Tietoturva on meidän jokaisen asia

Vuonna 1992 Tim Berners-Leen esittelemän HTML-kielen ja Web-selauksen myötä siirryttiin WWW-aikakauteen. Samalla muuttuivat myös organisaatioiden ja järjestelmien tietoturvavaatimukset. Enää ei verkkomaailmassa oltukaan omassa suljetussa ja turvallisessa lintukodossa, vaan hypättiin kuvaannollisesti pikkukylästä suurkaupunkiin. Avoin verkko tarjoaa paljon uusia asioita, niin hyvää kuin pahaakin.

Tietoturvan merkitys organisaatioissa ei ole vähenemässä, päinvastoin se kasvaa jatkuvasti. Puutteellinen tietoturva organisaatiossa johtaa ongelmiin, joista saattaa seurauksina olla taloudellisia tappioita, uskottavuuden tai luottamuksen menetystä.

Mitä tietoturva on? On ehkä helpompaa lähteä liikkeelle siitä, mitä tietoturva ei ole. Tietoturva ei ole ohjelma, joka voidaan asentaa tietokoneeseen, jonka jälkeen kaikki uhkatekijät on huomioitu, ja sen jälkeen voidaan olla turvallisin mielin. Tietoturva ei ole teknologiaa. Tietoturva on osa organisaation jokaisen henkilön toimintaa. Tietoturva merkitsee jatkuvaa opiskelua, organisaation henkilöstön koulutusta ja opastusta, tietoturvan huomiointia ohjelmistoprojekteissa heti projektin alusta lähtien, ja jatkuvaa hereilläoloa.

On tiedettävä, miltä ja keiltä halutaan suojautua, ja mitä halutaan suojata. On kyettävä suojaamaan laitteet, ohjelmistot ja resurssit, tiedon kuljetusmedia, ja itse tieto luvattomalta käytöltä. Luvattoman käytön voivat mahdollistaa mm. virukset, laitteiden ja ohjelmistojen tietoturva-aukkoja sekä menettelyjen porsaanreikiä hyödyntävät hyökkäykset, käyttäjää ohjailevat hyökkäykset, sekä huijaukset. Luvattomia käyttäjiä voivat olla mm. hakkerit, vakoojat, ammattirikolliset, sekä joskus organisaation oma henkilökunta.

Tietoturva yleisesti ottaa CIA-akronyymin (Confidentiality, Integrity, Availability) mukaan kantaa tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen. Luottamuksellisuuden voidaan ajatella tarkoittavan sitä, että tietoa pystyy hyödyntämään vain tahot, joilla on siihen oikeus. Eheydellä tarkoitetaan, että tieto on virheetöntä, ts. se ei ole muuttunut tietoa siirrettäessä tai käsiteltäessä. Saatavuudella tarkoitetaan, että tieto on tarvittaessa saatavissa niille, joilla on oikeudet ko. tietoon. Näitä peruskäsitteitä hyödyntävät kaikki, jotka ovat tietoturvan kanssa tekemisissä.

Tietoturvaan on useita näkökulmia riippuen tarpeesta, ja tietoturva-termillä on usein eri merkitys eri ihmisiltä kysyttäessä. Tässä numerossa pyrimme tarjoamaan lukijalle erilaisia näkökulmia tietoturvaan lähinnä IT-ammattilaisen silmin. Antoisia lukuhetkiä artikkelien parissa!

Simo Vuorinen,
Sytyke ry:n hallituksen jäsen
TietoEnator

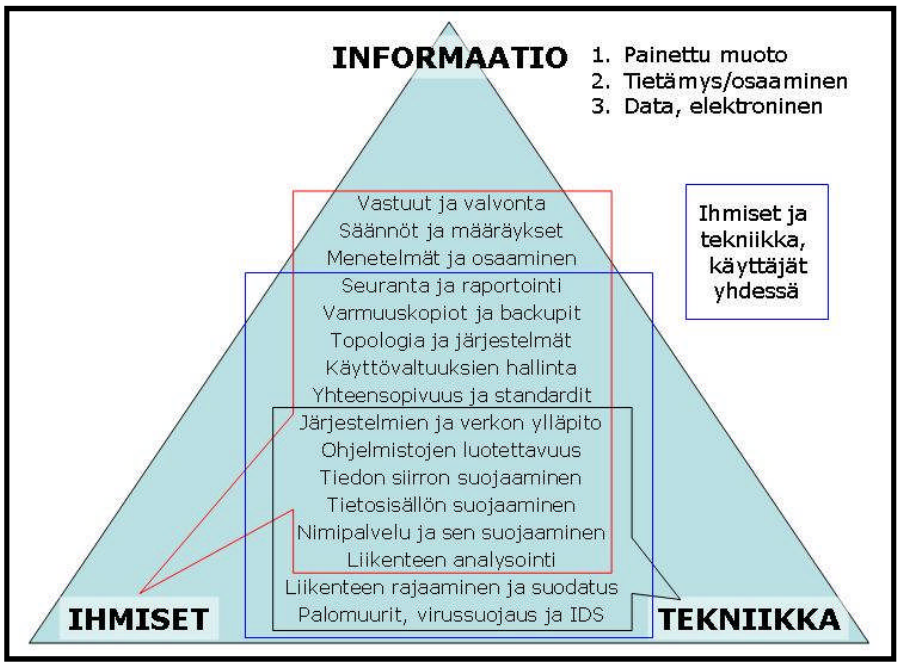
Tietoturvallisuus ja tietojärjestelmät

Arto Kangas,
Elisa Tietoturvapalvelut

Tietojärjestelmien toimivuus sekä sovellusten ja järjestelmien luotettavuus nousevat jatkuvasti yhä merkittävämmäksi tekijäksi organisaatioiden toiminnassa. Ylläpitohenkilöstö sekä heidän suorittamansa työ on muodostumassa myös korvaamattomaksi organisaatioiden jatkuvuuden kannalta tarkasteltaessa.

Kokonaisuudessaan tietoturvallisuus tulisi huomioida jokaisessa organisaatiossa ainakin seuraavan kolmen näkökulman valossa:

- Hallinnollinen tietoturvallisuus, säännöt ja ohjeet
- Ihmisten käyttäytyminen ja toiminta sekä normaali- että poikkeustilanteissa
- Tekniset tietoturvatoimenpiteet sekä valmiudet ja resurssit

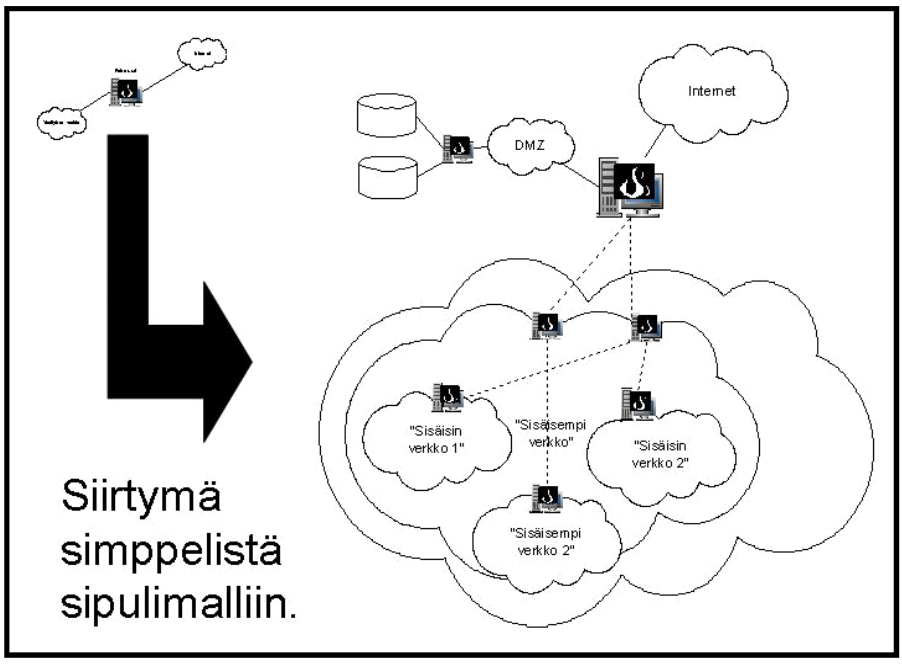


Kuva 1. Hallittaessa informaatiota tulisi pystyä riittävällä laajuudella huomioimaan sekä hallinnan kohde että hallintavälineet, käyttäjistä puhumattakaan. Kuvassa mainituista merkittävimmän riskin tuottavat pohjimmiltaan käyttäjät (ns. inhimillinen osuus). Inhimillinen vaikutus on suuri myös käsittelyvälineiden suunnittelijoilla, laatijoilla sekä em. käyttäjät. Yksi näkökulma tulee myös informaation tuottajien taholta.

On jotenkin käsittämätöntä, että tyypillisesti osataan todeta jonkin printatun materiaalin olevan luottamuksellista ja joskus jotkut ihmiset osaavat pitää suunsakin oikeassa paikassa pienemmällä – esimerkiksi edes kuiskauksia käyttäen – mutta luottamuksellisia asioita kuitenkin lähetetään julkisessa avoimessa internetissä tavallisella SMTP-sähköpostilla, jolla tyypillisesti on monien mielestä vain postikorttitasoinen luottamuksellisuustaso. Lisäksi luvattoman moni henkilö antaa perheenjäsentensä pelata ja puuhata samoilla välineillä, joilla a) käsitellään työasioita ja b) jotka vielä pahempaa – sisältävät työhön liittyviä tiedostoja ja dokumentteja, mutta luottamuksellisuutta ei oivalleta tarpeelliseksi huomioida.

Puutteelliset ohjeet ja menetelmäkuvaukset aiheuttavat tyypillisesti ”hätätilan” pienestäkin poikkeamasta normaalitilanteisiin verrattuna. Asioiden monitahoisuus ruokkii itsessään myös tarpeetonta ristiriitojen esiintymistä, mikäli yhtenäinen linjaus organisaation toimintatavoista on jätetty tekemättä.

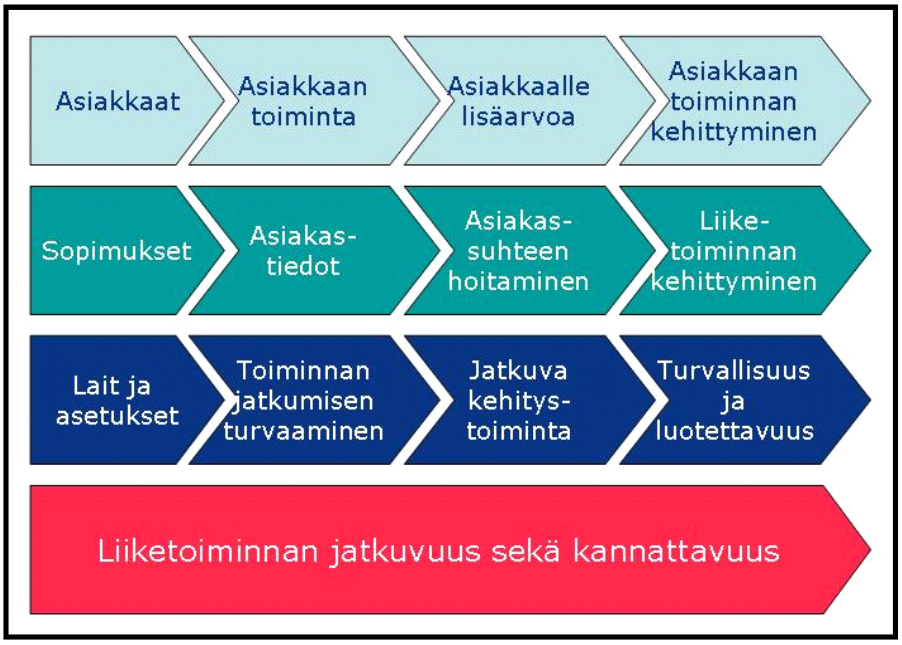
Paraskaan ohje vain paperilla ollessaan ei tuota kattavaa vaikutusta inhimilliseen käyttäytymiseen. Koulutuksella, valmennuksella sekä perehdytyksellä ja tarvittaessa asioiden kertaamisella voidaan vaikuttaa ihmisten osaamisen kasvamiseen sekä asioiden prosessissa huomioimiseen. Kertary-



Kuva 2. Oheisessa kuvassa on kaksi topologista ääripäätä kuvattuna. Henkilökohtaiset tai työasemakohtaiset palomuurit siitä puuttuvat, mutta trendi on muuttumassa organisaatioissa entistä monikerroksi- sss s ss sssss ssss sss s sss sssss ss

säys on tietysti parempi kuin ei mitään, mutta henkilöstön valmennuksessa tulisi huomioida jatkuvuus.

Teknisten toimenpiteiden huomioiminen on samalla sekä erittäin helppoa että erittäin haasteellista. On helppoa todeta hallinnollisesti päätäntävaltaa käyttäen, että palomuuri tarvitaan ja mitään luvatonta liikennettä ei sallita. Vastaavasti voidaan päättää virustorjunta pakolliseksi. Ongelmat tulevat vasta näiden toimenpiteiden seurauksena olevista ylläpitovelvoitteista. Hallinnollinen päätös on helppo toteuttaa – ehkä kertaluonteinen asennus ja ympäristöön implementointikin – käytäntö kuitenkin edellyttää jatkuvuutta. Korjaussarjojen asentaminen ns. ”pätsääminen” on osaltaan arkea, mutta se ei kuitenkaan saisi olla automaattisiin prosesseihin nojaava, vaan jokaisen korjaustoimen tarkoitus ja luotettavuus pitäisi pystyä todentamaan.



Kuva 3. Prosesseissa tulisi huomioida riittävällä laajuudella tavoitetila ja purkaa asiat ikään kuin loppupäästä alkaen, jotta pystyttäisiin pääsemään paremmin haluttuun lopputulokseen. Jatkuvuus ja kannattavuus ovat liiketoiminnan kantavia perusasioita.

Teknisorientoitunut ICT-/IT-/ATK-väki on herkkää muutoksissa ja ilmeisesti kaupallisen kilpailun kireys on vaikuttanut välillisesti siihen, että kaikki mikä ei ole enää aivan uutta mielletään ajastaan jääneeksi ja halutaan hylätä vähemmän tarpeelliseksi kuviteltuna. Virustorjunnasta puhutaan jatkuvasti, spämmi on kasvava puheenaihe, verkkomadot loistavat lehtien palstamillimetreillä laskettavassa huomioarvossa alan kärjessä – palomuurista puhutaan harvemmin, vaikka hakkereista puhutaankin. Palomuuri on pohjimmiltaan kohtuullisen yksinkertainen toiminnaltaan – otetaan kantaa sovituilla määreillä siihen mikä on sallittua ja mikä ei ja pyritään varmistamaan, ettei ainakaan se ”ei-toivottu” pääse läpi.

Tarve ”sipulimalliin” on ollut jatkuvasti, mutta vasta järjestelmien yli rajojen toiminnallisuus on pakottanut huomioimaan myös sisäisessä organisaatiossa rajapintojen ja segmenttien välisen viestinnän koordinoimiseen.

Palomuuri on siis edelleen välttämätön ja lähtökohtaisesti vähintään yhtä pakollinen perusväline kuin virustorjunta. Käytännön tietoturvallisuutta ei mitata pelkällä julkisuudella tai keskustelun määrällä. Paremminkin pitäisi tehdä johtopäätöksiä sen pohjalta, että mitä enemmän julkista keskustelua sitä suuremmat ongelmat todellisuudessa ovat taustalla. Luonnollisesti kehitystä tapahtuu palomuurien ja virustorjuntojen sekä tunnistamisen alueilla kuten yhtälailla myös turvallisten yhteyksien ja salausaiheiden parissa.

IDS:t eli tunkeutumisen havaitsemisjärjestelmät (Intrusion Detection Systems) ovat hieman polkeneet toteutusten osalta paikallaan. Tekniikkaa kyllä löytyy kohtuullisesti, mutta niiden todellinen pullonkaula on henkilöiden resurssointi. Ohjelmistolla ei ainakaan vielä löydy riittävää ”vainoharhaa” arvioimaan saman tasoisista hälytyksistä sitä, kumpi on mahdollisesti tahallinen haitantekoyritys ja kumpi taas jotain satunnaista ”eksynyttä datavirtaa”.

Palveluita rakennettaessa tulisi osata riittävästi asiakkaan tarvemaailmaa ja ymmärtää asiakkaan toimintaan etuja tuottavia asioita. Vastaavasti sopimuspuolella tulisi sen sijaan, että pyritään sulkemaan ja rajoittamaan mahdollisimman paljon esimerkiksi luottamuksellisuuden säilymiseen kohdistuvia riskejä ja uhkia, yrittää ymmärtää kumppanuuksien ja yhteistyön tarkoitus pitkäjänteiseen liiketoiminnan kehitykseen ja luoda sopimuksia tukemaan tätä kehitystä. Mikäli ympäristö olisi turvallinen ja luotettava, niin lakeja ja asetuksia ei tarvittaisi. Jos liiketoiminta tapahtuisi absoluuttisen jatkuvan lineaarisen kasvun mukaan, kannattavuudestakaan ei tarvitsisi huolehtia.

