



TRENDID JA TÄHELEPANEKUD KÜBERRUUMIS

I KVARTAL 2023

1. Valimised küberruumis tormi ei toonud
2. Tegevjuhi petuskeem tõi ligi 100 000 eurot kahju
3. Globaalne lunavararünnete laine puudutas ka Eestit
4. Eesti riigiasutusi sihitakse õngitsustega

1. Valimised kübertormi ei toonud

Viimase aasta oleme näinud Eesti küberruumis tavapärasest rohkem rünnakuid, sestap valmistusime Riigikogu valimisteks erilise hoole ja innuga.

Olukord

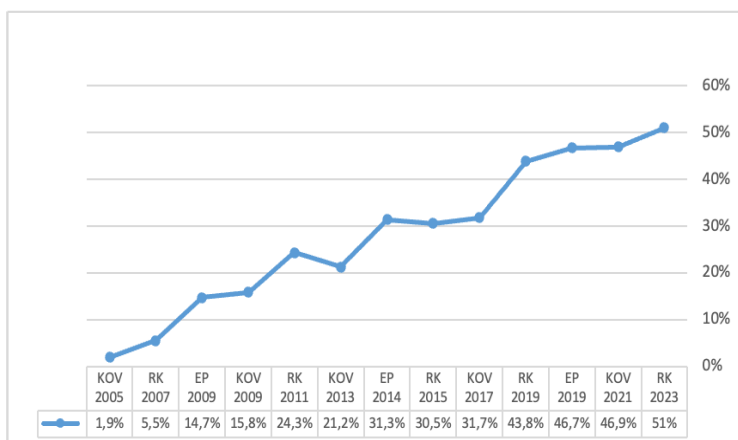
Aktiivsed ettevalmistused veebruari lõpus alanud valimistenädalaks käisid RIAs terve aasta. Moel või teisel oli sellesse kaasatud sadakond ameti töötajat, lisaks partnerid väljapoolt. Vastutasime valimiste infosüsteemi (VIS) arenduse ja töös hoidmise, e-hääletamise kogumislahenduse halduse, jaoskonnatöötajate arvutite kaitsmise ning valimiste küberturbe eest.

Enne valimistenädalat pakkusime valimisjaoskondade töötajatele ja kandidaatidele küberhügieeni koolitust ning testi. Praktiline õppematerjal aitas meelde tuletada levinumaid küberohte ja andis nõu, kuidas end nende eest kaitsta.

Lisaks pakkusime erakondadele ja üksikkandidaatidele võimalust kontrollida, kas nende süsteemides on haavatavusi, mida pahatahtlike kavatsustega ründajad saaks ära kasutada.

Päev enne eel- ja e-hääletuse algust läks RIA kõrgendatud valmisolekusse, et tagada valimiste, sh e-hääletamise turvalisus ja tehniline tugi. Moodustati staap ja väiksemad staabigrupid, mis jälgisid ööpäevaringselt valimistega seotud infosüsteemide tööd, võimalikke tõrkeid ja rünnakuid.

ÜLE POOLE HÄÄLTEST ANTI ELEKTROONILISELT



E-hääle osakaal Eestis toimunud valimistel

RIA hinnang

Valimistenädalale tagasi vaadates saame kergendustundega öelda, et see möödus oodatust rahulikumalt. Valimisega seotud infosüsteemid toimisid tõrgeteta ja olukord küberrindel oli suhteliselt vaikne.

Viimase aasta jooksul tavapäraseks muutunud teenusetõkestusründeid tuvastasime ka valimiste ajal, kuid nende hulk ja maht oli tagasihoidlik ning mõju valimistele neil polnud. Lisaks tuvastas CERT-EE mõned katsed anda e-häält mitteametliku rakendusega, kuid needki üritused ei õnnestunud.

