bilgiler doğrulandıktan sonra işleme alınacaktır.

2. Online Ödeme Servisi Oluşturmak

Eğer bir işletme banka hesabına erişim sağlayamıyorsa veya ücretler çok fazla ise PayPal gibi bir online ödeme servisi oluşturmak bir çözümdür. PayPal kredi kartı işlemlerine izin verir ve ödemelerin güvenli ve uygun bir şekilde yapılmasını sağlar. Ayrıca müşterilere direk banka hesabından ödeme yapma imkanı da sunar.

Eğer bir alıcı checkout esnasında PayPal ile ödeme yapmak istediğini bildirirse, işlemini tamamlamak için bir PayPal hesabına giriş yapması için yönlendirilir.

PayPal ödeme imkanı sunan işletmelerde bu işten karlı çıkabilir. Çünkü kurulum masrafı, aylık ödeme gibi ücretlendirmeler yoktur. PayPal her işlem için ücret alır.

1.5.9. İŞLEM GÜVENLİĞİ SAĞLAMA

Online girişimciler web sitelerini kullanan kişilere karşı güvenli bir alışveriş sağlamakla yükümlüdürler. Fakat onlar güvenli bir siteye sahip olmak için bilgi teknolojileri güvenliği uzmanı olmak zorunda değiller. Bu konunun uzmanları küçük işletmeler için bazı güvenlik önlemleri geliştirmişlerdir. Küçük işletmelerin bu konuda neye ihtiyacı olduğuyla ilgili bütün güvenlik önlemlerinin bir araya getirildiği bir servis vardır.

1.5.10. GİZLİLİK POLİTİKASI GELİŞTİRME

Müşterilerin kimlik çalınması, spamler aracılığıyla kızdırılmak gibi olaylardan korkması, gizlilik politikasını işletmeler için çok önemli hale getirmiştir. Müşteriler online işletmelerden, gizlilik politikalarını sitelerinde sunmalarını istemektedirler.

Bir gizlilik politikası, müşterinin kişisel bilgileri veya finansal detaylar gibi verilerin nasıl toplandığını ve kullanıldığını açıklar. Müşterilere satın alma bilgilerini, e-posta haber bülteni alma veya gönderme isteklerini veya diğer firmalarla ilişkilerini istedikleri zaman çıkarma hakkı verilmelidir.

Bir online işletme gizlilik politikası yayınlamak ve buna uymak zorundadır. Bu tip politikalar müşterilerin gizliliğine ne kadar önem verildiğini gösterir.

1.5.11. BİR ONLİNE İŞ KURMAK İÇİN 10 ADIM

1. Rakip firmaların sitelerinin nasıl göründüğünü gözden geçir ve kendi sitenin onlarınkinden nasıl farklılaştıracağını düşün.
2. Bir domain ismi alarak URL oluştur.
3. Bir web site tasarımcısı tutarak veya bir web gelişim yazılımı alarak sitenin dizaynı ve yönlendirilmesini ayarla.
4. Bir server satın alarak veya bir taşeron internet servisi sağlayıcısı ile anlaşarak teknolojik konularda bilgi al.
5. Alışveriş kartı ve ödeme servisi içeren güvenli bir online sipariş programı bul.
6. Anti virüs programları kullanarak siteyi koru.
7. Müşteri hizmetleri politikası geliştirmesini içeren bir pazarlama planı oluştur.
8. Ürün sağlayıcıları, arama motorunu en iyi şekilde kullanmanı sağlayacak firmalar, uygulama servisleri, kargo hizmetleri, web teknikerleri, pazarlama ve halkla ilişkiler firmaları gibi önemli partnerlerle anlaşmalar kur.
9. Online kataloglar ve listeler hazırla.
10. Stokları her zaman koru ve müşteriler için katalogları ve listeleri güncelle.

2. e-TİCARET GÜVENLİĞİ - HUKUKSAL AÇILIMLAR

Bu bölümde, elektronik ticarette bilgi güvenliği ile ilgili hususların hukuksal açılımları üzerinde durulacaktır. Daha önceki bölümlerde anlatılan teknik hususların ülkemizdeki yasal düzenlemeler ile ne şekilde belirlendiği, elektronik ticaret yapan firmaların ve kullanıcıların hak, yükümlülük ve sorumlulukları, mevcut ve muhtemel yasal düzenlemelerle regülasyon politikasının ne şekilde belirlendiği detaylı olarak bu bölümde incelenmektedir.

Bu bölüm içerisinde yer alan bilgilerin kapsamı, çalışmanın genel kapsamı olan elektronik ticaret kapsamındaki bilgi güvenliği ile ilgili hususlar ile sınırlandırılmış olup elektronik ticaretle ilgili tüm hukuksal açılımlar bu bölüm içerisinde yer almamaktadır.

2.1. ELEKTRONİK TİCARETTE TÜKETİCİ HAKLARI

Elektronik ticarette tüketici hakları (mesafeli sözleşmeler ile bir süreç belirlenmesi sebebiyle) özellikle elektronik ticaret firmalarının iş süreçlerini etkilemekte ve bu doğrultuda mevzuatla ortaya çıkan süreç içerisinde ortaya çıkabilecek bilgi güvenliği risklerinin belirlenmesi gerekmektedir. Söz konusu düzenlemeler doğrultusunda ortaya konan sürece uyulup uyulmadığı ve olası hukuki uyuşmazlık veya suç hallerinde mevzuat ile belirlenen yükümlülüklerin yerine getirilip getirilmediği ve getirilmediği takdirde sorumluluklar; bilgi güvenliği yönetimi kapsamında varlıkların değerlendirilmesi, varlıkların korunması için önlemler ve risk hesaplaması konuları altında değerlendirilmelidir.

Bu bölüm içerisinde elektronik ticaretle ilgili tüketici düzenlemeleri ile belirlenen haklar doğrultusunda ortaya çıkan hususlar değerlendirilecek, bunun dışında tüketici hakları kapsamında da sayılabilecek olan mahremiyet ve tüketici verilerinin korunması, tüketici hesap ve kullanıcı bilgilerinin çalınması gibi konular ilgili bölümler altında ayrıca incelenecektir.

Ülkemizde elektronik ticarette tüketici hakları temel olarak "mesafeli sözleşmeler" ile ilgili düzenlemeler ile düzenlenmiş durumdadır. AB uyum süreci çalışmaları içerisinde 97/7/EC sayılı "Uzaktan Pazarlama Yöntemi ile Kurulan Sözleşmelerde Tüketicinin Korunması Hakkında Yönerge"[1] doğrultusunda tüketicinin korunması hakkında düzenlemelerle ilgili uyum

[1] ATRG 04.06.1997, L144/19

çalışmalarının yapılması ve ülkemizde yeni başlayan iletişim araçları aracılığıyla satış ve pazarlama faaliyetlerinin tüketici açısından düzenlenmesi amacıyla; 06.03.2003 tarihli ve 4822 sayılı "Tüketicinin Korunması Hakkında Kanunda Değişiklik Yapılmasına Dair Kanun"[2] ile TKHK'na 9/A maddesi eklenerek mesafeli sözleşmeler düzenlenmiştir. Mesafeli sözleşmelere ilişkin uygulama usül ve esasları ise TKHK'nın 31. ve 9/A maddesine dayanılarak 14 Haziran 2003 itibariyle yürürlüğe giren[3] "Mesafeli Sözleşmeler Uygulama Usul ve Esasları Hakkında Yönetmelik" (MSHY) ile düzenlenmiştir. Tüketicinin korunması açısından önemli bir ilerleme teşkil eden Türk hukukundaki bu yeni düzenlemelerin bazı noktalarda fazla korumacı ve özelikle ticaret hayatının sürat ve basitlik gibi ihtiyaçlarını göz ardı eder bir tarzda kaleme alınmıştır[4]. MSHY'de yapılan son değişiklikler ile[5] bu sakıncaların bir kısmı giderilmekle beraber, özellikle yeni eklenen tanımların ve iyileştirilen süreçlerin belirsizliği uygulamada belirsizliklere yol açabilecek mahiyettedir.

2.1.1. MESAFELİ SÖZLEŞME KAPSAMINA GİREN İŞLEMLER

TKHK ve MSHY'de mesafeli sözleşmeler, "yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmeler" olarak tanımlanmıştır. Hukuki açıdan bakıldığında mesafeli sözleşmelerle ilgili yapılan ayrım, sözleşmenin unsurlarına ilişkin değil, sözleşmenin kurulma aşamasında satıcı ve tüketici arasındaki fiziksel uzaklık esas alınarak ortaya konmuştur. Şöyle ki, mesafeli sözleşme kapsamına, herhangi bir malın veya hizmetin tüketiciye sunumu (teslim ve ifa) için yapılan herhangi bir sözleşme girebilmektedir, ancak bu sözleşmelerin tarafların karşı karşıya gelmedikleri bir durumda yapılması gerekmektedir.

Kanunla mesafeli sözleşmelerin ayrıca düzenlenmesinin sebebi, malı görerek ve muayene ederek satın alma şansı olamayan tüketicilere, normal şartlarla yapılan alım işlemine göre fazladan koruma sağlamaktır. Örnek vermek gerekirse, bir mağazadan alınan elbisenin tüketici tarafından incelenmesi hatta denenmesi mümkün iken; internet aracılığıyla bir elektronik ticaret sitesinden alınan elbisenin tüketici tarafından sadece sitede bulunan

[2] RG 14.03.2004, sy.25048
[3] RG 13.03.2003, sy.25137
[4] Atamer, Tüketicinin Korunması Hakkında Kanun M.9/A ve Mesafeli Sözleşmelere İlişkin Uygulama Usul ve Esasları Hakkında Yönetmelik'in Avrupa Birliği Mevzuatı İle Uyumuna İlişkin Görüş ve Değişiklik Önerileri, http://www.bilisimsurasi.org.tr/hukuk/docs/yesim_atamer_rapor.doc, s. 1
[5] RG 09.10.2007, sy.26668

görseller, animasyonlar ve elbise ile ilgili verilen bilgiler doğrultusunda incelenmesi mümkün olabilecektir. Böyle bir durumda kötü niyetli bir satıcının tüketiciyi aldatması çok kolay bir hale gelebileceği gibi, görseller ve bilgiler aracılığıyla inceleme yapan tüketicinin de aslında almak istediği mal dışında bir malın, almak istediği mal olduğunu zannetmesi oldukça muhtemeldir.

Açıklanan sebeplerle, yasa koyucular; internet ve benzeri iletişim araçlarıyla gerçekleştirilen alış veriş işlemlerinde tüketiciyi korumak ve elektronik ticareti daha güvenli bir hale getirmek amacıyla, tüketicilerin detaylı bir şekilde bilgilendirilmesi ve almak istedikleri dışında bir malla karşılaşmaları halinde her hangi bir sebep göstermeden bu maldan vazgeçebilmeleri haklarını düzenleyen düzenlemeler geliştirmişlerdir.

Tüketici hakları, Tüketicinin Korunması Hakkında Kanun (TKHK) ile düzenlenmekte ve kapsamı "Tüketici tanımı çerçevesinde belirlenmektedir. Tüketici Kanunu'nda bir mal veya hizmeti ticari veya mesleki olmayan amaçlarla edinen, kullanan veya ondan yararlanan gerçek ya da tüzel kişi olarak belirlenmiştir. Tanım içerisinde belirtilen "Ticari veya mesleki olmayan amaçlarla edinme" şartı uygulamada farklı şekillerde anlaşılsa da genel olarak temin edilen mal veya hizmetin şahsi amaçlarla tüketilmesi anlamına gelmektedir. Buna göre ticari veya mesleki amaçlarla, internet üzerinden alınan mallarda yapılan sözleşmelerde ve işlemlerde TKHK kapsamı içerisine girilmeyecek ve bu bölümde belirtilen mesafeli sözleşmeler ile ilgili sürecin kurulması gerekmeyecektir.

Yukarıda açıklandığı üzere, satın alan kişinin TKHK kapsamında tüketici kapsamına girdiği durumlarda, elektronik ortamda gerekleştirilen ve tarafların fiziken karşı karşıya bulunmadığı durumlarda mesafeli sözleşmeler uygulanacaktır. Ancak tarafların fiziksel olarak karşı karşıya bulunduğu ve alıcının mal veya hizmeti tetkik etme şansı bulunduğu durumlarda, alış onayı internet üzerinden veya mobil araçlar aracılığıyla verilse ve ödeme elektronik ortamdan geçekleştirilse dahi, yapılan alışveriş işlemi mesafeli sözleşme kapsamına girmeyecektir.

TKHK'da yapılan satıcı tanımı da gerçekleştirilen alışveriş işleminin mesafeli sözleşme kapsam içerisine girip girmediğinin belirlenmesinde etkili olmaktadır. Şöyle ki; TKHK'ya göre satıcı "Kamu tüzel kişileri de dahil olmak üzere ticari veya mesleki faaliyetleri kapsamında tüketiciye mal sunan gerçek veya tüzel kişiler" olarak tanımlamıştır. Bu durumda tanım ile belirlenen "ticari ve mesleki faaliyetleri kapsamı" dışında internet üzerinden elektronik ticaret siteleri aracılığıyla satış yapan kişilerin gerçekleştirdikleri

satış işlemleri de mesafeli sözleşme kapsamı içerisine girmeyecektir. Örnek vermek gerekirse, özellikle ikinci el ürünlerin satışının yapıldığı ve/veya açık artırma usulüyle satışların gerçekleştirildiği alışveriş ve ilan sitelerinde gerçekleştirilen satışlar mesafeli sözleşme sürecine ihtiyaç duymadan gerçekleştirilebilmektedir. Ancak bu portallar üzerinden olsa dahi, söz konusu mal ve hizmet satışı işini ticari veya mesleki faaliyet haline getirmiş kişilerin yaptıkları işlemler uygulamada mesafeli sözleşme süreci içerisinde değerlendirilmektedir. Uygulamadaki iş modelleri incelendiğinde gerçekten bazı satıcıların, bu internet siteleri üzerinde oluşturulan sanal dükkanlarda çeşitli mal ve hizmet satışlarını gerçekleştirdikleri görülmektedir. Mesafeli sözleşmeler ile ilgili denetleme yetkisine sahip regülatör kurum olan Sanayi ve Ticaret Bakanlığı da yaptığı denetimlerde belirli kriterler belirleyerek (satılan mal sayısı, üyelik statüsü), bu kriterler üzerinde kalan kullanıcıların işlemlerini mesafeli sözleşme prosedürü kapsamında saymakta ve bu prosedüre uymayan kullanıcılara idari para cezası yaptırımında bulunmaktadır.

Bu doğrultuda dikkat edilmesi gereken husus; yukarıda bahsedildiği şekilde üyelerin birbirleri arasında alışveriş yapmaları amacıyla bir internet sitesinin kurulmasının amaçlanması halinde, site tasarımı gerçekleştirilirken, belirli kriterlerin üzerinde kalan alışverişlerde taraflar arasında mesafeli sözleşmenin gerçekleştirilmesi gereken alt yapının kurulmasının da göz önünde bulundurulmak zorunda olduğudur. Bu şekilde çalışan internet sitelerinde kullanıcı konumunda bulunuluyor ise, bu defa üyesi bulunan internet sitesinin söz konusu alt yapıya sahip olup olmadığı sorgulanmalıdır; zira mesafeli sözleşme prosedürü uygulamak zorunda olan satıcı olduğu için böyle bir alt yapının bulunmaması halinde, idari para cezası satıcı konumundaki kullanıcıya kesilecektir.

Mesafeli sözleşme prosedürü, yukarıda belirtilen şartların oluşmasına rağmen (tüketici ve satıcı tanımı, fiziksel olarak karşı karşıya bulunmama) bazı sözleşme türlerinde uygulanamamaktadır. MSHY'nin 11. maddesiyle istisna olarak belirlenen ve mesafeli sözleşme prosedürü içerisine dahil edilmeyen sözleşme türleri şunlardır:

a. Banka, sigorta ile ilgili,
b. Otomatik satış makineleri vasıtasıyla akdedilen,
c. Halka açık jetonlu telefonlar vasıtasıyla akdedilen,
d. Açık arttırma yolu ile akdedilen,
e. Gıda, içecek ve günlük tüketim için tüketicinin evine veya iş yerine düzenli olarak sağlanan malların tedariki ile ilgili,

f. Sağlayıcının üstlendiği, barınma, ulaşım, yemek tedariki, sportif ve kültürel faaliyetler ve eğlence hizmetlerini özel bir günde veya sürede tedarik etmesine ilişkin hükümler içeren sözleşmeler.

2.1.2. ÖN BİLGİLENDİRME YÜKÜMLÜLÜĞÜ ve SÖZLEŞME DÜZENLEME SÜRECİ

MSHY'nin 7. maddesine göre, mesafeli sözleşmenin tüketici tarafından kullanılabilir veya sürekli olarak erişilebilir başka bir sürekli veri taşıyıcısıyla tüketiciye verilmesi zorunludur. MSHY'de yapılan değişiklikle getirilen bu yeni düzenleme ile satıcı/sağlayıcının tüketiciye kağıt ortamında yazılı olarak sözleşme vermesi engellenmiş bulunmaktadır zira madde metnine göre sözleşme sadece "Sürekli veri taşıyıcısı" ile verilebilecektir. Sürekli veri taşıyıcısı MSHY'de "Tüketicinin, kendisine kişisel olarak gönderilen bilgiyi, bu bilginin amacına uygun olarak makul bir süre incelemesine elverecek şekilde kaydedilmesini sağlayan ve kaydedilen bilgiye aynen ulaşılmasına imkan veren her türlü araç" olarak tanımlanmıştır. MSHY'de değişiklik yapılmasının amacı, değişiklik öncesi sözleşmenin yazılı yapılması ve tüketiciye teslim edilmesi zorunluluğunun mevcut ticaret hayatının koşullarına uymaması ve MSHY hükümlerinin uygulanamamasıdır[6].

