Küberpettur ründas Eesti firmat

22. juuni 2015, 08:00
Allikas: Äripäev
Autor: Marge Väikenurm, marge.vaikenurm@aripaev.ee
Foto: Väinu Rozental

Jalatsitootja Samelin omanikult Leida Kikkalt ja tema Norra äripartnerilt üritas meilipostkastidesse tunginud küberpettur suurt summat välja meelitada. Norra ettevõtja on praeguseks politseisse pöördunud.

"See oli nii peen trikk!" imestas Leida Kikka, kellele saatis Norra koostööpartner e-kirja lubadusega üle kanda 73 000 dollarit, millega Kikka firma Pakistani ettevõttele kauba eest maksaks. Kikka oli nõus.

Sama päeva õhtul aga helistas norrakas Kikkale, uurides, miks viimane makse tagasi kutsuda palus. "Küsis, et mis juhtus? Miks ma ei või sulle raha kanda? Sain sinult praegu meili, et ära kanna - meil on Eestis dollarikanded keerulised, meie valitsus ei ole seda aktsepteerinud ja annan teise arvenumbri, kuhu kanda," meenutas Kikka vestlust ettevõtjaga, kellega on pikalt, 20 aastat äri ajanud. Pettur sekkus kirjavahetusse, suunates norrakat võõrale arvelduskontole raha kandma. Kuna Norra ettevõtja raha tagasikutsumisega kaasa ei läinud, jõudis teele saadetud summa probleemideta Samelini arvele.

Kui Kikka kinnitas, et ei saatnud kirja, kontrollis norrakas aadressi, millelt e-kiri tegelikult saabus. Aadress sarnanes Kikka omale, aga petukirja saatja oli selle teele pannud domeenilt, mille lõpp oli ee asemel net, kusjuures kirjast koopia saanute meiliaadress oli samamoodi muudetud. Võõras aadress oli registreeritud päeval, mil kiri teele läks.

Suhtles petturiga

"Olin püha viha täis. Võtsin meiliaadressi l.kikka@samelin.net (petturi meiliaadress - toim) ja saatsin meili," ütles Kikka, kes uuris häkkerilt, kuidas ta kirjavahetusele ligi pääses ja hoiatas, et on pöördunud politseisse. Viimast ei ole Kikka tegelikult siiani teinud, kuigi politsei ja Riigi Infosüsteemide Amet (RIA) seda tungivalt soovitab.

Kikkale saabus ootamatult kahe päeva pärast petturi vastus, kus ta lubas oma tegevuse lõpetada ja anda Kikkale nõu, kuidas oma e-postkasti kaitsta. Kikka jättis kirjale vastamata. "Muutsime, nii mina kui ka Norra partner, kõiki arvutiparoole," lausus Kikka.

Saaga ei olnud sellega siiski ühele poole saanud. "Kirjutasin Norra partnerile kirja, et palun selgita välja, kas materjal on olemas - olen nüüd valmis raha Pakistani saatma. Esmaspäeva hommikul saabus meil, et materjal on valmis ja kohe teatan, kuhu võid raha kanda," kirjeldas Kikka.

Järgmine kiri saabus tunni pärast. "Selles oli, et pean kandma raha offshore-firmale, sest Pakistanis on praegu probleemid maksetega. Kaasa jooksis minu ja partneri eelneval nädalal olnud kirjavahetus," sõnas

Kikka. Ettevaatlik Kikka kontrollis meiliaadresse. Sel korral oli nendesse lisatud liigne l-täht. Koopia oli näiliselt saadetud ka Norra firma finantsdirektorile, kelle nimes oli sama muudatus tehtud.

Kumbki ettevõtja tänu tähelepanelikkusele rahast ilma ei jäänud, küll aga kinnitab juhtum, et uus petuskeem on Eestis liikvel.

RIA analüütik Anto Veldre kirjeldas, kuidas aastaid tagasi käis arvete kaaperdamine füüsiliselt - ühes Euroopa riigis korjasid kurjategijad väärikas rajoonis postkastidest kokku portsu arveid. Arved kujundati ümber. Sarnaste rekvisiitidega paberil muudeti pangaarve numbrit, seejärel pandi arved postkastidesse tagasi. Kurjategijatel õnnestus vähese vaevaga varastada mitu miljonit eurot.

Täna on arvete kaaperdamine kolinud elektroonilisse keskkonda, tõdes Veldre. Kurjategijad hangivad endale ligipääsu firma arvutivõrku ning ühel või teisel moel saavutavad selle, et ülekanne tehakse kurjategijate kontrolli all olevale kontole. Sisuliselt sooritatakse kaks kuritegu korraga: nii pettus kui ka häiritakse arvutisüsteemi tööd. “Olete tõsise asja peale sattunud. See on väga kaval asi ja lõppkasutajale väga ohtlik, sest nõuab tõsiselt head IT-kvalifikatsiooni, saamaks aru, kuhu sisse on murtud,” ütles Veldre.

Läinud töönädala lõpus tegi Norra ettevõtja Kikka sõnutsi politseisse avalduse. "Norra politsei jõudis jälgede uurimisega Ungarisse," ütles Kikka, kes ise politseisse pöördunud ei ole. "Kuna Norra esitas avalduse, siis mina ei esita. Mul on nii kiire."

