Jari Pirhonen 6.1.2008
Artikkeli Turvallisuus-lehteen 1/2008

Tietoturva-ammattilaisen osaamisvaatimukset

Tietoturva-ammattilaisilta odotetaan monipuolista osaamista

Tietoturva-asiantuntijalta odotetaan teknisen osaamisen lisäksi mm. projektiosaamista, liiketoimintanäkemystä ja ulkoisten vaatimusten ymmärrystä. Tietoturva-asiantuntijan on oltava moniosaaja, joka soveltaa tietämystään eikä pelkää työskennellä myös epämukavuusalueillaan.

Tietoturvajohdon on kehitettävä erityisesti liiketoiminta- ja viestintäosaamistaan. Tietoturvaa on kehitettävä riskilähtöisesti organisaation liiketoiminnan tarpeisiin perustuen. Tietoturvajohdon tehtävänä on usein ohjata organisaation muu henkilöstö huomioimaan tietoturva omilla vastuualueillaan.

Tietoturva-ammattilaisen tehtäväkenttä on muutoksessa

Historiaa ovat ne ajat, kun tietoturva-asiantuntijan ydinosaamista olivat virustorjunnan tai palomuurin ylläpito. Näiden tietoturvan perusvälineiden tuntemuksen voidaan olettaa jo kuuluvan tietoverkkoasiantuntijan osaamisiin. Tietoturvaosaamista edellytetään nykyään monen muunkin asiantuntijatehtävän suorittamiseksi.

Tietoturvan osaamisen laajetessa tietoturvaan erikoistuneen ammattilaisen ei kuitenkaan tarvitse olla huolissaan töiden loppumisesta. Päinvastoin – tietoturvaosaajista on pula ja tehtävät käyvät mielenkiintoisimmiksi.

Muutos tietoturva-alalla on ollut melkoinen. Kymmenen vuotta sitten Ernst & Youngin tekemässä tutkimuksessa (Global Information Security Survey) havaittiin, että vain reilulla puolella yrityksistä yleensäkin oli tietoturvahenkilöstöä. Viime vuonna tehdyssä vastaavassa tutkimuksessa tietoturvaosaajien puute oli jo noussut yritysten suureksi huolenaiheeksi.

Tietoturvan näkyvyys organisaatioissa on jatkuvasti kasvanut ja sen merkitys ymmärretään paremmin. Monella toimialalla tietoturva nostetaan korostetusti esille joko toimialan oman sääntelyn tai ulkoisten vaatimusten kautta. Organisaatiot ja sovellukset verkottuvat entistä monimutkaisemmin samalla kun halutaan käyttöön tietotekniikan uusimmat mahdollisuudet. Monimutkaisuuden hallinta ja oleelliseen keskittyminen ovat tärkeitä.

Tietoturvaosaamisen osa-alueet

US Department of Homeland Security on määritellyt tietoturva-ammattilaisen osaamisvaatimukset eri tietoturvatehtäviin. Lähtökohtana on 14 osaamisaluetta, joita katsotaan hallinnan, suunnittelun, toteutuksen ja arvioinnin näkökulmasta.

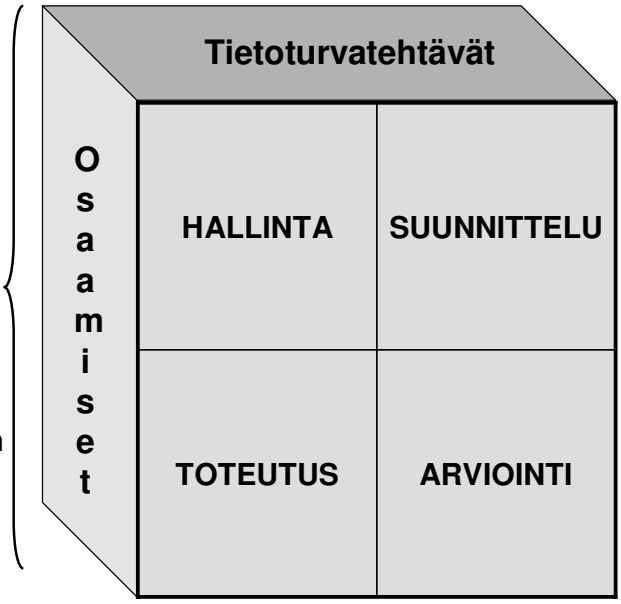
Määrittelyssä on mielenkiintoista nimenomaan se havainto, että eri tietoturvatehtävät vaativat paitsi eri osaamisia, myös erilaista näkökulmaa osaamisten sisällä. Esimerkiksi tietoturvapäälliköltä odotetaan erityisesti hallintaan, suunnitteluun ja arviointiin liittyvää osaamista, kun taas tietoturva-asiantuntijalta edellytetään suunnittelu- ja toteutustaitoja.

