Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus

nro 15

20.5.2014

Yrityksiin kohdistuva tietoverkkorikollisuus

Yritysturvallisuuden kansallinen yhteistyöryhmä

Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekatsaus

Sisältö

Johdanto

Tämä on järjestyksessään 15. yrityksiin kohdistuvan ja yrityksiä hyödyntävän rikollisuuden tilannekatsaus. Tilannekatsauksen julkaisee sisäasiainministeriön asettama poikkihallinnollinen yritysturvallisuuden kansallinen yhteistyöryhmä, jossa on edustettuna aiheen kannalta keskeiset viranomaiset, elinkeinoelämä sekä ammattijärjestöt. Tilannekatsauksen valmistelusta on vastannut Keskusrikospoliisi yhteistyössä useista eri toimijoista koostuvan asiantuntijaverkoston kanssa.

Tilannekatsausta on julkaistu vuodesta 2006 kahdesti vuodessa siten, että syksyllä on ilmestynyt yleinen, yrityksiin kohdistuvan rikollisuuden tilannekatsaus. Keväällä on ilmestynyt teematilannekatsaus, jossa on tarkemmin syvennytty yhteen rikollisuusilmiöön.

Kansallinen yhteistyöryhmä päätti kokouksessaan elokuussa 2013 tilannekatsauksen uudistamisesta. Päätöksen mukaisesti syksyllä ilmestyvä tilannekatsaus sisältää jatkossa enintään neljä yrityksiin kohdistuvan rikollisuuden kannalta keskeistä teemaa. Valituista teemoista kuvataan suppeasti ilmiö ja sen laajuus, tekojen luonne sekä tekojen vaikutukset yrityksiin. Tavoitteena uudessa rakenteessa on, että eri rikosilmiöt ovat keskenään vertailukelpoisia. Lisäksi kunkin ilmiön kehittymistä ajallisesti on mahdollista seurata. Syksyn tilannekatsaus perustuu olemassa oleviin tietoihin.

Keväällä julkaistava tilannekatsaus tulee jatkossakin olemaan teematilannekatsaus. Teemaksi valitaan yksi edeltävän syksyn tilannekatsauksessa käsitellyistä teemoista. Teematilannekatsauksessa tuotetaan valitusta aiheesta syventävää tietoa, jota kerätään mm. kyseisen tilannekatsauksen valmistelua varten kokoon kutsuttavalta asiantuntijaverkostolta. Tällä järjestelyllä kyetään tuottamaan tarkempaa tietoa esimerkiksi sellaisista ilmiöistä, joissa suuri osa rikoksista on poliisin tietoon tulematonta piilorikollisuutta. Tämä tietoverkkorikollisuus -tilannekuva on laadittu yksityisen ja julkisen sektorin tietoturva-asiantuntijoiden yhteistyönä.

Tiivistelmä

Tietotekniikan ja tietoverkkojen käytön laajenemisen myötä on niiden käyttö myös rikollisen toiminnan välineenä voimakkaasti lisääntynyt, ja suuntaus jatkuu palvelujen siirtyessä yhä enenevässä määrin Internetiin ja mobiiliverkkoihin.

Käsillä olevassa tilannekatsauksessa painopiste on kohdistetuissa hyökkäyksissä. Kohdistettuja hyökkäyksiä tehdään jonkin tietyn valitun yrityksen hallitseman tiedon kaappaamiseksi. Koska yritysten keskeisenä tuotanto- ja kilpailukykytekijänä on nykyisin tieto, yksittäinenkin kohdistettu hyökkäys voi vaarantaa tai jopa tuhota yrityksen toimintaedellytykset.

Yrityksiin kohdistettuja hyökkäyksiä on viimeisten vuosien aikana alkanut näkyä entistä suuremmassa mitassa. Tapaukset ovat lisääntyneet, koska rikollisten verkottuminen on yhdistänyt kohdistettujen hyökkäystyökalujen valmistajat ja niistä kiinnostuneet käyttäjät. Suurin osa havaituista tietokaappausyrityksistä (suurinta osaa yrityksistä ei havaita ollenkaan) on tehty tietoa keräävän haittaohjelman avulla. Haittaohjelmat toimitetaan yrityksen sisäverkkoon pääasiassa sähköpostin, haavoittuvan WWW-selaimen tai USB -muistivälineen kautta.

Yrityksiin kohdistuvat monimuotoisen tietoverkkorikollisuuden uhkat eivät koske pelkästään yksityisen elinkeinoelämän toimijoita. Suuri valtaosa yhteiskunnan kokonaisturvallisuuden päivittäisistä voimavaroista on yksityisellä sektorilla. Yritysten keskeisenä tuotantotekijänä on nykyisin tieto. Tietoverkkojen turvallisuus on yrityksille arjen tietoturvaa, jolla ylläpidetään paitsi tietojen eheyttä, jäljitettävyyttä, oikea-aikaista saatavuutta ja käytettävyyttä, ennen kaikkea pitkälle automatisoitujen prosessinohjaus-, tietoliikenne- ja palvelujärjestelmiä, joista yrityksen toiminta on riippuvainen. Olennaista on kyetä ennakoimaan, havaitsemaan, torjumaan ja rajoittamaan yritysten häiriötöntä toimintaa uhkaavat tietoturvariskit niiden ilmenemismuodoista riippumatta. Ennen kaikkea yritysten on itse ymmärrettävä ja tunnistettava mikä on keskeinen suojattava tieto ja mikä merkitys sen väärinkäytöllä on yritykselle. Yritysten tietoturvatyön on palveltava yrityksen liiketoiminnan tavoitteita.

Organisaatio voi suojautua menestyksellisesti tietokaappauksilta vain, jos se tunnistaa sekä oman tietopääomansa eri osat että niihin kohdistuvien uhkien konkreettiset ilmenemismuodot. Yritysten tietoturvamallin korjaamiseksi on tehtävissä paljon. Tällä hetkellä tietorikokset tekee kannattaviksi puutteellinen tietojenkäsittely-ympäristön hallinta. Tekniset suojauskeinot eivät yksin riitä tiedon suojaamiseen. Tietoturvariskien toteutumisessa ihmisen toiminnalla on tärkeä rooli: työntekijä voi sekä estää tiedon joutumista vääriin käsiin että olla itse tietoturvallisuuden uhkatekijä.