Seekordsete valimiste kuulsaimat viperust ei põhjustanud küberrünnak, vaid asjaolu, et valimisnädala esimesel päeval jõudsid valijate nimekirja viimased muudatused e-hääletamise süsteemi väikse viitega. Seetõttu kuvas valijarakendus 57 inimesele, kelle elukoha-andmed olid rahvastikuregistris hiljuti muutunud, vana valimisringkonda ja selle kandidaate. Vales ringkonnas antud hääled tühistati ja nende omanikel paluti uuesti hääletada.

Ühtekokku andis Riigikogu valimistel oma hääle 615 009 inimest. See on rekordiline arv ja esmakordselt 18 aasta jooksul oli sel korral e-hääle andnud rohkem kui pabersedeliga hääletanud. Meie jaoks on see usalduse märk.

2. Tegevjuhi petuskeem tõi ligi 100 000 eurot kahju

Ehkki otsese kahju kannatajateks olid ettevõtte partnerid välismaal, oli see tõsine löök Eesti ettevõtte mainele.

Olukord

Möödunud kvartalis saime taas teateid ettevõtetelt ja asutustelt, kellelt üritati raha välja petta tegevjuhi petuskeemiga.

See skeem toimib nii, et kurjategijad saavad näiliselt tegevjuhi nimelt maksekorraldusi või võltsarveid, mille kasusaajaks on kurjategijad ise. Kogu sündmuste ahel saab sageli alguse ettevõtte mõne meilikonto kompromiteerimisest, mis annab kurjategijatele võimaluse jälgida meilivestlusi ning koguda taustinfot, et siis õigel hetkel usutavalt vestlusesse sekkuda.

Mõned pettusekatsed osutusid paraku ka edukaks. Ühe Eesti põllumajandusettevõtte kliendid välismaal jõudsid tasuda ligi 100 000 euro eest arveid, enne kui saadi aru, et need on võltsitud. Skeem oli hästi läbi mõeldud: arvete kiire tasumise korral sai allahindlust ning Eesti ettevõtte nimel oli loodud ka libakonto WhatsAppis, mille kaudu klientidega suheldi ja kinnitati, et kõik on õige.

Ühe Eesti põllumajandusettevõtte kliendid välismaal jõudsid tasuda ligi 100 000 euro eest arveid, enne kui saadi aru, et need on võltsitud.

RIA hinnang

Taolised petuskeemid on juba aastaid laialt levinud nii Eestis kui välismaal. Kirjeldatud juhtumi puhul on tähelepanuväärne selle mitmekihilisus – ettevõtete nimelt mitte ainult ei saadetud võltsitud meile ja arveid, vaid võltsitud olid ka alternatiivsed suhtlemiskanalid ning klientidega suheldi lisaks telefoni teel. Kuna petuskeemid muutuvad järjest keerukamaks, peavad ka nende vastu rakendatavad meetmed olema mitmekesised.

KORDAME AGA ÜLE MÕNED PÕHITÕED, MILLEST ALUSTADA:

1. Ole teadlik sellistest petuskeemidest ja kindlastest ohumärkidest. Koostööpartneri pangaandmete muutus, tasumisega tagant kiirustamine, ootamatud ja kiireloomulised rahalised korraldused tegevjuhi nimelt on tüüpilised võtted, mida petturid kasutavad.
2. Kui tekib vähimgi kahtlus arve või ülekandepalve õigsuses, helista saatjale ja küsi üle. Kasuta selleks varem saadud kontakte, mitte neid, mille leiad kahtlase meili või arve juurest.
3. Järgi ettevõtte protseduurireegleid, kuidas arveid ja ülekandeid kooskõlastatakse. Ka siis, kui asjaga on „väga kiire“.

MILLISED RÜNDED TABASID EESTI ETTEVÕTTEID EELMISEL AASTAL KÕIGE ROHKEM?

Loe [RIA aastaraamatust](#).



