Riigi Infosüsteemi Amet

Küberturvalisus 2018

Sisukord

Sissejuhatus: olukord Eesti ja rahvusvahelises küberruumis

Hea lugeja!

Möödunud aasta oli maailma küberruumis erakordselt sündmusrikas. Globaalselt kahju põhjustanud pahavarakampaaniad, ulatuslikud andmelekked ja fundamentaalsed turvanõrkused seni turvaliseks peetud tehnoloogiates pakkusid kogu aasta jooksul avalikkusele kõneainet. Kasvas üldine teadlikkus küberohtudest, aga ka arusaam seniste saavutuste piiratusest. Küpsenud on laiem ühiskondlik ja rahvusvaheline valmidus anda küberturvalisuse tagamisele sisu, mis läheb kaugemale pelgast selle tähtsuse nentimisest.

Eesti küberturvalisusele võib möödunud aastat pidada heaks aastaks. Tulime hästi toime mitme suure väljakutsega, mis andsid meile enesekindlust, et oleme enda kaitsmiseks küberruumis valinud õige viisi, ning julguse ja vajalikud õppetunnid edasi liikumiseks. Selles vallas oli olulisimaks sündmuseks Eestis kindlasti ID-kaardi päästmine. Üleilmset mõju omanud turvanõrkusele reageerides näitasime, et meie eduka küberriigi kuvand põhineb tugeval sisul, milleks on kiire ja paindlik lähenemine ning toimiv kogukond – ettevõtted, teadusasutused ja riik –, kes suudab tegutseda koostöös. Selles mõttes oli ID-kaardi päästmine kasulik kriis – meil on praktiline ja omal nahal läbi elatud kogemus, et saame oma digitaalse ühiskonna kaitsmisega hakkama. ID-kaardi ja e-teenuste kasutamine on jätkunud nagu enne kriisi, inimeste usaldus e-teenuste vastu on säilinud. Kogu ühiskond mõistab paremini küberohtude olemust ja seda, missugune on nende võimalik mõju harjumuspärasele eluviisile. Samas saime ühiskonnana elulise kogemuse, et küberturvalisuses on meil kõigil oma roll: tavakasutajal, teenuseosutajal ja IT-taristu pakkujal. Kõik see teeb ID-kaardi päästmise õppetunnid kohaldatavaks ka laiemalt meie digitaalse eluviisi kaitseks.

ID-kaardi kiibil avastatud turvanõrkus pole ainus omasugune, eelmine aasta tõi mitu vähemalt sama kaalukat näidet, kus aastaid laialdaselt kasutusel olnud ja turvaliseks peetud tehnoloogial on avastatud turvanõrkus – mullu sügisel avastatud WiFi protokolli haavatavus ja pea kõigi arvutite protsessorite turvavead on vaid mõned näited selles reas. Üha enam kasutusel olevate lahenduste nõrkusi otsivad nii teadusasutused, riigid kui kriminaalid ning võib üsna kindel olla, et täna turvalist lahendust tuleb homme paikama asuda.

Eestit suhteliselt vähe puudutanud WannaCry ja NotPetya pahavarakampaaniad said ohtralt rahvusvahelist kõlapinda ning tõid möödunud aasta ühe olulisema positiivse trendi – rahvusvahelise kogukonna valmiduse omistada küberrünnakud nende läbiviijatele. Põhja-Korea ja Venemaa korraldatud küberrünnakute eesmärk ei olnud teenida raha, vaid toetada nende riikide poliitilisi eesmärke. Kui veel paar aastat tagasi ei toonud küberruumi pahatahtlik kasutamine riikide poolt oma eesmärkide saavutamiseks kaasa mingeid olulisi negatiivseid tagajärgi, siis just WannaCry ja NotPetya järel on astutud esimesed suured sammud, et panna pahategijad vastutust kandma ja heidutada neid edasisi ründeid ära jätma. Selles kontekstis tasub ära märkimist Eesti eesistumise ajal heakskiidu saanud Euroopa Liidu küberdiplomaatia raamistik, mille abil riiklikele küberrünnakutele reageerida. Eesti eesistumise aega langes ka oluline Euroopa küberturvalisuse keskkonna uuendamine, millele Eestile omane eesmärgile suunatud lähenemine hoogu andis.

Kõige eelneva kõrval liikusime jõudsalt edasi ka Eesti enda küberturvalisuse arendamisel, millest vast olulisemana saab välja tuua küberturvalisuse seaduse eelnõu, mida riigikogu praegu menetleb.

Digitaalsest tehnoloogiast sõltub suur osa meie igapäevasest elukorraldusest. Ärgem siis unustagem, et küberturvalisust loome me kõik, olgu tavakasutajana, juhina, poliitikuna või muus rollis. Lisaks huvitavale ülevaatele, mis küberruumis toimumas, aitab järgnev lugemine lahti mõtestada, kuidas igaüks meist saab panustada, et Eesti oleks küberruumis paremini kaitstud.

Taimar Peterkop
Riigi Infosüsteemi Ameti peadirektor

SÜNDMUSED EESTI KÜBERRUUMIS 2017

2017. aasta arvudes

Olgugi et eelmisel aastal registreerisime Eesti küberruumis esmakordselt enam kui 10 000 küberturbejuhtumit, oli niisuguseid intsidente, millel otsene mõju mõnele riigi ja ühiskonna toimimiseks olulisele teenusele, vaid 122, mis on viimase kolme aasta madalaim näitaja.

Eestis registreeritud küberturbejuhtumite arv ületas mullu 10 000 piiri: 2017. aastal käsitles RIA Eesti arvuti- ja andmesidevõrkudes kokku **10 923** juhtumit. Küberturbeintsidendina – see tähendab juhtumina, millega kaasnes otsene mõju teabe või süsteemide konfidentsiaalsusele, terviklusele või kättesaadavusele – tuvastati neist üle veerandi ehk **3162** juhtumit.

Põhjused juhtumite taga on väga erinevad – seadmerikkest ja inimlikust eksimusest pahatahtliku tegevuseni. Nagu varasematel aastatel, on kõige sagedamini endiselt tegu kõikvõimalikku pahavara levitavate veebidomeenide ja e-kirjadega. Kaugeltki iga intsidendi taga pole küberrünne ning paljud ründekatsed ka peatatakse, mistõttu kahju ei tekigi.

Eesti küberturvalisuse seisukohast on kõige olulisemad just need teenused, millel on määrav mõju ühiskonna harjumuspärase toimimise ja inimeste turvatunde jaoks. Seesuguseid riigi ja ühiskonna toimimiseks olulist teenust mõjutanud ehk kõrge reageerimisprioriteediga intsidente oli mullu **122** – see on viimase kolme aasta madalaim näitaja. Mõjutatud teenuste seas oli näiteks elektroonilise isikutuvastuse ja digiallkirjastamise kasutus sideoperaatorite võrkudes, tervishoiu- ja pangateenused. Neist kirjutame siinses kokkuvõttes lähemalt.

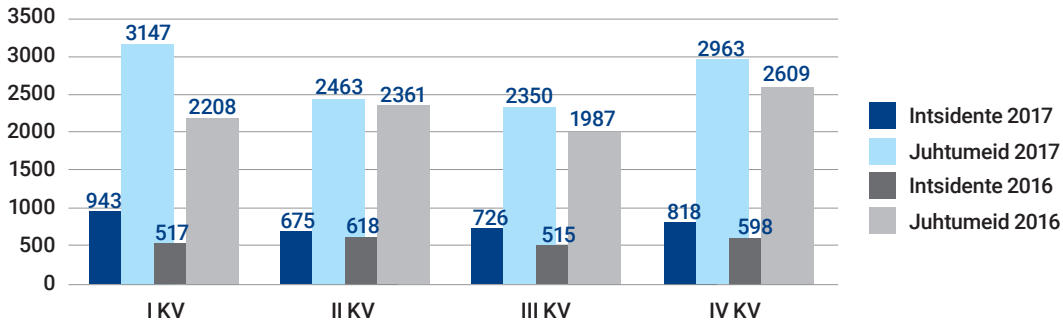
2017 KOKKUVÕTTES

10 923
käsitletud juhtumit

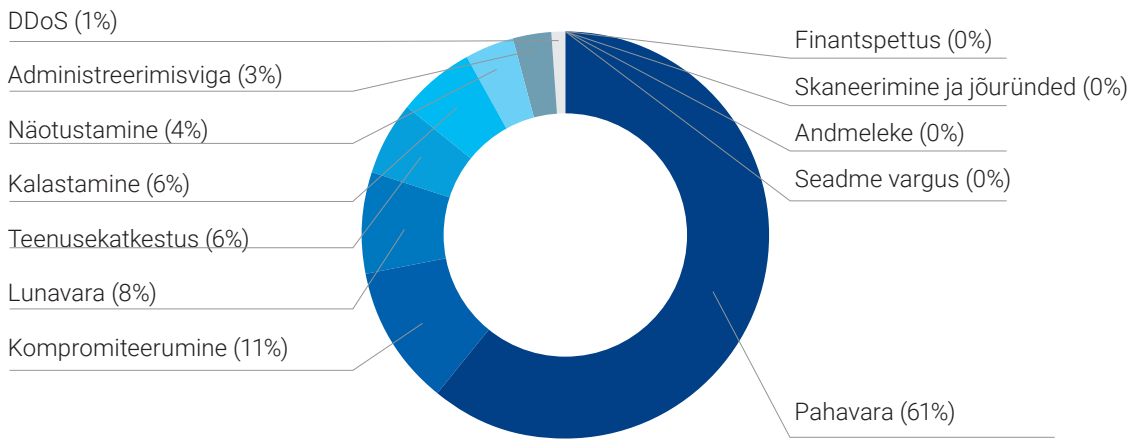
3162
küberintsidenti

122
kõrge prioriteediga intsidenti

2017. aastal käsitletud juhtumid võrdluses 2016. aastaga



2017. aastal registreeritud küberturbeinsidentide osakaal liigiti



MIS ON KÜBERINTSIDENT?

Küberintsidendiks loetakse juhtumit, millega kaasneb otsene mõju teabe, seadme või süsteemide konfidentsiaalsusele, terviklusele või käideldavusele. Korraga võib neist olla mõjutatud üks või mitu ja põhjuseks võib olla nii inimkäitumine kui loodus- või tehiskeskkonnast tulenev häire.

Konfidentsiaalsus on andmete või süsteemi kaitstus kolmandate osapoolte loata juurdepääsu eest.

Konfidentsiaalsusintsident on näiteks *andmeleke, puudutagu see krediitkaardi- või terviseandmeid, konfidentsiaalseid dokumente või sotsiaalmeediakontode salasõnu.*

Terviklus on andmete kaitstus loata muutmise või hävimise eest.

Terviklusintsident on näiteks ravimiretsepti muutmine infosüsteemis või *makseandmete muutmine kliendile edastatud digitaalsel arvel.*

Käideldavus on süsteemi või andmete kättesaadavus ja ootuspärane toimimine.

Käideldavusintsident on näiteks teenusetõrke tõttu lakanud juurdepääs veebilehele või teenustõkestusründe tõttu kättesaamatuks muutunud digitaalne teenus.

Meil on parem ülevaade Eesti küberruumis toimuvast…

Eestis registreeritud küberintsidentide arv on olnud tõusteel mitu viimast aastat. Põhjuseid on mitu. Ühest küljest digitaalse keskkonna suurenev tähtsus ühiskonnale: laiem valik digitaalseid teenuseid, rohkem kliente ja teenuste agaram kasutamine tähendab, et tõuseb ka organisatsioonide sõltuvus digikeskkonnast igapäevategevuse korraldamises. Küberintsidentide mõju nii organisatsiooni enese kui ühiskonna jaoks tervikuna on seetõttu üha olulisem. Ühtaegu tähendab see ka suuremat loodetavat tulusust ründajale – võrreldes mullusega on kasvanud ka tahtlike rünnete arv.

Aastatega on pidevalt paranenud meie intsidentide avastamise võime – seda nii tänu parematele tööriistadele, süstemaatilisemale seirele kui ka tõhusamale koostööle partneritega, mistõttu suudame ründekampaaniaid tihti tõkestada juba enne, kui need Eestisse jõuavad, ning anda välja hoiatused koos tegutsemisjuhistega. Oleme aastaid pingutanud selle nimel, et Eesti küberruum oleks pahatahtlikele tegutsejatele ebasoodus keskkond – nii näiteks oleme teinud partnerite ja Eesti teenusepakkujatega pidevat koostööd õngitsemislehtede kiireks avastamiseks ja eemaldamiseks. Selle tulemusel on Eestis edukate andmepüügijuhtumite hulk märkimisväärselt vähenenud.

… ent ühiskonna teadlikkus ja oskused on endiselt ebaühtlased

Paranemas on ka organisatsioonide küberturbeoskused – arusaam, et organisatsioonil peab olema ülevaade oma infosüsteemides toimuvast ning valmisolek ohte ennetada ja neile kiiresti reageerida, on vähehaaval jõudmas „IT-spetsialisti" töölaualt ülespoole. Varem teadvustamata jäänud juhtumeid, millega tegeles – või siis mitte – üksnes infosüsteemi haldaja ise, märgatakse ning info neist jõuab sagedamini meieni. Sellest on kasu nii infosüsteemi omanikul kui riigil tervikuna: meil on operatiivsem ja terviklikum teave levivate ohtude või ründekampaaniate kohta, mistõttu oleme võimelised varakult hoiatama neid, keda oht puudutada võib, samuti saame organisatsioonile pakkuda eksperttuge ja nõustada turbe parandamisel. Paranenud ohuteadlikkus ja rünnete varane avastamine aitab vähendada riske teenuste toimepidevusele ja võimalikest rünnetest tulenevat kahju.

Paranenud teadlikkusele vaatamata on ilmne, et valmisolek on eri sektorites väga ebaühtlane ja palju intsidente jääb süsteemide

omanikel endiselt märkamata – ning need ohustavad lisaks süsteemi omanikule ka tema teenuste kasutajaid. Ligi poole möödunud aastal registreeritud küberintsidentidest avastasime ise seire käigus. Ülejäänute kohta andsid meile enamasti teada teiste riikide küberturbeasutused, Eesti elutähtsate teenuste osutajad ja riigi IT-keskused. Näiteks tänu siseministeeriumi infotehnoloogia- ja arenduskeskuse (SMIT) järjepidevale tööle ja meievahelisele heale koostööle on riigil siseturvalisuse valdkonna juhtumitest operatiivne ülevaade ja reageerimisvalmidus ning tõsisema mõjuga intsidente on vaatamata süsteemide kriitilisusele vähe. Suur töö on veel teha tervishoiuvaldkonnas või väikeettevõtjate hulgas, kus küberrünne avastatakse enamasti alles siis, kui oluline kahju juba sündinud.

MIDA TÄHENDAB KÜBERRUUMI SEIRE?

RIA intsidentide käsitlemise osakond (CERT-EE) seirab Eesti riigivõrgu võrguliiklust, tuvastamaks pahatahtlikule tegevusele viitavat liiklust.

Infot ohtude, kriitiliste haavatavuste ja ulatuslike pahavarakampaaniate kohta saadakse nii koostööpartneritelt Eestis ja välismaal kui ka avalikest allikatest.

Küberintsidentide arv kasvab üle ilma, ja Eesti ei ole erand. Läinud aastat jäävad iseloomustama järgmised näitajad:

- Lunavaraintsidentide hulk maailmas kasvas aastaga 36 protsenti ja pahavara levitavate e-kirjade osakaal kasvas aastaga kolmandiku võrra.
- Tõusuteel on teenustõkestusrünnete arv – 2017. aastal registreeriti üle maailma 7,5 miljonit DDoS-rünnet ja maksimaalne ründemaht on paari aastaga pea kahekordistunud.
- Mobiilseadmetele mõeldud pahavara levik kasvab endiselt – pahavararakenduste arv on aasta jooksul rohkem kui kahekordistunud ning tuvastatud nakatumiste hulk ulatub paarikümne miljoni ligi. Ohustatud on ka järjest lisanduvad nutikad olmeseadmed.
- Kasutajainfo (kasutajanimede ja paroolide) lekked on massilised – 2016. aastal registreeritud 1,1 miljardit juhtumit tähendas võrreldes aasta varasemaga pea kahekordset kasvu. Tubli täienduse andis ka 2017. aasta lõpul tumeveebis avaldatud 1,4 miljardi kasutaja infot sisaldav andmebaas.
- Statistiliselt kulub keskmisel ettevõttel oma infosüsteemi kompromiteerumise avastamiseks 168 päeva. See aeg väheneb rohkem kui kümme korda, kui ettevõte ise oma võrke monitoorib.[1]

Mille poolest oli möödunud aasta eriline?

Valmistusime 2017. aastaks pikalt – ees ootas Euroopa Liidu Nõukogu eesistumine, toimusid kohalikud valimised, mille turvalisusele pidime liitlaste kogemuse najal pöörama täiendavat tähelepanu; sügisene ID-kaardi turvanõrkuse lahendamine sai meie digiriigi küpsustestiks. Saime kinnituse oma veendumusele, et küberintsidente täiesti ära hoida ei ole võimalik, kuid hea ettevalmistus aitab vältida nende oluliselt häirivat ja halvavat mõju.

ID-kaardi turvariski maandamine

Riigi tagatud turvaline digitaalne identiteet – ID-kaart ning selle derivaadid mobiil-ID ja digi-ID – on Eesti e-teenuste üks alustalasid. Digiallkirja võrdne kaal paberil antava allkirjaga ja võimalus ennast elektrooniliselt tuvastada on Eesti digiriigi toimimise eeldus. Seetõttu on iga risk, mis seotud digitaalse identiteediga, meie kõrgendatud tähelepanu all.

30. augusti õhtul teavitas Masaryki ülikooli krüptograafiauuringute keskuse teadlane meid Eesti ID-kaartide kiipe puudutavast turvanõrkusest.[2] Rahvusvaheliselt ROCA (*Return of the Coppersmith Attack*) nime saanud turvanõrkus puudutab uurimisrühma analüüsi kohaselt RSA krüptovõtmete genereerimise funktsiooni ühe maailma juhtiva turvakiibitootja Infineoni kiipidel. Paljude muude toodete ja teenuste seas kasutatakse neid ka Eestis alates 2014. aasta sügisest väljastatud ID-kaardil, samuti digi-ID, diplomaadi ID- ja e-residendi kaardil.

Teoreetiliselt võimaldanuks leitud turvanõrkus ID-kaardiga autentimist ja allkirjastamist võimaldava salajase krüpteerimisvõtme matemaatiliselt tuletada avalikult saadaoleva võtme põhjal – ehk teoreetiliselt oli võimalik luua ohvri krüptovõtmetest virtuaalne koopia ja kasutada seda isiku tuvastamiseks, tema eest allkirjade andmiseks ja talle mõeldud andmete dekrüpteerimiseks, seda ka kaarti füüsiliselt omamata.