Yrityksiin kohdistuvaan tietoverkkorikollisuuteen kuuluu myös Internetissä tapahtuva maksukorttirikollisuus. Maksukorttirikollisuus on monimuotoista, yleensä rajat ylittävää ja tuottoisuutensa vuoksi hyvin houkuttelevaa rikollisuutta, joka lisääntynee lähitulevaisuudessa tuntuvasti. Maksukorttirikosten toteuttamiseksi tarvitaan myös runsaasti erilaisia toimijoita. Maksukorttirikolliset kuuluvat siksi lähes poikkeuksetta järjestäytyneisiin rikollisryhmiin.

Rikollisia kiinnostavat ensi vaiheessa maksukorttien sisältämät tiedot. Korttidataa rikolliset hankkivat muun muassa Internetissä levitettävillä räätälöidyillä haittaohjelmilla kuten viruksilla ja vakoiluohjelmilla. Haittaohjelma kerää koneelta rikollisen haluaman tiedon. Maksukorttidatan perusteella rikolliset voivat valmistaa luottokortteja, joilla voidaan tehdä ostoksia tai käteisnostoja. Verkkokaupassa korttidataa voidaan hyödyntää sellaisenaan. Väärinkäytön estämiseksi on monia teknisiä rajoituksia, mutta monimuotoisessa infrastruktuurissa on aina myös teknisiä heikkouksia.

Tietoverkkorikollisuus

Tietoverkkorikollisuus ilmiönä

Ilmi tulleet rikokset ja piilorikollisuuden määrä. Vain pieni osa tietoverkkorikollisuudesta havaitaan ja vielä pienemmästä osasta tehdään rikosilmoitus poliisille. Esimerkiksi kohdistettujen hyökkäyksien osalta ei ole saatavilla luotettavaa tilastotietoa tekojen ja vahinkojen määrästä. Koska yrityksiin kohdistuvan tietoverkkorikollisuuden kokonaiskuvasta ei voida tehdä arvioita, piilorikollisuuden määrästä ei voida tehdä edes perusteltuja oletuksia.

Kokonaiskuvan hahmottamista hankaloittaa suuresti kaksi tekijää: toisaalta kyse on asianomistajarikoksista, joita monikaan yritys ei halua viedä julkiseen ja pitkäkestoiseen rikosprosessiin. Asianomistajarikoksissa poliisi voi aloittaa rikoksen tutkinnan vasta, mikäli asianomistaja ilmoittaa asiasta poliisille ja vaatii samalla tekijälle rangaistusta. Toisaalta rikostutkinnan yhteydessä on usein käynyt ilmi, että asianomistajana ollut yritys on saanut tiedon rikoksesta poliisilta tai Viestintäviraston Kyberturvallisuuskeskukselta.

Edes poliisin tietoon tulleesta tietoverkkorikollisuudesta ei ole saatavissa luotettavaa tilastotietoa, koska rikostilastointi tehdään rikosnimikkeittäin. Esimerkiksi tietomurto -rikosnimikkeen soveltamisala on hyvin kapea. Sitä voidaan soveltaa lähinnä vain silloin, kun tekijä on paljastunut ja epäonnistunut tavoitteessaan.

Kun tietomurron tekijä onnistuu teossaan, tällöin täyttyy jonkin muun rikosnimikkeen edellytykset ja tietomurto muuttuu toiseksi rikosnimikkeeksi esitutkinnassa. Toisin sanoen jos tekijä pääsee luvatta sisään toisen tietokoneelle, teko katsotaan useimmiten joksikin muuksi rikokseksi kuin tietomurroksi. Rikoksen määrittely riippuu siitä, mitä rikoksentekijä tietokoneessa tekee. Liikkuessaan luvatta toisen tietokoneessa tekijä käyttää toiselle kuuluvaa "tietokoneaikaa" ja syyllistyy näin koneen luvattomaan käyttöön. Tekoon sovelletaan samaa rikoslain pykälää kuin auton tai muun kulkuneuvon luvattomaan käyttöön (RL 28:7§). Tietoverkkorikoksista suurimman joukon muodostavat luvattomat käytöt, jolloin samassa poliisin tietojärjestelmästä poimitussa datassa esiintyvät myös esimerkiksi autojen, moottoripyörien, mopojen ja polkupyörien luvattomat käyttörikokset.

Edelleen jos tekijä asentaa erilaisia omia tarkoitusperiään palvelevia ohjelmia toisen koneelle, tällöin luvattoman käytön lisäksi on syytä epäillä, että tällöin täyttyy myös vahingontekorikoksen tunnusmerkistö. Kyseessä olisi sama vahingonteko, jota sovelletaan esimerkiksi ikkunan rikkomisen yhteydessä (RL 35:1§).

Yritysuhrit. Keskuskauppakamarin ja Helsingin seudun kauppakamarin "*Yritysten rikosturvallisuus 2012*" -selvitystutkimuksen mukaan erityisesti suuret yritykset valikoituvat tietoverkkoon murtautumisen kohteeksi. Selvityksen mukaan neljässä kymmenestä (43 %:ssa) suuresta yrityksestä oli havaittu luvattomia yrityksiä päästä tietoverkkoon. Keskisuurista yrityksistä joka neljäs (24 %) ja pienistä yrityksistä vain joka viides ilmoitti murtautumisyrityksistä yrityksen tietoverkkoon. Pääsääntöisesti näistä selvitystutkimukseen vastanneiden yritysten havainnoista ei ole tehty poliisille rikosilmoitusta.

Rikosvahinko. Tietoverkkorikollisuudesta koituvia kokonaistappioita on mahdotonta esittää rahamääräisesti, koska merkittävä osa alan rikollisuudesta on piilorikollisuutta ja kaapatun tiedon rahallista arvoa on usein mahdoton määrittää. Monissa tapauksissa yritykset ja erityisesti suuret yritykset eivät ole halukkaita viemään asiaa pitkäkestoiseen esitutkintaan ja oikeusistuinten julkiseen käsittelyyn todennäköisten tietoturvaan liittyvien imagotappioiden ja niitä seuraavia asiakasmenetysten vuoksi. Esimerkiksi yrityksiin kohdistuvat vakavammat eli törkeät tietomurrot tai niiden yritykset näkyvät erittäin harvoin poliisin järjestelmissä.