MSHY'nin 7. maddesine göre aşağıdaki bilgilerin mesafeli sözleşme içerisinde bulunması gerekmektedir.

---

[6] Mesafeli sözleşmelerin yazılı şekil ile yapılması zorunluluğu ile ilgili düzenleme MSHY'de ile yapılan değişiklik ile ortadan kaldırılmış gibi gözükse de TKHK'nın 6. maddesinde açıkça;

"6/A, 6/B, 6/C, 7, 9, 9/A, 10, 10/A ve 11/A maddelerinde yazılı olarak düzenlenmesi öngörülen tüketici sözleşmeleri en az oniki punto ve koyu siyah harflerle düzenlenir ve sözleşmede bulunması gereken şartlardan bir veya birkaçının bulunmaması durumunda eksiklik sözleşmenin geçerliliğini etkilemez. Bu eksiklik satıcı veya sağlayıcı tarafından derhal giderilir."

hükmü bulunmaktadır. Maddedeki 9/A maddesinde yazılı olarak düzenlenmesi öngörülen tüketici sözleşmeleri hükmü doğrultusunda 9/A maddesine bakıldığında ilk etapta maddede yazılı şekil şartından bahsedilmediği için sözleşmenin yazılı şekil şartına tabi olup olmadığı tartışılır mahiyette gözükmektedir. Ancak 9/A maddesinde ayrıca:

"Cayma hakkı süresince sözleşmeye konu olan mal veya hizmet karşılığında tüketiciden herhangi bir isim altında ödeme yapmasının veya borç altına sokan herhangi bir belge vermesinin istenemeyeceğine ilişkin hükümler dışında kapıdan satışlara ilişkin hükümler mesafeli sözleşmelere de uygulanır."

hükmü bulunduğu için şekil şartına ilişkin hususlarda da kapıdan satışlara ilişkin hükümlerin uygulanacağı ortaya çıkmaktadır. Kapıdan satışlara ilişkin 9. maddede de:

"Tüketici, sahip olduğu haklarının da yazılı bulunduğu sözleşmeyi imzalar ve kendi el yazısı ile tarihini yazar. Satıcı veya sağlayıcı, bu bilgilerin sözleşmede yer almasını sağlamak ve taraflar arasında akdedilen sözleşmenin bir nüshasını tüketiciye vermekle yükümlüdür."

şeklinde bir hüküm bulunmaktadır. Maddeye göre tüketici ile yapılan sözleşme yazılı olmak zorunda olduğu gibi ayrıca tüketici tarafından kendi el yazısı ile imzalanmak ve tarih atılmak zorundadır. TKHK'daki mesafeli sözleşmelerin şekil ile ilgili bu düzenlemesi sebebiyle MSHY'de sözleşmelerin elektronik ortamdan gönderilmesine ilişkin yapılan değişikliğin uygulanması mümkün değildir, zira Kanun ile belirlenmiş bir husus Yönetmelik ile değiştirilemez. Kanaatimizce mesafeli sözleşmeler yazılı olarak yapılmaya devam edilmelidir.

a. Tüketicinin, satıcı veya sağlayıcının isim, unvan, açık adres, telefon ve varsa diğer erişim bilgileri,
b. Sözleşmenin düzenlendiği tarih,
c. Malın veya hizmetin teslim veya ifa tarihi ve şekli,
d. Teslimat ve ifaya ilişkin masrafların tutarı ve kimin tarafından karşılanacağına dair bilgiler,
e. Sözleşme konusu malın veya hizmetin cinsi veya türü, miktarı ve varsa marka ve modeli,
f. Malın veya hizmetin Türk Lirası olarak vergiler dahil peşin satış fiyatı,
g. Vadeye göre faiz ile birlikte ödenecek Türk Lirası olarak toplam satış fiyatı,
h. Faiz miktarı, faizin hesaplandığı yıllık oran ve sözleşmede belirtilen faiz oranının yüzde otuz fazlasını geçmemek üzere gecikme faizi oranı,
i. Peşinat tutarı,
j. Ödeme planı,
k. Borçlunun temerrüde düşmesinin hukuki sonuçları,

Bilgilendirme yükümlülüğü de TKHK md. 9/A'da düzenlenmiştir, buna göre;

"Mesafeli satış sözleşmesinin akdinden önce, ayrıntıları Bakanlıkça çıkarılacak tebliğle belirlenecek bilgilerin tüketiciye verilmesi zorunludur. Tüketici, bu bilgileri edindiğini yazılı olarak teyit etmedikçe sözleşme akdedilemez. Elektronik ortamda yapılan sözleşmelerde teyid işlemi, yine elektronik ortamda yapılır."

Maddede söz edilen bilgilerin ne olduğu tebliğ ile değil MSHY ile belirlenmiştir. MSHY'nin 5. maddesine göre aşağıdaki bilgilerin sözleşmenin akdinden önce tüketiciye verilmesi zorunludur;

a. Satıcı veya sağlayıcının isim, unvan, açık adres, telefon ve varsa diğer erişim bilgileri,
b. Sözleşme konusu mal ya da hizmetin temel özellikleri,
c. Sözleşme konusu mal ya da hizmetin tüm vergiler dahil satış fiyatı,
d. Satıcı veya sağlayıcının fiyat dahil tüm vaatlerinin geçerlilik süresi,
e. Tüketicinin ödemelerinin nasıl yapılacağına dair bilgiler,
f. Teslimat ve ifanın nasıl yapılacağına ve varsa buna ilişkin masrafların tutarı ve kimin tarafından karşılanacağına dair bilgiler,
g. Cayma hakkı ve bu hakkın nasıl kullanılacağına dair bilgiler,
h. Tüketiciye bir maliyeti varsa kullanılan iletişim yollarının ücreti,
i. Sözleşme konusu mal ya da hizmetin, teslim ve ifa tarihlerine ilişkin program,

j. Tüketicinin talep ve şikayetlerini iletebileceği satıcı veya sağlayıcının açık adres, telefon ve varsa diğer erişim bilgileri.

MSHY'nin 5. maddesine göre söz konusu bilgiler "Bilgilendirme formunun verilmesi suretiyle açık, anlaşılır ve kullanılan iletişim vasıtasına uygun bir şekilde" tüketiciye sunulmalıdır. Ayrıca MSHY'de yapılan değişiklikle "Sözlü iletişim araçlarının kullanılması durumunda, ayrıca satıcı veya sağlayıcının, kimliğini ve görüşmenin ticari amacını her görüşmenin başında tüketiciye açık bir biçimde bildirmesi" zorunluluğu getirilmiştir.

Söz konusu bilgilerin tüketici tarafından alındığının yazılı olarak, elektronik ortamda yapılan sözleşmelerde ise elektronik olarak teyit edilmesi gerekmektedir[7]. Teyit işlemi elektronik ortamda tüketicinin iradesini göstermesini sağlayacak herhangi bir teknikle yapılabilir. Teyit işleminin yapılmaması halinde TKHK 9/A'ya göre sözleşme akdedilemeyecektir. Sözleşmenin akdedilemeyecek olmasının hukuki sonucu kanaatimizce sözleşme öncesi bir şart yaratılmış olması, şarta bağlı bir sözleşme yapma yasağı oluşturulmuş olması durumudur. Burada tarafların iradesinden önce bir şart konulmuş, bu şartın gerçekleşmesi halinde taraf iradelerinin sözleşme olarak kabul edilecek şekilde sonuç doğurabileceği düzenlenmiştir[8].

MSHY'nin 6. maddesine göre satıcı veya sağlayıcı, mallar için sözleşme konusu mal tüketiciye ulaşmadan, hizmetler için de en geç sözleşmenin ifasından önce yazılı olarak, elektronik ortamda yapılan sözleşmelerde ise tüketici tarafından kullanılabilir veya sürekli olarak erişilebilir başka bir sürekli veri taşıyıcısıyla bilgilendirme formunu tüketiciye ulaştırmak zorundadır.

Yukarıda belirtilen hususlardan sonra, burada uygulamada bilgilendirme yükümlülüğünün ve sözleşmenin düzenlenmesinin ve onaylanmasının ne şekilde olabileceği üzerine senaryolardan bahsetmenin faydalı olacağını düşünüyoruz. Oldukça karmaşık ve anlaşılması zor olan mevzuatın, uygulamadaki örneklere bakıldığında regülatör kurumun yönlendirmeleri sonucunda yorumlandığı görülmektedir. Öncelikle bilgilendirme yükümlülüğünün bir kısmının, internet sitelerinin yardım bölümlerinde yer alan kuralların kullanıcının erişimine açık hale getirilmesinin söz konusu yükümlülüğün yerine getirilmesi olarak kabul edildiği görülmektedir. Bunun dışında

[7] Mehaz Yönerge'de bilgilere ilişkin yazılı teyidin satıcı/sağlayıcı tarafından verilmesi öngörülmüştür; Atamer, s. 3

[8] Arslan'a göre söz konusu düzenleme sözleşmenin geçersizliğine değil TKHK 25. madde doğrultusunda para cezasına ve tüketicinin bu durumdan kaynaklanan zararlarının satıcı/sağlayıcı tarafından karşılanmasına sebebiyet verecektir; Arslan, Tüketici Hukuku Dersleri, Bursa, 2006 s. 249

bilgilendirme yükümlülüğü içerisinde yer alan satılacak malla ilgili bilgilerin alıcıya satıştan önce gösterilmesi ve onayının alınması (teyid) yükümlülüğünün ise, satış onaylama sayfasından önce MSHY ile belirlenen malla ilgili bilgilerin yer aldığı bir formun alıcıya gösterilmesi, bu formun onaylanması halinde satış onay bölümüne geçilmesi şeklinde yerine getirildiği görülmektedir.

Bilgilendirme formunun ve sözleşmenin kullanıcıya verilmesi yükümlülüğünün ise kullanıcının internet sitesine bildiği e-posta adresine e-posta olarak gönderilmesi veya satıştan sonra kendisine internet sayfası içerisinde gösterilmesi gibi yöntemlerle karşılandığı görülmektedir.

Yukarıda belirtilen yöntemler, mesafeli sözleşme akdeden kişi ve kurumların denetlenmesi hususunda yetkili regülatör kurum olan Sanayi ve Ticaret Bakanlığı'nın uygulamalarından gözlemlendiği kadarıyla uygun bulunmaktadır. Kanaatimizce ilgili kurumun bu yöntemleri uygun bulması yasal uyumluluk denetimi için yeterli olsa da çeşitli problemler sebebiyle doğabilecek uyuşmazlıklarda mevzuatı yorumlayacak Tüketici Mahkemeleri ve/veya Tüketici Heyetleri tarafından mevzuatın farklı yorumlanması sebebiyle uygun bulunmayabilir.

Yukarıda bahsedilen yöntemler, mevzuatın ortaya koyduğu isterler ve mevcut iş kuralları birlikte düşünüldüğünde uyuşmazlıkta sorun olarak karşımıza çıkabilecek hususlar, sözleşme ve bilgilendirme formunun usulüne uygun düzenlenip düzenlenmediği ve bunların tüketiciye gönderilip gönderilmediği konusundaki tartışmalar olabilecektir.

Bu tür sorunların yaşanmaması için yukarıda bahsedildiği üzere TKHK ve MSHY arasındaki sözleşmenin şekli ile ilgili kanaatimizce oluşan ayrılığın ortadan kaldırılabilmesi için yine kanaatimizce en uygun yöntem otomatik bir süreçte yaratılan sözleşmelerin yine otomatik bir süreçte Elektronik İmza Kanunu (EİK) kapsamında güvenli elektronik imza ile imzalanarak yaratılmasıdır. Aşağıda ilgili bölümde detaylı olarak anlatılacağı üzere, EİK kapsamında bir güvenli elektronik imza ile imzalanan bir elektronik metin hukuken yazılılık şartını taşımakta böylece MSHY'nin yanı sıra TKHK'nın 6, 9 ve 9/A maddeleri uyarınca talep edilen yazılılık şartını karşılamaktadır.

Uyuşmazlığa konu olabilecek bir diğer sorun olan, sözleşme ve bilgilendirme formunun tüketiciye gönderilip gönderilmediği hususunun çözümü ise, kanaatimizce, mevcut uygulamada da yapıldığı üzere bunların kullanıcının bildirdiği e-posta adresine gönderilmesidir. Ancak bu gönderme işlemiyle

ilgili hukuki durumun (sözleşme ve bilgilendirme formunun kulacının kendi bildiği e-posta adresine gönderileceği ve bu gönderme işleminin TKHK ve MSHY ile belirlenen tüketiciye teslim şartını yerine getirdiğini ve kullanıcının bu hususları kabul ve beyan ettiği) ayrıca kullanıcının siteye ilk üye olurken akdettiği kullanıcı sözleşmesi içerisinde yer alması gerekmektedir.

Sözleşme ve bilgilendirme formunun tüketiciye geçerli bir şekilde tesliminin elektronik ticaret içerisinde hukuki olarak çok büyük bir önemi bulunmaktadır. MSHY'nin 8. maddesinin son fıkrasına göre:

"Satıcı veya sağlayıcının 6'ncı veya 7'nci maddede belirtilen yükümlülüklerini (sözleşme ve ön bilgilendirme formu) yerine getirmemesi halinde, satıcı veya sağlayıcı en geç otuz gün içerisinde eksikliği giderir. Bu durumda yedi günlük süre, söz konusu eksikliğin giderildiğine dair bilginin yazılı olarak tüketiciye ulaştırıldığı tarihten itibaren başlar. Aksi takdirde, tüketici cayma hakkını kullanmak için yedi günlük süre ile bağlı değildir."

Maddede belirtildiği üzere bu belgeler teslim edilmeden cayma hakkı ile ilgili 7 günlük süre başlamamaktadır; yani bu yükümlülükler yerine getirilmeden tüketici her zaman aldığı malı herhangi bir sebep göstermeden iade etme hakkına sahiptir.

2.1.3. CAYMA HAKKI

MSHY'nin 8. maddesine göre:

"Tüketici; mal satışına ilişkin mesafeli sözleşmelerde, teslim aldığı tarihten itibaren yedi gün içerisinde hiçbir hukuki ve cezai sorumluluk üstlenmeksizin ve hiçbir gerekçe göstermeksizin malı reddederek sözleşmeden cayma hakkına sahiptir. Hizmet sunumuna ilişkin mesafeli sözleşmelerde ise, bu süre sözleşmenin imzalandığı tarihte başlar. Sözleşmede, hizmetin ifasının 7 günlük süre dolmadan yapılması kararlaştırılmışsa, tüketici ifanın başlayacağı tarihe kadar cayma hakkını kullanabilir. Cayma hakkının kullanımından kaynaklanan masraflar satıcı veya sağlayıcıya aittir."

Cayma hakkı, maddede belirtildiği şekilde belirli bir süre içerisinde tüketicinin herhangi bir sebep göstermeden malı iade edebilme hakkıdır. Bu hususun, malda çıkan bozukluk, eksiklik sebebiyle iadesiyle karıştırılmaması gerekmektedir. Yukarıda detaylı bir şekilde açıkladığımız üzere, elektronik ortamda yapılan satışlarda tüketicinin ayrıca korunması amacıyla böyle bir

prosedür geliştirilmiştir. Tüketici elektronik ticaret yöntemiyle internet üzerinden aldığı bir malı teslim aldığı tarihten itibaren yedi gün içerisinde herhangi bir sebep göstermeden iade edebilecektir. Bu iade hakkı içerisinde, malın genel kullanımından kaynaklanan eskime de satıcı tarafından geri almama için bir sebep olarak gösterilemeyecektir. Kanaatimizce internet üzerinden mal veya hizmet satışı gerçekleştirmek isteyen bir elektronik ticaret girişimcisi için göz önünde bulundurulması gereken en büyük risklerden biri bu durumdur. Risk mal satışlarında tamamen kendini gösterirken, hizmet sunumlarında en azından bu hak hizmetin ifasına kadar kullanılabilmektedir. Riskin hesaplanmasında göz önünde bulundurulması gereken başka bir husus ise cayma hakkının kullanımından kaynaklanan masrafların satıcı veya sağlayıcı tarafından karşılanacak olmasıdır; buna göre alıcının malı veya hizmeti cayma hakkını kullanarak iade etmesi durumunda geri iadeye ilişkin kargo ve benzeri masraflar satıcı veya sağlayıcı tarafından karşılanacaktır.

TKHK ve MSHY ile düzenlenen cayma hakkına MSHY içerisinde bazı sınırlar getirilmiştir. MSHY'nin 8. maddesine göre:

"Elektronik ortamda anında ifa edilen hizmetler ve tüketiciye anında teslim edilen mallara ilişkin sözleşmeler cayma hakkı ve kullanımına ilişkin hükümlere tabi değildir".

"Tüketicinin özel istek ve talepleri uyarınca üretilen veya üzerinde değişiklik ya da ilaveler yapılarak kişiye özel hale getirilen mallarda tüketici cayma hakkını kullanamaz. Ayrıca tüketici, niteliği itibariyle iade edilemeyecek, hızla bozulma veya son kullanma tarihi geçme ihtimali olan mallar söz konusu olduğunda cayma hakkını kullanamaz."

MSHY'deki bu düzenleme ile cayma hakkının kullanılabileceği alanlar sınırlandırılmıştır. Buna göre elektronik ortam üzerindeki mal ve hizmetler, müşterinin talepleri doğrultusunda değiştirilen veya oluşturulan ürünler ile çabuk bozulan ürünler cayma hakkı kapsamına girmeyecektir.

2.2. e-TİCARETTE VERİ KORUMASI ve MAHREMİYETİ

Elektronik ticarette veri koruması ve mahremiyet konusu, elektronik ticaret firması tarafından toplanan tüketici bilgilerinin korunması, bu bilgilerin kullanılmasının sınırları ve yöntemleri ile bu bilgilerin hukuka aykırı kullanımı karşısında oluşabilecek suçlar kapsamında incelenmelidir.

