Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte

Sisukord

Küberturvalisus sõltub meist kõigist

Tänavu aprillis möödub kümme aastat Eestit 2007. aastal tabanud küberrünnakutest. Rünnete suhteliselt lihtsast iseloomust ja piiratud tagajärgedest hoolimata osutus nende mõju suuremaks, kui keegi tol ajal arvata oleks osanud. Esimest korda tekkis avalik arutelu küberrünnete mõjust riikide julgeolekule, küsimus kübersõja klassifitseerimisest sõjategevuse liigina ning mis kõige olulisem – avalikkus hakkas aru saama, et „bittide ja baitide" kasutamine rünneteks kübermaailmas toob kaasa mõju igapäevasele elule füüsilises keskkonnas: ei saa lugeda uudiseid, ei tööta internetipank või puudub juurdepääs tavapäraseks kommunikatsioonivahendiks saanud sotsiaalmeediakanalitele. Eestile tõid ründed kaasa ka aina kasvava kuulsuse arenenud e-riigina ning küberturvalisuse valdkonnas peetakse meid üheks maailma juhtriigiks.

Kümme aastat hiljem on selge, et Eesti küberturvalisuse valdkonna arendamisel tehtud otsused on üldjoontes olnud õiged. Praegust küberturvalisust kindlustavad toimiv e-riigi taristu, usaldusväärne digitaalne identiteet, kõikidele riigiasutustele rakendamiseks kohustuslik turvameetmete süsteem, keskne küberturbeintsidentide seire, lahendamise ja raporteerimise süsteem. Kõige olulisemaks on tõenäoliselt ühine arusaam, et küberturvalisust on võimalik tagada vaid koostööga ning selleks on vaja kõikide – riigi, ettevõtjate ja üksikisikute – ühist panust. 2007. aasta sündmused lahenesid koostöös: nii riigi kui eraettevõtete infoturbeekspertidest koosnev „kollektiivne aju" suutis ühiselt kiiresti tõrjuda ründekatsed ning aitas järgmisteks aastateks välja töötada tegevusplaani, mida oleme saanud järgida siiani.

Küberturvalisust ei saa tagada riik üksi. See oleks võimatu isegi suurimate riikide jaoks sel lihtsal põhjusel, et internet ei kuulu riikidele. Küberturvalisuse tagamise edukus sõltub niihästi sellest, kui hästi suudavad riigid omavahel koostööd teha, kui ka riikide koostööst internetis teenuseid pakkuvate ettevõtjate ja organisatsioonidega, kes interneti toimimist korraldavad.

Sel aastal saab läbi Eesti 2014–2017 küberjulgeoleku strateegia rakendusperiood. Praegune küberjulgeolekustrateegia oli Eestile juba teine valdkonnastrateegia. Küberjulgeolek on nüüdseks muutunud meie jaoks enesestmõistetavaks. Eestis pole kümme aastat juhtunud ühtki sellist küberintsidenti, mis

oleks ühiskonna igapäevaelu oluliselt häirinud.

Ometi sõltub Eesti riigi ja ühiskonna toimimine küberturvalisusest rohkem kui eales varem. Halvenenud rahvusvaheline julgeolekuolukord on suurendanud välisriikide eriteenistuste aktiivsust nii küberspionaaži kui ka küberrünnete ettevalmistamise valdkonnas. Eesti riigiasutuste andmesidevõrke skaneeritakse ja kaardistatakse pidevalt, kontrollitakse meie kommunikatsioonivahendite võimekust ja üritatakse lisaks riigiasutustele tungida ka elutähtsaid teenuseid pakkuvate ettevõtete arvutivõrkudesse. Igapäevast turvalisust seavad aga veel rohkem ohtu küberkurjategijate ründed: krüptolunavara levitamisega kasumit teenida lootev organiseeritud kuritegevus seab oma tegevusega ohtu isegi inimeste elu ja tervise. Sagedased rünnakud haiglatele põhjustavad halvemal juhul isegi arstiabi andmise katkemise. Selliste rünnakute vastu ei piisa ei parimatest infotehnoloogiavahenditest ega kõige pädevamast küberturvalisust tagavast meeskonnast. Sellised ründed saavad õnnestuda vaid siis, kui ründajatel õnnestub leida arvuti- või nutiseadme kasutaja, kes pole riskidest teadlik või on hooletu.

Küberturvalisus sõltub meist kõigist. Oskus küberruumis turvaliselt toimetada ja riske õigesti hinnata võimaldab tagada küberjulgeoleku nii isiku, ühiskonna kui ka riigi plaanis. Tõhus küberkaitse saab olla ainult totaalkaitse – sellesse peab panustama igaüks. Loodetavasti leiab iga lugeja siit mõne hea mõtte, kuidas enda, oma organisatsiooni ja kogu ühiskonna küberturvalisust parandada.

Toomas Vaks
Riigi Infosüsteemi Ameti peadirektori
asetäitja küberturvalisuse alal

Küberturvalisuse ohuhinnang. 2016. aasta Eesti ja rahvusvahelises küberruumis

Sissejuhatus

Küberruum kannab üha olulisemat osa nii üksikisikute, ettevõtjate kui ka vabaühenduste siseste ja vaheliste suhete toimimises. Kuna põhiõigusi ja -vabadusi ei ole võimalik realiseerida lahus keskkonnast, kus toimitakse, mõjutab IT-süsteemide turvaline ja häireteta töötamine nii üksikisikute võimalusi oma õiguste ja vabaduste teostamiseks kui ka tervikuna ettevõtluskeskkonna ja kodanikuühiskonna toimimist. Sellest tulenevalt on riigi digitaalse keskkonna turvalisus saanud osaks riigi julgeolekust.

Rahvusvahelises küberruumis toimuv on üha mitmekihilisem ja keerukam ning küberohtude mõju on raske piiritleda selgete valdkondade või toimijatega. 2016. aasta läheb ajalukku mitme pretsedenditu kübersündmusega maailmas. Nägime, kuidas küberruumi kaudu püüdis üks riik mõjutada teise riigi valimisprotsessi ning kuidas tööstusjuhtimisseadmete manipuleerimisega põhjustati elektrikatkestusi. Nägime niinimetatud asjade interneti – internetti ühendatud seadmete – ärakasutamist interneti baasteenuste ründamiseks, mille mõju ületas nii riikide kui kontinentide piire.

Eesti ei ole rahvusvahelises keskkonnas toimuvale immuunne ning pole põhjust oodata, et küberruumis kujunevad üleilmsed suundumused meist mööda lähevad. Samas on Eestil küberkeskkonnas spetsiifilised tugevused, haavatavused ja huvid, mis tulenevad meie valikutest e-riigi arendamisel ning rollist, mida info- ja kommunikatsioonitehnoloogia ühiskonna toimimises kannab. Seetõttu räägime seekordses Riigi Infosüsteemi Ameti (RIA) küberturvalisuse teenistuse (KTT) aastakokkuvõttes nii Eestis kui maailmas aset leidnud sündmustest ja kujunevatest suundumustest, mis olulised Eesti elaniku

ja riigi küberturvalisuse jaoks. Eesmärgiks on anda Eesti lugejale arusaam, mis meid küberkeskkonnas ohustab, missuguste riskidega peame arvestama ja kuidas end paremini kaitsta.

Nagu küberturvalisus on igaühe asi, nii on ka RIA küberturvalisuse aastakokkuvõte mõeldud Eesti avalikkusele kõige laiemas mõttes. Mõned digitaalse keskkonna riskid puudutavad ühtviisi iga arvutikasutajat, mõnega peavad iseäranis arvestama teatud valdkonnas või erialal tegutsejad. Oleme kokkuvõttes siiski hoidunud välja valimast üksnes üldhuvitavaid või „spetsialistiteemasid" – küberturvalisus ongi just nii läbipõimunud ja mitmekülgne väljakutse, nagu siin kajastatud teemadest nähtub. Väljaanne on seetõttu mõeldud pakkuma mõtteainet nii eraisikule kui avaliku sektori asutuse, ettevõtja ja vabaühenduse töötajale, juhile ja IT-spetsialistile, et olla riskidest teadlik ning astuda samme oma turvalisuse parandamiseks.

Seekordne RIA küberturvalisuse aastakokkuvõte jaguneb kahte ossa. Esimene keskendub Eesti küberturvalisuse ohuhinnangule, kus räägime mullustest küberintsidentidest ning ohtudest ja haavatavustest, mis Eestit praegu ohustavad. Teises osas teeme kokkuvõtte RIA 2016. aasta peamistest tegevustest Eesti küberturvalisuse suurendamisel, mida ohuhinnang ei kajasta.

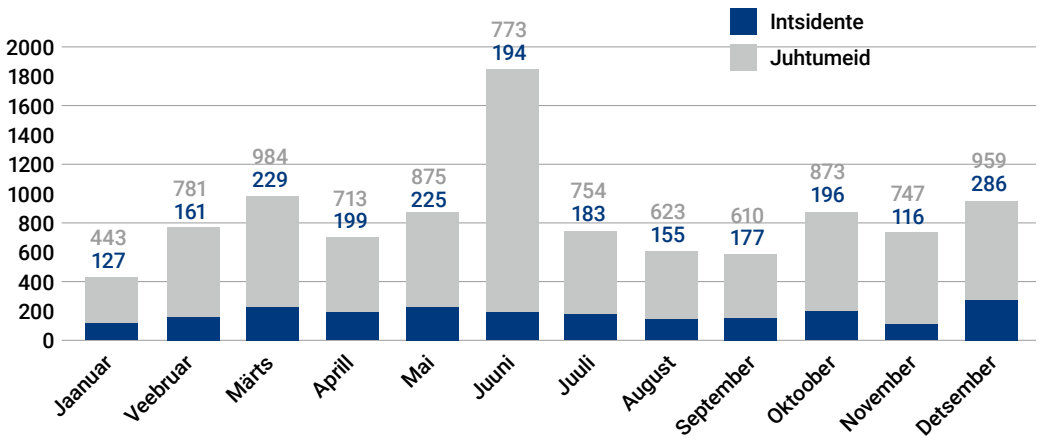
Sündmused Eesti küberruumis 2016

2016. aastal käsitles RIA infoturbeintsidentide käsitlemise osakond CERT-EE Eesti arvuti- ja andmesidevõrkudes 9135 juhtumit. Neist küberturbeintsidendina – see tähendab juhtumina, millega kaasnes otsene mõju teabe või süsteemide konfidentsiaalsusele, terviklusele või kättesaadavusele – tuvastati 2248 juhtumit ehk ligikaudu neljandik.

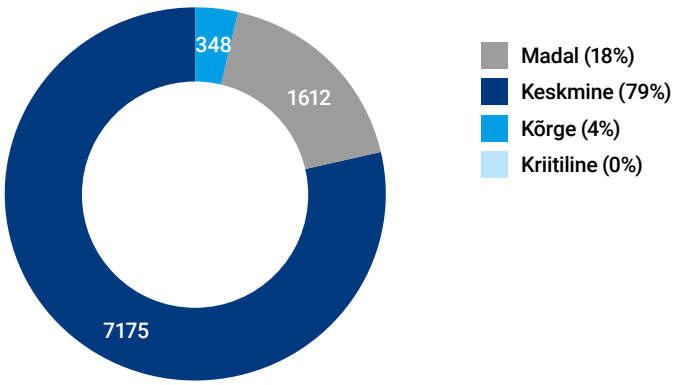
RIAni jõuab teave küberturbejuhtumitest kahel viisil: neist teavitavad partnerasutused või puudutatud isikud, või tuvastab CERT-EE need seire käigus kui võimaliku küberintsidendi.

Ühtegi kriitilist küberintsidenti, millega oleks kaasnenud oht inimeste elule ja tervisele, aasta jooksul ei registreeritud. Küll oli aasta vältel 348 kõrge prioriteediga intsidenti, mis mõjutasid riigile olulise teenuse või lehe toimimist. Siia alla loetakse ka katkestused elutähtsa teenuse osutaja infosüsteemi toimimises või ründed nende vastu. Kõrge prioriteediga juhtumitele reageerib RIA otsekohe, sest intsident vajab lahendamist või rünne peatamist vahel minutite jooksul.

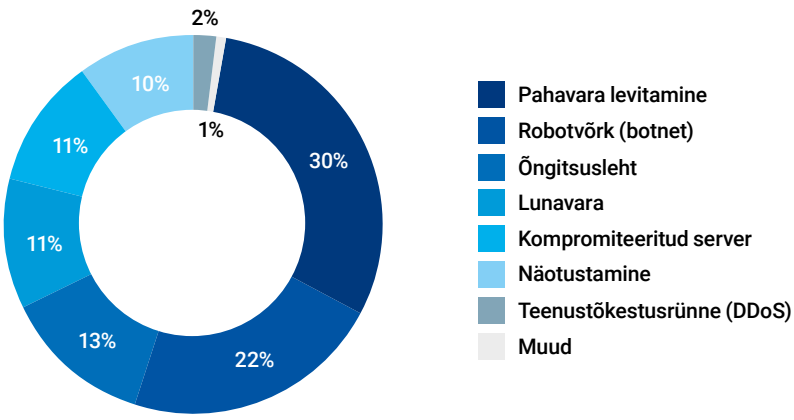
Laekunud juhtumid aasta lõikes



Juhtumite prioriteetsus aasta kokkuvõttes



2016. aastal registreeritud küberturbeintsidentide osakaalud liigiti



Levinumad küberohud

Eesti elaniku ja riigi jaoks on olulisemateks küberohtudeks endiselt küberkuritegevus ning vaenulike välisriikide mõjutustegevus küberruumi kaudu. Globaalse küberkuritegevuse jaoks on iga internetti ühenduva seadme kasutaja potentsiaalselt huvipakkuv sihtmärk, olgu siis võimaluse tõttu temalt raha välja petta või kasutada tema seadet hüppelauana teiste isikute või ühenduste ründamiseks. Arvutikasutajate teadmatus või hooletus kombineerituna teenuse või asutuse turvanõrkustega põhjustavad rahas mõõdetavat kahju, aga võivad ka luua võimaluse nii elutähtsate teenuste kui ka demokraatliku riigikorralduse ründamiseks.

Suurima osakaalu 2016. aastal Eestis registreeritud küberturbeintsidentide seast moodustasid pahavara levitavad e-kirjad ja veebidomeenid. Järgnesid teavitused nakatunud ja robotvõrku hõivatud seadmetest sidevõrkudes, ning enam-vähem võrdse osakaaluga õngitsemisjuhtumid ja lunavaraintsidendid ning kompromiteeritud seadmete ja veebilehtede näotustamisega seotud juhtumid. Endiselt on suur osa intsidentidest otse või kaudselt põhjustatud aegunud tarkvara kasutamisest. Samuti väärivad eraldi käsitlust arenevate tehnoloogiate ja teenustega seotud ohud – möödunud aasta suundumuste põhjal on ilmne, et need annavad edaspidi üha enam kõneainet.

Lunavaraohud on üha oskuslikumad ning ohustavad elutähtsaid teenuseid

Üheks 2016. aastal enim kõneainet andnud küberohuks nii Eestis kui mujal maailmas oli e-kirjade ja veebilehtede vahendusel leviv lunavara. Tüüpiline lunavara levitav e-kiri oli saadetud ühele konkreetsele adressaadile, enamasti korrektselt kirjutatud ning sellele oli manusena lisatud kas arve, CV või muu

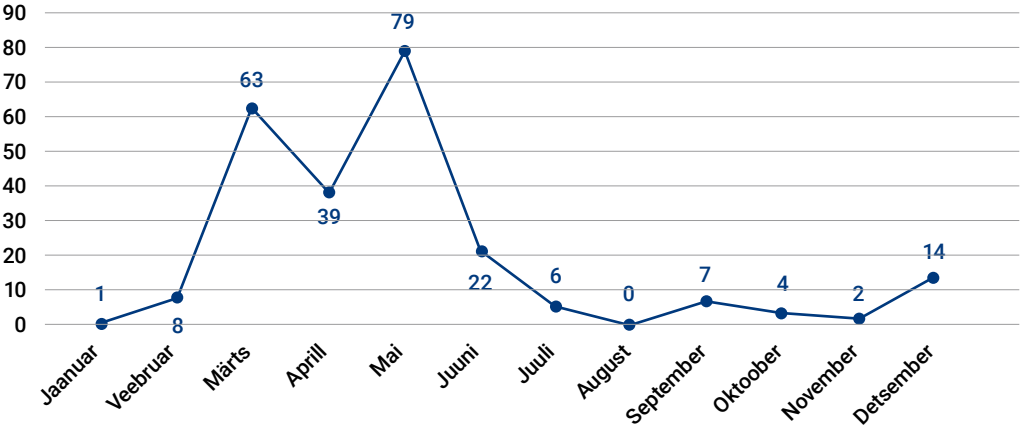
MIS ON *BOTNET* JA MIKS SELLEGA TEGELETAKSE?

Viiendiku 2016. aastal tegelemist vajanud küberturbeintsidentidest moodustasid robotvõrkude ehk *botnet*'idega seotud sündmused. Robotvõrk on enamasti kasutaja teadmata ülevõetud arvutitest ehk zombidest koosnev arvutivõrk, mida kasutatakse koordineeritud küberrünnete toimepanemiseks – näiteks rämpsposti saatmiseks või teenusetõkestusrünneteks.*

Info selliste küberrünnete taristuna kasutatavate seadmete kohta jõuab RIAni nii teiste riikide partnerasutuste teavituste kui ka järjest paremaks muutunud seirevõimaluste kaudu. Ründajate ülevõetud seadmetest lõviosa moodustavad korralikult uuendamata ja turvapaikamata seadmed. Selliste seadmete tuvastamisel saadetakse koostöös internetiteenuse pakkujatega seadmete omanikule teavitus vajadusest ülevõetud seade uuesti oma kontrolli alla saada, et välistada ründe jätkumine.

* Vt ka http://akit.cyber.ee/term/118-botnet-2.

CERT-EE registreeritud lunavaraintsidendid Eestis 2016



pealtnäha ehtne dokument. Oli juhtumeid, kus seesuguse kirja oli näiliselt saatnud legitiimne asutus – näiteks maksu- ja tolliamet –, kasutades ära teenuseid, mis võimaldavad saatja andmete võltsimist.

Lunavara sisaldava manuse avamisel käivitunud fail krüpteeris arvutis asuvad failid ning võrgukettale juurdepääsu korral ka viimase, misjärel arvutikasutajale anti juhised lunaraha maksmiseks, et saada andmete lahtikrüpteerimiseks vajalik võti. Tähtajaks tasumata jätmise korral ähvardas andmete loetamatuks jäämine. Kui andmetest polnud varukoopiat, oli kasutaja seega valiku ees: maksta kurjategijatele või jääda oma andmetest ilma.

Lunavarajuhtumite kõrgaeg Eestis jäi kevadesse, ent lainetena levisid selle erinevad variandid aasta lõpuni, jätkudes praegugi.

