Tietoturvallisuuden ajankohtaiset haasteet

Mitä vaaditaan tietoturvaosaamiselta?

Turvallisuusalan neuvottelupäivät
7.5.2008

Jari Pirhonen
Turvallisuusjohtaja, CISSP, CISA
Samlink – www.samlink.fi

Samlinkin visiona on olla finanssialalla asiakaslähtöisin, kasvava ja arvostettu palvelukeskus integraattori- ja lisäarvopalveluissa

Asiakkaamme
- Aktia
- Finnvera
- Henkivakuutusyhtiö Duo
- Handelsbanken
- Paikallisosuuspankit
- Suomen Hypoteekkiyhdistys
- Säästöpankit

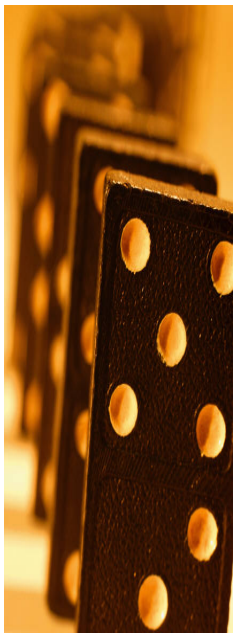
Palvelumme
- Peruspankkijärjestelmät
- Verkkopalvelut
- Vakuutusjärjestelmät
- Johdon ja viranomaisjärjestelmät
- Asiakashallintajärjestelmät
- Laskenta- ja taloushallinnon palvelut
- Infrastruktuuri…

Verkkomme
- Asiakaspankeissa työskentelee kaikkiaan reilut 3000 henkilöä
- Asiakaspankit palvelevat yhteensä vajaassa 500 konttorissa
- Asiakaspankeilla on tällä hetkellä 1-1,5 miljoonaa asiakasta,
- …joista yli puolet käyttää internet-pankkipalveluja

Lyhyesti meistä
- Pitkäaikainen finanssisektorin tuntemus muodostaa toiminnan perustan
- Toimitamme järjestelmiä ASP palveluna ja BPO palveluita (esim. kirjanpito)
- N. 300 asiantuntijaa + laaja kumppaniverkosto
- Liikevaihto 60,6 M€ vuonna 2007
- Paras AAA luottoluokitus

Sisältö

1. Tietoturvaan kohdistuu ristiriitaisia paineita
2. Tietoturva on turvallisuusalan suurin haaste nyt ja tulevaisuudessa
3. Tietoturva-ammattilaisilta vaaditaan laajaa osaamista
4. Avainasemassa on koko organisaation sitouttaminen tietoturvatyöhön



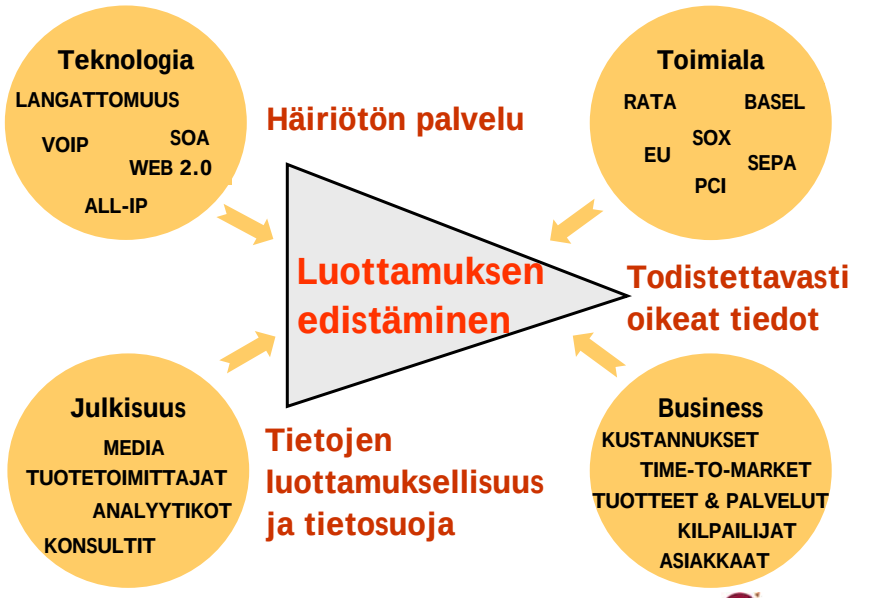
Samlink

Tietoturvaan kohdistuu ristiriitaisia paineita

The major difference between a thing that might go wrong and a thing that cannot possibly go wrong is that when a thing that cannot possibly go wrong goes wrong it usually turns out to be impossible to get at and repair.
-- Douglas Adams,
The Hitchhiker's Guide to the Galaxy