EESTI ID-KAART: MAAILMAS UNIKAALNE PLATVORM

- Kehtivaid kaarte: **1 295 844,** neist 26 199 e-residendi kaarti kokku 142 riigis
- Esimene dokument allkirjastati ID-kaardiga **7. oktoobril 2002**
- 481 miljonit digiallkirja ja 658 miljonit autentimist ehk kokku üle **miljardi toimingu** 15 aasta jooksul
- Vähemalt kord aastas digitaalselt kasutatavaid ID-kaarte on **747 580**. 42 000 inimest kasutab ID-kaarti digitaalselt vähemalt sada korda kolme kuu jooksul
- Aastast 2016 vastutab ID-kaardi digitaalsete elementide eest RIA, kaart isikut tõendava dokumendina kuulub endiselt politsei- ja piirivalveameti pädevusse. Sertifitseerimisteenust osutab (väljastab sertifikaate ID-kaardile) SK ID Solutions AS
- Uue hädaolukorra seaduse (2017) kohaselt on ID-kaardiga autentimine ja digiallkirjastamine **elutähtis teenus**
- 2017. aasta hilissuvel teatavaks saanud krüptograafiline nõrkus, mis tegi ID-kaardi teoreetiliselt haavatavaks, puudutas ligi **800 000** kaarti, mis olid väljastatud 16. oktoobrist 2014 kuni 24. oktoobrini 2017
- ID-kaardi (kaug)uuendamine – sertifikaatide asendamine uute sertifikaatidega sai võimalikuks 25. oktoobril 2017
- **3. novembril 2017** peatati vigaste sertifikaatide kehtivus
- Peatatud sertifikaatide uuendamine oli võimalik 31. märtsini 2018. Selle aja jooksul uuendati **494 000** ID-kaarti ehk 94% digitaalses kasutuses olnud kaartidest, neist 354 000 kauguuendamise teel
- 2017. aasta lõpu seisuga oli mobiil-ID 160 000 ja Smart-ID 140 000 inimesel

Turvanõrkuse ärakasutamine ei olnud lihtne ega odav; teadaolevalt ei ole seda Eesti ID-kaardi ega sarnaste kiipidega ka reaalselt tehtud. Lisaks isiku avalikule võtmele oli selleks vajalik märkimisväärne krüptograafiaalane oskusteave, spetsiifiline ründetarkvara ja suur arvutusvõimsus, mis nt Amazoni pilveteenuse pakkuja hinnakirja alusel maksnuks kuni 80 000 USA dollarit. Samas oli ilmne, et murdmisrisk suureneb märgatavalt kohe, kui uurimisgrupi kasutatud metoodika saab avalikuks ja sertifikaadid jäävad käibele. Saabunud infot hinnanuna oli meile selge, et tegemist oli kiiret lahendust vajava probleemiga.

Mõjutatud digitaalsete sertifikaatide suure arvu ja laialdase kasutuse tõttu nii riigi kui erasektori teenustes mõjutanuks tühistamine ulatuslikult e-teenuste kasutatavust – tõrked tekkinuks näiteks e-tervise, e-maksuameti, riigiasutuste dokumendivahetuskeskkonna kasutamisel, arvete maksmisel. Häiritud olnuks ka asutuste sisemine töökorraldus, sealhulgas riigiasutuste vahel. Turvanõrkus ei mõjutanud mobiil-ID-d, kuid seda kasutas tollal vaid veidi enam kui 100 000 inimest ning hulk digitaalseid teenuseid ei võimaldanud mobiil-ID kasutamist.

Olukorra lahendamisel tuli ühtaegu taastada ID-kaardi kõrge turvalisus ja samal ajal mitte halvendada teenuste kättesaadavust. Sisuliselt algas septembri alguses meie võidujooks ajaga, kus otsisime koos politsei- ja piirivalveameti (PPA) ja partneritega uut

turvalist lahendust ja valmistusime seda rakendama, teades samal ajal hästi, et varem või hiljem tuleb mõjutatud sertifikaatide edasine kehtivus peatada.

Kriisi lahendamise juhtgrupp tegi varakult otsuse olla avalikus kommunikatsioonis avatud ning tuua teada olevad faktid avalikkuse ette. Selle sammuga välditi spekulatsioonide ja erinevate tõlgenduste tekkimist ning tagati töörahu sisulise lahenduse leidmiseks. Kokku tähendas see, et uus – RSA-teegi asemel elliptilistele

ID-kaardi turvariski avalikustamise pressikonverents 5. septembril 2017. Foto: Taavi Sepp/ Ekspress Meedia

MIDA ROCA TURVANÕRKUS VEEL MÕJUTAB?

Eesti 800 000 turvanõrkusega ID-kaarti on üleilmsest mõjust kaduvväike osa. Kokku hinnatakse probleemsed olevat vähemalt miljard kiipi, mis on kasutusel üle maailma nii arvutite tarkvara osana kui plastkaartides. Eesti ID-kaardi turvanõrkuse põhjuseks olnud Infineoni kiipe kasutatakse juhilubades, kiibiga passides, töötõendites ja mujal.[3]

Vähemalt kümne riigi isikut tõendavaid dokumente. Sama nõrkusega kiipe kasutatakse teadaolevalt nt Slovakkia, Austria, Poola, Bulgaaria, Kosovo, Itaalia, Taiwani, Hispaania, Brasiilia ja Malaisia isikut tõendavates dokumentides. Näiteks Hispaanias mõjutas haavatavus 17 miljonit kaarti. Samas on teiste riikide sõltuvus veast väiksem kui Eestis, kuna kaartide kasutamine on palju piiratum kui Eestis ja nendega seotud teenuseid on vähem.

Arvutite turvamooduleid. Krüptoprotsessor ehk TPM on moodsate arvutite turva-arhitektuuri alus. Turvanõrkus puudutab vähemalt Lenovo, HP, Toshiba, Fujitsu arvuteid . See mehhanism on kasutusel eelkõige ettevõtete võrkudes olevates arvutites, seega kodukasutaja ei ole üldjuhul haavatav. Näiteks Microsoft Windowsis kaitseb turvamoodul kettakrüptograafiat (Bitlocker) ja teisi operatsioonisüsteemi turvamehhanisme. Microsoft on Windows Update'i kaudu välja andnud ajutise paiga, mis sisuliselt asendab TPM töö tarkvaralise lahendusega. Sarnased turvapaigad on välja andnud ka teised tootjad.

Krüptovahendeid. Neid kasutatakse virtuaalse privaatse võrgu (VPN) juurdepääsu, e-posti turbe ning kriitiliste turvaoperatsioonide jaoks. Avalikult on teada, et mõjutatud on vähemalt Gemalto ja Yubikey tooted, viimased vahetab tootja omal kulul välja.

Võimalik, et haavatud on ka osa kiibiga **maksekaartidest**.

kõveratele baseeruv – lahendus oli kättesaadav enne, kui tekkis vajadus kehtivad sertifikaadid peatada. Ka säilis kasutajate usaldus ning elektrooniliste teenuste kasutamine. Näiteks osales oktoobris 2017 toimunud kohalikel valimistel rekordarv e-hääletajaid ja ID-kaardiga tehtud toimingute hulk jäi järgnenud päevadel ja nädalatel tavapärasele tasemele – seda ajal, kui mobiil-ID kasutus märgatavalt kasvas.

Lisaks ID-kaardi laiale kasutusele tegi Eesti unikaalseks sertifikaatide kauguuendamise võimalus – inimesed said oma ID-kaardi tarkvara uuendada igast internetti ühendatud ja ID-kaardi lugejaga arvutist – ning võimalus sertifikaatide kehtivus peatada. Praktika näitas, et teistes sarnasesse olukorda sattunud riikides neid kaht võimalust polnud, mistõttu tuli leida võimalus väljastada uued ID-kaardid või olemasolevaid teeninduspunktides uuendada ning olles sertifikaadid tühistanud, polnud võimalust neid uuendada.

SÜNDMUSTE KRONOLOOGIA

30. august kl 19.35	Rahvusvahelise krüptograafiateadlaste uurimisgrupi liige saadab CERT-EE-le ametliku teavituse Infineoni kiipide turvariski kohta, mis mõjutab Eesti ID-kaarte. Risk seisneb kasutatava RSA krüptoteegi haavatavuses.
31. august	RIA esialgne hinnang kinnitab turvariski võimalikkust. Teavitatakse PPA-d ja MKM-i.
1. september	Teavitatakse majandus- ja kommunikatsiooniministrit. RIA kaasab välised tehnilised eksperdid (Cybernetica, Nortal) ning partnerid nii riigiasutustest kui erasektorist. Kogunevad asutuste juhid – selle baasil kujuneb strateegiline staap.
3. september	Peaministri ja teiste asjaomaste ministrite nõupidamine. RIA ja PPA töögrupid analüüsivad erinevaid stsenaariume, hindavad lahendusalternatiive. Eksperdid on välja selgitanud esmased mõjud teenustele ja andnud oma soovitused.
4. september	Vabariigi Valitsuse erakorraline istung. PPA-s alustab staap, mis tegeleb meediamonitooringu, analüüsi, meediapäringutele vastamisega, sellega ühineb RIA ja teised valitsusasutused. Teavitatakse mõjutatud era- ja avaliku sektori asutusi, sh panku ja sideettevõtteid. Suletakse avalik juurdepääs sertifikaatide andmebaasile (LDAP).
5. september	Peaministri, IT-ministri, RIA ja PPA peadirektori pressikonverents, avalikkust ja välispartnereid teavitatakse turvanõrkusest. www.id.ee lehel avatakse teabevärav, mida täiendatakse RIA, PPA ja SK ID Solutions koostöös.

September-oktoober	Regulaarselt kohtuvad tehnilisele lahendusele, kriisijuhtimisele, õiguslikele aspektidele ja kommunikatsioonile keskenduvad töögrupid. Vajadust mööda kaasatakse teisi asutusi ning väliseid eksperte.
5.-11. oktoober	Toimub kohalike omavalitsuste volikogude valimiste e-hääletamine, osaleb rekordarv ehääletajaid. E-hääletanuid on 31,7 protsenti kõigist valimistel osalenutest, mis on veidi kõrgem eelmistest valimistest.
16. oktoober	Teatavaks saab turvanõrkuse globaalne mõju: üheaegselt avaldavad turvaraportid Microsoft, Google (Chrome OS), Yubico, Gemalto ja mitu suuremat arvutitootjat (Lenovo, Fujitsu).
25. oktoober	Alustatakse uute, elliptkõveratel põhinevat krüptoalgoritmi kasutavate ID-kaartide väljastamist. Algab Eesti ID-kaardi kauguuendamise testperiood. Kuue testimispäeva jooksul uuendatakse kauguuenduslahenduse kaudu ligi 20 000 turvanõrkusest mõjutatud ID-kaarti. Kõik toimib, uuendused õnnestuvad.
30. oktoober	RSA krüptoteegi turvanõrkusele keskendunud teadustöö tehakse avalikuks.[4]
31. oktoober	Kaardiomanikke kutsutakse üles kaarte uuendama. Suur nõudlus põhjustab uuendamisel ulatuslikke tõrkeid, süsteemid stabiliseeruvad 2. novembriks. Slovakkia sulgeb 60 000 ROCA turvanõrkusega sertifikaati, nende omanikud peavad taotlema uue kaardi.
1. november	Hispaania sulgeb turvanõrkusega kaardid, kokku 17 miljonit.
2. november	Teadustöö kantakse täismahus ette USAs toimuval akadeemilisel konverentsil.
3. november	740 000 turvanõrkusega Eesti ID-kaardi sertifikaatide kehtivus peatatakse, kuid peatatud sertifikaatidega kaarte saab kauguuendada. Lisaks avab PPA sertifikaatide uuendamiseks aasta lõpuni lisateeninduspunktid.
5. november	Teenuste kasutusstatistika näitab, et sertifikaatide peatamine ei toonud kaasa langust ID-kaardi digitaalses kasutuses. Üllatuslikult on e-residentide kasutusaktiivsus veidi kasvanudki.
2017. aasta lõpp	Uuendatud on 400 000 ID-kaarti. Oluliselt on kasvanud mobiil-ID ja Smart-ID kasutajate arv ja kasutusaktiivsus.
Veebruar	RIA tellimusel alustab TTÜ uurimisgrupp riigi- ja asutusteülese õppetundide hindamisega.
5. veebruar 2018	ID-kaardi eest vastutavad Margus Arm RIAst ja Kaija Kirch PPAst saavad riikliku teenetemärgi.
1. aprill 2018	Uuendamata sertifikaadid tunnistatakse kehtetuks ning neid ei ole enam võimalik elektrooniliselt kasutada.

MIDA ME ID-KAARDI JUHTUMIST ÕPPISIME?

ID-kaardi turvariski juhtum illustreerib hästi Eesti sõltuvust oma „digitaalsest alustaristust" kogu ühiskonna ulatuses – mõjutatud on nii riik, ettevõtjad kui ka kasutajad. Ehkki juhtumi lahendamine kinnitas vajadust vaadata üle konkreetsed protsessid – nende seas nii ID-kaardi haldamine, riskide hindamine ja maandamine kui ka ametitevaheline koostöö –, on ilmne vajadus näha riigi digitaalse arhitektuuri arendamist ja juhtimist tervikuna. Uute tehnoloogiariskide avaldumine tulevikus on reaalsus, millega tuleb arvestada, ning ehkki jälgime tehnoloogia arengut tähelepanelikult, ei saa ootamatusi välistada – neile tuleb olla valmis kiiresti reageerima.

Et head kriisi mitte raisku lasta, hindame tõsiselt õppetunde, mida ID-kaardi juhtum pakub.

- **Sõltuvus ja alternatiivlahendused.** ID-kaart on digitaalse autentimise ja allkirjastamise vahendiks ligi 5000 erinevas avaliku ja erasektori teenuses. Selge on, et enamiku puhul neist ei paku võimalus näost näkku isikutuvastuseks ja omakäeliseks allkirjaks enam ühiskonnale vastuvõetavat alternatiivi, seega saavad alternatiivid olla eeskätt teised digitaalsed, mitte füüsilised lahendused – mobiil-ID, Smart-ID, arendatavad uued lahendused. Nende levik ja kasutusvalmidus teenustes peab suurenema. Meid päästis see, et meie ID-kaardil oli juba olemas mitu krüptoteeki, mis võimaldas uute turvaliste võtmete kiibil genereerimise.
- **Paindlik ja avatud arhitektuur** on riigi harjumuspärasele toimemustrile – teha ise või hankida väljast – väljakutse. Vähestel riikidel on endal kogu vajalik pädevus, enamik kompetentsi jääb erasektorisse. Rahvusvahelised suurkorporatsioonid, kes lahenduste ja teenuste pakkumisel võimekaimad, lähtuvad eeskätt oma riskidest – sedavõrd mastaapse turvanõrkuse puhul on riik vaid üks klient paljude seas. Kauguuenduslahenduse olemasolu andis meile paindlikkuse, mis võimaldas sertifikaadid peatada hilisemaks uuendamiseks, mis võrreldes teiste riikidega pani meid võrreldamatult paremasse olukorda.
- **Reageerimine ohule.** Reageerimiseks toimunud intsidendile, mille mõju on juba ilmnenud, on Euroopas ja Eestis välja kujunenud korrad. Teoreetilise ohu korral, kus loodetakse leida lahendus enne mõju ilmnemist, ei ole põhjust neid rakendada ja need ei ole ka sobivad. Seetõttu peame välja töötama sarnase rutiinid ka veel ilmnemata mõjudega ohtude ja riskide puhuks.
- **Avatus.** Digitaalse alustaristu haavatavuse riske ei ole võimalik hallata avalikkust kaasamata, kuivõrd need mõjutavad kogu

digitaalset ökosüsteemi. See tähendab, et tehnoloogiariski ühiskondliku ja majandusliku mõju vähendamiseks peab riskihaldus – lisaks keeruka tehnoloogilise probleemi lahendamisele – olema ennetav, avatud ja suuteline lahendust inimkeeli selgitama kogu ühiskonnale, et avalikkuse vajadustele vastata.

- **Laialdane koostöö** väga erinevate rollide, ootuste ja valmisolekuga osaliste vahel on möödapääsmatu. Õhukese riigi kriisivaruks on tugev erasektor. Avalikku sektorisse inimeste juurde palkamine ei ole lahendus, mistõttu Eesti tehnoloogiaettevõtete toetamine – eeskätt hariduse ja teaduse kaudu, et teadmus ja inimesed oleksid olemas – loob eelduse, et neid on võimalik vajadusel riigile appi kutsuda.
- **Digi- ja küberoskuslik ühiskond.** Tänapäeva digisõltuvas ühiskonnas ei ole iga inimese elementaarne tehnoloogiline kirjaoskus enam iluasi, vaid hädapärane oskus. Vajame üha enam hulgipädevustega inimesi, kes korraga valdavad nii tehnoloogiat kui mittetehnoloogilist eriala nagu majandus, riigi- või õigusteadus.

ID-kaardi juhtumi järeldustest ja õppetundidest ülevaate saamiseks ja analüüsiks oleme lisaks tellinud sõltumatu uuringu. Hanke võitnud Tallinna Tehnikaülikooli uurimisrühm hindab juhtumit nii riigihalduse, tehnoloogiajuhtimise kui infoturbe vaates ja esitab oma soovitused 2018. aasta kevadel. ■

Euroopa Liidu Nõukogu eesistumine

Eesti riigiametnike ees möödunud aastal seisnud suurim väljakutse oli mõistagi Euroopa Liidu Nõukogu eesistumine, mille üheks põhiteemaks oli ka Euroopa Liidu küberturvalisus. Varasemate eesistujariikide kogemus näitas, et koos eesistumisega suurenes ka küberrünnete arv riigi ja ühiskonna oluliste teenuste ning sihtmärkide pihta. Eesti eesistumine keskendus ju digiteemadele, mille tõttu oleks igal meid tabaval nähtava mõjuga edukal ründel olnud kindlasti laiem mõju kui pelgalt meie enda elanikkond.

Eesistumise küberturvalisuse tagamine seisnes nii tehnilistes ettevalmistustes, ametnike koolitamises, ohuolukordadeks valmisoleku arendamises kui ka olukorrateadlikkuse pidevas tagamises, mille juures mängisime kõiki stsenaariume koos partnerasutustega läbi juunis toimunud õppusel. Õnneks olime kõigeks toimunuks väga hästi valmis ja lõviosa kõigist eesistumisega seotud küberintsidentidest oli tingitud tehnoloogilistest riketest (näiteks elektrikatkestustest) ja inimlikest eksimustest, mis avastati ja lahendati kiiresti ning mille mõju jäi minimaalseks.

Üks ohustsenaariume, millega arvestasime, oli politiliselt motiveeritud maineründed küberruumi kaudu. ELi tippkohtumise eel levis sotsiaalmeedias libauudis Eesti peaministri toetusavaldusest Kataloonia iseseisvusliikumisele. Konto on tegev senini, viidatud postitus on eemaldatud.

