RIIGI INFOSÜSTEEMI AMET

Kaugtöö riskid seoses pahavara levikuga

Lühidalt

Pandeemiast tulenevalt on kaugtöö muutunud väga paljude töötajate ja ettevõtete jaoks igapäevaelu osaks ja see jääb nii ka edaspidi. Ehkki kaugtöö lahenduste turvalisemaks muutmise vajadustest on palju kirjutatud nii Eestis kui mujal, soovime juhtida tähelepanu ühele tööandja jaoks kaasnevale selgele riskile: **kaugtöö puhul võib olla oluliselt raskem tuvastada tööjaama nakatumist pahavaraga ja sellele õigel ajal jaole saada**. Kaugtööd võimaldavad seadistused ja turvareeglid tuleks seetõttu üle vaadata ja vajadusel korrigeerida.

Emotet pahavaralainest tulenevad ohud

Käesoleval sügisel on Eestis ja ka mujal maailmas väga laialt levimas Emotet troojalane, millega nakatumine toimub enamasti e-postiga kaasas olevate pahaloomuliste manuste avamise, harvemini linkide klikkimise teel. Taolisi Emoteti sisaldavaid meile on viimasel ajal liikunud Eesti küberruumis ainuüksi ühes nädalas tuhandeid. Tõhusamad viirusetõrjeprogrammid ja õigesti seadistatud meilifiltrid ja tulemüürid aitavad seda ohtu märkimisväärselt vähendada, ent ka pahavara on võimeline oma tunnuseid ja levimisviisi kiiresti muutma ning on praeguse laine ajal seda ka mitmeid kordi teinud (vt ka viimane RIA kvartaliülevaade). Ehkki nakatumisest ei pruugi kasutajale olla esialgu ühtegi nähtavat märki, on ettevõtte või asutuse IT-spetsialistidel seda siiski võimalik tuvastada ebaloomuliku liikluse ja autoriseerimata andmevahetuse tõttu. Emotetiga nakatumisel loob seade ühenduse kurjategijate kontrolli all oleva juhtserveriga ning esimeses etapis varastab näiteks brauseritesse talletatud kasutajatunnused ja paroolid ning meilikliendis oleva postkasti sisu ja kontaktiraamatu ning edastab need andmed juhtserverile.

Kaugtöö tõttu on paljud asutused ja ettevõtted olukorras, kus kasutajate seadmed on töötajatel kodus, ühendatud kodusesse WiFi võrku. Kuigi ametialane suhtlus (töömeilid) liigub enamikel juhtudel VPNi kaudu, kasutab sama seade muude lehtede sirvimiseks või näiteks erameili lugemiseks otse kodust internetti (nn *split tunnel*). Endiselt leidub ka tööandjaid, kes ei nõua töömeili kasutamiseks üldse VPN-i (või asub väline teenus mõnes avalikus pilves ning sel juhul ei ole VPN vajalik). VPN-i väline liiklus asutuse seadmes aga ei ole kuidagi tööandjal seiratav ega vajadusel kontrollitav.

Seega võib juhtuda, et tööandja seadme nakatumine ja andmete kadu toimub ettevõtte jaoks märkamatult ning ka tagantjärele on pea võimatu aru saada, kuidas nakatumine toimus ja kas ja milliseid andmeid on lekkinud. Eestis aset leidnud rohkem kui saja Emotetiga nakatumise hulgas on mitmeid juhtumeid, kus intsidendi mõju ja tekkinud kahju ei ole võimalik adekvaatselt hinnata, kuna seadet on kasutatud ka mujal kui asutuse sisevõrgus. Kuna Emoteti ja paljude teiste pahavaradega nakatumine **tähendab enamasti ka andmeleket,** millega kaasneb Andmekaitse inspektsiooni teavitamiskohustus ja halvemal juhul trahvid ning usaldusekadu, on kahjude hindamine ja piiritlemine aga hädavajalik.