Kirjoittaja Arto Kangas on Tietoturva ry:n hallituksen puheenjohtaja ja toimii päätyössään Elisalla tietoturvakonsulttina. Tietoturva ry on Tietotekniikan liitto ry:n teemayhdistys, jossa on nykyisin jo runsaat 650 jäsentä. (www.tietoturva.org)

Tietoturva - Finnish Information Security Association ry (FISA) on Tietotekniikan liiton jäsenyhdistys, joka toimii valtakunnallisesti. Yhdistyksen tarkoituksena on mm. tukea jäsenten pyrkimyksiä kehittää ja ylläpitää tietoturvatoiminnan ammattitaitoa ja laatua, edistää tietoturvallisuutta ja hyvien tietoturvatapojen noudattamista tietoturvallisuuden kaikilla eri osa-alueilla.

7 ohjetta kotikoneen tietoturvaan

Tomi Tuominen

1. Käytä henkilökohtaista palomuuria. (esim. F-Secure Client Security)
2. Käytä ajantasalla olevaa virustentorjunta-ohjemaa
3. Käytä hyviä salasanoja (väh. 10 merkkiä, sisältää erikoismerkkejä ja numeroita eikä löydy minkään kielen sanakirjasta)
4. Älä ikinä avaa "tuplapäätteisiä" liitetiedostoja (esim. ohje.doc.exe)
5. Älä avaa liitetiedostoja, joiden pääte on kummallinen (esim. ohje.pif, ohje.shs)
6. Lue sähköpostit "plain text" -muotoisena. Tämä tarkoittaa sitä, että esim. HTML/RTF -muotoiset viestit muunnetaan "pelkäksi tekstiksi".
7. Älä asenna koneeseen ohjelmia, joiden alkuperästä ei ole tietoa

Tomi Tuominen

Tietokoneviirusten kehityskaaria

Ilkka Keso,
Osuuspankkikeskus

Tietokonevirusten aika alkaa jostakin 1980-luvun alusta. Internetin edeltäjään Arpanettiin kaavailtiin matotyyppisiä päivityksiä, ja kirjassa "Shockwave rider" kuvattiin hyökkääviä matoja. Professori Fred Cohen sanoi osaavansa tehdä viruksia suurkoneympäristöön, jolloin NSA vaati häntä vaikenemaan niihin liittyvistä yksityiskohdista siihen saakka, kunnes USA:n suurkoneet on näiltä Madoilta suojattu. Cohen vaikenee edelleen...

Suuren yleisön tietoon virukset tulivat 1987, kun paljastui, että pakistanilaiset tietokonekauppiaat olivat merkanneet myymiään levykkeitä Brain-viruksella, ja tuo käynnistysvirus oli ehtinyt levitä jo yli 300 000:een mikroon. Käynnistys-alueen virus levisi suunnilleen ihmisen kävelyvauhtia, tyypillisesti levyke oli vietävä mikrosta toiseen. 1990-luvun alussa tavatuista viruksista noin 80% oli käynnistysviruksia. Aikaansa edellä oleva, Internetissä liikkunut Morrisin mato aiheutti unix-piireissä säpinää 1988.

Tietokoneita alettiin vähitellen verkottaa, ja Dos käyttöjärjestelmää oli monella tavoin hyödynnettynä työasaemissa, Windows-ympäristön alustana ja jopa Os/2 palvelinten ikkunassa. Edellistä nopeammin leviäville tiedostoviruksille tarjoutui suotuisat olosuhteet, ja niiden tunnistamisen vaikeaksi tekevät mutaatiokoneistot edesauttoivat tiedostovirusten voittokulkua.

90-luvun puolivälissä julkaistu Windows 95 mullisti virusmaailmaa monin tavoin. Dokumentteihin haudattiin makroja, ja makroista tehtiin uusia viruksia. Yhtäkkiä data lakkasi olemasta passiivista ja turvallista siirrettävää. Kesti ainakin kolme vuotta, ennen kuin datan käsittelyyn saatiin luoduksi järkeviä toimintoja, kuten ohjelmia, jotka tappavat siirrettävästä datasta erotuksetta kaikki siihen haudatut makrot.

Keväällä 1999 ilmaantui sitten Melissa, eräänlainen viruksen ja madon risteytys. Matona Melissa pyrki tartuttamaan toisia tietokoneita, ja aktiivisin menetelmin, kun tyypillinen virus pyrkii tartuttamaan toisia tiedostoja hyvin vaivihkaisesti isäntäohjelman päästessä suoritukseen. Melissa lisääntyi myös viruksen tapaan tartuttaen mikrojen sisällä tiedostoja. Pahinta tässä madossa kuitenkin oli uudenlainen tuhomekanismi: Melissa varasti mikrosta asiakirjoja ja siirteli tietoa koneen käyttäjän ulottumattomiin.

Dos-mikrot enää muodostaneet suuria populaatioita, joissa laajat virustartunnat pystyisivät leviämään. Ollakseen tehokas viruksen kannatti hallita monia eri versioita Windowseis-

Virusten valtakaudet

Käynnistysvirukset	1987 - 1991
Tiedostovirukset	1991 - 1995
Makrovirukset	1995 - 1999
Sähköpostimadot	1999 - 2003
Verkkomadot	2003 -

Virusten alayypit maaliskuu 1995

Käynnistysvirus	(Boot virus)
Kumppanivirus	(Companion/Spawning virus)
Panssaroitu virus	(Armored virus)
Piilovirus	(Stealth virus)
Kuljetinvirus	(Dropper virus)
Monitoiminen virus	(Multi-partite virus)
Monihahmoinen virus	(Polymorphic virus)
Retrovirus	(Anti-antivirus)
Nopea tartuttaja	(Fast infector)
Hidas tartuttaja	(Slow infector)
Rakennussarjavirus	(Construction set virus)
Salasanan varastaja	(Password stealer)
Mutaatiokonevirus	(MtE/DAME/TPE/DSME virus)
Linkkivirus	(Link/Dir virus)
Viipalevirus	(Slice virus)
Modulivirus	(Modular virus)
Binäärivirus	(Binary virus)
Suojatun tilan virus	(Protected mode virus)
Sorsavirus	(Source code virus)
BIOS virus	(Flash BIOS virus)
UNIX virus	(UNIX virus)
Windows(3) virus	(Windows virus)
Windows NT virus	(Windows NT virus)

CIH-Virusvahingot 26.4.1999

Kiina	360 000
Etelä-Korea	250 000
Turkki	240 000
Intia	100 000
Venäjä	100 000
Thaimaa	30 000
Bangladesh	30 000
USA	10 000
Indonesia	10 000
Israel	10 000
Suomi	600
Viro	500
Englanti	400
Ranska	300
Espanja	300
Sri Lanka	250
Singapore	200
Saksa	100
Japani	50
Australia	50

Kokonaisvahingot koko maailmassa olivat 2 000 000 mikroa, niistä noin 400 000 korjauskelvottomina. Viruksen kirjoittaja Chen Ing-Hau [CIH] on nuori tietokoneinsinööri, ja hän tunsi joitakin BIOS-päivityskoodeja, joiden avulla BIOS saatiin sekoamaan ja tietokoneen emolevy käyttökelvottomaksi.

Virus oli kosto pelifirmoille ja se levisi Taiwanin lähistöllä tehtyjen piraattipeliromppujen mukana. Virus laukesi myös vuonna1998, ja jo tuolloin länsimaisittain toimivat yritykset suojattiin tältä virukselta. ”Kolmannessa maailmassa” oli kuitenkin tapana käyttää huonompaakin, jostakin kopioitua vanhaa virustorjuntaohjelmistoa, johon valmistajan virustunnistepäivityksiä ei ymmärrettävästi ollut saatavissa.

ta. Madoista, makroista ja skripteistä huolimatta jotkut tiedostoviruksetkin pystyivät yhä yllättämään. Keväällä 1999 laukesi CIH tuhoten tiedot noin kahdesta miljoonasta tietokoneesta maissa, joissa ei ohjelmista ole ollut tapana maksaa täyttä hintaa (katso erillistä CIH-artikkelia).

Kymmenisen vuotta sitten työasemat, jotka olivat eniten viruksille alttiita, olivat verkottuneita Dos-mikroja. Tällä hetkellä suurin riski kohdistuu ympäristöön, jossa käytetään Intel-pohjaista emolevyä, Windows-käyttöjärjestelmää, Office-työkaluohjelmistoja, Outlook-sähköpostia ja Exchange-selainta. Riskiä edelleen lisäävät laaja kontaktipinta ulkomaailmaan ja Internettiin, erilaisten ohjelmaversioiden käyttö rinnakkain (esim. Windows 98, NT4 ja 2000), työasemien kiintolevyjen jako verkon resursseiksi, kannettavien mikrojen ja etätyöskentelyn yleistyminen sekä paikallisen tuen ulkoistaminen ja hallinnon hajauttaminen. Sähköpostiin läheisesti liittyviä riskejä ovat lisäksi laajat jakelulistat, liitetiedostojen suosiminen sekä makrojen, skriptien ja active-x:n rajoittamaton käytettävyys.

Nopeasti ja massiivisesti sähköpostissa leviävät madot, kuten Melissa, ExploreZip ja LoveLetter testaavat virussuojausten todellista toimintakykyä ja usein pakottavat sulkemaan palveluita tai ajamaan alas palvelimia tai jopa vaihtamaan ohjelmistoja. Yritys saattaa tahtomattaan jakaa asiakkailleen matoja tai viruksia, jolloin hyvien suhteitten ylläpito vaatinee nopeaa ja tarkoituksenmukausta reagointia.

Tuhomekanismeiltaan virukset voivat olla lähes millaisia tahansa. Melissa siirsi yrityksen tiedostoja Internettiin, ExploreZip tuhosi ohjelmien lähdekoodeja sekä Word-, Excel- ja Power Point -tiedostoja. LoveLetter puolestaan tuhosi erilaisia kuvatiedostoja. CIH-virus tuhosi tiedot 2 miljoonan mikron kiintolevyiltä, ja romutti lisäksi jopa 400 000 em. mikrojen emolevyistä. Jotkut virukset uhkaavat tiedon eheyttä esimerkiksi aiheuttamalla piileviä virheitä laskentataulukkoihin, tekstin oikeinkirjoitukseen tai sanojen sijaintipaikkoihin. Usein tällaiset virheet ovat hitaasti kumuloituvia vaikeuttaen oikean lähtökohtatilanteen löytämistä edes varmistusten avulla.

Osa viruksista ja troijalaisista asentaa järjestelmään takaovia, joitten avulla hakkeri pääsee tunkeutumaan suojattuihin tietojärjestelmiin ja NetBus-tyyppisten etähallintaohjelmien avulla sen jälkeen tekemään lähes mitä hyvänsä. Tähän ryhmään kuuluu myös viruksia, jotka nauhoittavat käyttäjätunnuksia ja salasanoja sekä etsivät salasanatiedostoja, ja siirtävät näitä sitten hakkerin haluamiin osoitteisiin.

Klez-mato osoitti vuoden 2002 alussa, kuinka kevyellä pohjalla Internetin osoitetiedot ovat. Mato väärensi systemaattisesti lähettäjäosoitteensa, ja virustartunnoista tuli pysyväisluontoinen ongelma. Enää ei voitu ottaa yhteyttä madon lähettäjään ja kehoittaa häntä pitämään mikronsa virustorjuntaa ajan tasalla. Operaattoreita vaadittiin suodattamaan Klez-tyyppiset madot pois sähköpostin joukosta, mutta tätä ei tehty -ja ongelmakin on globaali - minkä seurauksena nyt kymmenissä eri madoissa on samanlainen osoitteiden väärennysmekanismi.

Tänä vuonna viruksellinen uhka on entisestään kasvanut. Slammer-mato hyökkäsi tammikuussa, ja tartutti lauantaina 24.1. kymmenessä minuutissa lähes 90 000 Internet-palvelinta. Yksi Slammer sinkosi mikrosta noin 30 000 pientä matoa joka sekunti, ja parissa vuorokaudessa koko Internet-verkkoavaruus oli käyty läpi.

Loppukesällä iski sitten Blaster-mato, ja siinä yhteydessä jouduttiin toteamaan, että jatkuvasti ajossa oleva virustorjuntakaan ei pysty matojen leviämistä verkossa estämään. Yritys- ja työasemakohtaiset palomuurit ovat tulossa tärkeiksi matojen torjunnassa. Blaster aiheutti vakavia ongelmia monissa yrityksissä, ja sen kannoille ilmaantuikin normaalin virustorjunnan lisäksi merkittävä uutuus: matoa syö-

Case Lovsan/Blaster, elokuu 2003

Tyyppi:	Löydetty:	Matotiedosto:	Koko:	Palveluneston kohde:
Blaster.A	11.8.2003	msblast.exe	6176 tavua	windowsupdate.com
Blaster.B	13.8.2003	penis32.exe	7200 tavua	windowsupdate.com
Blaster.C	13.8.2003	teekids.exe	5360 tavua	windowsupdate.com
Blaster.D	19.8.2003	mspatch.exe	11776 tavua	windowsupdate.com
Blaster.E	28.8.2003	mslaugh.exe	6176 tavua	kimble.org
Blaster.F	1.9.2003	Enbiei.exe	11808 tavua	tuiasi.ro
Welchia	18.8.2003	Dllhost.exe	10240 tavua	Tuhoaa Blaster.A matoja

ja asentaa MS-26/2003 tietoturva-aukon paikkauksia. Itsetuhooja 1.1.2004. Suunnattu leviämään erityisesti kiinalaisissa verkoissa.

Case MiMail, marraskuu 2003

Tyyppi:	Löydetty:	Palveluneston kohde:
MiMail C	31.10.2003	Darkprofits.com
MiMail D	1.11.2003	Fethard.biz, Fethard-Finance.com
MiMail E, H	2.11.2003	Spamcop.net, Spamhaus.org, Spews.org
MiMail F	2.11.2003	Fethard.biz, Fethard-Finance.com
MiMail G	2.11.2003	Mysupersales.com
MiMail I	14.11.2003	varastaa pankkikorttitietoja

Case Sobig.F, elokuu 2003

Tyyppi:	Löydetty:	Itsetuhooja:	Koko:
Sobig.A	9.1.2003	ei itsetuhoojaa	65538 tavua
Sobig.B	18.5.2003	31.5.2003	50425 tavua
Sobig.C	31.5.2003	8.6.2003	57241 tavua
Sobig.D	18.6.2003	2.7.2003	76003 tavua
Sobig.E	25.6.2003	14.7.2003	86528 tavua
Sobig.F	19.8.2003	10.9.2003	72892 tavua

Palvelunestohyökkäykset vaikuttavat kostolta spammauksen vastustajille. Lisäksi mukana saattaa olla tilattuja hyökkäyksiä ”nuijikaa kilpailijani kotisivut”. Tämäntyyppinen, Windows-pohjainen hyökkäys jatkuu ehkä kuukausia. Aiemmat palvelunestohyökkäykset ovat yleensä olleet unix-pohjaisia ja koneiden oppilaitoskäytön vuoksi nopeammin löydettävissä ja lopetettavissa.

vä mato. Jos katsoo Kiinan selviytymistä CIH-viruksesta, on helppo ymmärtää, että viranomaiset ovat saattaneet päätyä melko epätoivoisiinkin keinoihin suojellakseen suurta kansakuntaansa. Welchi/Nachi/Sachi niminen mato ainakin vaikuttaa järkevältä yritykseltä torjua Blasteria. Selvää on, että jokainen virustorjuntayritys kuitenkin tulee tämän järkevyyden kiistämään.

Sobig-matoihin liittyy vielä huolestuttavampi ilmiö: virukset ovat osa liiketoimintaa, ja niitä rakentelevat osaavat ohjelmoijat oletettavasti hyvää korvausta vastaan. Tähän saakka viruksia ovat rakentaneet pääsääntöisesti nuoret miehet - yksi tunnettu poikkeus on olemassa, hollantilaistyttö peitenimi Sharpei. Jos viruskirjoittajaa pitäisi etsiä, nuori mies on naista todennäköisempi tekijä suunnilleen suhteessa 10 000 : 1.Tähän saakka ammattimaiset virustorjuntayritykset ovat jokainen tutkineet jokaisen virusnäytteen, ja sen jälkeen implementoineet torjuntakyvyn omiin järjestelmiinsä.

Jatkossa vastassa on spammibisnes, joka Sobig-madoilla ja niiden asentamilla takaovilla kontolloi jatkuvasti suurta joukkoa heikosti suojattuja mikroja. Aika ajoin spammaaja sitten etäoperoi uhrinsa mikroa siirtäen sinne spammauskoneen ja listan uhreista. Yksi tällainen mikro saattaa lähettää 100 000 mainosviestiä vuorokaudessa. Ihmiset, jotka klikkaavat viestin kohtaa “en halua lisää näitä viestejä” päätyvät spammibisnekseen kauppatavaraksi (“varmistettu Internet-osoite”). Osoitelistoja myydään hämäräbisneksessä ehkä $ 200/miljoona osoitetta. Viaton suomalainen, jonka mikron kautta tämä liiketoiminta kiertää, saattaa madon ja koneen takkuilun jälkeen lisäksi tulla spammaajana tai madon levittäjänä irroitetuksi Internetistä.