Yrityksiin kohdistuvaan tietoverkkorikollisuuteen kuuluu myös Internetissä tapahtuva maksukorttirikollisuus. Maksukorteiksi luetaan muun muassa luottokortit, maksuaikakortit, pankkikortit, käteisautomaattikortit ja debit-kortit. Maksukorttirikollisuus on monimuotoista, yleensä rajat ylittävää ja tuottoisuutensa vuoksi hyvin houkuttelevaa rikollisuutta, joka lisääntynee lähitulevaisuudessa tuntuvasti. Tuottoisuudestaan huolimatta merkittävä osa maksukorttirikollisuudesta jää piilorikollisuudeksi. Esimerkiksi Internetissä tai ulkomailla väärinkäytetty korttidata näkyy harvoin poliisin järjestelmissä, sillä pankkisektori ja kauppa torjuvat rikokset järjestelmillään tai kantavat tappiot.

Rikosten luonne

Tekijät. Tieto on tänä päivänä käytännössä kaikille yrityksille tärkein pääoma ja kilpailukykytekijä. Tämän vuoksi siitä ovat kiinnostuneet myös kilpailijat ja verkossa toimivat rikolliset. Tietotekniikan ja tietoverkkojen käytön laajenemisen myötä on niiden käyttö myös rikollisen toiminnan välineenä voimakkaasti lisääntynyt, ja suuntaus jatkuu palvelujen siirtyessä yhä enenevässä määrin Internetiin ja mobiiliverkkoihin.

Rikoksen tekeminen ei vaadi erityistaitoja, jos tiedon suojaus on puutteellinen. Tapaukset ovat lisääntyneet myös, koska rikollisten verkottuminen on yhdistänyt kohdistettujen hyökkäystyökalujen valmistajat ja niistä kiinnostuneet käyttäjät. Vielä vuosikymmen sitten henkilötietojen kaappaus satunnaisilta kotikoneilta edellytti huomattavaa hyökkäysohjelmistojen kehitystyötä. Samat hyökkäystyökalut voidaan nyt ostaa pienin räätälöidyin muutoksin myös yritysvakoilun kaltaisten tiettyyn uhriin kohdistettujen rikosten toteuttamista varten.

Tekotavat. Tietotekniikkaan ja tietoverkkoihin kohdistuvia rikoksia ovat esimerkiksi tietomurrot, haittaohjelmien avulla tehdyt tietokaappaukset tai erilaiset verkkohyökkäykset. Tietomurto ilmenee yrityksissä hyvin erilaisina rikoksina: aina resurssikuormituksesta, muutetun WWW-sivun tai toiminnallisen tietokannan kautta yrityksen keskeisen tietopääoman oikeudettomaan kaappaamiseen.

Yritysten resurssikuormituksessa rikolliset ottavat sivullisilta koneita haltuunsa. Haltuun saatua infrastruktuuria on käytetty lähinnä roskapostin lähetykseen sekä vakavampien tietomurtoyhteyksien peittelyyn.

Nykyisin hyödynnetään myös laskentakapasiteettia. Uutena ilmiönä on noussut esiin rikollisen infrastruktuurin käyttäminen bitcoin-digitaalisen valuutan saamiseen. Bitcoineja käytetään valuuttana erityisesti erilaisissa Internet-palveluissa, yhä enenevässä määrin muun muassa verkkokaupassa. Aiemmin bitcoineja saattoi hankkia jopa kotikoneella, mutta laskutoimitukset ovat jo niin monimutkaisia, ettei bitcoinien luominen enää kannata. Tietokoneen kuluttama sähkö maksaa enemmän kuin laskennassa saatavat bitcoinit. Niinpä rikolliset valjastavat sivullisilta, esimerkiksi yrityksiltä, kaapatun infrastruktuurin laskentaan – kunkin koneen omistajan kustannuksella.

Yritysten WWW-palvelinten murtoihin liittyy sekä kohtalaisen harmittomia että aidosti uhkaavia ilmiöitä. Yrityksen WWW-palvelimeen tunkeutuminen ja WWW-sisällön muuttaminen liittyy yleisimmin (h)aktivismiin, jossa tekijä tavoittelee mainetta edustamalleen aatteelle. Yritysten WWW-sivujen turmelijoissa on mukana myös yksittäisiä "nörttejä", jotka hakevat lähinnä arvostusta vertaisiltaan. Ilmiön laajuus johtuu pääasiassa vain siitä, että monet yritykset laiminlyövät WWW-sivujensa turvallisuuden ylläpidon. Yritys voi olennaisesti vaikuttaa siihen kuinka helpoksi kohteeksi asettautuu. WWW-sivun suojaaminen satunnaiselta murtautujilta on teknisesti varsin helppoa. Se kuitenkin edellyttää yritykseltä jatkuvaa tietoturvallisuuden ylläpitoprosessia.

Yrityksiin kohdistettuja hyökkäyksiä on viimeisten vuosien aikana alkanut näkyä entistä suuremmassa mitassa. Kohdistettuja hyökkäyksiä tehdään jonkin tietyn valitun yrityksen tai kokonaisen teollisuudenalan hallitseman tiedon kaappaamiseksi. Uutta ei ole ilmiön olemassaolo, vaan sen muuttuminen näkyväksi. Kohdistettuja hyökkäyksiä koskevien havaintojen lisääntymisen taustalla on sekä tunnistusmetodologian kehitys että tapausten määrä voimakas kasvu. Yrityksiin kohdistetuista hyökkäyksistä on tullut käytännössä sarjatuotantoa.