Kutsusime eesistumise küberkonverentsile „Digitaalne ühisturg, ühine digitaalne turvalisus" küberturvalisuse tuleviku üle arutlema Euroopa tippspetsialistid.[7] *Foto: Karolin Köster*

Lisaks sellele, mis toimus kodumaal, olid Eesti suhtes suured ootused ka Brüsselis, arendamaks ELi küberjulgeolekut tervikuna. Meie eesistumise kõige olulisem põhimõtteline tulem oli see, et Eesti eesistumise järel ei ole enam ühtegi sisulist takistust kõikide ELi ühiste välispoliitikameetmete (sh majandussanktsioonid) rakendamiseks küberrünnetele reageerimisel. Eesti juhtimisel saavutati Brüsselis riikidevaheline kokkulepe vastavate protseduuride kohta ja nüüd peab iga küberrünnakuid planeeriv, toetav või võimaldav riik arvestama sellega, et karistus rünnakute eest võib maailma olulisimalt majandusühenduselt tulla ka erinevate majanduslike või välispoliitiliste vahendite kasutamise kaudu.

Teiseks valmis meie eesistumise ajal **Euroopa Liidu uus küberstrateegia**[5], mis loob aluse mitmele olulisele initsiatiivile, millel võiks ELi kui terviku küberjulgeolekule olla pikk mõju. Olulisemad neist on kindlasti ettepanek ELi-ülese küberjulgeoleku sertifitseerimise raamistiku loomiseks ja plaan luua ELis kübervaldkonna teadus- ja arendusasutusi koondav kompetentsikeskuste võrgustik. Just sellel viimasel on suur potentsiaal toetada euroliidu rahaga küberteemalist teadusarendust ja sundida sellega ka praegu erinevaid väikeseid teadus- ja arenduskeskusi senisest suuremat koostööd tegema. Selle tulemuseks peaks lisaks küberjulgeoleku arengule olema ka euroliidu majanduse ja tööstuse tugevnemine selles valdkonnas. Selles kontekstis ei ole sugugi vähetähtis ka **Eesti Infoturbe Assotsiatsiooni** loomine 2017. aasta lõpus[6] – sel on kõik eeldused saada ELi võrgustiku liikmeks ja selle kaudu saab meie e-riigile turvalisust tagavate lahenduste loomine koostöös meie ettevõtetega senisest pikaajalisema aluse.

Kolmandaks oli meie eesistumisel suur roll ka selles, et 2016. aasta võrgu- ja infoturbedirektiivi raames loodud, ELi liikmesriikide küberturvalisust tagavate asutuste koostöövõrgustikud hakkaksid aktiivselt toimima – ja seda nii tehnilisel kui ka strateegilisel tasandil. Justnimelt meie pidime ära sisustama strateegilise tasandi koostöögrupi ja ELi CSIRT-võrgustiku* reaalse argipäeva. Eestlaslik paindlikkus ja keskendumine tulemustele aitas meil ka siin ELi efektiivselt juhtida. Koostöögrupis algas RIA peadirektori juhtimisel lisaks võrgu- ja infoturbedirektiivi elluviimisele keskenduvale tööle ka veel ELi riikide küberasutuste sisuline koostöö valimisprotsesside küberturvalisuse ja piiriüleste sõltuvuste maandamise teemadel. Tehnilisel tasandil aga tagas meie CERTi töökas meeskond oma juhtimise ja tehniliste platvormide loomise abil selle, et ELi loodud tehniline koostöövõrgustik pakkus WannaCry ja NotPetya intsidentide lahendamisel juba nähtavat lisaväärtust. ■

* ELi CSIRT võrgustik koondab ELi liikmesriikide küberintsidentidele reageerimise riiklikke üksusi.

Kohalikud valimised

Eesti oli esimene riik maailmas, mis elektroonilise hääletamise 2005. aastal valimistel kasutusse võttis. Praegu, üheksa valimistsüklit hiljem, on Eesti endiselt ainuke, kus saab riigi tagatud turvalise elektroonilise identiteedi alusel anda interneti vahendusel hääle üldvalimistel võrdsena valimispäeval jaoskonnas antud häälega.

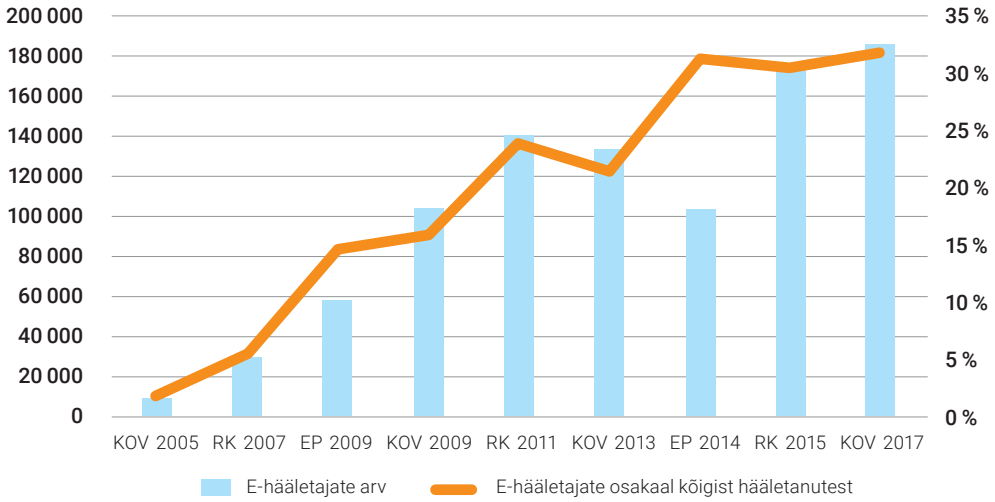
Kui 2005. aastal andis oma hääle elektrooniliselt vähem kui iga viiekümnes valimistel osalenu, siis enam kui tosinkond aastat hiljem eelistab umbes kolmandik valijaid hääletada just sel viisil (2014. aasta Euroopa Parlamendi valimistel 31,3 protsenti ja 2015. aasta riigikogu valimistel 30,5 protsenti). 2017. aasta sügisestel kohalikel valimistel tehti napp osalusrekord, kui elektrooniliselt andis oma hääle 31,7 protsenti hääletanutest.

Usaldus e-hääletuse vastu ning ka selle turvalisus põhineb suuresti Eesti ulatuslikul ja laialdasel turvaliste elektrooniliste teenuste ökosüsteemil. Esiteks on Eesti inimesed harjunud ja õppinud kasutama paljusid era- ja riigisektori teenuseid alates pankadest ja lõpetades rahvastikutoimingutega, mistõttu nad usaldavad ka teisi e-teenuseid. Teiseks võimaldavad valimisi turvaliselt läbi viia teised hästi välja kujunenud digitaalsed süsteemid alates rahvastikuregistrist – mille alusel koostatakse ka valijate nimekirjad – ja lõpetades riigi tagatud turvalise digitaalse identiteediga, millel e-hääletus põhineb. Lisaks on Eesti valinud järjekindla läbipaistvuse strateegia, mis tähendab, et suur osa valimiste dokumentidest ning tarkvara lähtekoodist on avalikud. Enesestmõistetavalt on lisaks tehnilistele meetmetele ka valimiste toimingud ja protseduurid üles ehitatud turvalisust silmas pidades.

Arvestades üleilmseid arenguid, oli valimistehnoloogia küberturvalisus 2017. aastal ka Eestis kõrgendatud tähelepanu all. Varem on e-hääletamise ohuanalüüs keskendunud ennekõike süsteemide tehnilistele riskidele. Arvestades muutunud ohumaastikku, koostati meie juhtimisel e-hääletuse terviklik ohuhinnang, mis vaatles ka võimalikke poliitiliselt motiveeritud küberrünneid, jagatud vastutusega juhtimismudelit ja muid valimiste legitiimsust potentsiaalselt mõjutavaid valdkondi. Selline laiapindne lähenemine põhines arusaamal, et valimiste legitiimsus ei olene vaid häälte kogumiseks ja lugemiseks kasutatavate tehniliste süsteemide turvalisusest, vaid ka ühiskonna usaldusest kogu riigi digitaalse ökosüsteemi vastu. Analüüs kaardistas ka süsteemid ja lahendused, millest valimiste toimumine sõltub.

Oleme olnud riigi valimisteenistuse ja vabariigi valimiskomisjoni partner e-hääletamise häälte kogumise süsteemi majutajana ning

E-hääletamise kasutus valimistel alates 2005



Tüüpiline e-hääletaja ei erine tüüpilisest paberil hääletajast

Tartu Ülikooli Skytte Instituudi direktori kt, tehnoloogiauuringute vanemteadur dr Mihkel Solvak kommenteerib e-hääletamise levimist

Elektroonilise hääletamisviisi võimaldamise/mittevõimaldamise diskussioonid algavad ja lõppevad tihtilugu kahe küsimusega, „kes seda kasutama hakkab?“ ning „kes sellest kasu saab?“. Eesti e-hääletamise levik ja kasutusmustrid lubavad mõlemale küsimusele sama vastuse anda. Esimesel kolmel e-hääletamise võimalusega valimisel olid elektrooniliselt hääletanud selgelt erinevad tüüpilisest valijast. E-hääletajad olid 30–40-aastased, paremini haritud, jõukamad ja selgelt paremate digioskustega inimesed. Aja möödudes kadusid aga pea kõik need faktorid sellises ulatuses, et praegu ei ole e-hääletaja paberhääletajast enam statistiliselt olulisel määral erinev. Teisisõnu tähendab see, et e-hääletamine on elanikkonnas niivõrd levinud, et tüüpiline e-hääletaja on nüüdseks muutunud tüüpilise paberhääletaja sarnaseks. Kuna valimas käinute struktuur on tegelikult samaks jäänud ja muutunud on vaid valimisviis, on põhiline kasusaaja tavaline valija, kes hoiab kokku teekonna valimisjaoskonda.

osalenud e-hääletamise korraldustoimkonnas. Kuna 2017. aastal võeti kasutusele uus serveritarkvara, panustasime lisaks selle turvatestimisse – meie juhtimisel ja rahastusel viis turvateste läbi kaks turvatestimisele spetsialiseerunud ettevõtet, kes mõlemad raporteerisid ka erinevaid leide. Ka testis e-hääletuse lahendust küberkaitseliit. Leitud puudused parandati, ent ükski testimine ei toonud välja kriitilisi vigu.

Lisaks kõigele kirjeldatule panustas meie turvaintsidentide käsitlemise üksus CERT-EE e-hääletuse rakkerühma e-hääletamise taristu võrguliiklust jälgides, hoides silmi lahti ennekõike anomaaliate, näiteks teenustõkestusrünnete suhtes. Samamoodi osalesime ka kommunikatsioonitöös ja selle planeerimises.

Pea 186 000 loetud e-häält – kõigi aegade absoluutne rekord – näitas, et usaldus e-hääletamise vastu püsib ning seda ei mõjutanud ka ID-kaardi turvanõrkus ega üleilmsed „valimiste häkkimised" (viimasest kirjutame lähemalt peatükis „Kes ründab ja miks?"). ■

PEAMISED KÜBEROHUD – MIS ON MUUTUNUD?

Suurima osa Eesti elanikke ja organisatsioone mõjutavatest küberintsidentidest moodustab jätkuvalt seadmete nakatumine kõikvõimaliku pahavaraga. Globaalselt olid eelmisel aastal suurima mõjuga lunavarakampaaniad WannaCry ja NotPetya, mille üleilmne kahju ulatub miljarditesse. Eestis oli tänu ennetustegevusele ja õigeaegsele reageerimisele kahju minimaalne.

Ehkki küberintsidendi võib põhjustada nii inimkäitumine kui ka tehnoloogiarike või loodusõnnetus, moodustab ligi neli viiendikku – mullu üle 2500 – intsidentidest tahtlik tegevus ehk küberründed. Selle näitaja kõrval tingisid administreerimisvead ja tehnoloogiatõrgetest tingitud teenusekatkestused alla 10 protsendi kõigist küberintsidentidest.

Nakatatud seadet saab kasutada erinevateks küberrünneteks – teenustõkestusrünneteks, andmete varastamiseks, vääruudiste

AVALANCHE'I ROBOTVÕRGUSTIK

Pea kolmandiku Eestis mullu registreeritud pahavaraintsidentidest tingis Avalanche'i robotvõrgustik. Avalanche oli aastaid aktiivselt tegutsenud globaalne robotvõrgustik (*botnet*), mille abil levitati lunavara, varastati isiku- ja pangaandmeid ning rünnati finantsinstitutsioone. Seda renditi ka ründekampaaniateks teistele kurjategijatele.[9] Üleilmselt arvatakse Avalanche'i tekitatud kahju sadadesse miljonitesse eurodesse, ainuüksi Saksamaa internetipankade kahjuks hinnatakse umbes kuus miljonit eurot.[10] Kahjusumma Eestis ei ole teada; arvata on, et näiteks Eesti pangateenuste kasutajad on tänu turvalistele autentimisvahenditele – ID-kaart, mobiil- ja Smart-ID – üldiselt paremini kaitstud, ent internetikaubanduse ja muude teenuste kaudu mõjutas oht neidki.

Rahvusvahelise politseioperatsiooni tulemusel peatati Avalanche'i tegevus 2016. aasta detsembris,[11] ent pahavara ei kustu seadmetest automaatselt ning need tuleb eraldi puhastada, et vältida sama taristu hilisemat ülevõtmist ja elustamist uuteks rünneteks. Kuna see on pikk protsess ja paljud kasutajad ei ole oma seadmete nakatumisest teadlikud, teeme koostööd paljude riikide küberturbeasutustega ja see tegevus jätkub vähemalt 2018. aasta lõpuni.[12]

Kurjategijad otsivad seksuaalkuritegude ohvreid internetist

Veebikonstaabel Maarja Punak leiab, et aina enam otsivad seksuaalkurjategijad oma ohvreid internetist.

Veebikonstaabliteni jõuab aina enam infot olukordadest, kus keegi on hädas ahistamise või väljapressimisega. Noored käituvad internetis vabamalt kui füüsilises maailmas, jagatakse isiklikku infot ja intiimseid pilte. Kübermaailma ohte ei tajuta nii nagu füüsilises maailmas.

„Petlikult levib arvamus, et lubada võib kõike, sest suhtlus näib anonüümsena. Tegelikult ei saa aga kunagi kindel olla, kellele sa infot jagad ning millised on vestluspartneri kavatsused. Halvemal juhul levitatakse saadud isiklikku infot edasi ning esmapilgul süütuna tundunud naljast võib välja kasvada reaalne süütegu," märkis Punak.

Erinevate suhtlusportaalide, sealhulgas Facebooki kaudu otsivad noortega ühendust seksuaalkurjategijad, kes üritavad lastest kas pilte või videosalvestusi saada. Nii mõnegi juhututtavaga vestlusse asunud noort meelitatakse kohtumisele või rahuldatakse enda fantaasiaid veebikaamera vahendusel.

Eelmisel aastal registreeris politsei 557 seksuaalkuritegu, millest ligi 300 ehk rohkem kui pool on toime pandud veebi vahendusel. Siia kuluvad seksuaalne ahistamine ja peibutamine erinevates suhtluskeskkondades. Lapseealise seksuaalse ahvatlemise juhtumeid registreeriti 130, neist 80 internetikeskkonnas.

Veebikonstaabli soovitused:

- Ära avalikusta oma isiklikke andmeid, jaga endast paljastavaid pilte või videoid võõrastele või juhututtavatele
- Ära aktsepteeri tundmatute kasutajate sõbrakutseid
- Vaata üle oma sotsiaalmeedia profiili seaded ning veendu, et seinal olevad postitused on nähtavad ainult sõbralisti liikmetele
- Avalikust arvutist ja nutiseadmest (näiteks telefoniesindused) logi pärast kasutamist alati välja
- Räägi oma murest kindlasti usaldusväärse inimese, teiste hulgas oma vanematega
- Kui oled langenud kuriteo ohvriks, võta ühendust veebikonstaabli või politseiga

levitamiseks.[8] Järjest rohkem kasutatakse nakatunud seadmete arvutusressursi krüptoraha kaevandamiseks, need juhtumid oli aasta lõpupoole tõusuteel ka Eestis.

Enamik küberkurjategijaid tegutseb valimatult, otsides haavatavaid seadmeid ja hooletuid või kergeusklikke kasutajaid. Tüüpiliselt aitab pahavara ohvriks langemisele kaasa aegunud tarkvara, mis võimaldab ründajal tarkvara turvanõrkusi ära kasutada, kusjuures ohver võib olla nii uuendamata süsteemi omanik ise kui selle pahaaimamatu kasutaja, näiteks veebilehe külastaja. Kehv või olematu turve ei ole kaugeltki üksi omaniku enese risk.

Riikide algatatud kampaaniad sihtmärke ei valinud

2017. aasta kevadel leidis kuuajase vahega aset kaks ülisuurt kahju põhjustanud pahavarakampaaniat – WannaCry ja Petya/NotPetya. Mai teise nädala lõpus nakatus mitusada tuhat seadet **WannaCry** lunavaraga ning ohvreid oli nii meditsiiniasutuste, pankade, telekommunikatsiooni- ja logistikaettevõtete kui ka suurte tööstusettevõtete hulgas ligi 150 riigis. Märkimisväärsematena võib välja tuua Hispaania suurima telekommunikatsioonieettevõte Telefonica ja Renault' Prantsusmaal asuvad autotehased, kus oldi sunnitud töö mõneks päevaks peatama.[13] Üks suuremaid ohvreid oli Ühendkuningriigi riiklik tervishoiusüsteem (*National Health Service* – NHS), mille piirkondlikest asutustest rohkem kui kolmandiku tööd WannaCry tõsiselt häiris. Kokku mõjutas intsident rohkem kui 600 Ühendkuningriigi tervishoiuasutust; tuhanded visiidid ja operatsioonid tühistati ning viies piirkonnas pidid patsiendid mujalt erakorralist abi otsima.[14]

WANNACRY		PETYA/NOTPETYA
150 riiki	*Globaalne levik*	65 riiki
400 000	*Nakatunud seadmeid*	20 000
4 miljardit USD	*Teadaolev kahju*	1,2 miljardit USD
Põhja-Korea	*Arvatav päritolu*	Vene Föderatsioon
Ei olnud	*Kahju Eestis*	Saint-Gobain Eesti (Ehituse ABC) Kantar Emor

Foto: pexels.com

Juuni lõpus liikvele läinud **Petya/NotPetya** levis Ukraina päritolu raamatupidamistarkvara kaudu kõigile ettevõtetele, kes tarkvara kasutasid ja selle pahavara sisaldanud uuenduse paigaldasid. Pealtnäha lunavara, sel tegelikult failide lahtikrüpteerimise võimalust polnudki ja pahavara kustutas krüpteeritud süsteemides andmed. Rünnak usutakse olevat mõeldud Ukraina asutuste ja suurettevõtete vastu, sealt pärinesid ka esimesed nakatumised.

