



TRENDID JA TÄHELEPANEKUD KÜBERRUUMIS

IV KVARTAL 2022

1. Aasta lõpp tõi suured õngitsuslained
2. Veebikestad ohustavad kaitsetuid veebilehti
3. 2022 oli ummistusrünnete aasta
4. Eestis toimus unikaalne küberõppus

1. Aasta lõpp tõi suured õngitsuslained

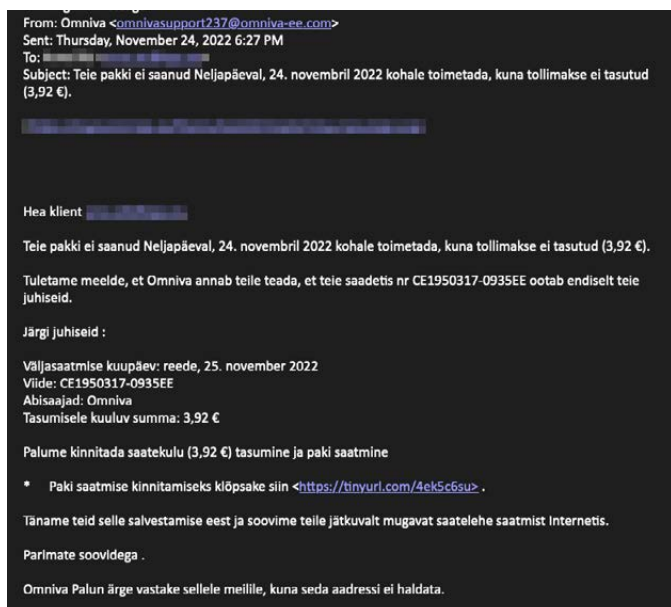
Õngitsuslehed moodustavad kõige suurema osa CERT-EE registreeritud intsidentidest. Kui vaadata viimase kvartali statistikat, siis üle kolmandiku juhtumitest on seotud just õngitsuslehtedega.

Olukord

Aasta viimasel paaril kuul sagesid erinevad õngitsuskampaaniad, seda võis mõjutada nii nn must reede, mille ajal telliti keskmisest rohkem postipakke, kui ka jõulupühad.

Kõige enam nägime erinevate pankade (LHV, Swedbank, SEB) ja logistikaettevõtete (DHL, Omniva) nimel saadetud õngitsusi. Need laekusid kas e-kirja või SMSi teel ning enamas ti suunasid teate saajat kiirelt tegutsema ja enda andmeid sisestama. Petturite eesmärgiks on kätte saada ohvri nimi ja pangakaardi andmed ning seejärel hakata pangakontot tühjendama.

Pankade nimel saadetud pettuses võis olla näiteks märgitud, et panga mobiilirakenduse kasutamine aegub või pangakonto on turvakaalutlustel peatatud ja selle uuesti avamiseks tuleb sisestada saadetud lingile enda kontoandmed. Omnivat jälgendavatest pettustest üks annab inimestele e-kirja teel teada, et kuller proovis kohale toimetada pakki, kuid see ei õnnestunud. Teist tüüpi Omnivat matkivad õngitsuskirjad väidavad, et kirjasajale jäi pakk kohale toomata, sest tollimaks summas 3,92 eurot on tasumata. DHLi nimel saadetud sõnumis oli samuti nõue tasuda tollitasud summas 1,99 dollarit. Kõigi nende kirjade ja sõnumite sees on link, mis viib kurjategijate loodud andmeid õngitsevale lehele.



RIA hinnang

Näeme, et õngitsuskirjad muutuvad üha usutatavamaks. Kui varasemalt kaitses meid teatud määral keelebarjäär, sest vigased laused tekitasid kahtlust, siis viimaste puhul oli keelekasutus üldiselt korrektne. Pettust ära tunda on raske ja igaüks võib sattuda õngitsuskirja ohvriks. Kuna õngitsuslehtedel küsitakse kasutaja pangakonto andmeid, siis võib kahju olla väga suur. Halvemal juhul tehakse pangakonto tühjaks ning raha tagasi saamiseks suurt lootust ei ole.

