JUSSI HELTTUNEN

Kotikäyttäjien reitittimillä tehty palvelunestohyökkäys aiheutti ongelmia OP:n pankki- ja luottokorttiasiakkaille.

Kaappari vaanii verkkolaitettasi

Tarpeettomasti verkkoon päin avoimet palvelut tai tehdasasetukset voivat altistaa modeemit ja reitittimet hyväksikäytölle.

VUODEN VAIHTEESSA verkkopankkeja kaataneet hyökkäykset tehtiin pääosin kaapattujen modeemien ja reitittimien kautta. Perinteisesti palvelunestohyökkäyksissä on käytetty kaapattuja tietokoneita.

”Verkkolaitteissa voi esimerkiksi olla auki käyttäjälle tarpeettomia palveluja, joita hyväksikäyttämällä hyökkäykset tehdään. Jos lisäksi oletussalasanoja ei ole vaihdettu, laitteet ovat alttiita hyväksikäytölle esimerkiksi botnetin osana”, Soneran johtava tietoturva-asiantuntija **Arttu Lehmuskallio** sanoo.

Lehmuskallion mielestä peruskäyttäjän ei voi odottaa miettivän tai hahmottavan tällaisia ongelmia. Hänestä myyjän olisi järkevämpää toimittaa laitteet konfiguroituna niin, että kaikki tarpeettomat palvelut on suljettu ja käyttäjä voi avata niitä tarvittaessa.

Lisäharmia aiheuttaa se, että kotikäyttäjät harvemmin päivittävät verkkolaitteidensa laiteohjelmistoa eli firmwarea. Vastuu laiteohjelmiston päivittämisestä on kuitenkin laitteen omistajalla. Vaikka reitittimen olisi ostanut teleoperaattorilta nettiyhteyden kylkiäisenä, päivitysvastuu säilyy kuluttajalla, ellei toisin ole sopimuksessa mainittu. Poikkeuksen muodostavat vuokralaitteet, jotka liittyvät usein esimerkiksi Elisan tai Soneran tarjoamiin viihdepaketteihin.

”Lähtökohtaisesti kyse on kuluttajan omasta vastuusta”, vahvistaa tietoturva-asiantuntija **Aleksi Tarhonen** Kyberturvallisuuskeskuksesta.

VERKKOLAITTEEN HYVÄKSIKÄYTTÖ tapahtuu usein omistajan huomaamatta. Seurauksena voi äärimmäisissä tapauksissa olla internet-liittymän sulkeminen, jos operaattori huomaa, että tietystä ip-osoitteesta lähtee häiritsevää liikennettä. Operaattorit pyrkivät ilmoittamaan sulkemisesta, jos se vain on mahdollista.

”Jos kuluttajan laitetta käytetään hyväksi hänen tietämättään, uhrihan hän siinä tilanteessa on”, Tarhonen sanoo.

Turvaa reitittimesi

SUURIN OSA uusista teleoperaattoreiden toimittamista modeemeista ja reitittimistä on konfiguroitu valmiiksi turvallisiksi, mutta jos olet ostanut laitteesi itse tai et ole varma päivitysvastuusta, seuraa näitä ohjeita:

1. Kirjaudu reitittimen hallintaliittymään. Kirjoita selaimeen hallintaliittymän ip-osoite, usein muotoa 192.168.x.x. Oikea osoite löytyy esimerkiksi laitteen käyttöohjeesta tai valmistajan tai palveluntarjoajan verkkosivulta.
2. Vaihda oletussalasana ja estä pääsy hallintapaneeliin muualta kuin lähiverkostasi.
3. Tarkista hallintaliittymässä, onko laitteeseen saatavilla uutta laiteohjelmistoa (firmwarea). Myös valmistajan verkkosivuilta voi etsiä tietoa uusista päivityksistä.
4. Sulje tarpeettomat portit ja palvelut. Jos et tiedä, mitkä ovat tarpeettomia, kysy palveluntarjoajan teknisestä tuesta.

Hyökkääjä pani pankit polvilleen

Vuodenvaihteen palvelunestohyökkäykset osoittivat, ettei pankkien torjuntavalmius ole riittävä.