Lunavara levitajaks on sageli „elukutselised" kurjategijad ning kuna nende tulu sõltub nende töö professionaalsusest, on lunavara sisaldavad e-kirjad tihtipeale hästi koostatud, need mõjuvad legitiimsena ning kirja saatja kasutab ära organisatsiooni tavapäraste tööprotsesside toimimist – näiteks arvete saatmist meilitsi. Viirustõrjest möödapääsemiseks töötatakse lunavarast välja uusi versioone. Neil põhjustel ei ole lunavaraga nakatumist võimalik alati vältida. Seda enam on oluline, et kasutaja oleks lunavaraohtudest teadlik ning käituks vastutustundlikult nii isiklikke kui tööseadmeid kasutades.

Samuti on möödapääsmatu asutuse arukas IT-haldus ja administreerimispoliitika ning varukoopiate tegemine, eriti kui andmete kättesaadavusest sõltub organisatsiooni põhiülesannete täitmine või elutähtsa teenuse toimimine. Möödunud aastast võib paraku tuua mitmeid näiteid, kuidas administreerimisvead võimendasid lunavaranakkusi organisatsiooni tasemel. Mitmel juhul levis nakkus kasutaja tööjaama kaudu terve asutuse infosüsteemi, kuna arvutikasutajatele olid antud põhjendamatult ulatuslikud kasutajaõigused.

Eriti ohtlikuks tuleb pidada ründeid, kus sihikule on võetud kõrge kriitilisusega ehk elutähtsad teenused, nagu tervishoid või energiavarustus. Sageli on sellised teenused ka oluliselt sõltuvad aegkriitiliste andmete kättesaadavusest, mistõttu kurjategijad panustavad tõenäosusele sealt ründe õnnestumise korral lunaraha hõlpsasti kätte saada ja pingutavad seega ründe õnnestumise nimel. Näiteks võib lunavara levitamiseks kasutatav e-kiri olla loodud võimalikult usutavalt just konkreetset asutust silmas pidades. Elutähtsa teenuse osutajaid puudutanud lunavaranakkusi oli Eestis aasta jooksul kaksteist. Tavapäraselt on selliste rünnete eesmärgiks kriminaalne tulu, kuid vajadusel saab neid kasutada ka riigi julgeoleku kahjustamiseks.

JÄRELDUSED

- Teadlikkus krüptolunavarast on tõusnud; sellele on kaasa aidanud ka CERT-EE vahetu teavitustöö ja meediakajastus. Samas kehtib inimliku mugavuse ja uudishimu jäävuse seadus endiselt ning selle muutmine nõuab pidevat tööd.
- Organisatsioonide IT-personali teadmised ennetamise ja kahjude minimeerimise vallas on tõusnud. Siiski teeb muret korduvate intsidentide muster, eriti tervishoiuasutustes. Ühetaoliste intsidentide kordumine viitab, et organisatsiooni juhtkond ei teadvusta piisavalt töötajate tegevuses rutiinselt ette tulevaid riske ning nende tegelikku mõju organisatsiooni osutatavatele teenustele.

RIA SOOVITUSED

Arvutikasutajale

- Ära ava manuseid ja linke, mille usaldusväärsuses sa kindel ei ole. Pöördu IT-spetsialisti või organisatsiooni kasutajatoe poole, kus see on olemas. Kahtlane e-kiri edasta koos päiste ja manusega aadressile cert@cert.ee (või laadi üles https://paste.cert.ee) ning kustuta kiri ise kohe.
- Ära maksa lunaraha, see toetab vaid kuritegevust ega garanteeri failide tagasisaamist. Kui lahendust failide taastamiseks veel ei ole, hoia nakatunud kõvaketas siiski alles: üldjuhul taastamisvõimalus varem või hiljem tekib.
- Parim kaitse lunavara vastu on tagavarakoopia. Kui sa ise ei oska oma arvutist või nutiseadmest tagavarakoopiat teha, pöördu asutuse IT-toe või tuttava IT-spetsialisti poole.

Asutuse IT-juhile

- Väldi vananenud tarkvara kasutamist ja uuenda viirustõrjet regulaarselt.
- Segmenteeri võrgukettad; anna kasutajale vaid põhjendatud juurdepääsuõigused.
- Korralda andmete regulaarne varundamine – soovitavalt selliselt, et ajakohane ja sõltumatult säilitatav varukoopia oleks hoitud vähemalt kolmes eksemplaris ja vähemalt kahes erinevas tehnoloogias ning vähemalt üks koopia asuks füüsiliselt teises asukohas.

Organisatsiooni juhtkonnale

- Teadvusta küberohtude mõju oma organisatsiooni põhitegevusele ja pakutavate teenuste osutamisele. Tööta riskide maandamiseks välja asutuse küberturbepoliitika.

Loe lisaks: https://blog.ria.ee/lunavarajuhtumi-ennetamine/

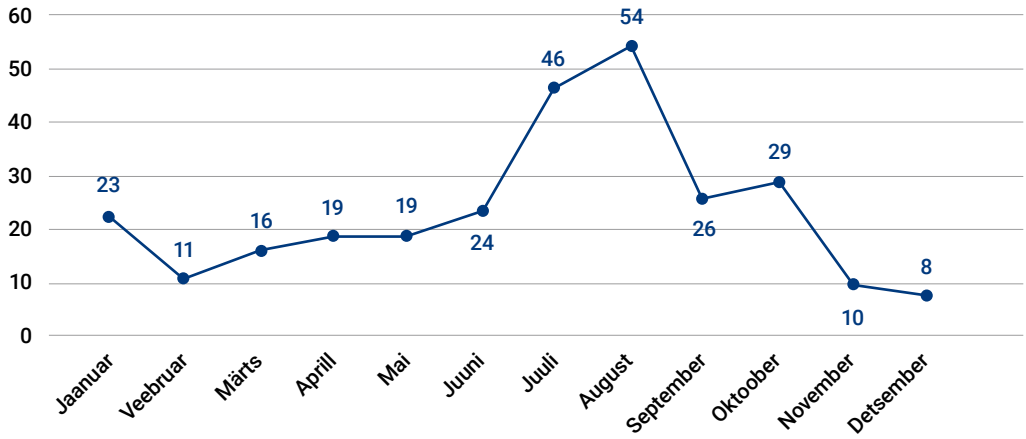
Õngitsetakse nii raha kui tundlikke andmeid

Aasta-aastalt on küberohtude seas üheks enimlevinuks õngitsuskampaaniad, kus e-kirjaga püütakse eri ettekäänetel suunata kasutajat sisestama oma e-posti konto, internetimakse või muu teenuse andmeid legitiimseid jäljendavatele veebilehtedele. Seesuguse sisuga õngitsusteateid levib ka sotsiaalmeedia, eeskätt Facebooki kaudu.

Kui varematel aastatel on andmeid püüdvad kirjad tihti olnud sisult väheusutavad, arvukate õigekirjavigadega ja seetõttu kergesti äratuntavad – ning kasutajate teadlikkus selliste üleskutsete eiramiseks on nüüdseks üsna hea –, on üha enam hästi viimistletud manipuleerimisründeid (nn *social engineering*), kus pingutatakse saatja usaldusväärsena mõjumise nimel ning mängitakse otseselt kasutaja uudishimule, hirmule või kaastundele. Nii saadetakse kasutajale teenusepakkuja nimel libahoiatuskirju kontolimiidi ületamise kohta või kuvatakse talle Facebookis teade, et sõber on postitanud teda kuvava pildi või video. Muster on kõigil juhtudel üks: ühel või teisel ettekäändel suunatakse kasutaja libaveebilehele, kuhu sisestatud kasutajanimi ja salasõna satuvad kurjategijate kätte.

Et veenvamalt mõjuda, saadetakse selliseid kirju ka Eesti teenusepakkujate nimel. Praktikast on tuua näiteid, kus konto blokeerimise eest hoiatavas libakirjas esineti Eesti sideteenuse osutajana. Läbimõeldud ja sihitud kampaania näiteks oli ka juhtum möödunud aasta juunist, kus õngitsuskirju saadeti maksu- ja tolliameti nimel. Kirjade adressaadid suunati ameti veebilehte jäljendavale lehele, kuhu soovitati „enammakstud maksu tagasisaamiseks" sisestada krediitkaardiandmed. Teadaolevalt ükski adressaat selle konkreetse üleskutse õnge ei läinud, ent RIA-le igal kuul saadetud teated edukaks osutunud õngitsemiskatsetest näitavad, et kasutajatel ei ole tihtipeale lihtne libakirja ära tunda.

Õngitsuslehtede ja -kirjadega seotud intsidendid 2016



Õngitsuslehed ise, kuhu kasutaja suunatakse, asuvad enamasti väljaspool Eestit. CERT-EE on teinud partnerite ja Eesti teenusepakkujatega pidevat koostööd õngitsemislehtede kiireks avastamiseks ja eemaldamiseks ning selle tulemusel on Eesti elanikele suunatud õngitsemine teinud läbi märkimisväärse languse.

Suunatud ja professionaalselt viimistletud petukirjad, mis koostatud konkreetse isiku sidemeid ja eeldatavat käitumismustrit arvestades, ringlesid septembris avaliku sektori ja valitsusasutuste seas, mõned ka erasektoris. Kirjad olid saadetud riigiasutuste peadirektorite ja ka peaministri nimel asutuste raamatupidajatele ning nendega üritati välja petta kuni 35 000-euroseid rahaülekandeid. Teadaolevalt ühtegi reaalset rahaülekannet avalikus sektoris ei tehtud, erasektoris selliseid juhtumeid siiski oli.

Endiselt ei ole kuhugi kadunud ka käisin-reisil-kaotasin-dokumendid-saada-raha-tüüpi kirjad, mis saadetud kurjategijate poolt ülevõetud e-posti kontolt isiku tuttavatele.

Kõikvõimalike õngitsemisrünnete motiiviks on enamikul juhtudest kriminaalne tulu, aga mitte ainult – ligipääsu püütakse saada ka rahalist väärtust omavatele või tundlikele andmetele, või ka saada juurdepääsu isikutele, kellelt edaspidi on lootust varastada potentsiaalselt huvipakkuvat teavet. Sellise motiivi näitena võib oletada 2016. aasta kevadel üles seatud õngitsemislehte riigikaitse valdkonna kasutajate info kalastamiseks, mis välimuselt meenutas varem kasutusel olnud veebipõhist e-posti sisselogimislehte.

-----Original Message-----
From: Taimar Peterkop [mailto:taimar.peterkop@ria.ee]
Sent: Tuesday, September 06, 2016 4:15 PM
To: Tiia Uibooss
Subject: Re: pangaülekandega

Tere Tiia

Sa peaksid saatma £35,431.00 Euro et pangakonto allpool.

Panga nimi: Halifax Bank
nimi kontohavare: Miss S Howman
konto number: 11454962
IBAN: GB60HLFX11065811454962
SWIFT/BIC: HLFXGB21

Viited / Koda: 442 Arve 39AS11 442 - (442 - Arhitektuuri-, ingenjörs- och andra tekniska tjänster.)

Palun andke mulle teada niipea,sa lõppenud pangaülekandega .

Taimar Peterkop

Pahatihti ei piirdu kahju ühe konto kompromiteerumisega. Kuna digitaalseid keskkondi on palju ja inimmälu on piiratud, on salasõnade taaskasutamine erinevates teenustes ja keskkondades liigagi levinud ning välja petetud kasutajanime ja salasõna abil saadakse tihti ligipääs rohkem kui ühele kasutaja kontole.

Kasutajad on üldiselt teadlikud õngitsemisohtude olemasolust, ent jäävad hätta teadmiste rakendamisega praktikasse olukorras, kus õngitsusmeetodeid pidevalt täiustatakse, muutes adressaadile pakutavat legendi ja varieerides levitamiskanaleid. Seetõttu on CERT-EE aasta jooksul järjepidevalt teavitanud avalikkust muutustest õngitsemisohtudes ning uute õngitsemisviiside levikust. Teadlikkuse paranemisse on tänuväärse panuse andnud ka RIA partnerasutused ja meediaväljaanded.

JÄRELDUSED:

- Õngitsemistehnikad ja -meetodid täiustuvad. Libakirja on tõelisest üha raskem eristada, sest kasutatakse reaalsetelt isikutelt üle võetud kontosid isiku kontaktide ründamiseks või esinetakse reaalse, kasutajale tuttava teenusepakkujana. Õngitsemine mängib kasutajate uudishimule, ahnusele, hirmule või kaastundele.
- Enamiku õngitsemisrünnete motiiviks on raha. Kõrge riskiga on tundlikku teavet õngitsevad kirjad, kus ründaja kavatsus ei piirdu ainult ühele kontole või teenusele juurdepääsu saamisega, vaid neid ollakse valmis kasutama ka hüppelauana teiste kontode juurde. Selles seisnebki salasõnade ristkasutamise ohtlikkus – ründajal on saadud andmete abil pahatihti võimalik ligi pääseda ka teistele teenustele.

RIA SOOVITUSED

Kasutajale

- Enne parooli ja kasutajanime sisestamist veendu, et tegemist on tegeliku teenusepakkuja veebilehega. Kui aadressiribal kuvatav veebiaadress tekitab kahtlusi, ei tohi sinna oma andmeid sisestada. Kui oled oma parooli juba sisestanud, vaheta parool kohe.
- Ära saada raha ega vasta petukirjale. Kui raha küsiva kirja on saatnud sõber, helista talle ja uuri järele, kas ta on tõesti hädas. Kui oled petukirja saatjale juba raha saatnud, pöördu kindlasti politseisse (cybercrime@politsei.ee) ning hoia uurimise tarbeks alles küberkurjategijatega peetud kirjavahetus.
- Lülita võimalusel sisse kaheastmeline autentimine, eriti e-posti kontol. Juhendid selleks leiad RIA blogist (blog.ria.ee).
- Kahtlasest aadressist või õngitsuskirjast anna teada e-posti aadressil cert@cert.ee.

Asutuse juhtkonnale ja IT-juhile

- Ära kasuta kollektiivkontot, kus ühte postkasti sisenevad vaheldumisi ja sama kasutajanime ja parooliga mitu töötajat.
- Hoia töötajate isiklikud ja töised e-posti kontod lahus ja sea sisse korralik paroolipoliitika.

Loe lisaks: https://blog.ria.ee/petukirjadest-googie-pole-g00gle-pole-google/

MÕNED VÄÄRAMATUD JA ÜLDKEHTIVAD KÜBERTURBETÕED

1. Kui miski on internetiga ühendatud, siis varem või hiljem püüab keegi sinna sisse murda.
2. Kui sellel, mis internetiga ühendatakse, on väärtust, siis keegi investeerib aega ja vaeva selle varastamiseks.
3. Kui varastatul ei ole rahalist väärtust varga enese jaoks, on sellele ikkagi võimalik ostja leida.
4. Varastatu müügiväärtus on üsna kindlasti väiksem, kui selle väärtus ohvri jaoks.
5. Kes ei pea vajalikuks kulutada murdosa vara väärtusest, et seda kurjategijate eest kaitsta, võib eeldada, et pääseb oma vara koormast kurjategija abiga.

Allikas: Brian Krebs*

* https://krebsonsecurity.com/2017/01/krebss-immutable-truths-about-data-breaches/

Aegunud tarkvara põhjustab enamiku registreeritud küberintsidentidest

Igikestev probleem, mis otse või kaudselt põhjustas enamiku 2016. aastal Eestis registreeritud küberintsidentidest, on vananenud tarkvara – olgu see siis uuendamata hooletusest või teadmatusest.

Standardne ja suure kasutajaskonnaga tarkvaralahendus on üldjuhul niihästi mugav kui ka turvaline, sest kasutamise käigus ilmnenud vead parandatakse versiooniuuendustega kiiresti. Teisalt on ka kurjategijad standardlahenduste puudustega hästi kursis ning uuendamata tarkvara puhul on tõsine risk, et puudusi ja haavatavusi kasutatakse ära nii andmevarguseks, pahavara jagamiseks kui ka teenusetõkestusrünneteks kolmandate isikute teenuste vastu. Iseäranis atraktiivsed kaaperdamise sihtmärgid on veebipõhised teenused, mille kaudu tehakse reaalseid rahalisi tehinguid ning edastatakse teavet, millel on rahaline väärtus (nt krediitkaardiandmed). Selliste turvanõrkuste ärakasutamisele tugineb tihtipeale terve kuritegelik „tööstusharu".

Eestis laialdaselt kasutatava veebilehtede sisuhaldustarkvara WordPress abil hallatavatest lehtedest oli möödunud aasta lõpul uusimale versioonile uuendamata üle 20%. Veel kurvem oli olukord Joomla sisuhaldustarkvara osas, kus ligi 85% veebilehtedest kasutas sisuhaldustarkvara aegunud versiooni.[1] Veebilehe haldaja teadmatuse või tegevusetuse hinnaks pole üksi tema enese haavatavus rünnetele, vaid haavatavate veebilehtede kaudu saab pahavaraga nakatada ka lehekülje külastajaid. Seadusest ja teenuselepingust lähtudes on sideteenuse osutajal õigus asuda piirama teenuse osutamist kliendile, kui tema tegevuse (või tegevusetuse) tõttu seatakse ohtu sideteenuse toimimine ja teised kasutajad.[2] Vajadusel on Eesti teenuseosutajad seda õigust teiste kasutajate ning sidevõrgu turvalisuse ja terviklikkuse kaitseks ka rakendanud.

1 CERT-EE seire andmed 2016. aasta oktoobri lõpu seisuga.
2 Elektroonilise side seadus § 98.

Selle näiteks, kuidas uuendamata tarkvara võib kaasa tuua reaalse rahalise kahju ohu teenusepakkuja klientidele, oli möödunud aastal Eestiski laialt levinud veebipoetarkvara Magento vanemas versioonis leidunud turvaviga, mis võimaldas varastada kasutajate krediitkaardiandmeid. Puuduse parandamiseks oli turvapaik küll välja antud, aga tuhanded veebipoed üle maailma, nende seas ka tosinkond Eesti veebipoodi, toimetasid veel aasta pärast paranduse väljaandmist haavatavat versioonil. Kõigi puudutatud veebipoepidajatega Eestis võttis CERT-EE ühendust ning juhendas neid haavatavuse parandamisel. Pole teada, kas keegi Eesti e-poodide klientidest ka tegelikku kahju kannatas – Eestis on kombeks e-kauplustest ostes tasuda pigem pangalingi kaudu. Ent arvestades, et Eestis on välisriikide veebipoodides ostlemine üha populaarsem, ei tarvitse Eesti kasutaja sellistest ohtudest sugugi puutumata jääda.

JÄRELDUSED

- Aegunud ja uuendamata tarkvara kasutamine on Eestis enamiku küberintsidentide otsene või kaudne põhjus.
- Aegunud sisuhaldustarkvara kasutamine on epideemiline. Veebilehe haldaja teadmatuse või tegevusetuse hinnaks pole üksnes tema enese haavatavus, vaid pahavaraga nakatatakse ka lehekülje külastajaid. Ohtlikuks muutunud veebilehe pidaja peab arvestama võimalusega, et kasutajate ligipääsu tema veebilehele piiratakse sidevõrgu ja teiste kasutajate turvalisuse kaitseks.

