

Lunavararünnaku ennetamine

Kuidas kaitsta ennast lunavararünnaku eest?

Lunavaraga nakatumise ennetamiseks ja tagajärgede leevendamiseks on mõned lihtsad reeglid, mida järgida:

- kasuta viimast tarkvaraversiooni ning veendu, et kõik uuendused on paigaldatud,
- tee regulaarselt varukoopiaid,
- piira süsteemi kasutajate õigusi,
- koolita personali küberohtude teemal.

Lühijuhend lunavarajuhtude ennetamiseks ja lahendamiseks

Ülevaade

Lunavara on muutunud üheks suurimaks ohuks kõikidele internetikasutajatele. Ründajad nakatavad süsteemi pahavaraga, mille eesmärk on krüpteerida kasutaja failid. Pärast krüpteerimist üritavad ründajad kasutajalt failidele ligipääsu taastamise eest raha nõuda. Sellised ründed võivad olla väga edukad, eriti korporatiivvõrkudes, kus on laialdaselt kasutusel failiserverid.

Soovitused

Isegi kui sa ei ole kunagi lunavararünde ohvriks langenud, tuleks siiski mõelda, milliseid ennetavaid meetmeid saaksid rakendada, et ka tulevikus nakatumist vältida või nakatumise korral minimaalseid kahjusid kanda.

Ennetavad meetmed

- Krüpteeriva lunavara tagajärgi aitab leevendada töökindel varundamine. Kui saad tagavarakoopiast andmed taastada, siis pole ründajal võimalik andmete vabastamise eest lunaraha nõuda. Samas ei kaitse see paraku andmevarguse eest.
- Vähemalt üks varukoopia peab asuma *offline*-režiimis (näiteks väline kõvaketas, DVD või lint). Kuna lunavara püüab krüpteerida faile nii kohalikul kettal, välistel andmekandjatel kui ka võrguketastel, peab varukoopia asuma eraldi, et tagavarakoopia omakorda võrguketta krüpteerimise korral ei nakatuks.
- Ära unusta, et lunavara võib taustal toimida mitu päeva enne kui see ükskord avastatakse.

- Pea meeles, et ka tagavaraserverid on haavatavad ning on samamoodi ründajate sihtmärgiks.
- Kontrolli, millist varundusmeetodit kasutad. Olukord, kus failid on krüpteeritud ning peaks toimuma näiteks inkrement ehk sammvarundus, võib juhtuda, et varukoopiaid kirjutatakse üle krüpteeritud failidega.
- Kontrolli regulaarselt varunduse seisukorda ning terviklust.
- Aktiveeri failiserverites *audit logging* ehk revisjonlogimine tuvastamaks ka võimalikud nakatunud arvutid, mis omakorda võrgukettal asuvaid faile krüpteerida võivad.
- Keela kõikjal SMBv1 kasutamine.
- Teavita töötajaid, eriti eemal viibivaid, ohust ning tuleta neile meelde, et tundmatutele linkidele ei tohi vajutada ega tundmatuid manuseid avada.
- Võta kasutusele monitooringuskriptid tuvastamaks süsteemid, mis muudavad lühikese aja jooksul suure hulga faile. Sellist monitooringut saab kasutada tuvastamaks proaktiivselt faile krüpteeriv süsteem.
- Lunavaraga nakatumine toimub kõige sagedamini järgmiselt:
 - E-kirja manuses sisalduv käivitab pahatahtliku koodi.
 - E-kirjaga saadetud lingid viitavad pahatahtliku sisuga dokumentidele.
 - Kasutatakse ära haavatavaid veebilehitsejaid või tarkvarakomponente.
 - Kasutatakse ära avalikke kaugtöölaua teenuseid nagu Remote Desktop Protocol (RDP), mille kaudu saadakse ligipääs ohvri süsteemile.
- Vaata üle oma meililüüsi ja veebilüüsi turvapoliitikad ning kindlusta, et logimine on sisse lülitatud (see aitab ka tuvastada nakatunud kasutajad).
- Meililüüs ja veebilüüs peaksid blokeerima või panema karantiini kõik dokumendid, mis sisaldavad käivitatavaid faile, konteineriformaate ja faile, mis võivad potentsiaalselt sisaldada aktiivsisuga faile. Näiteks tuleks blokeerida või panna karantiini alltoodud faililaiendid:
 - Konteineriformaadid: .zip, .rar, .ace, .gz, .tar, .7z, .z, .bz2, .xz, .iso
 - Potentsiaalselt aktiivsisu sisaldavad failid: .pdf, .doc, .rtf, .ppt, .xls, .odt
 - 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
- Kindlusta, et uuenduspoliitikat rakendatakse ka veebilehitsejatele, sealhulgas laienditele ja pistikprogrammidele.
- Vaata üle oma “Too ise oma seade” (BYOD) poliitika, vähendamaks nakatunud seadete arvu, mis ettevõtte masinaid nakatada võivad.
- Rakenda minimaalõiguste printsiipi ehk pääsupoliitikat, millega tagatakse kasutajatele nende igapäevatööks minimaalsed õigused. Tugev pääsupoliitika aitab piirata lunavara levikut või võib isegi peatada lunavara käivitumise, sest selle jaoks pole piisavaid õigusi.

Lunavarajuhtumi lahendamine

- Juhtumi tuvastamise korral eemalda kohe nakatunud seade võrgust (ära unusta juhtmevaba võrku).
- Juhul kui tahad ise sooritada esmase pahavaraanalüüsi, peab enne kettahõivet läbi viima mäluhõive (juhul kui süsteemi ei ole välja lülitatud).
- Mõnel harval juhul on võimalik mõne faili taastamine (näiteks Windowsi varjukoopiad, tömmiste või vigast krüpteerimist kasutanud lunavara puhul).
- Sellise meetodi peale ei tohi lootma jääda ning tuleb rakendada ülal kirjeldatud ennetavaid meetmeid.
- Nakatumise korral soovitab CERT-EE operatsioonisüsteemi tagavarakoopiast taastada või teha puhas install taasnakatumise vältimiseks. Enne tagavarakoopiast taastamist tuleb veenduda, et tagavarakoopia pole samuti pahavaraga nakatunud.
- Enne ründajatega ühendust võtmist kaalu hoolikalt riske. Pole garantiid, et lunaraha maksmisel dekrüpteerib kurjategija failid. Samuti toetatakse maksmisel kurjategijate edasisi tegevusi.
- Võimalusel jäta alles tegelik nakatunud seade, mille saad dekrüptori väljatulekul taas kasutusele võtta.
- Kui langed lunavara ohvriks, on võimalik teada saada, mis lunavaraga oli tegemist aadressil id-ransomware.malwarehunterteam.com.
- Dekrüptori olemasolu saad kontrollida aadressil <https://www.nomoreransom.org/en/index.html>.
- Kui langed lunavara ohvriks või kahtlustad, et saadud fail on pahatahtlik, teavita kindlasti CERT-EE'd cert@cert.ee. Saame sind abistada. Saadud info annab meile parema ülevaate Eesti kübermaastikust ning oskame siis paremini teha ennetustööd lunavara ja teiste sarnaste intsidentide vältimiseks.