Ehkki võrreldes WannaCryga levikult piiratum (70 protsenti ohvritest asus Ukrainas), oli NotPetya majanduslik mõju märkimisväärsemgi, kuna rünne oli mõeldud ärisüsteemide vastu.[15] FedExi Euroopa harul TNT Expressil kulus oma infosüsteemide tavapärase töö taastamiseks enam kui kuu ja osa andmekaost on ettevõtte teatel jääv.[16] Taani laevandusettevõte Maersk pidi rünnakust taastumiseks kümne päeva jooksul uuesti paigaldama sisuliselt kogu ettevõtte infosüsteemi – 4000 serveri ja 45 000 tööjaama kogu

tarkvara. Nii Maersk kui FedEx hindavad kahju suuruseks kuni 300 miljonit dollarit.[17] Suurte ohvrite seas oli ka ravimifirma Merck, kellel veel kaks kuud pärast juhtunut oli märkimisväärseid probleeme ravimiarenduse ja tootmise taastamisega täismahus, häiritud oli ka mõne turu ravimitega varustamine.[18] Tervise- ja hügieenitoodete hiiule Reckitt Benckiserile intsidendist põhjustatud tootmis- ja tarnehäired kestsid üle kahe kuu ning mõjutavad ettevõtte hinnangul märgatavalt ettevõtte aastatulemusi.[19]

REAKTSIOON JA JÄRELDUSED

Nii WannaCry kui NotPetya kampaaniad kasutasid ära aprillis USA riikliku julgeolekuagentuuri NSA lekkinud tööriistu Microsoft Windowsi operatsioonisüsteemide haavatavuste ärakasutamiseks.[20] Microsoft väljastas märtsis kasutajaid kaitsva turvauuenduse, ent uuendamata süsteemid jäid haavatavaks ja kuna süsteemi nakatumiseks polnud kasutaja poolt tegevust vaja, levis WannaCry kiiresti. Erakorraline turvapaik anti välja ka Windows XP operatsioonisüsteemile, millele ametlikult alates 2014. aastast enam tuge ei pakuta.[21] Mullu sügisel väljastas Microsoft turvauuenduse kaitsemehhanismiga seesuguste rünnete vastu, ent see on mõeldud Windows 10 operatsioonisüsteemile ja ei kaitse teisi levinud operatsioonisüsteeme, nagu Windows 7 ja Windows 8.1.

Eestis teadaolevalt WannaCry ohvreid ei olnud. Nakatada üritati paarikümmet süsteemi, ent neis oli kasutusel turvapaigatud operatsioonisüsteem, mistõttu lunavara ei käivitunud. NotPetya tõttu said kannatada Saint-Gobain Eesti tütarettevõtted, kellest Ehituse ABC pidi kõik oma Eestis asuvad kauplused sulgema.[22] Kantar Emor peatas oma infosüsteemide töö ettevaatusabinõuna, sest emaettevõtte võrgus oli nakatumisi.[23]

Kahju ärahoidmisel oli oma roll nii valmidusel kui kiirel reageerimisel. Oma osa nakatumiste ärahoidmisse andis meie 2013. aastal korraldatud teavituskampaania Windows XP kasutamisest loobumiseks, mille järel vähenes selle osa Eestis vähem kui 20 protsendini operatsioonisüsteemidest. Ka olime terve 2016. aasta pööranud erilist tähelepanu tervishoiusektori infoturbe parandamisele. Nii WannaCry kui Petya/NotPetya kampaaniate puhul võtsime kohe ühendust potentsiaalselt ohustatud asutustega, et ohust teavitada ja juhendada süsteemide turvamisel, samuti teavitasime riigiasutuste ja elutähtsate teenuste osutajate infoturbejuhte ning avaldasime hoiatusi ja juhiseid avalikkusele.[24] Ehkki intsidente ei saa kunagi täielikult välistada, on nii süsteemide kui inimeste valmisolekul oluline kaal, et kahju ära hoida või minimeerida.

Kasutades oma rolli peatse ELi eesistujana, käivitasime nii WannaCry kui NotPetya puhul koos viie riigi partnerite ja Euroopa küberturbeagentuuri ENISAga kiire Euroopa-ülese reageerimise, korraldades ja tagades operatiivset info edastamist riikide vahel.

WANNACRY JA NOTPETYA: KAS RIIKLIKUD RÜNDED?

Mõlemad 2017. aasta suured lunavarakampaaniad kahjustasid valimatult nii ettevõtjaid, riigiasutusi kui ka eraisikuid ning seadsid lisaks varale ohtu ka inimeste elu ja tervise. Ettevõtete kõrval kandsid ilmselt veelgi enam kahju tavalised kasutajad, kelle kahju on pea võimatu kokku lüüa. Mõlemad kampaaniad levisid suhteliselt kontrollimatult ja kiiresti üleilmseks.

Juba pärast WannaCry massilise leviku lõppu osutasid mõned allikad võimalusele, et WannaCry taga võis olla Põhja-Koreaga seostatav Lazaruse-nimeline rühmitus.[25] Novembris esinesid Ühendkuningriigi valitsus ja Microsoft avaldustega, milles süüdistasid WannaCry lunavaralaines Põhja-Koread.[26] Sellele järgnes USA valitsuse ametlik avaldus 19. detsembril, milles viitega USA ametkondade ja erasektori (sh Microsoft ja küberturbeettevõtted) koostöös saadud tõenditele omistati WannaCry Põhja-Koreale. Hinnangu andmisel tugineti ründe tööriistade ja -võtete ning kasutatud infrastruktuuri kattuvusele Põhja-Korea varasemate küberoperatsioonidega.[27] USA seisukohaga ühinesid ka Ühendkuningriik, Austraalia, Kanada, Uus-Meremaa ja Jaapan.

Samamoodi tekkisid kahtlused NotPetya päritolus üsna pea pärast selle leviku algust. Mitme allika hinnangul oli pahavara käekiri sarnane Ukrainas 2016. aasta detsembris elektrijaamade vastu korraldatud küberründega.[28] Ukraina julgeolekuteenistuse väitel viitavad kogutud faktid, et rünne pärines Venemaalt ning pandi toime sealsete eriteenistuste osalusel.[29] Rahvusvahelise ekspertkogukonna valdav seisukoht on, et ründe tegelik eesmärk oli tekitada võimalikult suurt kahju ja lunarahanõue oli vaid kattevari.[30] Tänavu veebruaris omistasid Ühendkuningriigi, Taani, USA, Austraalia ja Uus-Meremaa valitsus vastutuse NotPetya eest Venemaa valitsusele ja sõjaväele. USA avalduse kohaselt on tegemist ajaloo destruktiivseima ja kulukaima küberründega, mis põhjustas miljardeid kahju Euroopas, Aasias ja Ameerika mandritel.[31] Ühendkuningriigi avaldust toetas ka Eesti välisministeerium, mõistes küberrünnaku hukka ja kutsudes Venemaad üles käituma küberruumis vastutustundlikult ja rahvusvahelise õiguse kohaselt.[32] ■

Andmepüük, andmelekked ja turvaline digitaalne identiteet

Ulatuslikud andmelekked on maailmas muutunud sedavõrd tavapäraseks, et vaevu möödub rahvusvahelises meedias nädal mõne teateta, ja keegi ei julge ennustada olukorra paranemist. 2017. aasta suurimate andmelekete sekka jäävad USA vabariiklaste rahvuskomitee (RNC) andmeleke ja krediidibüroo Equifax leke, millest esimene tõi avalikuks ligi 200 miljoni inimese – pea kõigi USA valijate – isikuandmed ja teine 150 miljoni ameeriklase krediidiinfo.[33] Euroopa poolelt pakkus samaväärse andmekaitsekatastroofi Rootsi transpordiamet, kui välisriigi ettevõttele anti üle riigi julgeolekut, siseturvalisust ja kriminaalmenetlust käsitlevat teavet sisaldava andmebaasi haldamine ning viimane selle avalikku pilveteenusesse üles laadis. Juhtum vallandas Rootsis valitsuskriisi, mis päädis siseministri ja taristuministri väljavahetamisega.[34]

Vaatamata sellele, et juhtumite põhjused erinesid – ühel juhul inimlik eksimus valijate andmebaasi seadistamisel, teisel lootusetult puudulik andmeturbepraktika ettevõttes ning kolmandal turbenõuete teadlik ignoreerimine –, viitavad need ühesugustele fundamentaalsetele nõrkustele nii teenuste arhitektuuris kui ka intsidentideks valmisoleku ja nende lahendamise osas.

Eesti riigiasutustes või teenusepakkujate juures ei registreeritud möödunud aastal ühtki tõsist andmelekke juhtumit. Eesti digiriigi läbipaistev ülesehitus, turvalise autentimise kasutamine ja muud meetmed, millega tagatakse oluliste andmete terviklust, muudavad sellises mõõdus andmelekked Eestis väga raskesti teostatavaks, kuid riskide maandamine vajab endiselt pidevat tööd.

Küll kasutavad Eesti elanikud aktiivselt suurte rahvusvaheliste teenusepakkujate teenuseid, kuhu registreeritakse kontosid ka tööalast e-posti aadressi kasutades. Möödunud aasta lõpus avaldati tumeveebis 1,4 miljardi kasutaja infot ja parooli lihttekstina sisaldav andmebaas, kus sisaldus ka 198 000 .ee-lõpuga e-posti aadressi, mida oli kasutatud kontot luues. Ehkki andmebaasist ei selgu täpselt, millisest keskkonnast kasutajanimed ja paroolid täpselt lekkinud on, sisaldab see LinkedIni, MySpace'i, Twitteri, Tumbleri, DropBoxi, Bitcoini foorumite, Zomato, Gmaili ja Yahoo lekkinud kasutajainfot. Neist 2830 olid Eesti avaliku sektori ja ligi 2600 elutähtsa teenuse osutajate töötajate meiliaadressid. Puudutatud asutuste infoturbejuhte teavitasime lekkest koos soovitusega lähtestada kasutaja parool ning selgitada kasutajatele paroolide ristkasutamise ohtusid.

Andmekaitsemääruse nõuete täitmine on töö- ja ajamahukas

25. mail 2018 hakkab kehtima Euroopa isikuandmete kaitse üldmäärus, mis asendab senise isikuandmete kaitse seaduse. Andmekaitse Inspektsiooni peadirektor Viljar Peep selgitab lühidalt, mis ja miks muutub.

Foto: Andmekaitse Inspektsioon

Mis uue määrusega muutub

Andmekaitse põhimõtted on jäänud küll samaks, kuid reeglid on oluliselt täpsemad ja põhjalikumad ning lähtuvad riskipõhisusest. Rangemad reeglid kehtivad siis, kui tegeletakse ulatusliku andmetöötluse või tundlike andmetega. Sel juhul tuleb kindlasti määrusesse süveneda, sest reeglite täitmine võib vajada suuri ja aeganõudvaid muudatusi organisatsiooni infosüsteemis, klienditeninduses või personalitöös. Näiteks tekib kohustus määrata andmekaitsespetsialist, kohustus pidada isikuandmete töötlemise toimingute registrit ja palju muud.

Ettevõte ja asutus, kel tundlikku andmetöötlust pole ning kes ka seni andmekaitse reegleid korralikult täitis, ei pea suuri muudatusi tegema.

Suurim sisuline muudatus – isikuandmete ülekantavus – mõjutab peamiselt erasektorit. Inimene võib võtta oma digitaalandmed ettevõttest A ja viia need ettevõttesse B. Ettevõtetel tasub oma infosüsteemid üle vaadata, et andmeid oleks võimalikult hõlbus ja lihtne üle kanda.

Miks selline määrus kehtestati

Põhjus on Euroopa ühisturg – andmeid on vaja liigutada üle riigipiiride. Kui igas riigis on eri regulatsioon, on seda keeruline teha. Seetõttu on reeglid täpsemad erasektori puhul ning avaliku sektori andmetöötluseks on liikmesriikidele jäetud rohkem mänguruumi.

Millest tuleks organisatsioonil alustada

Avaliku sektori asutused, ulatuslikud andmetöötlejad ja suured ettevõtted peaksid alustama oma andmetöötluse tervikhindamisest: vaatama uue andmekaitseõiguse pilguga üle kogu oma töökorralduse, infosüsteemid ja dokumendipõhjad. Riigiasutused peavad sealjuures arvesse võtma ka avaliku teabe seadust ja oma asutusele suunatud õigusakte.

Ettevõtjad peavad kindlasti üle vaatama andmete ülekantavuse – info peab olema üldkasutatavas masinloetavas vormingus struktureeritud kujul.

Vaata ka
http://www.aki.ee/et/soovitused_maaruseks_valmistumisel.

Muutunud paroolisoovitused

Paroolide peatset surma autentimisvahendina on ennustatud aastaid. Mitmeastmeline autentimine on turvalise alternatiivina ammu kättesaadav ka massiteenustes nagu Google ja sotsiaalvõrgustikud, samuti on selle kasutusmugavus aastatega märgatavalt paranenud. Kasutusaktiivsus seevastu on endiselt nigel – näiteks Google'i 2011. aastast pakutava kaheastmelise autentimise (2FA) on seadistanud alla kümne protsendi Google'i teenuste kasutajatest.[35] Eesti 15-aastane kogemus ID-kaardi ja selle alternatiivide mobiil-ID ja

RIA SOOVITUSED

Kasutajale

- Kasuta salasõna asemel salafraasi. Ära taaskasuta sama salasõna eri teenustes.
- Vaheta seadme või teenuse vaikeparool (esmane salasõna) uue turvalise salasõna vastu.
- Kui võimalik, kasuta kaheastmelist autentimist (seda on ka ID-kaart, mobiil-ID või Smart-ID). Eelista olemasolevat kaheastmelise autentimise vahendit uue kasutajanime ja parooliga kasutajakonto registreerimisele.
- Hangi paroolihaldur (tuntumad on näiteks LastPass, Bitwarden, 1Password, Dashlane ja KeePass). See aitab iga veebilehe jaoks genereerida unikaalse, tugeva salasõna ning vähendab seega riski, et ühe salasõna lekkimise korral mitu sinu kasutajakontot ohtu satuvad.
- Kui sul on kahtlus, et su parool on teatavaks saanud kõrvalistele isikutele, olgu või heale tuttavale, vaheta see kohe.

Teenuseosutajale

- Disaini teenus turvaliseks ja ole realistlik kasutaja suutlikkuse suhtes. Selle asemel et nõuda kasutajalt järjekordse originaalselt keerulise salasõna väljamõtlemist, rakenda teenuses kaheastmeline autentimine.
- Andmeturbe seisukohast ei ole mõistlik nõuda kasutajalt teenuse tarbimiseks (näiteks veebipoest ostmiseks) kasutajakonto loomist. Kaalu, kas see on tingimata vajalik.
- Võimalda pikki salasõnu ehk salafraase (minimaalselt 8, maksimaalselt vähemalt 64 märki) ja võimalda salasõna moodustamisel kõigi märkide kasutamist.
- Loobu nõuetest salasõna ehitusele – suuna kasutaja raskesti meeldejäävate või näiliselt keerukate salasõnade (nagu p4r00L) asemel kasutama pikki paroole.
- Piira süsteemis levinumate nõrkade salasõnade (nagu 123456, password, admin või kasutajanimi) kasutuselevõttu.
- Ära nõua ega paku paroolivihjete (näiteks ema neiupõlvenimi, lemmiklooma nimi) kasutust – need on sageli kergesti äraarvatavad või leitavad sotsiaalmeediakontode kaudu.
- Loobu paroolide aegumistähtajast, eriti kui see on lühike – lähtu põhimõttest, et parool tuleb muuta juhul, kui see on unustatud või lekkinud või sattunud teise isiku või küberkurjategija kätte.

Vaata ka:

RIA kaheastmelise autentimise juhised
https://blog.ria.ee/tag/kaheastmeline-autentimine/
USA riikliku standardi- ja tehnoloogiainstituudi (NIST) uued paroolisoovitused:
https://pages.nist.gov/800-63-3/
Ühendkuningriigi riikliku küberturbekeskuse (NCSC) soovitused:
https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach
Unikaalse ja meeldejääva paroolipõhja genereerimiseks võid kasutada ka
https://rabool.eu

Smart-IDga näitab paremaid tulemusi, ent needki on universaalsest kasutusest kaugel. Näiteks riigiportaali eesti.ee sisenemiseks kasutab ID-kaarti või mobiil-IDd kolm külastajat neljast, ülejäänud sisenevad pangalingi kaudu, kasutades enamasti koodikaarte.

Sestap ei saa me ka 2018. aastal läbi paroolidest rääkimata.

Möödunud aasta tõi uuenduse 15 aastat kehtinud paroolisoovitustesse. USA standardiamet NIST asendas 2003. aastast kehtinud suunised, mis kirjeldasid turvalist parooli kui kombinatsiooni suurtest ja väikestest tähtedest, numbritest ja erimärkidest. Muutuse põhjus on lihtne: nõuded on liiga keerukad ja nende tõhusus küsitav.[36] Uued soovitused seavad kasutajale realistlikumad ootused ning panevad rohkem rõhku teenusedisainile, mis toetaks kasutaja andmete turvalisust. Soovituste tuum on lihtne: parool peab olema pikk ning keskkond peaks võimaldama mitmeastmelist autentimist.

Eesti kasutajate 12 levinumat salasõna

1. 123456
2. parool
3. qwerty
4. 123456789
5. lammas
6. 12345
7. minaise
8. maasikas
9. kallis
10. killer
11. armastus
12. lollakas

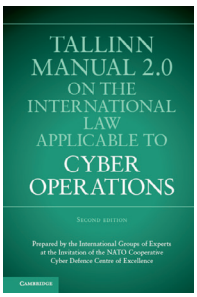
Allikas: CERT-EE[37]

KES RÜNDAB JA MIKS?

Eestile olulisimad küberohud pärinevad endistviisi (organiseeritud) kuritegevuselt ja vaenulikelt välisriikidelt. Rahvusvaheline kogemus näitab, et järjest enam on tõsiste küberintsidentide taga just riiklikud rühmitused.

Riigid kasutavad digitaalse keskkonna võimalusi traditsioonilise teabehanke kõrval üha vilunumalt mõjutustegevuseks ja oma geopoliitilise positsiooni tugevdamiseks. Järjest enam riike kinnitab küberründevõimekuse arendamist. NATO liitlased avaldasid 2016. aasta Varssavi tippkohtumisel, et küberruum on muutunud sõjapidamise domeeniks, kus NATO peab olema suuteline end kaitsma sama tõhusalt nagu õhus, maal ja merel. Eesti 2017. aastal vastu võetud julgeolekupoliitika aluste kohaselt korraldab Eesti küberjulgeolekut ühetaoliselt ja samade struktuursete lahendustega nii rahuajal kui ka sõjaolukorras, sedastades, et Eesti küberruum on kaitstav, kui riik ja ühiskond tervikuna selle kaitsmises osalevad, kui selleks on olemas vajalik kompetents ning ühiskond teab digitaalse keskkonna ohtusid ja oskab neid parimal viisil vältida ning probleemide korral reageerida.