RIA SOOVITUSED

- Uuenda sisuhaldustarkvara kohe uue versiooni või turvapaiga väljaandmise järel.
- CERT-EE avaldab RIA veebilehel ja sotsiaalmeediakanalites regulaarselt teavitusi uute turvapaikade ja leitud turvanõrkuste kohta, jälgi neid!

Arenevate tehnoloogiate ja teenustega seotud ohud

Üha enam annavad üleilmset kõneainet küberohud, mis on seotud kiiresti arenevate tehnoloogiate ja teenustega, nagu nutiseadmed ja nn asjade internet, mille kasutusala laieneb ning mille turvalisusriskid mõjutavad varem puutumata valdkondi. Näitena võib tuua ulatuslikud infolekked delikaatseid terviseandmeid haldavatest nutirakendustest, millest kirjutas eelmise aasta lõpus välisajakirjandus, või Ukraina konfliktis riigikaitselise teabe vastasele kättesaadavaks saamise manipuleeritud nutirakenduse kaudu.[3] Samuti põhjustavad üha enam peavalu asjade interneti seadmeid ära kasutavad teenusetõkestusründed, kus ründemahud näitavad üha kasvavat tendentsi ja tõhusaid vahendeid rünnete vältimiseks ei ole.

3 Vt https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_detsember_2016.pdf.

MOBIILISEADMETE TURVANÕRKUSED JA NUHKVARA

Küberturvalisuse ettevõte Kryptowire avaldas 2016. aasta novembris teate Androidi mobiiliseadmete ADUPS turvaveast, mis seab ohtu väga paljude seadme kasutajate teabe konfidentsiaalsuse.* Ettevõte tuvastas Androidi operatsioonisüsteemis pahavara, mis saadab kolmandate isikute serveritesse personaalset ja tundlikku kasutajainfot nagu kõnelogid ja lühisõnumite sisu. Mainitud haavatavusega seadmeid on maailmas pea 700 miljonit ning enam kui 200 riigis.

CERT-EE tegi kindlaks, et ka Eestis on arvukalt selliseid seadmeid, mis tihedalt suhtlevad kasutajatelt konfidentsiaalset teavet koguvate serveritega. Ainuüksi Kryptowire avaldatud artiklis mainitud BLU telefone on Eestis teadaolevalt kasutusel tuhandeid. Siiski ei ole probleem mitte telefoni tootjas, vaid operatsioonisüsteemi ADUPS konkreetses tootes (FOTA ehk *Firmware on the Air*). Operatsioonisüsteemi tootja on turvanõrkusest teadlik ning on juba ka väljastanud ADUPS FOTA järgmise versiooni, kus väidetavalt on viga parandatud.

Esialgne kontroll ei ole näidanud, et selle haavatavusega seadmetel Eestis oleks olnud juurdepääs riigiasutuste sisemistele infosüsteemidele (nt meiliserverid). RIA hoiatas ohust riigiasutusi ja riigi kõrgemat juhtkonda ning tegi koostööd suuremate mobiilioperaatoritega, kes võtsid ka omalt poolt meetmeid kasutajate riskide maandamiseks.

RIA SOOVITUSED

- Hoidu vähetuntud tootjate seadmete soetamisest. Vii end kurssi nutiseadmete turvariskidega ning turvalise kasutamise põhimõtetega. RIA kodulehel on avaldatud soovitusi nutiseadmete turvaliseks kasutamiseks nii tavakasutajatele kui ka arendajatele.

Asutuse IT-juhile

- Tuvasta nakatunud seadmed oma organisatsiooni infosüsteemides ning võta meetmed selliste seadmete juurdepääsu tõkestamiseks infosüsteemile.
- RIA soovitab tungivalt pöörata tähelepanu asutuste infoturbepoliitika järgimisele ning hoiduda võimalusel vähetuntud tootjate seadmete soetamisest.

Loe lisaks: https://www.ria.ee/public/toetusskeem/koolitusmaterjalid/teadl_Jaotusmaterjalid2016.pdf

* https://www.kryptowire.com/adups_security_analysis.html

Ründavad vidinad: asjade interneti teenusetõkestusründed

Kõikvõimalike internetti ühendatud „vidinate" arv ületab juba kordades seadmete arvu, mida oleme traditsiooniliselt arvutiks pidanud: 2016. aastal oli asjade interneti ehk esemevõrgu seadmeid käibes hinnanguliselt 15,4 miljardit.[4] Internetti ühendatavate seadmete kasutusala laieneb üha, valvekaameratest ja aktiivsusmonitoridest meditsiiniseadmete ja kaugjuhitavate termostaatideni, ning need täidavad igapäevaelus järjest kaalukamat rolli.

Sellise esemevõrgu tekkimine on aga toonud kaasa ka uut tüüpi ohud, millega ei ole arvestanud ei tootjad ega kasutajad. Möödunud aasta tõi hulga juhtumeid, kus esemevõrgu seadmed osutusid nii küberrünnete sihtmärgiks kui ka nende toimepanemise vahendiks.

Uuele üleilmsele suundumusele osutasid aasta teises pooles toimunud väga suure mahuga teenusetõkestusründed (DDoS), mille läbiviimiseks kasutati digibokse, valvekaameraid ja muid asjade interneti seadmeid. Sääraste internetti ühendatud koduseadmete turvalisus on valdavalt nõrk ning nende pahavaraga nakatamine ja rünneteks ärakasutamine on osutunud liigagi hõlpsaks.

Ülaltoodu räägib selget keelt, et nutikate koduseadmete turvalisus või selle puudumine ei ole üksi kasutaja enese privaatsuse mure, nagu sageli ekslikult arvatakse, vaid võib mõjutada oluliste teenuste – sh hädaolukorra ajal riigi pakutavate teenuste – kättesaadavust elanikkonnale ning paljude ettevõtjate majandustegevust.

Eesti internetitaristu väiksust arvestades ei nõua 2007. aasta omaga sarnanevate küberrünnete korraldamine olulisi oskusi ega raha. Sama kehtib ka meist märkimisväärselt suuremate riikide

MIRAI ROBOTVÕRK

Üks sügisestest rekordilise mahuga teenusetõkestusrünnetest tabas üht Ameerika Ühendriikide suurimat domeeninimeteenuse pakkujat.* Intsidendi tagajärjel muutus USA ja mõne Euroopa riigi kasutajate jaoks tundideks kättesaamatuks üle tuhande veebilehe, nende seas üle maailma populaarsed sotsiaalvõrgustikud, rahvusvahelised meediakontsernid ning e-kaubanduse ja e-teenustehiiud nagu Amazon ja PayPal. Ent katkestus puudutas ka näiteks Rootsi valitsuse ja tsiviilhädaolukordade agentuuri veebilehtede kättesaadavust, mille kaudu edastatakse elanikkonnale teavet kriisiolukordades.**

Mirai-nimelise pahavaraga nakatatud koduseadmete kaudu õnnestus rünnata interneti baasarhitektuuri, kusjuures suhteliselt väikese hulga seadmete abil genereeriti ründemaht, mis ekspertide hinnangul oli seninähtuist suurim (ligikaudu 100 000 seadme abil tipphetkel kuni 1,2 terabitti sekundis).***

4 https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#e2c59c9292d5.

* Domeeninimeteenus teisendab sõnalised domeeninimed numbrilisteks IP-aadressideks, võimaldades nii kasutaja päringute kohaletoimetamist.

** https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_oktoober_2016.pdf.

*** http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html.

puhul.[5] Teenusetõkestusrünnete senist mustrit hinnates ei saa samuti välistada võimalust, et seesuguseid ründeid on võimalik kasutada ka interneti kui terviku aluseks oleva taristu ründamiseks, eesmärgiga peatada kogu interneti toimimine – küsimus pole niivõrd suutlikkuses ründeid toime panna, kuivõrd selles, kellel võiks selleks motivatsioon olla.

JÄRELDUSED

- Esemevõrgu seadmetele pole spetsiifilisi küberturbenõudeid ja -standardeid. Tootjate tähelepanu turvalisusele on madal; tööstusharu on tekkinud nullist nii kiiresti, et tururegulaatorid ei ole jõudnud tehnoloogia arengule reageerida. Seetõttu on lähenemine esemevõrgu seadmetest lähtuvatele ohtudele seni pigem reaktiivne: tegeldakse intsidentide lahendamise ning tagajärgede minimeerimise ja kõrvaldamisega.
- Esemevõrgu seadmete abil korraldatavad suuremahulised teenusetõkestusründed on potentsiaalne oht nii riikide kui interneti baastaristu enese jaoks. Teenusetõkestusrünnete juhtimine ei nõua olulist ressurssi ning vajalik pahavara on internetist kättesaadav; sageli juhivad ründeid ebastabiilsed noorukid lihtsalt uudishimust või saamahimust. Praegu pole vahendeid teenusetõkestusrünnete ärahoidmiseks – ka 2016. aasta suuri ründeid ei sulgetud, vaid need lakkasid ise. On suur tõenäosus, et selliseid ründeid näeme tulevikus veel, ning üha suuremas mahus.[6]
- Lisaks võimalusele seadmete nõrka turvalisust küberrünneteks ära kasutada on rünnetele haavatavad ka esemevõrgu seadmed ise. Kui need võimaldavad kaughaldamist või andmete edastamist internetti, võivad need saada kurjategijate sihtmärgiks.

5 https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_november_2016.pdf.
6 https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf.

RIA SOOVITUSED

- Mõtle, kas konkreetse seadme võrku ühendamine on tõepoolest vajalik. Kui vastus on jah, osta esemevõrgu seade tootjalt, kes suudab pakkuda turvalisust.
- Tea oma seadmete võimalusi – eriti nende omi, mille häireteta toimimisest sõltub sinu elu, tervis või füüsiline turvalisus (meditsiiniseadmed).
- Vaheta seadme vaikeparool tugevama parooli vastu ja luba seadmel töötada ainult turvatud WiFi võrgus. Võimalusel eralda esemevõrgu seadmed eraldi turvalisse võrku.
- Uuenda esemevõrgu seadmete tarkvara kohe, kui uuendus välja antakse.

Loe lisaks: RIA soovitused https://blog.ria.ee/asjade-internet-suurendab-kuberkuritegevust/

Valdkondlikud riskid

Avalik sektor on nii juhuslike kui suunatud rünnete sihtmärk

Riigiasutuste osakaal möödunud aasta küberjuhtumite üldarvus jääb 20–30% piirimaile. Aasta jooksul registreeris CERT-EE 1687 riigisektori asutustega seotud kübersündmust. Olulist kasvu võrreldes 2015. aastaga võib eeskätt seostada asutuste suurenenud aktiivsusega intsidentidest teavitamisel ning tõhustunud koostööga RIA ja asutuste vahel. Suur osa riigiasutuste edastatud teavitusi on seotud neile teatavaks saanud turvanõrkuste või leitud administreerimisvigadega, millega reaalset intsidenti ei kaasnenud, ent mille kohta teabe saamine annab RIA-le parema olukorrateadlikkuse võrkudes toimuvast ning aitab seeläbi kaasa intsidentide ärahoidmisele.

Juhtumite levinumate põhjuste seas on seadmete rikete ja inimlike vigade kõrval endiselt küberründed. Samas pole enamik tõsise tagajärjega küberintsidentidest tingitud mitte rünnetest, vaid just riskide alahindamisest ja inimlikest eksimustest.

Eesti ametiasutuste töö on paljudes valdkondades väga sõltuv infosüsteemide toimimisest. Sisejulgeoleku valdkonnas on ka mõnekümneminutiline katkestus näiteks piirivalvet või häirekeskust teenindavates süsteemides kriitiline. Avaliku sektori teenuste eripäraks on ka alternatiivide puudumine: häired avalikke teenuseid toetavates infosüsteemides võivad kaasa tuua oluliste teenuste katkestuse, ilma et oleks võimalik lülituda ümber teisele teenusepakkujale. Selliste teenuste näiteks on nii sisejulgeoleku valdkonna sideteenused, rahvastikuregister kui digiretsept. Seetõttu oleme seisukohal, et riigiasutuste osutavate kriitiliste teenuste toimepidevuse tagamine vajab tõsist tähelepanu ning lisainvesteeringuid, et kindlustada teenuse käideldavus.

Alates 2008. aastast on Eestis riigi infosüsteemi moodustavate andmekogude turvalisuse tagamisel kasutusel kolmeastmeline etalonturbe raamistik ISKE,[7] mille rakendamine tagab riigiasutuste ja kohalike omavalitsuste andmekogudes töödeldavate andmete turvalisuse minimaalsel vajalikul baastasemel. Riigiasutuste võimekus tagada nende peetavate andmekogude vastavus ISKE turvameetmetele on viimase kahe aasta jooksul hüppeliselt tõusnud – seda kinnitab asjaolu, et mullu jõudis ISKE auditi läbinud andmekogude osakaal ministeeriumite vaates esmakordselt 80%ni. Koos haldusala asutuste peetavate andmekogudega on see suhtarv peaaegu 70%.

Kohalike omavalitsuste küberturvalisuse korraldus üldiselt ja ISKE turvameetmete rakendamine andmekogude turvalisuse tagamiseks konkreetselt on endiselt väga ebaühtlane. Ootus on, et haldusreformi järel paraneb nii kohalike omavalitsuste teadlikkus infoturbe vajalikkusest kui ka infoturbe korraldamise võimekus.

Nii riigi- kui kohalike omavalitsuse asutuste kogemust analüüsides võib järeldada, et infoturve on suuresti juhtimis- ja alles seejärel ressursiküsimus. Pahatihti on küberturvalisusalane teadmatus tingitud

7 Infosüsteemide turvameetmete süsteem (Vabariigi Valitsuse 20.12.2007 määrus nr 252; RT I 2007, 71, 440).

huvipuudusest ja vastupidi. Teadmiste puudumisel kiputakse ressursinappust takistusena üle tähtsustama; samas kinnitab nende kogemus, kes on infosüsteemide turvameetmed rakendanud, et turvalisuse parandamiseks on palju võimalik ka investeeringuteta ära teha.

Riigiasutuste vastu toime pandud küberrünnetest olid möödunud aastal enim levinud juhuslikud ja suunatud õngitsemiskampaaniad, mille eesmärgiks oli petta välja raha või saada ligipääs tundlikele andmetele. Kui mõnel puhul võib eeldada lihtsalt adressaatide sattumist laiema kampaania sihtmärkide sekka, siis mitme ründe tunnused viitasid toimepanija taotlusele rünnata konkreetset adressaati. Selle näiteks olid eespool kirjeldatud pettusekatsed, kus kasutati näiliselt riigiasutuse peadirektorite ja peaministri nimel saadetud kirju, ning riigikaitseorganisatsioonile sihitud õngitsemiskirjade levitamine ja suunatud õngitsuslehtede loomine.

Oli ka üksikuid riigiasutuste vastu suunatud väljapressimisjuhtumeid, kus asutusi ähvardati DDoS-rünnete korraldamisega. Enamasti oli neil juhtudel nõude sisu rahaline, ent väljendati ka ideoloogilisi või poliitilisi seisukohti. Nende juhtumite tegelik mõju jäi siiski väheoluliseks ning asutuste tööd need ei häirinud.

JÄRELDUSED

- Avaliku sektori küberriskide juhtimisel tuleb silmas pidada peamiselt kaht enim ohustatud valdkonda: teisi avalikke teenuseid või riigi julgeolekut toetavate infosüsteemide toimepidevus (kus intsidentide toimumise põhjus on sageli tingitud sisemistest, mitte välistest teguritest) ning rahalisel, poliitilisel või ka ideoloogilisel motiivil suunatud ründed.
- Riigiasutuste töötajate vastu suunatud rünnetega tahetakse eeskätt ligipääsu mitteavalikule teabele, ent ründeid võidakse kasutada ka sabotaaži ettevalmistamiseks, et luua võimalus takistada infosüsteemi tööd või muuta või kustutada andmeid.

Kasutajaandmete lekked

Eestis ei registreeritud 2016. aastal ühtki tõsist andmelekke juhtumit ei ametiasutustes ega ka teenusepakkujate või ettevõtjate juures. Laiemat tähelepanu pälvis aga nn Dropboxi intsident septembris, kus internetis sai kättesaadavaks Dropboxi pilveteenusest mõni aeg tagasi varastatud kasutajakontode andmebaas umbes 68 miljoni kasutaja parooliräsiga. RIA analüüs leidis andmete seast rohkem kui 20 000 Eesti e-posti aadressiga seotud kontot. Nende seas leidus omakorda kümnete Eesti kõrgete riigiametnike ja oluliste asutuste töötajate kontosid, kes olid kasutanud oma tööalaseid e-posti aadresse avalikku pilveteenusesse sisenemiseks. Lekkinud parooliräside võrdlemise kaudu võib järeldada, et mitmete nimetatud kontode puhul kasutati väga nõrga turvalisusega paroole. Kõiki puudutatud asutuste infoturbe- ja IT-juhte on RIA küberturvalisuse teenistus leidudest teavitanud.

Ilmselgelt ei puuduta andmeleke ega avalikes teenustes tööalaste e-posti aadresside kasutamise probleem üksnes riigiametnikke, vaid praktika on laialt levinud nii Eestis kui väljaspool. Riigi jaoks on risk selles, et lekkinud info abil saab rünnata nii inimeste ametialaseid kontosid kui ka nendega seotud asutusi. Nii kurjategijad kui ka välisriikide luureteenistused teavad hästi,

et inimestele on omane kasutada erinevatesse kohtadesse sisselogimisel samu või sarnaseid paroole. Seega lihtsustab ühe parooli murdmine ka teiste kasutusel olevate aadresside vastu rünnete korraldamist.

Suuremahulised paroolilekked on muutunud tavaliseks. Möödunud aastal teavitas internetiteenuste osutaja Yahoo ligi miljardi Yahoo kasutaja andmete lekkimisest. Kõnealune andmeleke on seni teadaolevaist mahukaim, ent sadadesse miljonitesse ulatuvaid andmevargusi on olnud mitu; ainuüksi möödunud aastal lekkis teadaolevalt kokku üle nelja miljardi andmekirje.[8]

JÄRELDUSED

- Üksnes salasõnadel põhinevat autentimist ei saa enam turvaliseks pidada. Häkkerid kontrollivad ühest allikast leitud paroole automaatselt ka kõikvõimalikes teistes teenusekeskkondades ning leiavad ristseosed (paroolide ristkasutuse) kiiresti. See muudab üksnes parooliga autentimise ebaturvaliseks hoolimata sellest, kui hästi konkreetne teenus ise oma tööd korraldab, sest teistelt lehtedelt lekkinud kasutajaandmete kuritarvitamise vastu abi ei ole. Sedavõrd massiivsete lekete korral ei ole tegelikult võimalik kõiki andmelekkest mõjutatud kasutajakontosid sulgeda ega nende paroole muuta.
- Eestis on ID-kaardil ja mobiil-ID-l põhinevat autentimist kasutavad riiklikud süsteemid ja olulised e-teenused hästi kaitstud. Võrreldes muu maailmaga teeb see näiteks Eesti riiklikest ja pangateenustest andmete kättesaamise kurjategijale ülikeeruliseks ja kulukaks, mis vähendab nende teenuste atraktiivsust küberkuritegevuse sihtmärgina. Suured globaalsed teenuseosutajad nagu Google, Facebook ja Microsoft on kahetasemelise autentimise oma teenustes hästi käima saanud ning selle kasutus on 2016. aasta jooksul tublisti tõusnud.