Kohdistettujen tietokaappausten tarkoituksena on päästä käsiksi jonkin tietyn kohdeorganisaation tiettyyn tietoon. Siten kyse on eri ilmiöstä kuin verkon tietokaappauksissa yleensä. Kohdistettuja hyökkäyksiä on tullut ilmi Suomessa erityisesti puolustustoimialan yrityksissä, mutta kohteeksi sopii mikä tahansa tuotekehitystä tekevä yritys, jolla on rikollisia kiinnostavaa aineistoa. Tätä nykyä suurin osa yritysvakoiluorganisaatioista kohdistaa hyökkäystoimintansa eri teollisuuden aloille. Tähän mennessä hyökkäykset ovat kohdistuneet erityisesti energia-, ilmailuelektroniikka- ja ohjelmistoteollisuuteen.

On ennustettavissa, että lähitulevaisuudessa kansainväliset rikollisorganisaatiot mutta yhtä lailla myös tietyt "kansallisen edun" pohjalta toimivat valtiolliset teollisuusvakoiluorganisaatiot kohdistavat vahvan mielenkiinnon cleantech- eli "puhdasta teknologiaa" tuottaviin yrityksiin ja niiden alihankkijoihin. Tätä nykyä Suomessakin on noin parituhatta yritystä, jotka suunnittelevat, kehittävät ja valmistavat aikaisempaa ympäristöystävällisempiä ja energiatehokkaampia tuotteita, palveluita, prosesseja ja teknologioita. Ympäristöliiketoiminnan maailmanmarkkinoiden on arvioitu kasvavan yli 10 prosenttia vuosittain, myös Suomessa ala kasvaa samassa mitassa.

Kohdistetun hyökkäyksen toteuttaminen edellyttää käytännössä jotakin erityistä haavoittuvuutta tiedon käsittelemisen prosesseissa. Haavoittuvuus voi olla tekninen tietoturva-aukko tai suunnittelun heikkous, mutta se voi liittyä myös yrityksen työntekijöiden tapaan käsitellä tietoa. Yrityksen tietopääoman suojaamisessa onkin keskeistä se, että päivitysprosessi toimii, tiedon kulku on hallittua ja työntekijät tuntevat turvalliset toimintatavat. Käytännössä yritykseltä vaaditaan sekä oman liiketoimintansa että tietovirtojen teknisen toteutuksen riittävää ja ajantasaista ymmärtämistä.

Huolella ylläpidettyyn tietojärjestelmään tunkeutuminen edellyttää aina hyvin vahvaa intressiä, mittavia resursseja ja suunnitelmallisuutta. Puhtaasti taloudellisella motiivilla toteutetun yritysvakoilun estämiseksi riittää, että hyökkäyksen toteutuskustannukset ylittävät suojattavan tiedon arvioidun arvon. Tällöin rationaalinen rikollinen valitsee kohteensa muualta. On kuitenkin muistettava, että on olemassa muunkinlaisia uhkia. Korkean teknologian tuotekehitysyritysten, kriittistä infrastruktuuria ylläpitävien ja turvallisuutta sivuavilla toimialoilla toimivien yritysten sekä palveluita tuottavien alihankkijoiden on syytä varautua torjumaan myös "kansallisen edun" pohjalta toimivien valtiollisten teollisuusvakoiluorganisaatioiden kiinnostus. Suojautumisessa valtiolliselta toimijalta automaattiset valvonta- ja tunkeutumisestojärjestelmät eivät yksin riitä. Suojautuminen vaatii lisäksi taitavaa, motivoitunutta ja analyysityöhön kykenevää ylläpitohenkilökuntaa, jolla on riittävät toimintaresurssit.

Suojautumisessa yritysten on kiinnitettävä erityistä huomiota palveluita tuottavien alihankkijoiden tietoturvallisuuden asianmukaiseen ylläpitoon. Yritysvakoilua harjoittavat tahot pyrkivät murtamaan uhriyrityksen tietoturvallisuusketjun heikoimman lenkin, joka usein on yrityksen alihankkija. Yritysten alihankkijat ovat aina hyökkääjien mielenkiinnon kohteina. Alihankkijoiden puutteellisesti ylläpidetty tietoturvallisuus voi mahdollistaa hyökkääjälle hyvin helpon ja huomaamattoman reitin päästä käsiksi uhriyrityksen tietovarantoihin.

Suurin osa havaituista tietokaappausyrityksistä (suurinta osaa tietokaappausyrityksistä ei havaita ollenkaan) on tehty tietoa keräävän haittaohjelman avulla. Kun rikollinen on onnistunut

toimittamaan haittaohjelma yrityksen sisälle palomuurien läpi, haittaohjelma voi tallettaa näppäinpainalluksia, ottaa kuvakaappauksia käyttäjän ruutunäkymistä, käyttää tietokoneen mikrofonia ja kameraa tiedon keruuseen sekä kerätä talteen käyttäjän toimistodokumentit kaikilta niiltä levyiltä, jonne käyttäjä pääsee käyttöoikeuksillaan. Mitä laajemmin haavoittuvalta työasemalta pääsee käyttäjän oikeuksin yritysorganisaation keskeiseen tietoon käsiksi, sitä laajemmin hyökkäyksen tekijäkin saa tietoa haltuunsa.

Kohdistetun hyökkäyksen tekijän tavoitteena on
1. toimittaa haittaohjelma kohdeyritykseen kenenkään havaitsematta
2. saada joku ennalta valittu yrityksen työntekijä aktivoimaan haittaohjelma, jotta se pystyy keräämään haluamansa tiedon
3. saada kerätty tieto ulos kohdeyrityksestä kenenkään havaitsematta.

1. Haittaohjelmat toimitetaan yrityksen sisäverkkoon pääasiassa sähköpostin, haavoittuvan WWW-selaimen tai USB-muistivälineen kautta. Sähköpostissa sinänsä ei ole mitään sellaista suunnitteluvirhettä, joka tekisi siitä erityisen houkuttelevan välineen tiedonkaappauksiin. Rikolliset käyttävät sähköpostia, koska vain hyvin harva yritys on aidosti erotellut sähköpostin käsittely-ympäristön muun tietopääoman käsittelystä. Sähköposti tarjoaa rikolliselle suoran käytävän yrityksen sisäverkkoon ja tietopääomaa sisältäviin levyasemiin.