Riikide võimearenduse kõrval jätkub rahvusvaheline debatt selle üle, missugused mängureeglid riikidele kübersfääris kehtivad. Selle valdkonna ühe autoriteetseima allika, küberoperatsioonidele kohalduva rahvusvahelise õiguse käsiraamatu täiendatud väljaanne ehk Tallinna käsiraamat 2.0 ilmus mullu veebruaris NATO küberkaitse koostöökeskuse eestvedamisel.[38] Käsiraamat analüüsib riiklike küberoperatsioonide kõiki vorme – küberspionaažist relvastatud ründega võrreldavate küberrünneteni – kehtivate rahvusvahelise õiguse normide kontekstis ning identifitseerib hulga rahvusvahelise õiguse norme, mis määratlevad riikide õigusi ja kohustusi küberoperatsioonide läbiviimisel. Vaatamata nt Vene Föderatsiooni ja samameelsete riikide retoorikale, on ilmne, et küberruum ei ole õiguslik vaakum, kus normid ei kehti.



Sellele vaatamata, või ehk just seetõttu, jätkuvad osa riikide püüdlused reeglite hallis alas toimetada ja seda laiendada.

Eesti saab juurde sõjalise võimekuse küberruumis

Selle aasta augustis moodustatakse kaitseväe koosseisu küberväejuhatus, mis saavutab täieliku valmisoleku lähiaastatel. Staabi- ja sidepataljoni ülema abi major Silver Andre selgitab, mida küberväejuhatus endast kujutab.

Küberväejuhatus hakkab kaitsma kaitseministeeriumi valitsemisala küberruumi. Tänapäeval vaadeldakse küberruumi sõjaliste operatsioonide neljanda domeenina maa, õhu ja vee kõrval. NATO jõudis sellise käsitluseni 2016. aasta kaitseministrite kohtumisel.

Eraldi väeliiki kaitseväes juurde siiski ei teki. Küberväejuhatus on staabi- ja sidepataljoni baasil moodustatav struktuurüksus kaitseväe juhataja otsealluvuses, mis on NATO võrgustiku üks osa ning üksuse ülesandeks on parandada kaitseväe arusaamist küberruumist ja saavutada selles olukorrateadlikkus, tuvastada küberohtusid ja neid ennetada. Erinevaid operatsioone küberruumis ollakse valmis läbi viima nii rahuajal kui ka sõjaolukorras.

*O*leme 24/7 rünnaku all

Küberruumis toimuv vaenulik luure- ja mõjutustegevus on igapäevane. Infokeskkonna kaudu mõjude saavutamine on kõige kuluefektiivsem, sest süvaoperatsioone on võimalik kauge maa tagant läbi viia väikeste kuludega ja suhteliselt turvaliselt. IT-lahendustest sõltuva ja halvasti turvatud riigi halvamine on kübermõjutusega lihtsam kui konventsionaalse sõjapidamisega.

Eestit rünnatakse küberruumis igalt poolt ja igal ajal. Kasutatakse teiste riikide infosüsteeme, nii et USAst tehtud rünnaku taga võib olla hoopis mõni Aasia või Euroopa riik. Riigina oleme teadlikkuse ja reageerimise osas heal järjel, aga kübersõja mõistes on veel palju vaja ära teha, et saavutada vähemalt rahuldav tase.

Kes üksuse moodustavad

Küberväejuhatuse suurus saab rahuajal olema umbes 300 inimest. Lisaks infooperatsioonidele (mille üks osa on küberoperatsioonid) vastutatakse IKT teenuste osutamise, juhtimistoetuse ja strateegilise kommunikatsiooni tagamise eest. Rakenduse uues üksuses leiavad nii juba kaitseväes töötavad oma ala eksperdid, kuid kindlasti ka asjatundjad erasektorist. Küberväejuhatus asub füüsiliselt peamiselt Tallinnas, aga virtuaalselt siis, kui vaja, ja seal, kus vaja.

Riikide küberründed elutähtsate teenuste vastu

Pöördepunktiks elutähtsate teenuste küberturvalisuse jaoks sai 2015. aasta jõuludele eelnenud küberrünnak Ukraina elektrijaama vastu, mis kahjustas selle juhtimissüsteemi ja lõi jaama töö tundideks rivist välja. Kahtlus juhtumiga seoses langes Vene Föderatsioonile.39 Selle sündmuse järel on avalikkuse ette jõudnud hulk juhtumeid, kus küberründeid mõne ühiskonna toimimiseks kriitilise teenuse vastu on seostatud vaenuliku välisriigiga.

ENERGIASEKTOR

Suvel kirjutasid USA ja Briti meedia sissetungimistest USA energeetikaettevõtete ärivõrkudesse ja energiatööstuses kasutatavaid tööstuskontrollsüsteeme tootva ettevõtte infosüsteemidesse.[43] Ründevahendina kasutati pahavaraga varustatud õngitsuskirju, mille abil saadi juurdepääs vähemalt tosina ettevõtte kontorivõrgule, nende seas ka Kansases paiknev tuumajaam. Mõlema ründe eest arvatakse vastutavat välisriigi heaks töötavad isikud ning peamine kahtlusalune on Venemaa. Sama grupeeringut seostati ka kevadsuvel toimunud rünnetega energiatootjate vastu USAs, Iirimaal ja Türgis.[44] Need ohud on aktuaalsed ka Eestis – eelmisel aastal kirjutasime oma aastakokkuvõttes suunatud ründest Viru Keemia Grupi vastu, mis osutab erinevaid kriitilisi teenuseid Ida-Virumaal.

Ehkki USAs tuvastatud intsidendid ei mõjutanud vahetult energiatootmist ega energiavõrkude toimimist laiemalt, suurendab kontorivõrgule juurdepääsu saamine tootmissüsteemide haavatavust. Energiatootmist korraldavad süsteemid on küll eraldatud eraldi võrgusegmenti, kuid tihti pole kaasaegsete turvalahendustega varustatud. Ründaja ligipääs kontorivõrgus töödeldavale teabele tootmise korralduse ja riskide kohta (kirjavahetus, taristu dokumentatsioon jne) võimaldab hilisema ründe ettevalmistamist ja elluviimist.

Möödunud aastal jäid selliste operatsioonide sihtmärgina enim silma energia-, side- ja pangandussektor.

Septembris toimunud Vene-Valgevene sõjalise ühisõppuse Zapad 2017 ajal täheldati Venemaa ja Hiina internetiaadressidelt lähtunud teenustõkestusründeid Soomes Ahvenamaa mobiilsidevõrgus; sarnaseid intsidente oli lisaks Soomele väidetavalt ka Ühendkuningriigis ja Hollandis.[40] Läti seimi julgeolekukomisjoni asejuht kinnitas, et ka Läti mobiilsidevõrke suve lõpul tabanud seitsmetunnine katkestus oli suure tõenäosusega tingitud Venemaa militaartegevusest Läänemerel.[41]

Eestis Zapadiga seoses teenustõkestusründeid ei täheldatud. Küll kinnitas Norra samal ajal Venemaalt lähtunud raadiohäireid, mis mõjutasid lennuliiklust, põhjustades GPS-teenuse tõrkeid.[42] Sarnaseid juhtumeid on tulnud ette ka varasemate Vene Föderatsiooni sõjaliste õppuste käigus ja ilmselt ei ole tegu taotlusliku ründe, vaid kõrvalmõjuga, mida mööndakse, ent ei püüta vältida.

Kasvab ka ekspertide mure Põhja-Korea kasvava küberründevõimekuse ja -valmiduse üle. Mitme viimasel paaril aastal pangandussektorit tabanud küberründe taga nähakse just Põhja-Korea päritolu küberrühmitusi, eesotsas riigi huve teeniva Lazarus kinniskinnisründeohu ehk APT-ga. Lisaks 2016. aastal Bangladeshi keskpanga vastu toime pandud suuremahulisele kelmusele peetakse sama rühmitust vastutavaks ka pikaajalise kampaania eest 31 riigi pangandussektori sihtmärkide vastu.[45] Konkreetsel juhul sisestati veebilehtede turvanõrkusi ära kasutades neisse senitundmatut pahavaravarianti, mis nakatas spetsiifilistele parameetritele vastavate külastajate seadmed. Teiste seas nakatusid Poola kommertspangad, keda nakatati Poola finantsjärelevalveasutuse veebilehe kaudu.[46]

Lazarus APT tegevuse fookus on viimasel paaril aastal üha enam liikunud pankade, hasartmänguplatvormide, finantstarkvara tootjate ja krüptorahaäri osaliste ründamisele: püütakse manipuleerida SWIFT-liideseid ja tehingute kontrollimehhanisme või kasutatakse spetsiaalselt sihtmärgile kohandatud pahavara.[47] Peamiselt andmepüügi kaudu varastatud kontoandmete abil rünnatakse nii krüptorahaettevõtteid, krüptovaluutabörse kui krüptoraha kaevandamise teenuseid.

Küberruumist alguse saanud ründed demokraatlike protsesside vastu

2017. aastal läbiviidud ja ka seni käimasolevad uurimised on praeguseks andnud hea ettekujutuse, kuivõrd ulatuslikult ründas Vene Föderatsioon USA presidendivalimiste eel ja ajal USA valimistega seotud infosüsteeme.

Juba 2017. aasta esimestel päevadel avaldasid **USA** luureametkonnad ühisraporti Vene Föderatsiooni luureteenistuste küberrünnakute kohta USA presidendivalimiste eel.[48] Raporti põhijärelduste kohaselt olid rünnete korraldajaks Vene Föderatsiooni luureteenistused, kes tegutsesid riigi kõrgeima juhtkonna korraldusel. Demokraatliku partei infosüsteemidesse sissemurdmise ja varastatud sisedokumentide avaldamise eesmärk oli avalikkuse meelsusega manipuleerimine, et tagada valimisedu eelistatud kandidaadile, diskrediteerida vastaskandidaati ja tekkinud segaduse läbi kahjustada avalikkuse usaldust USA valimis- ja valitsemisprotsessi vastu. Selle saavutamiseks kombineeriti andmepüügirünnakuid, nende abil saadud tundliku teabega manipuleerimist ja valikulist lekitamist, toites sellega Venemaa riiklikult rahastatavat propagandat meedias ja sotsiaalvõrgustikes.

Tõdetakse ka, et Vene Föderatsiooni luureteenistused saavutasid juurdepääsu mitme osariigi valimiskomisjonide infosüsteemidele, ehkki häältega manipuleerimist valimisseadmetes ei kinnitata. Hiljem on selgunud, et rünnata on püütud nii teenust pakkuvaid ettevõtteid kui ka näiteks häälte kogumiseks kasutatavaid süsteeme.

See näide ilmestab hästi, kuidas vaenulike riikide jaoks on küberruum üks lahinguväljadest, kus saavutada mõjuvõimu teiste riikide üle.

Küberründed demokraatlikke protsesse võimaldava tehnoloogia vastu on sageli oportunistlikud – eesmärk ei pruugigi olla süsteemide toimimist halvata või andmeid varastada, poliitiline tulemus on saavutatud juba siiski, kui õhku jäävad küsimused näiteks valimisprotsessi legitiimsuse osas. Lisaks – nagu tõestavad ründed USA 2016. ja Prantsusmaa 2017. aasta presidendivalimiste vastu – on küberelement alati integreeritud laiemasse lähenemisse ning ka küberründed ise võivad tähendada läbipõimununa nii kampaaniaaegseid andmevargusi ja teabelekkeid kui valimissüsteemide turvanõrkuste ärakasutamist.

Valimistehnoloogia on seega õigustatult olnud kõrgendatud tähelepanu all, eriti kuivõrd ründed ei ole sageli suunatud mitte valimiste toimumiseks kasutatavate kesksete süsteemide (valijate ja kandidaatide nimekirjad, häälte kogumine, lugemine ja tulemuste avalikustamine), vaid nendega seotud (digitaalsete) teenuste ning ennekõike kandidaatide ja erakondade vastu. Kuigi viimane ei mõjuta valimiste toimumist, on võimalik mainekahju valimiste legitiimsusele kõrge. Veelgi enam, enamik viimaste aastate „kampaaniahäkkidest" ongi olnud suunatud just nende kaasnevate süsteemide vastu ja sageli toitnud just edasiste info- ja mõjutusoperatsioonide pikemaajalisi eesmärke.

Lisaks USA presidendikandidaatide kampaaniate vastastele küberrünnakutele teatas Emmanuel Macroni kampaaniameeskond vahetult **Prantsusmaa** presidendivalimiste teise vooru eel „massiivsest ja koordineeritud" küberründest, mille tagajärjel paisati anonüümses internetikeskkonnas avalikkuse ette suur hulk erakonna sisemist kirjavahetust ja dokumente.[49] Dokumendileke toimus vahetult enne valimiseelse poliitdiskussiooni keelu jõustumist, mis ei võimaldanud nende sisu ametlikult kommenteerida ega ajakirjanduses kajastada ning jättis tõlgendamise ja vandenõuteooriate levitamise sotsiaalvõrgustike meelevalda. Nagu USA valimiste eel, kombineeriti ründajate lekitatud materjale ka nüüd väärinfoga, et külvata segadust ja kahtlusi.[50] Macroni kampaaniameeskond oli juba varem valimiskampaania käigus korduvalt viidanud erakonna juhtide e-posti kontode vastu üritatud häkkimiskatsetele ning nii Prantsusmaa kui Saksamaa informeerisid avalikkust juba kuid enne valimisi märgatavalt hoogustunud küberrünnetest riigi digitaalse taristu vastu. Mõlemad võtsid kasutusele abinõusid valimistega seotud intsidentide ärahoidmiseks, pöörates enam tähelepanu erakondade teadlikkusele küberriskidest ning otsides viise libauudiste leviku tõkestamiseks sotsiaalmeedias.[51]

„Valimistevastased" küberründed ei ole eesmärk omaette ega ka Venemaa ainus viis küberruumi kaudu lääneriike mõjutada. Arvestada tuleb nii vahetute mainerünnete, spetsiaalselt majanduslike või poliitiliste huvide või ka taristu kahjustamiseks mõeldud

rünnetega. Viimaste tõenäosus on Eesti puhul madal, aga mitte olematu. Möödunud aasta ulatuslike WannaCry ja NotPetya pahavarakampaaniate varal võib öelda, et stsenaarium, kus suhteliselt kitsast eesmärki täitev küberrünnak väljub ründaja kontrolli alt, on väga tõenäoline.

Eesti riigi ja ühiskonna harjumuspärase toimimise jaoks on oluline, et küberriskidega arvestatakse riigi ohuhinnangute koostamisel ja riskistsenaariumide planeerimisel praeguseks läbivalt. Isoleeritud nähtust nimega „infotehnoloogiline oht" esineb üliharva, enamasti on küberohtudel tähendus just laiema riskistsenaariumi võimaldaja või võimendajana.

KÜBERÜNNETE OMISTAMINE JA RIIKIDE VASTUS

Võrreldes veel aastatagusega on 2017. aastal toimunud selge muutus selles, et välisriikide toimepandud küberründed avalikustatakse ja viidatakse nende riiklikule päritolule. USA valimiskampaania ründed, WannaCry ja NotPetya olid selles otsustavad suunamuutjad.

Rahvusvahelises poliitikas ei ole omistamine pelgalt hinnang kindlaks tehtud tehnilistele faktidele – see on selge signaliseerimise vahend, et küberrünnet ei peeta triviaalseks või aktsepteeritavaks käitumisviisiks. Pingestunud rahvusvahelises olukonnas on küberrünnete omistamisel võtmeroll heidutuse loomises. Seda võimaldab Eesti ELi eesistumise ajal Euroopa Liidu liikmesriikide vahel kokku lepitud välispoliitikameetmete raamistik (*Cyber Diplomacy Toolbox*)[52], mis loob aluse ELi riikide kollektiivseks reaktsiooniks. Seega muutub omistamise puhul järjest olulisemaks poliitiline ja õiguslik element.

Tehnoloogia riskid

Kogu Eesti ühiskond sõltub niinimetatud digitaalse alustaristu – nii interneti alusarhitektuuri, -teenuste ja -protokollide (DNS, BGP) kui ka Eesti riigi eID ja X-tee – toimimisest. Kogu süsteemi ulatuslik häire või teenuse täielik katkemine on vaevalt tõenäoline, aga selliste ehmatustega, nagu ID-kaardi juhtum möödunud sügisel, tuleb arvestada ning neiks valmis olla. See, et ilmneb mõni varem teadmata kriitiline turvanõrkus nagu Meltdown ja Spectre tänavu jaanuaris, mis mõjutab väga paljusid süsteeme ja kasutajaid ning mis tuleb kiirkorras ära paigata, on juba aastases väljavaates üsna ootuspärane. Niisuguste nõrkuste otsimises võistlevad nii riigid (kaitse- või ründemotivatsiooniga), teadusasutused kui kurjategijad. Alati tuleb arvestada, et tehnoloogia ise pole kunagi sajaprotsendiliselt turvaline ja turvalisus on ajas muutuv.

Mis on „tugev krüptograafia“ ja miks see on oluline?

Praegune avalik debatt krüptograafia ja tagauste teemal keskendub valikule riiklik julgeolek ehk jälgimisvõime versus privaatsus. Eesti jaoks on enne neid fundamentaalsem riikliku identiteedi usaldusväärsuse küsimus, millele tugineb kogu meie digiriigi ökosüsteem.

Sisult on krüptograafia andmeturve matemaatiliste meetoditega, mille ülesandeks on tagada andmete konfidentsiaalsus ja terviklus, seega ka autentne ja usaldusväärne digitaalne identiteet. Usaldusväärsuse ja turvalisuse sünonüümina on krüpteerimistehnoloogia digitaalse ühiskonna alustala. Ehkki riiklikult tagatud digitaalse identiteedi mõttes on Eesti endiselt suhteliselt unikaalne, kasutatakse krüptograafial põhinevaid lahendusi laialdaselt nii valitsuste, ettevõtete kui ka üksikisikute tasandil.

OLEME MONOKULTUURI PANTVANGIS

RIA küberturvalisuse teenistuse uurimis- ja arendusosakonna juht Kaur Virunurm hoiatab, et tehnoloogiline keskkond paremaks ei muutu ja peame harjuma sellega toime tulema.

Maailm on väheste suurfirmade käes pantvangis. Igas IT valdkonnas – kiibid, operatsioonisüsteemid, telefonid, teenused – domineerib paar-kolm suuremat tootjat, kel on oma tehnoloogilises kihis pea täielik ülemvõim, ning see monopol on globaalne, st sama elektroonikat ja tarkvara kasutavad nii USA, Venemaa kui Eesti.

Ka kodanike ja kasutajate andmed on suurte ühisteenuste (Google, Facebook) käes koos. Sisuliselt on tekkinud monokultuur. Apple ja Microsoft, AMD ja Intel, Google ja Amazon on monopolid, kellest sõltub kogu maailma töö.