3. Globaalne lunavararünnete laine puudutas ka Eestit

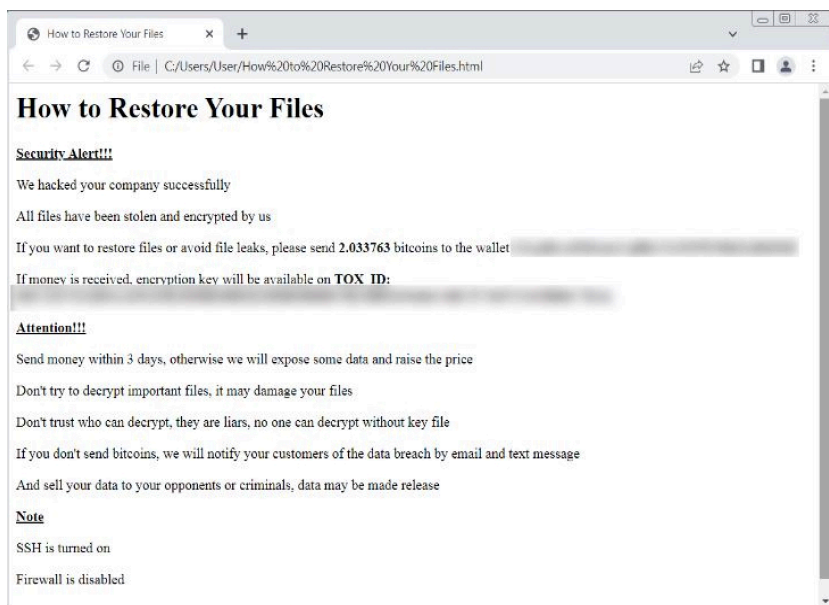
Veebruaris asusid ründajad massiliselt ära kasutama kaks aastat vana turvanõrkust levinud virtualiseerimistarkvaras VMware ESX.

Olukord

Kõnealune tarkvara võimaldab ühes füüsilises serveris luua ja töös hoida mitmeid virtuaalmasinaid ning on laialt kasutusel nii Eestis kui mujal maailmas. Senistel andmetel õnnestus ründajatel enim kompromiteerida Prantsusmaa, USA ja Saksamaa servereid ning see tõi kaasa suure lunavararünnete laviini.

Kuna ründajad sihtisid rünnakute algfaasis üht kindlat avalikult kättesaadavat teenust, tuvastas CERT-EE Eesti küberruumis kõik vastavad teenused ja saatis hoiatusteavitused teenusega seotud võrkude omanikele. Siiski on CERT-EE-le teada vähemalt üks kohalik juhtum, kus ründajatel õnnestus haavatavust ära kasutada ja lunavararünnak toime panna.

ESX LUNAVARANÕUE



ESXiArgs ransom note (BleepingComputer)

RIA hinnang

Kõnealune laine paistis silma kolmel põhjusel. See oli ulatuslik ja krüpteeris lühikese aja jooksul tuhandeid süsteeme, puudutades oluliselt ka Euroopa riike.

Teiseks ei ole nende lunavararünnete puhul siiani selge, kas lisaks krüpteerimisele varastasid ründajad ka andmeid. Üldjuhul kasutavad kriminaalsed rühmitused spetsiaalseid veebilehti ja foorumeid, kus ohvrid avalikustada, lisaks varastatakse tavaliselt kompromiteeritud süsteemist andmeid, et neid hiljem väljapressimise käigus ära kasutada. Antud ründelaine puhul aga ei ole seda täheldatud.

Kõik ründelaine ohvrid kasutasid paikamata virtualiseerimistarkvara, millele pääses internetist ligi. See ei ole hea praktika, sest avaliku ligipääsuga sihtmärgid on alati potentsiaalsetele ründajatele väga ahvatlevad. Lisaks oli riskide alahindamisest või lihtsalt teadmatusest jäänud paikamata juba kaks aastat tagasi avalikustatud turvanõrkus.

See laine tõestas taas, et regulaarne tarkvara uuendamine on oluline ning ka vanu turvavigu võidakse hakata uuesti massiliselt kuritarvitama. RIA andis veebruaris nende rünnete taustal avaliku ohuhinnangu ja soovitused, mille leiate [siit](#).

