Lehti tietoturvan ilmiöistä, tapahtumista ja ihmisistä

ylivuoto

2/2005

Tietoturvasää tänään ja huomenna

Ammattina hakkeri

Tietoturvatyön eettiset säännöt

Kääntyikö tietoturva luojaansa vastaan?

tietoturva-RATKAISUT?

http://www.ylivuoto.fi

Sisällys 2/2005

Mediatiedot

Päätoimittaja
• Tiina Kaksonen

Ulkoasu
• Pasi Kemi

Julkaisija
• mediakarhut.com

Menossa mukana
• Oulu University Secure Programming Group (OUSPG)
• Mobile Forum

Toimitus tässä numerossa
• Tiina Kaksonen, Pasi Kemi, Erno Kuusela, Timo Lehtimäki, Jorma Kajava, Reijo Savola, Jani Kenttälä

WWW-sivu
• http://www.ylivuoto.fi

Yhteystiedot
• toimitus@ylivuoto.fi

Painopaikka
• Raahen Kirjapaino Oy

Painos
• 3000

ISSN 1796-0835

mediakarhut.com

http://www.mediakarhut.com

OU SPG

http://www.ee.oulu.fi/research/ouspg

mobileFORUM

http://www.mobileforum.org

Pääkirjoitus

Tiina Kaksonen
tiina.kaksonen@iki.fi
päätoimittaja

Ohjelmistoalan hurjan kasvun 1990-luvun lopulla on viime aikoina nähty tasoittuneen. Myös tietoturva-alalla suhdanteet ovat kääntyneet. Erityisesti pienet, suppeahkon tuotevalikoiman omanneet ohjelmistoyritykset ovat olleet vaikeuksissa. Suuremmat yritykset ovat selvinneet taantumasta paremmin. Tietoturva-alan osalta on myös esitetty markkinoiden kypsyneen, mikä on johtanut ankaraan kilpailuasetelmaan. Erityisesti tämä koskee erilaisia tietoturvatuotteita tarjoavia yrityksiä. Kireässä kilpailutilanteessa markkinoinnilta vaaditaan entistä enemmän tehokkuutta. Maallikon näkökulmasta tietoturvatuotteiden uhkia korostava, ajoittain jopa aggressiivinen markkinointi voi kuitenkin herättää pelkoa ja epävarmuutta.

Tietoturvatuotteiden tarjoaminen onkin varsin haastava liiketoiminta-alue, jolla tarvitaan poikkeuksellisen laaja-alaista ja syvällistä tietotekniikan ymmärrystä. Sama koskee muutakin tietoturvakenttää. Tässä numerossa esitellään muutamia varsin erilaisia tietoturva-alan yrityksiä, jotka tarjoavat pitkälle vietyä tietoturvaosaamista. Tavallisen pk-yrityksenkin näkökulmasta on kuitenkin tärkeä huomata, että vaikka tietoturvatuotteilla ja -palveluilla on tärkeä asema yrityksen tietoturvan hallinnassa, se ei vielä riitä. Tarvitaan myös esimerkiksi hallinnollisia ratkaisuja, ja ihmisten toimintatapojen syvällistä ymmärtämistä.

Tietoturvatietoisuus on viime vuosina parantunut selvästi aiempaan tilanteeseen verrattuna. Silti edelleen voi tavata yrityksen atk-vastaavan tarkistamassa salasanojaan näppäimistön alta. Asenteissa riittää siis edelleen paljon korjattavaa. Tietoturvaa on usein verrattu liikenneturvallisuuteen, ja näissä asioissa onkin paljon yhtymäkohtia. Tietokoneesi on kuin autosi, jonka kunnosta täytyy säännöllisesti huolehtia kun sillä liikennöidään tiedon valtateillä. Yhteiset liikennesäännöt ja periaatteet on tunnettava, jottei aiheuta vaurioita itselle tai muille. Liikenneturvallisuuteen liittyvän asennetietoisuuden puolesta on kampanjoitu useita vuosikymmeniä, ja paljon edistystä onkin saatu aikaan. Tietoturva näyttää alueelta, jolla kansalaistaitojen ja –asenteiden muokkaamista jatkossa riittää ainakin yhtä paljon. Oma näkökulmansa tähän asiaan on tietoturvaan liittyvien eettisten periaatteiden pohdinta, josta Jorma Kajava ja Reijo Savola tässä numerossa kirjoittavat.

Toki tietoturvan erityisasiantuntemustakin yhteiskunnassa tarvitaan, ja sille on paljon kysyntää. Uutta koulutusta alueelta onkin lisätty viime vuosina. Esimerkiksi Oulun ammattikorkeakoulun Raahen tekniikan ja talouden yksikkö tarjoaa nykyään tietoturva-alan suuntautumisvaihtoehtoa tietoteknikan insinöörikoulutuksessaan. Myös yliopistotasoista koulutusta alkaa jo olla tarjolla. On tarpeen, että esimerkiksi jokaisessa pk-yrityksessä on tietoturvan perustiedot ja -taidot omassa hallinnassa. Vuoden loppua kohden monissa yrityksissä tehdään suunnitelmia tulevan vuoden varalle. Nyt onkin oivallinen ajankohta pohtia, olisiko tietoturvaosaamisen päivittäminen organisaatiossa ensi vuonna ajankohtaista.

Ratkaiseeko tietoturvaratkaisu todella tietoturvaongelmasi?

Tiina Kaksonen

Tietoturvayhtiöiden keskeinen tavoite on myydä tuotteitaan ja palveluitaan, siis tietoturvaratkaisujaan, yrityksille. Mainonnan perusteella syntyy helposti kuva, että tietoturvariskit ovat vältettävissä ostamalla tällainen tuote tai palvelu ja integroimalla se yrityksen järjestelmään. Sitten koko ongelma onkin hoidettu ja poissa päiväjärjestyksestä. Aivan näin yksinkertaisesta asiasta ei kuitenkaan ole kyse.

Tietoturvallisuudella tarkoitetaan erityisesti tietojen, tietojärjestelmien ja tietoliikenteen asianmukaista suojaamista kaikkien olojen varalta sekä hallinnollisilla, että teknisillä toimilla. Tietoturvaratkaisuina myytävät kokonaisuudet vastaavat moniin teknisiin ongelmiin, mutta lisäksi yrityksen on huomioitava tietoturvan hallinnollinen puoli. Hyvän ja tehokkaan tietojenkäsittelytavan ja -kulttuurin luominen organisaatioon on tietoturvan kannalta olennaisen tärkeää.

Tutkimukset ja selvitykset kertovat karua kieltä tietoturvaongelmien todellisesta luonteesta. Usein peruskäsitys tietoturvasta on, että järjestelmiä turvaamalla suojaudutaan jotain organisaatiota ulkopuolelta uhkaavaa vaaraa vastaan. Kuitenkin tutkimukset osoittavat, että vähintään kolme neljästä tietoturvaongelmasta on alun perin lähtöisin organisaation sisältä. Ihmisten toiminta on tietoturvan kannalta keskeisessä asemassa.

Toinen yleinen tietoturvaan liittyvä käsitys on, että tietoturvan hallinnollinen puolikin on hoidossa kun yrityksen tietoturvapolitiikka on kirjoitettu. On kuitenkin voitu todeta, että jopa 96 % tietoturvaongelmatilanteista olisi voitu välttää, jos organisaatioiden oma henkilökunta olisi noudattanut organisaation tietoturvapolitiikkaa. Todellisten ongelmakohtien ja riskien arviointi onkin tietoturvaratkaisuja pohdittaessa keskeisessä asemassa.

Riskianalyysia ja hankintapäätöksiä

Tietoturva ei ole absoluuttisesti mitattavissa oleva kokonaisuus. Tietoturvaongelmiin keskeisesti liittyy kysymys siitä, mitkä ovat todelliset riskit ja miten niihin voidaan varautua. Keskeistä on myös pohtia, mitkä riskeistä ovat sellaisia, että niihin todella voidaan ja kannattaa varautua. Tietoturvaratkaisuja hankittaessa yrityksessä tuleekin tarkasti miettiä, mitä riskiä pyritään välttämään, miten se parhaiten tapahtuu ja mitä riskejä ylipäänsä on järkevä välttää.

Tekniset tietoturvaratkaisut ovat tärkeä osa kokonaisuutta, mutta eivät yksistään kykene suojaamaan organisaatiota kaikkia uhkia vastaan. Tärkeimmät

tekniset tietoturvaratkaisut, jotka pienikin yritys tarvitsee, ovat virustorjunta ja palomuurit. Tietoturvan tulisi kuitenkin olla mukana jo organisaation tietojärjestelmän rakentamisvaiheessa. Turvallisuusasiaa on syytä pohtia esimerkiksi hankittaessa organisaatioon uusia ohjelmistoja: onko tämä ohjelmistontoimittaja sellainen, jonka tuotteet ovat varmatoimisia. Toimittajaa valittaessa on syytä myös pohtia, onko kyseinen toimittaja aikaisemmin onnistunut tehokkaasti korjaamaan tuotteestaan löytyneet virheet ja näin vastaamaan esimerkiksi ohjelmistohaavoittuvuuksien aiheuttamiin tietoturvariskeihin.

Turvallisuusasia on syytä pitää mielessä myös esimerkiksi hankittaessa langattomia laitteita ja suunniteltaessa verkkorakennetta.

Tietoturvaratkaisujen valinta on haasteellinen tehtävä ja vaatii tarkkaa perehtymistä asiaan. Viruksentorjuntaohjelmistoissa on eroja esimerkiksi siinä, miten usein tietokannat, joista virustiedot tarkistetaan, päivittyvät. Myös ohjelmistojen käytettävyydessä voi olla suuriakin eroja. Toiset viruksentorjuntaohjelmistot vaativat huomattavasti enemmän kapasiteettia pyöriäkseen, kuin toiset, mikä voi huonossa tapauksessa aiheuttaa käyttäjien turhautumista. Tietoturvaratkaisun vaikutukset tekniikan käytettävyyteen ovatkin erityisen huomion arvoinen asia. Jos käyttäjä turhautuu tietoturvaratkaisuun sen käytettävyysongelmien vuoksi, huonossa tapauksessa hän voi jopa kytkeä kyseisen ratkaisun pois päältä. Seurauksena voi olla arvaamattomia ongelmia.