8 https://en.wikipedia.org/wiki/List_of_data_breaches; https://en.wikipedia.org/wiki/Yahoo!_data_breaches; http://www.securityweek.com/42-billion-records-exposed-data-breaches-2016-report.

RIA SOOVITUSED

Kasutajale

- Väldi oma tööaadressi sidumist pilveteenuste või eraviisiliseks kasutamiseks mõeldud kontodega. Selline tegevus lihtsustab tuntavalt küberkurjategijate ja vaenulike võõrriikide luureteenistuste sihitud rünnakuid ametialaste kontode vastu, sest tekib võimalus leida miljonite kasutajate hulgast just need kasutajad, kelle paroolide murdmisele ja andmete kättesaamisele tasub aega ja vaeva kulutada.
- Väldi paroolide ristkasutamist, eriti tööarvuti parooli kasutamist teistes teenustes. Kus vähegi võimalik, lülita sisse kaheastmeline autentimine.

Asutuse IT- ja infoturbejuhile

- Tasub eeldada, et paroolidel põhinev autentimine on eelduslikult ebaturvaline ning inimesed kasutavad samu paroole erinevates teenustes.
- Soovitame seadistada teenustes kaheastmeline autentimine igal pool, kus võimalik.

Erasektori turvateadlikkus on ebaühtlane ja turvalisusse investeerimine ebapiisav

Ootuspäraselt puudutas lõviosa möödunud aasta küberjuhtumitest erasektorit, kes kasutajaskonnalt kõige arvukam. Siia kuuluvad nii suured ja väikeettevõtjad, vabaühendused kui ka üksikisikuist arvutikasutajad, kelle digitaalne sõltuvus ning küberturvalisusalane teadlikkus erinevad väga palju. Samas on tõsi ka see, et digitaalsete lahenduste toimimise tähtsust kiputakse alahindama ning riskide ennetamise asemel pööratakse turvalisusele tähelepanu alles pärast intsidenti.

Kui elutähtsaid teenuseid osutavatel ettevõtjatel on seadusest tulenev kohustus oma IKT-riske hinnata ja maandada ning nende infosüsteemide kaitse on suhteliselt paremini korraldatud, siis väikeste ja keskmise suurusega ettevõtjate ning vabaühenduste peamiseks kitsaskohaks on nende madal teadlikkus küberriskidest ning asjaolu, et tihti nad end küberkuritegevuse sihtmärgiks ei pea. Kuivõrd nende ressursid on piiratud – iseäranis vabaühendustel, kelle toimimine põhineb suuresti vabatahtlikkusel ja eesmärk pole liikmetele tulu teenimine –, pole ka investeeringuid infotehnoloogiasse nende jaoks prioriteet.

Viimast väidet kinnitavad ka välisriikides tehtud uuringud: ehkki vabaühenduste küberriskid on sarnased äriühinguteomadega,onneileiseloomulikmadal riskiteadlikkus ühes ressursinappusega, mis muudab vabaühendused hõlpsaks sihtmärgiks. Vabaühenduste seas on ka mõned magusamad sihtmärgid, näiteks poliitiliste või sotsiaalsete eesmärkidega ühingud, kelle organisatsioonisiseseks kasutuseks mõeldud teabest võivad olla huvitatud nii kurjategijad kui ka välisriikide luureteenistused. Olgu siinkohal meenutatud, et Venemaa küberoperatsioon USA valimiste mõjutamiseks sai alguse erakonnale kuulunud infosüsteemi, mitte valimissüsteemi enese ründamisest.

Väikeettevõtjate ja vabaühenduste sagedasemaks kitsaskohaks küberturvalisuse mõttes on aegunud veebilehed, mille turvanõrkusi kasutatakse ära andmevarguseks või mis levitavad pahavara. Kehva turvalisusega – nt teada-tuntud turvanõrkuste tõttu – veebilehtede puhul võivad olla ohus ka töötajate või liikmete, klientide ja koostööpartnerite isikuandmed ning avalikult kättesaadavad meiliaadressid võivad saada õngitsemise või lunavarakirja sihtmärgiks. Lisaks eelnevale on väikeettevõtjate ja vabaühenduste küberturvalisuses peamiseks murekohaks nende infosüsteemide turvavead ja administreerimisvead, mida küberkurjategijad võivad rünneteks ära kasutada.

Eesti majanduse väljakutseks on kujunenud suutlikkus pakkuda kõrgema lisandväärtusega tooteid ja teenuseid[9] ning digiteerimine pakub märkimisväärseid võimalusi nii piirkondlikus kui globaalses konkurentsis osalemiseks. Eesti kõrgtehnoloogilistel ja võtmetähtsusega ettevõtjatel tehnoloogiakesksetes valdkondades (energiatööstus, info- ja kommunikatsioonitehnoloogia, keemiatööstus ja biotehnoloogia) tasub arvestada, et nende tegevus võib huvi pakkuda ka digitaalse tööstusspionaaži või

9 https://valitsus.ee/sites/default/files/content-editors/failid/majandusarengu_raport.pdf.

saboteerimise seisukohalt. Viimane toimub tavaliselt välisriigi toel, kuna majanduslik ja tööstusspionaaž on enamasti äärmiselt aeganõudev ja kulukas ning kiiret kriminaalset tulu ei paku.

Tööstusjuhtimisseadmete haavatavus on paratamatus, millega tuleb arvestada. Seadmete elukaar on väga pikk, mis pärsib võimalust neid uuendamistega turvalisemaks muuta, samuti ei ole nende seadmete mitteühendamine internetiga iseenesest mingi turvagarantii, kuna ründajad leiavad tavaliselt võimaluse sellistesse võrkudesse ründevara sisse toimetada. Seega peab igal elutähtsa või kriitilise teenuse osutajal olema varuplaan juhuks, kui ICS/SCADA[10] süsteem muutub mittekasutatavaks.

JÄRELDUSED

- Erasektori teadlikkus küberriskidest on lünklik, seda nii üksikisiku kui ettevõtjate tasandil. Iseäranis väikeettevõtjad ja vabaühendused ei pea end küberohtude sihtmärgiks ning turvalisusse ei investeeri.
- Eesti tehnoloogiakesksetes valdkondades tegutsevad ettevõtjad võivad olla digitaalse spionaaži sihtmärgiks. Välistada ei saa ka sabotaažimotiivi, eriti elutähtsat teenust osutavate ettevõtjate puhul.

10 Industrial control systems (ICS), tööstuslik automaatjuhtimissüsteem, mida kasutatakse tööstusprotsesside automatiseerimiseks, seireks ja juhtimiseks. Supervisory Control and Data Acquisition (SCADA) on üks tööstuslike automaatjuhtimissüsteemide tüüpe.

VIRU KEEMIA GRUPI JUHTUM

2016. aastal tuvastati Viru Keemia Grupi (VKG) arvutivõrgus pahavarale iseloomulik liiklus. Tarkvaraekspertiisi tulemusena leiti VKG kontorivõrgu arvutitest tarkvara Mimikatz, mida kasutatakse Windowsi süsteemides identsustõendite (näiteks paroolide, parooliräside jms) kogumiseks. Ühtlasi leiti ka n-ö tagauksetarkvara, mida kasutati kontrollserveriga ühenduse pidamiseks. Järgnenud seirega tuvastati mitu kahtlast ühendust ning leiti ka sertifikaate, mis sarnanesid tagaukseühenduse puhul kasutatavatega. Sisevõrgu seire rohkem (pahavara) ühendusi kontrollserveriga ei tuvastanud, samuti ei leitud muid pahavaraga nakatunud seadmeid.

2016. aasta juunis tuvastati taas võrguühendus sama kontrollserveriga. Sel korral õnnestus ühenduse andmete põhjal tuvastada ka ühenduse algatanud arvuti nimi. Kontrollimisel selgus, et pahavaraga oli nakatunud SCADA monitoorimissegmendis paiknev tööjaam, mis seejärel võrgust eemaldati. Arvuti tarkvaraekspertiisis selgus, et arvutisse oli paigaldatud sama tagauksetarkvara, mis leiti varasemalt kontorivõrgu arvutitest.

Nii võrguliiklus kui ka arvutitest leitud pahavara näidised viitasid sellele, et tegemist oli suunatud ründega. Kasutatavat pahavara ja kontrollserverit on seostatud APT28-ks nimetatud küberspionaaži grupeeringuga.*

RIA spetsialistid nõustasid VKGd intsidendi lahendamisel ning võrguturbearhitektuuri ja seadistuste valikul ja ettevõtja IT-haldusprotseduuride uuendamisel. Ühtlasi aitas RIA tõsta ettevõtte töötajate turvateadlikkust.

* Vt nt https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

RIA SOOVITUSED

Kasutajale

- Jälgi RIA teavitusi aktuaalsete küberohtude kohta. Need on saadaval nii RIA veebilehel, CERT-EE Twitteri kontol kui ka meedia vahendusel. RIA blogis avaldame pikemaid juhiseid ja kirjutisi e-riigi ja küberturvalisuse teemal.

Loe lisaks: https://www.ria.ee/public/toetusskeem/koolitusmaterjalid/teadl_Jaotusmaterjalid2016.pdf

Elutähtsad teenused on üha enam kübersõltuvad

Eesti jaoks on endiselt oluline risk mõne elutähtsa teenuse katkemine kübertegevuse tulemusena. RIA on alates 2013. aastast regulaarselt korraldanud elutähtsate teenuste[11] digitaalse toimepidevuse uuringuid, mis näitavad elutähtsate teenuste kasvavat digisõltuvust.

2016. aastal RIA tellimusel läbiviidud elutähtsate teenuste osutamist mõjutavate tegurite uuringuga hinnati missioonikriitiliste ehk riigi toimimiseks vajalike elutähtsate teenuste küberriske ning rakendatud lahendusi nende teenuste toimepidevuse tagamiseks.[12] Uuring kinnitas, et erandita kõik osalenud elutähtsa teenuse osutajad[13] sõltuvad teenuse osutamisel sidest ja elektrivarustusest ning paljud neist loevad oma sõltuvust kriitiliseks. Rohkem kui viiendik küsitletud teenuseosutajatest sõltub kriitilisel määral kolmandate isikute pakutavast IKT-taristust või teenustest – see tähendab, et elutähtsa teenuse toimimine on otseses sõltuvuses väliste IKT-teenuste toimimisest.

IT-riske hindavad paljud kõnealused ettevõtjad üksnes üldises plaanis ning vaid kolmandikul neist on olemas nüüdisajastatud riskianalüüs ja toimepidevuse plaan. Infoturberiskide haldus on hästi korraldatud elektriga varustamise, telekommunikatsiooni ja finantsteenuste valdkonna ettevõtetes; siiski ei kinnitanud ükski uuringus osalenud teenuseosutaja ettevõtte täielikku vastavust infosüsteemide turvameetmete süsteemi[14] nõuetele ning paljudel teenuseosutajatel ei ole piisava detailsusega ülevaadet oma teenuste IKT-alastest ristsõltuvustest. Uuring tõi ka välja, et liiga vähe on tehtud ettevalmistusi pikaajalise elektrikatkestuse puhuks. Samuti napib ettevõtjatel tehnilisi vahendeid, et osutada katkestuste korral teenust alternatiivlahenduste abil.

Eesti tegeleb aktiivselt alternatiivlahenduste leidmisega, et vähendada elutähtsate teenuste sõltuvusi nii

11 Elutähtsad teenused 2017. aasta 30. juunini kehtiva hädaolukorra seaduse mõistes.

12 https://www.ria.ee/public/Kuberturvalisus/Elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf.

13 Uuringuga hõlmatud teenused olid järgmised: elektri, maagaasi ja vedelkütusega varustamine, riigimaanteede ja kohalike teede sõidetavus ning raudteeveoteenuste toimimine, telekommunikatsiooniteenused, finants- ja tervishoiuteenused, kommunaalteenused nagu kaugküttega varustamine, veevarustus ja kanalisatsioon; sadamate ja laevaliikluskorralduse ning aeronavigatsiooniteenuste ja lennuväljade toimimine.

14 ISKE või ISO 27001 standard.

kolmandate isikute teenustest kui ka välisriikides asuvast taristust ning seeläbi vähendada riske teenuste toimepidevusele. Hädaolukorra seadus sätestab teenuseosutajale kohustuse tagada toimepidevusplaanide abil teenuse pidev toimimine ning selle kohustuse täitmisel teevad Eesti era- ja avalik sektor tihedat koostööd.

2016. aasta üleilmseid sündmusi hinnates oli küberintsidentide üha kaalukamast mõjust elutähtsatele teenustele põhjust rääkida eeskätt energia-, tervishoiu-, finants- ja transpordisektoris. Ohtralt rahvusvahelist tähelepanu pälvisid aastase vahega toimunud rünnakud energiasüsteemide vastu Ukrainas, millest esimene jättis elektrita umbes veerand miljonit elanikku ning teine lülitas välja umbes viiendiku pealinna elektrivarustusest.[15] Mõlemal juhul õnnestus energiavarustus mõne tunni jooksul taastada, ent kui aasta varem räägiti küberründe abil energiasüsteemi töö õnnestunud halvamisest kui erakordsest sündmusest, siis 2016. aastal on ohtlikud küberhaavatavused elektrienergiavõrkudes kõneks ka väga arenenud ja stabiilsetes riikides.[16]

Mõistagi ei ole ulatusliku mõjuga katkestused digisõltuvate elutähtsate teenuste toimimises alati tingitud küberrünnetest, nagu võib illustreerida kahe näite varal meie lähedalt. Möödunud kevadel suleti IT-probleemidele viidates tundideks Rootsi pealinna Stockholmi ja ümbritsev õhuruum. Mõni kuu varem põhjustas päikesetormist tingitud radarisüsteemi häire sealsamas lennuliikluse katkestuse.[17]

Eestis 2016. aastal ulatusliku mõjuga küberintsidente elutähtsate teenuste vastu ei olnud. Alates möödunud aastast eristab CERT-EE intsidentide statistikas eraldi elutähtsate teenuste osutajaid puudutanud küberintsidente – see tähendab, et registreeritud juhtumid ei tarvitse olla mõjutanud elutähtsa teenuse toimimist, küll aga teenuse osutajat ennast. Selliseid intsidente oli 253, mis moodustab registreeritud juhtumite üldarvust alla 3% ning tuvastatud intsidentide üldarvust (st kõigist juhtumeist, millega kaasnes vahetu mõju teabe või süsteemi konfidentsiaalsusele, terviklusele või käideldavusele) veidi üle 11%. Enamiku tuvastatud intsidentide puhul oli tegemist nakatunud ja robotvõrku ülevõetud seadmetega sideteenuste osutajate võrkudes, aga oli ka kaksteist lunavaraga nakatumise juhtu.

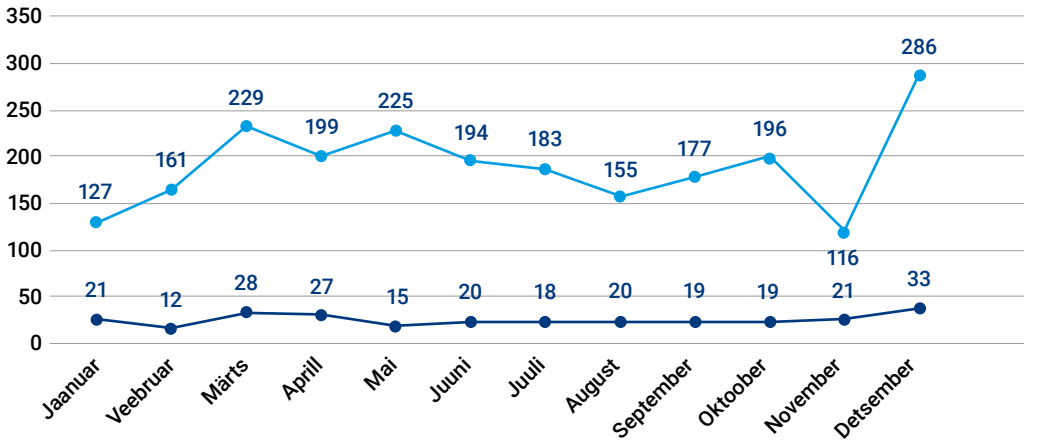
Enim teavitati elutähtsate teenuste osutajaid puudutanud intsidentidest sideteenuste valdkonnas, mis on ootuspärane, arvestades, et sideteenuste toimimisest sõltuvad väga paljud muud teenused ning valulävi sideteenuste katkemisel on seetõttu madal ja teavitamine operatiivne. Enamiku selles sektoris toimunud intsidentide põhjuseks olid seadmerikked, teenusekatkestused või hooldustööde käigus tekkinud kõrvalekalded tavapärasest toimimisest, mille mõju jäi ajaliselt või geograafiliselt piiratuks.

15 http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF; vt ka RIA KTT 2016. aasta jaanuari, veebruari ja detsembri kokkuvõtteid https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html.

16 http://www.ibtimes.com/after-ukraine-cyberattacks-fbi-dhs-urge-us-power-companies-develop-better-safety-2355649; https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

17 https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_mai_2016.pdf; http://www.thelocal.se/20151104/solar-storm-grounds-swedish-air-traffic.

Elutähtsa teenuse osutajat puudutanud küberintsidendid võrrelduna tuvastatud küberintsidentide üldarvuga



NULLPÄEVA HAAVATAVUS SIDEVÕRGU SEADMETES

Kriitilise iseloomuga intsident toimus oktoobris ühe Eesti suurima andmeside-teenuse osutaja tuumikvõrgus. 5. oktoobri varahommikul hakkas osa ettevõtja ülekandevõrgu toimimist tagavatest tuumikvõrgu seadmetest teadmata põhjustel iseeneslikult taaskäivituma. Esmane logide analüüs näitas, et vahetult enne taaskäivitumist raporteerisid seadmed veateadet. Selle veateatega pöördus ettevõtja seadmete tootjafirma poole, kes kinnitas teenusetõkestusründe toimumist, mis halvas seadmete käideldavuse. RIA ja sideettevõtja koostöös koguti ründepakettide salvestused ning edastati need seadmete tootjale; saadud paketid aitasid tootjal välja töötada tarkvarauuendused kriitilise vea parandamiseks. Tarkvarauuenduse väljatöötamiseni suutis ettevõtja edukalt rakendada alternatiivseid meetmeid, et vältida intsidendi kordumist.