Üldjuhul kõigis õngitsuskirjades ja -sõnumites püütakse inimest sundida kiirelt tegutsema. Teame juhtumeid, kus üldiselt kõrge teadlikkusega inimesed langesid seekord pettuse ohvriks, kuna oodatigi päriselt pakki ja aastalõpu saginas oli ka tavapärane valvsus madalam.

Tuletame meelde mõned soovitusel, kuidas õngitsusi ära tunda ja vältida:

- ▶ Ära sisesta enda isiklikke ega kontoandmeid kahtlastele ja kiiret tegutsemist nõudvatele lehtedele.
- ▶ Jälgi alati kirja saatja aadressi ja veebilehe aadressi (domeeni), kuhu sind suunatakse.
- ▶ Kui saad kahtlase kirja või sõnumi näiteks pangast või logistikaettevõtetelt, siis helista ja küsi üle kas tege mist on õige kirjaga. Väldi küsimuse esitamist samas kanalis, mille kaudu tuli kahtlane kiri või sõnum.
- ▶ Pea meeles, et ei pank ega ka postifirma ei küsi kunagi sinu konto- ega pangakaardi andmeid.
- ▶ Nutiseadmetes aitab libalehtedele sattumise võimalust vähendada RIA äpp (*Encrypted DNS*), mis blokeerib teadaolevate ohtlike veebilehekülgedele külastamise.
- ▶ Kahtluse korral saada kiri **CERT-EE** meeskonnale uurimiseks.

2. Veebikestad ohustavad kaitsetuid veebilehti

Lõppenud kvartalis tuvastas CERT-EE mitukümmend Eesti veebilehte, kuhu ründajatel oli õnnestunud laadida veebikest (ingl k *websHELL*). Mis see on ja kuidas end selle eest kaitsta?

Olukord

Kompromiteeritud veebilehed esindasid erinevaid eluvaldkondi alates tantsuspordist kuni turunduseni ja enamasti oli tegemist lihtsamate WordPressi põhiste lehtedega, mille haavatavuste kaudu oligi rikkumine toimunud.

Veebikest on oma olemuselt miniprogramm või koodirida, mida saab kasutada veebiserverile süsteemikäskude andmiseks. Näiteks võib selle abil üles laadida pahaloomulist sisu, reklaamida illegaalseid kaupu, õngitseda kasutajate andmeid või nakatada lehe külastajaid pahavaraga.



RIA hinnang

Veebikesta abil tehtud ründed pälvivad möödunud aastal meie tähelepanu mitmel põhjusel. Kui ründajad on veebikesta edukalt üles laadinud, kaitstakse nendele ligipääs sageli parooliga ja neid paroole ehk sisuliselt tagauksi suurele hulgalte kompromiteeritud veebilehtedele müüakse edasi juba järgmistele klientidele. Selline spetsialiseerumine ja teenuse pakumine muutub küberkuritegevuses järjest tavalisemaks ja laiendab ründajate arsenalit. Nii näiteks kasutasid häktivistid veebikesti erinevate riikide veebilehtedel selleks, et mitmekesistada teenusetökestusründeid enda jaoks ebasõbralike riikide vastu.

Eestis viimases kvartalis tuvastatud kompromiteeritud veebilehtede halduritele tuli CERT-EE teavitust veebikesta olemasolust üldjuhul üllatusena, kuid sageli jõuti need kahjutuks teha enne, kui ründajad edasisi samme ette võtsid. Murelikuks teeb aga asjaolu, et veebikesta paigaldamise suhtes kaitsetuid, see tähendab uuendamata tarkvara või muul põhjusel haavatavaid veebilehti on Eestis sadades, kui mitte tuhandetes. Meenutame veebilehtede omanikele, et tarkvara (ka tasuta tarkvara) ja kasutatavad pluginad vajavad regulaarset uuendamist ning veebilehtede haldamisel tuleb järgida ranget ja turvalist paroolipoliitikat.

3. 2022 oli ummistusrünnete aasta

Läinud aastal tabas Eestit neli korda rohkem ummistusründeid, kui aasta varem. Ka rünnete mahud ja kestus on kasvanud.