Resursointia ja organisointia

Järjestelmät ja laitteet vaativat myös jatkuvaa ylläpitoa hankinnan jälkeen, ja ylläpidon organisointi onkin syytä tehdä tehokkaasti. Pienessä yrityksessä ylläpitoon ei ole välttämättä mahdollisuutta varata omia resursseja. Tällöin ylläpito voidaan ulkoistaa. Vaikka ulkoistamiseen päädyttäisiinkin, tietoturva-asioiden perustietämys on silti järkevää hankkia myös organisaatioon sisälle. Näin voidaan säilyttää

Tietoturvapolitiikan kirjoittaminen on sinänsä tärkeä ponnistus yrityksessä, mutta sen todellinen jalkauttaminen on erityinen voimanponnistus. Tämä edellyttää koko organisaation sitoutumista politiikassa asetettuihin tavoitteisiin, säännöllistä kou-

TURVAMIES TARJOAA RATKAISUA, KUN VAHINKO ON SATTUNUT

Turvamies tietoturvapalvelut on suomalainen, Ylöjärvellä pari vuotta toiminut tietoturvayritys, joka tarjoaa palveluaan tietojen saavutettavuuteen liittyvissä ongelmatilanteissa. Turvamies palvelee asiakkaitaan siinä vaiheessa, kun vahinko on jo tapahtunut. Tällainen tilanne voi olla esimerkiksi tietojen hukkuminen vian tai virheellisen käytön seurauksena. Turvamies on erikoistunut erityisesti tietojen palauttamiseen sekä sähköiseen rikostutkintaan. Turvamies työllistää vakituisesti kaksi henkilöä ja lisäksi toimintaan osallistuu joukko freelancereita sekä alihankkijoita.

Tietojen palauttamiselle voi syntyä tarve esimerkiksi, jos tietokoneen kiintolevy hajoaa eikä varmuuskopioinnista ole huolehdittu. Turvamiehen palvelun avulla tiedot voidaan palauttaa lukuisista eri medioista, kuten kiintolevyltä, CD-, DVD- ja ZIP –levyiltä, varmistusnauhalta, digikameran muistikortilta tai USB-muistitikulta. Tietojen palauttaminen onnistuu jopa formatoidulta kiintolevyltä ainakin, jos levylle ei ole tallennettu uusia tiedostoja alustamisen jälkeen. Vanhojen tiedostojen palauttaminen voi onnistua vaikka tallennusvälinettä olisi käytetty alustamisen jälkeenkin, mutta tällöin alkuperäinen hakemistorakenne kuitenkin todennäköisesti menetetään.

Jos kiintolevyssä on erittäin vaikea fyysinen vika, tapahtuu kiintolevyn sisällön pelastaminen käsityönä steriilissä puhdasilmalaboratoriossa. Tällainen työ on luonnollisesti varsin työlästä ja kallista, mutta tiedot voidaan näin varsin suurella todennäköisyydellä saada palautettua muutoin epätoivoiseltakin vaikuttavissa tilanteissa.

Turvamies auttaa myös tietomurtojen, talousrikosten ja muiden väärinkäytösten selvittämisessä keräämällä ja analysoimalla todistusaineiston. Tämä voidaan usein tehdä koneen käyttäjän asiaa tietämättä. Todisteina voivat toimia esimerkiksi poistetut tiedostot, sähköpostiviestit, Internet-selaimen historiatiedot jne. Tutkinnan tavoitteena voi olla paitsi syyllisyyden myös syyttömyyden osoittaminen.

Katri Asikainen Turvamies Tietoturvapalveluista korostaa, että alalla toimimisessa keskeistä on erityisesti kattava asiantuntemus ja kokemus, sillä ne ovat esimerkiksi tietojen palauttamisessa onnistumisessa ehdoton edellytys. Ala on haastava, ja vaatii valtavan yleistiedon tietotekniikasta.

lutusta ja ongelman todellisen luonteen ymmärtämistä.

Ennakointi kannattaa myös taloudellisesti

Tietoturvatason parantaminen järjestelmässä jälkikäteen, ikään kuin päälle liimaamalla, aiheuttaa helposti monia ongelmia. Jälkikäteen reagoimalla syntyy kuluja, kun totuttuja toimintatapoja joudutaan muuttamaan. Tulokset eivät välttämättä ole toivottuja, vaan ratkaisun liittäminen jälkikäteen aiheuttaa helposti esimerkiksi yhteensopivuusongelmia järjestelmän muiden osien kanssa. Myös käytettävyysongelmat korostuvat tällaisessa tilanteessa. Kuitenkin luonnollisesti näin on toimittava, mikäli asiaan ei ole jo järjestelmän suunnitteluvaiheessa kiinnitetty huomiota.

Tietoturvaa suunniteltaessa yrityksessä kannattaa huomioida, että tietoturva on ennen kaikkea prosessi, ei niinkään yksittäinen tuote tai palvelu. Erilaiset tietoturvatuotteet ja -palvelut ovat sinänsä tarpeellisia ja tärkeitä tietoturvan osa-alueita, mutta eivät yksistään riitä turvaamaan pienenkään yrityksen tietojärjestelmiä. ■

Tietoturva määritellään yleisesti niin kutsutun CIA-mallin mukaisesti. CIA-mallin nimi tulee sanoista luottamuksellisuus (confidentiality), eheys (integrity) ja saavutettavuus (availability). Luottamuksellisuudella tarkoitetaan, että tietojen tulee olla vain niihin oikeutettujen saavutettavissa. Eheydellä viitataan tietojen luotettavuuteen siinä mielessä, että tiedot eivät saa päästä muuttumaan mistään syystä niiden käsittelyn myötä. Saavutettavuudella tarkoitetaan, että tietojen tulee olla niihin oikeutettujen käytettävissä määräajassa, eivätkä tiedot saa olla esimerkiksi tuhottavissa vikojen, tapahtumien tai muun toiminnan seurauksena.

Ajan kuva

ylivuoto

Hyviä päivittäisten ja ajankohtaisten tietoturvauutisten tietolähteitä ovat mm.

- ***http://www.digitoday.fi***
- ***http://www.itviikko.fi***
- ***http://hightechforum.kaleva.fi/***
- ***http://www.cert.fi***

CERT-FI:n varoitukset

Viestintäviraston CERT-FI-ryhmän laatimat varoitukset:

http://www.ficora.fi/suomi/tietoturva/varoitukset.htm

POMI

Luotettavuus kaikilla tasoilla on turvallisuutta – siksi Pomi.

POMI 9153 Toimiston tehokone

Pomi 9153, jossa hyrisee **Microsoft Office Pro 2003** on varma kumppani. Se kestää, toimii ja siihen voi luottaa. Ja jos jotain sattuisi, Pomin tekninen tuki palvelee sinua koko takuuajan puhelinmaksun hinnalla.

Pomi 9153 on täysin plug&play –valmis kokonaisuus työasemia uusiessanne, olipa niitä sitten kaksi, kaksisataa tai kaksituhatta. Ja kun jälleen tulee aika uusia konekantaa, Pomin ainutlaatuinen **takaisinostositoumus** on suureksi avuksi. Pääsette kätevästi eroon vanhoista Pomi -koneistanne ja saatte niistä vielä rahaa. Toki Pomin ylivertaisen pitkä **48 kk takuu** siirtää uusimistarvettakin reilusti tuonnemmaksi.

Kun pitää keskittyä olennaiseen, on syytä valita työkalut oikein. Silloin on helppo hymyillä, töissäkin.

2235,-

Microsoft Office Professional Edition 2003

Paketti sisältää mm.:
3.2 GHz Intel® Pentium® 4 prosessorin,
1GB DDR400 muistia, 200 Gt kovalevyn,
Microsoft Windows XP Pro -käyttöjärjestelmän,
Microsoft Office Pro 2003 -ohjelmistopaketin
ja **kaksi 17" LCD-näyttöä**.

POMI-rahoituksella 74,23 euroa / kk 36 kk:n ajan, luottohinta 2.672,42 euroa. Todellinen vuosikorko 12,69%.

Konalantie 47 A, 00390 Helsinki
Kurikkatie 6, 90440 Kempele
puh 0403 431 592
puh 0207 431 502
myynti@pomi.fi

Tietoturvan säätila

Timo Lehtimäki

Missä mennään tietoturvallisuudessa? Mitkä ovat tämän hetken todelliset riskit ja missä liioitellaan? Uudet asiat ja ilmiöt aiheuttavat aina epätietoa ja tietoturva-asioissa joskus tuskaakin – kuinka näihin tulisi suhtautua? Onko tietoturva jatkuvaa teknologiatrendien ja uusien uhkien perässä juoksemista?

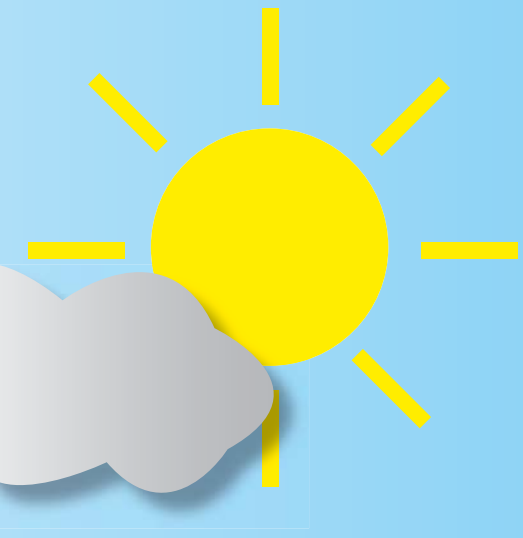
Tietoturvan hallinta helpottuu huomattavasti, jos voidaan kehittää tilanteeseen sopivia mittareita tarjoamaan todistusaineistoa hallittavan järjestelmän tietoturvasta. Mittaustulosten avulla voidaan reagoida mahdollisiin puutteisiin ja varmistaa että vaadittu tietoturvataso saavutetaan. Tällaisia mittareita voidaan kutsua tietoturvamittareiksi. Tietoturvamittareilla voidaan mitata esimerkiksi teknisiä järjestelmiä, organisaatioita tai liiketoimintaprosesseja — tai vaikkapa näitä kaikkia yhtä aikaa.

Tietoturvasää tänään ja huomenna

Virus- ja matoepidemiat eivät jyllänneet alkuvuoden otsikoissa. Onko tietoturvauhkien osalta vihdoin tapahtunut käänne parempaan? Valitettavasti virus- ja matoepidemioiden valossa ei kuitenkaan ole koko tietoturvan spektri edustettuna. Tämä vahvasti tietoturvajulkisuutta ja medianäkyvyyttä aikaansaava tietoturvan varjopuoli ei siis kuvasta tietoturvan tilaa – ei ainakaan siinä mielessä että voisi henkäistä helpotuksesta. Vakavia ohjelmistohaavoittuvuuksia löydetään jatkuvasti kiihtyvällä tahdilla, haavoittuvuuksien julkistamista seuraa entistä nopeammin sen hyväksikäyttö. Uhkia on siis koko ajan olemassa, ja samalla Internetin suosio jatkuvasti kasvaa. Erityisesti kiinteällä laajakaistayhteydellä varustettujen kotikoneiden määrä on voimakkaasti lisääntynyt. Seurauksena on ollut huonosti ylläpidettyjen ja helposti haltuun otettavien järjestelmien voimakas kasvu.