Samlink

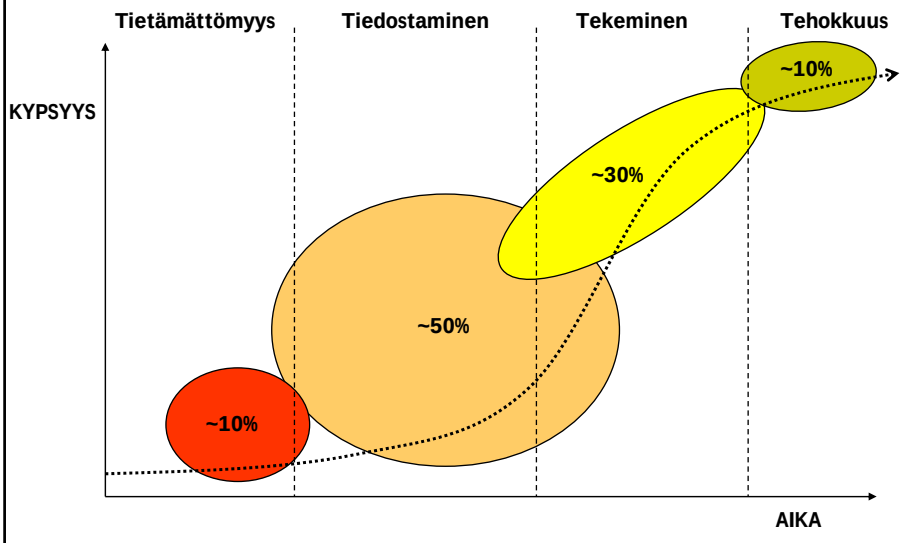
Tietoturvan ristiriitaiset vaatimukset



7.5.2008 Jari Pirhonen

Samlink

Arvio yritysten tietoturvakypsyydestä



7.5.2008 Jari Pirhonen **Lähde: Gartner ja Howard Schmidt puhe 29.4.08**

Samlink

Tietoturva on turvallisuusalan suurin haaste nyt ja tulevaisuudessa

Whenever someone tells you that there's a novel, easy, solution to security, it's either because they don't understand security or they're trying to sell you something that isn't going to work.
-- Marcus Ranum

Samlink

Uutisia 1998

Yritysten johto laiminlyö tietoturvaan panostamista

TAPIO KIVISTÖ
tapio.kivisto@sanoma.fi

Suomalaisten yritysten ja yhteisöjen johtajat eivät ole vielä paneutuneet riittävästi tietoturva-asioihin, arvioi keskusrikospoliisin tietotekniikkarikosryhmän päällikkö **Veli-Pekka Loikala**. Hän uskoo tietoturvan vaatimusten tulleen eteen niin nopeasti, ettei niitä ole huomattu ottaa osaksi johtamista.

– Ei voi ajatella, että turva-asiat laitetaan nyt kuntoon ja unohdetaan ne sitten pariksi vuodeksi. Tietoturva on jatkuva prosessi, toteaa Loikala.

Tietojärjestelmiin kohdistuvien hakkerointien, tietovarkauksien ja muiden vastaavien tapausten määrän arvioidaan kasvavan jatkuvasti, mutta poliisin tietoon tapauksia tulee edelleen harvakseltaan.

– Jutut ovat asianomistajarikoksia, eivätkä yritykset mielellään tee niistä ilmoituksia. Ilmeisesti imagon pelätään kärsivän. Asiat hoidetaan yrityksen sisällä, toteaa Loikala.