4. Riigiasutusi sihitakse õngitsustega

Eesti ametkonnad saavad õngitsusmeile pidevalt, viimastel kuudel on need muutunud sagedasemaks ja sihitumaks.

Olukord

Õngitsuskirjades kasutatakse usutavuse tõstmiseks sageli päevapoliitilisi teemasid: Venemaa agressiooni Ukrainas, sisserännet, sanktsioone, NATO kohtumisi ja muud ametnike tööd puudutavat.

Õngitsuste taga võivad olla nii küberkurjategijad kui riikliku taustaga küberründajad. Kui kurjategijad õngitsevad sageli huupi, et saadud andmeid või ligipääse lihtsalt edasi müüa, siis riikliku taustaga ohustajad sihivad üldjuhul just riigiasutusi (sh saatkondi) või ka huvipakkuvaid uurimisasutusi (üliskoole, mõttekodasid jm).

Muidugi oli ka õpituvastusi, näiteks RIA kriisirollide jaotus ja kohustused võiksid olla veelgi selgemad ning tööd tuleb jätkata küberreservi ettevalmistuse ja koolitustega, et kriisi korral toimuks kaasumine võimalikult sujuvalt. Ka haigla hinnangul oli selline läbimäng igati kasulik ning taolisil õppusi on kindlasti plaanis korraldada ka tulevikus.

RIA hinnang

Tõenäoliselt on eri motiividega ründajate huvi Eesti ja teiste Euroopa riikide suunal tõstnud Venemaa agressioon Ukrainasse. Ummistusrünnete (DDoS) hüppelisest kasvust oleme kirjutanud kõikides viimastes ülevaadetes. Nüüd ilmestab küberohupildi aina tõsisemaks muutumist ka õngitsuste intensiivsuse kasv.

Eri tüüpi õngitsuste eesmärk on saada inimene vajutama ründaja soovitud linkidel, jagama infot või avama pahavaraga nakatunud faili. Mida oskuslikum ja motiveeritum on ründaja, seda rohkem eeltööd ta teeb, et just valitud ohvri jaoks kõige usutavam püüdis teele panna. Seetõttu võivad riigiasutuste suunas saadetud õngitsused olla vägagi tõepärased. Lisaks e-mailile levitatakse õngitsusi aina enam ka sotsiaalmeedia vahendusel, näiteks tööpakkumiste ja -kuulutuste kaudu.

Nagu pea kõikide küberohtude puhul, on õngitsuste tõkestamiseks vajalikud nii tehnoloogilised meetmed (nt meilifiltrid, tõhusad viirusetõrjeprogrammid) kui ka kasutajate teadlikkus ja vastutustunne. Tundmatute linkide või kahtlaste manuste mitte avamine on küberturvalise käitumise üks alustõdesid, nagu ka erinevate paroolide kasutamine erinevates keskkondades.

Väga oluline on aga ka see, et kasutajad, olles siiski teinud vale liigutuse, sellest kohe oma it-toele teada annaksid. Intsidendi kahtluse korral võid alati pöörduda ka cert@cert.ee



Läheb hästi

23. märtsil kuulutas Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) välja aasta tunnustuse saajad, kes on aidanud kriitilisel ajal kaasa julgeoleku tagamisele. Aasta teo pälvis RIA küberturvalisuse keskuse meeskond Eesti küberjulgeoleku tagamise eest. Tunnustus on meile suur au ja püüame ka edaspidi kasulikud olla!



Saaks paremini

Viimaste kuude jooksul oleme saanud keskmisest rohkem teavitusi erinevate õngitsuste kohta ning kahjuks on paljud inimesed ka nende ohvriks langenud. Kui varem saadeti peamiselt õngitsuskirju, siis nüüd on tavaliseks saanud SMS-sõnumid, mille puhul võib olla isegi raskem pettust ära tunda. Tihti ei pööra SMSi saaja sõnumis olevale lingile tähelepanu ning kui saatjaks on näiliselt pank, siis tundub kõik õige. Meile teadaolevalt on kõige suurem eraisiku kahju olnud 14 000 eurot.