Uusien uhkien jatkuva esiinmarssi ja lisääntyvä käyttäjäkunnan heterogeenisuus aiheuttaa ongelmia kaikille – itse asiassa koko infrastruktuurille. Puutteelliset asenteet ja jossain määrin myös tiedot aiheuttavat globaalin ongelman ns. epäsymmetrisen uhkan muodossa: toisten tietoturvan laiminlyönneistä joutuvat kärsimään myös ne, jotka itse huolehtivat tietoturvastaan. Tämä on seurausta vallalla olevasta ilmiöstä, jossa hyökkääjän intresseissä on ensisijaisesti saavuttaa itselleen tai yhteistyökumppanilleen hyödynnettäviä resursseja. Näitä ovat helpoimmillaan lukuisat haavoittuvat ja nopeilla tietoliikenneyhteyksillä varustetut kotitietokoneet. Tämän epäsymmetrisen uhkan lisäksi myös taistelu tietokoneen herruudesta on valitettavasti epätasainen: hyökkääjän tulee löytää yksi aukko, puolustuksen tulee tukkia kaikki.

Hyökkääjien toiminta on myös muuttumassa entistä enemmän näkymättömämmäksi ja ammattimaisemmaksi. Hyökkäyksiä tehdään esimerkiksi kohdistetusti ja niillä tavoitellaan joko suoraa tai välillistä taloudellista hyötyä. Kohdennettuja haittaohjelmahyökkäyksiä on esimerkiksi tehty valtion toimijoita ja merkittäviä yrityksiä vastaan. Tämän kaltaisilla hyökkäyksillä tyypillisesti tavoitellaan taloudellis-teknillisiä tietoja kohdeorganisaatioista, ja hyökkäyksissä käytetään edistyksellisiä sosiaalisen hakkeroinnin elementtejä niin, että viestien sisältö on ollut kohdelukijan substanssin kannalta mielenkiintoista ja varsin paikkaansa pitävää informaatiota. Haittaohjelmia on esimerkiksi ujutettu kohdeorganisaatioihin sähköpostin lii-



tetiedostojen välityksellä sekä html-linkkeinä, jotka ohjaavat vastaanottajan haittaohjelman sisältämälle www-sivustolle. Huomattavaa on, että virustorjuntaohjelmistot ja palomuurit eivät anna täydellistä suojaa tämän tyyppisiltä hyökkäyksiltä, sillä hyökkääjät ovat käyttäneet haittaohjelman teknisissä ominaisuuksissa mm. palomuurin ohittavia tekniikoita, kuten yleisesti käytössä olevia tietoliikenneportteja.

Vaikka organisaatio ei kuuluisikaan kriittisiin yhteiskunnan toimijoihin tai vaikka taloudellisen edun tavoittelu ja esimerkiksi yrityssalaisuuksien varastaminen ei olisikaan uhka yritykselle, ei tietoturvauhkiin voi silti suhtautua välinpitämättömästi. Tällaisissa tapauksissa käytännön ongelmat liittyvät usein hyvin arkipäiväisiin asioihin, joilla on vahva kytkös tietoturvan toteutumiseen. Käytännön konkreettiset uhkat liittyvät järjestelmien käytettävyyteen ja palveluiden saatavuuteen. Toiminnan jatkuminen voi olla uhattuna yleisten tietoverkkojen kautta leviävien uhkien myötä ja kullan kallista työaikaa ei saisi tuhrautua tietoteknisiin ongelmiin eikä varsinkaan tietoturvaongelmien kanssa painimiseen.

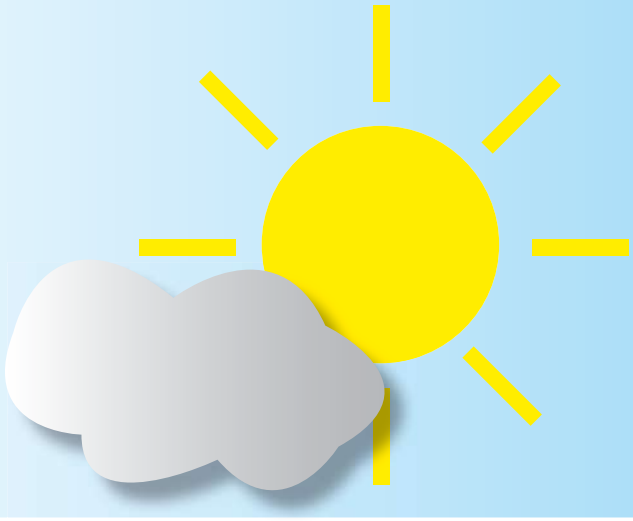
Tällä hetkellä tuoreina ilmiöinä ovat melko vahvasti esillä myös mobiilivirukset ja phishing. Erilaisten huijausviestien (ns. phishing-hyökkäykset) yleistyminen on ollut voimakasta, mutta Suomessa tämä ilmiö ei kuitenkaan elä mitään kulta-aikaa (toistaiseksi). Meitä auttavina tekijöinä ovat esimerkiksi moniin muihin maihin verrattuna paremmin suojatut verkkopankkitoteutukset sekä niinkin yksinkertainen asia kuin kielimuuri. Useimmat phishing-huijausviestit on tehty englanniksi, ja näihin ei välttämättä Suomessa tartuta. ”Hoonolla Soomella” tehtyjen viestien joukko taasen kuuluu lähinnä vitsikirjaan. Matkaviestimiä uhkaavien mobiilivirusten esiinmarssi on väistämätön, mutta toistaiseksi käytännön tapaukset ovat mikroskooppista luokkaa perinteisiin haittaohjelmiin ja ohjelmistohaavoittuvuuksiin verrattuna.

Vaikka tänään paistaa aurinko, voi huomenna olla rankkasadetta – muutokset voivat verkottuneessa maailmassa olla nopeita. Kehitystrendinä uskotaan jatkuvan taloudellisen hyödyn tavoittelun ja haittatoiminnan ammattimaistumisen. Toisena huomioitavana trendinä ovat matkapuhelimiin kohdistuvat haittaohjelmauhkat. On todennäköistä, että tulevaisuudessa älypuhelimiin pyritään kohdistamaan hyökkäyksiä, joilla voidaan tavoitella myös taloudellista hyötyä. Tällä alueella on nyt kiire tehdä ennakoivia toimenpiteitä – lisäksi on muistettava, että tulevaisuuden maailma on käyttäjänäkökulmasta mobiili.

Mihin pitäisi panostaa?

Tietoturva on jo pitkään kuumana käynyt alue. Koko käsite saattaa jo kyllästyttääkin, mutta kyseessä on jatkuvia ponnisteluja vaativa alue, jossa vastuu jakaantuu laajalle joukolle toimijoita. Koko alueen hallitseminen aina loppukäyttäjiin asti on haastavaa. Organisaatioiden varautumistoimet Internetin uhkia vastaan korostuvat jatkuvasti, mutta samalla tietoverkkojen tietoturvauhkat kohdistuvat myös entistä enemmän kotitietojärjestelmiin. Vuoden 2004 kansallisen tietoturvapäivän teesit - palomuurin ja ajantasaisen virustorjunnan käyttö sekä ohjelmistojen päivittäminen - korostuvat myös jatkossa. Ohjelmistojen päivittäminen on nykyään ensimmäinen edellytys turvalliselle toiminnalle. Valitettavasti tietoturvakulttuuri ei ole kotiutunut vielä niin hyvin Suomeenkaan, että tämä perusasia olisi hoidettu kuntoon. Tietotekniset järjestelmät vaativat jatkuvaa huolehtimista ja ylläpitoa toimiakseen turvallisesti ja tehokkaasti. Valitettavasti tämä sama tarve tullee olemaan arkipäivää myös mobiilimaailmassa älykkäiden päätelaitteiden ohjelmistohaavoittuvuuksien johdosta. Haavoittuvien ohjelmistojen päivittäminen on noussut yhä merkittävämpään asemaan tietoturvan hallinnan kannalta.

Tietoturvallisuus ei siis saa rajoittua virustorjunnan käsitteeseen. Tulevaisuuden uhkilta ja edes haittaohjelmilta suojautumiseen eivät riitä virustorjuntaohjelmistot ja palomuurit. Esimerkiksi myös nopeasti leviävät verkkomadot kykenevät saastuttamaan kaikki Internetin järjestelmät nopeammin kuin virustorjuntaohjelmistojen päivitykset



ovat valmiita. Puolustuksellinen syvyys on tärkeää, ja tietojärjestelmien turvallisuustason tarkennus uusia uhkia vastaan sekä ongelmien huomioiminen mm. kohdeorganisaatioiden riskianalyyseissä ja ennaltaehkäisevissä tietoturvallisuustoimissa on välttämätöntä.

Miksi haavoittuvia järjestelmiä ei sitten päivitetä? Eikö tarjolla ole riittävästi tietoa haavoittuvuuksista ja haavoittuvien ohjelmistojen päivittämisen merkityksestä? Tietoisuus uhkien vaaroista ja toimet tietoturvan toteuttamiseksi ovat organisaatioissa usein heikoissa kantimissa. Teknisistä asioista puhuminen on tietoturvallisuusajattelussa kuitenkin vain johdatusta aiheeseen. Tekniset toimet ja keinovalikoimat ovat vain yksittäisiä askelia koko elinkaaren kestävässä maratonjuoksussa. Tietoturvallisuus olisikin hyvä mieltää laatukriteerinä, ja samalla tiedostaa, että sen toteuttaminen maksaa. On ensiarvoisen tärkeää, että organisaatioiden johdolla on riittävä näkemys tietoturvan merkityksestä. Organisaatioiden tietoturvaa voidaan ylläpitää ja kehittää ainoastaan johdon tuella – käytännössä siis rahalla ja resursseilla. Vanha hokema on edelleenkin validi: tietoturvallisuuden toteuttaminen ei ole aina hauskaa, helppoa ja halpaa. Ongelma on siis tietoturva-alueen ali-investoinnit ja laajan kokonaisuuden näkemys. Toisaalta myös aiheen mediaseksikkyys ja halu tietää naapuria koskevista ongelmista vaikuttaa aiheeseen. On lyhytnäköistä, mutta tuiki tavallista pistää pää pensaaseen ja toivoa parasta. Toisten ongelmat kyllä ovat hauskoja tarinoita, mutta itse ei olla valmiita konkreettisiin toimiin.