Yli 500 pk-yritystä otti yhteyttä supoon

Myös suojelupoliisi on kiinnittänyt huomiota varsinkin huipputeknologian pk-yritysten tietoturvallisuuteen. Nopeasti kasvavissa ja kansainvälistyvissä yrityksissä turva-asioihin ei selvästikään ehditä panostaa riittävästi.

Supo käynnisti viime talvena pk-yrityksille suunnatun hankkeen, jonka avulla viranomaiset pyrkivät paitsi jakamaan tietoa myös laskemaan yritysten yhteydenottokynnystä tietoturvaloukkauksissa. Tarvetta hankkeelle tuntui olevan, sillä peräti 500 pk-yritystä kiinnostui supon projektista.

Hankkeeseen liittyen supo on kevään ja syksyn aikana järjestänyt alueellisia infotilaisuuksia yrityksille.

Vastaanoton kerrotaan olleen myönteistä, ja monissa huipputeknologian yrityksissä tietoturvaan on vasta nyt kunnolla herätty.

Suuremmat yritykset ovat jo olvaltaneet

Keskusrikospoliisin Loikalan mukaan poliisi ei halua ryhtyä mestaroimaan yritysten käytännön tietoturvallisuutta.

– Asiat eivät ole enää niin yksinkertaisia kuin parikymmentä vuotta sitten. Silloin voitiin neuvoa, että ottakaa ura-avain niin turvallisuusasiat ovat kunnossa. Nyt kannattaa ottaa yhteyttä alan ammattilaisiin, sanoo Loikala.

Tietoturvaratkaisuja toimittavan Instrumentointi Oy:n osastonjohtaja **Esa Einola** arvioi, että varsinkin suurempien yritysten tietoisuus tietoturva-asioista on viime aikoina jo parantunut selvästi.

– Esimerkiksi pankkisektori, terveydenhuolto ja julkinen sektori laajemminkin ovat nyt liikkeellä. Samoin yleisemmin suuryritykset sekä informaatioteknologian ja tietotekniikan alueilla toimivat yritykset. Ne jotka haluavat liikutella tietoa verkossa ja tehdä bisnestä tiedon avulla, ymmärtävät turvan merkityksen, sanoo Einola.

Instrumentointi tarjoaa muun muassa johdon tietoturvakonsultointia sekä salaustekniikkaan liittyviä ratkaisuja.

Tampereella pääpaikkansa pitävän monialayrityksen tietoturvaliiketoiminnan liikevaihto nousee tänä vuonna 40 miljoonaan markkaan eli kaksinkertaistuu viime vuodesta.

– Tuotetoimitukset pystytään hoitamaan, mutta osaamista ja konsultointia ei pystytä myymään niin paljon kuin haluttaisiin. Kysyntää on nyt niin paljon, toteaa Einola.

TCB-hakkerin tutkinta valmistuu

■ Keskusrikospoliisi saa lähiviikkoina valmiiksi yli vuoden tutkinnassa olleen laajan hakkerointitapauksen.

Nimimerkkiä TCB (Trouble Came Back) käyttänyt nuori suomalaismies tunkeutui yli sadan yrityksen ja yhteisön tietojärjestelmiin toissa keväänä.

Hakkeri ei ilmeisesti vahingoittanut järjestelmiä, vaan tyytyi muun muassa lukemaan työntekijöiden sähköposteja.

Valtavan suuri tutkintapöytäkirja

– TCB-juttu osoittaa, että uloskoista tietoturvaa tulisi kehittää suomalaisyrityksissä ja -yhteisöissä, sanoo ylikomisario Veli-Pekka Loikala krp:stä.

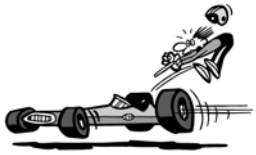
Jutun tutkinta on ollut monipolvinen vyyhti. Viimeisiä kuulemisia tehdään parhaillaan, jonka jälkeen juttu siirtyy syytehaitkintaan.

– Pelkkä tutkintapöytäkirjan johdantokin on 70 sivun mittainen, sanoo Loikala.