Ka turvavead mõjuvad korraga kõikidele süsteemidele ja teenustele üle kogu maailma. Suurem mõju tõstab turvavigade olulisust ja hinda. Kuna aukude leidmiseks luuakse aina efektiivsemaid lahendusi, kasutatakse automatiseerimist ja masinõpet, siis leitakse vigu ka vanades süsteemides. Mustal turul maksavad mõjusamad turvaaugud miljoneid dollareid. Turvanõrkuste leidmine ja vahendamine on seetõttu muutunud pea omaette majandusharuks.

Meie ID-kaardi murdnud turvanõrkus (ROCA) on üle kümne aasta vana. 2017. suvel murti lahti seni turvaliseks peetud WiFi. Seegi viga oli tehtud ammu, aga leiti alles nüüd. 2018. alguses avaldatud Inteli ja AMD protsessorite turvavead (Spectre/Meltdown) on üle 20 aasta vanad.

Vanu vigu on aga keeruline ja kallis paigata.

Spectre/Meltdowni parandused lihtsalt ei töötanud, tegid arvutid aeglaseks või rikkusid need sootumaks. ROCA parandus nõudis arvutite sisemise tarkvara (*firmware*) uuendust ja jäi enamasti juurutamata. Enamik vanemaid Androidi telefone ei saa mingeid turvauuendusi.

Vigu võimendavad veelgi nende „kogujad". Shadow Brokersi nimeline grupp avaldas 2016–2017 suure paki (ilmselt USA julgeolekuametkondade kogutud) ründevahendeid ja *exploit'*e. WannaCry ja NotPetya intsidendid algasid just sellest lekkest.

Selliseid kogujaid on veel, ja kuna nad kasutavad ise sama tehnoloogiat, mida ründavad, on nad ise samuti haavatavad.

Seega ühed grupid koguvad turvavigu; teised ründavad esimesi, varastavad ja müüvad nende „tööd"; kolmandad kasutavad neid ära, rünnates või häirides kõiki teisi.

Kokkuvõttes peame – vastumeelselt – leppima maailmaga, kus kõik süsteemid on haavatavad või kus täna turvaline lahendus on homme kogu maailmale valla. Saame loota vaid sellele, et kui meid kaitsvaid turvakihte on palju, siis mõni neist peab ja tõkestab ründe või laseb meil sellest taastuda.

Praegu teadaolevate eelduste säilimisel ei too tulevik leevendust. Tehnika ja selle nõrkused jõuavad kõikjale, ka sinna, kus neid hetkel pole: nutiautod ja targad teed, andmekaevandamine ja totaalne jälgimine, robootika ja tehisintellekti areng ning kvantarvutus toovad meile ühiskonna, mida suudame praegu vaid aimata. Karta on, et uue maailma küberriskid saavad olema hullemad kui 2017. aasta omad.

Eesti riikliku digitaalse identiteedi turvakindlus sõltub täiel määral tugevast krüptograafiast – sellest, et on objektiivselt võimalik usaldada, et isik ja tema tahteavaldus vastavad sellele, kellena nad näivad. Mitte keegi ei saa esineda kellegi teisena, et tema

nimel midagi teha. Sellele kindlusele tugineb kogu meie digiriigi ökosüsteem.

Mis tahes tagauks teenuses murraks seetõttu ka digitaalse ökosüsteemi usaldusväärsuse ja kahjustaks usaldust selle vastu. Oluline on toonitada, et siin ei räägita privaatsusest, vaid teenuste toimimisest. Kui krüptograafia on „nõrk", siis teenused ei toimi. Sama usaldus on kogu riikliku digiökosüsteemi ja küberturvalisuse vältimatu alus: kui usaldus ökosüsteemi vastu kaob, kaob ka Eesti võime praegusel harjumuspärasel viisil riigina toimida. Kui digitaalsed teenused ei ole usaldusväärsed, peab pöörduma tagasi füüsiliste teenuste osutamise juurde. Meie ühiskonna ressursside puhul tähendab see vältimatult, et avaliku teenuse kvaliteet ja maht langeb ning riik tervikuna nõrgeneb.

Praeguses maailmas on võimalused üldiseks krüptograafia nõrgestamiseks kadumas – krüptograafiat ei saa nõrgestada ilma digitaalseid süsteeme kompromiteerimata. Ei ole võimalik luua tehnilist võimalust krüpteeritud infole ligipääsemiseks üksnes valitud isikutele – sellega koos luuakse ühtlasi turvanõrkus kurjategijatele, terroristidele ja vaenulike riikide välisteenistustele. Tarkvara turvanõrkusi puudutavaid teabelekkeid ei saa garanteeritult välistada ka väga kõrge infoturbestandardiga organisatsioonide puhul, nagu kinnitab mullu kahest USA julgeolekuametkonnast lekkinud teave küberoperatsioonide tööriistade kohta.

Nii tarkvaraturg kui ka kuritegevus on fundamentaalselt piiriülesed. Seetõttu ei ole kuidagi võimalik välistada krüpto- ja suhtluslahenduste loomist, mida riikide kontrollile allutada ei saa.

Riikliku identiteedi turvakindlus pole riikliku jälgimisvõime *versus* privaatsuse küsimus. See on avalike teenuste toimimise ja mittetoimimise küsimus – ja selle kaudu sootuks laiem ühiskonna turvalisuse küsimus.

VALDKONDLIKUD RISKID JA VALMISOLEK

Eesti küberturvalisuse alused määratlenud esimese küberjulgeoleku strateegia jõustumisest möödub tänavu kümme aastat. Suures plaanis on see meid hästi teeninud. Sellest, et Eesti rahvusvaheline kaal ei ole üksnes mainekujunduslik edu või üksikute innovaatiliste saavutuste tagajärg, annab kinnitust 2017. aasta Rahvusvahelise Telekommunikatsiooni Liidu (ITU) üleilmne küberturvalisuse indeks, mis paigutab Eesti küberturvalisuse korralduse poolest maailmas viiendale kohale.53

Ent edetabelikohad on siiski vaid pinnapealne hinnang ja turvalisuse tagamiseks ei piisa üksnes heade eelduste olemasolust. Eesti on 2018. aastal üks maailma digitaalselt sõltuvamaid riike. Riigi ja ühiskonna valmidus küberturvalisusse panustada jääb praegu sellele sõltuvusele alla.

EESTI KÜBERTURVALISUSE ALUSED

- Küberjulgeoleku strateegia: strateegilised eesmärgid ja pädevusjaotus
- Turvanõuete miinimumraamistik: infosüsteemide turvameetmete süsteem (ISKE) riigi ja kohalike omavalitsuste andmekogudele; elutähtsate teenuste osutajate riskihinnangud ja toimepidevusplaanid; riigi digitaalse alustaristu (eID, X-tee) turvalisus
- Riiklik 24/7 reageerimisvõimekus (CERT-EE)
- Kriisideks valmisolek ehk küberturvalisus osana riigikaitse laiast käsitlusest
- Teadlikkus ja oskused
- Koostöö riigiasutuste vahel ja erasektoriga ning rahvusvaheline koostöö

RIA KÜBERTURBEFOOKUS 2017: VALMISOLEK JA ENNETUS

- Mõju- ja trendihinnangud
- Hoiatused
  – *Avalikkusele aktuaalsetest ohtudest ja turvanõrkustest*
  – *Elutähtsate teenuste osutajatele valdkonna- või trendipõhiselt koos analüüsi ja soovitustega*
- Valmisoleku kujundamine: plaanid ja õppused
- Küberhügieen ja koolitused
- Turbe- ja koostöökultuuri ning küberturbekogukonna ehitamine

Riik

Riigiasutuste intsidendid näitavad, et võimalus küberturvalisust teadlikkuse tõstmisega parandada on ammendunud ning keskenduda tuleb turvalisele arhitektuurile ja kompetentsele personalile.

Globaalselt on riigiasutused finants-, side- ja tervishoiuvaldkonna kõrval ründeobjektide loetelu tipus.[54] Riigiasutusi puudutavate vahetute ohtude seas on endistviisi levinuim andmepüük, ent selle juures tuleb arvestada, et küberrünnakud on tihtipeale osa vaid üks osa rünnakust riigi kui terviku usaldusväärsuse vastu. Eesti riigi ja ühiskonna harjumuspärase toimimise kindlustamiseks on väga oluline arvestada küberriskidega riigi kõikides ohuhinnangutes ja riskistsenaariumides. Nagu tõdetud, esineb isoleeritud nähtust nimega „infotehnoloogiline oht" tegelikkuses üliharva, enamasti on küberohtudel tähendus just laiema riskistsenaariumi võimaldaja või võimendajana.

Eesti riigiametnike küberturbealane teadlikkus on üsna heal järjel, sellele on kaasa aidanud ka meie küberturbekoolitused eesistumisele eelnenud aasta jooksul, kus kokku osales ligi 1200 ametnikku. Mullu kevadel avasime riigiasutustele kasutamiseks Digitesti digitaalse õpikeskkonna, kus küberteadmisi testida ja täiendada.

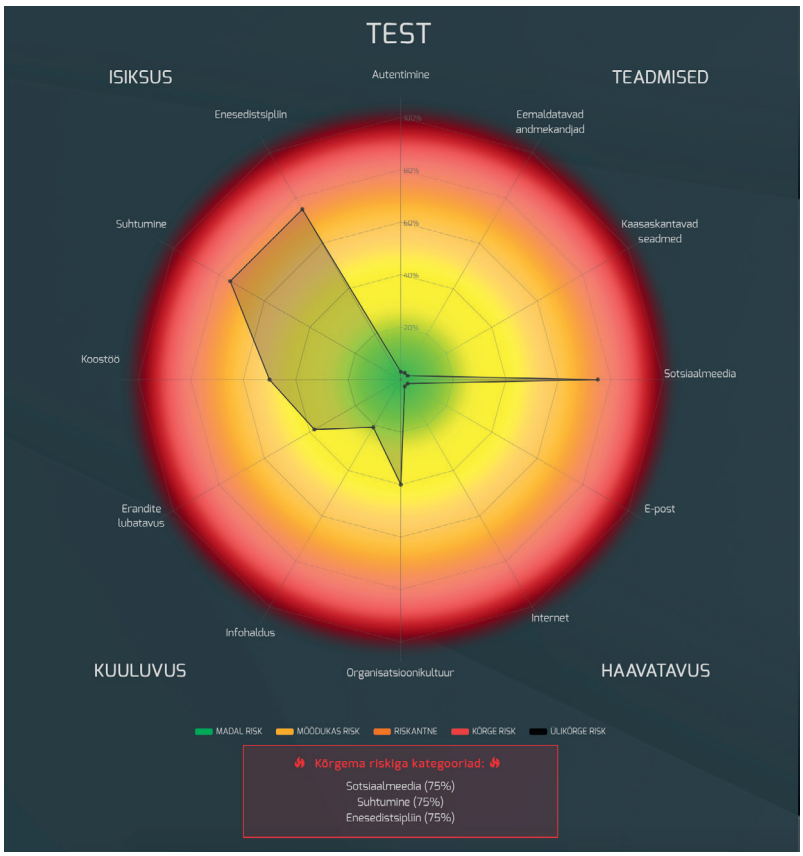
Eesti riigiasutustes oli eelmisel aastal pahavaraga nakatumise juhtumeid vähe, näiteks lunavaraga nakatumisi polnud ühtki. **Avaliku sektori küberturvalisuse suurimaks murekohaks on seadmeriketest või inimlikest eksimustest tingitud teenusekatkestused**. Iseäranis on need kriitilised neis süsteemides, mille toimimisest sõltub siseturvalisus ja riigi julgeolek – politsei, piirivalve või päästeteenused – või inimeste elu ja tervis, nagu häirekeskus ja digiretsept. Et riigi funktsioonidele ei saa pakkuda alternatiivi teine teenusepakkuja, on ülioluline tagada neile teenustele piisav ressurss varulahenduste toimimiseks. Paremat turvet ja

Digitesti kursuse on edukalt läbinud tuhanded riigitöötajad

2017. aasta kevadel valmis RIA ja küberturbeettevõtte CybExer Technologies koostöös riigiasutustele mõeldud digiõppeplatvorm, millega on praeguseks testitud tuhandete riigitöötajate küberteadmisi ja välja selgitatud nende küberriskid.

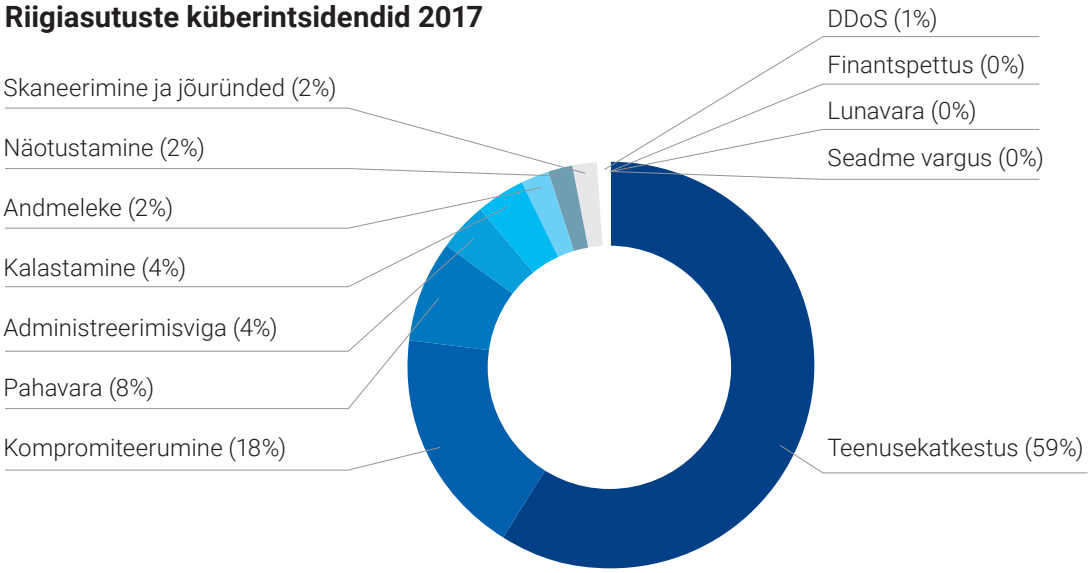
Praeguseks on Digitesti kursuse läbinud tuhanded Eesti riigiametnikud. Kasutuslitsentsi on omandanud kümned Eesti era- ja avaliku sektori asutused, paljud ülikoolid ning mitmete välisriikide ametid ja ettevõtted, kes on huvitatud oma töötajate küberteadlikkuse tõstmisest. Kuigi Digitesti tulemused jäävad turvakaalutlustel iga asutuse enda teada, on tulevikus plaanis välja arendada tulemuste anonüümne ja turvaline jagamismehhanism, mis võimaldaks igal asutusel end üldise olukorraga võrrelda.

Tulevikus soovime Digitesti kasutusala riigisektoris veelgi laiendada ning selle läbimine võiks saada kohustuslikuks kõikidele riigi- ja kohalike omavalitsuste töötajatele. Selleks, et panna alus küberoskustele uue põlvkonna hulgas, on plaanis jagada Digitesti koolidega, et küberhügieeni õpet saaksid ka koolilapsed põhihariduse ühe osana.



Digitest annab riskiprofiili kasutaja, organisatsiooni ja riigi tasemel. See võimaldab täpsemat riskijuhtimist, kus pööratakse tähelepanu konkreetsetele nõrkustele.

Riigiasutuste küberintsidendid 2017



toimekindlust on suutnud tagada just riigiasutuste IT-keskused, kes on teenusetõrked ja -katkestused suutelised ka kiiresti kõrvaldama ning rünnetele reageerima.

Eesti riigiasutused ei saa unustada ka seda, et nende infosüsteeme ja vastupidavust skaneeritakse pidevalt. Jälgime seda tegevust hoolikalt ja vajadusel informeerime kõigest ebatavalisest. Üheks näiteks seesugusest juhtumist oli 2017. aasta lõpul aset leidnud seeria lühiajalisi väikesemahulisi teenustõkestusrünnedeid mitme Eesti riigi- ja teadusasutuse vastu. Märgatavat mõju teenustele ründed ei avaldanud, eriliseks tegi need just ajaline lähestikkus, madal intensiivsus ning sarnane muster ehk liiklus täpselt mõõdetud ajavahemikes.

Kuna sellise tegevusega on võimalik valmistada ette ka hilisemaid ründeid, on iga sellise juhtumi järelanalüüs alati oluline ja sellistest juhtumitest tuleks alati meile teada anda e-posti aadressil cert@cert.ee.

Kohalikud omavalitsused

Võrreldes riigiga on kohalike omavalitsuste küberturvalisuse tase endiselt ebaühtlane.

Kuna kohalikud omavalitsused on Eesti digiriigi lahutamatu osa, võib nende nõrk infoturve tekitada riske ka riigi kesksetele andmekogudele. Näiteks töötavad omavalitsused rahvastikuregistri või sotsiaalvaldkonna kesksete andmekogudega, mis nõrga infoturbe korral võib kaasa tuua riske delikaatsetele isikuandmetele. Kohalikel omavalitsustel on ISKE baasturbenõuete rakendamise kohustus, mida paljud omavalitsused siiski ei täida.

Rahandusministeerium on haldusreformi raames toetanud omavalitsuste IKT konsolideerimist ja töös on platvorm, mis muu hulgas lihtsustaks omavalitsustel infosüsteemide turvalist ülesehitamist. Seda võiksid kõik omavalitsused kasutada. Korraldame avalikule sektorile regulaarselt infopäevi ja seminare, millest on võimalik osa saada ka kohalikel omavalitsustel. Turbetaset aitaks omavalitsustes oluliselt parandada ka infoturbe eest vastutava isiku määramine, kes selle teemaga süstemaatiliselt tegeleks. Praegu on Eestis selliseid omavalitsusi üksikuid.

„TURVALINE HARJUMAA" VALVEKAAMERAD

2017. aasta sügisel toimus rida sissemurdmisi Harju Omavalitsuste Liidu projekti „Turvaline Harjumaa" raames paigaldatud valvekaameratesse neljas omavalitsuses. Rünneteks kasutati ära kaamerate lappimata turvaauke ning asjaolu, et ligipääs seadmetele oli piiramata. Kompromiteeritud kaamerad ei edastanud ega salvestanud mitme päeva vältel pilti. Tänu ühe valla infoturbetöötaja teavitusele saime juhtunust teada ning edastasime hoiatuse teistele omavalitsustele, avaliku sektori infoturbejuhtidele ja elutähtsate teenuste osutajatele ning andsime suunised turvanõrkuse kõrvaldamiseks.

Erinevalt riigist oli omavalitsustes mullu enamik intsidentidest pahavaraga nakatumised ja aegunud tarkvara kasutamise tõttu veebilehtede ärakasutamine rünneteks omaniku enda vastu (näotustamine) või veebilehtede külastajate vastu. Näiteks kasutati 2017. aastal omavalitsuste kodulehti rämpsposti levitamiseks ja ka pangaandmete õngitsemiseks.