Miten sitten suhteuttaa toimet vastaamaan todellista tarvetta? On muistettava, että täydellisyyteen pyrkiminen kuuluu tietoturvakentässä vain harvoille (esimerkiksi tietoturvatuotteita valmistaville yrityksille). Teknisillä osa-alueilla ei useinkaan ole mahdollista päästä täydellisyyteen, sillä uusia teknisiä uhkia tulee esiin jatkuvasti. Tällöin on ensiarvoisen tärkeää hallita organisaation riskejä ja tehdä tarvittavat toimenpiteet riskianalyysien perusteella. Laajempana kokonaisuutena voidaan kuitenkin todeta, että tietoturvallisuuden hallinnolliset osa-alueet on saatettavissa kuntoon jos halua ja resurssipanostusta on riittävästi. Puutteellinen yhteistyö ja tietämättömyys ovat edelleen suuria ongelma-alueita. Liian usein tietoturva on yksittäisten säätäjien yksinäistä puuhastelua vailla hallittua lähestymistapaa ja avointa yhteistyötä parhaiden käytäntöjen levittämiseksi.

Koska täydellisyyteen ei päästä, on todennäköistä että syntyy tilanteita joissa tietoturvauhka realisoituu. Toiminnan jatkuvuuden kannalta on siis väänjäämättä panostettava myös reaktiiviseen toimintaan ja esimerkiksi laadittava erillinen toipumissuunnitelma vastuuhenkilöineen ja toimenpideluetteloineen. Mikäli mahdollista, tulisi myös etukäteen selvittää järjestelmien kyky sietää erilaisia vika- ja ongelmatilanteita. Tulevaisuudessa vikasietoisten ympäristöjen suunnittelu tulee olemaan keskeinen osa kriittisten järjestelmien tietoturvasuunnittelua.

Mistä saa apua?

Tulevaisuuteen investoinnin soisi yleistyvän tietoturvan alueella. Kansallisen tietoturvallisuusstrategian hankkeet ovat askelia tähän suuntaan. Kuinka esimerkiksi saadaan tietoturvauhkista tietoja, jotka toimivat päätöksenteon apuvälineinä? Viestintäviraston vastuualueena oleva tietoturvallisuuden tilannekuva –hanke on pyrkimys edetä kohti tätä tavoitetta. Eräänlaista sääennustetta pyritään luomaan tietoturvatilanteesta. Ennusteissa on aina epätarkkuuksia, eivätkä ennusteet aina toteudu. Tavoitteena on tarkentaa kuvaa ajan edetessä.

CERT-FI ryhmä on ryhtynyt julkaisemaan neljännesvuosittain raporttia ajankohtaisista tietoturvallisuusasioista. Tällä tilanneseurannalla CERT-FI pyrkii mm. auttamaan yrityksien, yhteisöjen ja yksityisten henkilöiden ennaltaehkäisevää tietoturvallisuustyötä. Vuoden lopun raportti kokoaa koko vuoden tapahtumat tiiviisti yhteen ja ennustaa tulevan vuoden ilmiöitä. Erilaisten katsausten on tarkoitus antaa apua tietoturva ilmiöiden seurannassa ja tarvittavien toimenpiteiden suhteuttamisessa. CERT-varoituksilla on tarkoitus aiheuttaa välittömiä toimenpiteitä. Tilannekuvan tai tietoturvan säätilan on tarkoitus toimia päätöksenteon apuvälineenä. CERT-FI:n tärkeimpiin tehtäviin kuuluukin nostaa ylläpitäjien tietoturvatietämystä neuvomalla ja ohjeistamalla sekä ennen kaikkea aktiivisesti tiedottamalla ajankohtaisista tietoturvauhista.

Ei kannata heittää kirvestä kaivoon

Tietoyhteiskunta-sanan käyttö tulisi lopettaa, sillä kyse on jo normaalitilasta. Tähän on tultu eikä pois päästä – ei tosin kyllä halutakaan. Nyky-yhteiskunta tarjoaa niin paljon, ettei siitä haluta luopua ja siirtyä ajassa takaisin. Tietoturvattomuus voi tosin tämän harppauksen hetkellisesti tehdä puolestamme. Verkottuneisuus ja yhteiskunnan – mukaan lukien kriittinen infrastruktuuri - sidonnaisuus tietoverkkojen ja -palvelujen toimivuuteen on välttämätöntä eikä virheisiin tietoturvan osalta ole varaa.

Kaukana on kuitenkin vielä se ”haavemaailma” jossa jatkuvasti tehdään uusia tietoturvallisia innovaatioita ja turvallisuus on integroitunut osaksi tuotteita ja toimintaa. Haavemaailmassa tietoturvallisuutta käytetään jopa markkinointikeinona ja kriteerinä yhteistyökumppanin valinnassa. Tämä tosin vain uutuuksien osalta – minimitasoa kuten ”turvavöiden” olemassaoloa ei kukaan enää pidä valttina. Tavoitteena tulisi siis olla tietoturvan jalkauttaminen organisaatioiden tavaksi toimia ja samalla sisäänrakennetuksi ominaisuudeksi tuotteissa ja palveluissa.

Jani Kenttälä

Luojaansa vastaan kääntynyt tietoturva

Sähköpostien liitetiedostot jäävät matkan varrelle. Virustorjuntaohjelmisto vie koneen resurssit. Liian tiukat palomuurisäännöt estävät työnteon. Nyt on hyvä aika pohtia, kääntyikö tietoturva jossakin vaiheessa luojaansa vastaan. Tarvitsemmeko kurinpalautusta? Miten teemme tietoturvasta jälleen hyvän rengin?

Uhrattu saatavuus

Perinteiseen tietoturvan määritelmään kuuluvat termit luottamuksellisuus, eheys ja saatavuus. Tiedon luottamuksellisuuden ja eheyden takaamiseen meillä on ainakin teoreettisesti hyviä menetelmiä. Saatavuuden takaaminen on kuitenkin hankalaa. Ongelma on tuttu myös PK-yrityksissä. Sähköposti ei toimi, liitetiedostot jäävät saamatta, ja WWW-sivut eivät lataudu. Tällaisiin ongelmiin tietoturvatuotteet harvoin puuttuvat onnistuneesti. Monet tietoturvatuotteet päinvastoin heikentävät palveluiden saatavuutta.

Esimerkiksi henkilökohtaiset palomuurit ja antivirusohjelmat aiheuttavat vikatilanteita ja hankaloittavat verkkotyöskentelyä. Me innokaat tietoturva-ajattelun kannattajat emme usko, että kyseessä on ongelma. Joko luotamme turvatuotteiden täydellisyyteen tai teemme tietoisesti kompromisseja palvelun saatavuuden ja muun turvallisuuden välillä. Olemme valmiit uhraamaan esimerkiksi sähköpostin toimintavarmuuden vähentääksemme roskapostin määrää. Toisinaan taas palomuuraamme työntekijämme karsinaan uskoen, että näin estämme toivomattoman liikenteen pääsyn ulkomaailmaan.

Monimutkaisuus on kallista

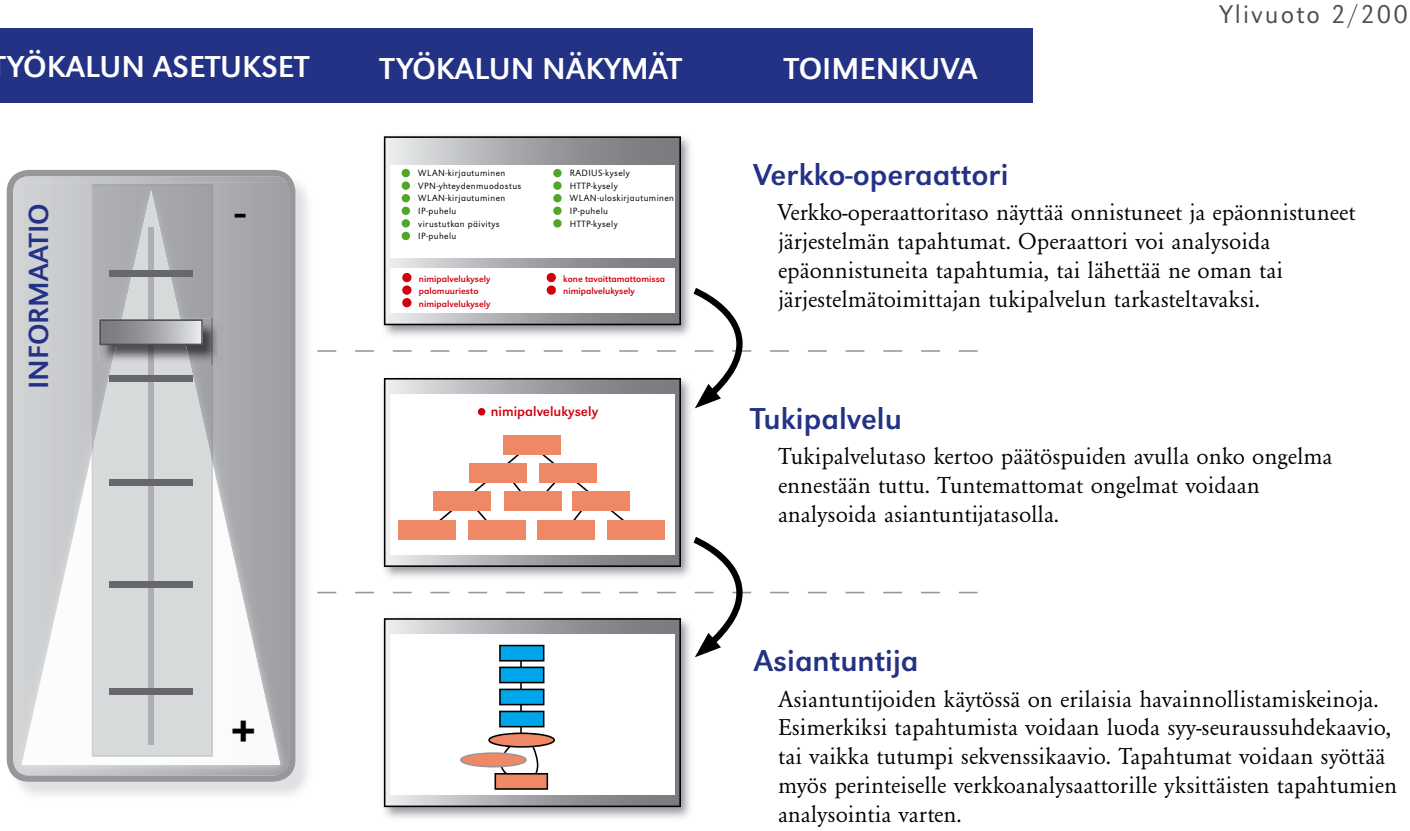
Erillisten turvaominaisuuksien laajamittainen hyödyntäminen monimutkaistaa järjestelmiä. Kasvanut monimutkaisuus tuo mukanaan hankalat vikatilanteet. Protokollien, verkkolaitteiden, tietojärjestelmien ja tietoturvarajoitusten viidakko tarjoaa oivan piilopaikan yksinkertaisillekin violle. Joudumme haaskaamaan vikojen paikallistamiseen tarpeettoman paljon aikaa. Missä on vika, kun sivut eivät lataudu? Keneen otetaan yhteys tilanteen korjaamiseksi? Onko ongelma itseaiheutettu, vai onko palveluntarjoan verkossa häiriö? Asiat eivät ole kunnossa suurissakaan yrityksissä. Maailman 2000 suurinta yritystä käyttävät Gartnerin mukaan keskimäärin 40,7 miljoonaa dollaria per yritys odottamattomien vikatilanteiden selvittämiseen.