Samlink

Ajankohtaista 1998

- **Tietoturvallisuus etätyössä**
- **Tietoturvallisuus ja lainsäädäntö**
- **Palvelujen ulkoistaminen**
- **Teollisuusvakoilu**
- **Tietoturvatason arviointi**
- **Tietoturvallisuus järjestelmäkehityksessä**



lähde: Tietoturva ry historiikki, http://www.tietoturva.fi/downloads/TTRY_10v_historiikki.pdf

Samlink

Vuosisadan suunnitteluhaasteet


Make solar energy economical


Provide energy from fusion


Manage the nitrogen cycle


Provide access clean water


Advance health informatics


Engineer better medicines


Prevent nuclear terror


Secure cyberspace


Advance personalized learning

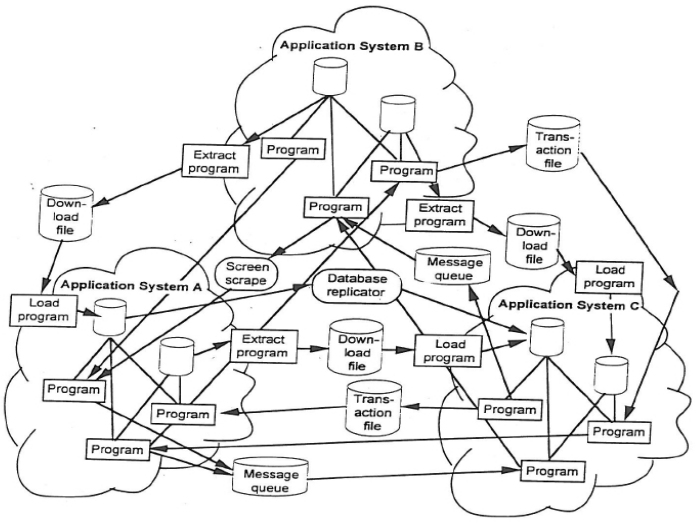

Engineer the to of scientific discovery

- **laitteiden, sovellusten, tiedon ja käyttäjien vahva todentaminen**
- **turvallisten sovellusten tuottaminen ja turvallisuuden todentaminen**
- **tietoliikenteen aitouden ja oikeellisuuden varmistaminen**
- **turvallisuuspoikkeamien välitön huomaaminen ja tilanteen korjaaminen**
- **kokonaisuuksien turvaaminen**
- **käytettävyyden huomiointi tietoturvaratkaisuissa**
- **lakien vaikutusten analysointi**
- **tutkimustyön edistäminen**

lähde: http://www.engineeringchallenges.org/

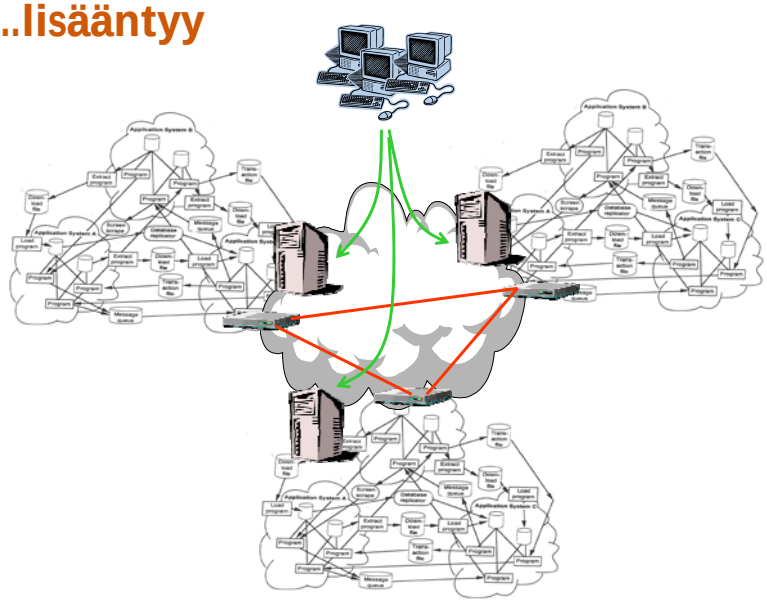
Samlink

Monimutkaisuus...