Olukord

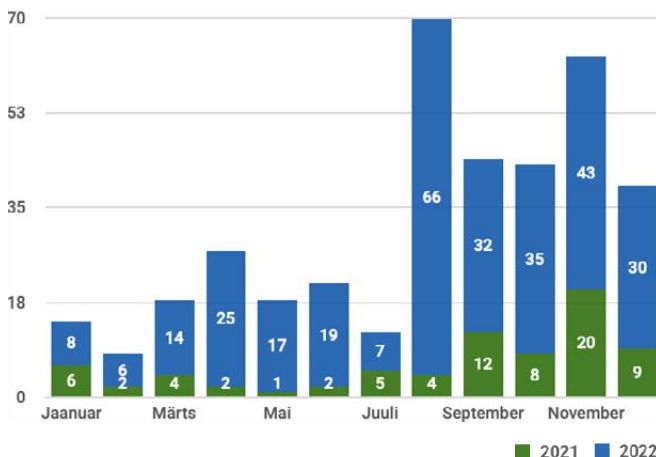
Aasta viimased kuud möödusid endiselt teenusetökestusrünnete (DDoS) tähe all. Kui tavapärase ummistusrünnete tase on kümnekond märkimisväärset rünnet kuus, siis oktoobris registreerisime neid 35, novembris 43 ning detsembris 30.

Läinud aastat tervikuna jääb ilmestama enneolematult suur teenusetökestusrünnete arv. 2022. aastal tabasid Eesti ettevõtteid ja asutusi märkimisväärsed ummistusründed 300-l korral, aasta varem oli see number neli korda väiksem.

Neljandas kvartalis nägime mitut suuremat ummistusrünnete lainet. Oktoobri alguses toimunud rünnete tõttu katkesid Eesti Raudtee veebilehe ja e-residentide portaali töö, sihtmärkide seas olid muuhulgas ka Vabariigi Presidendi, valitsuse ning ERRi veebilehed. Novembris DDoS-ründed jätkusid, suurima mõjuga olid 19. novembril läbi viidud rünnakud, mis olid suunatud ka Eesti Energia, Eesti Panga ja EASi veebilehetele vastu. Detsembri alguses aset leidnud ummistusrünnete laine tabas 11 riigiasutust, teiste seas olid sihtmärkiks Riigikogu ning Majandus- ja Kommunikatsiooniministeeriumi veebilehed.

Lisaks ummistusrünnete arvu kasvule oleme viimaste kuude lõikes näinud ka rünnete mahtude ning ajalise kestuse tõusu: näiteks pandi ühe transpordiettevõtte vastu suunatud ummistusrünnaku käigus teele enam kui kaks miljardit pahatahtlikku päringut.

EESTIT TABANUD MÄRKIMISVÄÄRSETE TEENUSETÖKESTUSRÜNNETE ARV 2021. JA 2022. AASTAL.



RIA hinnang

Ründajad õpivad pidevalt ning rünnakuid mitmekesistades otsitakse võimalusi levinumatest kaitsemeetmetest läbi tungida. Oleme ettevaatavalt rakendanud mitmeid täiendavaid kaitsemehhanisme, et tuvastada ja pidada kinni erinevaid rünnakukatseid. Ehkki juba tuttavaid tööriistu ja ründeviise kasutatakse jätkuvalt palju, oli aasta lõpus tehtud ummistusrünnete puhul märgata muutuseid ründeviisides, samuti olid rünnakud üles ehitatud sihitumalt. See aga tähendab, et peame olema pidevas valmisolekus ning mõtlema ette, kuidas selliste rünnakute edu paremini nullida.

Pole alust arvata, et erasektori olukord kuidagi eristuks. Neljandas kvartalis nägime lisaks avaliku sektori asutustele ummistusrünnete sihtmärkide seas nii finants-, kinnisvara-, kui ka ehitussektori ettevõtteid. Küberrünnakute katsed on pidevad ning pahatihti mõistetakse küberturbe tähtsust alles siis, kui ettevõtet on juba tabanud ränkade tagajärgedega küberrünnak.

Nagu paljudes teistes valdkondades, kehtib siingi reegel: ennetus ja kaitse on soodsam kui tagajärgedega tegelemine. Erinevaid tehnilisi meetmeid, millega DDoS-ide mõju ära hoida või leevendada, pakuvad suuremad interneti-teenuste pakkujad ja paljud küberturbeettevõtted, riigivõrgus olevatele klientidele laieneb RIA pakutav kaitse. Prognoosime teenusetökestusrünnete kasvu ka alanud aastal ning soovime asutustel ja ettevõtetel nendeks jätkuvalt valmis olla. RIA juhend teenusetökestusrünnete ennetuseks asub [siin](https://ria.ee) ja nõu võib küsida ka cert@cert.ee.

