RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] Juuni 2020

Lunavararünnakutega kaasneb üha sagedamini andmevarguse ja -lekke risk

Kõik asutused peaks lähtuma eeldusest, et lunavararünnaku korral nende seadmetes olnud andmeid mitte ainult ei krüpteerita, vaid üha kasvava trendina ka varastatakse ja avalikustatakse. Seetõttu ei piisa lunavararünnakute vastu võitlemisel andmete varundamisest.

Lunavararünnak – mis see on ja kuidas toimib?

Klassikaline lunavararünnak toimib järgmiselt:

1. Ründaja paigaldab ohvri arvutisse lunavara. Tihti toimub vastava pahavara levitamine e-kirjaga saadetud failide või linkide avamisel. Sageli kasutatakse lunavaraga nakatamiseks ka haavatavaid veebilehitsejaid, tarkvarakomponente või avalikult kättesaadavaid kaugtöölaua teenuseid nagu Remote Desktop Protocol (RDP).
2. Lunavara krüpteerib kas osa arvutites või serverites olevatest failidest või kõvakettad tervikuna. Pärast seda ei saa ohver enam faile avada.
3. Ründaja nõuab andmete taastamise ehk lahtikrüptimisvõtme eest lunaraha, enamasti mõnes krüptovaluutas nagu Bitcoin või Monero.

Kuna asutused teevad oma failidest varukoopiaid üha sagedamini ning kaitsevad neid, pole sellistel puhkudel põhjust maksta lunaraha, sest krüpteeritud andmed saab taastada ka ilma lahtikrüptimisvõtmeta. Sellest tulenevalt on lunavararünnakute läbiviijad muutnud oma taktikat ja kasutavad ohvrite survestamiseks andmete varastamist ning ähvardust need maksmata jätmise korral avalikustada.

Sedalaadi rünnakut on keerukam läbi viia, sest andmete liigutamine ohvri arvutitest ründaja omadesse võtab aega ja jätab jälgi. Nende põhjal on võimalik rünne avastada enne, kui kõik andmed varastatud või krüpteeritud. Lisaks peavad ründajad suures andmehulgas orienteeruma, leidma osad, mille avalikustamine ohvrit enim kahjustavad.

Hoolimata asjaolust, et andmevargus muudab lunavararünnaku keerukamaks ja aeglasemaks ning suurendab varase avastamise tõenäosust, kasvab sedalaadi rünnakute osakaal. Prantsusmaa küberturbe-agentuuri ANSSI hinnangul moodustavad andmevargust ja nende avaldamise ähvardust sisaldavad rünnakud ligi veerandi neile teadaolevatest lunavararünnakutest.

[1] [1] KüTS'i paragrahv 12:
(3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

Hiljutine intsident

CERT-EEle on teada, et hiljuti tabas üht suurt meditsiinisektori asutust säärane lunavara-rünne. Rünnaku käigus krüpteeriti andmed, kuid lisaks sellele need ka varastati. Kui ohver keeldus dekrüpteerimisvõtme eest maksmast, teatasid ründajad, et avalikustavad rünnaku käigus varastatud andmed. CERT-EE saab kinnitada, et andmeid avalikustati, mis tähendab, et neid ka varastati. Leke sisaldas patsientide ees- ja perenime, sünniaega, sugu, rahvust, ametikohta, postiaadressi ja telefoninumbrit. Lisaks võib sealt leida arsti nime ja telefoninumbri, märkmeid allergiate, testitulemuste ja ravi kohta.

Summa, mida kurjategijad välja pressivad, ulatub miljonitesse eurodesse. Olukorras, kus GDPR ehk isikuandmete kaitse määrus on jõustunud ja sealsed trahvid võivad küündida kuni 20 miljoni euroni või kuni 4% üleilmsest käibest, on tõenäoline, et andmete avaldamise ähvardused sagenevad.

Lunavararünnakuga kaasnevad riskid

Lunavararünnakuga kaasneb rida riske. Toome välja kolm olulisemat.

Tegevusrisk – lunavararünnak võib peatada asutuse töö, kuna tööks või süsteemide toimimiseks vajalikud andmed pole kättesaadavad.

Mainerisk – töö katkemine kahjustab asutuse mainet, kuid suuremat kahju põhjustab andmete vargus ja nende avalikustamine.

Finantsrisk – tegevuse peatumine tekitab asutusele rahalist kahju, kuid sellest suurema kulu võib põhjustada Euroopa Liidu isikuandmete kaitse üldmääruse (*GDPR*) nõuete rikkumine. GDPR näeb karistusena ette rahatrahvi kuni 20 miljonit eurot või juriidilise isiku puhul kuni 4% tema eelmise aasta käibest. Maksimumtrahvi määr sõltub sellest, kumb nimetatud summadest on suurem.