Samlink

...lisääntyy



Samlink

Selain riittää sovelluksen väärinkäyttöön

ENNEN

Linux + ohjelmointi

⇩

Windows + valmistyökalut

⇩

Web-selain + syötteen manipulointi

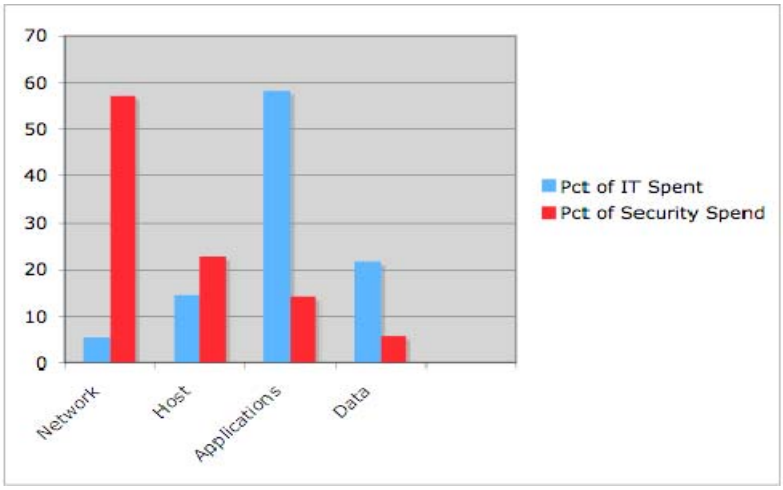
⇩

NYT

2.5.08 sivustolta xss.dy.fi löytyi yli 100 suomalaista haavoittuvaa web-sivustoa: Finnmatkat, Hkin yliopisto, Yle, Talentum, StoraEnso, TeliaSonera, Elisa, STT, Hätäkeskuslaitos, Helsingin Sanomat, Tampereen kaupunki, Tekla, Neste Oil, F-Secure, YIT, Endero,...

Samlink

Tietoturvabudjetti epäbalanssissa?



lähde: http://1raindrop.typepad.com/

Samlink

Tietoturvauhat 2010

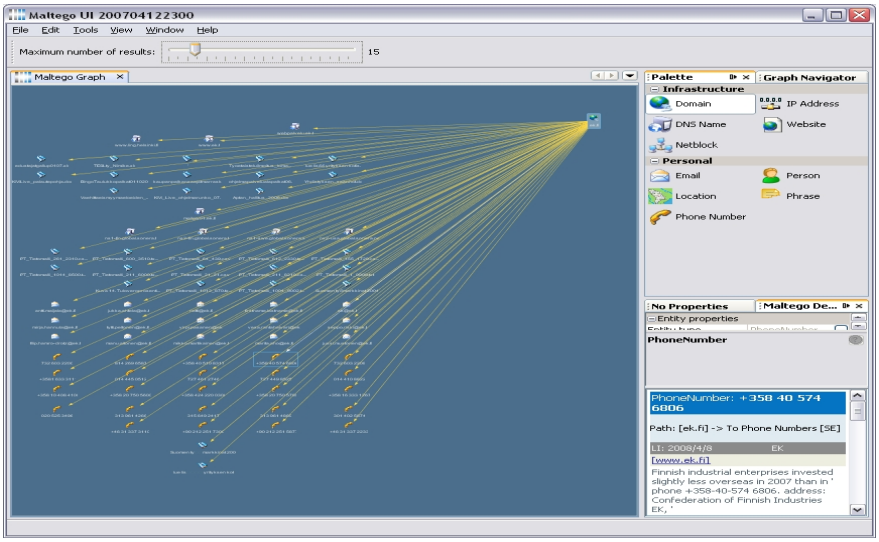
Poliittinen	Valtioiden välinen ja kaupallinen vakoilu lisääntyy. Kansalaisten luottamus valtion ja kaupallisten toimijoiden kykyyn suojata tietoja heikkenee. Kyberterrorismi, kuten kohdistetut palvelunestohyökkäykset kriittistä infrastruktuuria ja verkkopalveluja vastaan lisääntyvät
Juridinen	Immateriaalioikeuksiin liittyvä lainsäädäntö ja niiden toimeenpano tiukkenevat vastauksena vakoilutapauksiin ja piratismiin. Yleinen huoli yksityisyyden ja henkilötietojen suojasta vaikuttaa ko. alueen lainsäädäntöön. Yrityksiin vaikuttava lainsäädäntö lisääntyy Euroopassa (EuroSox). Elektroniseen todistusaineistoon käyttö oikeudenkäynneissä vaatii entistä suurempia ponnistuksia ja kustannuksia.
Taloudellinen	Hyvinvointivaltioiden talouskasvun hiipumista tasapainottaa kehittyvien kansantalouksien jatkuva kasvu, mutta hiipuminen vaikuttanee tietoturvabudjetteja alentavasti. Organisoitu rikollisuus vahvistuu.
Sosio-kulttuurinen	Työvoimassa tapahtuu merkittäviä demografisia ja kulttuurillisia muutoksia. Teknisesti erittäin osaava, mutta vähemmän riskitietoinen työvoima lisääntyy. Talouden laskusuhdanteen uhatessa työntekijöiden lojaliteetti työnantajaansa kohtaan vähenee.
Tekninen	Web 2.0 ja muut uudet teknologiat ovat laajassa käytössä. Panostus sovellusturvallisuuteen laimenee liiketoiminnan vaatiessa IT-osastoilta entistä nopeampaa muutoskykyä. Laitteiden kirjo ja yhteystarpeet kasvavat. Langattomasti käytettävien mobiili-laitteiden määrä kasvaa eksponentiaalisesti.