RIA hinnangul ei saa toimunut pidada tingimata suunatud ründeks. Analoogseid juhtumeid ilma välise sekkumiseta on erinevate tootjate võrguseadmetega varemgi olnud. Praeguse informatsiooni põhjal on tõenäoline, et tegemist oli seadme tarkvaraveaga, mis lihtsalt teatud tüüpi pakette protsessida ei suutnud. On ka võimalik, et seda tüüpi skaneeringuga otsiti Eesti võrkudest SIP/VoIP* seadmeid, millega VoIP kõnepettusi teha, kuid seejuures tekitati Eesti ühele suuremale internetiteenust pakkuvale ettevõttele mastaapne käideldavuse intsident. Ettevõtja operatiivne tegutsemine ja tulemuslik reageerimine aitas vältida ohtlikku tuumikvõrgu „nullpäeva" *(Zero Day)* haavatavuse levikut.

* Session initiation protocol/voice over IP.

Küberohud tervishoius

Tervishoius oli aktuaalsetest ohtudest aasta jooksul märkimisväärseim ilmselt krüptolunavara. Sektorit üleilmselt tabanud lunavararünnete ja nakatumiste hulk näitab, et tõenäoliselt on küberkurjategijate arvates just nimelt aegkriitilistest andmetest sõltuvast tervishoiust lootus lunaraha kätte saada märksa suurem, kui teisi valdkondi rünnates.

Möödunud aastast võib tuua hulga näiteid lunavaraohvriks sattunud haiglatest nii Euroopa riikides kui Põhja-Ameerikas, kus lunavaraga nakatumine päädis nii patsientide raviandmete loetamatuks jäämise kui ka sellega, et haiglad olid mitme päeva vältel sunnitud ära jätma plaanilised operatsioonid, arstivisiidid ja diagnostilised toimingud.[18] On oluline mõista, et Eesti tervishoid on kõrge digiteerituse tõttu avatud täpselt samadele riskidele ja sellega seoses on meil oht, et ei katke mitte ainult mugavate tervishoiuga seotud e-teenuste kättesaadavus, vaid katkeb arstiabi kui elutähtsa teenuse enda osutamine.

Ehkki Eestis ülal viidatutega samavõrra drastilisi juhtumeid ei olnud, ei jäänud ka Eesti tervishoiusüsteem lunavaraintsidentidest puutumata. Ühes Eesti suuremas haiglas levis lunavara nakatunud tööjaamadest failiserverisse. Raviteenuste osutamine häiritud ei olnud, küll aga oli tõsiseid probleeme muudes tööprotsessides. Paraku ei jäänud see intsident ka ainsaks selletaoliseks.

Lunavarast tingitud kahju ärahoidmiseks on andmete varundamine ja riske minimeeriv administreerimispoliitika möödapääsmatud. Möödunud kevadel USA Kansase osariigi haiglas aset leidnud juhtum, kus lunaraha maksmise järel andmeid tagasi ei saadud, vaid haiglale esitati hoopis uus nõue järgmise summa maksmiseks, peaks olema värvikas õppetund, kuivõrd halb mõte on krüpteeriva lunavara ohvriks langemise korral mõelda lunaraha maksmisele.

Mullused küberintsidendid Eesti tervishoius räägivad selget keelt vajadusest parandada nii spetsialistide oskusi kui ka raviasutuste infosüsteemide kasutajate teadlikkust küberohtudest ja nende vältimisest. Ka juhul, kui administreerimisviga või pahavaraga nakatumine ei too kaasa tõrget raviteenuse kättesaadavuses, on raviasutuse töötajate e-posti kontode ülevõtmine või kolmandate isikute õigustamatu juurdepääs asutuse infosüsteemile tõsine probleem nii patsiendi delikaatsete isikuandmete kaitse kui ka tervishoiuasutuse usaldusväärsuse seisukohast. Just selliste probleemide vähendamiseks on RIA sel aastal pööranud suuremat tähelepanu infoturbe tagatusele Eesti tervishoius – seda nii koolituste, turvatestimiste kui ka teadlikkuse tõstmisega.

JÄRELDUSED

- Elutähtsate teenuste kübersõltuvus kasvab aasta-aastalt, samas ei ole teenuseosutajad piisavalt teadlikud teenuse toimimist ohustavatest riskidest ning riskihinnangud on koostatud ebaühtlaselt ja erineva detailsusastmega. Põhjuseks on nii madal teadlikkus – spetsialistidest kuni juhtkonnani – kui ka oskuste nappus. Õigusruum, mis peab tagama riigi keskse koordineerimise ja ettevalmistuse kriisiolu-

18 Neid sündmusi on lähemalt kajastatud RIA küberturvalisuse teenistuse 2016. aasta märtsi, mai ja novembri kokkuvõtetes: https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html.

kordadeks, on ebapiisav; elutähtsa teenuse toimepidevuse korraldajate (peamiselt ministeeriumite, aga ka kohalike omavalitsuste) panustamine teenuse toimepidevuse tagamisse on sõltuvalt valdkonnast väga ebaühtlase tasemega ning puudub selgus teenustasemetest, mida valdkonniti järgida tuleb.

- Küberohtudele altina paistavad üle ilma silma tervishoiu-, energia-, finants- ja transpordisektor; Eestis eeskätt esimene. Tervishoiuvaldkonna kõrge küberrisk on tingitud mitme asjaolu kombinatsioonist: raviteenuse toimimisest või mittetoimimisest sõltub otseselt inimeste elu ja tervis, raviteenuste osutamine on sõltuv infosüsteemides töödeldavate (aegkriitiliste) andmete kättesaadavusest ning valdkonnas pole infoturbele tähelepanu pööratud. Kõik see muudab tervishoiuteenuse osutajad küberkurjategijatele hõlpsaks sihtmärgiks.
- Tervishoiuteenuste osutamist toetavate teenuste digiteerimist ei saa käsitleda üksnes valdkondliku kokkuhoiukohana. IT-teenus ei ole üheski valdkonnas enam pelgalt tugiteenus, vaid selle olemasoluta ei saa enam ka asutuse põhitegevuses kindel olla. Infosüsteemide tõrgete või küberründe tagajärjel on võimalik raviteenuste katkemine või kättesaadavuse halvenemine, samuti on ohus patsientide terviseandmete konfidentsiaalsus ja terviklikkus. Nende riskide maandamine nõuab nii investeeringuid kui ka kogu personali paremat teadlikkust ning turvalisuse prioriteerimist raviasutuste juhtkonnas. Kuni tervishoiu küberjulgeolekut ei peeta tähtsaks, näeme 2016. aastal toimunutega sarnaseid intsidente veel, ning varem või hiljem mõjutab küberintsident raviteenuse toimimist juba konkreetselt, mitte enam abstraktselt.

RIA SOOVITUSED

Elutähtsa teenuse osutajale

- Kriitilise sidesõltuvusega teenuseosutajate olulisematele objektidele tuleb tagada dubleeritud sideühendused, et välistada sõltuvus ühest sideteenuse osutajast ja ühest füüsilisest taristust.
- Võtta kasutusele abinõud, et tagada elutähtsa teenuse riskianalüüsides ja toimepidevuse plaanides sisalduva tundliku teabe turvaline haldamine ja hoiustamine.

Elutähtsa teenuse toimepidevuse korraldajale ja koordineerijale

- Eristada teenuseosutaja tegevuses elutähtsad teenused neist, mis on vajalikud avalikust huvist või ärilistest eesmärkidest lähtuvalt, ning kehtestada elutähtsatele teenustele konkreetsed toimepidevuse ja käideldavuse nõuded seadusega.
- Kaaluda ühise turvalise elektroonilise keskkonna loomist elutähtsa teenuse riskianalüüside ja toimepidevuse plaanide hoiustamiseks ning dokumendivahetuseks.
- Arvestades elutähtsate teenuste universaalset sõltuvust elektrivarustusest, koostada plaanid prioriteetsete elutähtsate teenuste toimimiseks vajalike tarbimiskohtade varustamiseks pikaajalise elektrikatkestuse puhuks.

- Tagada vajalike ja mõjutatud osapoolte olukorrateadlikkus teenusekatkestustest. Pakkuda vajadusel abi intsidentide analüüsimiseks ning protsesside muutmiseks, et vältida intsidentide kordumist.

Loe lisaks: https://www.ria.ee/public/Kuberturvalisus/Elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf

Tervishoiuteenuse osutajale

- Vältimaks infosüsteemi tõrgetest või küberründest tingitud ohte raviteenuste osutamisele või patsientide delikaatsete isikuandmete lekkimist, on ülioluline tagada kvaliteetne IT-teenus. Selleks soovitame tungivalt investeerida asutuse IT-personali ja -vahenditesse või osta teenust sisse ise või koostöös teiste asutustega. Viimast soovitame kaaluda iseäranis väiksematel tervishoiuasutustel, kel võimalused ise kvaliteetset infoturvet tagada on piiratud.

Loe lisaks: https://blog.ria.ee/kas-tervishoid-on-kuberkurjategijate-lihtsaim-sihtmark/

Allikad, toimijad ja motiivid

Lihtsustatult öeldes on nii riik, ettevõtjad kui üksikisikud küberohtude sihtmärgiks eeskätt kahel lihtsal põhjusel: raha ja mõjuvõim. Küberruum pakub madala riskiga lisavõimalusi nii Eesti suhtes vaenulikele riikidele oma eesmärkide edendamiseks kui ka professionaalsetele kurjategijatele kriminaalse tulu saamiseks.

Välisriikide küberoperatsioonide eesmärk on eeskätt teabehange ja mõjutustegevus

Välisriigid kasutavad digitaalse keskkonna võimalusi üha vilunumalt oma geopoliitilise, sh diplomaatilise, majandusliku või sõjalise positsiooni tugevdamiseks. Riiklikult korraldatud küberoperatsioonid ei toimu juhuslikult, vaid peegeldavad sihtmärkide valikul konkreetse riigi geopoliitilisi huve. Praeguseks on kinnistunud muster ka see, et riikidevahelised pinged leiavad füüsilise keskkonna kõrval väljenduse küberruumis.

Eesti ei saa mööda vaadata asjaolust, et meie idanaaber Venemaa käsitleb NATO allianssi peamise ohuna oma julgeolekule ning kasutab küberruumi rutiinse vahendina oma mõjuvõimu suurendamiseks ja eesmärkide saavutamiseks.[19] 2016. aastal nägime Venemaa hoogustunud ja varjamatut kübertegevust meie liitlaste suunal. Selle markantseim näide oli USA presidendivalimiste kampaania vastu korraldatud mõjutusoperatsioon, mis kombineeris küberründeid, andmete lekitamist ning riiklikult rahastatud propagandat meedias ja sotsiaalvõrgustikes, et tagada valimisedu Vene Föderatsiooni administratsiooni

19 https://www.ft.com/content/6e8e787e-b15f-11e5-b147-e5e5bba42e51; http://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6YOAsHD5v.pdf.

MIS IKKAGI ON APT?

Riikide poolt lähtuvatest küberohtudest rääkides kasutatakse märksõna APT (*Advanced Persistent Threat*). APT rünnete all on alates 2006. aastast tavaliselt mõeldud kindlat tüüpi ohvri (nt riigiasutused) ründamiseks loodud kõrgetasemelist (*Advanced*) ründevahendite komplekti, mille abil tungitakse ohvri infosüsteemi ning omandatakse pikaajaline (*Persistent*) varjatud kontroll seal hoitava ja töödeldava info üle. Tavapäraselt on ründajateks (*Threat*) isikute organiseeritud grupp, kes tegutseb mõne riikliku eriteenistuse huvides.

APT ründekampaaniaid eristatakse ründeviiside iseloomulike tunnuste kaudu. Küberturbeettevõtte FireEye 2014. aastal avaldatud raportis* APT28-ks nimetatud rühmitust seostatakse Venemaa eriteenistustega (täpsemalt Vene Föderatsiooni sõjaväeluure keskasutusega). Muu hulgas olid rünneteks kasutatud „tööriistad" loodud vene keeles ning grupp oli aktiivne tööpäevadel kella 8.00–18.00 Loode-Venemaa ajavööndis.

2017. aasta 10. veebruaril avaldas US-CERT põhjaliku ülevaate APT kampaaniast *Grizzly Steppe,* millega rünnati USA ametiasutusi.**

- Levinuim APT ründeviis on endiselt spetsiaalselt ohvri profiiliga kohandatud õngitsuskirjad. Seega tuleb tundlikku infot käsitlevate riigiasutuste töötajatel olla alati väga tähelepanelik neile saadetud e-kirjade suhtes ning vähimagi kahtluse korral – näiteks juhul, kui kirja sisu, saajate nimekiri või saatja aadress pole päris loogiline – teavitada juhtunust oma asutuse infoturbejuhti.
- APT kampaaniate korraldajad analüüsivad pidevalt rünnete edukust ja muudavad oma ründeviise ja -vahendeid. Seega pole kuigi tõenäoline, et selliseid ründeid oleks ka edaspidi võimalik tõrjuda vaid perimeetrit kaitstes. Ainus lahendus on pidevalt seirata kasutajate käitumist ning otsida ja analüüsida hälbeid tavapärases võrguliikluses.
- Kuigi APT kampaaniate eesmärgiks on enamasti küberspionaaž ning tegutsetakse riiklikes huvides, võivad rünnete toimepanemisega tegeleda ka n-ö eraettevõtjad ja saadud teavet võidakse kasutada kuritegelikel eesmärkidel.

* https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.
** https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf.

suhtes soodsamalt meelestatud kandidaadile.[20] Venemaalt pärinevatest küberrünnetest on hiljuti avalikult teatanud ka mitu Euroopa riiki, nende seas Saksamaa, Prantsusmaa, Tšehhi Vabariik, Rootsi ja Poola.[21] Võime eeldada, et Venemaa kasutab küberoperatsioone käsikäes traditsioonilise mõjutustegevusega vastavalt oma tehnoloogilisele võimekusele, doktriinile ja välispoliitilistele võimalustele.

20 https://www.dni.gov/files/documents/ICA_2017_01.pdf.
21 https://www.theguardian.com/world/2016/nov/29/german-spy-chief-russian-hackers-could-disrupt-elections-bruno-kahl-cyber-attacks; http://www.businessinsider.com/ap-intelligence-agency-russia-trying-to-destabilize-germany-2016-12 ; http://www.france24.com/en/20170219-france-condemns-cyberattacks-targeting-presidential-candidate-macron-points-russia. Vt ka RIA 2017. aasta jaanuari kokkuvõtet: https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html.

Eesti-vastase küberspionaaži peamiseks sihiks on ligipääsu saamine (salastatud) teabele, eeskätt poliitilist otsustusprotsessi, julgeolekut ja riigikaitset – sh NATO tegevust – ning välissuhtlust puudutavale teabele, mille omamine annaks vastaspoolele vajadusel võimaluse mõjutada riigi sisepoliitilist olukorda või rahvusvahelist mainet ning selle kaudu laiemalt ka meie liitlaste otsuseid. Küberspionaaži sihtmärgiks on esmajoones valitsusasutused ning nende töötajad, kellel olulisele teabele ligipääs. Väheolulised ei ole ka ründed, millega püütakse saada ligipääsu elutähtsate teenuste või võtmetähtsusega ettevõtjate infosüsteemidele, kas siis teabehanke (spionaaž, sh majanduslik ja tööstusspionaaž) või sabotaaživõimaluse loomise tarbeks. Mullused Venemaa eriteenistustega seostatud küberoperatsioonid mujal maailmas annavad aimu küberrünnete märkimisväärselt laienenud kasutusalast viimase kümnendi jooksul: lisaks teabe hankimisele ja teenustele ligipääsu blokeerimisele on need tulusad ka teenuste endi toimimise katkestamiseks või avalikkuse meelsusega manipuleerimiseks.

Välisriikide toetatavatele küberoperatsioonidele on iseloomulik, et ründajate huvi on pikaajaline, mistõttu avastamist püütakse kõigiti vältida. Spionaažijuhtumeid avastatakse harva ning reeglina alles hulk aega pärast kordaläinud sissemurdmist, sest süsteemile ligi pääsenud „agendi" eesmärk on koguda ja edastada teavet pika aja jooksul või saavutada positsioon tundlikku teavet töötlevates süsteemides ja jääda ootama edasisi võimalusi. Neil põhjustel on selle kategooria juhtumite koguhulka keeruline hinnata. Selge on ka see, et katseid kriitilistele süsteemidele ligi pääseda tehakse palju enam, kui neid õnnestub. Ka eespool kirjeldatud VKG juhtumi puhul on põhjust arvata, et rünne korraldati välisriigi toel.

Küberkuritegevus

Digitaalses keskkonnas tegutseb väga erineva tasemega kurjategijaid – lihtsate petukirjade levitajatest kuni oskuslike ja oma ründeid hoolikalt planeerivate infosüsteemikaaperdajateni välja. Küberkurjategijate oskused arenevad pidevalt, kohanedes nii tehnoloogiliste muutuste kui turuolukorraga, mis on näha ka seekordses raportis kirjeldatud lunavara- ja õngitsusrünnete mustrist. Samas ei ole küberkuritegevus enam üksnes väheste valitute pärusmaa, vaid soovitud „teenust" on võimalik kurjategijatelt osta ka neil, kel endal vajalikke oskusi ei ole.

Erinevalt riiklikku päritolu rünnetest, mis peegeldavad riikidevahelisi pingeid ja huvisfääre, ei ole küberkurjategijatel samaväärseid geograafilisi eelistusi: globaalse küberkuritegevuse jaoks on iga digiseadmete kasutaja potentsiaalselt huvipakkuv sihtmärk, olgu siis võimaluse tõttu saada temalt raha või rahalist väärtust omavat teavet või kasutada tema seadet hüppelauana teiste isikute või ühenduste ründamiseks. Õngitsemisründe kaudu välja petetud teavet, nagu krediitkaardiandmed, kasutajanimed ja paroolid, kasutatakse arvutikelmuste toimepanemiseks või müüakse kuritegelikele ühendustele hinnakirja alusel edasi. Pahavaraga nakatatud arvutit on võimalik kasutada teenusetõkestusrünneteks või nendega ähvardamiseks väljapressimise eesmärgil. Automatiseeritud rünnete sihtmärgiks

on ka tavaline arvutikasutaja, kes end küberkurjategijate jaoks huvipakkuvaks ei pea – tema arvuti vananenud tarkvara ja viirustõrje puudumist kasutatakse ära teiste isikute ründamiseks.

Küberkuritegevus võimaldab tulu teenida ka väljapressimise abil. Nii krüptolunavara, teenusetõkestusründeid kui ka andmevargust kasutatakse selleks, et nõuda ohvrilt raha – enamasti virtuaalvääringus Bitcoinis – ründe lõpetamiseks või andmete avaldamisest hoidumiseks. Niisuguse väljapressimiskirja sai 2016. aastal ka üks Eesti põhiseaduslik institutsioon, keda ähvardati nõude tasumata jätmise korral teenusetõkestusrünnetega.