Sähköpostilla toteutetussa hyökkäyksessä lähettäjäkenttä on väärennetty. Viestin liitteenä oleva tiedosto on joko melko uutta tai toistaiseksi korjaamatonta ohjelmistohaavoittuvuutta hyväkseen käyttävä haittaohjelma. Haittaohjelman toimittaminen kohdeyrityksen palomuurien läpi kenenkään havaitsematta ei ole erityisen haasteellista, sillä palomuuri ei saa häiritä yrityksen liiketoimintaa seulomalla liian voimakkaasti sähköposti- ja WWW-liikennettä.

2. Kohdistetussa hyökkäyksessä vastaanottajien kiinnostus ja luottamus pyritään voittamaan monin eri tavoin. Huolellisen tiedustelutyön perusteella sähköpostipostiviestejä ei lähetetä massoittain, vaan ainoastaan muutamille avainhenkilöille, jotta mikään automaattinen tietoturvatyökalu ei havaitsisi poikkeamaa. Taitavasti toteutetussa hyökkäyksessä hyökkääjä on tiedustellut kohdeorganisaation henkilökunnan nimiä ja työtehtäviä. Lista viestin vastaanottajista on usein kaikkien nähtävillä ja näin vastaanottajiksi merkityt tuntevat entuudestaan toinen toisensa. Viestin sisällöstä pyritään tekemään mahdollisimman uskottava ja kiinnostusta herättävä. Viesti voi sisältää esimerkiksi kohdeyrityksen toimialaan liittyvän kokouskutsun, julkaisun tai merkittävän asiakkaan tiedonannon. Kohdistettujen hyökkäysten tavoite ei ole kohdejärjestelmän liittäminen rikollisen hallitseman jopa satojen tietokoneiden muodostaman bottiverkon "orjakoneeksi", vaan niiden kautta saavutettava tietosisältö.

Tietoturvallisuuden asiantuntijat korostavat, että sähköpostin vastaanottaja, joka avaa haitallisen liitetiedoston, ei syyllisty laiminlyöntiin saati toimi harkitsemattomasti, sillä haittaohjelman sisältävät viestit laaditaan hyvin huolellisesti. Varsinainen vika on nykyisessä tietoturvamallissa, joka ei juurikaan suojaan kohdistetuilta tietokaappauksilta. Nykyinen tietoturvamalli mahdollistaa lähinnä tökerösti ja huomiota herättävästi toteutettujen mutta jokseenkin harmittomien hyökkäysten havaitsemisen ja torjumisen.

Viime aikoina tehdyissä kohdistetuissa hyökkäyksissä rikolliset ovat onnistuneesti viemään haittaohjelman yrityksen sisäverkkoon haavoittuvan WWW-selaimen avulla. Rikolliset murtavat kohdeyrityksen verkon ulkopuolelta huonosti suojatun WWW-palvelun, jota kohdeyrityksen työntekijät oletettavasti hyödyntävät säännöllisesti, esimerkiksi uhriyrityksen lähiravintolan lounaslistapalvelimen. Palvelimelle rikolliset asettavat lounaslistan kylkeen haittakoodia, joka aktivoituu jos lounaslistan lukijalla on haavoittuva WWW-selain. Yrityksillä ei ole käytännössä mahdollisuuksia selvittää työntekijöiden suosimien ja oletettavasti asiallisten sivustojen turvalli-

suustilannetta. Tämänkaltaiset kohdistetut hyökkäykset ovat onnistuneet, koska lukuisat yritykset laiminlyövät omien WWW-selainten säännöllisen päivittämisen.

3. Kerätyn tiedon toimittaminen ulos yrityksen sisäverkosta on rikolliselle haastavin joskin täysin toteutettavissa oleva vaihe. Vallalla olevan tietoturvamallin pohjalta moni suurikin yritys on niin keskittynyt torjumaan vain ulkoa tulevia uhkia, ettei kiinnitä riittävästi huomiota yrityksestä ulos kulkevaan tietopääomaan.

Yrityksiin kohdistuvassa ja Internetissä tapahtuvassa maksukorttirikollisuudessa tarvitaan myös runsaasti erilaisia toimijoita. Maksukorttirikolliset kuuluvat siksi lähes poikkeuksetta järjestäytyneisiin rikollisryhmiin.

Järjestäytyneen maksukorttirikollisuuden ymmärtämisessä, analysoimisessa ja torjunnassa on tärkeää ottaa huomioon ilmiön valtionrajat ylittävä luonne. Luottokortit on kehitetty yleensä kansainvälisiksi maksuvälineiksi ja niillä maksetaan paljon esimerkiksi ulkomaanmatkoilla. Tällöin korttiostoksiin liittyvä korttidata kulkee monen valtionrajan yli. Maksukorttirikolliset käyttävät hyväkseen kansallisen viranomaistoiminnan hitautta ja lainsäädäntöjen suuria eroja: maksukorttidata kiertää maapallon muutamassa sekunnissa, mutta ilmitulleen maksukorttirikoksen kansallisessa tutkinnassa tarvittavat tiedot ovat usein pankkisalaisuuden piirissä, ja niiden saaminen toisesta maasta edellyttää usein vähintäänkin oikeusapupyyntöä.

Rikollisia kiinnostavat ensi vaiheessa maksukorttien sisältämät tiedot. Korttidataa rikolliset hankkivat muun muassa Internetissä levitettävillä räätälöidyillä haittaohjelmilla kuten viruksilla ja vakoiluohjelmilla. Maailmassa on lukuisia maita, joissa tietoa kaappaavien haittaohjelmien kirjoittaminen on laillista tai muista syistä yleistä. Haittaohjelma kerää koneelta rikollisen haluaman tiedon; esimerkiksi luottokortin numeron käyttäjän tehdessä ostoksia verkkokaupassa.

Maksukorttidatan perusteella rikolliset voivat valmistaa luottokortteja, joilla voidaan tehdä ostoksia tai käteisnostoja. Verkkokaupassa korttidataa voidaan hyödyntää sellaisenaan. Väärinkäytön estämiseksi on monia teknisiä rajoituksia, mutta monimuotoisessa infrastruktuurissa on aina myös teknisiä heikkouksia.