Spammeja aktiivisesti inhoavat ovat perustaneet palveluita, joissa on tietoa spammaajista, mustia listoja jne. Hämäräorganisaatio suojelee reviiriään, ja spammauksen vastustajat ovat parhaillaan melko voimakkaan palvelunestohyökkäyksen kohteena. Ammattilaiset ovat luoneet yhden toimivan madon, (MiMail) ja tehneet siitä eri muunnoksia eri kohteita vastaan. Mahdollisesti tähän liittyy myös uusi hämäräbisnes, nujerramme kilpailijanne Internet-palvelun sopivaa korvausta vastaan.

Koska ict-maailman reagointi uusia uhkia vastaan vie yleensä vuosia, ja lainsäätäjien globaali reagointi saattaa suorastaan törmätä eturistiriitoihin, vuodesta 2004 on helppo ennustaa kaikkien aikojen pahinta virusvuotta.

Ilkka Keso,
Tietoturva-asiantuntija,
Osuuspankkikeskus

Lähteet

F-Secure- ja Symantec-virustorjuntayritykset sekä Virus Bulletin -lehti.

WLANin käyttö ja tietoturvallisuus

Kimmo Rytkönen,
TietoEnator Oyj

1 Johdanto

WLAN-teknologiaan (Wireless Local Area Network) perustuvat langattomat lähiverkot yrityksissä ja julkisten tilojen hotspot-alueet ovat yleistyneet viime vuosien aikana. On ennustettu että pelkästään läntisessä Euroopassa olisi 70000 hotspot-tukiasemapistettä vuoteen 2007 mennessä ja käyttäjiä kymmeniä miljoonia (lähde: wirelesshouse.fi). Tähän on vaikuttanut WLAN-tekniikkaa tukevien päätelaitteiden ja kannettavien tietokoneiden markkinoille tulo, työntekijöiden halu päästä yrityksen tietoverkkoihin mobiilisti sekä tarve päästä eroon työasemakaapeloinnista sellaisissa tiloissa, jotka eivät ole kiinteitä työpisteitä kuten neuvottelutilat.

Gartner-tutkimuslaitoksen vuonna 2002 laaditun arvion mukaan Euroopassa myydyistä kannettavista tietokoneista 80%:ssa on WLAN-tuki valmiina. Lisäksi useat PDA-laitteet (Personal Digital Assistant) tukevat WLANia. Arvion mukaan WLAN-tukiasemien ja –korttien lukumäärä osoittaa tasaista kasvua seuraaville vuosille. Viimeisimpien markkina-arvioiden mukaan globaalit WLAN-markkinat kasvoivat 9%:lla 398 miljoonaan Euroon vuoden 2003 kolmannella vuosineljänneksellä. Samana ajankohtana WLAN-tukiasemien myynti kasvoi 25%. Markkinajohtaja on Cisco, muita isompia toimittajia ovat mm. 3COM ja Proxim (lähde: 13.11.2003 RDSL infobites).

Monet operaattorit kuten TeliaSonera ovat alkaneet tarjoamaan langattomaan teknologiaan perustuvia liittymäpalveluja julkisilla paikoilla mm. lentokentillä, areenoilla ja rautatieasemilla. Näitä kutsutaan hotspot-alueiksi, joiden kautta on mahdollisuus päästä Internetiin tai muodostaa etäyhteyksiä yrityksen lähiverkkoon. Langattomilla WLAN- niin kuin Bluetooth-yhteyksillä on arvioitu olevan paljon sovelluskohteita, mm. kodin elektroniikkalaitteet on mahdollista varustaa langattomalla tekniikalla. Tällä hetkelläkin WLAN-lähiverkkoja on jo teollisuuden ja kaupan varasto- ja tuotantotiloissa tiedonkeruu ja –jakelukäytössä.

Tässä artikkelissa esitellään WLAN-tekniikkaan ja erityisesti sen tietoturvaominaisuuksia yrityksen toimitiloissa sekä etäyhteyksillä.

1.1 WLAN-spesifikaatiot

WLAN-teknologia ei ole kovin vanhaa, sillä ensimmäiset viralliset spesifikaatiot julkistettiin vuonna 1997 IEEE:n (Institute of Electrical and Electronics Engineers) toimesta. WLAN-järjestelmiä koskevat spesifikaatiot määrittelevät kolme WLAN-järjestelmää 802.11a, 802.11b ja 802.11g, joista viimeisin ratifioitiin kesällä 2003 (kts. taulukko alla).

Edellä mainituista WLAN-järjestelmistä 802.11b on yleisin, koska kaikki WLAN-laitteet tukevat sitä ja julkiset WLAN-toteutukset perustuvat sen käyttöön. Luultavasti 802.11g tulee saavuttamaan suosion, koska samalla peittoalueella saavutetaan parempi siirtokapasiteetti. 802.11g –järjestelmä on rakennettu siten, että se on taaksepäin yhteensopiva 802.11b-järjestelmän kanssa eli 802.11g-järjestelmän tukiasema pystyy palvelemaan 802.11b-järjestelmän mukaisia yhteyksiä b-järjestelmän siirtokapasiteetilla. 802.11g-standardia tukevia WLAN-laitteita on jo markkinoilla ja useat toimittajat ovat julkistaneet tukevansa sitä. Tätä standardia tukevien laitteiden markkinoille tulo selittää hyvin edellä mainitut kasvulukemat WLAN-markkinoilla.

WLAN-järjestelmän valintaan vaikuttaa monet asiat. Esimerkiksi 2.4GHz:n taajuusalueella toimivat laitteet ovat herkempiä interferenssihäiriöille, koska taajuuskanavajaon vuoksi samalle alueelle voidaan sijoittaa ainoastaan kolme tukiasemaa, jolloin ne eivät häiritse toisiaan. 802.11a –järjestelmässä yhden tukiaseman peittoalue on pienempi, mutta taajuuskanavajako mahdollistaa useamman tukiaseman sijoittelun samalle alueelle, jolloin

	802.11a	802.11b	802.11g
Ratifioitu	2002	1999	2003
Radiotaajuus	5 GHz	2.4 GHz	2.4 GHz
Siirtokapasiteetti	max 54 Mb/s	max 11 Mb/s	max 54 Mb/s
Peittoalue	max 50 m	max 100 m	max 100m

ne eivät häiritse toisiaan. Tällä tavalla saavutetaan suurempi siirtokapasiteetti. Yksi tukiasema pystyy palvelemaan kymmeniä WLAN-yhteyksiä. Markkinoilla on tällä hetkellä tukiasemia, jotka mahdollistavat myös kahden järjestelmän käytön samanaikaisesti. Tämä tarkoittaa sitä, että samassa tukiasemassa on kaksi radiota, esim. a- ja b-radio. Tämä yhdistelmä mahdollista myös sen, että b-radio-osa voidaan päivittää g-radio-osaksi.

Muut IEEE:n WLAN-spesifikaatiot (802.11d, e, f, g, h, i ja j), joista osa on keskeneräisiä, ovat täydentäviä määrittelyjä, joita WLAN-järjestelmät voivat ottaa käyttöön. Näistä spesifikaatioista 802.11i on tietoturvaspesifikaatio.

1.2 Wi-Fi

WLAN-teknologian alkuvaiheessa havaittiin, että eri toimittajien WLAN-toteutukset (tukiasemat, kortit) eivät toimineet keskenään moitteettomasti IEEE:n 802.11-spesifikaation mukaisesti. Siksi 1999 perustettiin Wi-Fi-organisaatio (Wireless Fidelity), jonka tehtävä on ollut sertifioida 802.11-spesifikaatioiden mukaiset WLAN-toteutukset. Organisaatiolla on muutama sata WLAN-järjestelmätoimittajaa jäsenenään. Viime aikoina organisaation tehtävänä on ollut kehittää 802.11-spesifikaatioissa määritellylle WEP-salausmenetelmälle (Wired Equivalent Privacy) kehittyneempi versio. Syynä tähän oli se, että alunperin määritelty WEP-salausmenetelmä sisälsi heikkoja tietoturvamenetelmiä, joita WLAN-toimittajat yrittivät ratkaista omilla keinoilla, jotka eivät välttämättä toimineet kaikissa WLAN-ympäristöissä. Lopputuloksena Wi-Fi kehitti WPA-tietoturvamenetelmän (Wi-Fi Protected Access), jonka on määrä korvata WEP-toteutukset. WPA sisältää tällä hetkellä tuen 802.1X-autentikointimenetelmälle sekä avainten vaihtoprotokollalle TKIP (Temporary Key Interchange Protocol). WPA on myös osa tulevaa 802.11i –tietoturvaspesifikaatiota, jossa tuetaan myös AES-salausta (Another Encryption Standard). 802.11i tulee olemaan kaikille WLAN-toimittajille yhteinen tietoturvaspefikaatio, jossa 802.1X-autentikointimenetelmällä ja WPA:lla on keskeinen merkitys. 802.1X-menetelmä sisältää EAP-protokollan (Extensible Authentication Protocol). 802.11i-spesifikaatio on määrä ratifioida vuoden 2004 aikana. Tällä hetkellä Wi-Fi sertifioi WPA-yhteensopivat WLAN-toteutukset, joita on jo markkinoilla. Lisää tietoa Wi-Fin toiminnasta saa web-sivulta http://www.weca.net.

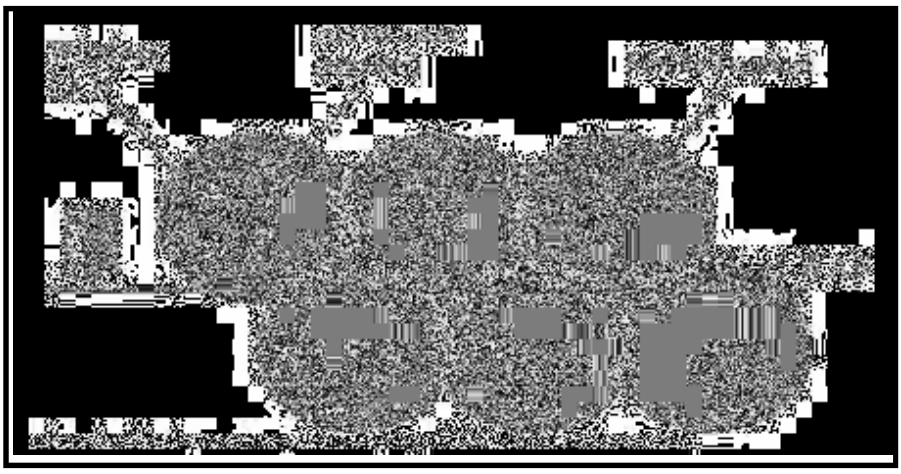
2 WLANin käyttö ja tietoturvallisuus

Yrityksen WLAN-verkkoa suunniteltaessa on mietittävä millaiseen käyttötarkoitukseen se tulee. Jos yrityksellä on olemassa toimiva kiinteä Ethernet-verkko, ei välttämättä ole mitään syytä hankkia tämän rinnalle samaan käyttötarkoitukseen hitaampaa langatonta verkkoyhteyttä, jos ratkaisu ei tuo selvää lisäarvoa tai paranna nykyisten verkkoresurssien käytettävyyttä. Jos kiinteä työpiste on kytketty 100Mbit/s -verkkoyhteyteen, ei langaton 10Mbit/s - tai 54Mbit/s – yhteys ole mikään lisäarvo, enemmin pullonkaula isompaa tiedonsiirtoa vaativien sovellusten käytölle. On muistettava, että kahden verkon ylläpito vaatii resursseja (kts. kuva alla verkkojen yhteiskäytön periaatteesta).

Langattomalla verkkoyhteydellä pyritään saamaan joustavuutta työpisteiden sijoitteluun. Langaton yhteys on paras vaihtoehto, kun käytettävissä ei ole kiinteää työpistettä. Esimerkiksi avoimien toimistotilojen, konesalitilojen, aulojen, ruokailu- ja kahvilatilojen, varastojen, tehdasalitilojen ja neuvottelutilojen verkkosuunnittelussa päästään helpommalla, jos ei tarvitse asentaa verkkorasioita työasemakäyttöä varten. Tällöin voidaan unohtaa myös työasemakaapelointi. Verkkosuunnittelun ratkaisuna on tukiasemien sijoittelu siten, että saadaan aikaan riittävän kattava ja signaalivoimakkuudeltaan riittävän suuri peittoalue. WLAN-pohjaista radioverkkoa suunniteltaessa onkin mietittävä missä yhteydessä langatonta yhteyttä tarjotaan ja kunkin käyttäjän on päätettävä kumpaa vaihtoehtoa käyttää, jos tarjolla on vielä kiinteä verkkoyhteys. Päätökseen vaikuttaa tarvittava siirtokapasiteetti, käytössä oleva päätelaite (mm. pöytäkone, kannettava kone, mobiililaite) ja henkilön liikkuvuus työpisteestä toiseen samassa kerroksessa tai kerrosten välillä.

2.1 Tietoturvallisuus

Yrityksen tietoturvapolitiikka määrittelee yrityksen tietoturvan perusperiaatteet. Tämän rinnalla on usei-



ta tarkempia tiettyä aihealuetta käsitteleviä sääntöjä ja ohjeistuksia. Yksi tällainen ohjeistus käsittelee WLANin käyttöä yrityksen tiloissa, etäyhteyksillä hotspot-alueilla kuten lentokentillä ja hotelleissa, asiakkaiden luona ja kotona. Tätä ohjeistusta kutsutaan langattomaksi tietoturvapolitiikaksi (wireless security policy), joka kuvaa WLANin tietoturvauhat ja -ratkaisut turvalliselle WLANin käytölle. Politiikkadokumentti voi esimerkiksi määritellä ainoaksi hyväksytyksi autentikointimenetelmäksi toimikorttipohjaista vahvaa tunnistautumista.

2.1.1 Tietoturvauhat

Yrityksen sisäiset ja julkiset WLAN-toteutukset eroavat tietoturvatason suhteen melkoisesti toisistaan. Esimerkiksi kaikki WLAN-tukiasemat eivät tue viimeisimpiä tietoturvastandardeja, vaikka WLAN-verkkokortti niitä tukisi. Tämä voi tarkoittaa sitä, että yrityksen sisällä käytettävät tietoturva-asetukset eivät toimi esimerkiksi julkisissa WLAN-verkoissa, vaan yhteyden luomiseksi on tyydyttävä tasoltaan heikompiin tietoturva-asetuksiin.

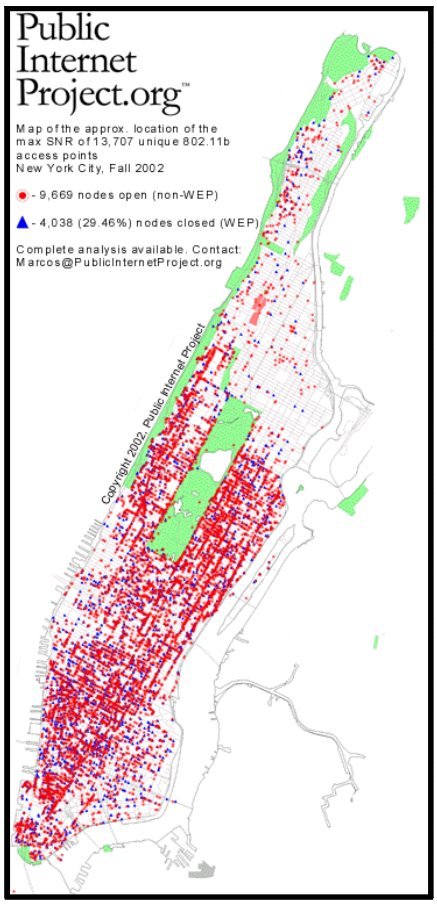
WLAN-verkon tietoturvauhat perustuvat siihen, ettei verkon peittoaluetta pystytä rajaamaan yrityksen toimitiloihin, vaan verkko näkyy yrityksen toimitilojen ja rakennusten ulkopuolellakin. Suurin uhka on verkon liikenteen salakuuntelu, koska se voi tapahtua yrityksen tilojen ulkopuolella. Hyvä esimerkki WLANin tietoturvatasosta on joulukuussa 2002 tehty kartoitus New Yorkin Manhattanilla, missä tutkija Marcos R. Lara kartoitti ajamalla saaren jokaisella kadulla ja analysoimalla siihen tarkoitetuilla sovelluksilla WLAN-verkkojen mainostamaa tietoa itsestään (verkon nimi, salaus käytössä tai ei, toimittaja, signaalivoimakkuus, jne...). Hän havaitsi kaikkiaan 14000 WLAN-verkkoa (kts. kuva alla), joista 70%:ssa ei ollut salausta ollenkaan päällä. Lopuissa 30%:ssa tapauksista oli käytössä WEP-salaus (lähde: 12.12.2002 NY Times). On arvioitu, että vuoden 2003 aikana paikkakunnalle on perustettu useita tuhansia WLAN-verkkoja lisää.

Suurimmat tietoturvauhkat ovat muodostuneet silloin, kun tunnukset ja salasanat ovat paljastuneet (ne on varastettu tai hukattu), käytössä on ollut heikko WEP-salausmenetelmä, WLAN-tukiasema tai –kortti on väärin konfiguroitu, tai yksinkertaisesti radiohäirinnällä on aiheutettu palvelunesto tukiasemalle tai suoraan WLAN-kortille (adhoc-yhteydet on sallittu).