Tietoturvatehtävissäkin osaamistarpeet siis vaihtelevat, mutta ominaista on laaja-alaisuus. Tietoturva-asiantuntija pohtii ratkaisujen vaikutuksia ja riskejä organisaation laajuisesti, joten osaamista täytyy olla monelta alueelta. On ymmärrettävä verkkotekniikkaa, sovelluksia, arkkitehtuureita, ulkoisia vaatimuksia ja jopa lainsäätöä. Samalla on osattava huomioida liiketoiminnan tarpeet sekä projektien fokus, aikataulut ja resurssit.

Kapean erityisalueen spesialisteja toki tarvitaan myös, mutta heidän työpaikkansa on todennäköisesti IT- tai tietoturvapalveluja tarjoava yritys. Vaatimustaso osaamiselle on tällöin kova, koska palveluntarjoajien ympäristöt ovat laajoja ja monimutkaisia moniasiakasympäristöjä.

Tietoturvaosaamiset

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, http://www.us-cert.gov/ITSecurityEBK/

Uusien teknologioiden käyttöönoton yhteydessä tietoturva-asiantuntija on kuitenkin usein hetken aikaa organisaation parhaita asiantuntijoita ko. tekniikan osalta. Tekniikat on tunnettava tietoturvatarpeiden tunnistamiseksi. Uuden tekniikan laajemman käyttöönoton myötä tähän liittyvä tietoturvaosaaminen sulautuu muihin asiantuntijatehtäviin.

Tietoturvajohdon uudet tuulet

Tietoturvajohto on perinteisesti taustoiltaan teknistä. Palomuuriasiantuntijasta on edetty tietoturvapäälliköksi. Haasteena onkin usein liiketoiminnan ymmärtäminen sekä esimies- ja kommunikointitaidot.

Jari Pirhonen 6.1.2008
Artikkeli Turvallisuus-lehteen 1/2008

Information Security Forum (www.securityforum.org) on tutkinut jäsenistönsä keskuudessa tietoturvapäällikön haasteita ja nykypäivän osaamisvaatimuksia. ISF määrittelee nykyaikaisen tietoturvapäällikön ominaisuuksiksi seuraavaa:

- päätöksentekijä ja vastuunkantaja
- omaa hyvät esimies- ja verkostoitumistaidot
- ymmärtää liiketoiminnan ja organisaation
- johtaa tietoturvastrategian liiketoiminnan tarpeista
- varmistaa perusasiat kuntoon ensimmäiseksi eikä ”juokse tulipaloja sammuttamassa”
- toimii riskilähtöisesti huomioiden yrityksen riskinottohalukkuuden
- toimii IT:n ja liiketoiminnan tulkkina

Osaamisvaatimusten muuttuessa tietoturvapäällikön paikasta saattaa kilpailla hyvinkin erilaisen taustan omaavia henkilöitä. Perinteisen insinööri- tai poliisikoulutuksen sijaan henkilöllä saattaakin olla juristin tai MBA tutkinto. Tietotekniikan jatkuvan kehittymisen ja monimutkaistumisen takia kuitenkin uskon, että tietoturvapäälliköllä täytyy olla hyvä, osittain syvällinenkin, ymmärrys tietotekniikasta ja tietoturvatekniikoista.

Tietoturvapäälliköille paineita ja toimintaedellytyksiä luo se, että yritysjohto on erittäin kiinnostunut tietoturvasta. Tuoreessa tutkimuksessa, turvallisuusjohtaminen ylimmän liikkeenjohdon näkökulmasta (Laurea, 2007), havaittiin johdon arvostavan tietoturvan yritysturvallisuuden tärkeimmäksi osa-alueeksi.

IDC:n tutkimuksen (Global Information Security Workforce Study) mukaan organisaatioiden ylin johto on ottanut näkyvämmin tietoturvavastuuta kantaakseen. Samalla tietoturvavastuu organisaatioissa on siirtymässä pois IT:n alaisuudesta.

Valitettavasti satsaus tietoturvaresursseihin ei useinkaan kulje käsi kädessä ylimmän johdon tietoturvakiinnostuksen kanssa. Liian usein haetaan pistemäisiä tuoteratkaisuja kun kestävämmät toimenpiteet liittyisivät koulutukseen ja toimintatapojen kehittämiseen.

Tietoturvan näkyvyyden kasvaessa organisaatioissa, on luonnollista, että kiinnostuneita vastuunkantajia löytyy entistä enemmän. Tietoturva ja muu yritysturvallisuus on usein pidetty organisaatioissa erillään, mutta viime vuosina yhä useampi tietoturvapäällikkö on saanut huomata päässeensä yritysturvallisuusjohtajan tai riskien hallinnasta vastaavan johtajan alaisuuteen.