Kiinnijäämisriskin pienentämiseksi maksukorttirikollisten organisaatioissa on yleensä selkeä ennalta määrätty työnjako; rikoksella haltuun saadun korttidatan sähköinen lähettäminen ja siirtäminen väärennettyihin eli kloonikortteihin sekä edelleen kloonikorttien tekeminen, niiden käyttäminen käteisen rahan nostamisessa ja rahojen kuljettaminen maasta toiseen on jaettu eri rikollisten tahojen tehtäväksi. Laillisen yritystoiminnan piiristä opitut riskien hajauttamisen periaatteet toimivat myös organisoidussa rikollismaailmassa. Tarvittavat asiantuntijapalvelut ostetaan vapailta markkinoilta. Internetin, Usenetin ja IRC-palvelujen mahdollistama korttirikollisten maailmanlaajuinen verkostoituminen tekee korttirikollisuudesta kansallisvaltioiden rajat ylittävää ja tehokasta laitonta taloudellista toimintaa.

Suurta rikoshyötyä hankitaan tällä hetkellä tietoverkossa toteutetuilla identiteettivarkauksilla, joissa joko verkkomaksuja välittäviltä palvelimilta tai asianomistajan työasemalta kaapataan verkkoasioinnin yhteydessä rahaksi muutettavissa olevaa identiteettitietoa. Internetissä levitettävien haittaohjelmien avulla maksukorttirikolliset voivat anastaa haavoittuvista kohteista suuria määriä luottokorttitietoja ja verkkopankkitunnuksia vähäisellä kiinnijäämisriskillä.

Tietoverkkorikosten vaikutukset yrityksiin

Tietoverkkorikosten vaikutukset yrityksiin. Tietoverkossa toimivan rikollisuuden vaikutus voi uhriksi joutuneessa yrityksessä ilmetä teosta riippuen kohtalaisen harmittomana resurssikuor-

mituksena tai mainevahinkona, mutta myös yrityksen koko toiminnan vaarantavana tapahtumana.

Yritysten keskeisenä tuotanto- ja kilpailukykytekijänä on nykyisin tieto. Yritysten päätöksenteon pohjana olevan tiedon on oltava oikeaa sekä oikea-aikaisesti saatavilla. Toisaalta tiedon on oltava vain sen käsittelyyn oikeutettujen tahojen tiedossa. Myös tietoverkkorikosten vaikuttavuudessa on eroja. Ensimmäistä tuotekehitystään tekevän startup-yrityksen tietokonekaluston varastaminen aiheuttaa yrityksen omistajille taloudellista vahinkoa, mutta siltä voi osittain suojautua vakuutuksin. Sen sijaan tuotekehitysdatan anastaminen saattaa tuhota yrityksen, eikä tämänkaltaista riskiä voi ulkoistaa vakuutusyhtiölle.

Kansainvälinen maksukorttirikollisuus tulee kasvamaan verkkomaksamisen voimakkaan lisääntymisen seurauksena. EU-maiden poliisiorganisaatioiden yhteenliittymän Europolin vakavan ja järjestäytyneen rikollisuuden uhka-arvio SOCTA 2013:n (*The EU Serious and Organised Threat Assessment*) mukaan jo noin 60 prosenttia maksuvälinepetosten aiheuttamista tappioista koituu Card-Not-Present (CNP) -tapauksista, joissa itse korttia ei väärinkäytetä, vaan korttidata on useimmiten anastettu palveluntarjoajien sähköisistä järjestelmistä.

Europolin SOCTA 2013 toteaa, että maksuvälinedataan kohdistuneita anastuksia koskevan vahvan ilmoitusvelvollisuuden puuttuminen lainsäädännöstä estää maksukorttirikollisuuden tehokasta tutkintaa ja torjuntaa. Yritykset jättävät hallussaan olevaan tietoon kohdistuvat rikokset usein ilmoittamatta poliisille oman maineensa suojelemiseksi. Kuitenkin kasvava määrä EU-maissa toimivia liikkeitä ja maksupalvelukeskuksia on joutunut maksutietojen anastuksen kohteeksi viime vuosina. Europolin SOCTA 2013 korostaa, että maksukorttidataa hyödyntävää rikollisuutta koskeva tiedustelutieto on huomattavan puutteellista. Lisäksi pelkkää korttidataa hyödyntävä maksukorttirikollisuus ja tietoverkkorikokset ovat usein vaikeasti eroteltavissa toisistaan käytännössä, mikä vaikuttanee CNP -rikollisuuden näkyvyyteen tilastoissa.

Rikoksilta suojautuminen. Jotta tietorikollisuudesta aiheutuva vahinko voidaan minimoida, yrityksillä on oltava edellytykset havaita rikos mahdollisimman nopeasti. Vallitseva tietoturvakulttuuri valitettavasti keskittyy torjumaan helposti estettäviä ja havaittavia hyökkäyksiä, jolloin yrityksellä voi olla virheellinen käsitys todellisesta turvallisuustilanteestaan.

Kohdistetut hyökkäykset pyritään lähtökohtaisesti toteuttamaan siten, etteivät pelkät tietoverkon ulkorajojen automaattiset tunkeutumisenestojärjestelmät niitä havaitsisi. Tunkeutuja nimenomaisesti pyrkii naamioimaan sekä murtoyhteyden että tiedon uloskuljetuksen legitiimin liikenteen näköiseksi. Automatiikan merkitystä ei silti pidä aliarvioida. Se on välttämätön apu poikkeamatilanteiden havaitsemisessa.

Suuren osan tietorikoksista yritys voi torjua kohtalaisen tehokkaasti huolehtimalla kahdesta seikasta:

1. ilmeisten haavoittuvuuksien poistamisesta

2. omaan toimintaan liittyvien tietovirtojen ymmärtämisestä ja rajaamisesta.

Haavoittuvuuksien poistaminen edellyttää yritykseltä jatkuvaa reaaliaikaista ylläpitoprosessia. Jos yrityksen käyttämää ohjelmistoa ei voida sopimusoikeudellisista syistä päivittää, laite on eristettävä verkosta siten, ettei sen hyväksikäyttäminen ole kustannustehokasta. Verkkoeristämisen lisäksi päivittämättömän järjestelmän tiedostoista on ylläpidettävä eheydenvalvontapöytäkirjaa, jonne merkityt tiedostoja koskevat tiedot on myös säännöllisesti tarkistettava.