Yksi ratkaisu tietoturvauhkiin on liikenteen riittävän vahva salaus. Riittävä salaus ja pääsynvalvonta on ratkaisu myös laittomille pääsyoikeuksille. Radioliikenteen häirintä ja datan muokkaamisen aiheuttamat eheys- ja palvelunesto-ongelmat voidaan ratkaista eheyden tarkistavilla ja palveluneston havaitsevilla rutiineilla.

2.1.2 Hyviä käytäntöjä tietoturvan toteuttamiseksi WLAN-verkoissa

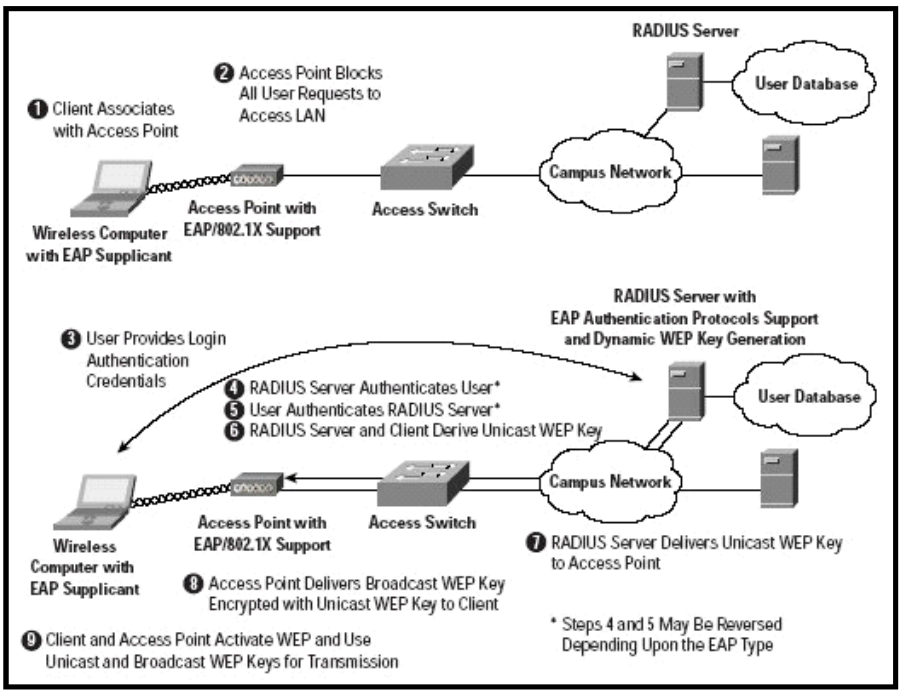
Hyviä käytäntöjä WLAN-verkon suunnitteluun ovat yhdenmukainen radioverkkosuunnittelu, verkon ylläpidettävyys ja turvallisuusasiat. Verkon suunnittelussa pitää huomioida sen kattavuus niin, ettei katvealueita ja heikon signaalivoimakkuuden alueita muodostu, verkko ei näy siellä missä sen ei toivottaisi kuuluvan, käytettyjen taajuuskanavien jako pitää tehdä niin, ettei lähellä olevat tukiasemat häiritse liikennettä, sekä pitää huomioida, ettei tukiasemat aiheuta interferenssi-ilmiöitä tai muuta häiriötä ympäristön laitteille. Verkon ylläpidettävyyteen kannalta tukiasemia pitäisi pystyä hallinnoimaan ja valvomaan keskitetysti. Tämä liittyy esim. tukiasemaohjelmistojen päivityksiin, asetusten konfiguroimiseen, konfigurointitietojen tallennukseen ja palauttamiseen sekä automaattisiin valvontaominaisuuksiin, joilla voidaan havaita esim. tukiaseman kytkeytyminen pois päältä tai laittoman tukiaseman liittyminen verkkoon.



WLAN-tukiasemat ja –verkkokortit ovat oletusasetuksiltaan sellaisia, ettei niissä ole liikenteen salausta ja käyttäjien tunnistamista automaattisesti päällä. Siksi on tärkeätä konfiguroida tukiasemat oikein ja opastaa käyttäjiä omien tietoturva-asetusten käytössä mielellään siten, että niihin ei tarvitse tehdä mitään muutoksia riippumatta siitä missä WLAN-yhteyksiä käytetään. Käyttäjille on luotava yrityksen toimitiloissa ja etäyhteyksillä toimivat profiilit (konfiguroinnit tietoturva-asetuksineen) valmiiksi.

Edellä mainitut asiat liittyvät WLAN-verkon tietoturvatason toteutukseen. Lisäksi verkon tietoturvaan liittyvät seuraavat asiat:

- käyttäjien tunnistaminen
- liikenteen salausmenetelmä
- tukiasemien konfigurointimenetelmät ja fyysinen suojaus
- tukiasemien muodostaman verkon tunnistetietojen näkyvyys
- tukiasemien tunnistaminen
- adhoc-yhteydet päätelaitteiden välillä



Perusvaatimus WLAN-verkon tietoturvalle on käyttäjien tunnistauminen keskitetysti ja hallitusti ilman, että se aiheuttaa mahdollisimman vähän ylimääräisiä toimenpiteitä käyttäjiltä. Hyvä käytäntö on toteuttaa tunnistautuminen olemassaolevia käyttäjähakemistoja vasten kuten LDAP- (Lightweight Directory Access Protocol) tai AD-pohjaiset (Active Directory) käyttäjähakemistot sekä NT/Windows-toimialueet, kun toimitaan yrityksen toimitiloissa. Tämä voidaan toteuttaa Radius-pohjaisella autentikoinnilla, kun tukiasemat tukevat sitä. Tämä edellyttää päätelaitteessa toimivaa Radius-autentikointia tukevaa asiakasohjelmaa, joka kysyy verkkotunnuksen ja salasanan ja välittää ne tukiaseman tiedossa olevalle Radius-palvelimelle, joka tukee edellä mainittuja autentikointimenetelmiä em. käyttäjähakemistoja vasten. Verkkotunnusten käyttö on perusteltua, sillä käyttäjätiedot hallitaan yhdessä paikassa eikä WLAN-yhteyksille tarvitse luoda omia tunnuksia. Esimerkki 802.1X/EAP-pohjaisesta autentikointimenetelmästä on esitetty seuraavassa kuvassa (lähde: 2003 Cisco Safe: WLAN security in depth, White Paper).

Etäyhteyksillä suositellaan käytettäväksi IP-tasolla suojattuja VPN-yhteyksiä, jolloin käyttäjien tunnistautuminen voi tapahtua esim. Radius-palvelimen käyttäjähakemistoa tai SecurID-autentikoinnilla ACE/Server-käyttäjähakemistoa vasten.

Tukiasemat tukevat myös MAC-osoitteisiin perustuvaa pääsynvalvontaa ja käyttäjien hallintaa. Näillä keinoilla pystytään rajaamaan pääsy ainoastaan tietyn MAC-osoitteen omaaville verkkokorteille tai käyttäjätunnuksille. MAC-osoitelistan toteuttaminen ei ole käytännöllistä ja turvallista yritysverkossa, sillä sen avulla ei voida tunnistaa todellista käyttäjää, se vaatii jokaiseen tukiasemaan MAC-osoitelistat ja näiden ylläpito on työlästä ja toisaalta sallitun MAC-osoitteen väärinkäyttö on aina mahdollista. Myös käyttäjien hallinta tukiasemissa vaatii paljon ylläpitoa. Tällaiset ratkaisut toimivat pienessä ympäristössä, jossa on muutamia tukiasemia ja vähän käyttäjiä.

Toinen perusvaatimus WLAN-verkon tietoturvalle on liikenteen salaaminen vahvalla salausmenetelmällä. Tämä tarkoittaa ratkaisua, jossa käytetään hyväksyttyjä (esim. FIPS 140-2 standardin mukaan hyväksyttyjä menetelmiä salauksen toteuttamiseksi) salausalgoritmejä, riittävän pitkiä salaus- ja istuntokohtaisia avaimia salatiedon tuottamiseksi, joista jälkimmäiset vaihtuvat riittävän usein, jotta viestiliikennettä kuuntelemalla ja keräämällä dataa ei pystyttäisi ratkaisemaan käytettyjä avaintietoja. Tukiasemissa salaus pitää olla päällä ja verkkokorteissa pitää olla valittuna sopiva salausmenetelmä.

Kolmas perusvaatimus on tukiasemien konfigurointi, joka ei saa tapahtua langattomasti, vaan kiinteän verkon kautta. Pääsy tukiasemien konfigurointitietoihin pitää varustaa pääkäyttäjän tunnuksella ja salasanalla. Tällä tavoin vältetään se mahdollisuus, että jotain tietoa saattaa paljastua, jos liikennettä kuunnellaan ja viestiliikenne pystytään tulkitsemaan. Fyysisen suojauksen osalta tukiasemat pitää sijoittaa sellaisiin paikkoihin, joissa ne eivät joudu muun radiosäteilyn kohteiksi tai niitä voidaan helposti vahingoittaa.

Neljäs perusvaatimus on tukiasemien muodostaman verkon tunnistetietojen (mm. verkon nimi) mainostamisen estäminen. Vaikka WLAN-verkontunnuksen suojaamisella ei ole paljon merkitystä, on parempi estää tukiasemien sanomien lähettäminen, joissa ko. tietoja esiintyy, jotta verkko ei mainostaisi itseään turhaan ja näin välttyisi siihen kohdistuvilta hyökkäyksiltä.

Viides perusvaatimus on tukiasemien tunnistaminen niin, että yrityksen lähiverkkoon pystyy tunnistautumaan ainoastaan tunnetuista tukiasemista. Tukiasemat on tällöin määritelty Radius-palvelimelle ja ne tunnistetaan IP-osoitteen lisäksi salatiedon perusteella. Laittomat tukiasemat pitää pystyä tunnistamaan siihen soveltuvien valvontaohjelmistojen avulla.

Kuudes perusvaatimus on määritellä tarkoin tukiasemien kautta muodostettavat adhoc-yhteydet päätelaitteiden välillä sekä päätelaitteiden keskinäiset ad-hoc-yhteydet. Oletusasetuksiltaan jopa kymmenen päätelaitteen välille muodostettava ad-hoc –yhteys ei vaadi salausta tai autentikointia. Ad-hoc –yhteydelle voidaan määritellä salaus ja salasanalla tapahtuva tunnistautuminen. Tietoturvaltaan adhoc –yhteydet eivät ole riittäviä, joten niitä ei suositella käytettäviksi.

2.2 Yhteenveto

Yhteenvetona voidaan sanoa, että tarvittavat tietoturvaelementit WLANin turvalliselle käytölle ovat nyt olemassa kunhan ne vaan tiedostetaan ja otetaan käyttöön. Tietoturva-aukot ovat yleensä muodostuneet tiedostamatta, kun ei ole osattu kiinnittää huomiota tietoturvaan. Hyvällä radioverkkosuunnittelulla voidaan luoda toimivia yritysratkaisuja, jotka vastaavat käyttötarkoitusta ja käyttäjien opastuksella vältetään tietoturvaongelmat etätyössä mm. kotona tai julkisilla paikoilla käytettäessä WLAN-yhteyksiä.

Artikkelin kirjoittaja Kimmo Rytkönen toimii TietoEnatorissa Telecom&Media-alueella konsulttina ja tietoturvapäällikkönä.

Käyttöoikeudet ja tietoturva SAP:ssa

Vesa Oinonen,
Pohjola-Yhtymä Oyj

SAP on maailman yleisin suurten yritysten toiminnanohjausjärjestelmä. Koska yritysten käyttöoikeus- ja tietoturvavaatimukset ovat moninaiset, myös mahdollisuudet käyttöoikeuksien toteutukseen ovat SAP:ssa erittäin monipuoliset. Esimerkiksi pörssiyhtiössä taloushallinnon käyttöoikeuksiin on suhtauduttava suuremmalla vakavuudella kuin listaamattomissa yhtiöissä. Tulostietojen vuotaminen väärille tahoille ennen virallista julkistamista on estettävissä osin myös asianmukaisesti hoidetuin käyttöoikeuksin. Myös kaikkiin järjestelmän toiminnallisuuksiin, joissa on mahdollista vaikuttaa rahasuoritusten vastaanottoon ja lähettämiseen, on tietoturvamielessä suhtauduttava erityisen vakavasti ja huolellisesti.

SAP-järjestelmässä käyttöoikeuksin rajataan ensinnäkin, mihin eri toiminnallisuuksiin käyttäjä pääsee. Toiminnallisuuden sisällä voidaan lisäksi rajata valtuuden taso; esim. onko oikeus näyttämiseen, muuttamiseen vai luomiseen tai mihin organisaatio-osaan käyttäjällä on valtuus. Yleensä eri käyttäjäryhmille luodaan ns. käyttöoikeusroolit, joihin käyttäjä toimenkuvasta riippuen kiinnitetään. Käyttäjälle kiinnitettyjen roolien kautta muodostuu myös käyttäjäkohtainen menu.

Huolellinen suunnittelu lähtökohtana

Huolellinen määrittely on tärkein osa-alue käyttöoikeuksien toteutuksessa. Määrittelyssä on tunnistettava yrityksen prosessit ja erilaiset käyttäjäryhmät. Lisäksi on tunnettava SAP:n mahdollisuudet ja rajoitteet, ts. mitä pystytään toteuttamaan ja mitä ei. On myös varmistettava, että suunniteltu ratkaisu ei ole ylläpidollisesti huono. Kun käyttäjiä on satoja ja käytössä on useita SAP:n moduuleja, suunnitellun ratkaisun yksinkertaisuus on ylläpidon ja jatkokehityksen kannalta erityinen etu.

Testaus

Testaus varmistaa, että käyttöoikeuksien määrittely ja konfigurointi vastaavat tarpeita. Lisäksi tavoitteena on havaita mahdolliset virheet. Testaajien on edustettava jokaista valtuuksiltaan toisestaan poikkeavaa käyttäjäryhmää, jotta testauksesta saadaan riittävän kattava. Testitapausten suunnitteluun kannattaa panostaa laadukkaan ja tarkoituksenmukaisen testauksen takaamiseksi. Suunnittelussa on huomioitava sekä positiivinen että negatiivinen testaus. Positiivisella testauksella varmistetaan että käyttöoikeudet ovat riittävät ja tarkoituksenmukaiset. Negatiivisessa testauksessa varmistetaan, että valtuusrajaukset todella purevat. Testauksen hallintaan sopiva työkalu on esim. Mercury Interactiven Test Director, josta on Pohjolassa hyviä kokemuksia. Sen sijaan automaattitestityökaluista ei ole kokemukseni mukaan juurikaan apua käyttöoikeustestauksessa.

Salasana- ja muut kontrollit

Salasanakontrollit vaikeuttavat omalta osaltaan asiattomien pääsyä järjestelmään. Salasanalle on määriteltävä mm. minimipituus, vanhentumisaika ja lukkiutumiskynnys. SAP:n kontrollit kannattaa määritellä yhtenäiseksi esim. Windows NT:n tai XP:n kontrollien kanssa, jotta käyttäjien ei tarvitse omaksua useita toisistaan poikkeavia salasanasääntöjä.

SAP:n käyttäjätunnukset ovat aina henkilökohtaiset ja yhteiskäyttöisiä tunnuksia ei hyväksytä. Kaksinkertainen kirjautuminen samaa käyttäjätunnusta käyttäen on siis järkevää estää parametroinnissa. Myös käyttämättömän istunnon katkaisuajan avulla vaikutetaan tietoturvaan.

Ylläpito

Uusien käyttäjien perustamiseen ja valtuusmuutoksiin liittyvät menettelytavat kannattaa sopia ja pitäytyä niissä tiukasti. Sovittavia asioita ovat esimerkiksi valtuusmuutosten hyväksymismenettely.

Oleellinen osa tietoturvaa on se, keille annetaan valtuudet käyttäjien perustamiseen ja valtuuksien ylläpitoon. SAP:n suositus on, että *käyttäjätunnuksen ylläpito*, *käyttöoikeusroolin luominen* sekä *käyttäjätunnuksen ja käyttöoikeusroolin yhdistämisen* valtuus olisi eriytetty käyttöoikeuksin eri henkilöille. Käytännössä suosituksen noudattaminen voi olla pienissä SAP:n ylläpito-organisaatioissa hankalaa.

Hyvin hoidettuun ylläpitoon kuuluu myös säännönmukainen käyttäjätunnusten huoltaminen. Yrityksestä lähteneiden sekä käyttämättömät käyttäjätunnukset on säännöllisesti poistettava.

Vesa Oinonen,
Pohjola-Yhtymä Oyj,
vesa.oinonen@pohjola.fi

Tietoturvallisia sovelluksia

Jari Pirhonen
AtBusiness Communications Oyj

Sovellusten tietoturvallisuus on noussut kuumaksi aiheeksi viime aikoina ja sovelluksilta halutaan enenevässä määrin myös tietoturvanäkökohtien huomioimista. Tämä on loistava trendi, koska käytännössähän sovellusprojekteja tehdään nimenomaan asiakaslähtöisesti ja tietoturvallisuus huomioidaan kunnolla vain, jos asiakas sitä vaatii. Toisaalta ei ole järkevää vaatia yleisesti ”tietoturvaa”. Tietoturva on subjektiivista, sovellusten käyttöympäristöt ja uhat ovat erilaisia, riskinsietokyky vaihtelee. Haluttu tietoturvataso täytyy määritellä.