Tietoturvatöitä riittää

Tietoturvan perustekniikoiden ja tuotteiden ollessa kypsiä ja tietoturva-ammattilaisten kysynnän ollessa tarjontaa suurempi, on luonnollista, että perustietoturva hankitaan palveluna. Organisaatioiden omille tietoturva-ammattilaisille kyllä riittää tehtävää osa-alueilla, joilla ei vielä ole riittävän koeteltuja työkaluja ja käytäntöjä. Puhumattakaan siitä, että tietoturvapalvelujen ostaminen ja valvonta vaativat omaa erityisnäkökulmaansa tietoturvaan. Voimavaroja täytyisi vielä riittää organisaation tietoturvan jatkuvaan kehittämiseenkin. Tietoturva-arkkitehtuurin kehittäminen, tietoturvatilannekuvan ylläpitäminen, tietoturvan mittaaminen, tietoturvan integrointi organisaation päivittäiseen työhön ja muut mielenkiintoiset ponnistukset varmistavat, että tietoturva-ammattilaisen tehtävät muuttuvat entistä monipuolisemmiksi ja haastavammiksi.

Jari Pirhonen 6.1.2008
Artikkeli Turvallisuus-lehteen 1/2008

Tietoturva-ammattilaiselle asetetaan toiveita ja paineita monelta eri suunnalta. Tietoturvatoimenpiteet täytyy arvioida usealta kantilta ja perustella monelle taholle. Sopiva sekoitus laajaa näkemystä ja tietyn tietoturvan osa-alueen syvällisempää osaamista kommunikointitaitoihin yhdistettynä taannee mielenkiintoisia työtehtäviä vuosiksi eteenpäin.

Artikkelin kirjoittaja *Jari Pirhonen* (CISSP, CISA) työskentelee pankkitoiminnan IT- ja tukipalveluja toimittavan Samlink Oy:n turvallisuusjohtajana. Pirhonen toimi vuosina 2006 ja 2007 Tietoturva ry:n puheenjohtajana.

LIITE: Tietoturvasertifioinnit

Tietoturva-ammattilaisia palkatessaan voi ammattitaidon lisävakuutena edellyttää tietoturvasertifikaattia. Suomessa ja maailmanlaajuisestikin arvostetuimpia tietoturvasertifiointeja lienevät $(ISC)^2$ **CISSP**, SANS **GIAC** sekä ISACA **CISA**- ja **CISM**-sertifioinnit.

Kaikki nämä sertifikaatit edellyttävät ammattitaidon jatkuvaa ylläpitämistä ja sertifikaatin säännöllistä uusimista. Sertifioinnit ovat ANSI/ISO/IEC 17024 standardin mukaan hyväksyttyjä.

CISSP-sertifioituja (Certified Information Systems Security Professional) on maailmalla n. 50.000, Suomessa n. 250 kpl. CISSP-sertifiointi edellyttää todistettua viiden vuoden tietoturvatyökokemusta, kymmenen tietoturvallisuuden osa-aluetta käsittävän tutkinnon suorittamista ja sitoutumista eettisiin sääntöihin. CISSP soveltuu osoittamaan laajaa kokemusta ja tietämystä tietoturvallisuuden koko kentästä. Sertifiointia on myönnetty vuodesta 1989 lähtien. Lisätietoja www.tietoturva.fi ja www.isc2.org.

GIAC-sertifoituja (Global Information Assurance Certification) on maailmanlaajuisesti n. 20.000, maakohtaista tietoa ei ole saatavilla. GIAC-sertifioinnit vaativat käytännönläheistä osaamista ja keskittyvät eri osa-alueisiin, kuten langattomat verkot, tietoturvapoikkeamien analysointi, Windows ja Unix. GIAC-sertifioinnit edellyttävät tutkinnon suorittamista ja lopputyön tekemistä. Sertifioinnit soveltuvat erityisesti osoittamaan tietyn osa-alueen hyvää teknistä tietämystä. Sertifiointeja on myönnetty vuodesta 1999 lähtien. Lisätietoja www.giac.org.

CISA-sertifioituja (Certified Information Systems Auditor) on maailmanlaajuisesti n. 50.000, Suomessa n. 160 kpl. CISA-sertifiointi edellyttää viiden vuoden työkokemusta tietojärjestelmien tarkastamisesta tai turvaamisesta, kuusi tarkastuksen osa-aluetta käsittävän tutkinnon suorittamista ja sitoutumista eettisiin sääntöihin. CISA soveltuu osoittamaan laajaa tietämystä IT-järjestelmistä ja niiden tarkastamisesta. Sertifiointeja on myönnetty vuodesta 1978 lähtien. Lisätietoja www.isaca.fi ja www.isaca.org.

CISM-sertifioituja (Certified Information Security Manager) on maailmanlaajuisesti n. 6500 ja Suomessa n. 30. CISM-sertifiointi edellyttää todistettua viiden vuoden tietoturvatyökokemusta, viisi tietoturvan hallintaa käsittävän tutkinnon suorittamista ja sitoutumista eettisiin sääntöihin. CISM soveltuu osoittamaan tietoturvavastaavan tehtäviin tarvittavaa osaamista. Sertifiointeja on myönnetty vuodesta 2003 lähtien. Lisätietoja www.isaca.fi ja www.isaca.org.