1. Kohdistetut, suunnitellut verkkorikokset
2. Mobiililaitteiden haittaohjelmat
3. Web 2.0 haavoittuvuudet
4. Vakoilu
5. Häiriöt kriittisessä infrastruktuurissa
6. Tiukentuva lainsäädäntö
7. Ulkoistamisen tietoturvariskit
8. Tietoturvattomat sovellukset
9. Verkkorajojen eroosio
10. Teknologia-sukupolven asenne

Lähde: ISF, Threat Horizon 2010

Samlink

Maltego



Samlink

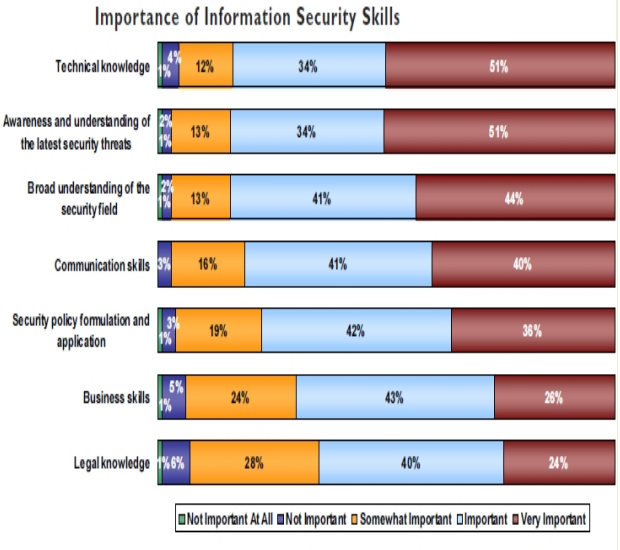
Tietoturva-ammattilaisilta vaaditaan laajaa osaamista

It is not enough to do your best; you must know what to do, and then do your best.