Tietoturvatuotteissa tietoturvaongelmia

Toinen ongelma on, että myös tietoturvatuotteet ovat ohjelmistoja. Mitä enemmän lähdekoodirivejä, sitä enemmän tietoturvaongelmia aiheuttavia virheitä. Kokemuksemme Oulun yliopiston tietoturvallisen ohjelmoinnin tutkimusryhmässä (OUSPG) osoittavat, että tietoturvatuotteetkin sisältävät tietoturvaongelmia. Esimerkiksi viimeisin PROTOS-hankkeessa julkaisemamme testityökalu ISAKMP paljasti haavoittuvuuksia nimenomaan tietoturvatuotteista.

Lääkkeeksi lisää osaajia?

Verkkolaitevalmistaja Cisco ehdottaa lääkkeeksi syväosaajien lisäkoulutusta. Cisco Skills Survey -tutkimuksen mukaan Euroopassa on puolen miljoonan syväosaajan vaje vuoteen 2008 mennessä. Arvio perustuu 950 tietohallintojohtajalle lähetettyyn kyselyyn.



Kuva 1. Havainnollistamistyökalun eri tarkkuustasot palvelevat eri kohderyhmiä.

Järjestelmien monimutkaistuessa syväosaajien kouluttaminen on entistä haasteellisempaa. Järjestelmien tarkka ymmärtäminen perinteisin menetelmin on hankalaa, koska ne tuottavat todella paljon tapahtumia. Kuva 2 havainnollistaa pelkkien verkkotapahtumien analysointia perinteisillä työkaluilla. Lyhyenkin aikavälin tapahtumat sisältävät kymmeniä protokollia ja tuhansia verkkotapahtumia.

Ei ole ihme, että osaajille löytyy kysyntää!

Osaajien tueksi uusi menetelmä

OUSPG:n Frontier-hankkeessa tartuttiin osaajapulan luomaan haasteeseen. Hankkeessa kehitetty menetelmä tarjoaa tietojärjestelmien kanssa painiskeleville helpotusta. Menetelmää tukemaan kehitetty tutkimusprototyyppi helpottaa tiedonkeruuta. Lisäksi se auttaa ihmisiä ymmärtämään verkon tapahtumia uusien havainnollistamismenetelmien avulla.

Tiedonkeruu helpommaksi

Tiedonkeruuta helpotetaan liittämällä ulkopuoliset luotaimet tiedonkeruuta ja tallennusta varten. Voimme esimerkiksi vikatilanteen sattuessa pyytää luotaimilta verkon tapahtumat virhetilanteen ajalta. Näin säästymme aikaavievältä ongelmatilanteen rekonstruoinnilta. Tapahtumat toimitetaan analysointityökalulle, joka havainnollistaa ne haluamassamme muodossa. Tapahtumien lisäksi saamme tiedon siitä, missä mittauspisteessä kukin tapahtuma on nähty.

Havainnollisuudella informaatiotulvaa vastaan

Tapahtumien havainnollistamisessa hyödynnetään järjestelmän tapahtumien syy-seuraussuhteiden tunnistamista. Menetelmä tarjoaa aiempaa paremmat mahdollisuudet havainnollistaa verkon tapahtumia. Menetelmän avulla pystymme erottamaan olennaiset tapahtumat epäolennaisista ja vertailemaan ongelmatilanteen tapahtumia toimivan järjestelmän dokumentaatioon.

Havainnollistamistekniikoilla on monta sovelluskohdetta, vikadiagnostiikka nopeutuu, ja ongelmien raportointi helpottuu. Lisäksi uusien järjestelmien kehitys, käyttöönotto ja dokumentointi automatisoituvat. Parhaimmillaan voimme paikantaa ja raportoida ongelmakohdan nopeasti siitä vastaavalle taholle.

Mielenkiinto uusiin haasteisiin

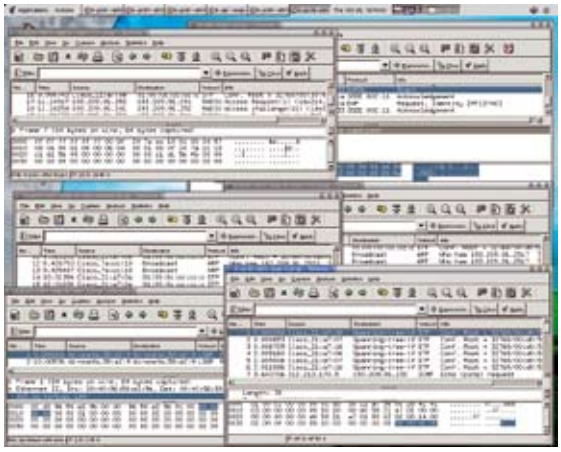
Nykyisten järjestelmien massiivisuus on loistava esimerkki ihmisten insinööritaidoista. Pitkälle viedyt taidonnäytteet asettavat kuitenkin suuret haasteet järjestelmien ylläpidolle ja vianselvitykselle. Brian Kernighan on pohtinut asiaa ohjelmistotuotannon näkökulmasta: ‘Vianmääritys on kaksi kertaa hankalampaa kuin ohjelmoiminen. Jos siis ohjelmoit mahdollisimman nerokkaasti, määritelmän mukaan et voi olla riittävän älykäs löytämään tuotoksesi vikoja.’ Onneksi hyvät työkalut parantavat mahdollisuuksiamme. Suuntaamalla mielenkiintomme monimutkaisuuden luomiin haasteisiin voimme palauttaa järjestelmät niille kuuluvaan rooliinsa, hyväksi rengiksi.

Käytännön esimerkki: Verkon selaaminen ei onnistu

Ratkaisumenetelmä: Tutkitaan verkkoliikennettä ja logiviestejä perinteisillä verkkoanalysaattoreilla

Perinteisillä menetelmillä järjestelmän vianselvitys on vaivalloista. Etenkin monimutkaisissa verkoissa selvittäjä joutuu keräämään verkkoliikennettä monista mittapisteistä. Tiedon määrä on valtava (kuva 2). Päästäkseen alkuun selvittäjän pitää erottaa olennaiset tapahtumat epäolennaisista. Tämän jälkeen hänen tulee vielä tuntea järjestelmälle normaalit tapahtumaketjut, jotta hän löytää täsmällisen ongelmakohdat.

Lähestymistavassa on monta ongelmaa. Poikkeuksellisten tapahtumien löytäminen vaatii paljon kokemusta. Lisäksi kokeneetkaan etsijät eivät huomaa kaikkia kummallisuuksia informaatiotulvan seasta. Jos viat saadaan paikallistettua, niiden raportointi järjestelmätoimittajalle on työlästä ja epätarkkaa.



Kuva 2. Perinteisten menetelmien tuottama informaatiotulva.

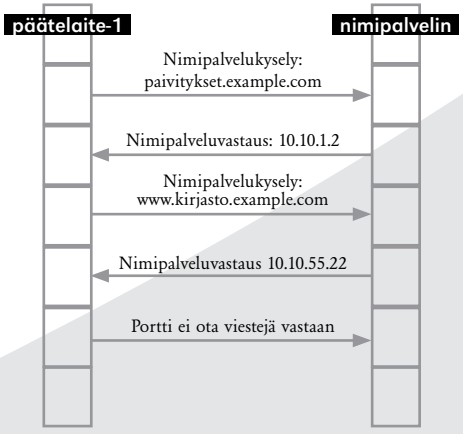
Ratkaisumenetelmä: Vikatilanteen selvitys verkon selkeytystyökalulla

Yrityksen työntekijät käyttävät kannettavia tietokoneita ja langatonta verkkoa työnteossa. Uusimpien standardien mukaiset langattomien verkkojen tietoturvaominaisuudet ovat käytössä.

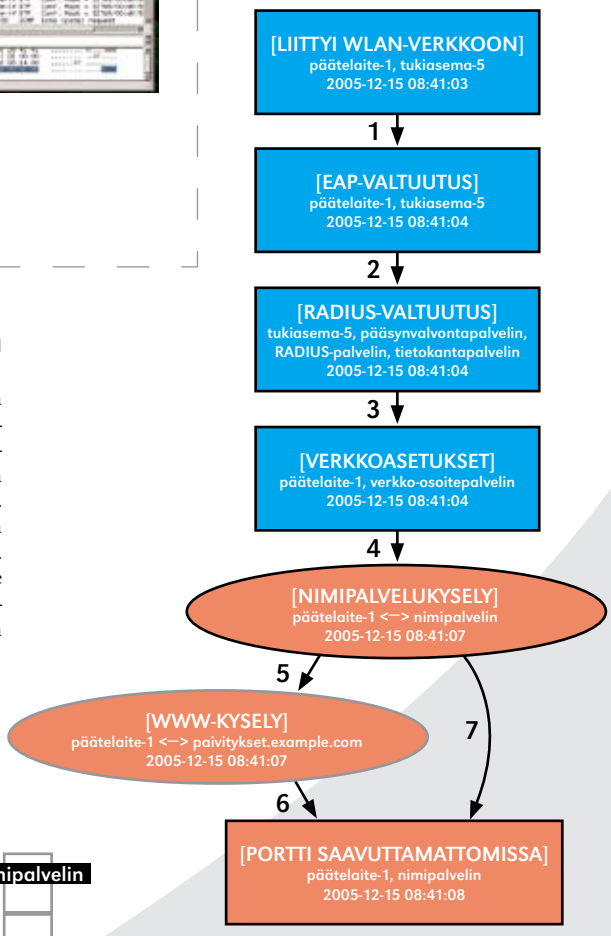
Verkon ylläpitäjän näytöllä on verkon selkeytystyökalu yksinkertaisimmalla tarkkuustasolla. Esimerkki nähdään kuvassa 1 tasolla 'verkko-operaattori'. Näytön yläosassa näkyy onnistuneita tapahtumia (vihreä teksti). Epäonnistuneet tapahtumat jäävät näytön alaosaan (punainen teksti). Ylläpitäjä huomaa, että epäonnistuneiden nimipalvelukyselyiden määrä kasvaa nopeasti. Hän ohittaa tukipalvelulle tarkoitetun toisen tason ja kasvattaa tarkkuuden suoraan syy-seurausstasolle. Tällä tasolla ylläpitäjä huomaa mielenkiintoisen tapahtumaketjun.