Olukorras, kus küberkuritegevusest saadava tulu ja sellega kaasneva riski vahel haigutab asümmeetria, ei ole küberkuritegevuse lokkamine üllatus. EUROPOLi 2016. aasta küberkuritegevuse ohuhinnangu väitel ületab mõnes ELi riigis küberkuritegude arv praeguseks juba traditsiooniliste kuritegude oma.[22] Eestis on registreeritud küberkuritegude iga-aastane juurdekasv alates 2012. aastast olnud 5–12% – seda olukorras, kus varavastaste kuritegude hulk tervikuna on samal perioodil kahanenud pea 35%.[23] Võib eeldada, et suur osa küberkuritegudest jääb endiselt avastamata ja registreerimata. Teisalt on ilmne, et kurjategijad jälgivad oma tegevuses hoolikalt riski ja tulu suhet, mistõttu teenuste turvaline arhitektuur (sh tugev elektrooniline identiteet), selge õigusruum ja õiguskaitseasutuste tõhus reageerimine küberkuritegudele vähendavad Eesti atraktiivsust küberkuritegevuse sihtkohana.

JÄRELDUSED

- Enamik küberkuritegusid – ka Eestis registreeritud – on kelmused, kus kurjategijad kasutavad ära ohvri ahnust või kergeusklikkust. Pettuse ohvriks langenutel on hiljem tihti endalgi raske uskuda, kuidas nad kandsid raha teadmata kuhu, saamaks kätte võidusummat loteriis, kus nad kunagi osalenud ei olnud.
- Ohtude realiseerumisel mängib rolli süsteemide puudulik turvatase ja kasutajate hooletus, oskamatus või madal teadlikkus.

22 Internet Organised Crime Threat Assessment (IOCTA) 2016.
23 http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_2015.pdf.

RIA SOOVITUSED

- Kübermaailmas suheldes tuleb arvestada võimalusega, et suhtluspartner pole see, kellena esineb. Tasub olla ettevaatlik ja umbusklik. Raha, oma isikuandmeid või muud olulist teavet tohib kuhugi saata vaid siis, kui ollakse teise poole isikus ja kavatsustes kindel.
- Olenemata sellest, kas kannatanu on teenusepakkuja või lõpptarbija, tuleb küberkuritegevuse tõttu kahju saamisel alati teavitada politseid (cybercrime@politsei.ee).

Terrorism, ideoloogilised ja juhuslikud toimijad

Kübertaristu kaudu ei ole maailmas seni terrorirünnakuid toime pandud; terrorirühmitused nagu Islamiriik kasutavad internetti peamiselt propaganda ja värbamise vahendina. Siiski võib terrorirünnakute taustal täheldada kõrgenenud küberrünnete ohtu, mis tingimata ei tarvitse olla terroristlikku päritolu – näiteks terrorirünnakutele Brüsselis 2016. aasta märtsis järgnes Belgias küberrünnete laine.[24] Sellele vaatamata on Eesti koostöös siseriiklike ja välispartneritega teadvustamas vajadust ennetada piisavate rahaliste vahendite ja kompetentsi koondumist terrorirühmituste kätte ning hoida ära ründeid elutähtsa taristu vastu, mis võiksid põhjustada suurt kahju tsiviilelanikkonnale ning destabiliseerida oluliselt riiki tervikuna.

Rahvusvaheliste pingete taustal aktiveeruvad ka poliitilistel ja ideoloogilistel motiividel tegutsevad küberaktivistid, kelle tegevusampluaa sisaldab tüüpiliselt teenusetõkestusründeid ja veebilehtede näotustamisi propaganda eesmärgil. Koostööd küberaktivistide ja küberkurjategijatega võivad teha ka Eesti suhtes vaenulikud eriteenistused ning sellisest „avaliku ja erasektori koostööst" saavad kasu mõlemad. See muudab Eesti jaoks olukorra järjest keerukamaks, kuna selgeid vastuseid peaaegu ei ole: enam ei saa kindel olla, kas Eesti elutähtsa infosüsteemi vastu justkui rahalise kasu eesmärgil suunatud rünnak pole tegelikult kurjategijatelt tellitud mingi hoopis muu kriteeriumi alusel.

Ning viimaks on küberruum lihtsalt tehnoloogiline keskkond, mida kasutavad ja väärkasutavad väga erineva oskuste taseme ja huviga isikud, sageli tagajärgedele mõtlemata. Küberrünnete motiiviks võib olla uudishimu, väljakutse otsimine, küberkiusamine jmt. Andmete või seadmete ebaseadusliku manipuleerimise ohvriks sattumise korral, eriti kui sellega on kaasnenud rahaline kahju, tasub alati teavitada politseid.

24 http://cytegic.com/wp-content/uploads/2016/02/DyTA-Intelligence-Report-March-2016.pdf.

Eesseisvad väljakutsed

Võimalik on küber- ja infooperatsioonide hoogustumine e-riigi vastu

CERT-EE kümne tegevusaasta jooksul oleme Eesti küberruumis näinud küberturbejuhtumite arvu pidevat kasvu ning vaevalt 2017. aasta ses osas erandlik tuleb. Lisaks küberaktiivsuse ootuspärasele orgaanilisele kasvule seisab Eestil sel aastal ees mitu olulist sündmust, mis esitavad väljakutse ka riigi digitaalse taristu turvalisele ja tõrgeteta toimimisele.

Juulis algava Euroopa Liidu Nõukogu eesistumisega seoses panustab RIA oluliselt üldisesse küberturvalisusse. Ettevalmistused selleks algasid juba 2016. aasta algusest. Eesistumise läbiviimiseks vajalike tehniliste lahenduste kasutuselevõtt, sh turvaliste kommunikatsioonilahenduste tagamine ametnikele

ja külalistele, nõuab ladusat koostööd paljude ametkondade vahel. Nagu on näidanud meie lõunanaabri Läti 2015. aasta kogemus, suureneb eesistumisperioodil riigile küberruumist tulenev surve ja rünnakute arv. Seetõttu arvestame võimalusega, et eesistumisega seotud suursündmuste toimumine muudab Eesti atraktiivsemaks sihtmärgiks võõrriikide luureteenistustele ja küberkurjategijatele, ent ka poliitilist sõnumit edastada soovivatele küberaktivistidele.

Nii eesistumise läbiviimiseks vajalike tehniliste lahenduste kasutuselevõtt kui ka Eesti IKT-taristu suurenenud atraktiivsus küberrünnete sihtmärgina nõuavad ametkondadelt tavapärasest oluliselt kõrgemat valmisolekut ohtude ennetamiseks. Selle valmisoleku parandamiseks on RIA alates 2016. aastast viinud läbi sarja infoturbekoolitusi nii riigikogu kantselei, riigikantselei kui ka ministeeriumite töötajatele, et tõsta ametnike teadlikkust aktuaalsetest küberohtudest ja infoturbe põhimõtetest.

On teisigi põhjuseid, miks alanud aastal võib oodata küber- ja infooperatsioonide hoogustumist Eesti vastu üldiselt ning Eesti e-riigi vastu konkreetselt. Laiemalt on need seotud eeskätt Venemaa suurenenud aktiivsusega oma strateegiliste huvide edendamisel. On hästi teada, et Venemaa sihiks on kehtiva julgeolekuarhitektuuri asendamine ning selle eesmärgi nimel kasutab ta muuhulgas mõjutusoperatsioone, millega püüab õõnestada avalikku usaldust riikide demokraatlike protsesside ning riigivõimu institutsioonide usaldusväärsuse vastu.[25]

2016. aastal USA presidendivalimiste vastu toimepandud küberründed olid osaks infooperatsioonist, kus demokraatliku partei infosüsteemidesse sissemurdmisse ja varastatud sisedokumentide avaldamise eesmärk oli avalikkuse meelsusega manipuleerimine, et tagada valimisedu eelistatud kandidaadile. Sarnaselt on Euroopa Liidu riikides eesseisvate valimiste eel drastiliselt kasvanud agressiivne riigivastane küberspionaaž ja -ründed kombineerituna infooperatsioonidega. See näitab valmisolekut kasutada USA valimiste käigus saadud õppetunde ka Euroopa riikide vastu.

Venemaa infooperatsioonide hoogustumisest meie liitlaste seas ei ole puutumata jäänud ka Eesti[26] ning pole põhjust oodata, et küberründed Eesti puhul sellest valemist välja jääksid. Vastaspool võib leida 2017. aastal eesseisvates sündmustes soodsa võimaluse propagandistliku punktivõidu võtmiseks. Tänavu aprillis möödub kümme aastat Eestit 2007. aastal tabanud massilistest küberrünnakutest, mis järgnesid pronkssõduri monumendi teisaldamisele Tallinnas. Siia saabuvad NATO liitlasvägede üksused on nii küberluure kui propaganda tähelepanu objektiks, nagu on osutanud teabeamet. Samuti toimuvad sügisel esimesed haldusreformijärgsed kohalike omavalitsuste volikogude valimised, kus esmakordselt võivad kandideerida ka riigikogu liikmed. Nende sündmuste ümber on oodata ka kübertegevuse aktiveerumist.

25 Venemaa infosõja doktriini kohta vt Richard Weitz, „Silmitsi Venemaa hübriidohtudega". Diplomaatia nr 135, november 2014. https://www.diplomaatia.ee/artikkel/silmitsi-venemaa-hubriidohtudega/. Pikemat analüüsi vt Ants Laaneots, „Putini Venemaa doktriin". Sõdur, 05/2014. https://issuu.com/sodur/docs/sodur0514_veeb.

26 Vt nt https://www.propastop.org/, kes jälgib Eesti-vastase propaganda levikut meedias.

Samuti on võimalik, et riigi digitaalse taristu usaldusväärsus ise saab mõjutusoperatsioonide sihtmärgiks; valimiste kontekstis võib see eeskätt tähendada e-valimiste usaldusväärsuse ründamist.

JÄRELDUSED

- Riigile poliitiliselt oluliste sündmuste, sh valimiste kontekstis suureneb oht agressiivseks riigivastaseks küberspionaažiks, -rünneteks ja mõjutustegevuseks. Pole põhjust arvata, et Eestis sügisel toimuvad kohalike omavalitsuste volikogude valimised jääksid sellisest tegevusest puutumata. Võime eeldada, et küberründeid kasutatakse ja tehakse seda info- ja mõjutusoperatsioonide vahendina.
- Eesti asutused ja turvaekspertide kogukond on e-hääletuse maksimaalse turvalisuse tagamiseks teinud koostööd alates esimestest internetivalimistest 2005. aastal ning see koostöö jätkub ka sel aastal toimuvate valimiste eel ja ajal.

RIA SOOVITUSED

- Eesti e-riik ja e-valimised, sealhulgas valimisprotsessi turvalisus, on hästi kaitstud. Hüpoteetilistesse ohustsenaariumitesse, mis ei arvesta Eesti e-valimiste korraldusega ning kannavad teiste riikide valimissüsteemide riske Eestile analüüsita üle, tasub suhtuda kriitikameelega. Samamoodi ei tasu tõsiselt võtta abstraktseid stsenaariume „e-valimiste riskidest" üldiselt.
- Konkreetse e-valimiste turvalisusega seotud oletatava kitsaskoha või murega tasub alati pöörduda vabariigi valimiskomisjoni või RIA poole (cert@cert.ee).
- Samamoodi, nagu valija on harjunud pöörama tähelepanu oma hääletamise turvalisusele traditsioonilise hääletamise puhul, on e-hääletamise turvalisuse puhul oluline ka valija enda hoolikus.

Digitaalne innovatsioon mõjutab digitaalse riigi toimimist ja turvalisust

Infosüsteemid on lahutamatu osa Eesti riigist. Meie seadused eeldavad registreid ja äriprotsessid iseteenindust. Infosüsteemide muutused tähendavad seetõttu ka suuremaid või väiksemaid muutusi riigi toimimises – ning innovatsioon tarkvara ümber tähendab seega vältimatult ka innovatsiooni riigi kui sellise juures. Igasugune innovatsioon hõlmab endas aga olemuslikult riske.

Eesti digitaalse riigiga on seotud kahte liiki riskid. Esiteks sõltub meie e-teenuste tõrgeteta töötamisest riigi ja ühiskonna harjumuspärane toimimine. Seetõttu peab e-riik suutma kaasas käia muutuvate ootustega teenuste kasutusmugavusele, aga ka tagama, et needsamad teenused oleksid kaitstud arenevate ohtude eest. Teisalt tuleb arvestada ka sellega, et ühe või teise tehnoloogilise uuenduse riskide realiseerumisel ei satu löögi alla mitte ainult konkreetne süsteem, vaid kogu riigi julgeolek.

RIA lähtub teenuste käideldavust puudutavates arendustes turvalise disaini põhimõttest. See üldine

arenduspõhimõte kehtib ka tehnoloogia arengust tingitud nüüdisajastuste juures, mis puudutavad Eesti e-riigi alustalasid, nagu isikutuvastuseks kasutatava elektroonilise identiteedi (eID) ja riigi infosüsteemide andmevahetuskihi X-tee lahendused.

Eesti e-riigi toimimine sõltub suures osas teenuste usaldusväärsusest, mis eeldab tugevate krüptograafiliste vahendite kasutamist. Usaldusväärne elektrooniline identiteet muutub digitaalses ühiskonnas aina tähtsamaks: on ülioluline, et teaksime kindlalt, kes kellena elektroonses maailmas esineb. Eesti on elektroonilise identiteedi osas olnud teerajaja ning meid on sageli toodud järgimist väärivaks eeskujuks. Ent tugeva elektroonilise identiteedi tagamine toob kiiresti muutuvas kübermaailmas kaasa ka omajagu väljakutseid.

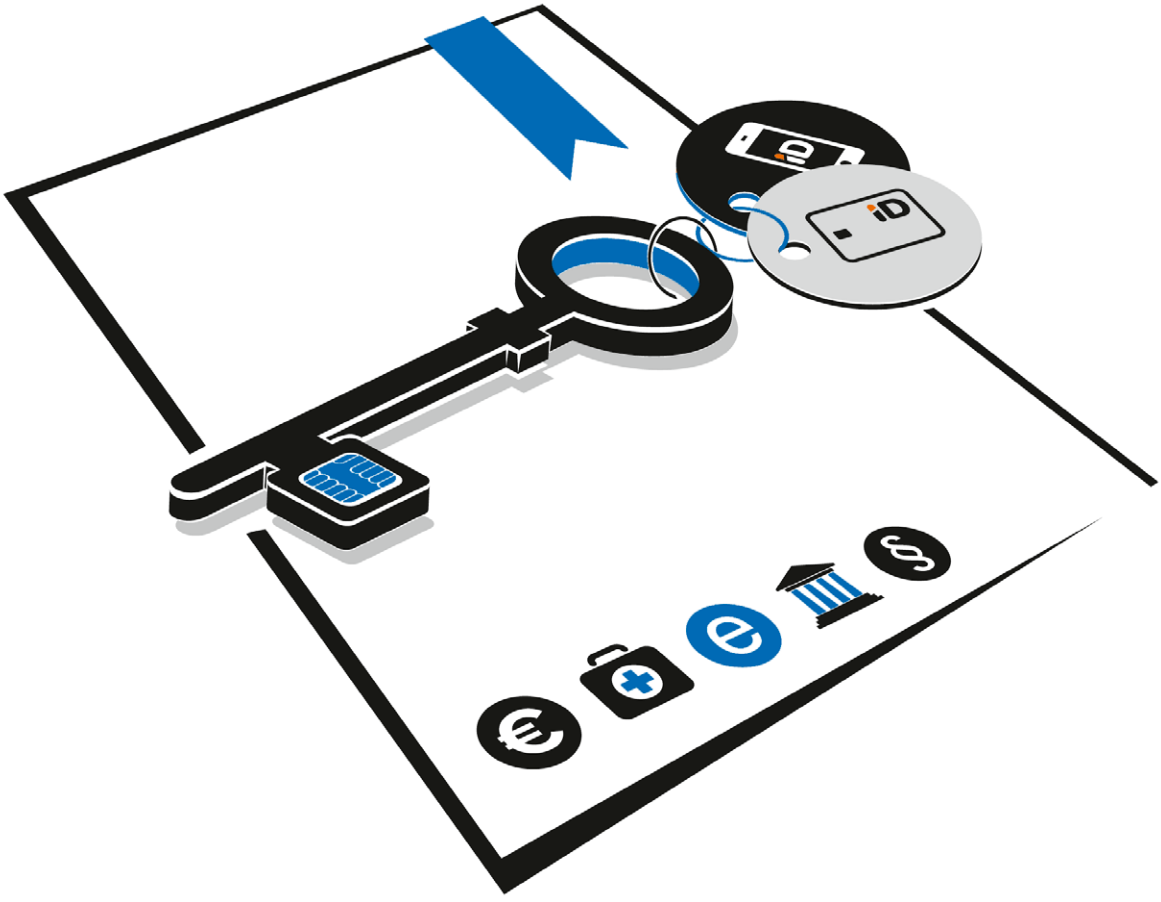
Üheks neist on muutused õiguskeskkonnas. Möödunud aasta veebruaris USAs lahvatanud FBI ja Apple'i vaidlus selle üle, kas tehnoloogiahiid peaks looma n-ö tagaukse, et võimaldada julgeolekuasutusel minna mööda seadme turvasätetest ja saada ligipääs telefonis olevatele andmetele, tõstatas uuesti debati tugeva krüptograafia üle. Kuna USA õigussüsteem põhineb pretsedendiõigusel, oleks FBI nõude rahuldamine sisuliselt tähendanud USA õiguskaitseasutustele antavat õigust nõuda tagauste loomist ka edaspidi – ning seeläbi ka rahvusvahelisele turule lastavate seadmete krüptograafia murdmist.

Seisukohad krüptograafiavaidluses lahknevad ka Euroopa riikide vahel. Madalmaade valitsus avaldas 2016. aasta jaanuaris krüptograafiat toetava seisukoha, mis rõhutas tugeva krüptograafia olulisust kodanike, riigi ja majanduse kaitsel ning teatas, et hoidub krüptograafiat piiravate õigusnormide kehtestamisest.[27] Ühendkuningriigi sügisel vastu võetud jälitustegevuse seadus (*Investigatory Powers Act)* seevastu annab ametkondadele laialdased õigused internetiliikluse jälgimiseks ning juurdepääsuks kasutaja andmetele, muu hulgas võimaldades nõuda teenuseosutajatelt krüpteeringu kõrvaldamist või tagauksi teenustes. Tugeva krüptograafia piiramist terrorismivastases võitluses on toetanud ka Prantsusmaa ja Saksamaa.[28]

Eesti seisukohalt on tugev krüptograafia oluline riigi e-teenuste usaldusväärsuse garantii, sest rohkemal või vähemal määral tuginevad tugevale krüptograafiale (ID-kaart) kõik riigi ja ka paljud erasektori pakutavad e-teenused. Pikemas perspektiivis vähendaks tagauste loomine seega ka usaldust Eesti e-riigi vastu – usaldus on aga Eesti jaoks ülioluline väärtus. Seetõttu ei ole Eesti toetanud riigi e-teenustesse tagauste loomist, ning RIA eesmärk ja ülesanne on jätkuvalt tagada Eesti elektroonilise identiteedi kõrge usaldusväärsus.