Yrityksen on tunnistettava tietovirtoihinsa vaikuttavat ja niitä ohjaavat prosessit ja arvioitava niitä koskeviin toimintamalleihin liittyvät riskit. Yrityksen on myös jatkuvasti varmistettava, että sen jokainen työntekijä täyttää työtehtäväkohtaiset osaamisvaatimukset.

Yritykselle yksi vaativimmista tehtävistä on tunnistaa mikä on normaalia liikennettä ja missä omaa dataa todella käsitellään. Mitä enemmän yrityksen verkkoa on osioitu, sitä parempi kyky yrityksellä on havaita automatiikan avulla liikenteen poikkeamia, joiden taustalla voi olla tiedon anastaminen. Jos tietoverkko erotellaan esimerkiksi siten, että tuotekehityspalvelimen kautta ei kulje minkäänlaista henkilöiden välistä viestintää, silloin yritys voi kaikkien yhteyksien osapuolena seuloa liikennettä varsin tarkasti.

Erityisen tärkeätä on jatkuvasti seurata tietoverkon eri laitteiden mahdollisia "roolista" poikkeamisia. Jos esimerkiksi työasema yhtäkkiä ottaa yhteyttä toiseen työasemaan tai jos palvelin ottaa odottamattomasti yhteyttä työasemaan, tällöin todennäköisesti on kyse ulkopuolisen yritykseen kohdistamasta hyökkäyksestä.

Yrityksen data ei yleensä ole vain huolella suojatuissa tietokantapalvelimissa, vaan sitä käsitellään myös työntekijöiden mobiililaitteilla esimerkiksi lentokenttien avointen WLAN-verkkojen kautta.

Tiedon suojaaminen väistämättä sekä vaatii taloudellisia resursseja että haittaa tiedon käytettävyyttä. Kohdistettujen hyökkäysten torjunnasta aiheutuvan toiminnallisen haitan ja kustannusten tulee olla järkevässä tasapainossa suojattavan intressin kanssa. Siksi yrityksen on tunnistettava mikä on keskeinen suojattava tieto ja mikä merkitys sen väärinkäytöllä on yrityksen toimintaan. Edelleen kohdistettujen hyökkäysten torjunta edellyttää yritykseltä vakiintuneen tietoturvayhteistyön luomista prosessien omistajien, IT-vastuullisten ja mahdollisten yritykselle palveluita tuottavien alihankkijoiden kesken.

Rikosuhalta suojautumisen tärkeäksi keinoksi lukeutuu yrityksen liiketoimintamallin muuttaminen. Tätä nykyä harvalla yrityksellä on taloudellisia resursseja hoitaa koko datan käsittelyyn liittyvä prosessi yksin. Erityisesti julkisesti noteerattujen yritysten taloudellisia tunnuslukuja mekaanisesti tarkastavat sijoittajat vaativat, ettei yrityksen pääomia sidota ydintoiminnon ulkopuolisiin toimintoihin. Ellei yritys kykene perustelemaan liiketoimintariskin kautta oman IT-osaston perustamisen välttämättömyyttä, datan käsittely on käytännössä ulkoistettava kaupalliselle palveluntarjoajalle. Tällöin yritys joutuu joko luottamaan palveluntarjoajan kykyyn turvata hallinnoimansa data tai sitten yrityksen on erikseen suojattava datansa myös palveluntarjoajalta, mistä aiheutuu ylimääräisiä kustannuksia.

Pienillä yrityksillä ei useinkaan ole taloudellisia resursseja tietoturva- tai ylläpitohenkilökuntaan, jolloin ainoa mahdollisuus on luottaa kaupallisten palveluntarjoajien tuottamien verkkopalveluiden turvallisuuteen. Esimerkiksi pienen kivijalkayrityksen siirtyminen verkkokaupaksi voi sisältää vakavia riskejä, joita ei aina riittävästi tunnisteta.

Poliisin rikostutkinnan yhteydessä on noussut esiin kolme keskeistä ulkoistamiseen liittyvää ongelmaa: Puutteellisesti toteutetut

1. vastuunjaon määrittelyt,
2. tiedonsaantioikeussopimukset,
3. todellisen turvallisuustilanteen tunnistamisen prosessit.

1. Jos ylläpitovastuuta ei ole määritelty, ylläpidosta ei käytännössä vastaa kukaan. Kohdistetun hyökkäyksen torjunnassa on aivan keskeistä, että edes tunnetut ohjelmistohaavoittuvuudet poistetaan.

2. Kaupallinen palveluntarjoaja sijoittaa kustannussyistä eri yritykset mielellään samaan virtuaalipalvelimeen, jos ei muusta sovita. Tästä kuitenkin seuraa, ettei palveluntarjoaja välttämättä voi luovuttaa rikoksen uhriksi joutuneelle yritykselle tilanteen selvittämiseksi tarvittavia lokitietoja, sillä tällöin asianomistajalle paljastuisi myös sivullisten tietoja. Ongelman vaikutus on jossain määrin pienentynyt uuden pakkokeinolain myötä, sillä poliisi voi nyt hankkia televalvontaluvan yritysvakoilun tutkimiseksi. Oikeudesta saada tarvittavat tiedot on silti hyvä sopia etukäteen.

3. Ulkoistetun palvelun turvallisuutta arvioitaessa luotetaan liian usein palveluntarjoajan ilmoitukseen. Jos datan turvaamisella on yritykselle merkitystä, todellinen tietotekninen turvallisuustilanne on tarkastettava. Markkinoilla on useita yrityksiä, jotka tarjoavat tietoturvatarkastusten asiantuntijapalveluita. Tällä hetkellä ongelmana on lähinnä asianmukaisen standardin puute. Suurin osa tietoturvastandardeista on aivan liian raskaita ja ne eivät ole riittävän teknisiä todellisen tilannekuvan selvittämiseen.