Ongelmatapauksissakin langattomaan verkkoon kirjautumisen eri vaiheet menevät onnistuneesti läpi. Monet tapahtumat tunnistetaan tyypillisiksi tapahtumasarjoiksi, joita kuvan 3 laatikkomuoto havainnollistaa. Päätelaitteen liittyttyä langattomaan lähiverkkoon tukiasema aloittaa valtuutusprosessin (1). Tämän seurauksena valtuutukseen liittyvä tapahtumaketju jatkuu syvemmällä verkossa (2). Onnistuneen valtuutuksen seurauksena päätelaite saa verkkoasetukset (3). Seuraavaksi päätelaite kysyy palomuurivalmistajan Internet-osoitetta nimipalvelimelta (4). Tämän jälkeen tutkimusprototyyppi tarjoaa kaksi vaihtoehtoa: Joko ensimmäinen nimipalvelupyyntö epäonnistui (7), tai epäonnistumista edelsi vierailu palomuurivalmistajan WWW-palvelimella (5,6). Ylläpitäjä analysoi nimipalvelutapahtuman ja portti saavuttamattomissa -tapahtuman tarkemmin. Hän avaa tapahtumat sekvenssikaaviossa (kuva 4). Kaavion mukaan ensimmäinen nimipalvelukysely on onnistunut. Jäljelle jää mysteerinen yhteys palomuurivalmistajan kotisivulle.

Ylläpitäjä valitsee WWW-kyselytapahtuman ja avaa tapahtumat vielä perinteisessä verkkoanalysaattorissa. Analysaattorin mukaan palomuuri näyttää päivittävän itsensä WWW-yhteyden avulla. Syyllinen on siis palomuurin uusi versio. Se estää verkon toiminnan kannalta olennaisen tapahtuman, nimipalvelutietojen vastaanoton. Ylläpitäjä raportoi vian palomuurin valmistajalle ja liittää mukaan visualisaatiot vikatilanteen. Palomuurivalmistaja rajaa ongelman yksiselitteisen ongelmakuvauksen avulla ja aloittaa korjaukset.



Kuva 4. Sekvenssikaavio nimipalvelukyselyistä.



Kuva 3. Tutkimusprototyypin tuottama syy-seurausnäkymä järjestelmän tapahtumista.

[Kiinnostuitko työkalusta?
Kysy lisätietoja osoitteesta
frontier@ee.oulu.fi]

Paranoidi fundamentalisti

Avointen verkkojen VAARAT

Kysyttiinpä asiaa sitten viranomaiselta tai kansalliselta tietotekniikan popularisoijalta, suurimpana tietoturvahuolena kotikäyttäjän kohdalla on tänä päivänä pidettävä liian helposti verkkoonpääsyä tarjoavaa kotiwlania. Kyberterroristien, pedofiilien ja talousrikollisten vaaniessa kaikkialla täytyy jokaisen olla silmä ja korva tarkkana, aina valmiina käräyttämään naapuri tai muu vaarallinen hiippailija, jos tämä omine lupinensa haksahtaa surffailemaan webissä kotiverkkosi kautta. Vain siten voimme yhteisvoimin voittaa tämän tietoverkkojamme mustaavan saastan. Naapurin mafioson ryhtyessä masinoimaan mittavaa talousrikosjuonta liittymäsi kautta voit syyttää vain itseäsi, kun sinua tullaan hakemaan.

Mutta vaikka olisitkin valpas kotona, jää silti vorojen käyttöön melkoinen arsenaali mahdollisia anonyymejä kommunikaatiovälineitä. Prepaid-puhelinliittymiä ollaan onneksi jo kieltämässä ja puhelinkioskit ovat poistumassa katukuvasta. Nettikahviloiden, muuten vain julkisten wlanien ja paperipostin osalta valvonta on vielä vajavaista. Nettikahviloiden ja muiden yleisissä tiloissa olevien tietokoneiden osalta Suomessa kannattaisi ottaa oppia Italiasta, jossa nettikahviloilla on laillinen velvollisuus varmentaa ja kirjata asiakkaiden henkilöllisyys esimerkiksi passista, ennen kuin potentiaalinen tuholainen päästetään selaimen ääreen.

Nykyisin isommat rosmot tosin hoitavat verkossa asiointinsa virusten kaappaamien kotitietokoneiden välityksellä, mutta tämähän johtuu vain loppukäyttäjien asiakasohjelmistojen haavoittuvuuksista. Eiköhän siihen ongelmaan keksitä jokin ratkaisu aivan lähitulevaisuudessa, vai mitä.

Kaikista ilmeisin uhka vapaalle yhteiskunnalle on kuitenkin anonyymi ja vaikeasti jäljitettävä, rajattoman tuhopotentiaalin omaava käteinen raha. Hyvänä kakkosena tulee ihmisten tulemisten ja menemisten jäljittämisen vaikeus. Kumpaankin näistä olisi helppo tekninen ratkaisu (korttiraha ja RFID-implantit). Poliitikot eivät ole selvästikään vielä ymmärtäneet asiaa, joka tietoturva-alalla on ollut yleisesti tiedossa jo pitkään: Ongelmiin löytyy yleensä helppo ja ongelmaton tekninen ratkaisu.

Ottaisikohan presidentinvaaleissa joku tämän asiakokonaisuuden ajaakseen – jos vaikka joku ehdokkaista kunnostautuisi ajamalla aluksi vaikka kontrollin ja vapauden tasapainon uudelleenharkitsemista kautta yhteiskunnan. Tai edes prepaid-liittymien kieltämistä.

Joskus kuulee hörhöjen mekastavan teletunnistetietojen tallentamista vastaan absurdein perustein. Vainoharhaiseen hölötykseen mahtuu touhottamista anonyymin kommunikaation tarpeellisuudesta ja EU-komission päätöksistä ojentaa satunnaisia röykkiöitä kansalaisia koskevia tietoja hyvään tarkoitukseen pahuuden akselia vastaan sotiville ameriikkalaisille. Kuka tahansa järkevä ihminen ymmärtää ettei Suomessa tarvitse olla huolissaan turvallisuusviranomaisten tai teleoperaattoreiden mahdollisista väärinkäytöksistä. Sitä paitsi tulevaisuudessa tarkasti taltioituja teletunnistetietoja tullaan käyttämään enimmäkseen EU:n yhteisissä turvallisuusorganisaatioissa jotka ovat varmasti paljon läpinäkyvämpiä ja kansanläheisempiä kuin nykyiset kansalliset.

Olet joko tietoturvaratkaisujen puolella, tai niitä vastaan.

EETTISET SÄÄNNÖT OVAT TÄRKEITÄ TIETOTURVA-TYÖSSÄ

Millaiseen toimintaan voidaan käyttää Internetiä kotona ja työpaikalla? Miten voidaan varmistaa, että henkilöiden yksityisyys ja kunnia säilyy, vaikka näitä asioita loukkaavaa tietoa on liikenteessä? Missä menevät rajat ihmisten käyttäytymisen monitoroinnille? Kysymyksiä on paljon eikä selviä sääntöjä ole määritelty moneenkaan tilanteeseen. Elämme aikaa, jolloin jokaisen ihmisen on havahduttava ja otettava osaltaan vastuu käyttäytymisestään informaatioyhteiskunnassa.

Reijo Savola,
Jorma Kajava

Etiikka, oppi oikeista ja vääristä teoista, on elintärkeä ominaisuus ihmiskunnan olemassaololle ja toiminnalle. Eettisen säännöstön luonti on aikaisemmin ollut pitkälti auktoriteettien kuten uskonnon ja lainsäädännön vastuulla. Uusi informaatio- ja tietoliikenneteknologia on nopeassa tahdissa tuonut tullessaan ihmisten käyttäytymiseen ja käsityksiin vaikuttavia ilmiöitä, joiden vauhdissa auktoriteettien säännöstöt eivät ole pysyneet mukana. Uuteen teknologiaan liittyvä lainsäädäntö onkin syytä pitää erityisen tarkkailun alla.

Usein ihmisillä on mielikuva, että kaikki tietotekniikan väärinkäyttöön liittyvät kysymykset kuuluvat tietotekniikan etiikan alueeseen. Valtaosa niistä on kuitenkin normaaleja, lainsäädäntöön liittyviä tapauksia. Jos henkilö syyllistyy rangaistavaan tekoon, hän saa siitä oikeuskäsittelyssä asianmukaisen rangaistuksen. Jo tieto mahdollisesta kiinnijäämisestä ja sitä seuraavasta tuomiosta toimii eräänlaisena pelotefunktiona, joka saa lainkuuliaisen henkilön palaamaan kaidalle polulle.

Korvaako tietoturva eettisen säännöstön?

Tarve tietoturvaratkaisuille korostuu, koska edes ilmiselviä lakiin perustuvia sääntöjä ja käytäntöjä ei noudateta. Esimerkiksi hakkereiden käyttäytyminen yritysten tietoliikenneverkkoja vastaan on lainvastaista toimintaa. Ajoittain on jopa esitetty väittämä, että tietoturvan hallintamekanismit korvaisivat ICT-alan eettisen säännöstön tulevaisuudessa. Ajan myötä löydetään uusia tietoturvaratkaisuja, joilla tähän toimintaan pystytään asianmukaisesti puuttumaan, mutta ihmisten omasta käyttäytymisestä riippuu, millaisiin ratkaisuihin loppujenlopuksi ajaudutaan. Tietoturvaratkaisuissa suunta on selvästi teknisten vaihtoehtojen rinnalla yhä voimakkaammin ihmisiin ja organisaatioihin liittyvissä kysymyksissä. Avainkysymykseksi tulee tietoturva-tietoisuusohjelma.

Tietoturvatietoisuudella haetaan ihmisten hyväksyntää tietoturvaratkaisuille ja ymmärrystä ratkaisujen olemassaolon välttämättömyydestä, jopa sille, että he ovat valmiita käyttä-mämään turvaratkaisuja. Kampanjoinnilla tässä yhteydessä pyritään tekemään tietoturva tärkeäksi, suosituksi osaksi organisaation toimintaa.