RIA soovitused: kuidas kaitsta oma asutust lunavararünnaku eest

Varunda andmeid
Parim kaitse krüpteeriva lunavara vastu on töökindel varundus. Kui rünnaku ohver suudab tagavarakoopiast andmed taastada, nurjab see lunavararünnakutest tuleneva andmekao ning kiirel taastamisel saab töö jätkuda. Kuna lunavara püüab krüpteerida faile nii kohalikul kettal, välistel andmekandjatel kui ka võrguketastel, peab varukoopia asuma eraldi, et tagavarakoopia võrguketta krüpteerimise korral ei nakatuks. Selleks soovitame hoida üht varukoopiat *offline*-režiimis. Kontrolli regulaarselt varunduse seisukorda ning terviklust.

Kasuta revisjonlogimist
Aktiveeri failiserverites *audit logging* ehk revisjonlogimine. See aitab tuvastada lunavaraga nakatunud arvuteid ja servereid, mis võivad krüpteerida võrgukettal asuvaid faile.

Kasuta monitooringuskripte

Võta kasutusele monitooringuskriptid, mis aitavad tuvastada süsteeme, mis muudavad lühikese aja jooksul suure hulga faile. Selline monitooring aitab tuvastada faile krüpteeriva lunavara enne, kui see on jõudnud suuremat kahju tekitada.

Koolita töötajaid
Teavita töötajaid, eriti eemal viibivaid, lunavara-ohust ning tuleta neile meelde, et tundmatutele linkidele ei tohi vajutada ega tundmatuid manuseid avada. Sageli nakatuvad arvutid lunavaraga just e-posti teel saabunud linkide või failide kaudu.

Muuda e-posti süsteem viirusekindlamaks
Vaata üle oma e-posti süsteemi turvapoliitikad ning veendu, et logimine on sisse lülitatud (see aitab ka tuvastada nakatunud kasutajad). E-posti süsteem peaks blokeerima või panema karantiini kõik dokumendid, mis sisaldavad käivitatavaid faile ja konteineriformaate.

Näiteks tuleks blokeerida või panna karantiini alltoodud faililaiendid:
Konteineriformaadid: .zip, .rar, .ace, .gz, .tar, .7z, .z, .bz2, .xz, .iso
Rakendused: .exe, .pif, .application, .gadget, .msi, .msp, .com, .scr, .hta, .cpl, .msc, .jar
Skriptid: .bat, .cmd, .vb, .vbs, .vbe, .js, .jse, .ws, .wsf, .wsc, .wsh, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .msh, .msh1, .msh2, .mshxml, .msh1xml, .msh2xml
Otseteed: .scf, .lnk, .inf
Muud: .reg, .dll
Office makrofailid: .docm, .dotm, .xlsm, .xltm, .xlam, .pptm, .potm, .ppam, .ppsm, .sldm
wirecode poolt keelatud failid: .asf, .asx, .au, .htm, .html, .mht, .vbs, .wax, .wm, .wma, .wmd, .wmv, .wmx, .wmz, .wvx

Rakenda minimaalõiguste printsiipi
Kehtesta pääsupoliitika, millega tagatakse kasutajatele nende igapäevatööks minimaalsed õigused. Tugev pääsupoliitika aitab piirata lunavara levikut ja võib peatada lunavara käivitumise, sest selle jaoks pole piisavaid õigusi.

Määra andmete tundlikkus
Rakenda asutusesiseselt praktikat, kus juurdepääsuõigused pole ainult IT-süsteemide/protsesside põhised, vaid sõltuvad ka konkreetsete andmete tundlikkusest. Sellise praktika eduka rakendamise eelduseks on andmete eelnev korrektne markeerimine (nn *data labeling*).

Uuenda tarkvara
Veendu, et töökohtades ja serverites kasutatavat tarkvara sh. pistikprogramme uuendatakse regulaarselt.

Avasta rünnak ja reageeri ruttu
Mõtle läbi, millised lahendused ja meetmed võimaldavad rünnakut kiiresti avastada ning kuidas toimub ründe kiire tõrjumine.

Teavita CERT-EEd
Kui langesid lunavara ohvriks või kahtlustad, et saadud fail on pahatahtlik, teavita CERT-

EEd cert@cert.ee. Saame omalt poolt nõustada, kuidas antud olukorras kõige paremini toimida, kuidas tuvastada ründevektorit, ründajat, millist pahavara on kasutatud, kas andmeid on varastatud ning mida teha, et samalaadne intsident ei korduks.

Teavita Andmekaitse Inspektsiooni

Kui asutust tabanud lunavararünnaku tõttu tekib olukord, kus kasvõi lühiajaliselt puudub asutusel endal või inimestel juurdepääs isikuandmetele ning inimene võib seetõttu saada varalist või mittevaralist kahju (nt võimalik tervisekahju, kui ei saa õigeaegselt ravimit või invasiivset ravi), on tegu rikkumisega isikuandmete kaitse üldmääruse tähenduses ning juhtunust tuleb teavitada Andmekaitse Inspektsiooni. Teavitada tuleb alati ka siis, kui on põhjendatud kahtlus, et andmed on juba ka varastatud.