27 https://www.tweedekamer.nl/downloads/document?id=b12f7a99-2615-441b-89a1-ab42631715a5&-title=Kabinetsstandpunt%20encryptie.pdf.

28 https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/.



2015. aastal selgus, et suurel hulgal Eestis välja antud ID-kaartidest on isiku tuvastamiseks kasutusel sellised sertifikaadid, mille tunnustamise plaanivad suuremad tarkvaratootjad lõpetada või on juba lõpetanud. Selleks et tagada Eesti ID-kaardi sertifikaatide jätkuv vastavus tunnustatud standarditele, alustasid politsei- ja piirivalveamet (PPA) ja RIA 2015. aastal koostöös ettevalmistusi ID-kaardi sertifikaatide vahetamiseks. Möödunud aasta märtsis algas ID-kaardi sertifikaatide uuendamine Eesti ID-kaardi baastarkvara kaudu: see tähendab, et isikud, kelle ID-kaardi sertifikaadid vajavad uuendamist, saavad seda teha kodust või kontorist lahkumata.

2016. aasta jooksul uuendas oma ID-kaarti rohkem kui 70 000 kaardiomanikku. Sertifikaatide automaatse uuendamise lahendus kehti kättesaadavaks 2017. aasta esimestel päevadel ja pärast seda on uuendatud umbes 10 000 kaarti nädalas. 2019. aastal peaks käibele tulema ka uus ID-kaart.

MIKS ON SERTIFIKAATIDE UUENDAMINE VAJALIK?

Arvutusvõimsuse kasvades muutuvad varasemad krüptograafilised algoritmid (kõnealusel juhul SHA-1) haavatavaks, sest hästi rahastatud ründajatel tekib võimalus neid murda. Esialgu on tegemist küll vaid teoreetilise haavatavusega, kuid pikemas perspektiivis oleks senistele algoritmidele truuks jäädes ohustatud Eesti avaliku võtme infrastruktuur, mis tagab inimese turvalise tuvastamise ID-kaardi, mobiil-ID või digi-ID abil.

Selleks et ohu realiseerumist ennetada, tuleb vananevad krüptograafilised algoritmid asendada tugevamatega: tavakasutaja jaoks tähendab see vajadust asendada ID-kaardi kiibil olevad sertifikaadid sellistega, mis põhinevad tugevamal krüptograafial (SHA-2). Niisuguseid ID-kaarte on ligikaudu miljon ja need on väljastatud enne 2016. aasta 1. märtsi, mil uutele kaartidele hakati väljastama SHA-2 algoritmil põhinevaid lõppkasutaja sertifikaate.

Tarkvaratootjad on võtnud kindla suuna lõpetada SHA-1 räsifunktsiooni toetamine, sest selle n-ö murdmise tõenäosus on muutumas liiga suureks. Asjaolu, et arvutusvõimsuse kasvades ning krüptoanalüütilise teadmuse täiustudes muutuvad vanemad krüptograafilised algoritmid tasapisi ebaturvaliseks, on krüptograafia seisukohalt tavapärane areng.

Mobiil-ID tuleviku osas veel selget lahendust ei ole. Teadupärast on nutiseadmete üha universaalsem kasutus õhutanud telefoni integreeritud eSIM-toodete arengut, Eesti mobiil-ID teenus põhineb aga SIM-kaardil paiknevatel võtmetel, mis eeldab füüsilise SIM-kaardi olemasolu. Integreeritud eSIM-i puhul kardetakse, et pole enam kohta, kus salajasi krüptovõtmeid hoida. Nii Apple'ilt kui Samsungilt on eSIM lahendusega toodete avalikustamist oodatud, ent praeguseks neid veel müüki lastud ei ole ning ka mobiilsideoperaatorid ei ole veel valmis üksnes eSIM-iga telefone oma võrgus teenindama. Seetõttu säilib SIM-kaart esiotsa suure tõenäosusega ka uutel eSIM-telefonidel ning sestap toimib edasi ka Eesti mobiil-ID. On teada, et tehnoloogiliselt on võimalik mobiil-IDd kasutada ka eSIM-iga, ent sel juhul on ebaselge, kuidas lahendada eIDASe tasemel seadmete sertifitseerimine ning siduva digitaalallkirja taseme säilitamine. RIA jälgib turu arenguid aktiivselt.

Väljakutseks on jätkuvalt ka ID-kaardi kasutamine arvukates veebilehitsejates, millest kõikidel ei ole tehnoloogilist võimekust toetada kiipkaarte. Suurimaks mureks on Windows 10 Edge veebilehitseja, mille puhul tavapärane lahendus kohalike arendajate loodud lisandprogrammi ehk plugina näol ei ole võimalik ning lootma peab Microsofti toele. Seesuguste probleemide sageda esinemise tõttu on mõtlema hakatud uue nn veebipluginate arhitektuuri peale.

JÄRELDUSED

- On oluline mõista, et ei innovatsioonist loobumine ega digisõltuvuse vähendamine ole lahenduseks olukorras, kus infosüsteemidest saadavad otsesed ja kaudsed hüved meie riiki praegusel määral toetavad. Seega tuleb panustada riskide juhtimisse,

kaaludes hästi läbi tehnoloogilised muutused, ning pöörata turvalisusele tähelepanu juba teenuse disainifaasis (*security by design*).

- RIA hindab pidevalt nii tehnoloogia arengust kui rahvusvahelisest geopoliitilisest keskkonnast tulenevaid mõjusid Eesti e-riigi toimimisele ja turvalisusele. Peame olema kohanemisvõimelised (turvastandardite ja õiguskeskkonna nüüdisajastamine), aga ka rääkima kaasa arengutes, mis on Eesti e-riigi toimimise seisukohast fundamentaalselt olulised (tugeva krüptograafia säilimine terrorismivastase võitluse kontekstis).

AUTONOOMSETE RÜNDE-TEHNOLOOGIATE TEKE

Möödunud aasta näitas, et arvutivõrgud ja infosüsteemid muutuvad aina targemaks ja autonoomsemaks. 2016. aasta DARPA kübervõistlus* pani esmakordselt omavahel võistlema autonoomsed süsteemid. Arvutivõrgud otsisid üksteise nõrkusi ning paikasid iseeneste omi – autonoomselt, ilma inimjuhtimiseta. Praegu on see oskus vaid maailma tipp-teadusasutuste käes, kuid võib eeldada, et varem või hiljem jõuab see häkkerite kätte ja päris ründesüsteemidesse.

* http://archive.darpa.mil/cybergrandchallenge/

RIA KTT tegevused 2016

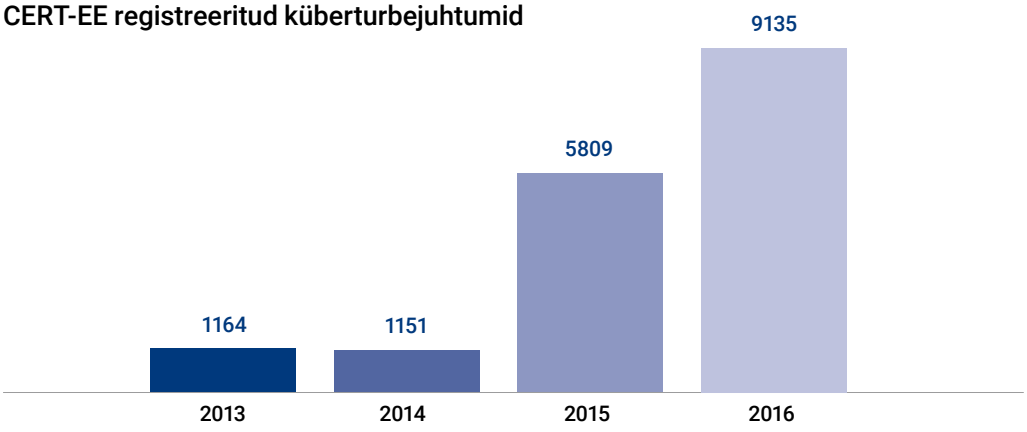
RIA küberturvalisuse teenistuse tegevus põhineb kolmel kesksel suunal: küberturbeintsidentide ennetamine ja lahendamine, elutähtsate teenuste infosüsteemide ja riigi infosüsteemi turvariskide haldamine ning Eesti küberturvalisuse kogukonda – eeskätt elutähtsa teenuse osutajate ja riigiasutuste turvajuhte – hõlmava võrgustiku koondamine, et edendada nendevahelist infovahetust ning kõrget kompetentsi.[29] Nende kolme põhisuuna toetamiseks korraldame hulka valdkonnaüleseid tegevusi. Siia kuuluvad avalikkusele ja spetsialistidele suunatud teavitustegevus, õppuste korraldamine ja toetamine, arendus- ja uurimistegevus ning ka küberturvalisust ja -julgeolekut tagava õigusruumi arendamises kaasalöömine ja rahvusvaheline koostöö. See peatükk teeb kokkuvõtte teenistuse olulisematest tegevustest 2016. aastal.

29 Riigi Infosüsteemi Ameti põhimäärus (majandus- ja kommunikatsiooniministri 25.04.2011 määrus nr 28; RT I, 29.12.2016, 14) § 13.

Küberturbeintsidentide ennetus ja lahendamine

Küberturvalisuse teenistuse intsidentide käsitlemise osakond CERT-EE korraldab küberintsidentide seiret ning tuvastab, jälgib ja lahendab Eesti arvutivõrkudes toimuvaid turvaintsidente. Intsidentide seire ja lahendamise kõrval on oluline tegevussuund küberturvalisuse arendamisel olukorrateadlikkuse pidev parandamine Eestis – seda nii tehnilisel kui strateegilisel tasandil.

CERT-EE registreeritud küberturbejuhtumid



Eesti küberruumi ööpäevaringne pidev seire on viimase aasta jooksul andnud meile senisest palju parema arusaama Eesti küberruumis toimuvast. Ühtaegu on oluliselt kasvanud ka küberintsidentide arv, mida tuvastame ja lahendame.

Olukorrateadlikkuse võime jätkuv arendamine on vajalik nii ressursside kindlustamise kui ka õigusruumi arendamise kaudu. Töötame selle nimel, et küberturvalisuse intsidentide tuvastamine ja seire, analüüs, riskide hindamine ja järelevalve, samuti ohuhinnangute alane ja teavitustegevus ning turvareeglistike loomine toimiksid ühtse süsteemina.

CERT-EE AVALIKUKS KASUTUSEKS MÕELDUD TEENUSED JA TÖÖRIISTAD

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).

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

Riskihaldus

Riskihalduse valdkonna tegevus on eeskätt suunatud avaliku sektori ja elutähtsate teenuste osutajate turvariskide teadvustamisele ja haldamisele. Koostöös elutähtsate teenuste osutajatega viisime möödunud aastal läbi infosüsteemide turvatestimisi, et anda ettevõtetele parem ülevaade nende võimalikest IT-haavatavustest ja -riskidest. Samuti konsulteerisime intsidentide ilmnemisel ja neile reageerimisel elutähtsate teenuste osutajaid, korraldasime valdkonnapõhiseid infopäevi ning teabevahetust. Võimalust mööda kaasame elutähtsate teenuste osutajaid ka riigisisestele ja rahvusvahelistele küberõppustele.

Riigi infosüsteemide turvalisuse tõstmisel oleme seadnud selge sihi, et riigiasutuste ja kohalike omavalitsuste andmekogude pidamisel kohustuslikku infosüsteemide turvameetmete süsteemi ISKE-t tõepoolest ka rakendataks. Selleks oleme lihtsustanud ISKE rakendamise korraldust, tegemata samas järeleandmisi turvanõuete sisulises tasemes. Lisaks ISKE portaali[30] avamisele 2015. aastal korrastasime möödunud aastal ISKE sisu, mille tulemusel vähenes ISKE maht hinnanguliselt viiendiku võrra. Alustatud töödega jätkame alanud aastal ning selle raames kirjutame teksti konkreetsemaks ja paremini hoomatavaks. Koos 2017. aasta alguses kehtestatud ISKE uue versiooniga muutsime ka nii rakendus- kui auditeerimisjuhendit. ISKE tööriista arendamiseks korraldame lähiaastatel hanke, et ehitada üles lahendus, mis lihtsustab rakendaja tööd, annab parema ülevaate infovaradest ja nendevahelistest seostest ning võimaldab ladusamat aruandlust.

2016. aasta esimeses pooles hindas ISKE töörühm ISKE kui riigi infosüsteemi kindlustava süsteemi jätkusuutlikkust. Alternatiivsete riskihalduspõhiste metoodikate kaalumine viis järeldusele, et ISKE on optimaalne metoodika avaliku sektori asutustele ning üleminek mõnele muule samaväärset turvalisust tagavale metoodikale ei oleks rakendajale vähem koormav, vaid tooks kaasa lisakulu. Seega oleme võtnud suuna infoturbereeglistike ajakohastamisele ja sellele, et tagada reeglite täielik sobivus Eesti oludesse. Rohkem tuleb arvestada infosüsteemide ja teenuste omavahelist ristsõltuvust ning era- ja riigisektori põimunud vastutust ühiskonna toimimise eest. ISKE arendamine peab muutuma regulaarseks, pidevalt toimuvaks protsessiks, milleks tuleb tagada nii raha kui ka toetav õiguslik ja administratiivne raamistik.

Infoturbemeetmete rakendamise üle teeb järelevalvet järelevalve talitus, kes kontrollib ISKE auditite läbiviimist, selgitab välja riske ja juhib tähelepanu puudustele. Seadustes[31] sätestatud järelevalvemenetluse kõrval on järelevalve talitusel ka muid tegevusi, mis ei pruugi kulmineeruda menetlusega, kui soovitud tulemus on võimalik saavutada väheminvasiivsete meetoditega. Samuti pöörab

30 https://iske.ria.ee/.

31 Avaliku teabe seadus (AvTS), hädaolukorra seadus (HOS), elektroonilise side seadus (ESS) ning möödunud aastast ka E-identimise ja e-tehingute usaldusteenuste seadus (EUTS).

talitus tähelepanu ennetavale tegevusele (teadlikkuse tõstmine, ISKE rakendajate nõustamine jms), et aidata ära hoida võimaliku kahju tekkimist.

Riigi infosüsteemi turvalisuse korraldamiseks ja arendamiseks toimuvad regulaarselt valdkondlikke eksperte koondava turvajuhtide komisjoni koosolekud. Selle kaudu koordineerime turvajuhtide tegevust ja vahendame infoturbe korraldusega seotud parimaid praktikaid.

Valdkonnaülesed tegevused

Teadlikkuse tõstmine ja koolitused

RIA 2016. aasta teavitustegevused olid ennekõike suunatud lõppkasutajate teadlikkuse kasvatamisele. Oma kodulehe ja sotsiaalmeediakanalite kaudu andsime praktilisi tegevusjuhiseid nii krüptolunavara vältimiseks, e-posti kontode kaitsmiseks kui ka sotsiaalmeedias varitsevatest ohtudest hoidumiseks. Eraldi avaliku kommunikatsiooni suunana käsitlesime tugevama krüptograafia kasutuselevõtmist riiklikes isikutuvastusvahendites: nii juhendasime eri aegadel kasutajagruppide kaupa, kuidas ID-kaartide, elamisloakaartide ja digi-ID dokumentide (ka e-residendi kaardi) krüptograafilist sisu kauguuendamise teel asendada.[32] Dokumente uuendas eelmise aasta jooksul enam kui 70 000 inimest.

Meedia kajastas RIA tegemistest X-tee kasutuselevõttu Soomes, samuti tunti huvi andmekogude piiriülese ristkasutuse vastu. Tähelepanu pälvisid ohud sotsiaalmeedias ja krüptolunavaraga nakatumised. Sügise hakul kajastati Dropboxi andmeleket, kuna see puudutas ka mitmeid kõrgeid riigiametnikke. Oktoobris aset leidnud esemevõrgu seadmete rünnaku ajal USA teenusepakkujate vastu selgitasime Eestis rünnaku uudset iseloomu ja mõju ulatust. RIA blogis avaldame pikemaid kirjutisi, selgitusi ja suuniseid küberturvalisuse teemadel.

2016. aastal viisime läbi sarja koolitusi küberturvalisuse alase teadlikkuse tõstmiseks, keskendudes eeskätt kahele sihtgrupile: elutähtsate teenuste osutajad ning riigi ja kohalike omavalitsuste teenistujad. Elutähtsate teenuste osutajate seas olid 2016. aastal esmatähtsad meditsiinivaldkonna ja energiatööstuse ettevõtete töötajaskonna koolitused; meditsiinitöötajate koolitustest võttis osa ligikaudu 400 inimest. Ühtlasi alustasime mullu Euroopa Liidu eesistumisega seoses ka küberturbeteadlikkuse tõstmise koolitustega eesistumisega seotud riigiametnikele.

Infoturbehalduse koolitusel või sissejuhataval infoturbeteadlikkuse koolitusel käis üle 300 inimese. 2017. aastal jätkame koolitustega ja laiendame sihtgruppi, hõlmates ka riigiasutuste ning elutähtsat teenust osutavate ja elutähtsat teenust korraldavate asutuste võtmeisikud, sh organisatsioonide keskastme- ja tippjuhid.

32 Tugevamale krüptograafiale üleminekust saab lugeda elektroonilist identiteeti kajastavast alajaotusest.

Hädaolukorraks valmisolek ja õppused

RIA üks põhiülesandeid on tagada valmisolek võimalikeks ulatuslikeks küberintsidentideks. Et tagada üleriigiline koordineeritud valmisolek hädaolukorraks ning hädaolukorra kiire ja tulemuslik lahendamine, uuendas RIA koostöös partnerasutustega ulatusliku küberintsidendi hädaolukorra plaani, mille valitsus kinnitas 2016. aasta mais.

Olulisemaks muudatuseks võrreldes varem kehtinud plaaniga on riigiülese koordinatsioonitasandi ja selle ülesannete piiritlemine. Ulatusliku küberintsidendi korral moodustab RIA operatiivstaabi, kuhu kaasatakse erinevates ülesannetes nii riigiasutusi kui ka teisi intsidendist mõjutatud osapooli. Plaani toimimist testiti esimest korda 2015. aastal üleriigilisel küberõppusel KüberSIIL ja selle järgi tegutsemist on harjutatud ka 2016. aastal toimunud õppustel.

Juunis toimus RIA juhtimisel õppus RIA Operatiivstaap, kus testisime asutustevahelist teabevahetust ja koostööd olulise mõjuga küberintsidentide lahendamisel. RIAga koos osalesid õppusel kuus meditsiini- ja transpordivaldkonna teenuseosutajat, samuti olid kaasatud siseministeeriumi ja kaitseministeeriumi haldusala asutused.