Soovitused infoturbejuhtidele

1. Olukorrapildi tagamiseks:

1.1. Täpsusta üle, kas sinu ettevõte kasutab oma meiliserverit või avalikku pilveteenust.
Oma meiliserveri puhul ei ole kahetasemelist autentimist sageli lihtne rakendada ning sel juhul peaks ligipääs toimuma vaid üle VPNi. Avaliku pilveteenuse puhul peaks olema rakendatud kahetasemeline autentimine (2FA) ning ligi peaks saama vaid lubatud seadmed.

1.2. Muuda tööseadmete kaudu toimuv internetiliiklus võimalikult nähtavaks ja kontrollitavaks. Seda saab teha suunates kogu liikluse läbi VPN-i või siis tuleb koguda ja säilitada keskselt tööjaamade võrgulogid.

1.3. Pööra praegu iseäranis suurt tähelepanu väljuva võrguliikluse anomaaliatele. Analüüsi väljuva liikluse logisid (http Proxy, DNS logid) tuvastamaks, kas seade on asunud suhtlema võõra juhtserveriga. Emotetiga seostatud juhtserverite äratundmiseks on abi sellest veebilehest:

https://feodotracker.abuse.ch/browse/

2. Nakatumise vältimiseks:

2.1. Veendu, et lõppkasutajate seadmetes on aktiivne ja uuendatud viirusetõrjeprogramm (soovitavalt rakendatud kohustuslik „full-scan“ vähemalt kord nädalas)

2.2. Vaata üle veebi- ja meilifiltrite seadistused. Soovitavalt blokeeri MS Office'i makrosid sisaldavad failid ning suuna käivitatavad- (nt. .exe) või konteinerfailid (.zip) täiendavaks kontrolliks võimaliku pahavara suhtes

2.3. Diferentseeri (ja minimeeri) kasutajaõigusi rollipõhiselt, vajadusel loo ühele kasutajale erinevad kontod erinevate õigustega

2.4. Soovitav on keelata brauserites paroolide ja kasutajanimede salvestamine ning kustutada ettesalvestatud paroolid. See aitab vähendada nakatumisest tekkivat kahju.

2.5. Hoia kasutajad aktuaalsete ohtudega kursis ja soovita jälgida CERT-EE postitusi Twitteris – sinna jõuavad hoiatused hetkel liikvel olevate pahavarade kohta kõige kiiremini

3. Kui on põhjust kahtlustada, et seade võib olla nakatunud:

3.1. Isoleeri seade võrgust niipea kui võimalik

3.2. Kontrolli esimesel võimalusel üle ka teised seadmed, mis võivad olla nakatunud

Emoteti tuvastamisel võib olla abi Jaapani CERT-i avalikuks kasutamiseks mõeldud tööriistast:

https://github.com/JPCERTCC/EmoCheck/releases

3.3. Muuda ära kasutajatunnused ja paroolid (eriti local admin ja domain admin)

3.4. Nakatunud konto omanik peaks alternatiivkanali kaudu teavitama oma kontakte, et temalt tulnud meilid, eriti manustega, võivad sisaldada pahavara

3.5. Teavita CERT-EE-d intsidendist https://raport.cert.ee/ kaudu või cert@cert.ee

Lisalugemiseks

1. PaloAlto Unit 46 blogipostitus, mis selgitab konkreetse näite najal lahti, kuidas Emotet levib varastatud meilivestluste abil:

https://unit42.paloaltonetworks.com/emotet-thread-hijacking/

2. Ameerika Ühendriikide riikliku julgeolekuagentuuri (NSA) soovitused, kuidas aru saada, et seade võib olla nakatunud pahavaraga:

https://media.defense.gov/2020/Sep/17/2002499615/-1/-1/0/COMPROMISED_PERSONAL_NETWORK_INDICATORS_AND_MITIGATIONS_20200914_FINAL.PDF