Yksityisellä sektorilla on havaittu ongelmaksi myös tiedon eheyden varmistamisen haasteet. Tietorikosriskiä ei muodosta ainoastaan tiedon päätyminen vääriin käsiin, vaan ihan yhtälailla tiedon oikeellisuus. Yritykselle voi aiheutua merkittävää vahinkoa esimerkiksi tuotetietojen oikeudeton muuttaminen ulkoistetun tuotetietotarjoajan palvelussa tai logistiikan pysäyttäminen tarkasti toiminnanohjausjärjestelmään kohdistetulla palvelunestohyökkäyksellä.

Tietoturvamallin korjaamiseksi yritykset voivat itse tehdä paljon. Tällä hetkellä tietomurrot ja ylipäätään tietorikokset tekee kannattaviksi puutteellinen tietojenkäsittely-ympäristön hallinta. Toimisto-ohjelmista, sähköpostien liitteinä lähettävistä PDF- ja Office-tiedostoista, WWW-selaimista ja niiden apuohjelmista käytetään monissa yrityksissä, erityisesti pk-yrityksissä tunnetusti haavoittuvia versioita, joiden kautta on helppoa päästä kohdeorganisaation toimistoverkkoon. Jos yritys suojautuu ulkomaailman uhilta vain verkon reunalla eli keskittymällä vain ulkopuolelta tulevan uhan torjumiseen, rikollisen yrityksen sisäverkkoon onnistuneesti toimittama tietokeräin pystyy varsin vapaasti kokoamaan ja toimittamaan ulos kenenkään huomaamatta kaiken haluamansa tiedon.

Tiedostojen monipuolisuuden voimakas kasvu on johtanut siihen, että niiden käsittelemiseksi käytettävistä ohjelmistoista on kasvanut suuria. Tämän seurauksena niiden kehityksestä on tullut vaikeasti hallittavaa. Ohjelmistoista löydetäänkin jatkuvasti vakavia virheitä ja haavoittuvuuksia, joita tietomurtoihin tähtäävät rikolliset käyttävät hyväkseen. Erityisesti aikaisemmin turvallisina pidettyjä PDF-dokumentteja käytetään nykyään suurimittaisesti haittaohjelmahyökkäysten välineenä, koska PDF-tiedostojen käsittelyyn käytettävät ohjelmistot ovat suurentuneet ja kehittyneet haavoittuviksi.

Tietoturvaohjeistuksista huolimatta verkkotulostimiin ja monitoimilaitteisiin liittyviä haavoittuvuuksia ei osata vielä ottaa riittävästi huomioon yritysten tietoturvallisuudessa. Aikaisemmin yksikertaisina ja tietoturvallisuuden kannalta vaarattomina pidetyistä kirjoittimista on kehitetty täysimittaisia palvelinlaiteita, jotka kytketään yrityksen sisäverkkoon. Toisin kuin muita palvelinlaitteita, verkkotulostimia ja monitoimilaitteita harvoin hallitaan keskitetysti tai päivitetään. Verkkojen turvallisuuden varmistamisessa sisäverkkoon kytketyt kirjoitinpalvelut muodostavat tätä nykyä turvallisuusketjun heikon lenkin.

Yritys voi suojautua menestyksellisesti tietokaappauksilta vain, jos se tunnistaa sekä oman tietopääomansa eri osat että niihin kohdistuvien uhkien konkreettiset ilmenemismuodot. Kriittisen tietopääoman tunnistamiseen on syytä kiinnittää erityistä huomiota yrityksissä. Keskuskauppakamarin ja Helsingin seudun kauppakamarin Yritysten rikosturvallisuus 2012 -selvityksessä vain 43 prosenttia yrityksistä arvioi hallussaan olevan laittoman tiedustelun tai yritysvakoilun kohteeksi otollista tietotaitoa tai omaisuutta, vaikka käytännössä jokaisessa yri-

tyksessä on ulkopuolisia mahdollisesti kiinnostavaa tietoa, jonka joutuminen vääriin käsiin tuottaa yritykselle vahinkoa. Yleisten hyökkäysvektoreiden tunnistamiseksi on saatavilla paljon tietoturvateollisuuden, muun tietoturvayhteisön ja viranomaisten tuottamaa tietoa. Ohjelmistohaavoittuvuuksia tunnistaa ja korjaustietoa julkaisee Viestintäviraston tietoturvayksikkö CERT-FI[1], jonka haavoittuvuusinformaatio voi suuresti auttaa yrityksiä oman ympäristön suojaamisessa.[2]

Tekniset suojauskeinot eivät yksin riitä tiedon suojaamiseen. Tietoturvariskien toteutumisessa ihmisen toiminnalla on tärkeä rooli: työntekijä voi sekä estää tiedon joutumista vääriin käsiin että olla itse tietoturvallisuuden uhkatekijä. Työtekijöiden tietoturvallisuusosaamista on syytä parantaa kouluttamalla heidät tiedon asianmukaiseen käsittelyyn. Ohjeistus on syytä ulottaa kattamaan liike- ja ammattisalaisuuksien käsittelyn lisäksi myös tiedon luokittelun, käsittelyn liiketoiminnan eri tilanteissa sekä tiedon elinkaaren eri vaiheissa. Sähköisessä muodossa olevan tiedon fyysiseen suojaamiseen, tiedon syöttämisen suojaamiseen (PIN-koodit, salasanat), laitteiden ja tiedon käsittelyoikeuksiin sekä tietojenkäsittely-ympäristön haavoittuvuuksien toteamiseen ja nopeaan korjaamiseen on syytä kiinnittää erityisesti huomiota.

Jos yrityksen tietojenkäsittely-ympäristö on ulkoistettu, oman ympäristön ajantasaisuutta voidaan hallita siviilioikeudellisin sopimuksin. Yritykselle kuitenkin aina jää lopullinen valvontavastuu. Valvonnan on oltava osa normaalia yrityksen johtamismallia riippumatta siitä onko yritykselle elintärkeän datan käsittely ulkoistettu alihankkijalle tai omalle IT-henkilöstölle.

[1] Viestintävirasto. Tietoturvakatsaukset, CERT-FI. Eniten yhteydenottoja on vuosina 2010–2012 tehty haittaohjelmiin ja neuvontaan liittyen.
[2] Ks. myös valtiovarainministeriön julkishallinnon tietoturvallisuuden ohjaukseen tarkoitettu VAHTI-sivusto.