2.2.1. KULLANICI BİLGİLERİNİN KORUNMASI

Elektronik ticaret firmaları, kullanıcılarını tanımlayabilmek için kullanıcılarının kişisel bilgilerini ve kullanıcıları tarafından belirlenen bazı bilgileri saklamakta ve işlemektedirler. Bu bilgilerin dışında kullanıcıların yaptıkları alışverişlerle veya elektronik ticaret firmasının faaliyetleri doğrultusunda kullanıcının yaptığı işlemlerle ilgili bilgiler de hizmetin kapsamında veya hizmetin kalitesinin arttırılması amacıyla korunmaktadır.

Elektronik ticaret firması yukarıda belirtilen verileri basiretli tüccar gibi davranma ilkesi altında ortaya koyulan bilgi güvenliği ile ilgili sorumluluğu doğrultusunda korumakla ve yine bu doğrultuda kullanmak ve işlemekle yükümlüdür. Elektronik ticaret firması ticaret hukuku kapsamında tüccar olarak değerlendirileceğinden basiretli tüccar gibi davranma yükümlülüğüne sahiptir. Basiretli tüccar gibi davranma ilkesi Yargıtay tarafından şu şekilde açıklanmıştır: *"Tacirin, ticari işletmesiyle ilgili tüm faaliyetlerinde basiretli bir iş adamı gibi davranması gerekir. Bu cümleden olarak ticari işletmesiyle ilgili sözleşmeleri yaparken ve bu sözleşmelerden doğan borçlarını yerine getirirken basiretli bir iş adamı gibi davranmak zorundadır.*[9]". Bu doğrultuda basiretli tacir, sözleşme ile üstlendiği yükümlülüklerini yerine getirirken, tedbirli ve "İşini iyi yapan" bir tacir gibi davranmak zorundadır. bu kriterlerin belirlenmesinde sözleşme konusu işin yerine getirilmesi için ülkedeki ve dünyadaki pratikler doğrultusunda oluşan ticari kurallar gözetilir. Dünyadaki ve ülkemizdeki iş pratiklerine bakıldığında da, yukarıda belirtilen kapsamdaki kullanıcı verilerinin bu verileri toplayan, saklayan ve işleyen elektronik ticaret firması tarafından sıkı bir şeklide korunduğu ve ancak kullanıcının izni doğrultusunda izin verilen kapsam ve sınırlarda kullanıldığı görülmektedir.

Bu iş pratiklerinin dışında kullanıcı verilerinin gereğince korunmaması, kullanılması, saklanması veya üçüncü şahıslara verilmesi, elektronik ticaret firmasının basiretli tacir gibi davranmamasına yol açacak ve ortaya çıkacak zararda kusurlu olmasına ve bu zararı tazmin etmek zorunda kalmasına sebebiyet verebilecektir.

2.2.2. KULLANICI BİLGİLERİNİN KULLANILMASININ YÖNTEMLERİ ve SINIRLARI

Yukarıda açıklandığı üzere, kullanıcı bilgilerinin hukuka aykırı kullanılması elektronik ticaret firmasının hukuki sorumluluğunu yaratabileceği gibi bir

[9] Yargıtay Hukuk Genel Kurulu E. 2000/19-1255 esas, 11.10.2000 tarihli kararı

sonraki bölümde anlatılacağı üzere cezai sorumluluğuna da yol açabilecektir. Bu sebeple kullanıcı bilgilerinin toplanması, saklanması, işlenmesi ve üçüncü kişilere iletilmesi ancak bazı şartlar halinde uygulanmalıdır. Bu şartların başında ise kullanıcıdan izin alınması hususu gelmektedir.

Kullanıcıdan kullanıcı verileri ile ilgili izin alınması işlemi, kullanıcıların onayladıkları kullanıcı sözleşmelerinin hükümleri içerisinde gerçekleştirilebileceği gibi, ilgili işlemden önce ayrı bir prosedür ile de (kullanıcıya ayrı bir onay ekranı açılıp onayının alınması) gerçekleştirilebilir. Burada önemli olan açık ve net bir şekilde kullanıcının hangi bilgilerinin, hangi amaçlarla, ne kadar süreyle, saklanacağı/işleneceği/üçüncü kişilerle paylaşılacağının metin içerisinde belirtilmesi gerekliliğidir. Kullanıcının her zaman için bu şartları kabul etmeme hakkı bulunmalıdır. Bu şartların kabul edilmemesi halinde kullanıcının üyelik statüsü kabul edilmeyebilir.

Üyelik statüsü gerektirmeden işlem yapılan elektronik ticaret sitelerinde ise, kullanıcının herhangi bir çaba harcamadan rahatlıkla görüp okuyabileceği bir alanda, kullanıcının bilgilerinin kullanımı, saklanması, işlenmesi ve gerekiyorsa üçüncü kişilere verilmesi ile ilgili şartlar bulunmalı, kullanıcının bu şartları kabul etmemesi halinde elektronik ticaret sitesini kullanmaması gerektiği belirtilmelidir. Burada önemle belirtmek gerekir ki, üyelik statüsü gerektirmeyen uygulamalarda, bu şekilde bir kullanım, kullanıcının açık onayının alınmaması sebebiyle her zaman için tartışma konusu olabilecektir. Olası bir uyuşmazlıkta, genel olarak dünyada kullanılan elektronik ticaret pratikleri de göz önünde bulundurularak, kullanıcının bilgilerinin kullanılmasıyla ilgili şartları bilip bilmediği ve buna göre hareket edip etmediği araştırılmalıdır. Burada kullanıcının fiillerinin sonuçları değerlendirilirken kullanıcının tüccar mı tüketici mi olduğu, hareketlerinin sonuçlarının belirlenmesinde önemli olacaktır. Kullanıcının da tüccar olması halinde onun da basiretli tüccar gibi davranması beklenmeli ve sitede belirtilen şartlardan haberdar olduğu kabul edilmelidir. Ancak tüketicide de bu durumda daha esnek kabul edilmeli ve ilgili şartların daha belirgin olarak yer alması aranmalıdır. Elektronik ticaret sitesinde kullanıcı bilgilerinin kullanılması ile ilgili şartların dünyadaki elektronik ticaret pratikleri de göz önünde bulundurularak, site kullanım koşulları ve mahremiyet politikası (privacy policy) bölümleri içerisinde yer almasında fayda vardır.

2.2.3. KULLANICI VERİLERİNİN HUKUKA AYKIRI ELDE EDİLMESİ ve KULLANILMASI

Kullanıcı verilerinin hukuka aykırı bir biçimde elde edilmesi, saklanması,

kullanılması, işlenilmesi ve üçüncü kişilere verilmesi yukarıda bahsedildiği üzere hukuki ve cezai sorumluluk doğurabilecektir. Hukuki sorumluluk, bu fiillerden dolayı maddi bir zarar doğması halinde zararın tazmin edilmesine yol açacak, cezai sorumluluk ise fiilin suç olarak değerlendirilmesi halinde para veya hapis cezası sonucunu doğurabilecektir. Kullanıcı bilgilerinin korunması bölümünde hukuki sorumluluktan bahsedildiği için bu bölümde cezai sorumluluktan bahsedilecektir.

Kullanıcı verilerinin hukuka aykırı kullanılmasında cezai sorumluluk yorumlanırken, kullanıcı verilerinin kişisel veriler ve kişisel olmayan veriler olarak ayrıştırılması gerekmektedir. Kişisel verilerin ne olduğu mevcut yasal mevzuatımız içerisinde belirtilmiş olmayıp[10], söz konusu tanım için Avrupa Birliği'nin Kişisel Verilerin Korunması'na Dair 95/46/EC sayılı Yönergesi doğrultusunda bir yorum yapılabilir. Yönergeye göre kişisel veri *"Belirli veya belirlenebilir gerçek kişiyle ilgili tüm bilgiler"dir. Yönerge belirlenebilir bir gerçek kişiyi ise "Özellikle bir id numarasına referans yapılmak suretiyle veya belirli fiziksel, psikolojik, ruhsal (zihinsel), ekonomik, kültürel ya da sosyal kimliği ile ilgili bir ya da birden fazla faktöre bağlı olarak doğrudan ya da dolaylı olarak tespit edilen veya tespit edilebilen kişi"* olarak tanılamıştır. Kanaatimizce, Yönerge ile belirlenen tanım, mevzuatımız ile belirlenen kişisel verilere ilişkin suçların yorumlanmasında da kullanılabilecektir. Bu tanım içerisine girmeyen bilgiler kişisel veri olarak kabul edilmeyecektir.

Türk Ceza Kanunu'nda (TCK) kişisel verilerin hukuka aykırı bir şekilde kaydedilmesi, ele geçirilmesi, üçüncü kişilere verilmesi ve yok edilmemesi suç olarak düzenlenmiştir. TCK'nın 135. maddesi şu şekildedir:

Kişisel verilerin kaydedilmesi
MADDE 135. *- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.*

Maddedeki hukuka aykırılık öncelikle yukarıda belirtildiği gibi kullanıcıdan izin alınmaması olarak yorumlanmalıdır. Ancak yapılan işin zorunlu olarak gerektirmesi ve kullanıcının menfaatine zarar verilmemesi halinde izin alınmaması, kanaatimizce, bu duruma istisna olarak kabul edilmelidir.

[10] Bilgi ve İletişim Teknolojileri Kurumu tarafından çıkartılan Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik'te kişisel veri tanımı şu şekilde yapılmıştır: "Tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi". Bu tanım da Avrupa Birliği'nin Kişisel Verilerin Korunmasına Dair 95/46/EC sayılı Yönergesinde yapılan tanımla tamamen uyumlu olup, düzenleme yasa düzeyinde olmaması sebebiyle metin içerisinde Yönerge ile belirlenen tanım tercih edilmiştir.

Kullanıcının izni olsa dahi mevzuata aykırı bir şekilde verilerin kaydedilmesi de ayrıca bu suç kapsamında sayılacaktır.

TCK'nın 135. maddesinin ikinci fıkrası şu şekildedir:

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

Görüldüğü üzere maddenin ikinci fıkrasında kişisel verilere örnek verilerek bazı durumlar için hukuka aykırılık şartı kaldırılmış (veya ayrıca hukuka aykırılık araştırmasının yapılmasına gerek kalmadan bu durumların kendiliğinden hukuka aykırılık yarattığı belirlenmiştir) ve bu nitelikteki verilerin de kaydedilmesinin suç kapsamına gireceği belirtilmiştir.

TCK'nın 136. maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesinden ayrıca, bu verilerin hukuka aykırı olarak verilmesi, yayılması veya ele geçirilmesi halinde ayrıca ceza düzenlenmiştir. Burada dikkat edilmesi gereken verilerin hukuka uygun olarak (izin alınarak) kaydedilmesine rağmen hukuka aykırı olarak (izin alınmadan) üçüncü kişilere verilmesi halinde söz konusu fiilin suç kapsamında değerlendirebileceğidir. TCK'nın 137. maddesinin ikinci fıkrasında da 135 ve 136. maddelerde belirtilen suçların "Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle" işlenmesi halinde ilgili cezanın yarı oranında arttırılacağı belirtilmiştir. Elektronik ticaret kapsamında kişisel verilerin toplanmasının "Belli bir mesleğin sağladığı kolaylıktan yararlanmak suretiyle" kapsamına girdiği tartışılmaz bir husustur.

TCK'nın 138. maddesinde ise "Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde" altı aydan bir yıla kadar hapis cezası verileceği belirlenmiştir. Burada dikkat edilmesi gereken husus ise, bu suçun ancak kanunla belirlenen sürelerin geçmiş olması halinde uygulanacağıdır. Kanunla belirlenen bir süre bulunmaması halinde bu maddenin uygulanmaması mümkün değildir. Mevcut mevzuatta elektronik ticaret firmalarının faaliyetleri doğrultusunda sakladıkları kişisel verileri ne kadar süre ile saklayacaklarına ilişkin bir hüküm bulunmamakla birlikte yakın zamanda yapılacak ilgili mevzuat çalışmaları ile bu şekilde bir sürenin belirlenmesi muhtemeldir.

Elektronik ticaret firmasının sakladığı bilgilerin, kişisel veri kapsamında olmaması ancak bu verilerin ticari sır, bankacılık sırrı veya müşteri sırrı kapsamında olması halinde ise TCK'nın 239. maddesi uygulama alanı bulabilecektir. Maddeye göre "Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi hâlinde de bu fıkraya göre cezaya hükmolunur." Maddede belirtilen kriterler içerisinde mesleği gereği sırlara vakıf olunması şartı kesinlikle çeşitli iş modelleri içerisinde çalışan elektronik ticaret firmalarının faaliyetleri kapsamı içerisinde sayılabilecektir. Özellikle B2B alanda ve güvenilir üçüncü parti (trusted third party) olarak belirlenmiş iş modelleri içerisinde faaliyet gösteren elektronik ticaret firmalarının, müşterisi olan firmaların ticari sırlarını mesleki faaliyetleri doğrultusunda öğrenmesi ve kayıtlarına geçirmesi muhtemeldir. Bu doğrultuda söz konusu firmaların müşterilerinin ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki verilerini müşterilerinden izin almadan üçüncü kişilere vermesi veya ifşa etmesi halinde, söz konusu fiil TCK'nın 239. maddesi kapsamında suç sayılabilecektir.

Kullanıcı verilerinin hukuka aykırı kullanımıyla ilgili başka bir düzenleme ise Banka Kartları ve Kredi Kartları Kanunu'nun 23. maddesiyle ortaya koyulmuştur. Maddeye göre *"Üye iş yerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına açıklayamaz, saklayamaz ve kopyalayamaz."* Maddede açıkça belirtildiği üzere, elektronik ticaret firmalarının, kredi kartı ile ödeme kabul ettiği hallerde, müşteriden alınan kredi kartının kullanımı ile ilgili bilgileri "Yetkili kılınan kurum ve kuruluşlar" ile "Müşterinin izin verdiği kişiler" haricindeki üçüncü kişilere açıklayamayacak, bu bilgileri saklayamayacak veya kopyalayamayacaktır. Hüküm kapsamı içerisindeki bilgiler "Kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgiler" olarak geniş bir şekilde tanımlandığı için, bu bilgiler içerisine kartla ilgili bilgilerin haricinde, güvenlik soruları, adres, bilgileri, kullanıcı bilgileri, satın alınan mal veya hizmetle ilgili bilgilerin tümü girecektir. Madde içerisinde yasaklanan fiiller içerisinde de, hem firmanın kendisi tarafından bu bilgilerin saklanması hem de üçüncü kişilere verilmesi sayılmıştır. Yukarıda belirtildiği üzere kullanıcıdan alınacak izin kullanıcı sözleşmesi içerisinde yer alabilir, ancak kullanıcı sözleşmesi içerisinde hangi bilgilerin bu şekilde saklanacağı açık bir şekilde belirtilmeli ve bu bilgiler üçüncü kişiler ile

paylaşılacaksa paylaşım kapsamı ve kimlerle paylaştırılacağı aynı şekilde belirtilmelidir.

Maddenin ikinci cümlesi ile ise *"Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez"* hükmü belirlenmiştir. Burada dikkat edilmesi gereken nokta, "Kullanıcıdan izin alınsa dahi" kart bilgilerinin üye iş yeri anlaşması yapan kuruluş (çoğu zaman bu kuruluş bankadır) dışında herhangi bir kimseyle paylaşılamayacağı, satılamayacağı, satın alınamayacağı ve takas edilemeyeceğidir. Madde içerisinde belirtilen kart bilgileri, kanaatimizce, doğrudan kartın kullanımıyla ilgili olan, kart sahibi, kredi kartı numarası, CVC kodu gibi bilgilerdir. Banka ve Kredi Kartları Kanunu'nun 39. maddesiyle de 23. maddeye uymayan üye iş yerlerinin işlerini fiilen yöneten görevliler ve işlemi yapan kişilerin bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılacağı belirlenmiştir.

2.3. ELEKTRONİK TİCARETTE KARŞILAŞILAN SUÇLAR ve KORUNMA YÖNTEMLERİ

Elektronik ticaret uygulamaları içerisinde sanıldığının aksine bilişim suçlarının dışında da çok çeşitli suçlarla karşılaşılabilmektedir. Özellikle kredi kartı hırsızlığı, dolandırıcılık, bilişim sistemlerine girme ve verileri bozma suçları sıklıkla karşılaşılan suçlar olmakla birlikte; elektronik ticaret firmalarının mağdur olduğu değil fail olarak yer aldığı suçlar da ortaya çıkabilmektedir. Bu suçlar çoğunlukla firmanın satışını gerçekleştirdiği mal ve hizmetin satışının yasak olduğu veya bazı şartlara bağlı olduğu durumlarda ortaya çıkmaktadır. Bu tür suçlarda hem suçlunun yakalanması, hem suçtan korunması, hem de suç sebebiyle ortaya çıkan zarardan sorumluluğun belirlenebilmesi amacıyla adli bilişim yöntemlerinin ve bunun öncü çalışması sayılabilecek bilgi güvenliği yönetim sistemleri içerisindeki kayıt politikalarının uygulanması elzemdir.

2.3.1. ÇALINTI KREDİ KART veya HESAP BİLGİLERİNİN KULLANILMASI ve DOLANDIRICILIK

Çalıntı kredi kartı veya hesap bilgilerinin elektronik ticarette kullanılması durumunda, hukuki açıdan iki hususun incelenmesi gerekmektedir. Bunlardan birincisi kredi kartı veya hesap bilgilerinin çalınması fiilinin suç olarak incelenmesi diğeri ise çalıntı kredi kartı veya hesap bilgilerinin kullanılması ve zarar doğması halinde ilgili tarafların sorumluluklarının belirlenmesidir.

TCK'da, kredi kartı veya hesap bilgilerinin çalınması fiiline, banka veya kredi kartının kötüye kullanılması olarak tanımlanmış ve yer verilmiştir. 245. maddeye göre, *"Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa"* bu fiil suç olarak değerlendirilecektir.