Eettiset säännöt ovat tärkeä yhteiskunnallisen keskustelun alue. Kansallisella tasolla niihin peilautuvat lait ja asetukset. Kuitenkin vaikutus on huomattavasti syvemmällä. Eettisen säännöstön syntyyn on vaikuttanut kyseisen valtion tai kansakunnan kulttuuri, uskonto, tavat, normit, historiatiedot, uskomukset ja vastaavat.

Tietoturvatutkijan kannalta tilanne on erittäin mielenkiintoinen. Niin tietoturvatietoisuus kuin eettiset säännöt ja normit sijoittuvat ihmisten tajunnassa niinsanotun hiljaisen tiedon alueelle. Eettiset säännöt ovat muokkautuneet vähitellen ihmisen ja kansakunnan muistiin ja sieltä heijastuviin toimiin. Nyt tietoturvatietoisuus yritetään saada osaksi tätä aluetta .

Tietotekniikkaan liittyvät omat eettiset säännöt ja niistä johdetut eettiset koodit. Lähivuosien suuri haaste on integroida niin tietotekniikan kuin tietoturvan eettisesti korrektit periaatteet osaksi ihmisten tajunnasta ohjautuvaa toimintaa.

Onko eettisen käsityksen vinoutuminen vaarana?

Onko tarjolla oleva uusi teknologia kuitenkin omiaan lisäämään tätä ongelmaa? Jos eettiset käsitykset muovautuvat väärään suuntaan, seuraa siitä myös tietoturvan hallinnalle uusia haasteita. Kysymys voi olla kilpajuoksusta myös sen kanssa, vinoutuuko eettinen käsityksemme. Vinoutuminen eettisten kysymysten alueella tarkoittaa sitä, että vain harvat ihmiset ymmärtävät, mistä etiikassa oikein on kyse. Ehkäpä etiikkaan pitäisi kiinnittää enemmän huomiota myös uusia teknisiä ratkaisuja suunniteltaessa. ICT-teknologia on vielä meille niin uusi asia, että sen käyttöön liittyvä eettinen säännöstö ja toimintatavat ovat vasta muovautumassa. Uusienkin eettisten

sääntöjen pohja on ikivanhoissa ihmiskunnan eettisissä käsityksissä. On varmistettava, että vanhoilla, hyviksi havaituilla säännöillä on jatkuvuutta, vaikka uutta teknologiaa onkin tullut ulottuvillemme lyhyessä ajassa.

Käsite etiikasta ja ”Computer ethics” –alueesta on laajasti väärinymmärretty tietokoneiden käyttäjien piirissä. Kyseessä ei ole tietokonerikollisuutteen liittyyvästä alueesta, jolla selvitetyistä rikoksista seuraa rangaistus. Termi ”Computer crime” pitää sisällään ne tapaukset, joissa tietokonetta on käytetty rikoksen tekovälineenä. Rikokset kuuluvat tekovälineestään riippumatta rikoslain piiriin. Etiikka sen sijaan on eräs arvostettu filosofian alue.

Liikenne – ja viestintäministeriö tehosti tietoturvaan liittyvää kansallista työtä käynnistämällä tammikuussa 2005 kaksi laajaa esitutkimushanketta, joista toinen liittyi mobiilimaailman tietoturvauhkiin ja toinen digi-tv:n tuomiin tietoturvauhkiin. Kummassakin hankkeessa oleellista oli palvelunkehittäjän näkökulma. Projektien loppuraportit julkaistiin kesäkuussa 2005. Nyt nämä LUOTI –ohjelmat ovat saamassa jatkoa, sillä syyskuussa julkistettiin uusi ohjelmahaku. Tässä LUOTI-ohjelmassa on tavoitteena käynnistää kolme merkittävää viihdepalveluhanketta syksyn 2005 aikana. Hankkeissa on tavoitteena tunnistaa ja kehittää tieto-turvallisuuden käsittelyn parhaita käytäntöjä käytännön palvelukehityshankkeissa.

Etiikka on tieteenalana vanha. Vain harvat ihmiset ymmärtävät sen korrektin roolin tietotekniikan – koneiden, ohjelmistojen, verkkojen ja ihmisten – keskellä. Karkeat tapaukset, joissa lain rikkomista on syytä epäillä, on hoidettu ja tullaan hoitamaan jatkossakin tuomioistuinmenettelyin. Uutena asiana kaikkien teletunnisteprosessien jälkeen esillä on jälleen erilaiset heikkoihin signaaleihin liittyvät prosessit. Kysymys kuuluu, voiko virheellistä tietoa käyttää esimerkiksi poliittisten päätösten tukena?

Jos haemme eettisistä säännöistä tukea tietoturvatyöhön, niin toivomme samalla voivamme toimia koko yhteiskunnan tienviittoina: tehokkaammasta ja laaduullisesti paremmasta yhteiskunnasta oikeudenmukaiseen ja arvoja kunnioittavaan yhteiskuntaan. ■

KUKA VASTAA HAASTEESEEN?

Tietoturvatietoisuuden parantamisessa tietoturva-ammattilaisilla, mutta myös tavallisilla kansalaisilla on tärkeä rooli.

Tietotekniikan ja erityisesti tietoturva-alan asiantuntijat ovat avainasemassa ICT-alan eettisten sääntöjen suhteen. Tietoturva-asiantuntijat ymmärtävät parhaiten tiedon ja tietoaineistojen luottamuksellisuuden merkityksen. Samoin heille on tärkeää turvata henkilötiedot ja yksityisyyteen liittyvät asiat. Heidän on siis pystyttävä toimimaan esimerkkinä myös eettisesti. Tämä on luonnollista, koska rakennettaessa tietoturvaratkaisuja on puntaroitava jatkuvasti sitä, mikä on oikein ja mikä väärin. Monessa tapauksessa on vaikea tehdä päätös – teknologisten kokonaisuuksien hahmottaminen eettisesti on haastavaa. Tunnettu kansainvälinen tietoturva-ammattilaisten sertifiointia tekevä järjestö (ISC)2 (International Information System Security Certification Consortium) on muunmuassa määritellyt tietoturva-ammattilaisten eettisen säännöstön (Code of Ethics), jonka hyväksymistä järjestö edellyttää tutkinnoissaan (esim. CISSP). Toinen esimerkki etiikkatyöstä on tietojenkäsittelyammattilaisten järjestö Computer Professionals for Social Responsibility (CPSR). Suomessa tietotekniikan eettisista koodeista ja niiden kehittämisestä kantaa vastuun Tietotekniikan liitto, jonka sivustolta oma koodistomme on saatavissa.

On syytä korostaa, että asiallinen ja oikeudenmukainen ammattilaisten toiminta on koko yhteiskuntamme peruspilari. Jos siihen saadaan lisää uskottavuutta erilaisilla tutkinnoilla ja sertifikaateilla, niin se vahvistaa koko rakennetta.

Vaikka vapaat tietoliikenneverkot, epäeettiset pelit, hakkeriohjelmistot, tieto haavoittuvaisuuksista, digitaalisen sisällön levitystekniikat jne. mahdollistavat nykypäivänä jopa arkipäiväiseksi luokiteltavan epäeettisen toiminnan, on meidän ymmärrettävä, että emme hyväksy tätä toimintaa emmekä ole siinä osallisena. Erityisen tärkeää on, että vanhemmat huolehtivat lastensa eettisestä kasvatuksesta, kun tarjolla on laaja valikoima epäeettisiä teknisiä apuneuvoja epäeettiseen käyttäytymiseen. Vanhempien on tärkeätä tiedostaa, mikä on nykypäivänä eri tavalla kuin heidän omassa lapsuudessaan ja nuoruudessaan. Kuinka paljon on sallittua pelata väkivaltaisia tietokonepelejä? Lapsen ei ole hyvä ottaa mallia toveristaan, joka kehuskelee imuroineensa ilmaiseksi suuret määrät elokuvia, musiikkia ja pelejä tai ilmoittaa käyttäneensä hyväkseen tietoturvattomasti kehitettyä sähköistä palvelua. ■

AMMATTINA HAKKERI

Hakkerointiin liittyy klassisesti mielikuva jostain hämäräperäisestä, tai vähintäänkin salamyhkäisestä toiminnasta, jota harjoitetaan yön pimeinä tunteina pizzalaatikoiden ja coca colan ympäröimänä. Hakkeroinniksi ymmärrettävää toimintaa harjoittaa kuitenkin usea yritys päätoimialanaan. Suomessakin toimii ammattihakkereita, joiden työnä on tunkeutua yritysten järjestelmiin. Toki se tehdään näiden omasta pyynnöstä. Yleensä toimintaa kutsutaankin hakkeroinnin sijaan esimerkiksi hyökkäystestaukseksi tai tietoturva-auditoinniksi.

Tiina Kaksonen

Puhelinhaastattelu 28-vuotiaan Joakim Sandströmin alkaa tyttären itkun säestämänä. Perjantaipäivää isä viettää kotona. Perheelläkin on sijansa kiireisen yrittäjän arjessa. Nuoresta iästään huolimatta Sandström on ehtinyt tehdä jo kymmenen vuoden uran ohjelmisto- ja tietoturva-alalla. Suoraan lukiosta ohjelmointitöihin rekrytoitu mies on ollut monessa mukana. Elämä johdatteli hänet Tanskaan ohjelmointiprojektitöihin. Vuoden 2005 lähestyessä loppuaan Sandström on aloittanut tanskalaisen nSense-yrityksen sisaryhtiön pyörittämisen Suomessa. nSensellä on tällä hetkellä neljä työntekijää Suomessa ja 20 Tanskassa emoyhtiö Ezenta A/S mukaan lukien. Liiketoimintaa on Tanskassa, Suomessa ja Belgiassa.

nSensen liiketoiminnan perusidea on pyrkimys tunkeutua erilaisten yritysten tietojärjestelmiin niiden www-sovellusten kautta. Yritys siis tarjoaa palvelua sovellustietoturvatestaukseen. Keskeinen osa palvelukonseptia on tarjota asiakkaille

... AMMATTINA HAKKERI

tietoturva-auditointeja projektipohjaisesti. Yrityksellä on itse kehittämänsä testaustyökalu tähän tarkoitukseen, jolla suuri osa testausta voidaan tehdä automatisoidusti. Käytännössä kuitenkin tällä toimialueella osa työstä joudutaan aina tekemään manuaalisesti. Yrityksen kautta on myös mahdollista hankkia haavoittuvuusskannausta omalle tuotteelle. Asiakkaina on muun muassa pankkeja ja finanssiyhtiöitä, sekä joukko sovelluksia kehittäviä ohjelmistotaloja, jotka käyttävät yrityksen tuotetta osana tuotekehitysprosessiaan. Lisäksi yritys tarjoaa koulutuspalvelua esimerkiksi tietoturvalliseen ohjelmointiin.