Teenusetökestusrünnete (nagu ka muude küberohtude) mõju oma äritegevusele tuleks hinnata ettevõtte riskianalüüsis ning planeerida selle põhjal optimaalsed kaitsemeetmed. Terviklikku lähenemist küberohtude eest kaitsmiseks pakub Eesti infoturbestandard (E-ITS), mille kohta leiab rohkem infot [Eesti infoturbestandardi portaalist](https://ria.ee).

4. Eestis toimus unikaalne küberõppus

Läinud aasta oktoobris korraldas RIA koostöös Põhja-Eesti Regionaalhaigla ja sihtasutuse CR14-ga ühise küberõppuse, kuhu kaasati riigi värskest loodud küberreserv ja aktiveeriti RIA kriisiplaanid.

Küberõppuse käigus lahendati haiglat tabanud lunavararünnakut. Stsenariumi järgi oli krüpteeritud mitukümmend seadet ning lunavara levis aktiivselt edasi, mistõttu katkes nii plaaniline kui erakorraline ravi.

Tegemist oli unikaalse küberõppusega, sest varem ei ole nii suurt asutuste-ülest läbimängu tehtud. Stsenarium võttis arvesse tänast ohupilti ja õppus mängiti läbi võimalikult realistlikult, näiteks nakatunud seadmed vahetati välja patsientide silme all. Õppusel oli kolm peamist eesmärki: küberreservi käivitamise läbimängimine, RIA kriisikorra, sh ametis käivititava juhtstaabi läbimängimine ja intsidendi tehniline lahendamine.

Õppusesse kaasati ka küberreserv, mis on kolmetasandiline vabatahtlik võrgustik, kuhu kuuluvad RIA enda töötajad (I tase), riigi IT-majade töötajad (II tase) ja Kaitseliidu küberkaitseüksus (III tase). RIA tegi õppuse käigus küberreservi kaasamiseks ametiabi palved, riigi igast IT-majast kaasati kübereksperte ja Kaitseliidust osales spetsiaalne küberkaitseüksus.

Üldiselt olid kõik osapooled ühel nõul, et küberõppus parandas riigi valmisolekut tõsiste küberintsidentide lahendamiseks. Õppuse kontseptsioon töötas ja osalejate huvi ja valmisolek panustada oli eeskujulik, palju andis juurde töötava suurhaigla keskkond.



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 taolisi õppusi on kindlasti plaanis korraldada ka tulevikus.



Läheb hästi

Kaua tehtud kaunikene! 8. detsembril 2022 kehtestati Vabariigi valitsuse määrusega kolme aasta jooksul välja töötatud uus Eesti infoturbestandard (E-ITS). See on nõuete ja parimate rahvusvaheliste praktikate kogum, mis loodud era- ja avalikule sektorile mõõtmaks ning juhtimaks IKT turvalisuse tegevusi.

Alates käesoleva aasta 1. jaanuarist on [küberturvalisuse seaduses](#) sätestatud E-ITSi kohuslastel uuele standardile üleminekuks aega kolm aastat. Standard on vabalt kättesaadav eelmisel suvel uuenenud [portaalis](#). Rakendajate tagasisidet ootame e-posti aadressile standard@ria.ee.



Saaks paremini

CERT-EE saab igapäevaselt keskmiselt 60-70 teavitust küberintsidentidest, millest mõjuga on umbes iga kümnes. See on aga vaid jäämäe tipp, sest meieni ei jõua teave kaugeltki mitte kõigist Eesti küberruumis aset leidvatest juhtumitest.

Hea lugeja – palun anna meile alati teada, kui Sinu või Su ettevõttega küberuumis midagi kahtlast juhtub. Juhtunust [raporteerimise](#) oleme teinud võimalikult lihtsaks. Iga sissetulev teave aitab meil paremini Eesti küberuumi kaitsta ja hoida päevakohast ohupilti.