Maddede suçun oluşabilmesi için "Banka veya kredi kartının" ele geçirilmiş olması aranmaktadır. Madde yorumlanırken, öncelikle korunan değerin fiziksel banka veya kredi kartı olduğu zannedilmektedir. Ancak esasta, korunan değerin bu banka ve kredi kartının bağlı olduğu banka hesabı ve bu hesabın sahibi kişi olması sebebiyle madde içerisinde geçen "Banka veya kredi kartı" tanımının fiziksel kartın yanı sıra bu kartların elektronik ortamda kullanılmasını sağlayan bilgileri de kapsadığı kabul edilmelidir.

Madde içerisinde söz konusu suçun gerçekleşmesi için oldukça önemli bir şartın gerçekleşmesi gerekmektedir. Bu şart banka veya kredi kartını ele geçiren veya elinde bulunduran kişinin rıza olmadan bu kartı kullanarak veya kullandırtarak "Yarar sağlaması" gerekmektedir. Bu durumda kartı kullanan veya kullandırtan kişinin henüz yarar sağlamamış olması halinde suçun oluştuğundan bahis edilemeyecektir. Uygulamada sıkça rastlanan çalıntı kredi kartı bilgilerinin paylaşılması veya sahibinden çalınması fiillerinde bu fiiller sebebiyle henüz yarar sağlanmamışsa (bilgilerin satışı karşılığında bir bedel veya benzeri bir kazandırma yaşanmamışsa veya bu bilgilerin kullanılması ile kart sahibinin hesabında bir azalma olmamışsa) söz konusu suç tamamlanmış olmayacaktır. Böyle bir durumda şartları oluşmuşsa "Teşebbüs" durumundan bahsedilebilir; ancak söz konusu durum banka veya kredi kartlarının kötüye kullanılması suçu olarak değerlendirilmese dahi, yine koşullarının oluşması durumunda bilişim sistemlerine yönelik suçlar kapsamında düşünülebilecektir.

TCK 245. maddenin ikinci fıkrasıyla da *"Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi"*nin suç olarak ayrıca düzenlenmiştir.

Çalıntı kredi ve banka kartı bilgilerinin kullanılması halinde, söz konusu fiillerin suç olarak değerlendirilmesinin yanı sıra, ortaya çıkan zarar sebebiyle sorumluluğun kime ait olacağı ayrıca değerlendirilmelidir. MSHY'nin 10. maddesine göre:

"Mesafeli sözleşmelerde, ödemenin kredi kartı veya benzeri bir ödeme kartı ile yapılması halinde tüketici, kartın kendi rızası dışında ve hukuka aykırı biçimde kullanıldığı gerekçesiyle ödeme işleminin iptal edilmesini talep edebilir. Bu halde, kartı çıkaran kuruluş itirazın kendisine bildirilmesinden itibaren 10 gün içinde ödeme tutarını tüketiciye iade eder."

Bu hüküm ile de ödeme kartları ile yapılan alış verilerde, kart bilgilerinin çalınması durumunda tüketicinin korunması öngörülmüştür. Ancak düzenlemede itirazın bildirilme süresini belirlemediği için bu düzenleme sebebiyle dolandırıcılık olaylarında tespitin yapılması daha güç bir hale gelebilecektir.

5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 12. maddesindeki benzer bir düzenleme ile *"Kartın ya da 16'ncı maddede belirtilen bilgilerin kaybolması veya çalınması halinde kart hamili, yapacağı bildirimden önceki yirmidört saat içinde gerçekleşen hukuka aykırı kullanımdan doğan zararlardan yüzelli Yeni Türk Lirası ile sınırlı olmak üzere sorumludur"* hükmü getirilerek dolandırıcılık olaylarının tespitinin sağlanabilmesi için sınırlı bir zaman aralığı temin edilmiştir. Bu düzenleme ile tüketicinin bildirim yapması halinde sınırlı sorumluluğu düzenlenerek dolandırıcılık olaylarının tespiti için tüketicinin bildirim yapması teşvik edilmeye çalışılmaktadır. Maddede yer alan sınırlı sorumluluk hali, yine madde metni içerisinde *"Hukuka aykırı kullanımın, hamilin ağır ihmaline veya kastına dayanması veya bildirimin yapılmaması hallerinde bu sınır uygulanmaz."* şeklindeki tanımla sınırlandırılmıştır. Buna göre sınırlı sorumluluk hali sadece kart hamilinin hafif kusur hallerinde geçerli olacaktır. Aynı madde içerisinde ayrıca, tüketicinin sorumluluğunun bedeli olarak belirlenen miktarın sigortalanması yükümlülüğü bankaya bırakılmış ve sigortanın usul ve esaslarının Bankacılık Düzenleme ve Denetleme Kurumu tarafından çıkarılacak yönetmelikle belirleneceği belirtilmiştir. Bankacılık Düzenleme ve Denetleme Kurumu tarafından çıkartılan Banka Kartları ve Kredi Kartları Hakkında Yönetmeliği'nin[11] 23. maddesi ile sigortanın banka tarafından karşılanacağı kart hamilinin kart çıkaran kuruluş tarafından tercih edilen sigorta şirketini kabul etmediği takdirde kendisi tarafından belirlenen sigorta şirketi aracılığıyla sigorta işlemlerini yapmakta serbest olacağı belirlenmiştir.

Elektronik ortamda gerçekleştirilen işlemlerde çalıntı kredi kartı ile işlem yapılması halinde tüketicinin sorumsuzluğu ise çok daha geniş bir sorumsuzluk kapsamı içerisine alınmıştır. Banka Kartları ve Kredi Kartları Kanunu'nun 15. maddesine göre: *"Bu Kanunun 20'nci maddesi uyarınca*

[11] RG 10.03.2007, sy.26458

harcama belgesi düzenlenmeksizin çeşitli iletişim araçları yoluyla veya sipariş formu vasıtasıyla yapılan mal ve hizmet alımlarındaki hukuka aykırı kullanımlardan kaynaklanan zararlardan kart hamili sorumlu tutulamaz."

Yukarıda görüldüğü üzere, özellikle elektronik ticaret kapsamında çalıntı kredi kart kullanımı halinde genel esas, kart sahibinin sorumsuzluğudur. Uygulamada da, hesap bilgilerinin çalınması olaylarının aksine bankalar, bildirim üzerine hukuka aykırı kullanım sebebiyle uğranılan zararı (kredi kartından çekilen parayı) kart sahibine iade etmektedirler. Ancak bankalar burada doğan zararı doğrudan üye iş yeri olan elektronik ticaret firmasına yönlendirmektedirler. Banka ile elektronik ticaret firması arasında yapılan sanal pos anlaşmalarında söz konusu zararın firmaya rücu edileceğine dair hükümler bulunmaktadır. Uygulamada elektronik ticaret firmalarının en büyük risklerinden bir tanesi; kendisine rücu edilen zararda kusursuzluğu ispat edememesi, kendisine rücu edilen bu zararı (chargeback) ödemek zorunda kalmasıdır. Elektronik ticaret firması, söz konusu olayda kusursuzluğunu kanıtlayabilmek amacıyla, gerekli bilgi güvenliği ve dolandırıcılık koruması (fraud protection) alt yapılarını kurmak ve işletmek zorundadır. Bu sistemlerin kurulması hem dolandırıcılık riskini azaltacak hem de olası uyuşmazlıklarda firmanın basiretli bir tacir olarak yükümlülüklerini yerine getirdiği ve zarardan sorumluluğu bulunmadığını kanıtlamasında faydalı olacaktır.

Elektronik ticaret uygulamalarında sıkça karşılaşılan bir başka suç ise dolandırıcılık suçudur. Bu suç, elektronik ticaret firmasının veya (iş modeline göre elektronik ticaret firmasının kullanıcılar arasında aracı olarak konumlandığı durumlarda) kullanıcının diğer kullanıcı tarafından dolandırılması şeklinde görülmektedir. Suçun görünüş şekilleri içerisinde mal satımı veya hizmetinin gerçekleştirileceği yönünde vaat verilip bunun gerçekleştirilmemesi, malın teslim alınmasına rağmen teslim alınmadığının belirtilmesi, malın teslim alınmasına rağmen ücretin ödenmemesi, kullanıcıya elektronik ticaret firmasından gelmiş gibi gösterilerek e-posta atılması ve bunun sonucunda zarar verilmesi gibi örnekler verilebilecektir. Bu ve benzeri davranışlar TCK 157. maddede düzenlenen dolandırıcılık kapsamına girmektedir. Maddeye göre: *"Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlayan kişi" dolandırıcılık suçunu işlemektedir. 158. maddenin f. fıkrasında ise söz konusu suçun "Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle"* işlenmesi halinde suçun nitelikli dolandırıcılık suçunu oluşturacağı ve cezasının daha ağır olacağı belirtilmiştir.

Uygulamada karşılaşılan çoğu bilgi güvenliği açığı olayında, olay dolandırıcılık (fraud) olarak tanımlanmaktadır. Ancak yukarıda açıklandığı üzere olay, TCK kapsamında tanımlanan suçlar dahilinde incelendiğinde, suçun banka veya kredi kartının kötüye kullanılması, dolandırıcılık ve hatta bazı durumlara hırsızlık suçu kapsamına girebileceği görülmektedir. Bu sebeple olayın değerlendirilmesinde, teknolojik alt yapı ve iş modeli ne olursa olsun, olayın unsurları, gerçekleştirilen fiiller, mağdur ve zararın incelenmesi ve buna göre yorumun yapılması gerekmektedir. Ayrıca suçun ve failin belirlenmesinde elektronik ticaret iş modeli içerisindeki tarafların iş modeli doğrultusundaki ticari sorumlulukları ile olayda ortaya konulan fiiller birlikte yorumlanmalıdır.

2.3.2. İÇERİKLE İLGİLİ SUÇLAR

Bilindiği üzere elektronik ortamda, fiziksel ortamda işlenebilen suçların pek çoğu işlenebilmektedir. Hakaret, hırsızlık, müstehcenlik, intihara azmettirme gibi fiziksel bir müdahale gerektirmeyen çok çeşitli suçların yanı sıra elektronik ortamda bazı müdahalelerin gerçekleştirilmesi ile fiziksel ortamda bazı sonuçların doğması sonucunda (yangın, sinyalizasyon arızası, vb.) adam öldürme veya yaralama suçunun dahi elektronik ortam aracılığıyla işlenebildiği bilinmektedir. Bu sebeple kanaatimizce, bilişim sistemlerine yönelik suçlar ve kendine has özellikleri sebebiyle banka ve kredi kartlarının kötüye kullanılması ve elektronik ticaret uygulamalarında dolandırıcılık istisna olmak üzere, elektronik ortam aracılığıyla işlenebilen suçlar şeklinde bir ayrım yapmak gereksizdir. Ancak kanaatimizce, elektronik ticaret uygulamaları içerisinde içerik sebebiyle şuçun oluştuğu durumların ayrıca incelenmesinde fayda bulunmaktadır.

Elektronik ticaret uygulaması içerisinde içerik olarak yer verilen bazı mal ve hizmetlerin ve/veya bunların sunuluş biçimlerinin suç kapsamında değerlendirilebildiği görülmektedir. Burada suçun oluşmaması için sunulan mal ve hizmetin, mevcut mevzuat doğrultusunda satılmasının veya sunulmasının yasal olup olmadığının her mal veya hizmet için ayrıca değerlendirilmesi gerekmektedir. Bazı mal veya hizmetlerin, satışı veya sağlanması mevcut mevzuatla belirli şartlara bağlanmış olabilir, böyle bir durumda bu şartların elektronik ortamda karşılanıp karşılanamadığı da yine ayrıca değerlendirilmelidir.

Elektronik ticaret içerisinde her türlü mal ve hizmetin satışı ve bazı mal ve hizmetlerin teslimi ve sunumu operasyonel olarak gerçekleştirilebileceği için bu çalışma içerisinde mal ve hizmet özelinde ayrıca bir uygunluk analizi

yapılmayacaktır. Ancak örnek olarak elektronik ortamda evcil hayvan satışı verilebilir[12].

Bilindiği üzere evcil hayvan satışı ülkemizde Hayvanları Koruma Kanunu ile belli şart ve koşullara bağlanmıştır. Kanunun,

5. maddesinin 3. fıkrasına göre:
"Ev ve süs hayvanı satan kişiler, bu hayvanların bakımı ve korunması ile ilgili olarak yerel yönetimler tarafından düzenlenen eğitim programlarına katılarak sertifika almakla yükümlüdürler."

5. maddesinin 6. fıkrasına göre:
"Ev ve süs hayvanlarının üretimini ve ticaretini yapanlar, hayvanları sahiplenen ve onu üretmek için seçenler annenin ve yavrularının sağlığını tehlikeye atmamak için gerekli anatomik, fizyolojik ve davranış karakteristikleri ile ilgili önlemleri almakla yükümlüdür."

Yukarıda görüldüğü üzere söz konusu şartların yerine getirilmesi halinde elektronik ortam aracılığıyla evcil hayvan satışı yapılmasında bir sorun bulunmamaktadır. Ancak şart ve koşullar açık bir şekilde sağlıklı bir fiziksel ortamın yaratılmasını ve sertifika alınmasını şart koşmaktadır. Bu şartlar gerçekleştirilmeden, sadece elektronik ortamda bu hayvanların resimlerin ve özelliklerine yer verilerek ve elektronik ödeme kabul edilerek hayvan satışının gerçekleştirilmesi halinde doğal olarak söz konusu fiiller hukuka uygun kabul edilemeyecektir. Ancak söz konusu şartların sağlanması ve gerekli fiziksel ortamın sağlanmasının yanı sıra, tanıtım amacıyla satışla ilgili bilgilere ve görsellere satışı gerçekleştirenin kendisine ait veya bu iş için kurulmuş bir elektronik ticaret sitesi üzerinde yer vermesi, kanaatimizce, herhangi bir suç oluşturmayacaktır.

2.3.3. BİLGİSAYAR SİSTEMLERİNE YÖNELİK SUÇLAR

Yukarıda belirtildiği üzere fiziksel ortamda işlenen suçların çoğu elektronik ortam aracılığıyla da işlenebilmektedir. Ancak bazı suçlar sadece elektronik ortamda işlenebilmektedir. Bu suçlar bilişim sistemlerine karşı işlenen suçlardır. TCK'nın 234 ve 235. maddelerinde bilişim sistemlerine yönelik işlenen ve doğrudan bilişim suçları olarak adlandırılan suçlara yer verilmektedir.

[12] Örnek sadece evcil havyan satışı için verilmiştir; vahşi hayvan satışı öncelikle CITES Sözleşmesi ve ilgili mevzuat doğrultusunda ayrıca değerlendirilmelidir.

TCK'nın 243. maddesinde bilişim sistemine girme suçu yer almaktadır. Maddeye göre, *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimse"* bilişim sistemine girme suçunu işlemiş olacaktır. Dikkat edilirse söz konusu suçun işlenmesi için hukuka aykırı olarak sisteme girilmesi ve orada kalınmaya devam edilmesi yeterli görülmüştür; suçun tamamlanması için ayrıca bir zarar verilmesi veya gizli bilgilere vakıf olunması gibi şartlar aranmamaktadır. Suçun tamamlanması için sadece girme ve orada kalmanın yeterli görülmesinin sebebi, daha sonra daha büyük zararlar verilmesi için sisteme giriş çabalarında bulunan kötü niyetli kişilerin fiillerinin de cezalandırılmasıdır. Sisteme giriş fiilinin cezalandırılmaması durumunda, sisteme giriş için saldırdığı tespit edilen ancak maddi bir zarar vermeyen kişilerin fiillerinin cezalandırılması mümkün olmayacaktır. Söz konusu maddi zarar verildikten sonra da uygulamada genelde kişinin yakalanması çok güç olduğu için düzenleme ile istenen sonuca ulaşılamayacaktır.

Suçun unsurlarının ortaya koyulabilmesi için madde içerisinde belirtilen "Hukuka aykırı şekilde" şartının ne olduğunun belirlenmesi gereklidir. Madde içerisinde belirtilen hukuka aykırılık, yasa ile belirlenen bir durumun aksine veya bilişim sistemi sahibi ve/veya bilişim sisteminden doğrudan yararlanan kişinin (sistem üzerinde bilgileri bulunan) rızası dışında sisteme girilmesi hallerinde ortaya çıkacaktır. Bu durumda mevzuat ile belirlenen bir şartın veya hakkın yerine getirilmesi için veya bilişim sistemi sahibinin ve/veya doğrudan yararlanan kişinin izni ile sisteme girmeye çalışılması suç oluşturmayacaktır. Burada genel kural olarak bu şekilde bir iznin bulunmadığı kabul edilmeli ve söz konusu iznin, girilecek sistemin hangi bölümlerine girileceğinin açık bir şekilde belirtilmesi suretiyle verilmesinin aranması gereklidir. Ancak kamuya açık bilgi sistemlerine (örnek olarak üyelik sistemi bulunmayan bir internet sitesi) giriş durumunda ayrıca bir iznin aranmaması, sistemin kamuya açık yapısının halihazırda bir izin anlamına geldiğinin göz önünde bulundurulması gerekmektedir.

Madde içerisinde belirtilen, "Orada kalma" şartı ise, kanaatimizce, yanlışlıkla hukuka aykırı bir şekilde sisteme girme fiillerinin kapsam içerisine sokulmaması için madde içerisinde yer verilmiş bir şarttır. Sisteme girme suçunun oluşması için, giren kişinin bu konuda kastının bulunması gerektiği genel ceza hukuku prensiplerince kesindir, ancak olayda kişinin kastının bulunup bulunmadığının belirlenmesi çoğu zaman oldukça güç olmaktadır. "Orada kalma" şartının gerçekleşmesi ile birlikte ise kişinin kastı net bir şekilde belirlenebilmekte ve kişi girdikten sonra sistemde makul bir süre kalıyorsa, girme kastının suçu işleme olduğu ortaya koyulabilmektedir.