-- W. Edwards Deming

Samlink

Tietoturva-ammattilaiset tänään



Tietoturva-ammattilaisia on maailmanlaajuisesti n. 1.6 miljoonaa

Ammattilaisista n. 3.5% on suorittanut CISSP-sertifioinnin

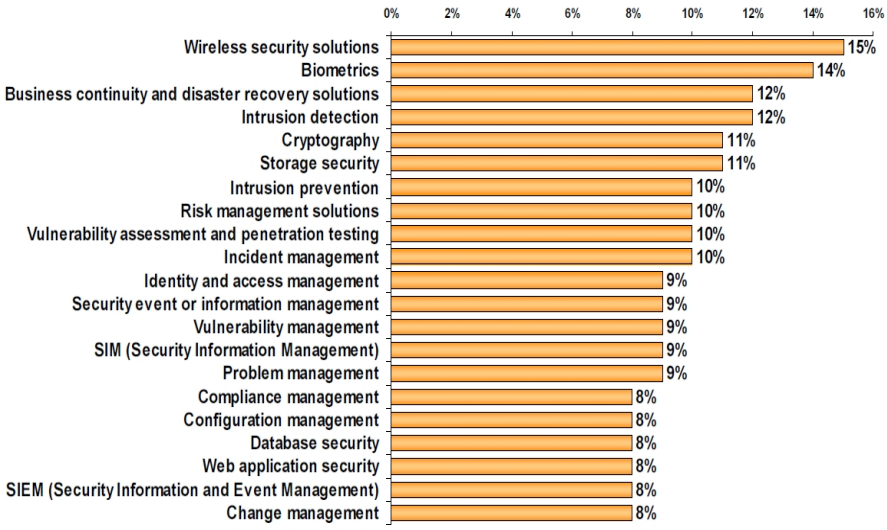
Ammattilaisten määrän arvioidaan kasvavan vuosittain 10% vuoteen 2012 asti (kokonaismäärä tällöin n. 2.7 milj.).

Suurin kasvu EMEA alueella, 13%.

Lähde: (ISC)², www.isc2.org
The 2008 Global Information Security Workforce Study

Samlink

Uudet käyttöönotettavat tietoturvateknologiat



7.5.2008 Jari Pirhonen

Lähde: (ISC)², www.isc2.org
The 2008 Global Information Security Workforce Study

Samlink

Perusratkaisuista strategiaksi

Tietoturva-johtaminen

Verkko- ja järjestelmä-ylläpidon tietoturva-asiantuntijuus

Tietoturvan erityis-asiantuntijuus

Palomuurit, haittaohjelmien torjunta, etäkäyttö, roskapostin torjunta, ...

kerta-kirjautuminen, hyökkäysten havainnointi, käyttäjätietojen hallinta, lokien hallinta ...

Riskien hallinta, mittaaminen, tilannekuvan hallinta, tietoturva-arkkitehtuuri, tietoturva projekti- ja systeemityössä, jatkuvuussuunnittelu, luotettavuuden osoittaminen, vaatimusten-mukaisuus ...