Tasub teada

Antud pettus on ohtlik, sest:

- valitakse piisava käibega firma ning modifitseeritakse piisavalt suuri arveid ohvri abistamine on komplitseeritud, kuivõrd ohvrile e-kirja saates satuvad ka nõuanded kurjategijate kätte kui petukatse on juba tehtud, kaasnevad sellega väljaminekud igal juhul. Küsimus on vaid, kas firma maksab oma IT-süsteemi puhastamise eest või kantakse raha mõttetult kurjategijatele.

Nõuanded:

- Kui on kahtlus, et teie e-postkast on kaaperdatud ja võidakse arve võltsida, siis:
- igal juhul ja esimesel võimalusel pöörduda politseisse. Enamasti viivad jäljed välismaale ning vaid politsei saab seal edukalt päringuid teha. koheselt informeerida CERT-EE-d, kust saate esmast abi ja nõuannet. Kui kirjakast on kaaperdatud, kasutage telefonisuhtlust, mitte e-posti. olla valmis kogu oma arvutivõrgu karantiini paigutamiseks, eesmärgiga see infiltreerunud kurjategijatest puhastada. Olenevalt sissetungi raskusastmest võib kogu IT-puhastusteenus olla suhteliselt kulukas.

Allikas: Riigi Infosüsteemide Amet

Mõni hetk hiljem otsustas Kikka, et siiski teeb politseisse avalduse. Politseist öeldi Äripäevale, et seejärel saab alustada ka menetlust ja vajadusel suhelda Norra kolleegidega.

Kikka andis RIAle nõusoleku võtta ühendust tema firma IT-spetsialistiga. "Et saaks minu serveris uurida - ehk õnnestub midagi tuvastada."

Kas RIA tegi serveris uurimistööd, ei osanud Anto Veldre kinnitada. "Kui ohver nii ütleb, ju nii on. Aga tean, et CERT (tegeleb küberturvalisuse tagamisega - toim) on temaga rääkinud ja sellest oli abi," sõnas Veldre ja rõhutas taas, et politseisse tuleks avaldus kirjutada. "Tavainimene ei näe kogupilti. On oluline, et küberkuritegu registreeritud oleks."

Ohtlik kirjavahetus

Kindlasti ei tohiks petturiga kirjavahetust pidada. "See võib tunduda huvitav ja pakub emotsionaalset rahuldust, aga seal on mitu ohtu. Võib teise poole välja vihastada, näiteks teeb veel ühe liigutuse, hävitades midagi. Sageli tekib ka IT-meestel kiusatus ja üritavad petturit sabapidi urust välja tõmmata. Jälgi peaksid aga koguma profid," rääkis Veldre.

Petturi lubadus ohvrile õpetada postkasti kaitsmist annab Veldrele põhjuse tabavaks võrdluseks. "Annan tänaval kellelegi vastu nina ja siis ütlen, et oi issand, vabandage väga, läks valesti. Viin teid nüüd apteeki - võib-olla selle käigus läheb käsi veelgi sügavamale taskusse. Ettevaatust-ettevaatust! Ei ole need asjad nii lihtsad kui paistavad."

Äripäev rääkis mitme ettevõtjaga, neist ükski polnud sarnase pettusega kokku puutunud. Näiteks logistikafirma Kühne + Nagel juht Mart Ambur rääkis, et nende IT-turvapoliitika on rahvusvahelise turvaosakonna hallata. Ambur nentis, et täielikku kindlustunnet ei saa aga ühelgi ettevõtjal olla. "Kui miski tundub kahtlane, tuleb äripartnerilt üle küsida."

Kommentaar

Väino Kiuru
Keskkriminaalpolitsei küberkuritegude juhtivuurija

- Sellistest juhtumitest on sel aastal politseid teavitatud vähem kui kümnel korral. Ühelgi juhul ei ole leidnud kinnitust, et kurjategija oleks tegutsenud Eestist, samas ei ole keeruline jätta maha välismaiseid digijälgi.
- Ainult parooli vahetusest alati ei piisa - näiteks kui arvutis on keylogger, mis salvestab kõik tegevused, sealhulgas kõik klaviatuuril tehtud klahvivajutused infoga.
- Pärast konto kaaperdamist tuleb üle vaadata kõik turvalisusküsimused, kuna konto parooli ja ligipääsu saab taastada mitmel moel.
- Samuti jäetakse sageli kahe silma vahele meilide suunamine - kõik sissetulevad ja väljaminevad meilid saab automaatselt suunata teisele meiliaadressile ehk küberpätil ei olegi vaja igapäevast ligipääsu kannatanu arvutisüsteemile.
- Et ennast maksimaalselt kaitsta, peab arvuti olema tihti ja regulaarselt uuendatud operatsioonisüsteemiga.
- Kasvav oht on igasugused nutikad seadmed, kus toimub automaatne andmete sünkroniseerimine, st et paroolid ja kasutajanimed on seadmesse salvestatud ning süsteem toimib automaatselt.
- Kui inimesel endal jäävad IT-teadmised tavakasutaja tasemele, tuleks aegajalt lasta oma seadmed üle vaadata IT-spetsialistidel.