TCK madde 243'ün ikinci ve üçüncü fıkralarında sisteme girme suçunun ağırlaştırıcı nedenleri düzenlenmektedir. Buna göre sisteme girme suçlarının bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi veya bu fiil nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hallerinde suçun cezası ağırlaştırılarak uygulanacaktır.

Elektronik ticaret sistemleri; uygulamada sıklıkla saldırıya uğramaktadır. Bu saldırıların çoğu sisteme giriş yollarının belirlenmesi amacıyla gerçekleştirilip, çoğunda maddi bir zarar verilmemekte ancak sistemin incelenmesi tamamlandıktan sonra zarar verici saldırı gerçekleştirilebilmektedir. Sisteme maddi zarar vermeden gerçekleştirilen ilk saldırılar sadece sistemin firewall kayıtlarından görülebilmektedir. Sistem güvenlik uzmanının söz konusu kayıtları incelemesi sırasında bu şekilde saldırılara rastlaması halinde gerekli teknik önlemlerin yanı sıra, hukuki önlemlerin de alınması gereklidir. Yukarıda bahsedildiği üzere, sadece sisteme girme de suç olarak düzenlendiği için konuyla ilgili derhal savcılığa suç duyurusunda bulunulmalıdır.

Sisteme girme dışında, sistemin işleyişinin engellenmesi, verilerin yok edilmesi veya değiştirilmesi hallerinde ise TCK'nın 244. maddesi uygulanacaktır. Maddeye göre *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi"*nin fiili suç olarak tanımlanmıştır. Maddede belirtildiği üzere, suçun oluşması için ayrıca verilerin zarar görmesine gerek bulunmamakta, sistemin işleyişinin bozulması veya engellenmesi yeterli olmaktadır. Ancak uygulamada verilerin bozulması gerçekleştirilmeden, sistemin işleyişinin bozulması mümkün değildir; verilerin bozulması durumunda da ikinci fıkra hükümleri uygulanacaktır. Kanaatimizce 244/1'in uygulama alanı, müdahale sonucunda sistemin işleyişinin bozulduğu, ancak verilerin değiştirildiğinin kanıtlanamadığı hallerdir.

Maddenin ikinci fıkrasında ise *"Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi"*nin fiilleri suç olarak düzenlenmiştir. Görüldüğü üzere bu fıkrada geniş bir şekilde verilere ilişkin tüm müdahaleler kapsam içerisine alınmıştır.

TCK 244. maddenin üçüncü ve dördüncü fıkralarında ise ağırlaştırıcı sebepler sayılmıştır. Buna göre sistemin işleyişinin engellenmesi, verilerin yok edilmesi veya değiştirilmesi suçlarının *"Banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi veya bu fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması"* halleri ağırlaştırıcı neden olarak düzenlenmiştir.

2.3.4. ADLİ BİLİŞİM

Adli[13] bilişim uzmanı Hilton Chan tarafından yapılan bir tanımla "*Adli bilişim; bilgisayarlar, bilgisayar depolama araçları ve elektronik aletlerin tanımlanması, araştırılması, geri getirilmesi, kurtarılması ve dijital delillerin elde edilmesi ve mahkeme tarafından talep edilen standarda uygun bulguların sunulması için bilimsel ve sistematik bir metodolojidir.*"

Uygulamada adli bilişim, uyuşmazlık öncesi (veya suç öncesi) ve uyuşmazlık sonrası (veya suç sonrası) süreçlerde bilgi güvenliği yönetimi ile birlikte değerlendirilmekte ve bilgi güvenliği yönetimi ile belirlenen prosedürler doğrultusunda adli bilişim çalışmalarının sonuçları etkilenmektedir. Bilgi güvenliği yönetimi ile belirlenen kayıt tutma prosedürleri adli bilişim çalışmasında önemli delillerin elde edilmesini kolaylaştırmakta ve adli bilişim çalışmasının daha hızlı ve daha az maliyetli gerçekleştirilmesini sağlamaktadır. Elektronik kayıtların kolaylıkla değiştirilebilir veya bozulabilir olması sebebiyle bu kayıtların delil değerlerini koruyabilmeleri için kayıtların değiştirilemez bir biçimde tutulması, kayıtlarda tarih ve kayıtları yaratan kişilerin bilgilerinin bulunması son derece önemlidir. Bu sebeple güvenilir elektronik delil yaratılması için kayıt prosedürlerinde bahsi geçen nitelikte kayıtların yaratılması için süreçler belirlenmektedir.

Adli bilişim çalışması sırasında daha önceden oluşturulmuş elektronik kayıtların ve verilerin değiştirilebilir ve bozulabilir olması sebebiyle, delil toplama aşamasında güvenilirliği sağlayacak bir biçimde verilerin değiştirilmeden toplanmasını sağlayacak bir çalışmanın gerçekleştirilmesi gereklidir. Bu çalışmanın gerçekleştirilmesi için delil toplama aşamasından önce yaratılmış, uluslararası standartlara ve ilgili yerel mevzuata uygun yazılı bir prosedürün bulunması ve delil toplama işleminin bu prosedüre uygun olarak gerçekleştirilmesi gereklidir. Adli bilişim çalışmasının uygulanacağı elektronik araçlara ve verilerin durumuna göre yapılacak çalışmanın değişecek olması sebebiyle, söz konusu yazılı prosedürlerde öncelikle genel ilkeler belirlenmeli daha sonra farklı ortam ve verilerin durumuna göre süreçler belirlenmelidir. Genel ilkelerde özellikle üzerinde araştırma yapılan elektronik eşyanın sahibi ve/veya kullanıcısı olan kişilerin temel haklarının korunması gözetilmeli, soruşturmaya veya uyuşmazlığa konu olaylar dışındaki verilerin incelenmemesine özellikle dikkat edilmelidir.

[13] Yasin Beceni ve Tuğrul Sevim, Adli Bilişim ve Hukuk, Güncel Hukuk Dergisi, Mart 2008.

Adli bilişim, elektronik ortamdaki delillerin bulunmasını ve değerlendirilmesini sağlaması sebebiyle hem ceza yargılamasında, hem de hukuki uyuşmazlıklarda ihtiyaç duyulan bir çalışma olarak karşımıza çıkmaktadır. Ceza yargılamasında elektronik ortamda işlenen bir suçla ilgili gerekli delillerin bulunması için emniyet görevlileri tarafından adli bilişim çalışması gerçekleştirilmektedir. Ülkemizde de özellikle son dönemlerde yoğun bir biçimde karşılaşılan e-posta, anlık mesajlaşma uygulamaları ve internet üzerindeki içerik aracılığıyla hakaret suçları, banka ve kredi kartı hesap bilgilerinin çalınması, şirket içi gizli bilgilerin rakip firmalara gönderilmesi, özel yaşamın gizliliğinin ihlali gibi suçlar başta olmak üzere elektronik ortamda delil bulunma ihtimali olan pek çok suçla ilgili soruşturmada emniyet yetkilileri adli bilişim çalışmaları yapmaktadır. Söz konusu çalışmalar yukarıda bahsedildiği gibi özel uzmanlık ve gerekli donanıma sahip alanlar gerektirmesi sebebiyle bu iş için kurulmuş özel birimler tarafından gerçekleştirilmektedir. Emniyet içerisinde bilişim suçları büro amirliğinin yanı sıra, asayiş ve mali şube gibi birimler içerisinde de elektronik delillerin bulunması ve incelenmesi amacıyla özel birimler kurulmuş durumdadır.

Elektronik ticaret firmaları için de yukarıda bahsedildiği üzere adli bilişim süreçlerinin öncesinde bilgi güvenliği yönetimi kapsamında kayıt politikalarının oluşturulması, bunların prosedürler dahilinde işletilmesi hem hukuk uyuşmazlıklarında, hem de ceza soruşturmalarında gerçeğe ulaşılması ve delil elde edilmesi açısından çok önemlidir. Burada kayıt politikaları oluşturulurken elektronik ticaret firmasının iş modeli, karşı karşıya kalabileceği suçlar (özellikle fraud olayları), operasyonel süreçleri ayrıca değerlendirilmeli ve yerel mevzuat da göz önünde bulundurularak buna uygun bir kayıt politikası oluşturulmalıdır.

2.4. 5651 SAYILI YASA KAPSAMINDA ELEKTRONİK TİCARET FİRMALARI

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile internet üzerindeki içeriklerin denetlenmesi ve bu içeriklerle ilgili kurumlara çeşitli yükümlülükler getirilmesi amaçlanmaktadır. Kanun yükümlülük ve sorumlulukların belirlenmesi açısından internet üzerindeki bileşenleri üç ayrı kategoriye sokmuştur. Ancak kanun içerisinde yer alan tanımlar teknik açıdan çok geniş bir kapsamda dile getirilmiştir. Bu durum internet üzerindeki herhangi bir bileşenin hangi kategoriye gireceğinin belirlenmesinde ciddi zorluklar çıkarabilecek bir mahiyettedir. Özellikle uyuşmazlık veya ceza

soruşturma ve kovuşturmalarında bu tanımların ilgili makamlar ve mahkemeler tarafından yorumlanmasında ve tarafların hangi tanım içerisine gireceğinin belirlenmesinde problemler çıkacağı düşünülmektedir.

İnternetin teknik alt yapısı doğrultusunda Kanun ve bu Kanun'a dayanarak çıkartılan yönetmelikler birlikte incelendiğinde ise Kanunda yer alan tanımlardan erişim sağlayıcının, internet servis sağlayıcı olduğu anlaşılmaktadır. Yer sağlayıcı tanımının içerisinde ise hem hosting firmalarının, hem de kullanıcı tarafından yaratılan içerikle işleyen (user-generated-content) sitelerin girdiği görülmektedir. Örnek vermek gerekirse Youtube sitesi bir yer sağlayıcıdır. Bu siteye video yükleyen kullanıcılar ise Kanun kapsamında içerik sağlayıcı olarak yer almaktadır. Burada dikkat edilmesi gereken konu içerik sağlayıcıların sağladığı içeriklerin belirli bir formatta ve anlamda olması gerekliliğinin bulunmamasıdır. Kanunda yer alan içerik sağlayıcı tanımı metni içerisinde yer aldığı gibi her türlü bilgi veya veri içerik sayılmakta ve bu veriyi üreten, sağlayan ve değiştiren herkes de içerik sağlayıcı kabul edilmektedir. Yine internetin teknik yapısı düşünüldüğünde interaktif bir şekilde internet üzerinde herhangi bir işlem yapan herkes bu tanıma göre içerik sağlayıcı olarak kabul edilecektir.

Elektronik ticaret firmaları iş modellerine göre 5651 sayılı Kanun kapsamında içerik sağlayıcı veya yer sağlayıcı olarak yer almaktadırlar. Firmanın içeriklerinin doğrudan kendisi tarafından sağlanması halinde firma içerik sağlayıcı, içeriklerin kullanıcılar tarafından sağlanması halinde ise firma yer sağlayıcı konumunda olacaktır. Burada içerikten kasıt, hem sunulan mal ve hizmetlerle ilgili bilgiler ve görseller, hem de bunlarla ilgili yorumlar, linkler ve benzeri içeriklerdir. İçerik sağlayıcı ve yer sağlayıcı olmanın farklılıkları hukuki sorumlulukları neticesinde ortaya çıkmaktadır. 5651 sayılı Kanun'un 4. maddesine göre: *"İçerik sağlayıcı internet ortamında kullanıma sunduğu her türlü içerikten sorumludur. İçerik sağlayıcı, bağlantı sağladığı başkasına ait içerikten sorumlu değildir. Ancak, sunuş biçiminden, bağlantı sağladığı içeriği benimsediği ve kullanıcının söz konusu içeriğe ulaşmasını amaçladığı açıkça belli ise genel hükümlere göre sorumludur."* Yer sağlayıcı ise aynı Kanun'un 5. maddesine göre: *"Yer sağladığı içeriği kontrol etmek veya hukuka aykırı bir faaliyetin söz konusu olup olmadığını araştırmakla yükümlü değildir"*. Ancak, *"Yer sağlayıcı, yer sağladığı hukuka aykırı içerikten, ceza sorumluluğu ile ilgili hükümler saklı kalmak kaydıyla, bu Kanunun 8'inci ve 9'uncu maddelerine göre haberdar edilmesi halinde ve teknik olarak imkân bulunduğu ölçüde hukuka aykırı içeriği yayından kaldırmakla yükümlüdür."*

Söz konusu 8. maddede belirtilen haberdar edilme durumu Telekomünikasyon İletişim Başkanlığı tarafından resmen veya mahkeme kararı ile ilgili içeriği erişimin engellenmesi kararı verilmesi ve bunun yer sağlayıcıya bildirilmesi durumudur. 9. maddede belirtilen haberdar edilme durumu ise; içerik sebebiyle hakları ihlal edilen kişinin yer sağlayıcıya içeriğin yayından çıkarılması için bildirimde bulunması ve bu talebinin kabul edilmemesi halinde Sulh Ceza Hakimi'ne başvurarak içeriğin yayından kaldırılmasını talep etmesi, talebinin haklı görülmesi halinde mahkemenin yer sağlayıcıya içeriğin yayından kaldırılmasını emretmesidir.

5651 sayılı Kanun'un düzenlenme amacı çocuk ve ailenin korunması olmasına rağmen yukarıda belirttiğimiz sakıncalar sebebiyle uygulamada çok geniş bir uygulama alanı bulma tehlikesi ile karşı karşıyadır. Elektronik ticaret firmalarının Kanun kapsamında hangi tanım içerisine gireceği yukarıda açıklanmış olmakla beraber, özellikle kullanıcı yorumları ve benzer durumlarda doğrudan sorumlulukla karşılaşmamak için yer sağlayıcı tanımı kapsamına girmek ve bu doğrultuda Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik hükümleri doğrultusunda Telekomünikasyon İletişim Başkanlığı'na "Yer sağlayıcı faaliyet belgesi" almak için başvuruda bulunmanın uygulamada çok büyük faydası olacağı kanaatindeyiz. Bu belgenin teminini takiben bu bölüm içerisinde de anlatılan yer sağlayıcılara ilişkin teknik yükümlülükler yerine getirilmeli ayrıca 5651 sayılı Kanun'un 9. maddesi ile belirlenen içerikten hakları ihlal edilen kişilerin şikayetlerinin alınabilmesi amacıyla site içerisinde etkin bir uyar-kaldır sisteminin kurulması gerekmektedir.

Yer sağlayıcılar ile ilgili ayrıntılı düzenlemeler Telekomünikasyon Kurumu tarafından 5651 sayılı Kanun'un verdiği yetkiyle çıkartılan "Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik" ile belirlenmiştir.

Yönetmelik ve Kanun incelendiğinde yer sağlayıcıların temel yükümlülüklerinin yer sağlayıcı belgesi alma, uygun bildirim karşısında hukuka aykırı içeriği kaldırma, bilgilendirme ve log tutma olduğu görülmektedir. Log tutma ile ilgili olarak Yönetmelik'te "Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini (hash) zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlüdür" şeklinde bir ibare bulunmaktadır. Yönetmeliğin tanımlar bölümünde de söz konusu yer sağlayıcı trafik bilgileri açıklanmıştır. Buna göre yer sağlayıcı trafik bilgisi "İnternet ortamındaki her

türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih-saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgisi gibi bilgileri" ifade etmektedir.

Bu durumda yer sağlayıcıların trafik bilgisi olan bilgilerin loglarını en az altı ay süreyle "Zaman damgalamak" suretiyle saklama yükümlülüğü bulunmaktadır. Burada bahsedilen "Zaman damgası" kanaatimizce, 5070 sayılı Elektronik İmza Kanunu kapsamında yetkili elektronik sertifika hizmet sağlayıcılar tarafından sağlanan zaman damgasıdır; zira 5651 sayılı Kanun ve ilgili mevzuatla "Zaman damgası"nın ayrıca tanımı yapılmadığı için, mevzuatta zaman damgasının tanımının yapıldığı EİK'ya bakılması gereklidir.

5651 sayılı Kanun ve ilgili mevzuatla hem yer sağlayıcılar, hem de içerik sağlayıcılar için getirilen bilgilendirme yükümlülüğü, 5651 sayılı Kanun'a dayanılarak çıkartılan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmeliğin 5. maddesiyle belirlenmiştir. Buna göre:

Ticari veya ekonomik amaçlı içerik sağlayıcıları, yer sağlayıcıları ve erişim sağlayıcıları, aşağıda belirtilen tanıtıcı bilgilerini, kendilerine ait internet ortamında, kullanıcıların ana sayfadan doğrudan ulaşabileceği şekilde ve iletişim başlığı altında, doğru, eksiksiz ve güncel olarak bulundurmakla yükümlüdür:

a) Gerçek kişi ise; adı ve soyadı, tüzel kişi ise; unvanı ve sorumlu kişiler, vergi kimlik numarası veya ticaret sicil numarası,

b) Yerleşim yeri, tüzel kişi ise merkezinin bulunduğu yer,

c) Elektronik iletişim adresi ve telefon numarası,

ç) Sunduğu hizmet, bir merciin iznine veya denetimine tabi bir faaliyet çerçevesinde yapılıyor ise, yetkili denetim merciine ilişkin bilgiler.

(2) Ticari veya ekonomik amaçlı içerik sağlayıcı, birinci fıkradaki bilgilerle birlikte, yer sağlayıcıya ilişkin tanıtıcı bilgileri (yer sağlayıcılık - hosting - işlemlerinin dış kaynak yoluyla kullanılması durumunda), doğru, eksiksiz ve güncel olarak ana sayfasında bulundurmakla yükümlüdür.