Foto: Arno Mikkor

Ühiskonnale olulised teenused

Ühiskonna küberturvalisus tervikuna toetub erasektorile, kes osutab enamikku (digitaalseid) teenuseid, millest ühiskonna normaalne toimimine sõltub. Kui oma küberturvalisuse eest vastutab ennekõike infosüsteemi omanik ise, siis ühiskonna kui terviku kaitse peab tagama riik.

Eestis on elutähtsate teenuste küberturvalisus teenuseosutaja kohustus alates 2009. aastast, mil jõustus hädaolukorra seadus. See pani elutähtsa teenuse osutajale kohustuse hinnata oma teenuste toimepidevusriske – ka neid, mille põhjus või väljendus on küberruumis – ja rakendada meetmeid toimepidevuse tagamiseks. Euroopa Liidu võrgu- ja infoturbedirektiiv, mille eest Eesti Euroopa Liidus seisis, võtab aluseks sama lähenemise – keskenduda tuleb teenustele, mis on vajalikud olulise ühiskondliku või majandusliku tegevuse toimimiseks. Need on teenused, mis on ka uue küberturvalisuse seaduse reguleerimisalas, millega Eesti direktiivi üle võtab.

Meie 2016. aastal tellitud uuringu kohaselt, millest kirjutasime lähemalt mulluses aastakokkuvõttes, sõltub kõigi Eesti elutähtsate teenuste osutamine elektrienergiast ja sideteenustest. Lisaks sellele, et energia- või sideteenuste katkestustel on otsene mõju teistele elutähtsatele teenustele, mõjutavad need ka riigiasutuste töö toimimist. Näiteks mullu hilissügisel põhjustas ühe sideettevõtja Pärnu sõlmpunktis paikneva toiteseadme rike andmesidekatkestuse, mis mõjutas nii sotsiaal- kui siseministeeriumi allasutuste pakutavaid teenuseid. Ehkki alternatiivlahendus oli olemas, sõltus ka selle töö samast seadmest ning kuluefektiivsuse kaalutlustel ei olnud asutustel lepingut dubleerivaks ühenduseks teiselt sidetaristu pakkujalt. Probleemiks oli seegi, et seaduse mõttes määrab intsidendi olulisuse see, kui suurt hulka teenusepakkuja lepingulisi kliente katkestus mõjutab. Olukord, kus häiritud on vaid ühe asutuse ehk ühe kliendi töö, ei anna alust erakorraliste abinõude rakendamiseks, ehkki mõjutatud isikuid võib olla arvukalt – teenusepakkujal on vähe võimalusi nende hulka kindlaks teha. Sarnane olukord on ka teiste riigiasutuste ja ettevõtetega, samuti eratarbijatega, kus leibkonnas on üldjuhul rohkem kui üks liige.

Valdkondlikud ohud, intsidendid ja meetmed turvalisuse tagamiseks

	Ohud ja riskid
Energiavarustus	Juurdepääsukatsed kontorisüsteemidesse, eesmärgiga pääseda ligi tootmistaristule. Sihitud andmepüük, nt pahavara alla laadivate e-kirjade kaudu, tagauksetarkvara paigaldamiseks. Päritolu: vaenulikud riigid Trend: ↗
Sideteenused	Tehnoloogia riketest ja inimlikest eksimustest tingitud teenusekatkestused. Sõltuvus välisühendustest. Trend: →
Meedia	Propaganda- ja maineründed infosüsteemide kompromiteerumise kaudu. Trend: ↗
eID	Teenuse kättesaadavuse sõltuvus teenuseosutajatest. Trend: →
Tervishoid	Lunavara, andmepüük; digitaalsete tugiteenuste (digiretsept, ravikindlustuse infosüsteem) mõju arstide töökorraldusele. Trend: ↗
Finantssektor	Finantspettuste katsed klientide suunal, sh arvete võltsimine küberkurjategijate poolt; krediit- ja paroolikaardiandmete õngitsemine; partnerpankade SWIFT-süsteemi manipuleerimiskatsed. Krüptoraha ja platvormid. Trend: ↗
Kommunaalteenused (kaugküte, veevarustus ja kanalisatsioon)	Lunavara; teenusekatkestused tingituna tehnoloogia riketest ja inimlikest eksimustest; administreerimisvead. Trend: →
Transport (lennuliiklus, lennuväljad, sadamad, raudteeliiklus, maanteevõrk)	Sõltuvus rahvusvahelistest infosüsteemidest. Trend: →
Haridus	Vähese teadlikkusega kasutajaskond; puuduv turbepoliitika ja vajalike oskustega töötajate nappus. Trend: →

Intsidendid Eestis 2017	Meetmed vastupanu- ja taastevõime tõstmiseks
Sideteenuse pakkuja seadmerikke tõttu lühiajaliselt katkenud kaugjuurdepääs energiatarnija tehnovõrgule.	Aktiivsem süsteemide seire nii administratiiv- kui tootmisvõrkudes, süsteemide turvatestimine. Kontori- ja tootmisvõrkude segmenteerimine.
Korduvad teenusekatkestused sideteenuse osutajate võrkudes, millest suurim mõjutas ligi 80 000 telefoniteenuse klienti, ent jäi õnneks öisele ajale.	Varulahendused ja toimepidevusplaanid.
Failiserveri paroolilekked.	Küberhügieen. Ristsõltuvuste haldamine.
Mobiil-ID teenusekatkestused sideteenuste osutajate võrkudes; ID-tarkvara allalaadimislehe teenusetõrked	Sideettevõtjate rakendatavad varulahendused; ristsõltuvuste haldamine.
Infosüsteemide rikked ja lunavarajuhtumid, mis mh häirisid haiglates patsientide vastuvõttu ja muutsid patsientide andmed kättesaamatuks *Vt ka eraldi alapeatükki*	RIA teadlikkuse tõstmise koolitused haiglatele; perearstikeskuste IT-teenuse ja turbe konsolideerimine; intsidentide seire juurutamine.
Lühiajalised (kuni tund) katkestused pankade kaardimaksete ja sularahaautomaatide ristkasutuse toimimises; häiritud välismaksete edastamine; mais Leedu SEB panga vastu toimunud teenustõkestusründe tõttu olid lühiajaliselt kättesaamatud kõigi kolme Balti riigi SEB panga kodulehed ja takistatud internetipanga kasutamine.	Eesti pankade kliendid on võrreldes enamiku riikidega paremini kaitstud, sest suuremate tehingute kinnitamiseks on vajalik turvaline autentimisvahend (ID-kaart ja selle alternatiivid). Jagatud olukorrateadlikkus pankade ning korraldavate ja järelevalveasutuste vahel.
Lunavarajuhtumid; administreerimisviga võimaldas välistel isikutel pääseda ligi teiste klientide andmetele.	Intsidentide seire juurutamine, varulahendused ja toimepidevusplaanid.
Väljalendude hilinemine tingituna seadmerikkest reisijate teenindamise infosüsteemis.	Varulahendused ja taasteplaanid.
Sagenev krüptoraha kaevandamine koolide arvutivõrkudes; kasutajaandmete leke kutseõppeasutuse arvutitesse paigutatud nn klahvinuhi kaudu.	Infosüsteemide administreerimisnõuded, juurdepääsuõiguste haldamine; küberhügieen.

Küberriskid tervishoiusektoris

Ehkki WannaCry-laadsed suured vapustused läksid Eesti tervishoiuasutustest mööda, oleme oma kõrgelt digiteeritud tervishoiuteenustega infosüsteemide töökindlusest erakordselt sõltuvad. Mullu leidis Eesti tervishoiusektoris meile teadaolevalt aset 32 küberturbejuhtumit, millest haiglate või perearstide tööd otseselt mõjutasid kümme. Seejuures oli mitmel juhul tegu ulatuslikuma teenusetõrke või -katkestusega, mis mõjutas korraga paljude arstide tööd ja hulga patsientide vastuvõttu – näiteks Lääne-Tallinna keskhaigla süsteemirike jaanuaris häiris tundideks haigla infosüsteemi tööd.[55] Patsientide terviseinfo leket ega sattumist küberkurjategijate kätte, millest mujal maailmas on värvikaid näiteid, mulluste juhtumitega teadaolevalt õnneks ei kaasnenud.

Haiglate ja tervishoiuasutuste tööd mõjutanud süsteemirikete kõrval paistavad silma mullused teenusekatkestused retseptikeskuse, kindlustusregistri ja haigekassa teenustes, mille kestus ühel juhul oli pikem kui ööpäev. Ka need intsidendid juhivad tähelepanu vajadusele pöörata küberriskide hindamisele ja infoturbe süsteemsele korraldusele rohkem tähelepanu.

PEREARSTIKESKUSTE LUNAVARAJUHTUMID

Teadaolevalt langes möödunud aastal lunavara ohvriks ka kaks Eesti perearstikeskust. Mõlemal juhul kasutati nakatamiseks kaugligipääsu perearstikeskuse infosüsteemile, mille kaudu paigaldatud lunavara krüpteeris patsientide terviseandmeid sisaldavad failid.

Esimesel juhul arvati esiotsa olevat tegu serveriveaga. Tõde selgus paar päeva hiljem, kui pea 4000 krüpteeritud faili avamise eest nõuti 1,5 *bitcoin*'i (u 3420 eurot) lunaraha. Perearstikeskus teavitas meid juhtunust, samuti informeeriti haigekassat, terviseametit ja politseid.

Lunavararünde tõttu tuli asendada kõvakettad perearstikeskuse serveris, uuesti paigaldada operatsioonisüsteem ja patsientide andmete töötlemiseks kasutatav infosüsteem. Krüpteeritud failid saadi küll kätte, ent neid ei olnud võimalik avada ning andmete varukoopiast taastamine tehnilise vea tõttu ei õnnestunud. Väljapääsmatus olukorras perearstikeskus maksis ründajale lunaraha ja sai dekrüpteerimisvõtmed.

Ka teise juhtumi puhul oli nakatumisteeks serveri kaugligipääs. Failide dekrüpteerimiseks nõuti taas lunaraha *bitcoin*'ides, summa pidi kujunema vastavalt ohvri kontakteerumise kiirusele.

Kaudselt mõjutas juhtum kõiki keskuse perearstide nimistu 4300 patsienti, kelle andmed – väljakirjutatud retseptid, tervisetõendid, digitaalsed tervisekaardid – mõneks päevaks ligipääsetavad polnud. Samuti jäi perearstikeskus ilma vastuvõtule registreerunute nimekirjast. Retseptide väljastamiseks saavutati kokkulepe teise perearstikeskusega, kes aitas probleemi lahendamiseni retsepte väljastada.

Kuna olulisemad failid õnnestus serveris krüpteerimata jäänud varukoopiast taastada, õnnestus piirata ka rünnakust tekkinud kahju. Sugugi alati ei taga lunaraha maksmine andmete tagasisaamist ning riskantne on seegi, et lunaraha maksmine annab ründajale sõnumi ründamise tulususest.

Kivimäe perearstikeskuse perearst Karmen Joller küberrünnaku õppetundidest

Meie õppetund on see, et teeme regulaarselt koopiaid välisele seadmele ja kindlasti eraldame selle pärast koopia tegemist ka arvutist. See on ainus hea lahendus, kuidas ennast kaitsta.

Intsidendi avastamisel võtsime ühendust nii politsei kui ka RIA intsidentide käsitlemise osakonnaga (CERT-EE). Juhised CERTi pöördumiseks sain oma hea küberturbega tegeleva sõbra käest. CERTist ei olnud ma sinnamaani kuulnudki.

Vaja oleks konkreetset juhendit, mida selliste intsidentide korral teha. See info võiks olla kusagil nähtaval kohal – nii nagu kõikjale kleebitakse 112 numbri kleepse.

Koostöö CERTiga oli ülihea. Me olime kogu see 24 tundi peaaegu kogu aeg ühenduses, nad aitasid meid väga palju. Ma ei kujuta ette, kuidas me ilma nendeta hakkama oleksime saanud.

Meie seisukoht on, et selliseid andmeid ei peaks perearstikeskuses füüsiliselt üldse säilitama – see on perearstidele liiga suur vastutus. Enamik perearste ei saa aru, millised riskid võivad kaasneda, kui server pole piisavalt uuendatud või kui varukoopiaid ei tehta. Ja isegi kui nad saavad aru, ei ole neil võimekust ega ressurssi andmeid kvaliteetselt kaitsta. Selleks peaksid olema oma ala asjatundjad. Vaktsineerimist me ju itimeestele ei usalda, miks siis peaks serverite kaitse perearstidele usaldama. Seadusega on küll igasugune andmekaitse ja andmete turvalisus nõutav, aga seaduse täitmisega on palju keerulisemad lood.

Küberturvalisuse seadus

Möödunud aastal majandus- ja kommunikatsiooniministeeriumi ning Riigi Infosüsteemi Ameti eestvedamisel valminud uue küberturvalisuse seaduse eelnõu* eesmärgiks on tugevdada ühiskonna jaoks määrava tähtsusega teenuste turvalisust. Samavõrra sätestab seadus ka ootused riigi ja kohaliku omavalitsuse asutuste töö toimimiseks kasutatavate võrgu- ja infosüsteemidele. Fookus on ennetusel ja tõhusamal reageerimisel, et kahjulikke tagajärgi vähendada ja ära hoida. Eelnõuga võetakse üle ka Euroopa Liidu võrgu- ja infoturbedirektiiv ehk nn NIS direktiiv.**

Mida seadus kaasa toob?

Seadus koondab oluliste teenuste osutajate kohustused võrgu- ja infosüsteemide turvalisuse tagamisel ühte seadusse ja täpsustab neid. Sarnaselt senisega peab teenuseosutaja hindama oma infosüsteemide turvalisust ja teenuse teoimepidevust mõjutavaid küberriske ning nende realiseerumise mõju organisatsioonile ja teenuse kasutajatele. Riskide haldamiseks tuleb kasutusele võtta vajalikud ja piisavad turvameetmed.

Lisaks peab teenuseosutaja tegema seiret oma võrgus ning pidama logisid, mis võimaldaksid tuvastada ja jäädvustada süsteemide tööd ohustavaid turvanõrkusi, manipuleerimiskatseid ja ebakorrapärasusi. Küberintsidendi korral peab olulise teenuse osutaja rakendama vajalikke abinõusid intsidendi mõju ja leviku vähendamiseks.

Seadus kohustab teenuseosutajat teavitama meid olulisest küberintsidendist, mille tunnused määratletakse seaduses – ennekõike on selleks oluline ebasoodus mõju teistele isikutele, nende tervisele ja varale.

---

* Seaduseelnõu 597 SE. Eelnõu läbis Riigikogu esimese lugemise 4. aprillil 2018.

** Euroopa Parlamendi ja nõukogu 6. juuli 2016 direktiiv (EL) 2016/1148.

	Ennetus	Reageerimine
Teenusepakkujad	Riskianalüüs Turvameetmed Süsteemi seire Dokumenteerimine	Intsidentidest teavitamine (RIA, võimalikud ohvrid) Süsteemi kasutuse või juurdepääsu piiramnine
Riigi Infosüsteemi Amet	.ee aadresside seire Ohuteated	Ohuteated ja juhised Õigus nõuda teavet Süsteemi kasutuse või juurdepääsu piiramine (üksnes erijuhud)

Küberturvalisuse seadus kehtestab nõuded teenuseosutajatele ning RIA pädevuse intsidentide ennetamisel ja neile reageerimisel

Vabatahtliku teavitamise võimalus jääb ja seda soosime endiselt, sest just see annab meile parima võimaluse varakult märgata laiemat keskkonda mõjutavate ohtude avaldumist Eestis, avastada varakult ründekampaaniaid ning avalikkust ja ohustatud osalisi – eriti oluliste teenuste osutajaid hoiatada. Samuti saame pakkuda nõu ja abi rünnete ennetamiseks ning abinõude kasutuselevõtmiseks, et olulist mõju vältida.

Riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide turvameetmed

Eelnõuga sätestatud kohustused võrgu- ja infosüsteemide turvalisuse tagamisel ning olulise mõjuga küberintsidentidest teavitamisel laienevad ka riigi ja kohaliku omavalitsuse üksusele. Olemuslikult pole nõuded avaliku sektori asutustele uued, kuivõrd need sisalduvad avaliku sektori asutustele kohalduva infosüsteemide kolmeastmelise etalonturbe süsteemi (ISKE) meetmetes.

Küberturvalisuse tagamise riiklik korraldus

Seni mitme seaduse ja nende rakendusaktidega reguleeritud riiklikud kohustused küberturvalisuse korraldamisel kirjeldatakse eelnõus paremini hoomatava tervikuna. Küberturvalisuse korraldamise keskne roll sätestatakse selgelt RIA-le, kelle pädevus ja ülesanded on määratletud eelnõus järgmiselt:

- koordineerida küberintsidendi ennetamist ja lahendamist seadusega antud piirides
- võtta ennetavaid meetmeid ning tuvastada ohuhinnangute põhjal turvanõrkustega seadmeid ja teenuseid
- edastada küberintsidentide ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

Eelnõu kohaselt määratakse RIA täitma ka NIS direktiivis sätestatud küberintsidentide lahendamise üksuse ülesandeid, sealhulgas tagama intsidentide seiret Eestis; tagama riskide ja intsidentide kohta varajaste hoiatuste andmise ning teabe jagamise partneritega; ja tagama intsidentidele reageerimise ning süsteemse riskide ja intsidentide analüüsi. Täidame ühtse rahvusvahelise kontaktpunkti rolli, kes on vastutav piiriülese koostöö, infovahetuse ja ELi tasandil võetavate meetmete koordineerimise eest.

Meile seadusega pandavate kohustuste täitmine eeldab koostööd partneritega era- ja avalikust sektorist, toimivat infovahetust ning selleks eraldi õigusliku aluse sätestamist. Sellest tulenevalt täpsustab eelnõu intsidentide lahendamise ja seire volitused ning sätestab järelevalvemeetmed avaliku korra kaitseks*, sealhulgas õiguse tõrjuda küberintsidendist tingitud vahetut kõrgendatud ohtu või kõrvaldada korrarikkumine.

Avalikku korda rikkuvate küberintsidentide tõhusamaks lahendamiseks näeb eelnõu meile ette ka õiguse küsida sideettevõtjatelt isikustamata andmeid võrguvoo kohta, mis aitaks tuvastada pahavara jagava seadme ja teha kindlaks ka ründeobjektid. Siinkohal on oluline rõhutada, et tegemist ei ole isikuandmete, vaid süsteeme puudutavate metaandmetega, mis on vajalikud küberintsidendi lahendamiseks.

* Riigi Infosüsteemi Amet täidab erikorrakaitseorgani ülesannet juba praegu ning asutusele laienevad korrakaitseorgani volitused vastavalt korrakaitseseaduses ja eriseadustes sätestatule.