Ammattilaiset ammattilaisia vastaan

Tietoturvatestaukseen erikoistuneena nSensen kaltainen yritys taistelee yhä voimakkaampaa vihollista vastaan. Sandström toteaa, että tietoverkoissa ammattimaisen rikollisuuden osuus sekä huijausten määrä on kasvamassa. “Uhkakuva on globaali: 10 dollaria on eri arvoinen ihmisille eri puolilla maailmaa.”, Sandström kuvailee ongelman luonnetta.

Esimerkiksi erilaisia www-pohjaisia palveluita tarjoavien yritysten tietoturvataso on hyvin kirjavaa. Toisille tietoturvasta huolehtiminen on itsestään selvää, toiset katsovat että ovat tähän saakka pärjänneet hyvin ilmankin, joten näin asian täytyy olla myös jatkossa.

“Mielestäni on hämmästyttävää, miten suuri ero fyysisessä liikkeessä ja internetissä toimivan kaupankäynnin välillä tänä päivänä on. Halutessasi perustaa tavallisen, fyysisesti toimivan yrityksen sinun täytyy hankkia toiminnalle lukuisia erilaisia lupia, vakuutuksia ja auditointeja lakisääteisesti vaikkapa palovahinkojen tai vastaavien torjumiseksi. Sen sijaan halutessasi perustaa liikkeen internetiin mikään viranomainen ei säätele, millainen tietoturvatasosi tulee olla.”, Sandström toteaa.

Asiaan on kuitenkin tulossa muutoksia lähiaikoina. Esimerkiksi Suomessa otetaan 1.1.2006 käyttöön uusi PCI-standardi (Payment Card Industry Data Security Standard), joka on Visan ja Mastercardin luoma kansainvälinen tietoturvastandardi. Se ohjaa tietoverkoissa tapahtuvaa maksukorttitapahtumien vastaanottamista, käsittelyä, tallentamista ja välittämistä. Samalla vaatimukset tietoturvatestaukselle kasvavat. Tanskassa lainsäädännössä ollaan jo nyt Suomea edellä, ja säätely on tiukempaa.

Ammattinsa puolesta tällaisten yritysten työntekijöiden on huolehdittava korkeiden eettisten periaatteiden ja salassapitovelvollisuuksien noudattamisesta. Esimerkiksi Sandströmillä on NATO:n salaisuusluokitus, jonka Tanskan tiedustelupalvelu on hänelle myöntämä.

Riskikartoitukseen on monta lähtökohtaa

Täysin suomalainen tietoturvatestaustyökaluja valmistava yritys Codenomicon Oy tekee työkaluja pitkälle automatisoituun tietoturvatestaukseen. Yrityksen päätoimipaikka on Oulussa ja lisäksi toimintaa harjoitetaan Yhdysvalloissa, Kalifornian piilaaksossa toimivassa sivukonttorissa. Yritys tekee työkaluja standardeihin verkkorajapintoihin. Työkaluilla voidaan testata ohjelmistojen näkymätöntä infrastruktuuria, joiden päällä esimerkiksi www-sovellukset toimivat. Näkökulma testauksen käytännön toteuttamiseen eroaa siis nSensen periaatteista siinä, että nSense testaa www:n loppukäyttäjällekin näkyviä rajapintoja, kun taas Codenomiconin työkaluilla testataan syvempää infrastruktuuria myös muiden kuin www-sovellusten alla.

Käytännössä sekä nSensen, että Codenomiconin tekemä työ on riskikartoitusta ja uhkakuvien todentamista Yritysten tehtävänä on todeta, että asiat ovat hyvin tai huonosti. Hyvälle tietoturvatestaukselle on ominaista, että ongelmia voidaan löytää epätodennäköisistäkin paikoista. Esimerkiksi Codenomiconin tuotteilla voidaan vielä tänäkin päivänä löytää virheitä joistakin IPv4-protokollapinoista huolimatta siitä, että kyseinen protokolla on ollut laajasti käytössä jo 1970-luvun lopulta saakka ja on mm. tiukkojen tietoturva-auditointien ansiosta pääsääntöisesti erittäin luotettava.

Tavoitteena vaikuttaminen ohjelmistojen tietoturvan kokonaistasoon

Yleiseen ohjelmistojen tietoturvatasoon vaikuttaminen on Codenomiconin tavoitteena. “Tarjoamalla ja rakentamalla työkaluja käytettäväksi osana uusien protokollapinojen toteutusta ja suunnittelua - oli kyseessä sitten IPv6, HTTP, jokin reititys tai vaikka jokin VoIP-protokolla - uskon vahvasti että pystymme tuottamaan työkaluja jotka eivät pelkästään

eliminoi vuosikymmenten kypsymisprosessia vaan ovat käyttökelpoisia koko protokollan elinkaaren ajan.”, toteaa yrityksen tuotepäällikkö Mikko Varpiola.

Kysymykseen, tunteeko Varpiola olevansa hakkeri, hän vastaa: “Koen henkilökohtaisesti valtavan motivoivaksi toimia osana tiimiä, jolla tuotamme tällaisia työkaluja. Kutsuisinko itseäni siltikään hakkeriksi - en. Hakkeri-sana on nykyään värittynyt tarkoittamaan ihmisten mielissä mitä ihmeellisimpiä asioita enkä koe mitään yhteistä introvertin finninaamaisen pahanhajuisen rasvaletin kanssa joka aamuneljältä vääntää tiukkaa innerlooppia kokakolan ja pizzalaatikon voimalla. Sen sijaan koen omalta osaltani tarjoavani työni tuloksena keinoja rakentaa turvallisempia ohjelmistoja ja siltä osin kuin keinoja ei ole - keksimään niitä - ennakkoluulottomasti. Ja mikäli tämä täyttää hakkerin määritelmän - otan mielelläni kunnian vastaan.”

Mikko Varpiola.

Joakim Sandström.

VÄENÖ

Tietoturvaongelma

Tietoliikennetekniikkaa on nykyään käytössä lähes kaikilla suomalaisilla: kotonaan, työpaikallaan ja jopa mukana taskussa. Tietoturvaa sen sijaan ei näytä olevan kellään ja sen on eräs hyvä ystäväni joutunut viime vuosina karvaasti kokemaan.

Tuo ystäväni on ihan tavallinen, ahkera ja kunnollinen suomalainen. Hänen tapansa ja kulutustottumuksensa ovat ihan normaalit eli hän pitää kunnia-asianaan kuluttaa mahdollisimman vähän säästääkseen ympäristöä ja tulevien polvien elämänedellytyksiä.

Ystäväni ei ole kiinnostunut rahasta kuten eivät useimmat muutkaan suomalaiset. Esimerkiksi veikkausta hän ei ole harrastanut koskaan, koska ei arvosta rahaa eikä kaipaa jännitystä, sillä hänen elämänsä on muutenkin riittävän jännittävää.

Toki ystäväni käyttää rahaa, koska se on välttämätöntä tänä aikana. Hänkin tarvitsee esimerkiksi ruokaa, vaatteita, sähköä ja vettä. Tavalliseen tapaan hän maksaa laskunsa verkkopankissa Internetin kautta. Tästä laskunmaksusta on sitten seurannut tuo mainitsemani tietoturvaongelma.

Jotenkin ystäväni pankkitilinnumero oli, ilmeisesti Internetin kautta, vuotanut ilkeämielisten ihmisten käyttöön. Tilinumero on levitetty varmaankin tuhansien ihmisten tietoon. Jo parin vuoden ajan ihmiset ovat kiusaamistarkoituksessa laittaneet ystäväni tilinnumeron veikkaus- ja lottokuponkeihinsa. Veikkausvoitot maksetaan kupongeissa ilmoitetuille tilinnumeroille. Nykyisenä Online-veikkauksen aikana ilkivallantekijöitä on mahdotonta saada kiinni, kun kuponkeihin ei tarvita veikkaajan nimeä eikä muita henkilötietoja, pelkkä tilinumero riittää. Niinpä joka viikko ystäväni tilille on kertynyt veikkaus- ja lottovoittoja, toisinaan jopa kymmeniä tuhansia euroja viikossa.

Ystäväni on ollut aivan epätoivoinen jatkuvasti tililleen karttuvan rahantulon takia. Hän ei pysty keksimään rahalle mitään järkevää käyttöä. Neuvoin häntä taannoin laittamaan rahaa erilaisiin hyväntekeväisyystarkoituksiin. Aluksi hän oli helpottunut asiasta, mutta helpotusta ei kestänyt kauan. Erilaisia hyväntekeväisyystarkoituksia ja tarpeita on niin paljon, että ystäväni väsyi pohtimaan, mitkä olisivat kaikkein hyödyllisimpiä rahankäyttökohteita.

Kerran ystäväni vaihtoi neuvostani tilinsä numeroa. Tilanne korjaantuikin vähäksi aikaa, jopa pariksi kuukaudeksi, mutta sitten tuo tilinnumeron vaihto paljastui ja rahavirta uudelle tilille alkoi. Jatkuessaan pitkään tilanne on käynyt aina vain uuvuttavammaksi. Ystäväni on joutunut käymään monta kertaa terapiassa tämän ilkivallan takia.

Nyt ongelma näyttää ainakin tilapäisesti taas ratkaistulta. Neuvoin ystävääni ohjaamaan tililleen tulevat veikkausvoitot suoraan kaupunginvaltuustomme käyttöön. Olemme valinneet valtuustoon ihmiset varta vasten päättämään yhteisistä asioistamme ja yhteisten rahojemme käytöstä. Suurtenkaan rahasummien kuluttaminen viisaasti ja oikeudenmukaisesti ei ole ainakaan vielä tuottanut kaupunginvaltuustoille minkäänlaisia ongelmia.

- Väinö Väistö

HOX!

TEHKÄÄ JOKU TÄHÄN MEDIAKARHUJEN MAINOS!

JOTAIN VISUAALISESTA JA VERBAALISESTA AKROBATIASTA:

WWW-SIVUT, GRAAFINEN SUUNNITTELU, MARKKINOINTIVIESTINNÄN

SUUNNITTELU, JNE. KYLLÄ TE TIJÄTTE.

JA OIS VÄHÄN KIIRE! LEHTI ON MENOSSA PAINOON!

- PASI

PS. MUISTAKAA MAINITA ETTÄ MEDIAKARHUT ON

TÄMÄNKIN LEHDEN TAKANA.

POSTI POSTEN SUOMI FINLAND

Tilaa Ylivuoto ilmaiseksi!

Ilmoittamalla meille osoitteesi varmistat, että saat Ylivuodon seuraavat numerot painotuoreena heti julkaisun jälkeen.

Tehdään tietoturvasta yhteinen asia!

http://www.ylivuoto.fi/palaute/

ISSN 1796-0835