2.5. ELEKTRONİK İMZA

"Elektronik imza" terimi, genellikle, elektronik ortamdaki irade beyanlarının tümü için kullanılan bir tanımdır. Geniş bir tanım yapmak gerekirse; elektronik imza, bir belgeyi imzalama niyetinde olan bir kişi tarafından sahiplenilmiş ya da icra edilmiş bir belgeyle/kayıtla mantıksal bir şekilde ilişkilendirilmiş veya eklenmiş bir süreç, elektronik bir ses, veya sembol anlamına gelir[14].

Elektronik imza, usul hukuku açısından hem ispat şartı hem de geçerlilik şartı özellikleriyle; hem özel hukuk alanında, hem de e-devlet uygulamalarında e-dönüşümün sağlanmasının en önemli etkenlerinden biri olarak görülmektedir. Uygulamada, elektronik imza ile elektronik sözleşmeler akdedilmekte, kamu kurumları ile yazışmalar ve başvuru prosedürleri gerçekleştirilmektedir.

Ülkemizde, 5070 sayılı Elektronik İmza Kanunu'nun (EİK) 23.07.2004 tarihinde yürürlüğe girmesinden sonra, elektronik imzanın hukuki değeri ile ilgili gerekli düzenleme yapılmıştır. Kanun'un 5. maddesine göre *"Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur"*. Kanun'la Borçlar Kanunu (BK) ve Hukuk Usulü Muhakemeleri Kanunu'na (HUMK) da çeşitli eklemeler yapılmıştır. EİK'nın 22. maddesi ile BK'nın 14 üncü maddesinin birinci fıkrasına şu cümle eklenmiştir; *"Güvenli elektronik imza elle atılan imza ile aynı ispat gücünü haizdir"*. EİK'nın 23. maddesi ile ise, HMUK'un 295/A maddesi eklenmiştir, madde metni şu şekildedir; *"Usulüne göre güvenli elektronik imza ile oluşturulan elektronik veriler senet hükmündedir. Bu veriler aksi ispat edilinceye kadar kesin delil sayılırlar. Dava sırasında bir taraf kendisine karşı ileri sürülen ve güvenli elektronik imza ile oluşturulmuş veriyi inkar ederse, bu Kanunun 308'inci maddesi kıyas yoluyla uygulanır"*.

Yukarıdaki açıklamalar doğrultusunda "Elle atılmış imza" ve "Senet hükmünde delil" kavramlarının ne olduklarının ayrıca açıklanmasının faydalı olacağını düşünüyoruz. Elle atılmış imza, fiziksel ortamda imzalayan kişi tarafından atılan imza anlamına gelmektedir. Hukuken elle atılmış imzanın değeri, BK'nın 13. maddesi ile belirlenmiştir. Maddeye göre hukuken yazılı olarak yapılması gereken sözleşmelerde, borç altına girenlerin sözleşmeyi imzalamaları gerekmektedir. Borçlar hukukunda genel kural, sözleşmenin oluşması için tarafların iradesinin yeterli olması olsa da,

[14] UETA, Uniform Electronic Transactions Act (1999)

bazı durumlarda hukuk güvenliğinin sağlanması için sözleşmenin yazılı olarak yapılması aranmaktadır. Bu durumdaki şekli zorunluluk geçerlilik şartı olarak değerlendirilmektedir. Bu tür durumlarda yazılı sözleşmenin yapılmaması söz konusu işlemin hukuken yapılmamış olması sonucunu doğurmaktadır. EİK'nın yürürlüğe girmesinden önce yazılı olarak yapılması gereken sözleşmelerin, elle atılmış imza şartı sebebiyle elektronik ortamda yapılması mümkün bulunmuyordu.

HMUK'un 288. maddesine göre ise: *"Bir hakkın doğumu, düşürülmesi, devri, değiştirilmesi, yenilenmesi, ertelenmesi, ikrarı ve itfası amacıyla yapılan hukuki işlemlerin, yapıldıkları zamanki miktar veya değerleri dört yüz milyon lirayı geçtiği takdirde senetle ispat olunması gerekir"*. Bu duruma "Geçerlilik şartı" denilmektedir. Maddeden anlaşıldığı üzere dört yüz milyon ve üstünde değere sahip her türlü hukuki işlemin mahkeme önünde ispatı ancak senetle yapılabilmektedir. Bu durum EİK'nın yürürlüğe girmesinden önce elektronik ticaret ve elektronik ortamda yürütülen işlemler açısından uygulamada çok büyük sorunlara yol açmakta idi; zira elektronik kayıtların senet niteliklerini taşımaması sebebiyle elektronik ortamda yapılan işlemlerde senetle ile ispat mümkün olmamaktaydı.

Yukarıda açıklandığı üzere EİK ile güvenli elektronik imzaya tanınan hukuki sonuçlar sayesinde, elektronik ortamda yaratılan sözleşmelerde geçerlilik ve ispat şartının gerektiği durumlarda gerekli olan hukuksal gereksinimler güvenli elektronik imza ile sağlanabilecektir. Elektronik ticaret uygulamaları içerisinde kullanılan sözleşme tiplerine bakıldığında, özellikle mesafeli sözleşmelerde güvenli elektronik imza bir şart olarak belirlenmemiştir. Ancak çeşitli elektronik ticaret uygulamalarında, iş modeli doğrultusunda kullanılan sözleşmelerde gerekli hukuki güvenliğin sağlanması için (geçerlilik ve ispat açısından) güvenli elektronik imza kullanılması tavsiye edilmektedir. Mevcut mevzuatımızda güvenli elektronik imzaya doğrudan hukuki sonuç bağlanmış olması sebebiyle özellikle uygulamada ve uyuşmazlık halinde mahkemede sözleşmede güvenli elektronik imza kullanılmış olması hukuken daha avantajlı bir konumda olunmasını sağlayacaktır.

3. e-TİCARET GÜVENLİĞİ - ALAKALI KANUN VE YÖNETMELİKLER

3.1. TÜKETİCİNİN KORUNMASI HAKKINDAKİ KANUN

Kanun Numarası: 4077
Kanun Kabul Tarihi: 23/02/1995
Yayımlandığı Resmi Gazete Tarihi: 08/03/1995
Yayımlandığı Resmi Gazete Sayısı: 22221

3.1.1. AMAÇ

Madde 1 - Bu Kanunun amacı, (...) kamu yararına uygun olarak tüketicinin sağlık ve güvenliği ile ekonomik çıkarlarını koruyucu, aydınlatıcı, eğitici, zararlarını tazmin edici, çevresel tehlikelerden korunmasını sağlayıcı önlemleri almak ve tüketicilerin kendilerini koruyucu girişimlerini özendirmek ve bu konudaki politikaların oluşturulmasında gönüllü örgütlenmeleri teşvik etmeye ilişkin hususları düzenlemektir.

3.1.2. KAPSAM

Madde 2 - Bu Kanun, 1 inci maddede belirtilen amaçlarla mal ve hizmet piyasalarında tüketicinin taraflardan birini oluşturduğu her türlü tüketici işlemini kapsar.

3.1.3. TANIMLAR

Madde 3 - (Değişik madde: 06/03/2003 - 4822 S.K./3. md.)
Bu Kanunun uygulamasında;

a) Bakanlık: Sanayi ve Ticaret Bakanlığını,
b) Bakan: Sanayi ve Ticaret Bakanını,
c) Mal: Alış-verişe konu olan taşınır eşyayı, konut ve tatil amaçlı taşınmaz malları ve elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayri maddi malları,
d) Hizmet: Bir ücret veya menfaat karşılığında yapılan mal sağlama dışındaki her türlü faaliyeti,
e) Tüketici: Bir mal veya hizmeti ticari veya mesleki olmayan amaçlarla edinen, kullanan veya yararlanan gerçek ya da tüzel kişiyi,
f) Satıcı: Kamu tüzel kişileri de dahil olmak üzere ticari veya mesleki faaliyetleri kapsamında tüketiciye mal sunan gerçek veya tüzel kişileri,

g) Sağlayıcı: Kamu tüzel kişileri de dahil olmak üzere ticari veya mesleki faaliyetleri kapsamında tüketiciye hizmet sunan gerçek veya tüzel kişileri,
h) Tüketici işlemi: Mal veya hizmet piyasalarında tüketici ile satıcı-sağlayıcı arasında yapılan her türlü hukuki işlemi,
ı) İmalatçı-Üretici: Kamu tüzel kişileri de dahil olmak üzere tüketiciye sunulmuş olan mal veya hizmetleri ya da bu mal veya hizmetlerin hammaddelerini yahut ara mallarını üretenler ile mal üzerine kendi ayırt edici işaretini, ticari markasını veya unvanını koyarak satışa sunanları,
j) İthalatçı: Kamu tüzel kişileri de dahil olmak üzere tüketiciye sunulmuş olan mal veya hizmetleri ya da bu mal veya hizmetlerin hammaddelerini yahut ara mallarını yurt dışından getirerek satışa sunan gerçek veya tüzel kişiyi,
k) Kredi veren: Mevzuatları gereği tüketicilere nakit kredi vermeye yetkili olan banka, özel finans kuruluşu ve finansman şirketlerini,
.....

İfade eder.

3.1.4. SÖZLEŞMELERDEKİ HAKSIZ ŞARTLAR

Madde 6 - (Değişik madde: 06/03/2003 - 4822 S.K./7. md.)
.....
6/A, 6/B, 6/C, 7, 9, 9/A, 10, 10/A ve 11/A maddelerinde yazılı olarak düzenlenmesi öngörülen tüketici sözleşmeleri en az oniki punto ve koyu siyah harflerle düzenlenir ve sözleşmede bulunması gereken şartlardan bir veya birkaçının bulunmaması durumunda eksiklik sözleşmenin geçerliliğini etkilemez. Bu eksiklik satıcı veya sağlayıcı tarafından derhal giderilir.
.....

3.1.5. KAPIDAN SATIŞLARDA SATICININ ve SAĞLAYICININ YÜKÜMLÜLÜĞÜ

Madde 9 - (Değişik madde: 06/03/2003 - 4822 S.K./13. md.)
Kapıdan satış sözleşmelerinde, sözleşmede bulunması gereken diğer unsurlara ilave olarak mal veya hizmetin nitelik ve niceliğine ilişkin açıklayıcı bilgiler, cayma bildiriminin yapılacağı açık adres ve en az on altı punto ve koyu siyah harflerle yazılmış aşağıdaki ibare yer almak zorundadır:

Tüketicinin hiçbir hukuki ve cezai sorumluluk üstlenmeksizin ve hiçbir gerekçe göstermeksizin teslim aldığı veya sözleşmenin imzalandığı tarihten itibaren yedi gün içerisinde malı veya hizmeti reddederek sözleşmeden

cayma hakkının var olduğunu ve cayma bildiriminin satıcı/sağlayıcıya ulaşması tarihinden itibaren malı geri almayı taahhüt ederiz.

Tüketici, sahip olduğu haklarının da yazılı bulunduğu sözleşmeyi imzalar ve kendi el yazısı ile tarihini yazar. Satıcı veya sağlayıcı, bu bilgilerin sözleşmede yer almasını sağlamak ve taraflar arasında akdedilen sözleşmenin bir nüshasını tüketiciye vermekle yükümlüdür.

Bu madde hükümlerine göre düzenlenmiş bir sözleşmenin ve malın tüketiciye teslim edildiğini ispat satıcıya veya sağlayıcıya aittir. Aksi takdirde, tüketici cayma hakkını kullanmak için yedi günlük süre ile bağlı değildir.

3.1.6. MESAFELİ SÖZLEŞMELER

Madde 9/A - (Ek madde: 06/03/2003 - 4822 S.K./14. md.)
Mesafeli sözleşmeler; yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmelerdir.

Mesafeli satış sözleşmesinin akdinden önce, ayrıntıları Bakanlıkça çıkarılacak tebliğle belirlenecek bilgilerin tüketiciye verilmesi zorunludur. Tüketici, bu bilgileri edindiğini yazılı olarak teyit etmedikçe sözleşme akdedilemez. Elektronik ortamda yapılan sözleşmelerde teyid işlemi, yine elektronik ortamda yapılır.

Satıcı ve sağlayıcı, tüketicinin siparişi kendisine ulaştığı andan itibaren otuz gün içerisinde edimini yerine getirir. Bu süre, tüketiciye daha önceden yazılı olarak bildirilmek koşuluyla en fazla on gün uzatılabilir.

Satıcı veya sağlayıcı elektronik ortamda tüketiciye teslim edilen gayri maddi malların veya sunulan hizmetlerin teslimatının ayıpsız olarak yapıldığını ispatla yükümlüdür.

Cayma hakkı süresince sözleşmeye konu olan mal veya hizmet karşılığında tüketiciden herhangi bir isim altında ödeme yapmasının veya borç altına sokan herhangi bir belge vermesinin istenemeyeceğine ilişkin hükümler dışında kapıdan satışlara ilişkin hükümler mesafeli sözleşmelere de uygulanır.

Satıcı veya sağlayıcı cayma bildiriminin kendisine ulaştığı tarihten itibaren

on gün içinde almış olduğu bedeli, kıymetli evrakı ve tüketiciyi bu hukuki işlemden dolayı borç altına sokan her türlü belgeyi iade etmek ve yirmi gün içerisinde de malı geri almakla yükümlüdür.

3.1.7. CEZA HÜKÜMLERİ

Madde 25 - (Değişik madde: 06/03/2003 - 4822 S.K./33. md.;Değişik madde: 23/01/2008-5728 S.K./476.mad)

6 ncı maddenin yedinci fıkrası uyarınca, Bakanlıkça belirlenen usul ve esaslara aykırı hareket edenlere, aykırılığı tespit edilen her bir sözleşme için yüz Türk Lirası idari para cezası verilir.

4 üncü maddenin altıncı fıkrasında, 5 inci maddede, 6 ncı maddenin altıncı fıkrasında, 6/A maddesinde, 6/B, 6/C maddeleri uyarınca Bakanlıkça belirlenen usul ve esaslarda, 7 nci maddenin beşinci fıkrasında, 9 uncu maddede, 9/A maddesinde, 10 uncu maddede, 10/A maddesinde, 10/B maddesinde, 11/A maddesinin ikinci ve dördüncü fıkralarında, 12, 13, 14 ve 15 inci maddelerde belirtilen yükümlülüklerden her birine aykırı hareket edenlere ikiyüz Türk Lirası idari para cezası verilir.

3.1.8. CEZALARDA YETKİ, İTİRAZ ve ZAMANAŞIMI

Madde 26- (Değişik madde: 23/01/2008-5728 S.K./477.mad)
25 inci maddenin birinci, dördüncü, yedinci, sekizinci, dokuzuncu ve onuncu fıkralarındaki idari yaptırımlara Bakanlık tarafından, diğer fıkralarındaki idari para cezalarına mahallî mülkî amir tarafından karar verilir.

Bu yaptırımlara ilişkin kararlar, kararı veren makam tarafından yedi gün içerisinde ilgilinin mensup olduğu meslek kuruluşuna bildirilir.

Bu Kanun hükümlerine göre verilen idari yaptırım kararlarına karşı 6/1/1982 tarihli ve 2577 sayılı İdari Yargılama Usulü Kanunu hükümlerine göre kanun yoluna başvurulur. Ancak, idare mahkemesinde dava, işlemin tebliği tarihinden itibaren onbeş gün içinde açılır. İdare mahkemesinde iptal davası açılmış olması, kararın yerine getirilmesini durdurmaz.

3.1.9. ÇEŞİTLİ HÜKÜMLER

DENETİM
Madde 27 - Bu Kanunun uygulamasında, Bakanlık müfettişleri ve kontrolörleri ile Bakanlıkça ve belediyelerce görevlendirilecek personel; fabrika,

mağaza, dükkan, ticarethane, depo, ambar gibi her türlü mal konulan ve/veya satılan veya hizmet sunulan yerlerde denetleme, inceleme ve araştırma yapmaya yetkilidirler.

Bu Kanunun kapsamına giren hususlarda yetkili ve görevli kişi ve kuruluşlara her türlü bilgi ve belgelerin doğru olarak gösterilmesi ve asıl ve onaylı kopyalarının verilmesi zorunludur.

3.2. MESAFELİ SÖZLEŞMELER UYGULAMA USUL ve ESASLARI

Sanayi ve Ticaret Bakanlığından:
Resmi Gazete Tarihi: 13/06/2003
Resmi Gazete Sayısı: 25137

3.2.1. AMAÇ

Madde 1 - Bu Yönetmeliğin amacı, mesafeli sözleşmeler hakkında uygulama usul ve esaslarını düzenlemektir.

3.2.2. KAPSAM

Madde 2 - Bu Yönetmelik, yazılı, görsel ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan, malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmelere uygulanır.

3.2.3. DAYANAK

Madde 3 - Bu Yönetmelik, 23/02/1995 tarihli ve 4077 sayılı Tüketicinin Korunması Hakkında Kanunun 31 inci ve bu Kanuna 4822 sayılı Kanunla eklenen 9/A maddelerine dayanılarak hazırlanmıştır.

3.2.4. TANIMLAR

Madde 4 - Bu Yönetmeliğin uygulanmasında;

a) Bakanlık: Sanayi ve Ticaret Bakanlığını,
b) Bakan: Sanayi ve Ticaret Bakanını,
c) Mal: Alış-verişe konu olan taşınır eşyayı, konut ve tatil amaçlı taşınmaz malları ve elektronik ortamda kullanılmak üzere hazırlanan yazılım, ses, görüntü ve benzeri gayri maddi malları,

d) Hizmet: Bir ücret veya menfaat karşılığında yapılan mal sağlama dışındaki her türlü faaliyeti,
e) Satıcı: Kamu tüzel kişileri de dahil olmak üzere ticari veya mesleki faaliyetleri kapsamında tüketiciye mal sunan gerçek veya tüzel kişileri,
f) Sağlayıcı: Kamu tüzel kişileri de dahil olmak üzere ticari veya mesleki faaliyetleri kapsamında tüketiciye hizmet sunan gerçek veya tüzel kişileri,
g) Tüketici: Bir mal veya hizmeti ticari veya mesleki olmayan amaçlarla edinen, kullanan veya yararlanan gerçek ya da tüzel kişiyi,
h) Kredi veren: Mevzuatları gereği tüketicilere nakit kredi vermeye yetkili olan banka, özel finans kuruluşu ve finansman şirketlerini,
ı) Mesafeli Sözleşme: Yazılı, görsel, telefon ve elektronik ortamda veya diğer iletişim araçları kullanılarak ve tüketicilerle karşı karşıya gelinmeksizin yapılan ve malın veya hizmetin tüketiciye anında veya sonradan teslimi veya ifası kararlaştırılan sözleşmeleri,
j) (Ek bent: 09/10/2007- 26668 S.R.G. Yön/1.md.) Sürekli veri taşıyıcısı: Tüketicinin, kendisine kişisel olarak gönderilen bilgiyi, bu bilginin amacına uygun olarak makul bir süre incelemesine elverecek şekilde kaydedilmesini sağlayan ve kaydedilen bilgiye aynen ulaşılmasına imkan veren her türlü aracı, ifade eder.