Sügisel toimusid Euroopa Liidu (EL) ja NATO tasandil läbi viidud küberõppused, mille läbiviimist Eestis juhtis RIA. NATO õppusel osalesid nii kaitse- (sh Kaitseliidu küberkaitseüksus) kui ka tsiviilvaldkonna riigiasutused. ELi suurimast, Euroopa Liidu võrgu- ja infoturbeameti (ENISA) korraldatavast õppusest *Cyber Europe* võtsid teiste hulgas osa eraõiguslikud elutähtsa teenuse osutajad andmeside ja transpordi valdkonnast.

Õppused näitavad, et erinevates asutustes on hea tehniline kompetents küberintsidentide lahendamiseks. Olulisemad puudujäägid seonduvad Eesti kübervaldkonna õigusmaastiku piisavusega; muu hulgas jääb vajaka meetmetest, mis võimaldaksid suunata asutuste tööd ning ressursse kriiside korral. Lisaks on õppused välja toonud vajaduse täiendada protseduure ja taasteplaane, et ulatuslike intsidentidega hakkama saada. Need aspektid on ühtlasi ka ühed olulisemad, et tagada erinevate asutuste koosvõime ja efektiivne tegutsemine ulatuslike intsidentide lahendamisel.

Märkimist väärivad ka RIA korraldatud kahepoolsed õppused rahvusvaheliste partnerasutustega, kus harjutatakse koostööd rahvusvaheliste intsidentide lahendamisel. Lisaks saadavatele praktilistele õppetundidele on õppused olulised strateegiliste partneritega suhete tugevdamiseks.

Kübervaldkonna õigusanalüüs: kas Eesti vajab küberjulgeolekuseadust?

RIA 2015. aasta küberturvalisuse kokkuvõte[33] tõi välja rea tehnoloogilisi ja õiguslikke arenguid, mis tingivad vajaduse ajakohastada küberjulgeoleku õigusraamistik. Eesti riigipilve[34] kontseptsiooni rakendamine vajab muudatusi õigusaktides, et tagada juurdepääsupiiranguga teabe konfidentsiaalsuse kaitse ning juurdepääsupiiranguta avaliku teabe kättesaadavus pilvandmetöötluse korral. Samuti mõjutab Eesti küberjulgeoleku tagamist hiljuti riigikogus vastu võetud

33 https://www.ria.ee/public/Kuberturvalisus/RIA_kuberturbe_aruanne_2015.pdf.
34 https://www.mkm.ee/sites/default/files/eesti_riigipilve_kontseptsioon.pdf.

uus hädaolukorra seadus, mis korraldab ümber elutähtsate teenuste toimepidevuse tagamise õiguslikud alused, ent jätab paljus ebaselgeks oluliste IKTst sõltuvate teenuste küberturvalisuse korralduse. Viimaks tuleb arvestada ka vajadust võtta Eesti õigusesse üle 2016. aastal vastu võetud Euroopa Liidu võrgu- ja infosüsteemide turvalisuse direktiiv (nn NIS direktiiv)[35], mis muu hulgas muudab küberintsidentidest teavitamise oluliste teenuste osutajate jaoks kohustuslikuks. Kõik need asjaolud teevad möödapääsmatuks valdkondlike normide muutmise.

2016. aastal tellis RIA kübervaldkonna õigusanalüüsi[36], et selgitada välja, kas erinevate valdkondlike seaduste olemasolu ning nende täiendamine infoturvet ja küberjulgeolekut puudutava regulatsiooniga on küberturvalisuse ja -julgeoleku tagamiseks toimiv ja piisav õiguslik mehhanism või tuleks välja töötada kübervaldkonna eriseadus. Kehtivate siseriiklikke küberjulgeoleku, infoturbe, riigikaitse ja muude valdkonnapõhiste õigusaktide analüüsi tulemusel tõid koostajad välja õiguslüngad ja regulatsiooni probleemkohad ning esitasid ettepanekud õigusaktide täiendamiseks.

Analüüs tõdes, et kübervaldkonna regulatsioonid vajavad ulatuslikku ülevaatamist ja korrastamist ning otstarbekas on see korraldada kübervaldkonna eriseaduses. Peamised argumendid eriseaduse kasuks on seaduslikkus, õigusselgus ja efektiivsus.

Praegu tulenevad RIA ennetus- ja planeerimisalased ülesanded küberturvalisuse valdkonnas peamiselt ameti põhimäärusest ning ameti roll järelevalveasutusena on sätestatud erinevates valdkondlikes seadustes. Analüüs juhtis tähelepanu, et eriti seal, kus RIA ülesanded kitsendavad isikute vabadusi info- ja võrgusüsteemide turvalisuse korraldamisel, peab RIA kui küberintsidentide käsitlemise ja lahendamise eest vastutava asutuse roll olema sätestatud seadusega. Praegune küberturvalisuse regulatsioon ei ole killustatuse tõttu ka läbipaistev ei avaliku sektori asutustele, nende lepingupartneritele ega elutähtsa teenuse osutajatele, kes nõudeid täitma peavad.

Analüüs leidis ka, et RIA efektiivsus võrgu- ja infosüsteemidega seonduvate riskide hindamisel on põhjendamatus sõltuvuses sellest, kas riskianalüüsi läbiviija peab võrgu- ja infosüsteemide turvalisuse hindamist vajalikuks. Toimepidevuse ja riskianalüüsid ei sisalda praegu kohustuslikku hinnangut teenuse küberturvalisusele.

Valdkonnapõhine eriseadus võimaldaks sisustada küberturvalisuse tagamiseks vajalikud õigused ja kohustused selgemalt ja täpsemalt ning tagaks seeläbi niihästi RIA ülesannete efektiivsema täitmise kui ka parema kontrollitavuse.

RIA tellitud riigipilve kontseptsiooni rakendamise õigusanalüüs[37] ei leidnud põhimõttelisi takistusi, mis välistaksid

35 http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1470661287196&uri=CELEX:32016L1148

36 Kübervaldkonna õigusanalüüsi tegi riigi infosüsteemi ameti tellimusel advokaadibüroo LEXTAL ja seda finantseeriti Euroopa Liidu struktuuritoetusest rahastatud toetusskeemist „Infoühiskonna teadlikkuse tõstmine". https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf.

37 Õigusanalüüsi riigipilve kontseptsiooni rakendamiseks tegi advokaadibüroo Sorainen. Analüüs tehti majandus- ja kommunikatsiooniministeeriumi tellimusel ning riigi infosüsteemi ameti läbiviidud riigihanke tulemusel Euroopa Liidu struktuuritoetuse toetusskeemist „Infoühiskonna teadlikkuse tõstmine". https://www.ria.ee/public/Kuberturvalisus/Riigipilve-rakendamise-oigusanaluus-2016-sorainen.pdf.

riigipilve kontseptsioonis kavandatud lahenduste rakendamise, ent tõi välja vajaduse teha Eesti õigusaktides mõõdukaid muudatusi. Näiteks tuleks pilvetehnoloogiate kasutuselevõtmiseks täpsustada avaliku teabe seadust, et piiratud juurdepääsuga teabe turvameetmete rakendamise kohustus andmete tervikluse, käideldavuse ja konfidentsiaalsuse tagamiseks oleks ka pilveteenuse osutajal, mitte üksnes teabevaldajal. Vajalik on ka riigi infosüsteemi kindlustav süsteem pilvandmetöötlusele nõuete kehtestamiseks või alternatiivina ISKE rakendusjuhendi kohandamine pilvandmetöötluse erisusi arvestavaks. Ühtlasi juhtisid analüüsi autorid tähelepanu kitsaskohtadele isikuandmete kaitse seaduse nõuete rakendamisele pilvandmetöötluse puhul.

Konkreetsete muudatus- ja täiendusettepanekute väljatöötamine eeldab, et riigipilve kontseptsiooniga seotud mõistekasutus (sh sellised baasmõisted nagu „digitaalne järjepidevus", „andmesaatkonnad") oleks selgelt ja üheselt sisustatud. Samuti on õigusraamistiku loomiseks vaja enne määratleda kontseptsiooni rakendamise täpsemad eesmärgid ja organisatoorne ülesehitus.

Riigi turvaline andmevahetuskiht X-tee laieneb

2016. aastal alustati RIA osalusel oluliste tehniliste ja organisatsioonilist laadi muudatustega riigi infosüsteemi turvalise andmevahetuskihi ehk X-tee juures.[38]

Tehniliselt läks 2016. aastal hoogsalt käima koostöö Soome Palveluväylä keskusega X-tee lahendustes tehniliste muudatuste sisseviimiseks. Eestis ja Soomes juurutatava teise põlvkonna X-tee v6[39] märkimisväärsemateks tegemisteks võib lugeda lahenduse koodi auditit ning X-teele lisatud monitooringuvõimalust, mille abil saab nii platvormihaldur kui ka liige ülevaate platvormi ja teenuste toimivusest. Et parandada riigi infosüsteemi kui terviku läbipaistvust, saavad inimesed pärida riiklikest andmekogudest informatsiooni selle kohta, kuidas on nende andmeid kasutatud.

Olulisima organisatsioonilise saavutusena on X-tee osas märkimist väärt infosüsteemide andmevahetuskihi määruse[40] uuendamine. Uues sõnastuses annab määrus selgemad vastutuse piirid kogu X-tee ökosüsteemi osalistele, loob paremad alused ökosüsteemi haldamiseks ning täpsustab liikmetele esitatavaid nõudeid. Kokkuvõttes suudab X-tee platvormina pakkuda liikmetele paremat turvalisust. Teine oluline organisatsioooniline algatus on X-tee ja Palveluväylä usaldusföderatsiooni loomine, mis loob aluse andmevahetuseks Eesti ja Soome riiklike andmekogude vahel. Turvaliste piiriüleste teenuste tekkimiseks vajalik koostöö Soome asjakohaste asutustega jätkub 2017. aastal.

Eelkirjeldatule lisaks on muudatused toimunud ka X-tee põhimõttelises käsitluses, et parandada X-tee turvalisust ja läbipaistvust. Tuumtehnoloogia arendus on järk-järgult viidud avatumasse keskkonda ning publitseeritud on ka kogu X-tee tuumtehnoloogia lahendus.[41]

38 X-teed tutvustav animatsioon: https://www.youtube.com/watch?v=Qbe5khu62jg; kvantitatiivset olemust iseloomustav faktileht: https://ria.ee/x-tee/fact.

39 https://www.ria.ee/ee/uleminek-x-tee-versioonile-6.html.

40 „Infosüsteemide andmevahetuskiht" (Vabariigi Valitsuse 23.09.2016. a määrus nr 105; RT I, 27.09.2016, 4).

41 https://github.com/vrk-kpa/xroad-joint-development; https://github.com/vrk-kpa/xroad-public.

Teisalt on eespool nimetatud valitsuse määruses X-tee defineeritud protokollistikuna – praegu veel ebapiisavalt spetsifitseeritud, kuid põhimõttelise valikuna on see pikaajaliselt jätkusuutlikum kui senine tootepõhine käsitlus.

Rahvusvaheline koostöö

2016. aasta oli RIA-le rahvusvahelises koostöös igakülgselt edukas. Viisime ellu mitu olulist algatust küberarenguabi valdkonnas, aitasime kujundada Eesti positiivset digikuvandit ja hoida usaldusväärse rahvusvahelise partneri mainet.

RIA-l on küberturvalisuse valdkonnas stabiilselt tugev koostöösuhe strateegiliste partneritega nii Euroopas, Põhja-Ameerikas, Lähis-Idas kui Kagu-Aasias. Lisaks igapäevasele infovahetusele ekspertide vahel toimusid 2016. aastal regulaarsed kohtumised nii poliitika- kui operatiivtasandil, et ühtlustada ohupilti, ennetada oluliste küberintsidentide toimumist ning kujundada sujuv koostöö puhkudeks, kus tuleb kriisiolukordades kiirelt reageerida ja partneritele abi osutada.

Olulisemateks RIA rahvusvahelise küberkoostöö formaatideks on lisaks kahepoolsele koostööle partnerametkondadega jätkuvalt koostöö Euroopa Liidu ja NATO raames, samuti CERTide koostööorganisatsioonid FIRST ja TERENA. Maailma digitaalselt arenenumaid riike ühendavas võrgustikus D5 (*Digital Five*) jätkas RIA küberturvalisuse teemade käsitlemist Eesti juhitaval, turvalisi digitaalseid isikutuvastuslahendusi käsitleval koostöösuunal. Kevadel korraldasime Tallinnas Balti riikide küberekspertide koordinatsioonikohtumise, mis kinnitas kolme riigi jätkuvalt tugevat koostööd ja üksteisemõistmist.

RIA toetas ka 2016. aastal mitut küberturvalisuse valdkonna arengukoostööprojekti. RIA eksperdid osalesid koolitusmissioonidel Gruusias, Ukrainas ja Lõuna-Ameerikas. RIA liitus ka Euroopa riikide konsortsiumiga, mis 2017. aastal asub ellu viima Euroopa Liidu esimest küberarenguabiprojekti Aafrikas ja Aasias. Küberturvalisuse valdkonnas vähem arenenud riikide nõustamine aitab RIA-l saavutada rahvusvahelist tuntust, kasvatada oma teadmisi ja kogemusi ning täita Eesti laiemaid välispoliitilisi eesmärke.

RIA 2016. aasta küberturvalisuse valdkonna kirjutised

Uuringud ja analüüsid

Elutähtsate teenuste osutamist mõjutavad tegurid
Projekti „Elutähtsate teenuste osutamist mõjutavate tegurite kaardistamise uuring" kokkuvõte. KPMG, november 2016
https://www.ria.ee/public/Kuberturvalisus/Elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf

Kübervaldkonna õigusanalüüs
Kübervaldkonna õigusanalüüs. Lextal, oktoober 2016.
https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf

Riigipilve kontseptsioon
Riigipilve kontseptsiooni rakendamise õigusanalüüs. Sorainen, märts 2016.
https://www.ria.ee/public/Kuberturvalisus/Riigipilve-rakendamise-oigusanaluus-2016-sorainen.pdf

Turvaline e-kiri
Eelanalüüs Eesti riigiasutuste turvalisele e-kirjavahetussüsteemile optimaalseima lahenduse leidmiseks. Tallinna Tehnikaülikool, 2016.
https://www.ria.ee/public/Kuberturvalisus/Eelanaluus-riigiasutuste-e-kirjavahetussusteem.pdf

Krüptograafiliste algoritmide elutsükkel
Cryptographic Algorithms Lifecycle. Report. Cybernetica, 2016.
https://www.ria.ee/public/RIA/Cryptographic_Algorithms_Lifecycle_Report_2016.pdf

Soovitused ja juhendid

Kahe- ja mitmeastmeline autentimine
Kaheastmeline autentimine: Gmail
https://blog.ria.ee/kaheastmeline-autentimine-gmail/

Kaheastmeline autentimine: Facebook
https://blog.ria.ee/kaheastmeline-autentimine-facebook/

Multiautentimisest
https://blog.ria.ee/multiautentimisest/

Elektrooniline identiteet
Eurodigiajastu mõisteselgitusi
https://blog.ria.ee/eurodigiajastu-moisteselgitusi/

RIA hinnangud ja ennustused 2017. aastaks

Elutähtsate teenuste kübersõltuvus kasvab.
Rohkem kui viiendik elutähtsate teenuste osutajatest sõltub kriitilisel määral kolmandate isikute pakutavatest IKT-teenustest. Katkestuste mõju ühiskonna ja majanduse toimimisele ning riigi julgeolekule on üha olulisem.

Avalik sektor on nii juhuslike kui suunatud rünnete sihtmärk.
Avaliku sektori peamised küberriskid on seotud teenusekatkestustega süsteemides, mille toimimisest sõltub riigi julgeolek, ning suunatud rünnetega rahalisel, poliitilisel või ideoloogilisel motiivil. Eraldi tuleb märkida kohalikke omavalitsusi, kel napib nii teadmisi kui ressursse küberohtude ennetamiseks.

Erasektori teadlikkus küberriskidest on lünklik nii üksikisiku kui ettevõtjate tasandil.
Iseäranis väikeettevõtjad ja vabaühendused ei pea end küberohtude sihtmärgiks ning turvalisusse ei investeeri.

Küberkuritegevus on üha professionaalsem.
Pahavara levitamisviisid on üha viimistletumad ning näha on keskendumist aegkriitilistest andmetest sõltuvatele valdkondadele, kus küberturvalisust pole seni oluliseks peetud (tervishoid). Suunatud ründed võivad olla äärmiselt usutavaks viimistletud. Ka ei ole küberkuritegevus enam üksnes väheste valitute pärusmaa, vaid soovitud „teenust" on võimalik kurjategijatelt osta ka neil, kel endal vajalikke oskusi ei ole.

Eesti on jätkuvalt Venemaa mõjutustegevuse sihtmärk.
Venemaa kasutab küberoperatsioone käsikäes traditsioonilise mõjutustegevusega vastavalt tehnoloogilisele võimekusele, doktriinile ja välispoliitilistele võimalustele. 2017. aastal eesseisvate oluliste sündmustega seoses tuleb valmis olla küberrünnete hoogustumiseks.

Arenevad tehnoloogiad ja teenused on haavatavad ning turvalisus ei jõua tehnoloogia arenguga sammu pidada.
Nutiseadmete ja esemevõrgu seadmete kasutusala laieneb. Ühes sellega laieneb nende turvalisusriskide mõju, aga ka atraktiivsus küberkurjategijate jaoks. Praegu ei ole täit arusaama, millised riskid kiirelt arenevate digitaalsete toodete, teenuste ja ettevõtlusvormidega kaasnevad. Tõenäoliselt näeme esemevõrgu seadmete rünnete puhul seniste rekordite purustamist nii mahu kui uute ründeviiside mõttes. Ühtlasi suureneb surve esemevõrgu seadmete turvalisuse parandamiseks.

Enamiku registreeritud küberintsidentide põhjus või seda soodustav tegur on aegunud tarkvara.
Aegunud veebihaldustarkvara kasutamine Eestis on epideemiline.

Üksnes salasõnadel põhinev autentimine ei ole enam turvaline.
Üha suurenev salasõnade hulk ning keerukamad nõuded paroolidele ei ole kasutajatele jõukohased. Kasutajate kohanemismeetodid (sh paroolide ristkasutus) suurendavad haavatavust. Kasvab surve võtta kasutusele turvalisemad isikutuvastusmeetod (kaheastmeline autentimine, biomeetrilised autentimismeetodid).

Õiguskeskkond vajab ajakohastamist.
Küberturvalisust tagavate organisatsioonide õigused ja kohustused peavad olema sätestatud seadusega, mitte rakendusaktides või haldusesisestes dokumentides. Praegune küberturvalisuse regulatsioon on killustatud ja adressaatide jaoks läbipaistmatu.