Valitettavan usein nouseva tietoturvatietoisuus näkyy vain siinä muodossa, että asiakas ymmärtää kysyä tietoturvan perään ja sovellustoimittaja kertoo asian olevan kunnossa: ”Käytämme SSL-salausta ja palomuuria”. Tietoturva on kuitattu ja molemmat osapuolet ovat tyytyväisiä. Alku tämäkin, toivottavasti kuitenkin jatkossa tietoturvatarpeet määritellään sekä asiakas- että toimittajapuolella samalla tasolla kuin muutkin sovellusvaatimukset. SSL- ja palomuurisuojaukseen luottaessaan kannattaa muistaa, että palomuuria käytetään estämään pääsy muualle kuin käytettävään sovellukseen. SSL:n käyttö puolestaan vaatii myös sovellusta vastaan hyökkäävän käyttämään tietoliikenteen salausta – tämä ei yleensä ole ongelma. Yksinkertaistaen voisi sanoa, että SSL-salaus ja palomuuri takaavat sen, että vain meidän sovellustamme vastaan voidaan hyökätä ja vieläpä salattua yhteyttä käyttäen.

Median rummuttaessa tietoturvallisuuden ääri-ilmiöitä, kuten virukset, madot ja web-sivustojen hakkeroinnit, yritysten huomiokin helposti keskittyy sovelluskehityksen tietoturvallisuuden parantamisen kannalta epäoleellisiin asioihin. Tietoturvallisuuden kehittäminen on kuitenkin enimmäkseen riskien arviointia, koulutusta, ohjeistusta, käytäntöjen luomista, sopivien työkalujen käyttöönottoa ja dokumentointia.

Yrityksissä, joissa sovellusten tietoturvallisuuden edistämiseksi on jo tehty töitä, ollaan varmaankin kiinnostuneita SSE-CMM (Systems Security Engineering Capability Maturity Model) kehyksen tai Common Criterian käyttöönotosta. Kokemukseni perusteella monet yritykset ovat kuitenkin vasta alkutaipaleella sovellusten tietoturvallisuuden parantamisessa, joten siksi lähestyn asiaa perusteista lähtien. Tavoitteenani on herättää huomioimaan tietoturvallisuus sovelluksissa jo nyt, ennen kuin asiakkaat siihen pakottavat. Tietoturvallisuutta ei nimittäin saada mukaan hetkessä – tarvitaan aikaa toimintatapojen muutokseen sovellusprojektin kaikissa vaiheissa: määrittely, suunnittelu, toteutus, testaus ja käyttöönotto.

Sovelluskehityksen haasteita

Sovelluskehittäjien osa ei ole kadehdittava. Uusia protokollia, middleware-tuotteita ja työkaluja tulee jatkuvasti ja on täysi työ pysyä ajan tasalla uusien tekniikoiden osalta. Sitten vielä pitäisi huomioida tietoturva-asiat. Tämä on kuitenkin välttämätöntä toimivien, laadukkaiden sovellusten tekemiseksi.

Sovellusprojektin yleisimmät tavoitteet ovat toiminnallisuus, helppokäyttöisyys ja tehokkuus. Nämä mielletään usein ristiriitaisiksi tietoturvatavoitteiden kanssa: saatavuus, eheys, luottamuksellisuus, jäljitettävyys ja luotettavuus. Näin ei kuitenkaan tarvitse olla, kunhan kaikki tavoitteet huomioidaan yhdessä.

Sovelluskehityksen jatkuva kiire käyttöönotto- ja julkistusaikatauluista johtuen saattaa pakottaa tinkimään sovelluksen laadusta ja usein tinkiminen tapahtuu siellä, mitä huonoiten ymmärretään – tietoturvallisuudessa. Sovellusprojekteja suunnitellaan edelleen niin optimistisilla aikatauluilla, että monelta lienee jäänyt lukematta Frederick P. Brooksin klassikkoteos: ”The Mythical Man-Month”. Brooks mm. toteaa, että tuotteistetun ohjelmistokomponentin tekemiseen menee 9 kertaa enemmän aikaa kuin pelkän toiminnallisuuden ohjelmoimiseen ja Brooks ei edes tuonut esille tietoturvaa.

Sovellusprojekteilla ja tietoturvallisuudella on kyllä usein yksi yhteinen tavoite: yksinkertaisuus. Monimutkaisuus on tietoturvallisuuden pahin vihollinen. Valitettavasti sovellusympäristö muuttuu koko ajan monimutkaisemmaksi. Yritykset verkottuvat, sovelluksia halutaan käyttää aina ja kaikkialta erilaisten verkkoyhteyksien ja päätelaitteiden kautta, sovelluksia on avattava asiakkaille, kumppaneille ja mahdollisesti myös kilpailijoille. Haasteita riittää käyttöliittymä- ja sovellusarkkitehtuurisuunnittelijoille ohjelmoijista puhumattakaan. Samalla tietoturvahaasteet kasvavat. Ennen tietoturvallisuutta kuvattiin linnakemallilla –

yrityksen sovellukset olivat suojassa yrityksen ”muurien” ja ”vallihautojen” takana. Nykyisin tietoturvallisuutta on ajateltava käyttäen mallina toria tai lentokenttää – huomio keskittyy käyttäjien hallintaan, todennukseen ja käyttöoikeuksiin.

Saatavuus on jo ajat sitten syrjäyttänyt luottamuksellisuuden useimpien yritysten tärkeimpänä tietoturvatavoitteena. Vastaavasti on esitetty näkemyksiä, joiden mukaan yritysten ensisijainen tavoite siirtyy tietojen ja sovellusten suojaamisesta selviytymiseen. Tärkeintä on, että palvelut toimivat, vaikka yksittäisiä palvelimia kohtaan hyökättäisiinkin tai verkkomato-epidemia kuormittaisi sähköpostia. Tämä vaatii turvallisten sovellusten lisäksi hyvää tietoturva-arkkitehtuuria, monistettuja järjestelmiä, tietoturvan monitorointia ja toipumissuunnitelmia.

Tietoturvallisuus sovelluskehityksessä

Parempien sovellusten aikaansaamiseksi on oleellista, että tietoturvatarpeet arvioidaan ja tavoitteet määritellään aivan kuten muutkin sovelluksen tavoitteet. Liian usein näkee määrittelydokumentteja, joissa tietoturvallisuus on ohitettu ylimalkaisilla huomautuksilla, kun taas muut sovelluskehittäjille tutummat asiat on kuvattu hyvinkin tarkasti. Tietoturvallisten sovellusten aikaansaaminen vaatii tietoturvallisuuden huomioimista koko sovelluskehitysprosessissa.

Sovelluskehityksen ammattilaisille on selvää, että virheiden korjaaminen on sitä edullisempaa, mitä aikaisemmassa vaiheessa ne huomataan. Kunnollinen määrittely ja suunnittelu säästävät kustannuksia sovelluksen koko elinkaaren aikana. Tietoturvaongelmat eivät tee poikkeusta tähän sääntöön – tietoturva-aukkojen korjaaminen jälkikäteen on kallista.

Kuva 1: Tyypillisiä tietoturvaongelmia

1. Käyttäjän istunnon kaappaus tai mahdollisuus uudelleen ajoon
2. Salasanakontrollien heikkous tai riittämättömyys
3. Puskuriylivuodot
4. Ylimääräiset, haavoittuvat tiedostot ja sovellukset
5. Heikko tai väärintoteutettu salaus tai satunnaislukujen luonti
6. Salasanojen kuuntelu
7. Evästeiden manipulointi
8. Ylläpitomekanismien heikkous tai väärinkäyttömahdollisuus
9. Lokien säilytys tai puute
10. Paljastavat virhekoodit

Lähde: http://www.atstake.com/research/reports/acrobat/atstake_app_unequal.pdf

Yritys nimeltä @Stake teki vuonna 2002 mielenkiintoisen tutkimuksen 45 sovelluksen tietoturvaongelmista. Tulokset olivat hälyttäviä – tietoturvaongelmia löytyi paljon ja jopa 70% näistä oli suunnitteluvirheitä. Vakavista tietoturvaongelmista jopa puolet olisi huomattu huolellisemmalla suunnittelulla. Tyypillisimmät löydetyt ongelmat liittyivät käyttäjän todennuksen ja valtuutuksen virheellisyyksiin, riittämättömään syötteen tarkistamiseen ja istunnon hallinnan turvattomaan toteutukseen. *Kuva 1* listaa tutkimuksessa löydetyt 10 yleisintä tietoturvaongelmaa.

Sovelluksen tietoturvallisuutta ei siis saa jättää ohjelmoijan vastuulle. Toki ohjelmoijalla on oleellinen rooli, mutta ei ole ohjelmoijan tehtävä päättää tietoturvatoteutuksesta: miten käyttäjätodennus tehdään, miten istunto hallitaan, kuinka käyttäjävaltuudet hoidetaan, mitä salausalgoritmeja käytetään, kuinka sovelluksen saatavuus taataan, jne.

Arkkitehtuurisuunnittelulla on oleellinen merkitys. Erityisesti on sovitettava yhteen toisiinsa vahvasti vaikuttavat tietoturva-arkkitehtuuri ja sovellusarkkitehtuuri. Sen sijaan esim. J2EE ja .NET Framework ympäristöjen tietoturvaominaisuuksilla ei ole merkittäviä eroja.

Sovelluskehitysprosessi

Seuraavassa esitän muutamia ohjeita tietoturvallisuuden parantamiseksi. Käytän pohjana vanhan tutun vesiputousmallin vaiheita: määrittely, suunnittelu, toteutus, testaus ja käyttöönotto. Sinällään ohjeet eivät ole riippuvaisia käytettävästä sovelluskehitysmallista. Käytettiinpä vaikka spiraalimallia tai XP-metodia, niin perusohje on sama: ennen toteutusvaihetta on hyvä tietää tavoiteltava lopputulos ja suunnitella tehtävät lopputulokseen pääsemiseksi. Sovellus on syytä myös testata varmistaaksemme, että tavoite ja lopputulos ovat yhtenevät.

Määrittely on tietoturvallisuuden kannalta oleellisin vaihe, jolloin päätetään tietoturvatavoitteet ja -taso. Tietoturvallisuus pitäisi perustaa sovel-

luksen riskianalyysiin, jossa arvioidaan sovellukseen kohdistuvat riskit ja mahdollisten vahinkojen seuraukset sekä päätetään vastatoimet. Ilman riskianalyysiä tietoturvaratkaisut ovat vain arvauksia. Riskianalyysiin käytettävä työmäärä vaihtelee sovelluksen käyttötarkoituksen ja osallistujien kokemuksen mukaan.

Keskusteluun on tärkeää saada mukaan sovelluksen käsittelemän tiedon omistaja, jolla pitäisi olla paras käsitys tiedon arvosta ja suojausvaatimuksista. Yrityksen tietoturvallisuusvastaavat osaavat neuvoa yrityksen tietoturvaohjeistuksen ja -käytäntöjen asettamista reunaehdoista, kuten sallituista verkkoprotokollista, sovellusten sijoittelumahdollisuuksista ja asennuskäytännöistä.

Olen havainnut olevan hyödyllistä miettiä useampia tietoturvaltaan ja kustannuksiltaan eroavia vaihtoehtoja. Tällöin tietoturvataso on helpompi valita ja kaikilla on selkeämpi ymmärrys valitusta ratkaisusta ja siitä, miten tietoturvallisuutta olisi voitu parantaa lisäkustannuksin.

Suunnitteluvaiheessa lyödään lukkoon tekniset tavat määrittelyn sanelemien tietoturvaratkaisujen toteuttamiseksi. Tekninen suunnitelma on ohjelmoijan käsikirjoitus. Sovelluksessa voi olla sekä toiminnallisia tietoturvavirheitä että loogisia ongelmia. Toiminnalliset virheet voi usein laskea ohjelmoijan osaamisen piikkiin, mutta loogiset virheet tulisi karsia suunnitteluvaiheessa. *Kuva 2* esittää tietoturvaan tähtääviä suunnitteluperiaatteita.

Tietoturvatoimintojenkin suunnittelun avuksi on jo olemassa valmiita malleja (security patterns) ja tietysti kannattaa hyödyntää alan tunnettuja parhaita käytäntöjä.

Toteutus on raakaa ohjelmointityötä. Ohjelmoijalla ei pitäisi olla liikaa vapauksia tietoturvaratkaisujen suhteen, vaan hän toteuttaa määrittelyn ja teknisen suunnitelman vaatimukset. Ohjelmoijan vastuulle jää käyttämiensä ohjelmointikielien ja työkalujen tietoturvapiirteiden ja haasteiden ymmärtäminen.

Tietoturvaohjelmointia ei juurikaan ole huomioitu alan koulutuksessa. Ohjelmoijalla täytyy olla hyvinkin erilainen näkökulma sen mukaan koodaako hän sovelluksen toiminnallisuutta, miettikö mahdollisia virhetilanteita ja niistä selviytymistä vai kirjoittaako koodia, jolla toteutetaan tietoturvaratkaisuja. Käsitykseni mukaan tietoturvaa taitavat ohjelmoijat ovat vielä harvinaisuus. Eräät tyypilliset tietoturvaongelmiin johtavat virheet kuten puskuriylivuoto ja syötteen tarkastamatta jättäminen eivät mielestäni taasen ole muuta kuin huonoa koodia.

Perusongelmilta vältytään, jos ohjelmoijien käytössä on kokoelma testattuja, tietoturvanäkökohdat huomioivia valmiskomponentteja ja valmiiksi mietitty kehys tai malli sovelluskehitykseen. Tällöin harvat tietoturvaohjelmointiresurssit voidaan kohdistaa komponenttien tekemiseen ja varsinaisten sovellusohjelmoijien mahdollisuus virheisiin vähenee.

Testauksessa on toiminnallisuuden lisäksi huomioitava tietoturvan testaus. Tietoturvaongelmat johtuvat usein siitä, että sovellukseen on hiipinyt ylimääräistä toiminnallisuutta. Sovellusta voidaan siis käyttää väärin tavalla, jota sovelluksen toteuttajat eivät ole osanneet arvioida.

Ross Andersson ja Roger Needham ovat osuvasti kuvanneet testaamisen ongelmaa termeillä “Murphy’s computer” ja “Satan’s computer”. Usein testaamista tehdään olettaen, että käyttäjä on hyväntahtoinen ja virhetilanteet ovat lähinnä huolimattomuusvirheitä tai taitamattomuutta (Murphy). Tietoturvaa testattaessa pitäisi olettaa, että käyttäjä on pahantahtoinen, sovelluksen väärinkäyttöön kaikkia sääntöjä rikkoen pyrkivä (Satan).

Kuva 2: Tietoturvaperiaatteita

- Suojaa heikoin kohta ensin
- Rakenna useita puolustuslinjoja
- Turvaa virhetilanteet
- Anna sovellukselle vain välttämättömät oikeudet
- Erottele toiminnallisuudet eri tasoisiin turvatiloihin
- Yksinkertainen on kaunista – ja turvallisempaa (KISS)
- Huolehdi yksityisyyden suojasta
- Muista, että salaisuuksien pitäminen on vaikeaa
- Luota säästeliäästi
- Käytä testattuja välineitä ja komponentteja

Lähde: Gary McGraw, John Viega, Building Secure Software

Tarkistuslistoja voi käyttää yleisimpien ongelmien nopeaan löytämiseen, mutta ei kannata luottaa pelkästään niihin. Kuormitustestaukseen, asennusten turvallisuuden testaukseen ja yleisempien ohjelmointivirheiden löytämiseen on olemassa hyviä työkaluja. Järeämpänä keinona voi käyttää ulkopuolisella teetettävää sovelluksen auditointia. Mikään ei kuitenkaan korvaa ammattitaitoista testaajaa. Tietoturvaa testaavan on oltava hyvin tekniikkaa ja ohjelmointia tunteva. Testaaja pyrkii rikkomaan sovelluksen suunnittelijan ja ohjelmoijan virheelliset oletukset, käyttää sovelluksen käyttöliittymien ulkopuolisia omia testiohjelmia ja hyökkää sovellusten ja komponenttien välisiin rajapintoihin.

Koodikatselmointi lienee yksi tehokkaimmista sovelluksen laatua ja tietoturvaa parantavista keinoista. On ihmeen motivoivaa tehdä huolellista jälkeä, jos tietää saavansa hutiloinnista armotonta kritiikkiä kollegoiltaan.

Käyttöönotossa on erityisesti huomioitava tietoturvalliset, kovennetut ja dokumentoidut asennukset. Monilta tietoturvaongelmilta olisi vältytty, jos käyttöjärjestelmistä, sovelluspalvelimista ja tietokannoista olisi asennusvaiheessa poistettu turha toiminnallisuus, esimerkkisovellukset ja oletusarvoiset käyttäjätunnukset ja salasanat.