Küberintsidendist tingitud hädaolukorra ennetamine

Lihtsamate ja levinud küberohtude kõrval võib küberintsident ulatuslikult mõjutada ka olulisi ühiskondlikke funktsioone ja teenuseid, milleks peame riigi ja ühiskonnana valmis olema. Hädaolukorra seadusest (HOS) tuleneb RIA-le kohustus koostada küberintsidendi hädaolukorra riskianalüüs. Igas valdkonnas riskianalüüsi koostav asutus pakub välja ohustsenaariumid, mis võivad eskaleeruda hädaolukorraks, ning nende põhjal koostatakse võimeanalüüs, et hinnata riigi valmisolekut hädaolukorra ennetamiseks, hädaolukorraks valmistumiseks ja selle lahendamiseks. Riskianalüüsid on aluseks hädaolukorra lahendamise plaani

Foto: Arno Mikkor

koostamisele ning hädaolukorra ennetamise, valmisoleku ja lahendamise meetmete planeerimisele, samuti asutuste ja riigi tegevusvaru moodustamisele.

Küberintsidendi riskianalüüs hindab nelja tõsisema sündmuse riskistsenaariume: elektroonilise isikutuvastuse teenuse katkemine, riigi toimimiseks oluliste andmete kadumine või muutmine, ulatuslikke elektrikatkestusi põhjustav küberrünnak ja andmesideteenuse katkestused.

Käsitletud stsenaariumide tõenäosus on kõrge ja tagajärjed võivad olla väga rasked. Tõenäosust tõstab asjaolu, et valdkond muutub ja areneb kiirelt, samuti kasvab infosüsteemidest sõltumise määr üha enam. Hädaolukorda Eestis viimastel aastatel aset leidnud ei ole, ent ulatusliku küberintsidendi oht kasvab kogu maailmas ning oskusteave, kuidas rünnata, areneb pidevalt. Meie digitaalne sõltuvus ja sellega kaasnevad riskid on märkimisväärselt suurenenud ning peame neid endale teadvustama. Üha olulisem on tegeleda riigi digitaalse baastaristu küberturvalisuse kaitsmise ja riskide hindamisega. Ehkki rünnete korraldamine on keeruline ning nõuab ressursse ja motivatsiooni, on see võimalik. Kui ründe alla peaksid sattuma e-valimiste, ID-kaardi, X-tee või riiklike registrite usaldusväärsus ja rahvusvaheline maine, tooks see kaasa väga rasked ja kauakestvad tagajärjed.

Riigi valmisolek ennetada ja lahendada küberintsidendist põhjustatud hädaolukorda on viimaste aastate jooksul oluliselt paranenud. Väljakutseks on aga oluliste ametikohtade täitmine ja arusaam riigi oluliste teenuste, infosüsteemide ja andmekogude omavahelistest sõltuvustest.

Küberturvalisuse tagamisse suunatud ressursside maht ei vasta enam valdkonna arengust tulenevatele vajadustele, mistõttu on oluline, et Eesti riik suurendaks investeeringuid nii teadlikkuse tõstmisesse kui infotehnoloogiliste süsteemide arendamisse, testimisse ja turvalisusesse juba teenuste disainimisel.

RIA 2017. aasta küberturvalisuse valdkonna kirjutised

Soovitused ja juhendid

Windows 10 turvajuhend
Soovituslik juhend Microsoft Windows 10 turvaliseks kasutamiseks riigisektoris
https://www.ria.ee/ee/windows-10-juhend.html

Turvaline meilivahetus
Turvaline meilivahetus avalikus sektoris
https://www.ria.ee/public/Kuberturvalisus/Turvaline_meilivahetus_avalikus_sektoris.pdf

Pilveteenused
Soovituslik juhend avalike pilveteenuste turvaliseks kasutamiseks riigisektoris
https://www.ria.ee/public/ISKE/Avalike-pilvede-kasutamise-juhend.pdf

Uuringud ja analüüsid

RIA pädevus küberohtude ennetamisel ja tõrjumisel
Riigi Infosüsteemi Ameti järelevalve meetmed haldusjärelevalve-menetlustes ning häda- ja eriolukorras (Sorainen 2017)
https://www.ria.ee/public/Kuberturvalisus/Oigusanalyys-2017-Sorainen.pdf

Krüptouuring
Krüptograafiliste algoritmide elutsükli uuring 2017
https://www.ria.ee/ee/kruptouuringud.html

RIA blogi

https://blog.ria.ee
Sisaldab pikemaid analüüse ja kirjutisi aktuaalsetel teemadel, sh küberturbest.

CERT-EE tööriistad ja teenused

IRMA – veebipõhine viiruskontrolli tööriist

https://irma.cert.ee/

Tööriist riigiasutuste andmesidevõrgu kasutajatele ja erasektori koostööpartneritele, mõeldud e-kirjaga saabunud kahtlaste manuste ja teiste ebakindla päritoluga failide kontrollimiseks. Tööriista eelis internetis leiduvate samalaadsete ees on, et sisestatud failid ei jää tundmatutesse kohtadesse ripakile, vaid paiknevad Eesti riigiasutuse failiserveris ja neid kustutatakse regulaarselt.

Infoturbeintsidentidest teavitamine

https://raport.cert.ee

Teavituskeskkonna kaudu saab RIA-le edastada teate infoturbeintsidendi kohta. Mõeldud eeskätt asutustele ja teenuseosutajatele detailsema teabe edastamiseks, lihtsa intsidenditeavituse võib saata ka aadressil cert@cert.ee.

Failide edastuskeskkond

https://paste.cert.ee

Tööriist võimaldab saata kahtlased failid CERT-EE-le analüüsimiseks. Sobib õngitsuskirjade ja nendega saabunud manuste, pahavaranäidiste jms edastamiseks.

CERT-EE „liivakast" (*Sandbox*)

http://cuckoo.cert.ee

IT-spetsialistidele mõeldud failide analüüsimise tööriist. Võimaldab turvalises keskkonnas järele kontrollida, kuidas erinevatel virtuaalsetel ja füüsilistel platvormidel töötavad operatsioonisüsteemid kahtlusaluse faili käivitumisel käituvad.

CERT-EE hoiatused ja teated

https://twitter.com/cert_ee

Kõige operatiivsem viis püsida kursis CERT-EE teadete ja hoiatustega.

Kübervaldkonna uudiskiri

https://www.ria.ee/ee/cert-kontakt.html

Iga päev ilmuv kokkuvõte avalikes allikates ilmunud küber- ja IT-uudistest. Listiga saab liituda ametliku e-posti aadressiga (ei sobi Gmail, Hotmail vms).

Kokkuvõte: järeldused ja hinnangud 2018. aastaks

- **Küberintsidentide vastu pole 100% kaitset – turvalisuse määrab valmisolek.** Eesti jaoks möödus 2017. aasta hästi, sest olime teinud tööd – eesistumise ja valimiste turvalisuse, riigi digitaalse alustaristu (ID-kaardi ökosüsteem) vastupidavuse ning ulatuslike intsidentide ennetamise ja nendeks valmisoleku nimel. Mullused pahavarakampaaniad põhjustasid maailmas miljarditesse ulatuvat majanduskahju ning kätkesid endas ka vahetut ohtu inimeste elule ja tervisele. Eestis oli kahju minimaalne; olime ohust sammu ees nii tänu turvapaigatud süsteemidele kui operatiivseirele ja kiirele infoedastusele. Viidatud kampaaniad ei jää aga viimaseks. Meditsiiniseadmete, haiglate, elektrijaamade, lennujaamade ja teiste eluliste teenuste halvamine päädib varem või hiljem inimohvritega. Teadlikkus, valmisolek ja kiire reageerimine määravad selle, kas Eesti saab järgmises laines pihta ning kuivõrd edukalt õnnestub kahjusid minimeerida.

- **Üha enam on tõsiste küberrünnete taga riigid,** kelle jaoks see on lihtsaim viis oma mõjuvõimu kehtestada – mõju on tõhus, kulud madalad, jäljed hägusad ja seoseid eitatakse. Ründed elutähtsate teenuste vastu on püsiv ja igapäevane oht; läänemaailma avatud ühiskondade demokraatlike protsesside õõnestamiseks korraldatud mitmetahulised küber- ja propagandarünnakud pakuvad eriti lihtsat võimalust riikide poliitikat mõjutada. Eestis on kõrge usaldus e-valimiste ehk internetipõhise hääletamise vastu ning oskused ja aastatepikkune kogemus valimiste küberturvalisuse tagamisel, mida jagame ka partneritega. Juhime Euroopa Liidus koostööd, mille tulemusena koostatakse soovitused valimiste küberturbe korraldamiseks.

- **Ründeid korraldavate riikide käitumise muutmiseks tuleb tekitada sellisele tegevusele poliitiline ja majanduslik hind.** Järjest varjamatumate ja agressiivsemate riiklike küberrünnete tõkestamiseks tuleb demokraatlikel riikidel ehitada üles usutav heidutus, mis ennekõike saab tekkida samameelsete riikide tõhusa koostöö abil. Üks heidutuse vahendeid on avalikult või diplomaatiliste kanalite kaudu selgelt välja öelda, et ründaja on tuvastatav ja tuvastatud, ent rünnete omistamisega peab kaasnema tegelikku poliitilist ja majanduslikku mõju omavate meetmete kasutamine, mis muudaks ründeid korraldavate riikide kalkulatsiooni.

  Eesti eesistumise ajal töötati Euroopa Liidus välja diplomaatiliste meetmete pakett, mida rakendada küberrünnete korral. See võimaldab küberründele vastata kõigi Euroopa Liidu ühise välispoliitika meetmetega diplomaatilistest sammudest kuni majandussanktsioonideni välja, ja nende vastumeetmetega peavad arvestama nii küberründeid korraldavad riigid kui ka need, kes ründeid oma tegevuse või tegevusetusega toetavad.

- **Küberründe oht ei sõltu sellest, kas sinu andmed on väärtuslikud kurjategijale, vaid sellest, kas nad on väärtuslikud sinule.** Enamik küberründeid ei pööra mingit tähelepanu kasutaja isikule, vaid sihivad valimatult kõiki kaitsmata seadmeid ja kasutajakontosid. Lõviosa Eestis juhtunud küberintsidentide puhul kehtib tõdemus, et kahju saanuks vältida, hoides tarkvara uuendatuna, säilitades olulistest andmetest varukoopiaid ning piirates hoolsamalt juurdepääsu oma andmetele ja seadmetele. Teisalt on küberkurjategijad üha professionaalsemad: ehkki jätkuvalt saadetakse ka lihtsakoelisi petu- ja õngitsuskirju, näevad ründajad piisava tuluväljavaate korral vaeva usutavuse nimel. Eluterve skepsis ja detailidesse süvenemine aitab sellistest juhtumitest tekkida võivat kahju oluliselt vähendada. Kui sinu andmed on sulle või sinu ärile olulised, siis kaitse neid!

- **Riigiasutuste küberturvalisuse parandamiseks sõnadest ei piisa.** Riigiasutused on kogu maailmas küberrünnete sihtmärkide tipus. Eesti ametnike küberhügieen on hea, aga riigiasutuste intsidendid näitavad, et võimalused küberturvalisust teadlikkuse tõstmisega parandada on ammendunud ning keskenduda tuleb turvalisele arhitektuurile, investeerida nõuete täitmisse ja tagada infoturbekompetentsi olemasolu asutustes. Muret tekitab piiratud infoturbevõimekusega riigiasutuste ja enamiku kohalike omavalitsuste küberturvalisuse korraldus. Riik peab küberturvalisuse korraldamisel püüdlema tervikuna suurema tsentraliseerimise poole.

- **Turvalisus ei ole staatiline.** Turvanõrkused laialdaselt kasutatavas tehnoloogias ei ole ühekordne šokk, vaid keskkonnale iseloomulik, ja selge on, et ilmnenud nõrkusi püütakse ära kasutada. Turvalisus ei lõpe infosüsteemi valmimise või seadme soetamisega, selle hoidmine tähendab järjepidevat tööd ning esmavastutus oma seadme või süsteemi turvalisuse eest on omanikul endal. Tõhus küberkaitse saab olla ainult totaalkaitse – sellesse peab panustama igaüks.

- **Küberturvalisuse seadus toob suurema õigusselguse, ent seadus ei lahenda kõiki haavatavate valdkondade muresid.** Uus küberturvalisuse seadus korrastab rollid, mõisted ja vastutuse Eesti küberturvalisuse korraldamisel, ent seaduse rakendamise kõrval jääb oluliseks tihe partnerlus riigi- ja erasektori asutustega. Samas on eelnõu menetlus toonud esile mitmed riskid, mis vajavad tähelepanu, nagu näiteks rahvusringhäälingu küberturve või oluliste teenuste sõltuvus seaduse kohaldamisalast välja jäävatest teenuseosutajatest ning piiriülestest sõltuvustest tulenevad riskid.

- Iseäranis **tervishoiuvaldkonna küberturvalisus vajab tõhusamat tuge.** Olukorras, kus haiglad ja perearstikeskused töötlevad meie kõigi delikaatseid isikuandmeid ja nende töö sõltub suurel määral digitaalsete süsteemide toimimisest, ei tohi neid jätta olukorda, kus küberturvalisus konkureerib ressursi pärast tervishoiuteenuse osutamisega. RIA jätkab tervishoiuasutuste nõustamise ja töötajate koolitustega. Samas on vajalik, et küberturvalisusele pööraks tähelepanu ka asutuste juhtkonnad ning seonduvaid riske maandataks, olgu terviklike teenuste sisseostmise või asutuste küberturbe kompetentsi arendamise abil.

Viited

1 https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf; https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf; https://www.infopoint-security.de/open_downloads/Trustwave_Global_Security_Report_2016.pdf

2 https://crocs.fi.muni.cz/

3 https://www.infineon.com/TPM-update; https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV170012; https://safenet.gemalto.com/technical-support/security-updates/; https://www.yubico.com/support/security-advisories/ysa-2017-01/.

4 https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf

5 https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52017JC0450&from=en

6 https://www.ria.ee/ee/riik-tugevdab-it-alast-koostood-teadus-ja-eraettevotetega.html

7 https://www.eu2017.ee/et/political-meetings/kuberturvalisuse-konverents

8 https://www.technologyreview.com/s/608561/first-evidence-that-social-bots-play-a-major-role-in-spreading-fake-news/

9 https://www.us-cert.gov/ncas/alerts/TA16-336A

10 https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

11 https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

12 https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/BotNets/botnets_node.html

13 https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs; https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack; https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/how-to-protect-yourself-from-the-global-ransomware-attack/?utm_term=.1de68a198290; http://www.reuters.com/article/us-renault-cybercrime-idUSKBN1890AK

14 https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

15 https://blogs.technet.microsoft.com/mmpc/2017/06/29/windows-10-platform-resilience-against-the-petya-ransomware-attack/

16 https://www.bleepingcomputer.com/news/security/fedex-says-some-damage-from-notpetya-ransomware-may-be-permanent/

17 https://www.maerskline.com/news/2017/07/25/25th-july-global-update; http://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/; https://www.europol.europa.eu/iocta/2017/index.html

18 http://securityaffairs.co/wordpress/61580/malware/notpetya-disrupted-merck-operations.html; http://www.darkreading.com/attacks-breaches/ransomware-attack-on-merck-caused-widespread-disruption-to-operations/d/d-id/1329503
19 https://www.ft.com/content/f6bc770e-064e-340d-949e-64d2a81216d5
20 https://nakedsecurity.sophos.com/2017/11/15/shadow-brokers-cause-ongoing-headache-for-nsa/ https://www.theregister.co.uk/2017/04/14/latest_shadow_brokers_data_dump/; https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/
21 https://blogs.windows.com/windowsexperience/2017/06/28/announcing-windows-10-insider-preview-build-16232-pc-build-15228-mobile/#r8Gmb6yu3id5ZlQq.97
22 https://majandus24.postimees.ee/4160147/ehituse-abc-sulges-kuberrunnaku-tottu-koik-oma-poed
23 http://arileht.delfi.ee/news/uudised/kantar-emor-sulges-kuberrunnaku-tottu-arvutisusteemid?id=78706774
24 https://blog.ria.ee/kas-tahad-nutta/
25 https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group
26 http://securityaffairs.co/wordpress/64834/malware/north-korea-wannacry-attack.html; http://www.independent.co.uk/news/world/asia/north-korea-responsible-wannacry-ransomware-microsoft-brad-smith-cyber-attack-nsa-a8000166.html
27 https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
28 https://threatpost.com/researchers-find-blackenergy-apt-links-in-expetr-code/126662/
29 http://www.theregister.co.uk/2017/07/04/sbu_claims_russia_was_behind_notpetya/
30 https://www.scmagazine.com/cisco-talos-notpetya-analysis-attacker-could-launch-again/article/673392/
31 https://www.wired.com/story/white-house-russia-notpetya-attribution/
32 http://vm.ee/et/uudised/valisminister-moistab-hukka-venemaa-kuberrunde-notpetya-ukraina-vastu
33 https://gizmodo.com/gop-data-firm-accidentally-leaks-personal-details-of-ne-1796211612?rev=1497834806031
34 https://www.ria.ee/public/Kuberturvalisus/RIA-KTT-kokkuvote-juuli-2017.pdf
35 http://www.theregister.co.uk/2018/01/17/no_one_uses_two_factor_authentication/
36 https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118
37 https://www.ria.ee/ee/tumeveebis-avaldati-14-miljardi-kasutaja-paroolide-seas-ka-eesti-inimeste-paroolid.html
38 http://www.cambridge.org/us/academic/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition

39 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
40 https://svenska.yle.fi/artikel/2017/09/15/overbelastningsattack-mot-alcom
41 https://www.reuters.com/article/us-russia-nato/russia-may-have-tested-cyber-warfare-on-latvia-western-officials-say-idUSKBN1CA142
42 https://www.nrk.no/finnmark/e-tjenesten-bekrefter_-russerne-jammet-gps-signaler-bevisst-1.13721504
43 http://uk.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6
44 https://www.theguardian.com/technology/2017/jul/18/energy-sector-compromised-state-hackers-leaked-gchq-memo-uk-national-cybersecurity-centre
45 https://www.wsj.com/articles/cyber-attacks-on-international-banks-show-links-to-hackers-who-hit-sony-1486918801
46 https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/; https://www.bleepingcomputer.com/news/security/polish-banks-infected-with-malware-hosted-on-their-own-governments-site/
47 https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies; https://www.scmagazine.com/union-bank-of-india-cyberattacked-similar-to-bangladesh-heist/article/649857/
48 https://www.dni.gov/files/documents/ICA_2017_01.pdf
49 http://www.reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ
50 http://edition.cnn.com/2017/04/24/europe/france-macron-hackers/index.html
51 https://euobserver.com/foreign/136474; http://www.france24.com/en/20170114-france-vulnerable-cyber-attacks-hacking-presidential-elections; http://www.pcworld.com/article/3158165/software-social/facebook-launches-fake-news-reporting-tool-in-germany.html
52 http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
53 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
54 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03140USEN&; http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/
55 http://www.delfi.ee/news/paevauudised/eesti/kogu-laane-tallinna-keskhaigla-arvutivork-utles-ules-patsiendid-jaid-hatta?id=77088768