UUDENVUODENAATTONA ALKANUT hyökkäys aiheutti Osuuspankin verkkopalveluihin vakavia häiriöitä, jotka jatkuivat tammikuun alkupäiviin asti. Verkkopankin kaatuilun lisäksi käteisen nostaminen ja korttimaksut saattoivat hetkellisesti estyä.

Nordeaan iskettiin 2. tammikuuta. Keskusrikospoliisin mukaan kumpaakin pankkia yritettiin kiristää. Danske Bankin tammikuiset verkkopankin ongelmat osoittautuivat sittemmin sisäiseksi järjestelmäviaksi.

OP:n viestintäjohtaja **Carina Geber-Teir** kertoo, että hyökkäykset olivat Suomen mittakaavassa laajuudeltaan ja kestoltaan ennen näkemättömiä. Hänen mukaansa suurin osa verkkopalveluista oli kuitenkin jatkuvasti käytössä.

Ulkomailta oli vaikea päästä OP:n verkkopankkiin pidempään kuin Suomesta, sillä hyökkäyksen vaikutusta pyrittiin vähentämään suodattamalla liikennettä tavallista tehokkaammin.

TÄYDELLINEN HYÖKKÄYKSEEN varautuminen on pankkien mukaan mahdotonta. Järjestelmiä eriytetään, jotta yhteen kohteeseen kohdistetun hyökkäyksen vaikutukset olisivat mahdollisimman pienet, Dansken **Taina Mustamo** kertoo.

”Hyökkäysmenetelmätkin kehittyvät. Nämä iskut osoittivat, että juoksuvauhtia on lisättävä”, Geber-Teir toteaa.

OP piti hyökkäyksen aikana puhelinpalvelunsa poikkeuksellisesti auki ympärivuorokautisesti, Nordealla palvelu on muutenkin jatkuvasti saatavilla. Juoksevia pankkiasioita saattoi hoitaa asiakaspalvelijoiden kautta salasanatunnistautumisen turvin.

Sosiaalisen median kanavat ovat osoittautuneet kaikilla pankeilla hyväksi lisävälineeksi tiedottamisessa.

HYVÄ TAPA varautua yhteysongelmiin on myös pyrkiä maksamaan laskut ajoissa ja hyödyntää e-laskumahdollisuutta. Jos verkkopankissa on varayhteys, sitä kannattaa kokeilla. Ulkomailta sivuille voi päästä sujuvammin F-Securen Freedomen kaltaisella vpn-yhteydellä.

Geber-Teir muistuttaa, että rikolliset voivat käyttää hyökkäysten aiheuttamaa kaaosta myös sumuverhona tietojen kalastelulle, jota voi tapahtua esimerkiksi sähköpostitse tai somessa. ”Maailmanlaajuisesti on olemassa viitteitä siitä, että ihmisten epätietoisuutta yritetään hyödyntää.” ◁

OLLI VÄNSKÄ

Soneran Lehmuskallio kertoo, että vastuukysymykset ovat askarruttaneet operaattoreita. ”Myyjällä on aina vastuu virheestä, mutta voidaanko tietoturvaongelma katsoa virheeksi”, Lehmuskallio kysyy.

Kilpailu- ja kuluttajaviraston lakimies **Jukka Kaakkola** kertoo, ettei kuluttajariitalautakunnasta ole nähtävästi vielä saatu suuntaa-antavia ennakkoratkaisuja, joiden perusteella voisi tehdä päätelmiä vastaavassa tilanteessa.

”Jos kuluttajariitalautakuntaan tulisi tällainen asia, se pitäisi ratkaista tapauskohtaisesti kaikki eri puolet arvioiden. Yleisellä tasolla arvioituna virheen tunnusmerkkeihin kuluttajansuojalaissa kuuluu se, ettei tuote ominaisuuksiltaan vastaa sitä, mitä kuluttaja voi perustellusti odottaa kyseiseltä tuotteelta. Lisäksi jos ongelman vuoksi tavara ei sovellu siihen tarkoitukseen, johon se on tarkoitettu, voitaisiin myös sitä pitää myyjän vastuulla olevana virheenä”, Kaakkola sanoo.