Nykyisissä sovellusympäristöissä on niin paljon asennettavia komponentteja erilaisine asetuksineen, että usein pyrkimyksenä on vain saada sovellus toimimaan ja toimivaan ympäristöön ei haluta koskea. Tietoturvalliset asennukset edellyttävät suunnittelua ja hyviä asennusohjeita.

Tietoturvallinenkin sovellusympäristö rapistuu hoitamattomana. Ylläpidossa ja tietoturvakorjausten asentamisessa korostuu hyvän dokumentaation ja suunniteltujen käytäntöjen merkitys.

Yhteenveto

Pyrittäessä laadukkaampiin sovelluksiin on tietoturvallisuus otettava mukaan yhdeksi laatukriteeriksi. Tietoturvallisuus on kuitenkin määriteltävä ja suunniteltava sovellukseen alusta pitäen. Ensimmäisenä askeleena tietoturvallisuuden parantamiseksi sovelluskehityksessä voisi terävöittää sovelluksen tietoturvallisuuden määritystä ja testausta. Näin olisi annettu sovelluksen tietoturvatavoitteet ja lisäksi testausvaiheessa saataisiin ongelmat kiinni.

Tietoturvallisuuden kunnollinen huomioiminen sovelluskehityksessä vaatii vuosien työn organisaatiossa. Sovelluskehitysprosessia ei voi muuttaa kertaheitolla, vaan tässäkin eteneminen pienin askelin lienee se helpoin tie.

Otan mielelläni sähköpostitse vastaan palautetta esittämistäni näkökohdista. Samoin olen kiinnostunut kokemuksistanne ja menestystarinoistanne sovellusten tietoturvallisuuden parantamisessa. Tietoturvallisuuspiireissä saatuja kokemuksia jaetaan yleensä melko varovaisesti. Toivottavasti sovelluskehityksen ammattilaiset voivat vapaammin jakaa keskenään osaamistaan ja kokemuksiaan.

Kirjallisuutta

Ross Anderson: *Security Engineering*

Gary McGraw, John Viega: *Building Secure Software*

Howard, LeBlanc: *Writing Secure Code*

Graff, van Wyk: *Secure Coding: Principles & Practices*

Mark O'Neill et al.: *Web Services Security*

Jay Ramachandran: *Designing Security Architecture Solutions*

Bruce Schneier: *Secrets & Lies*
Whittaker, Thompson: *How to Break Software Security*

Aiheeseen liittyviä linkkejä http://www.iki.fi/japi/security.html#prog

Jari Pirhonen,
Tietoturvallisuuspäällikkö ja –konsultti,
AtBusiness Communications Oyj,
japi@atbusiness.com
http://wwwiki.fi/japi/

Reaktiivisesta proaktiiviseen - näkökanta tulevaisuuden tietoturvatyöhön

Arsi Heinonen,
Viestintävirasto

Kuluvan vuoden tietoturvakehitys on monella tapaa ollut edellisten vuosien kaltainen: verkkohyökkäykset ovat kasvaneet lukumääräisesti voimakkaasti, vakavia haavoittuvuuksia löydetään jatkuvasti kiihtyvällä tahdilla, haavoittuvuuksien julkistamista seuraa entistä nopeammin sen hyväksikäyttö... Samalla Internetin suosio on jatkuvasti kasvanut ja erityisesti viime vuosina kiinteällä laajakaistayhteydellä varustettujen kotikoneiden määrä on voimakkaasti lisääntynyt. Seurauksena on ollut huonosti ylläpidettyjen ja helposti haltuun otettavien järjestelmien voimakas lisääntyminen. Koska kunkin verkkoon kytketyn järjestelmän tietoturvallisuus on riippuvainen muiden verkkoon kytkettyjen järjestelmien tietoturvallisuudesta, joutuu toisten tietoturvan laiminlyönneistä kärsimään myös ne, jotka itse huolehtivat tietoturvastaan. Kun vielä tietoverkkojen ja järjestelmien toiminnan merkitys on noussut erittäin korkeaksi, on suorastaan hämmästyttävää kuinka vähillä vahingoilla ollaan toistaiseksi selvitty. Kuitenkin kuluvan vuoden tapaukset ovat osoittaneet, että monet uhkatekijät ovat toteutumassa. Esimerkkitapauksena voidaan mainita taannoiset roskapostien ja virusviestien aiheuttaneet ongelmat operaattoreiden sähköpostipalvelimille, josta aiheutti jopa viikon mittaisia viiveitä sähköpostin kulkuun. Tällä tapauksella oli ikäviä vaikutuksia erityisesti niihin pienyrityksiin, jotka olivat tottuneet hoitamaan asioitaan sähköpostitse, eivät pystyneet siirtymään vaihtoehtoisiin kommunikointimenetelmiin.

Tietoturvaotsikoissa ovat viimeaikoina olleet useat virus- ja matoepidemiat, mitkä ovat aiheuttaneet kotikäyttäjien lisäksi monissa organisaatiossakin ongelmia. Näitä haittaohjelmaepidemioita pidetään usein tietoturvaongelmien jäävuorenhuippuna; Se on pieni osa tietoturvaongelmakokonaisuudesta, mikä pystytään havaitsemaan. Paljon julkisuutta saanneilla uhkatekijöillä, joiden aiheuttamat ongelmat pystytään myös selkeästi näkemään, vaikuttavat siihen, millä tavoin ja millä hankinnoilla tietoturvallisuutta parannetaan. Niinpä silloin tällöin kohtaa henkilöitä, joille tietoturvallisuus on muotoutunut käsitteeksi virustorjunta. Vaikka virustorjuntaohjelmistot ovat merkittävässä roolissa yhtenä osatekijänä luotaessa syvää puolustusta, eivät ne ole ratkaisu edes tulevaisuuden haittaohjelmilta suojautumiseen: nopeasti leviävät verkkomadot kykenevät saastuttamaan käytännössä kaikki Internetin järjestelmät paljon nopeammin kuin virustorjuntaohjelmistoja valmistavat yritykset pystyvät tarjoamaan päivityksen viruskuvaustietokantaan. Esimerkiksi Slammer-mato saastutti 90% haavoittuvista verkkoon kytketyistä järjestelmistä 10 minuutissa.

Haavoittuvien ohjelmistojen päivittäminen on noussut yhä merkittävämpään rooliin tietoturvan hallinnan kannalta – paitsi suojauduttaessa verkkomadoilta, myös ennen kaikkea niiltä hyökkäyksiltä, joita ei useinkaan havaita. Kuluvan vuoden pahimmilta verkkomatoepidemioilta, Slammerilta ja Lovsanilta, oltaisiin vältytty jos haavoittuvat ohjelmistot olisivat olleet päivitetty. Slammerin hyväksikäyttämään MS SQL Server- haavoittuvuuteen oli korjaus ollut saatavilla useita kuukausia, Lovsanin hyväksikäyttämän Microsoft RPC/DCOM haavoittuvuuden paikkaamiseenkin oli aikaa 7 viikkoa. On kuitenkin huomattava, ettei haavoittuvia ohjelmistoja paikata haittaohjelmien takia – esimerkiksi molempia em. matoepidemioita edelsi haavoittuvuuksien erittäin aktiivinen hyväksikäyttö. Monissa tapauksissa huomattavasti suuremmat vahingot aiheutui ennen haittaohjelman ilmestymistä tapahtuneista kohdistetuista tunkeutumisista, joissa hyväksikäytettiin samoja haavoittuvuuksia kuin mitä em. haittaohjelmat hyväksikäytti.

Herää kysymys, miksi haavoittuvia järjestelmiä ei päivitetä. Eikö ylläpidolla ole riittävästi tietoa haavoittuvuuksista ja haavoittuvien ohjelmistojen päivittämisen merkityksestä? Koska verkkoon kytketyt koneet koostuvat varsin kirjavasta joukosta, kotikoneista ja pienyrityksen järjestelmistä aina supertietokoneisiin, vaihtelee

myös ylläpitäjien osaamistaso saman skaalan mukaisesti. CERT-FI:n tärkeimpiin tehtäviin kuuluukin nostaa ylläpitäjien tietoturvatietämystä neuvomalla ja ohjeistamalla sekä ennen kaikkea aktiivisesti tiedottamalla ajankohtaisista tietoturvauhista. Toisaalta, vaikka ylläpitohenkilöstön tietoturvaosaamisessa on keskimäärin runsaasti parantamisen varaa, on ensiarvoisen tärkeää, että organisaatioiden johdolla on riittävä näkemys tietoturvan merkityksestä. Organisaatioiden tietoturvaa voidaan ylläpitää ja kehittää ainoastaan johdon tuella – vain näin saadaan riittävät resurssit ylläpidolle, jotta järjestelmien toiminnallisuuksista huolehtimisen lisäksi voidaan keskittyä myös tietoturvallisuuden parantamiseen ja tarvittaviin proaktiivisiin tietoturvatoimenpiteisiin.

Kun vakavia haavoittuvuuksia löytyy yhä kiihtyvällä tahdilla ja samaan aikaan ylläpidon resursseja jopa kiristetään, on tietojärjestelmien ajallaan päivittämisestä tullut monissa yrityksissä ylivoimainen tehtävä. Oman haasteensa päivittämiseen tuo haavoittuvuuksien julkistamista entistä nopeammin seuraava hyväksikäyttö, mikä on tehnyt paikkausajoista erittäin lyhyen. Ylläpito on joutunut lähes sietämättömään tilanteeseen, jossa toiminta on vääjäämättä muuttumassa yhä enemmän reaktiiviseksi toiminnaksi.

Vaikka tietoturvaongelmat johtuvat monesta eri tekijästä ja vaikka käyttäjät ovat edelleen usein se heikoin lenkki, juontaa varsin moni tietoturvaongelma juurensa ohjelmistohaavoittuvuuksista. Jos nykyinen meno jatkuu, lisääntyy haavoittuvuuksien määrä vääjäämättä ohjelmistojen koon kasvaessa ja monimutkaisuuden lisääntyessä. Jotta tietoturvatyö ei olisi jatkuvaa tuulimyllyjä vastaan taistelua, sopii toivoa, että tietoturvallisuus otetaan tulevaisuudessa nykyistä paremmin huomioon ohjelmistokehityksessä. Tuloksien saavuttamiseksi toivoisi ohjelmistojen kehitykseen osallistuvilta erilaista näkemystä ja asennetta ohjelmistojen turvallisuuteen ylimääräisten ominaisuuksien ja toiminnallisuuksien sijaan. Sitä näkemystä ja asennetta pitäisi löytyä myös ohjelmistoja tai järjestelmiä hankkivilta asiakkailta - tietoturvallisuus kun ei nykyään kovin usein tunnu olevan merkittävä tekijä ohjelmistoa tai järjestelmää hankittaessa.

Aina silloin tällöin tulee mieleen, miksi tietoturvanäkemys ja asenne on usein puutteellista myös hyvinkin teknisesti suuntautuneilla henkilöillä, kuten ohjelmistokehitykseen osallistuvilla? On totta, että ohjelmistojen tietoturvallisuus on näkymätön (silloin kun se toimii) ja siksi vaikea mieltää tärkeäksi tekijäksi, kun taas uudet toiminnallisuudet ja lisäominaisuudet tuntuvat todellisilta aikaansaannoksilta, vaikka ne olisivatkin vähemmän tarpeellisia. Myös ohjelmistojen laadunvarmistuksessa keskitytään poikkeuksetta ainoastaan toiminnallisuuden testaamiseen, eikä ohjelmistojen turvallisuutta huomioida riittävästi laadunvarmistuksessa. Itse uskon, että tietoturvanäkemyksen puute juontaa juonensa mitä suuremmassa määrin opituista malleista; esimerkiksi voidaan esittää kysymys, kuinka monta ohjelmistojen turvallisuuteen painottuvaa kurssia suomalaisista yliopistoista löytyy? Tai edes maailmalta? Entä kuinka monella ohjelmointikurssilla huomioidaan turvallinen ohjelmointi ja sen merkitys pelkän toiminnallisuuden sijaan? Uusien suojautumismenetelmien ja tunkeutumisen havaitsemistekniikoihin kehittämisen ja käyttöönoton lisäksi olisi hyvä kiinnittää huomiota nykyistä enemmän ongelmien ytimeen.

Lähteet

[1] Arsi Heinonen, Teemupekka Virtanen, Ronja Addams-Moring. *We are Running What? - Why the Slapper Worm was able to Spread to Finland*. 2nd European Conference on Information Warfare and Security, Reading, 30.6.-1.7.2003, ISBN 0-9544577-0-6, MCIL, pp.339-348, UK, 2003

[2] CERT/CC: *Overview of Attack Trends*. CERT/CC. http://www.cert.org/archive/pdf/attack_trends.pdf.

[3] D. Moore etc. *The Spread of the Sapphire/Slammer Worm.* http://www.cs.berkeley.edu/~nweaver/sapphire/

[4] CERT-FI. *Microsoft RPC/DCOM -haavoittuvuutta hyväksikäyttävä Lovsan-haittaohjelma leviää,* CERT-FI varoitus 52/2003, 12.8.2003. http://www.ficora.fi/suomi/tietoturva/varoitukset/varoitus-2003-52.htm

[5] John Viega, Gary McGraw. *Building Secure Software How to Avoid Security Problems the Right Way.* ISBN 0-201-72152-X, Addison-Wesley, 2001.

Arsi Heinonen,
Tietoturva-asiantuntija,
Viestintävirasto / CERT-FI

CERT-FI

CERT-toiminnassa keskitytään tietoturvaloukkaustilanteiden ennaltaehkäisyyn, niiden havaitsemiseen ja selvittämiseen. CERT-lyhenne tulee sanoista Computer Emergency Response Team. Viestintäviraston CERT-FI on Suomen kansallinen CERT-organisaatio, jonka asiakkaisiin kuuluu kaikki suomalaiset organisaatiot ja yritykset sekä yksityiset kansalaiset. Lisätietoja CERT-FI:stä ja sen tehtävistä on saatavilla osoitteesta http://www.cert.fi.

Ennaltaehkäisevästä tietoturvatyöstä CERT-FI huolehtii erityisesti aktiivisella tiedottamisella. CERT-FI julkaisee varoituksia ajankohtaisista tietoturvauhista, sekä yleisluonteisia, lähinnä kotikäyttäjille tarkoitettuja ohjeita. CERT-FI:n varoitukset ja ohjeet julkaistaan CERT-FI:n WWW-sivuilla, ja niitä on mahdollista tilata sähköpostitse liittymällä varoitusten ja ohjeiden jakelulistalle. Lisätietoja postituslistoille liittymisestä saa osoitteesta: http://www.ficora.fi/suomi/tietoturva/postituslista.htm

CERT-FI:hin kannattaa ottaa yhteyttä aina kun organisaatioon kohdistuu laajamittainen palvelunestohyökkäys, tietojärjestelmiin tai tietoverkkoihin on tunkeuduttu tai tunkeutumista epäillään. CERT-FI antaa asiantuntija-apua myös ennaltaehkäiseviin toimenpiteisiin liittyen. Erityisen tärkeää on ottaa yhteyttä CERT-FI:hin aina, kun havaitaan uuden tyyppinen hyökkäystapa tai on syytä epäillä uuden julkaisemattoman haavoittuvuuden hyväksikäyttöä.

CERT-FI:n sähköpostiosoite on cert@ficora.fi ja päivystysnumero on (09) 6966 510. CERT-FI:n tarjoamat palvelut ovat maksuttomia ja CERT-FI käsittelee sille ilmoitettuja tapauksia luottamuksellisesti.

Muistathan käydä tutustumassa
Systeemityöyhdistys SYTYKE ry:n kotisivuihin:

www.pcuf.fi/sytyke

Tietoturvan merkitys ja kehittäminen: Voiko metsän vielä nähdä puilta?

Antti Hemminki,
Secproof

Tietoturvan kehittäminen

Tietoturvasta on tullut käsite, johon jokainen meistä törmää jollakin tavalla joka ainoa päivä. Yhtään sanomalehteä ei voi avata, harvaa uutista seurata, tai edes teksti-tv:tä selailla ilman viittausta johonkin ajankohtaiseen tietoturvakysymykseen.

Tietoturvan kehittämisen yksi este kuitenkin piilee nimenomaisesti tässä osittain vääränlaisessa arkipäiväistymisessä. Ajattelumallimme korostavat yksittäisiä, usein tietoteknisesti rajattuja ongelmia, kuten yksittäisten järjestelmien haavoittuvuuksia ja uusimpia verkkomatoja. Huomattavan harvassa ovat ne ympäristöt, joissa tietoturvan kehittäminen lähtee esimerkiksi organisaation toiminnasta, tiedon ja tietosisällön merkityksen määrittämisestä ja korostamisesta, riskinhallintamallien rakentamisesta ja hyödyntämisestä, yrityksen prosessien optimoinnista.

Tämän artikkelin ensimmäisenä tavoitteena on valittuihin esimerkkeihin viitaten kuvata tietoturvan haasteiden monimuotoisuutta. Artikkelin toisena tavoitteena on tarjota kriittistä näkemystä tietoturvan todelliselle kehittämiselle. Kirjoittajana toivon, että artikkeli ennemminkin herättää oikeita kysymyksiä kuin antaa vastauksia. Itsestäänselvyyksien ajan pitää olla ohitse.