Tuote, palvelu

Projektit

Jatkuva kehittäminen

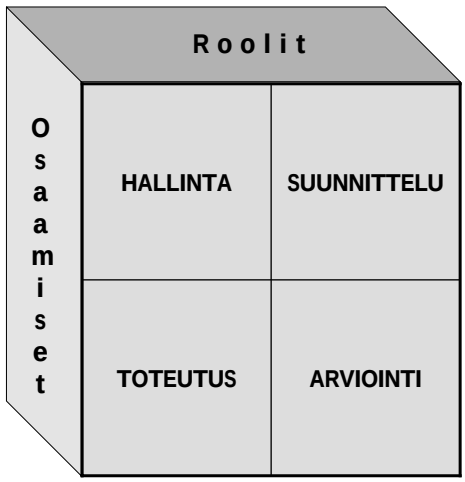
7.5.2008 Jari Pirhonen

Samlink

Tietoturva-ammattilaisen osaamisvaatimukset

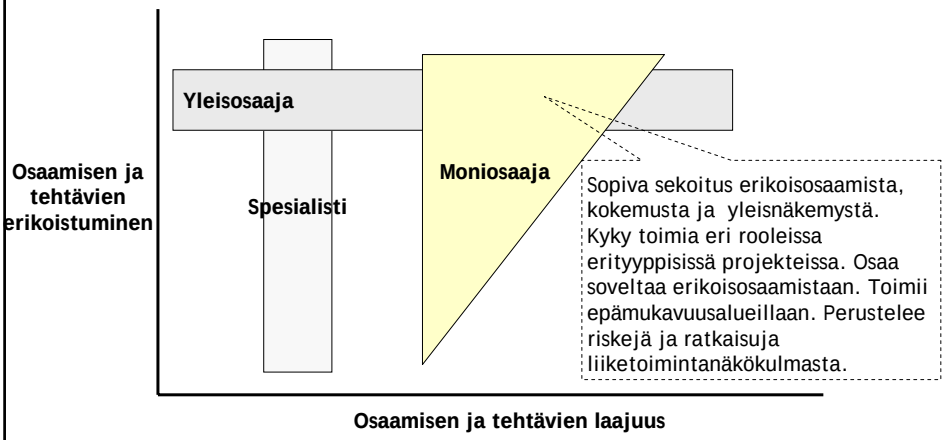
1. Tietojen suojaaminen
2. Tietorikosten tutkiminen
3. Liiketoiminnan jatkuvuus
4. Poikkeamien hallinta
5. Tietoturvakoulutus ja -tietoisuus
6. IT-järjestelmien operointi ja ylläpito
7. Tietoverkkojen turvallisuus
8. Henkilöstöturvallisuus
9. Fyysinen turvallisuus
10. Tuotteiden ja palvelujen hankinta
11. Ulkoisten vaatimusten täyttäminen
12. Riskien hallinta
13. Strateginen johtaminen
14. Sovellusten turvallisuus

Lähde: IT Security Essential Body of Knowledge
US Department of Homeland Security,
National Cyber Security Division
http://www.us-cert.gov/ITSecurityEBK/



Samlink

Tietoturva-ammattilainen on moniosaaja



Lähde: Gartner, The IT Professional Outlook

Samlink

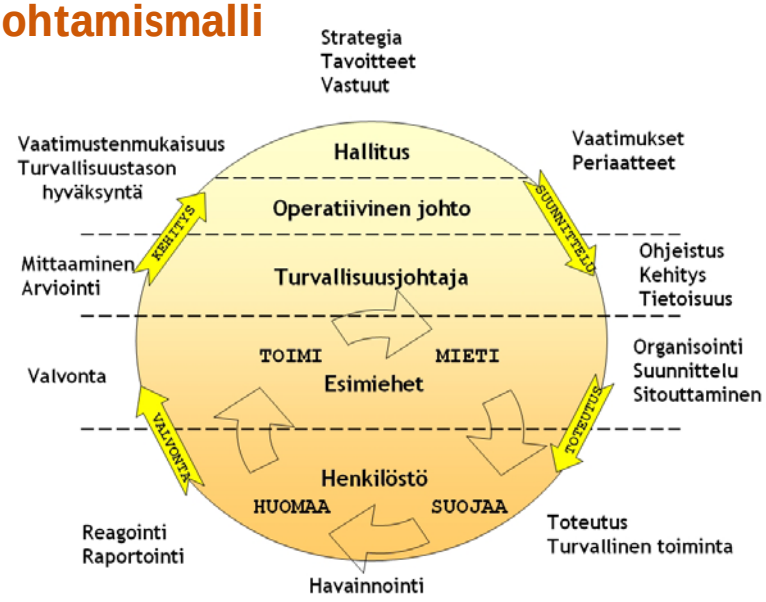
Avainasemassa on koko organisaation sitouttaminen tietoturvatyöhön

Among the other skills and knowledge you have you need to be able to tell people things they don't want to hear and have them asking for more.

-- cissp-forum mailing list

Samlink

Johtamismalli



Samlink

Yhteenveto

1. **Tietoturvaan kohdistuu ristiriitaisia paineita**
   - **tietoturvataso yrityksissä on enimmäkseen korkeintaan välttävä**
2. **Tietoturva on turvallisuusalan suurin haaste nyt ja tulevaisuudessa**
   - **erityisesti monimutkaisuuden lisääntyminen, laitteiden ja yhteyksien määrän kasvu, turvattomat sovellukset ja ulkoiset vaatimukset**
3. **Tietoturva-ammattilaisilta vaaditaan laajaa osaamista**
   - **tarvitaan kommunikointikykyisiä, liiketoiminnan ymmärtäviä, teknisesti päteviä moniosaajia**
4. **Avainasemassa koko organisaation sitouttaminen tietoturvatyöhön**
   - **tietoturvajohtaminen, keskijohdon sitouttaminen, tietoturvatietoisuus**

Samlink