Kaakkola huomauttaa, että kuluttajan voidaan edellyttää noudattavan saamiaan ohjeita, jos niitä on päivitysten osalta annettu.

TIETOTURVA-AUKKOJA PALJASTUU kuitenkin vähän väliä ja reitittimien valmistajat tekevät päivityksiä laiteohjelmistoihin. Operaattorit ajavat kyllä päivitykset niihin laitteisiin, joihin niillä on pääsy. Esimerkiksi DNA:n toimittamista modeemeista noin 65 prosenttia on etäpäivitettäviä ja operaattori pyrkii tarjoamaan laiteohjelmistopäivitykset internet-asiakkailleen, kertoo DNA:n tuotekehityksen esimies **Ville Partanen**.

”Haasteellisempia tapauksia ovat ne asiakkaat, jotka ostavat retail-kaupasta reitittimen ja meiltä pelkän nettiyhteyden, koska silloin emme pääse näiden laitteiden asetuksiin kiinni, ja niissä voi olla joitakin asetuksia päällä, jotka heikentävät tietoturvaa”, Partanen kertoo. ◁

HEIDI KÄHKÖNEN

LYHYESTI

▷ **GIGABYTE HEIKENTÄÄ** vaivihkaa tuotteidensa laatua. Huonompilaatuisia tuotteita ei pysty erottamaan mallinumeron perusteella. Esimerkiksi nyt kaupoissa myytävä B85M-HD3-emolevy on eri malli kuin aiemmin myyty. Nykyversiossa virransyöttö on huonolaatuisempi, mikä voi aiheuttaa lämpöongelmia.

▷ **HALVAT WINDOWS-LAITTEET** saapuvat kauppoihin ryminällä. Alhaiset hinnat selittyvät osittain Microsoftin Windows 8.1 With Bing -käyttöjärjestelmällä, joka on valmistajille ilmainen alle 9” näytöllä varustettuihin laitteisiin, ja vain 10 dollarin hintainen suurempinäyttöisiin laitteisiin.

▷ **PC-MYYNTI ELPYY.** Tietokoneita myytiin viime vuoden viimeisen vuosineljänneksen aikana prosentin verran enemmän kuin vuotta aikaisemmin. Kyseessä on ensimmäinen kerta kahteen vuoteen, kun pc-toimitukset ovat kasvaneet.

▷ **NÄYTÖNOHJAINVALMISTAJA NVIDIA** on julkistanut Geforce GTX 960 -mallin. Noin 220 euron hintaiset näytönohjaimet erottuvat edukseen etenkin suorituskykyynsä nähden alhaisella virrankulutuksella.

▷ **HUONOT SALASANAT** ovat yhä merkittävä tietoturvariski. Vuoden 2014 yleisin salasana oli 123456, toiseksi yleisin password ja kolmanneksi yleisin 12345.

▷ **WINDOWS 7:N** Mainstream-tukivaihe on päättynyt. Seiska ei saa enää uusia ominaisuuksia, mutta tietoturvapäivityksiä on luvassa vuoteen 2020 asti.

▷ **KESTÄVIMMÄT KIINTOLEVYT** valmistaa Hgst, pilvitallennusyhtiö Backblaze kertoo. Hgst:n kiintolevyt on suunnattu lähinnä yrityskäyttöön. Kotikäyttäjien kiintolevyistä Western Digitalit kestävät parhaiten, Seagaten levyt hajoavat herkimmin.

▷ **TIEDOSTOT PANTTIVANGIKSI** ottava kiristyshaittaohjelma leviää Suomessa sähköpostin välityksellä. Viestintäviraston Kyberturvallisuuskeskus muistuttaa, että epäilyttäviä ja tuntemattomilta saapuvia liitetiedostoja ei kannata avata.

▷ **KYBERHYÖKKÄYKSET ISKEVÄT** yhä useammin Silverlightiin. Aiemmin nettirikollisten kohteena oli Java, jonka hyväksikäyttö on hieman laantunut. Myös pdf-tiedostojen avulla yritetään hyökätä säännöllisesti.