Artikkelin kirjoittaja Antti Hemminki (antti.hemminki@secproof.com) on tunnettu ja arvostettu tietoturvan luenoitsija, kehittäjä ja valmentaja. Antti Hemminki omaa erittäin laajan kokemuksen sekä liikeyritysten että julkishallinnon toimeksiannoista, kansallisesti ja kansainvälisesti.

Tekniset haasteet

Kyllä, tekniikka on tärkeä osa modernin organisaation tietoturvaa. Teknisen tietoturvan kehittämiseksi yritykset ovat investoineet esimerkiksi seuraaviin ratkaisuihin: Palomuurit, todennusratkaisut, virustorjuntajärjestelmät, salausohjelmistot. Valitettavasti tämäkin vuosi on konkreettisesti osoittanut, että tekniikka ei ole riittänyt. Osuvathan hyökkäykset ja virukset toistuvasti kohteisiin, jotka uhrien mielestä olivat turvallisesti ylläpidetyn palomuurin takana.

Tietoturvan tekniset haasteet voidaan periaatteessa yksinkertaistaa muutamaan lauseeseen:

- Huolehdi siitä, että ainoastaan oikeat käyttäjät pääsevät järjestelmiin (todennus).
- Huolehdi siitä, että käyttäjien roolit vastaavat heidän tarpeitaan (valtuutus).
- Huolehdi siitä, että tiedät mitä järjestelmissäsi oikeasti tapahtui (seuranta).
- Huolehdi siitä, että tietosi ja järjestelmäsi ovat aina ajan tasalla (päivitykset).

Koska todellisuudessa jokin näistä periaatetason vaatimuksista pettää jo kustannusseurannan vuoksi, niin teknistä haastelistaa pitää välttämättä laajentaa esimerkiksi näin:

- Huolehdi siitä, että tiedät milloin ryhtyä poikkeaviin toimenpiteisiin (tarkennettu seuranta).
- Huolehdi siitä, että selviät jokaisesta poikkeustilanteesta oikein (palautuminen).

Listamme on tietysti yksinkertaistettu, mutta kattaa useimmat oleelliset kysymykset ja nimenomaan nykypäivän tiukimmat haasteet. Nämä haasteet pitää ymmärtää syvemmin.

Ensimmäinen vaatimus (todennus) on kenties oleellisin osa teknistä tietoturvaa. Ratkaisujen tavoitteena ei saisi olla pelkästään “pahojen pitäminen ulkona”, vaan ensisijaisesti “hyvien päästäminen sisälle”. Palomuuri jota ei edellä vahva todennus jättää armottomasti aukon, sillä luvalliseksi luultua, toivottua tai väärin tunnistettua yhteyttä voidaan käyttää estottomasti väärin. Juuri tämän vuoksi on ihmeteltävä, että vielä nykypäivänä löytyy palomuureja, joiden sääntölista sallii esimerkiksi kolmansien osapuolten yhteydet pelkän IP-osoitteen perusteella. Ja jos siinä palomuurissa on vapaan selailun salliva avaus, niin hyökkäyskin on vapaasti sallittu kunhan hyökkääjä vain muistaa käyttää pelkkää selausprotokollaa, tai vain osaa tunneloida taitavasti.

Tiukan todennuksen vaatimuksen pitää tietysti ulottua kaikkialle, erityisesti sisäverkon järjestelmiin ja sovelluksiin. Fyysinen kulunvalvonta on parhainta silloin, kun sallitut ovat avautuvat helposti oikeille henkilöille, mutta eivät koskaan väärille henkilöille. Samankaltaisen ajattelun pitää ulottua yhtä lailla tietoliikenteeseen ja edelleen kaikkiin tietojärjestelmiin. Mikäli todennus ei ole tarkkaa, ei roolittamiseenkaan voi luottaa – sitä ei voi edes toteuttaa.

Roolitus on erittäin tärkeätä kaikkialla, ja siihen on kiinnitettävä erityistä huomiota monimuotoisissa ympäristöissä. Järjestelmien pitää sallia ja tarjota vain se käyttö, mikä on organisaation toiminnan kannalta oleellista. Kirjanpitäjällä ei saa olla tilintarkastajien oikeuksia, pelkän http-palvelimen ei tarvitse pyörittää ftp-prosesseja, eikä sen tällä hetkellä kuuluisan RPC-portin tarvitse olla auki jos liiketoiminta ei sitä vaadi. Tätä logiikkaa noudattaen yritys huomaa, että järjestelmät ovat paitsi turvallisia niin myös tehokkaita, koska resursseja ei kuormiteta epäoleellisella roskalla. Toisin sanoen, teknisen suorituskyvyn optimointi ja tietoturva eivät ole toisiaan poissulkevia vaihtoehtoja vaan parhaimmillaan päinvastoin. Tietoturva on tehokkuutta.

Järjestelmien seuranta on oikeasti hankala haaste jo teknisesti: Miten toteuttaa ja järjestää kustannustehokkaasti edes verkon- ja järjestelmienvalvonta ja lokitietojen analysointi? Viimeistään tässä vaiheessa teknistä työtä huomataan, että oikea ratkaisu perustuu prosessien optimointiin, eikä oikeaa ratkaisua voida aloittaa puhtaasti teknisestä kehittämisestä. Valtavan informaation ja disinformaation muodostaman tilannekuvan hahmottaminen perustuu liiketoiminnan ja riippuvuussuhteiden ymmärtämiseen. Ja tämä ei enää ole pelkkä tekninen kyky.

Lähes kaikki tahot ovat viime kuukausina toistuvasti korostaneet ajantasaisten päivitysten merkitystä. Hyvin harva taho on kuitenkin valmis kantamaan teknisestä päivittämisestä todellista vastuuta, koska aidossa tuotantoympäristössä päivityksiä ei yksinkertaisesti voi tehdä ilman laadukasta testaamista ja varmentamista. Käyttöjärjestelmän päivittäminen voi sammuttaa sovelluksen, tietokannan päivittäminen voi sekoittaa esimerkiksi http-kutsujen rajapinnan, virustorjuntapäivitystä ei ehkä olekaan vielä saatavana, ja päivitettäviä järjestelmiä on liikaa. Kaikki tämä esitettynä vain lyhyenä listana, jokainen "sysadmin" keksii kymmeniä lisäsyitä.

Edellä kuvattu päivitysten mahdottomuus ei kuitenkaan saa antaa tekosyytä päivitysten välttämiseksi. Päinvastoin. Koska päivitysprosessi on hankala, se pitää suunnitella sitäkin tarkemmin! Edelleen, milloin päivittäminen on ns. mahdotonta, organisaatiolla pitää olla valmiiksi mietityt toimintasuunnitelmat miten toimitaan kohonneen riskitason aikana. Ja tämä edellyttää nimenomaisesti kykyä toimia poikkeustilanteissa, kykyä toipua poikkeustilanteista ja kykyä jatkaa toimintaa myös niissä tilanteissa kun kaikki lopulta menee pieleen ja järjestelmät kaatuvat.

Kaiken kaikkiaan, yritysten teknisen valmistautumisen tulee kattaa kaikki "mitä jos tämä tapahtuu" tilanteet, jotta jälkikäteen ei tarvitse miettiä "voi kunpa me olisimme sen tehneet". Teknisen epävarmuuden hallinta edellyttää kokonaisvaltaista tarttumista haasteisiin, mikä pelkästään teknisesti tarkoittaa esimerkiksi erillisten ratkaisujen integroimista toisiinsa sopivien rajapintojen kautta. Teknisessä tietoturvassa pitää olla topologista leveyttä ja syvyyttä, mutta saman aikaisesti keskitettyä hallintaa ja kontrollia. Ja kaiken takana on loppujen lopuksi se sovellus itsessään. Mikäli se sovellus ei ole sisäisesti rakennettu turvalliseksi, ei sen turvallisuutta voi rakentaa pelkästään ulkoisten paikkojen avulla. Salaus purkautuu sovelluksen rajapinnalla, palomuuri ei ymmärrä sovelluksen semanttista logiikkaa, todentaminen edeltää sovelluksen sisäistä roolitusta, madot kyllä tunkeutuvat myös sovellusten takaa löytyviin peruskiviin.

Tietoturvan tekniset haasteet voidaan siis poikkeuksetta osoittaa prosessihaasteiksi, ja jopa paljon syvällisemmiksi kysymyksiksi. Tietoturva on kokonaisuuteen sisäänrakennettu laatuparametri. Sitä ei voi rakentaa eikä kehittää erillisenä oliona.

Korkeammat haasteet

Teknisten haasteiden kautta olemme törmänneet tilanteeseen, jossa toteamme kehittämisen perustuvan prosesseihin. Mutta prosessithan liikuttavat ja ohjaavat ihmisiä ja ihmisten toimintaa, eli tietoturvan kehittämisen pitäisi tämän mukaan alkaa ihmisistä. Eiköhän asia olekin juuri näin.

Ihmiset ovat jokaisen järjestelmän suunnittelun ja rakentamisen takana, ja ihmiset myös hyödyntävät näitä järjestelmiä. Kokemusperäisesti esitän (Antti Hemminki) varsin tiukasti, että lähes poikkeuksetta niin kutsuttu "tekninen aukko" johtuu heikkouksista tietoturvan tavoitteiden asettamisessa, tietoturvaan liittyvien vastuiden ja toimenkuvien määrittämisessä, yrityksen prosessien ohjauksessa, yrityksen ja sen työntekijöiden kompetenssissa tai peräti heikkouksista, joihin yritys ei voi suoraan vaikuttaa koska ne löytyvätkin yrityksen sidosryhmistä. Kärkevimmät esimerkit viimeksimainituista olen (Antti Hemminki) kohdannut tilanteissa, joissa yritys on ulkoistanut toimintoja luottaen kolmanteen osapuoleen, mutta tällä ei sittenkään ollut todellista tietoturvaosaamista. Vastuuta ja mainetta ei valitettavasti voi ulkoistaa, vaikka niin haluaisimme.

Kompetenssiin ja sen kehittämiseen liittyvät erityiskysymykset ovat psykologia ja sosiologia. Monissa tapauksissa tietoturvan kehittäminen ei ole onnistunut tavoitteiden mukaisesti, koska ohjelmien vaikutukset henkilöstön todelliseen toimintaan jäävät vajavaisiksi. Näissä tapauksissa yritykset ovat jopa toteuttaneet laajoja "Security Awareness" ohjelmia, mutta ihmisten jokapäiväinen toiminta ei ole sittenkään muuttunut. Miksi yksilö muuttaisi toimintaansa, jos hän ei koe muutosta itselleen tärkeäksi? Muutos on aina perusteltava erittäin konkreettisesti, ja muutoksen valvonta on liitettävä kiinteäksi osaksi kaikkea valvontaa. Tästä johtopäätöksestä seuraa väistämättä se, että tietoturva on liitettävä osaksi yrityksen kaikkia ohjausjärjestelmiä.

Tietoturvan liittäminen yrityksen ohjausjärjestelmiin kuulostaa ensin turhankin kunnianhimoiselta haasteelta, sillä eihän tietoturva nyt voi vaikuttaa kaikkeen liiketoimintaan. Tämä kritiikki on ehdottomasti aiheellinen, mutta onko se tällä tavalla esitetty väärästä suunnasta?

Tietoturvan kehittäjien (eli meidän itsemme) tulee olla nykyistä nöyrempiä ja jatkuvasti etsiä olemassa olonsa oikeutusta liiketoiminnasta. Vain tällä tavalla voidaan saavuttaa yhteinen keskustelukieli kaikkien organisaation osien kanssa, jonka jälkeen tietoturvan liittäminen kaikkiin ohjausjärjestelmiin ei enää kuulostakaan kunnianhimoiselta vaan käytännönläheiseltä.

Koska henkilöstöä varten on olemassa perehdyttämis- ja koulutusvaatimukset, miksi tietoturvaa ei liitettäisi muutamaksi osaksi tätä jo olemassa olevaa rakennetta? Koska osastolla jo on prosessikuvaukset laatukansiossa, miksi tietoturvavaatimuksia ei kirjattaisi muutamaksi osaksi täsmentämään näitä prosessikuvauksia? Kaiken kaikkiaan, miksi tietoturvaa ei vain liitettäisi osaksi jokapäiväistä toimintaa, eihän tietoturva ole mitään salatiede vaan täysin normaali, tehokkuutta ja rationaalisuutta korostava ajatusmalli? Niinpä niin!

Tietoturvan haasteet ovat siis todellisuudessa vielä prosessihaasteitakin korkeammalla. Tietoturvan tulee olla kiinteä osa organisaation toimintaa, eikä missään tapauksessa erillinen olio.

Tietoturva ja liiketoiminta

Kaiken edellä esitetyn perusteella provoisoiva tiivistelmä jatkopohdintojen pohjaksi:

- Tietoturva on kiinteä osa organisaation riskinhallintaa ja laatutoimintaa. Tämän vuoksi sen tavoitteista ja toteutumisesta vastaa ainakin viime kädessää liiketoiminnasta vastuussa oleva johto. Tietohallinto ei yleensä ole oikea paikka tavoitteiden määrittämiseen, joskin se voi auttaa merkittävästi tietyissä toteutuksissa.
- Tietoturvan tavoitteita ei nykymaailmassa voi / saa määrittää itsekeskeisesti. Tavoitteiden asettamisessa on huomioitava kaikki vaikuttavat sidosryhmät. Viime kädessä, tietoturvatason määrää ainoastaan asiakas, tai jopa oman toiminnan kannalta kriittinen toimittaja.
- Tietoturvan tavoitteiden saavuttamista on seurattava. Tämä tapahtuu parhaiten siten, että seuranta liitetään osaksi organisaation muita seurantajärjestelmiä, myös esimerkiksi paljon puhuttuja "Balanced Scorecard" ratkaisuja. Siis: Myös henkilöstöhallinnon tuella on päästävä siihen, että tietoturvasta tulee virallinen ja konkreettinen kannustuselementti.
- Tietoturvan saavuttaminen edellyttää tarkkoja ja kontrolloituja prosesseja. Nämä prosessit perustuvat julkaistuihin tavoitteisiin (esimerkiksi organisaation tietoturvapolitiikkaan), ja niiden jatkuva kehittäminen on velvoitettava myös ja ennen kaikkea johtajille ja esimiehille.
- Kaikkien henkilöstöhallinnon rutiinien, mukaanlukien johtajien ja esimiesten velvoittamisen, on tähdättävä oikeiden toimintatapojen noudattamiseen ja näiden tapojen jatkuvaan kehittämiseen. Tietoturvatietoisuus ei riitä, kaikkien on myös oikeasti työskenneltävä oikein.
- Myös teknisen seurannan ja kehittämisen tulee olla jatkuvaa. Organisaation on kuitenkin ensin laitettava hallinnolliset rakenteensa kuntoon, koska teknisten ratkaisujen perusteleminen on liiketoiminnallisen kysymys. Vain implementointi on tekninen kysymys.
- Organisaatio voi sanoa olevansa tietoturvatasoltaan vahva, kun se kriisin iskiessä pystyy rehellisesti peiliin katsoessa toteamaan: "Tämä riski tunnistetiin ja otettiin tietoisesti. Nyt vain toivutaan kuten ennalta on suunniteltu ja harjoiteltu". Riskit ovat aina osa liiketoimintaa!

Tietoturva on siis kunnossa, kun siitä ei enää tarvitse puhua. Se on kiinteä osa organisaatiota. Tänä päivänä näyttää vain siltä, että huomisen tilanne on toistuvasti eilistä epävarmempi.

Tietoturva vaatii nöyryyttä.

Antti Hemminki,
M.Sc. (Eng),
Senior Partner, Secproof,
antti.hemminki@secproof.com

Laivaseminaari 2003:

Mallinnus ja menetelmät

Petteri Holländer,
SysOpen Oyj

Sytyke ry:n perinteinen laivaseminaari järjestettiin tänä vuonna 2.-4. syyskuuta aiheenaan mallinnus ja menetelmät. Loppuunmyydyn seminaarin ohjelmasta vastasivat tasokkaat esiintyjät eri tahoilta sekä tietenkin ansiokkaasti käytännön järjestelyt junaillut seminaaritoimikunta.

"Tärkeintä on se, mitä päissämme tapahtuu"

Tiistai-iltapäivän 2.9.2003 ohjelmassa oli 5 kpl esityksiä ennen buffet-illallista. Etukäteen oli tiedossa se, että illalliseen liittyi jokin yhteinen kisailu, ja joillekin oli jo tullut mieleen ajatus, että kisailu liittyisi päivän ohjelmaan, joten tarkkaavaisuus oli huipussaan alusta alkaen. Helena Venäläisen avattua seminaarin pääsi varsinainen ohjelma käyntiin seuraavin aihein:

- Mallinnus RUP:ssa, Jouko Poutanen, Rational Software
- Mallinnus keinona ohjelmistotyön tuottavuuden nostamiseen, Pekka Kähkipuro, SysOpen
- Informaation mallintaminen, Esko Marjomaa, Joensuun yliopisto
- Mitä uutta UML 2.0 tuo tullessaan? Tarja Raussi, Tieturin systeemityöosasto
- Perinteinen oliomenetelmä ketteräksi, Heini Holopainen ja Eija Hamina-Mäki, Tietoenator
- MDA, Henrik Jondell, Borland
- Määrittelymallit, Markku Niemi, STTF
- Systeemityön vallankumous - toimitusjohtaja puuttuu asiaan! Claus Günther, ChangeWare Group

Kuva 1: Helena Venäläinen avasi seminaarin.