3.2.5. ÖN BİLGİLER

Madde 5 - Tüketici, mesafeli sözleşmenin akdinden önce, aşağıdaki bilgilerin tamamının yer aldığı bilgilendirme formunun verilmesi suretiyle, açık, anlaşılır ve kullanılan iletişim vasıtasına uygun bir şekilde bilgilendirilir.
a) Satıcı veya sağlayıcının isim, unvan, açık adres, telefon ve varsa diğer erişim bilgileri,
b) Sözleşme konusu mal ya da hizmetin temel özellikleri,
c) Sözleşme konusu mal ya da hizmetin tüm vergiler dahil satış fiyatı,
d) Satıcı veya sağlayıcının fiyat dahil tüm vaatlerinin geçerlilik süresi,
e) Tüketicinin ödemelerinin nasıl yapılacağına dair bilgiler,
f) Teslimat ve ifanın nasıl yapılacağına ve varsa buna ilişkin masrafların tutarı ve kimin tarafından karşılanacağına dair bilgiler,
g) Cayma hakkı ve bu hakkın nasıl kullanılacağına dair bilgiler,
h) Tüketiciye bir maliyeti varsa kullanılan iletişim yollarının ücreti,
ı) Sözleşme konusu mal ya da hizmetin, teslim ve ifa tarihlerine ilişkin program,
j) Tüketicinin talep ve şikayetlerini iletebileceği satıcı veya sağlayıcının açık adres, telefon ve varsa diğer erişim bilgileri.
(Ek fıkra: 09/10/2007- 26668 S.R.G. Yön/2.md.) Sözlü iletişim araçlarının kullanılması durumunda, ayrıca satıcı veya sağlayıcının, kimliğini ve

görüşmenin ticari amacını her görüşmenin başında tüketiciye açık bir biçimde bildirmesi zorunludur.

3.2.6. ÖN BİLGİLERİN DOĞRULUĞUNUN YAZILI OLARAK KANITLANMASI

Madde 6 - (Değişik madde: 09/10/2007- 26668 S.R.G. Yön/3.md.)
Bu Yönetmeliğin 5 inci maddesinde belirtilen bilgilendirme formunun, sözleşmenin kurulmasından önce tüketiciye verilmesi zorunludur. Tüketici, bu bilgileri edindiğini yazılı olarak teyit etmedikçe sözleşme akdedilemez. Elektronik ortamda yapılan sözleşmelerde teyit işlemi, yine elektronik ortamda yapılır. Satıcı veya sağlayıcı, mallar için sözleşme konusu mal tüketiciye ulaşmadan, hizmetler için de en geç sözleşmenin ifasından önce yazılı olarak, elektronik ortamda yapılan sözleşmelerde ise tüketici tarafından kullanılabilir veya sürekli olarak erişilebilir başka bir sürekli veri taşıyıcısıyla bilgilendirme formunu tüketiciye ulaştırmak zorundadır.

3.2.7. SÖZLEŞMEDE BULUNMASI GEREKEN ŞARTLAR

Madde 7 - (Değişik fıkra: 09/10/2007- 26668 S.R.G. Yön/4.md.) Mesafeli sözleşmenin, tüketici tarafından kullanılabilir veya sürekli olarak erişilebilir başka bir sürekli veri taşıyıcısıyla tüketiciye verilmesi zorunludur.

Sözleşmede;
a) Tüketicinin, satıcı veya sağlayıcının isim, unvan, açık adres, telefon ve varsa diğer erişim bilgileri,
b) Sözleşmenin düzenlendiği tarih,
c) Malın veya hizmetin teslim veya ifa tarihi ve şekli,
d) Teslimat ve ifaya ilişkin masrafların tutarı ve kimin tarafından karşılanacağına dair bilgiler,
e) Sözleşme konusu malın veya hizmetin cinsi veya türü, miktarı ve varsa marka ve modeli,
f) Malın veya hizmetin Türk Lirası olarak vergiler dahil peşin satış fiyatı,
g) Vadeye göre faiz ile birlikte ödenecek Türk Lirası olarak toplam satış fiyatı,
h) Faiz miktarı, faizin hesaplandığı yıllık oran ve sözleşmede belirtilen faiz oranının yüzde otuz fazlasını geçmemek üzere gecikme faizi oranı,
ı) Peşinat tutarı,
j) Ödeme planı,
k) Borçlunun temerrüde düşmesinin hukuki sonuçları, yer alır.

3.2.8. CAYMA HAKKI

Madde 8 - Tüketici; mal satışına ilişkin mesafeli sözleşmelerde, teslim aldığı tarihten itibaren yedi gün içerisinde hiçbir hukuki ve cezai sorumluluk üstlenmeksizin ve hiçbir gerekçe göstermeksizin malı reddederek sözleşmeden cayma hakkına sahiptir. Hizmet sunumuna ilişkin mesafeli sözleşmelerde ise, bu süre sözleşmenin imzalandığı tarihte başlar. Sözleşmede, hizmetin ifasının 7 günlük süre dolmadan yapılması kararlaştırılmışsa, tüketici ifanın başlayacağı tarihe kadar cayma hakkını kullanabilir. Cayma hakkının kullanımından kaynaklanan masraflar satıcı veya sağlayıcıya aittir.

Elektronik ortamda anında ifa edilen hizmetler ve tüketiciye anında teslim edilen mallara ilişkin sözleşmeler cayma hakkı ve kullanımına ilişkin hükümlere tabi değildir.

Malın teslimi sözleşmeye taraf olan tüketici dışında bir kişiye yapılsa dahi tüketici cayma hakkını kullanabilir. Bu durumda satıcı malı 9 uncu maddenin dördüncü fıkrası hükmü uyarınca üçüncü kişiden teslim alır.

Tüketicinin özel istek ve talepleri uyarınca üretilen veya üzerinde değişiklik ya da ilaveler yapılarak kişiye özel hale getirilen mallarda tüketici cayma hakkını kullanamaz. Ayrıca tüketici, niteliği itibariyle iade edilemeyecek, hızla bozulma veya son kullanma tarihi geçme ihtimali olan mallar söz konusu olduğunda cayma hakkını kullanamaz.

(Değişik fıkra: 09/10/2007- 26668 S.R.G. Yön/5.md.) Satıcı veya sağlayıcının 6 ncı veya 7 nci maddede belirtilen yükümlülüklerini yerine getirmemesi halinde, satıcı veya sağlayıcı en geç otuz gün içerisinde eksikliği giderir. Bu durumda yedi günlük süre, söz konusu eksikliğin giderildiğine dair bilginin yazılı olarak tüketiciye ulaştırıldığı tarihten itibaren başlar. Aksi takdirde, tüketici cayma hakkını kullanmak için yedi günlük süre ile bağlı değildir.

Tüketicinin ödediği bedel kısmen veya tamamen satıcı veya sağlayıcı tarafından ya da satıcı veya sağlayıcı ile kredi veren arasındaki anlaşmaya dayanılarak karşılanıyorsa, cayma hakkının kullanılması halinde, kredi sözleşmesi de hiçbir tazminat veya cezai şart tutarını ödeme yükümlülüğü söz konusu olmaksızın kendiliğinden sona erer. Ancak bunun için, cayma bildiriminin kredi verene de yazılı olarak iletilmesi gerekir.

3.2.9. SATICI ve SAĞLAYICININ YÜKÜMLÜLÜĞÜ

Madde 9 - Satıcı veya sağlayıcı tüketicinin siparişi kendisine ulaştırdığı andan itibaren en geç otuz gün içerisinde edimini yerine getirmekle yükümlüdür. Bu süre tüketiciye daha önceden yazılı olarak bildirilmek koşuluyla en fazla on gün uzatılabilir.

Satıcı veya sağlayıcı, tüketicinin cayma bildiriminin kendisine ulaştığı tarihten itibaren on gün içinde almış olduğu bedeli, kıymetli evrakı ve tüketiciyi borç altına sokan her türlü belgeyi iade etmekle, ayrıca yirmi gün içinde de malı geri almakla yükümlüdür.

(Değişik fıkra: 09/10/2007- 26668 S.R.G. Yön/6.md.) Satıcı veya sağlayıcı mesafeli sözleşme konusu malın veya hizmetin tüketiciye teslimi veya ifasından önce 5 inci maddede yer alan bilgiler ile 7 nci maddede yer alan sözleşmeyi tüketiciye vermek ve 6 ncı maddede belirtilen yükümlülükler dahilinde ön bilgilerin teyidine ilişkin onayı almak zorundadır. Uyuşmazlık halinde ispat külfeti satıcı veya sağlayıcıya aittir.

Haklı bir sebebe dayanmak şartıyla satıcı veya sağlayıcı, sözleşmeden doğan ifa yükümlülüğünün süresi dolmadan ve sözleşmede belirtmesi şartıyla, tüketiciye eşit kalite ve fiyatta mal veya hizmet tedarik edebilir.

Satıcı veya sağlayıcı, sipariş konusu mal veya hizmetin yerine getirilmesinin imkansızlaştığını ileri sürerek, sözleşme konusu yükümlülüklerini yerine getiremiyorsa, bu durumu, sözleşmeden doğan ifa yükümlülüğünün süresi dolmadan tüketiciye bildirir. Ödemiş olduğu bedel ve borç altına sokan tüm belgeleri 10 gün içinde tüketiciye iade eder.

3.2.10. GERİ ÖDEME

Madde 10 - Mesafeli sözleşmelerde, ödemenin kredi kartı veya benzeri bir ödeme kartı ile yapılması halinde tüketici, kartın kendi rızası dışında ve hukuka aykırı biçimde kullanıldığı gerekçesiyle ödeme işleminin iptal edilmesini talep edebilir. Bu halde, kartı çıkaran kuruluş itirazın kendisine bildirilmesinden itibaren 10 gün içinde ödeme tutarını tüketiciye iade eder.

3.2.11. KAPSAM DIŞI SÖZLEŞMELER

Madde 11 - Bu Yönetmelik hükümleri;
a) Banka, sigorta ile ilgili,
b) Otomatik satış makineleri vasıtasıyla akdedilen,

c) Halka açık jetonlu telefonlar vasıtasıyla akdedilen,
d) Açık arttırma yolu ile akdedilen,
e) Gıda, içecek ve günlük tüketim için tüketicinin evine veya işyerine düzenli olarak sağlanan malların tedariki ile ilgili,
f) Sağlayıcının üstlendiği, barınma, ulaşım, yemek tedariki, sportif ve kültürel faaliyetler ve eğlence hizmetlerini özel bir günde veya sürede tedarik etmesine ilişkin hükümler içeren,
sözleşmelere uygulanmaz.

3.2.12. YÜRÜRLÜK ve YÜRÜTME

Madde 12 - Bu Yönetmelik 14/06/2003 tarihinde yürürlüğe girer.
Madde 13 - Bu Yönetmelik hükümlerini Sanayi ve Ticaret Bakanı yürütür.

3.3. TÜRK CEZA KANUNU

3.3.1. KİŞİSEL VERİLERİN KAYDEDİLMESİ

Madde 135 - (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

3.3.2. VERİLERİ HUKUKA AYKIRI OLARAK VERME veya ELE GEÇİRME

Madde 136 - (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

3.3.3. NİTELİKLİ HALLER

Madde 137 - (1) Yukarıdaki maddelerde tanımlanan suçların;
a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,
b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, işlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

3.3.4. VERİLERİ YOK ETMEME

Madde 138 - (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.

3.3.5. ŞİKAYET

Madde 139 - (1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır.

3.3.6. TİCARİ SIR, BANKACILIK SIRRI veya MÜŞTERİ SIRRI AÇIKLANMASI

Madde 239 - (1) Sıfat veya görevi, meslek veya sanatı gereği vakıf olduğu ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgeleri yetkisiz kişilere veren veya ifşa eden kişi, şikayet üzerine, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. Bu bilgi veya belgelerin, hukuka aykırı yolla elde eden kişiler tarafından yetkisiz kişilere verilmesi veya ifşa edilmesi hâlinde de bu fıkraya göre cezaya hükmolunur.

(2) Birinci fıkra hükümleri, fenni keşif ve buluşları veya sınai uygulamaya ilişkin bilgiler hakkında da uygulanır.

(3) Bu sırlar, Türkiye'de oturmayan bir yabancıya veya onun memurlarına açıklandığı takdirde, faile verilecek ceza üçte biri oranında artırılır. Bu halde şikayet koşulu aranmaz.

(4) Cebir veya tehdit kullanarak bir kimseyi bu madde kapsamına giren bilgi veya belgeleri açıklamaya mecbur kılan kişi, üç yıldan yedi yıla kadar hapis cezasıyla cezalandırılır.

3.3.7. BİLİŞİM SİSTEMİNE GİRME

Madde 243 - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

3.3.8. SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME veya DEĞİŞTİRME

Madde 244 - (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezasına hükmolunur.

3.3.9. BANKA veya KREDİ KARTLARININ KÖTÜYE KULLANILMASI

Madde 245 - (Değişik madde: 29/06/2005-5377 S.K./27.mad)
(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

(4) Birinci fıkrada yer alan suçun;
a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,
c) Aynı konutta beraber yaşayan kardeşlerden birinin,
Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) (Ek fıkra: 06/12/2006 - 5560 S.K.11.md) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır.

3.3.10. TÜZEL KİŞİLER HAKKINDA GÜVENLİK TEDBİRİ UYGULAMASI

Madde 246 - (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

3.4. BANKA KARTLARI ve KREDİ KARTLARI KANUNU

Kanun Numarası : 5464
Kanun Kabul Tarihi : 23/02/2006
Resmi Gazete Tarihi : 01/03/2006
Resmi Gazete Sayısı : 26095

3.4.1. AMAÇ

Madde 1 - Bu Kanunun amacı; banka kartları ve kredi kartlarının çıkarılmasına, kullanımına, takas ve mahsup işlemlerine ilişkin usûl ve esasları düzenlemek suretiyle kartlı ödemeler sisteminin etkin çalışmasını sağlamaktır.

3.4.2. KAPSAM

Madde 2 - Kartlı sistem kuran, kart çıkaran, üye işyeri anlaşması yapan kuruluşlar ile üye işyerleri ve kart hamilleri bu Kanun hükümlerine tabidir.

Kendi işyerleri ile sınırlı olmak üzere, mal veya hizmetlerin vadeli satışı ile alıcının borç alacak durumunun izlenmesi amacıyla kart çıkaran veya sistem oluşturan veya herhangi bir kredilendirme işlemi yapılmaksızın veya hesaba bağlı olmaksızın önceden belirlenen bir tutarla sınırlı olmak üzere kart düzenleyen gerçek veya tüzel kişiler bu Kanun hükümlerine tâbi değildir.

3.4.3. TANIMLAR

Madde 3 - Bu Kanunun uygulanmasında;

a) Kurul: Bankacılık Düzenleme ve Denetleme Kurulunu,
b) Kurum: Bankacılık Düzenleme ve Denetleme Kurumunu,
c) Banka: Mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını,
d) Banka kartı: Mevduat hesabı veya özel cari hesapların kullanımı dahil bankacılık hizmetlerinden yararlanmayı sağlayan kartı,
e) Kredi kartı: Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını,
f) Kartlı sistem kuruluşu: Banka kartı veya kredi kartı sistemi kuran ve bu sisteme göre kart çıkarma veya üye işyeri anlaşması yapma yetkisi veren kuruluşları,
g) Kart çıkaran kuruluş: Banka kartı veya kredi kartı düzenleme yetkisini haiz bankalar ile diğer kuruluşları,
h) Üye işyeri anlaşması yapan kuruluş: Banka kartı veya kredi kartı kabulünü sağlamak amacıyla işyerleriyle anlaşma yapan bankalar ya da kuruluşları,
i) Üye işyeri: Üye işyeri anlaşması yapan kuruluşlar ile yaptığı sözleşme çerçevesinde kart hamiline mal ve hizmet satmayı veya nakit temin etmeyi kabul eden gerçek veya tüzel kişiyi,
j) Kart hamili: Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişiyi,
k) Harcama belgesi: Banka kartı veya kredi kartı ile yapılan işlemler ile ilgili olarak üye işyeri tarafından düzenlenen, kart hamilinin işlemden doğan borcu ile diğer bilgileri gösteren ve kart hamilinin kimliğinin bir kod numarası, şifre veya kimliği belirleyici başka bir yöntemle belirlendiği haller dışında kart hamili tarafından imzalanan belgeyi,
l) Nakit ödeme belgesi: Bankalarca veya yetkili üye işyerlerince banka kartı veya kredi kartı hamiline yapılan nakit ödemelerde düzenlenerek, kart hamilinin kimliğinin bir kod numarası, şifre veya kimliği belirleyici başka bir yöntemle belirlendiği haller dışında kart hamili tarafından imzalanan belgeyi,
m) Son ödeme tarihi: Kart hamilinin, dönem borcunu veya ödemesi gereken asgari tutarını gecikmeye düşmeden ödeyebileceği son günü,
n) Dönem borcu: Hesap kesim tarihine kadar oluşan borç ve alacak kayıtlarının bakiyesi ile önceki hesap özeti bakiyesinin toplamını,
o) Asgari tutar: Dönem borcunun ödenmesi gereken en az tutarını,
p) Alacak belgesi: Banka kartı veya kredi kartı kullanılarak alınmış olan malın iadesi veya hizmetin alımından vazgeçilmesi veya yapılan işlemin

iptali halinde kart hamilinin hesabına alacak kaydedilmek üzere üye işyeri tarafından düzenlenen belgeyi,
r) Bildirim, talep, şikâyet ve itirazlar: Kart hamilinin yazılı olarak, elektronik ortamda veya telefon ile yapacağı bildirim, talep, şikâyet ve itirazları, ifade eder.