"Omaisuus siirtyy lähdekoodista malliin"

Jouko Poutanen (Rational Software) esitteli mallinnusta RUP (Rational Unified Process) buffet-pöydän muodossa: tarjolla on systeemityön parhaita käytäntöjä koeteltujen reseptien mukaan valmistettuna. Poutanen korosti korkean tason mallinnusta ja arkkitehtuurikeskeisyyttä, sekä tulevaisuuden kehityssuuntaa, jossa mallipohjaisen kehittämisen (Model Driven Development) myötä "omaisuus siirtyy lähdekoodista malliin".

Tuottavuuden visaisten kysymysten pariin meitä johdatti Pekka Kähkipuro (SysOpen), jonka mukaan tällä hetkellä vaaditaan huimaavaa suorituskykyä: projektit, jotka ennen tehtiin 2v aikataululla pitäisi saada valmiiksi 6kk:ssa. Mallien käyttäminen tai käyttämättömyys on Kähkipuron mukaan edelleenkin yleisesti ottaen ratkaisematon kysymys - onko guruista kompleksissa hankkeissa enemmän

Kuva 2: Mallintaminen lumosi osallistujat.

haittaa vai hyötyä - ja tuottavuus pysyvä haaste.

"Oletetaan pyöreä lehmä.."

Informaation mallintaminen oli monille pysähdyttävä kokemus - Esko Marjomaan (Joensuun yliopisto) esitys poikkesi muista esityksistä tuomalla mukaan vankan teoreettisen näkökulman informaatioon. Erilainen esitys saikin mukavasti yleisön harmaat aivosolut liikkeelle ja keskustelua aiheesta. Tarkemmin aiheeseen voi tutustua esityksen pohjana olleesta artikkelista (Informaation mallintaminen, Systeemityö 3/2003, s.28).

UML 2.0:n saloja puolestaan esitteli Tarja Raussi (Tieturi), joka ammattilaisen otteella osasi kertoa mitä uutta on tulossa ja mitä vanhaa katoamassa. Samalla laiva lähti liikkelle, ja esimerkinomaisesti mallinnettiin hytin avainkortin toimintaa - tätä oppia kukin saattoi soveltaa heti tuoreeltaan. Raussi kertoi myös hieman taustoja UML:n standardointiprosessista, ja antoi vinkin, että vaikka UML2.0 ei vielä virallisesti ole ihan valmis, ei enää kannata opetella vanhempaa UML1.5 versiota.

"Ketteryys katoaa koon myötä"

Vaikka joku ehkä ehti jo kaivata illallispöytään siirtymistä, ottivat Heini Holopainen ja Eija Hamina-Mäki (TietoEnator) ohjat estradilla käsiinsä ja innostivat osallistujia ketterien menetelmien maailmaan. Aihe kirvoitti myös runsaasti keskustelua ja herätti intohimoja - näihin kysymyksiin palattiin varmasti monessa yrityksessä heti seminaarin jälkeen. Esittäjät painottivat sitä, että ketteryyteen liittyy paljon valintoja, ja sitämyöten vapautta ja vastuuta.

Pienen hengähdystauon jälkeen ilta jatkui illallisella, jonka aikana keskustelut osallistujien kesken pääsivät toden teolla vauhtiin. Ja lupailtu kisailu ruokailun päätteeksi tosiaan tarkisti tarkkaavaisuutta päivän esityksistä. Kaikki olivat kuitenkin selvästi olleet hyvin hereillä eikä paremmuutta pöytäkuntien kesken saatu selville - tosin tuloksia tarkastettaessa voittajaksi ilmoittauduttiin jo pistelaskun puolivälissä.

"Lämpötila 11 astetta ja sää puolipilvinen.."

Illan rientojen jälkeen aamulla laivan kuulutukset tulivat myös japaniksi. Tosiaankin, laivalla oli reilusti nousevan auringon maan kansalaisia, eikä kyseessä ollut kuuloharha. Tukholmaan tutustuminen isommissa ja pienemmissä ryhmissä kävi mukavasti, kaupungissa valmistauduttiin aktiivisesti tulevaan euro-kansanäänestykseen autuaan tietämättömänä tulevasta tragediasta.

"MDA on abstraktiotason nostamista"

Iltapäivän ohjelman käynnisti Borlandin Ruotsin organisaatiosta Henrik Jondell, jonka englanninkielinen esitys käsitteli MDA:ta (Model Driven Architecture) ja miten se taipuu tämänhetkisissä välineissä. Mahdollisuudet vastata muutokseen kasvavat, kun on mahdollista todeta, että malli on sama kuin koodi ja päinvastoin. Saimme myös pikaisen maailmanensi-illan Borlandin uudesta MDA-tuotteesta.

Markku Niemi (STTF) jatko ensi-ilta -teemaa Tietojärjestelmän hankinta -oppaan (lisätietoja esim. http://www.ttl-tori.fi/, TTL-tietoutta, Tuotteet) toisen version esittelyllä.

Kuva 3: Keskustelu jatkui aktiivisesti myös illallispöydässä.

Keskustelu kävi kiivaasti, kun huomattiin että systeemityöläistenkin keskuudessa käsitteet eivät ole yksiselitteisesti samanlaisina käytössä: käsitekaavio vs. luokkakaavio -taisteluun ei ratkaisua kuitenkaan saatu.

Laivan moottorien käynnistyminen keskeytti keskustelun ja muistutti aikatauluista. Seuraavana vuorosso oli seminaarin yllätysohjelmanumero, eli taukojumppa. Suuren maailman malliin Kati Ahlgrenin vetämänä se keräsi pisteet kaikilta ja sai varmasti veren kiertämään joka sopukassa ennen viimeistä esitystä.

"Jokainen uusi IT-järjestelmä tarkoittaa muutosta"

Liiketoimintanäkemystä ja liiketoiminnan vastuuta järjestelmien määrittelyssä (BDIT, Business Drives IT) valotti Claus Günther (ChangeWare Group). Uudet järjestelmät tuovat aina muutoksia prosesseihin, koulutukseen, laadunvarmistukseen, jne. Kokonaisvaltaisen prosessiajattelun ja sen myötä liiketoimintavetoisuuden tuominen kaikille ja kaikkialle tulee Güntherin mukaan muuttamaan systeemityön luonnetta, mm. valmisohjelmistoihin siirtymisen myötä.

Tuhdin seminaarin esitysten jälkeen iltaohjelma jatkui saunomisella ja illallisella. Onnistuneen seminaarin soveltaminen alkoi heti illallisen yhteydessä: miten tarjoilijoiden kovin sujuvalta näyttävää prosessia voitaisiin mallintaa tai voisimmeko kenties oppia jotain olennaista näkemästämme? Rentoa, mutta kuitenkin juhlavaa tunnelmaa jatkettiin vielä yhteislauluilla.

"Loistava seminaari!"

Aurinkoisen syyssään tervehtimänä saavuimme torstaina takaisin Helsinkiin, ja siirtyminen arjen aherruksiin saattoi alkaa. Seminaariin osallistujat tekevät seminaarin, ja tällä kertaa mielestäni seminaari toimi hienosti - siitä kiitos kaikille osallistujille. Kiitokset seminaarin onnistumisesta kuuluvat myös yhteistyökumppaneille ja näytteilleasettajille: Borland, ChangeWare Group, FinanssiData, Rational Software, STTF Oy, SysOpen Oyj, TietoEnator Oyj, Tieturi.

Seminaarin yhteydessä kerätty palaute osoitti samaa kuin tunnelma laivalla: esityksiin ja järjestelyihin oltiin tyytyväisiä, ja yhdessä mietittiin jo ensivuoden osallistumista, ohjelmaa ja aikatauluja. Muutamia poimintoja palautteesta: "Olin ensimmäistä kertaa mukana ja olin positiivisesti yllättynyt ohjelmasta. Hyviä luentoja", "Hyvä aihepiiri, kiva tavata/tutustua ihmisiin", "Voisiko vähentää esiintyjiä ja lisätä esitysten kestoa?". Toiveista huolimatta käytännöt ja kustannukset rajoittavat hieman järjestelyjä, esim. toisen päivän pidempi ohjelma ei onnistu, koska laivan konferenssitila on käytössä rajoitetusti. Ensi vuoden aiheiksi oli jo runsaasti toivomuksia, mm. tietoturva, arkkitehtuurit, projektikulttuurit ja ohjelmistoliiketoiminta. Siispä ruori kohti ensi vuotta - seminaarissa nähdään!

Petteri Holländer,
SysOpen Oyj

Toimintasuunnitelma 2004

Yleistä

Yhdistyksen tavoitteena on seurata tiiviisti systeemityön kehittymistä ja osallistua kehittämistyöhön sekä jakaa aiheeseen liittyvää ammatillista tietoutta jäsenistölle.

Yhdistyksen keskeiset toimintamuodot vuoden 2004 aikana ovat:

- Jäsenlehti, jossa käsitellään systeemityöhön liittyviä aiheita ja tiedotetaan jäsenistölle yhdistyksen ja liiton toiminnasta.
- Kerhotoiminta, joka jatkuvana toimintamuotona tarjoaa yhdistyksen jäsenille pysyvän mahdollisuuden käydä ammatillista keskustelua systeemityöalueen eri aiheista.
- Jäsentilaisuudet, joissa valittujen systeemityöhön liittyvien teemojen pohjalta yhdistyksen jäsenet voivat asiantuntijoiden kanssa keskustella ja vaihtaa mielipiteitään.
- Jäsenistön verkostoituminen, ammatillisen identiteetin ja asiantuntijuuden edistäminen.

Kerhojen, jäsentilaisuuksien ja lehtien teemat haetaan systeemityöhön liittyvistä ajankohtaisista aiheista.

Johtokunta tiedottaa vuonna 2004 pääasiallisesti Internetin, Tietotekniikan liiton tarjoamien jäsenyhdistysten tiedotuskanavien ja Systeemityölehden kautta. Tarvittaessa tehdään ja lähetetään jäsenkirjeitä.

Mikäli tilaisuuksia ilmenee, tehdään yhteistyötä Tietotekniikan liiton, sen muiden jäsenyhdistysten sekä vastaavien kotimaisten ja ulkomaisten systeemityöläheisten yhdistysten kanssa.

Nykyiset jäsenet pyritään säilyttämään ja kasvattamaan jäsenten määrää 50:llä vuoden 2004 aikana. Vuoden 2003 lokakuun lopussa jäsenmäärä oli 2101.

Jäsenlehti

Sytykeen keskeisin toimintamuoto on jäsenlehti Systeemityö, jonka sisältöä kootaan kerhoista ja alan ammattilaisilta.

V. 2004 ilmestyy neljä numeroa, ensimmäisen numeron teemana ”Terveydenhoidon tietojärjestelmät”.

Muita mahdollisia teemoja:

- Prosessit
- Systeemityön osaamisalueet

Lehteä toimitetaan ammattimaisen toimitusassistentin avulla ja talkoovoimin. Kullekin lehdelle nimetään toimituskunta, joka vastaa lehden toimittamisesta yhdessä päätoimittajan kanssa. Lehden tuottamiskulut pyritään pääosin peittämään ilmoitushankinnalla.

Yhdistyksen lehteä jaetaan pääosin vain omille jäsenille. Lehteä voi myöskin tilata Sytykkeen toimistosta irtonumeroina tai vuositilauksena.

Kerhotoiminta

Kerhot ovat yhdistyksen jatkuvaa jäsentoimintaa. Kullakin kerholla on nimetty vetäjä ja johtokunnan jäsenistä nimetty yhteyshenkilö. Kerhot määrittelevät toimintamuotonsa itse. Yhdistys antaa puitteet kerhojen toiminnalle.

Yhdistyksen kerhoina jatkavat

- Relaatiokantakerho: yhdyshenkilönä Pirkko Leivo.
- Testaus -kerho: yhdyshenkilönä Erkki Pöyhönen.
- Datanomit ja tradenomit -kerho: yhdyshenkilönä Minna Oksanen.
- JavaSIG -kerho: yhdyshenkilönä Simo Vuorinen

Tarpeen mukaan perustetaan muita uusia kerhoja.

Työryhmät

- Vuoden 2004 aikana jatketaan pysyväisluonteisen WEB -työryhmän toimintaa. Sen pääasiallisena tehtävänä on vastata yhdistyksen oman sivuston ylläpidosta ja jatkokehittämisestä.

Muita työryhmiä perustetaan tarpeen mukaan. Tällainen tarve saattaa olla TTL:n Ammattilaispäivien 2004 järjestämiseen osallistuminen.

Jäsentilaisuudet

Jäsenillat

Jäsenillat ovat maksuttomia koulutus- ja keskustelutilaisuuksia, joissa käsitellään ajankohtaisia systeemityön aiheita. Valitusta teemasta osallistujat voivat keskustella tehtyjen alustusten pohjalta. Jäseniltojen järjestelyistä vastaavat johtokunta ja kerhot. Vuoden 2004 aikana pyritään järjestämään 1 - 2 jäseniltaa.

Jäsenseminaari

Jo kuutena peräkkäisenä vuonna järjestetystä laivaseminaarista on muodostunut vuosittainen huipputapahtuma systeemityöläisille. Yhdistys tulee myös seuraavan toimintavuoden aikana järjestämään risteilyn jäsenilleen. Vuoden 2004 risteily pidetään saman kokoisena (75 hlöä) kuin edellisenkin vuoden.

Hallinto ja talous

Hallintorutiinit hoidetaan vuonna 2004 edelleen ulkopuolisella toimistopalveluyrityksellä.

Kirjanpitopalvelut ostetaan vuonna 2004 edelleen kirjanpitotoimistolta.

Vuonna 2004 saatavien jäsenmaksujen ja lehden ilmoitustulojen avulla rahoitetaan yhdistyksen toiminta, hallintorutiinit, jäsenillat ja osittain myös muut jäsentilaisuudet (risteily) sekä lehden kustantaminen. Tarkemmat suunnitelmat ilmenevät talousarviosta.

Hallitus

VVV-toiminta aluillaan!

Minna Oksanen

Mitä kirjaimet VVV tuovat mieleen? Ehei, ei ole kysymys painovirheestä vaan sytykkeen uudesta toimintamahdollisuudesta. rivinvaihto V= virkistys, V= vapaa-aika, V= verkostoituminen. Näistä kolmesta elementistä on tarkoitus rakentaa aktiivista ja mukavaa toimintaa sytykkeen jäsenistölle. VVV:n historia lähtee DTry:n mukaantulosta Sytykkeeseen. DT-kerhona olemme toimineet muutaman vuoden hioen konseptia vapaa-ajan toiminnan kehittämiseen. Nyt mielestämme konsepti alkaa olla kunnossa ja sen laajentaminen koko Sytykettä koskevaksi on tarkoituksenmukaista. Haastavien ja kiinnostavien työtehtäviemme vastapainoksi tarvitaan myös toisenlaista vapaa-ajan toimintaa - ei vain ammattiin sidottua ja mikäs sen parempaa, jos toiminta tapahtuu samanhenkisessä, mukavassa seurassa.

Kuva: Helena Nurminen ja Marko Pudas

Heti helmikuussa 2004 ad on tarkoitus järjestää yhteinen tapahtuma. Eilen 24.11. kokoonnuimme Helian tuttuun kahvioon ideoimaan tulevaa toimintaa. Melkoinen määrä ideoita syntyi ja meitä oli vasta paikalla 4. Entäpä, kun Sytykkeen keskustelusivujen kautta kaikki jäsenet pääsevät kertomaan, millainen toiminta kiinnostaisi? Lehden ilmestyessä työryhmäsivuston vierailualueelle tulee ilmestymään taulukko, johon voit arvioida ideoita ja ennen kaikkea pääset kertomaan omista ideoista. Näiden ideoiden pohjalta sitten jatketaan toiminnan kehittämistä. Vierailualueelle pääset rekisteröitymään www.sytyke.org-sivuston kautta kohdasta, jossa lukee Fle3 rekisteröintipyyntö.

Yksi eilisistä ideoista, joka ainakin omasta mielestäni kuulostaa varsin houkuttelevalta, on, että pidetään digikamerakurssi, jossa myös opitaan käsittelemään kuvia. Toinen idea ilmestyi tuolta Joensuun suunnasta. Voisimme osallistua sikäläisille tietojenkäsittelypäiville 24-26.5, jottei toiminta rajoittuisi vain Kehä III:n sisäpuolelle. Näiden ideoiden lisäksi sitten tarjolla voisi olla vaikkapa viinikurssia, yhteistä ulkoilua ja vaikka mitä kivaa.

Kippariksi on lupautunut Marko Pudas ja toki me muut vvv-kerho aktivistit olemme vahvasti tekemässä työtä yhteisten mukavien hetkien eteen.

VVV = voikaa vinkeästi vuodenvaihde!

Minna Oksanen,
hallituksen yhteyshenkilö