3.4.4. KARTIN HAKSIZ KULLANILMASI ve SİGORTALANMASI

Madde 12 - Kartın ya da 16 ncı maddede belirtilen bilgilerin kaybolması veya çalınması halinde kart hamili, yapacağı bildirimden önceki yirmidört saat içinde gerçekleşen hukuka aykırı kullanımdan doğan zararlardan yüzelli Yeni Türk Lirası ile sınırlı olmak üzere sorumludur. Hukuka aykırı kullanımın, hamilin ağır ihmaline veya kastına dayanması veya bildirimin yapılmaması hallerinde bu sınır uygulanmaz.

Kart çıkaran kuruluş, yapılacak talep ve ilgili sigorta prim bedelinin ödenmesi koşulu ile kart hamilinin birinci fıkrada belirtilen yüzelli Yeni Türk Lirası tutarındaki sorumluluğunun sigortalanmasını sağlamakla yükümlüdür. Kartların sigortalanması ve sorumluluğun paylaşılmasına ilişkin usûl ve esaslar Kurum tarafından çıkarılacak yönetmelikle belirlenir.

3.4.5. KARTIN KONTROL ve KABULÜ

Madde 17 - Üye işyerleri, kart hamillerinin yapmış oldukları mal ve hizmet alımlarının bedelini banka kartı ya da kredi kartı ile ödeme taleplerini kabul etmek zorundadır. Bu zorunluluk indirim dönemlerinde de geçerlidir. Üye işyerleri, kart hamilinden kartın kullanılması dolayısıyla komisyon veya benzeri bir isim altında ilave bir ödemede bulunmasını isteyemez. Bu hükme aykırı davranılması halinde, üye işyeri anlaşması yapan kuruluşlar tarafından üye işyeri sözleşmesi feshedilir ve bir yıl süreyle yeni bir sözleşme yapılamaz.

Üye işyerleri, mal ve hizmet bedeli karşılığını banka kartı veya kredi kartı ile ödemek isteyen kişilerin imza gerektiren işlemlerde imza kontrolünü yapmak, kartın tahrifata uğrayıp uğramadığını kontrol etmek ve üye işyeri anlaşması yapan kuruluşlarca kendilerine ulaştırılan bilgiler çerçevesinde kartın geçerliliğini tespit etmekle yükümlü olup, gerekli durumlarda kart üzerinde yer alan bilgilerle kimlik belgesi üzerinde yer alan bilgileri karşılaştırmak üzere geçerli bir kimlik belgesi ibrazını talep etmek ve harcama belgesi üzerindeki bilgilerle kredi kartı üzerindeki bilgileri karşılaştırarak kontrol etmekle yükümlüdür. Bu kontrollerin yapılmamasından doğan zararlardan üye işyerleri sorumludur.

3.4.6. BİLGİLENDİRME SİSTEMİN GÜVENLİĞİNİN SAĞLANMASI

Madde 18 - Üye işyerleri, banka kartı ve kredi kartı ile işlem yapıldığını gösteren işaretleri, işyerinin girişinde ve kart hamilleri tarafından kolayca görülebilecek bir yere koymak, üye işyeri sözleşmeleri herhangi bir nedenle sona erdiği takdirde de, bu işaretleri kaldırmakla yükümlüdür. Üye işyerleri, teknik bir nedenle geçici bir süreyle işlem yapılamadığı hallerde kart hamillerini uyarmakla yükümlüdür.

Üye işyerleri, 20 nci madde uyarınca harcama belgesi düzenlenmeksizin çeşitli iletişim araçları yoluyla veya sipariş formu vasıtasıyla işlem yapılmasına olanak sağlamak üzere kuracakları sistemlerin güvenli bir şekilde çalışmasını temin etmekle yükümlüdür.

3.4.7. HARCAMA ve ALACAK BELGESİ

Madde 19 - Üye işyerleri, mal ve hizmet bedellerinin banka kartı ya da kredi kartı ile ödenmesi veya nakit talep edilmesi halinde, 20 nci madde hükümleri saklı kalmak kaydıyla, elektronik ya da mekanik cihazları kullanarak harcama belgesi veya nakit ödeme belgesi düzenlemek ve aslını sözleşmede belirtilen süre içinde muhafaza etmek ve bir nüshayı da kart hamiline vermek zorundadır. Bu hükme aykırılık halinde satılan hizmet veya mal bedeli üye işyeri anlaşması yapan kuruluştan talep edilemez.

Üye işyerleri kart kullanılarak satın alınmış bir malın iadesi veya hizmetin alımından vazgeçilmesi veya yapılan işlemin iptali halinde, alacak belgesi düzenleyerek bir nüshasını kart hamiline verdikten sonra diğer bir nüshayı da muhafaza etmekle yükümlüdür.

3.4.8. İMZA GEREKTİRMEYEN İŞLEMLER

Madde 20 - İşlemin niteliği nedeniyle harcama ve alacak belgesi düzenleme imkanı olmayan hallerde kartlar, hamil tarafından çeşitli iletişim araçları ile kart numarası bildirilmek veya imza yerine geçen kod numarası, şifre ya da kimliği belirleyici benzeri başka bir yöntemle işlem yapılmak suretiyle de kullanılabilir.

3.4.9. BİLGİLERİN SAKLANMASI

Madde 23 - Üye işyerleri, kartın kullanımı sonucunda kart ve kart hamili ile ilgili edindikleri bilgileri, kanunla yetkili kılınan kişi, kurum ve kuruluşlar hariç olmak üzere kart hamilinin yazılı rızasını almadan başkasına

açıklayamaz, saklayamaz ve kopyalayamaz. Üye işyerleri, kart bilgilerini üye işyeri anlaşması yaptığı kuruluş dışındaki şahıs veya kuruluşlarla paylaşamaz, satamaz, satın alamaz ve takas edemez. Üye işyeri anlaşması yapan kuruluşlar, bu fıkranın uygulanmasını gözetmekle yükümlüdür.

Kart çıkaran kuruluşlar, edindikleri kişisel bilgileri gizli tutmak, kendi hizmetlerinin pazarlanması dışında başka amaçlarla kullanmamak ve kanunla yetkili kılınan kişi, kurum ve kuruluşlar dışında kalanların bu bilgilere ulaşmasını engellemek amacıyla gereken önlemleri almakla yükümlüdür.

3.4.10. SIRLARIN SAKLANMASI

Madde 31 - Kurul üyeleri ile Kurum personeli, görevleri sırasında öğrendikleri bu Kanun kapsamındaki kuruluşlara, kart hamillerine ve kefillere ait sırları kanunen açıkça yetkili olanlardan başkasına açıklayamaz ve kendi yararlarına kullanamazlar.

Kartlı sistem kuran, kart çıkaran, üye işyeri anlaşması yapan kuruluşlar, 29 uncu maddede yer alan kuruluşlar ile üye işyerleri, bunların ortakları, yönetim kurulu üyeleri, mensupları, bunlar adına hareket eden kişiler ile görevlileri, sıfat ve görevleri dolayısıyla öğrendikleri sırları kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamazlar. Kart çıkaran kuruluşların destek hizmeti aldığı kuruluş ve çalışanları hakkında da bu hüküm uygulanır.

3.4.11. İSPAT YÜKÜ

Madde 32 - Kart numarası bildirilmek suretiyle üye işyerinden telefon, elektronik ortam, sipariş formu veya diğer iletişim araçları yoluyla yapılan işlemlerden doğacak anlaşmazlıklarda ispat yükü üye işyerine aittir.

3.4.12. ÖZEN YÜKÜMLÜLÜĞÜ

Madde 33 - Kartlı sistem kuran, kart çıkaran, üye işyeri anlaşması yapan kuruluşlar ve üye işyerleri bu Kanun ve ilgili düzenlemeler ile getirilen yükümlülüklerin yerine getirilmesinde gerekli basiret ve özeni göstermekle yükümlüdür.

3.4.13. BİLGİ GÜVENLİĞİ YÜKÜMLÜLÜĞÜNE AYKIRI DAVRANILMASI

Madde 39 - Bu Kanunun 8 inci maddesinin beşinci fıkrası ve 23 üncü maddesi hükümlerine kasten aykırı hareket eden kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevlileri ve işlemi yapan kişiler, bir yıldan üç yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılırlar.

Kartların kullanılması için zorunlu olup gizli kalması gereken kod numarası, kart numarası, şifre ya da kimliği belirleyici başka bir yöntemin dikkatsizlik veya tedbirsizlik veya meslekte yetersizlik veya emir ve kurallara aykırılık nedeniyle açığa çıkmasına neden olan kart çıkaran kuruluşlar, üye işyerleri ve üye işyeri anlaşması yapan kuruluşların işlerini fiilen yöneten görevli ve ilgili mensupları bin güne kadar adli para cezası ile cezalandırılırlar.

KAYNAKÇA

[1] AHUJA, Vijay, Secure Commerce on the Internet, Academic Press 1997.

[2] ARSLAN, İ. Yılmaz, Tüketici Hukuku Dersleri, Bursa, 2006

[3] ATAMER, Yeşim, Tüketicinin Korunması Hakkında Kanun M.9/A ve Mesafeli Sözleşmelere İlişkin Uygulama Usul ve Esasları Hakkında Yönetmelik'in Avrupa Birliği Mevzuatı İle Uyumuna İlişkin Görüş ve Değişiklik Önerileri,
http://www.bilisimsurasi.org.tr/hukuk/docs/yesim_atamer_rapor.doc

[4] BECENİ, Yasin, SEVİM, Tuğrul; Adli Bilişim ve Hukuk, Güncel Hukuk Dergisi, 2009 Mart

[5] CERT, Home Network Security,
http://www. cert.org/tech_tips/home_networks.html

[6] ENTREPRENEUR.COM, Exploring E-Commerce,
http://www.entrepreneur.com/growyourbusiness/howtoguides/article81238.html

[7] US Department of Commerce. Defining the Electronic Commerce Sector,
http://ita.doc.gov/investamerica/ecommerce.asp

[8] WINKLER, Ira, Case Study of Industrial Espionage Through Social Engineering, Proceedings of 1996 ISSA Conference, 1996.

İTO YAYINLARI (2009)

2009-1	Züccaciye-Turizm Sektörleri Ekonomik Etkileşimi
2009-2	Züccaciye-Turizm Sektörleri Ekonomik Etkileşimi (Broşür)
2009-3	Organik Tarım Bakımından Türkiye'nin Potansiyeli, Bugünkü Durumu ve Geleceği
2009-4	Sosyal Güvenlik ve Vergi Mevzuatındaki Düzenlemelerin Etkileri
2009-5	Profesyonel Mutfak ve Ekipmanları İçin Avrupa Direktifleri ve Standartlarının Uygulama Rehberi
2009-6	Haberlerden Yansıyan İTO: 2005-2008
2009-7	Toptancı Hallerin Tarım Sektörüne Katkıları ve Ekonomideki Önemi (Cd)
2009-8	Dünden Bugüne İstanbul'da Yaygın Eğitim
2009-9	E-Ticaret Güvenlik Rehberi
2009-10	Türkiye'de Optometrik Ürünler Sektörü
2009-11	Meslek Dalları İtibariyle İstanbul'daki Meslek Liseleri
2009-12	Fiyat İndeksleri (=Price Indices)
2009-13	İstanbul Balık Hali'nin Pazarlama ve Satış Durumu
2009-14	Türkiye'de ve Dünyada Tarımsal Destekleme Politikası
2009-15	Türkiye'de Madencilik
2009-16	Düzenleyici Etki Analizi Rehberi
2009-17	İstanbul'da Kırk Yıllık 40 Lezzet Durağı (=40 Relais Gourmands, 40 Ans d'Histoire des Saveurs d'İstanbul)
2009-18	Türkiye'de Otelcilik ve Kongre Turizminin Geliştirilmesi
2009-19	Halkla İlişkiler Yönetimi
2009-20	Geçmişten Günümüze İstanbul Hanları
2009-21	Herkes İçin Ekonomi
2009-22	Makroekonomik Göstergeler (=Macroeconomic Indicators)
2009-23	İşletmelerde İş Etiği
2009-24	Özürlüler Vadisi
2009-25	Telif Hukukunda Yayın Sözleşmesi Örnekleri

2009-26 Vergi-Sosyal Güvenlik ve Ticaret İşlemleri Açısından Fatura Uygulama Rehberi
2009-27 KOBİ Girişimcileri İçin Yatırım Projelerinin Hazırlanması ve Değerlendirilmesi
2009-28 İstanbul'un Esnaf Lokantaları (İngilizce-Almanca)
2009-29 Forty Years Old 40 Taste Havens in İstanbul (=Geschmacksoasen in İstanbul 40 Vierzig Jahre Tradition)
2009-30 Dünden Bugüne Kapalıçarşı:İstanbul
2009-31 Yaşayıp Unuttuğumuz İstanbul
2009-32 Türkiye'de Regülasyon ve Özelleştirmelerin Gelir Dağılımı Etkileri
2009-33 Türk İşletme Kültüründe Ortaklık ve Güven
2009-34 Devletin Bankacılık Sektöründe Düzenleyici Denetleyici Rolü ve Türkiye Uygulaması
2009-35 Türk Bankacılık Sektöründe Pazar Hakimiyeti ve Sektörün Rekabet Gücünün Uygumalı Analizi
2009-36 E-İhale
2009-37 Türkiye İnşaat Sektörü Hammadde Haritası
2009-38 İstanbul Ticaret Odası Yayın Broşürü
2009-39 Dersaadet Ticaret Odası 1882-1923: Türkiye Ticaretin Öncü Kuruluşu
2009-40 2010 Avrupa Kültür Başkenti İstanbul'da Gıda İşyerlerinin Potansiyeli Paneli (DVD)
2009-41 Türkiye İlaç Sanayi
2009-42 Türkiye'de Tıbbi Cihaz ve Malzeme Üretimi
2009-43 Türkiye'de Tıbbi Cihaz ve Malzeme İthalatı, Yarattığı Kayıplar ve Çözüm Önerileri
2009-44 Yeni Perakendecilik Sisteminde Toptancı Hallerinin İzlemesi Gereken Stratejiler
2009-45 İstanbul'un Ekonomik ve Sosyal Göstergeleri
2009-46 Social and Economıc Indicators of Istanbul
2009-47 Rakamlarla Türkiye Ekonomisi

2009-48 Turkey in Figures
2009-49 Türkiye'de Yayın Hayatı (Türkçe-İng-Alm.Fr.)
2009-50 Başarılı İhracatçılar 2008 (=Outstanding Exporters 2008)
2009-51 Sürdürülebilir kalkınma, yenilenebilir enerji kaynakları ve hidrojen enerjisi: Türkiye Değerlendirmesi
2009-52 2008 Yılı İstanbul Küçük Sanayi Kapasite Kullanım Araştırması
2009-53 Başarılı Vergi Mükellefleri: 2008 (Kitap-CD)
2009-54 Toplantı Yönetimi ve Kararlara Katılma
2009-55 Liderlik Sitilleri, Değişim Yönetimi ve Ekip Çalışması
2009-56 Ahilik Kuruluşu, İlkeleri ve Fonksiyonları (Broşür)
2009-57 İTO Bilgi Merkezi ve Uluslararası Ticari Sınıflandırma Sistemi
2009-58 Yaşayıp Unuttuğumuz İstanbul (2.bs.)

İTO YAYINLARI (2010)

2010-3 Bir Zamanlar İstanbul: Şehir Mektupları(2.bs.)

- Mart itibariyle

Not: 2004 Yılı ve Sonrası Çıkan Bütün Yayınlarımıza İnternet Sitemizden Tam Metin Olarak Ücretsiz Ulaşılabilmektedir.

e-TİCARET GÜVENLİK REHBERİ

Elektronik ticaret iş modelleri sistemlerinin kurulmuş oldukları bilgisayar ve ağ sistemlerinin açık sistemler olması ve teknolojideki gelişmelerle birlikte kötü niyetli kişilerin istismarına açık olmaları sebebiyle, e-ticaretin teknik ve hukuksal boyutları irdelenerek, güvenli e-ticaret ortamının nasıl oluşturulabileceğini irdeleme amacıyla hazırlanan "e-Ticaret Güvenlik Rehberi" isimli bu çalışma üç bölümden oluşmaktadır. Çalışmada elektronik ticaret güvenliği konusunda teknik ve hukuksal açılımlar ile elektronik ticaretle alakalı kanun ve yönetmelikler konu başlıkları irdelenmiş; uygulamacılar açısından özellikle elektronik ticaret kanalıyla iş yapmak isteyen kişi ve kuruluşlar için rehber niteliğinde bilgiler ile önemli ipuçları verilmeye; akademisyenler açısından ise son yıllarda büyük bir ilgi toplayan elektronik ticarette güvenlik sorunu tartışmalarına önemli bir entelektüel birikim sağlanmaya çalışılmıştır.

SKB 0594094 VİZ
KÜLTÜR ve TURİZM BAKANLIĞI

(Elektronik) ISBN 978-9944-60-464-2

ISBN 978-9944-60-463-5
9 789944 604635

002039 2

İSTANBUL TİCARET ODASI 1882
İSTANBUL TİCARET ODASI