Tietoturvapolitiikat

Riitta Mäkinen

Extended Abstract

Helsinki 4.3.2003

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Tietoturva nykyaikaisessa liiketoimintaympäristössä -seminaari

1. Johdanto

Yritysturvallisuuden tavoitteena on taata yrityksen toiminnan häiriötön jatkuminen sekä normaalioloissa että poikkeustilanteissa. Tietoturvallisuus on olennainen osa yritysturvallisuutta. Tieto on yrityksen omaisuutta ja tietoa on suojattava samoin menetelmin kuin yrityksen muutakin omaisuutta. Tietoturvallisuuden ytimen muodostavat tietoturvapolitiikat, joiden avulla määritellään tietoturvan kohteet ja periaatteet sekä määritellään vastuut. Koska tietoturvapolitiikat koskettavat tavalla tai toisella yrityksen koko henkilöstöä, ne ovat sidoksissa yrityskulttuuriin ja yrityksen henkilöstön tietoturvatietämyksen tasoon.

2. Tietoturvallisuus

Tietoturvallisuus on kiinteä osa yritysturvallisuutta ja siten se koskee kaikkia työntekijöitä. Valtioneuvoston periaatepäätöksessä [Val99] tietoturvallisuus on määritelty seuraavasti:

> Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietojen *luottamuksellisuutta, eheyttä ja käytettävyyttä* turvataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhkilta tai vahingoilta.

Samassa periaatepäätöksessä [Val99] tietoturvallisuus on suunnittelun, toteutuksen ja valvonnan helpottamiseksi jaoteltu osa-alueisiin seuraavasti: hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus sekä käyttöturvallisuus.

3. Tietoturvapolitiikka

Tietoturvapolitiikka on yrityksen johdon näkemys siitä, mitä tavoitteita yrityksen tietoturvalle tulee asettaa. Tietoturvapolitiikassa määritellään tietoturvan kohteet ja periaatteet sekä määritellään vastuut. Tietoturvapolitiikassa on otettava huomioon lakien ja sopimusten toiminnalle asettamat vaatimukset.

Tietoturvapolitiikkaa ei voi tehdä ilman yrityksen ydinprosessien määrittelyä ja riskianalyysiä. Kun on tunnistettu uhat, joita vastaan on suojauduttava voidaan riskianalyysin avulla tehdä päätökset riskien pienentämiseksi, siirtämiseksi tai hyväksymiseksi.

Yrityksen johdon vahvistama tietoturvapolitiikka toteutetaan tietoturvaperiaatteiden, alemman tason tietoturvapolitiikkojen sekä toimintaohjeiden, oppaiden ja koulutuksen avulla.

4. Tietoturvapolitiikkahierarkia

Politiikat muodostavat yrityksen tietoturvaohjeistuksen perustan. Niiden avulla määritellään se, mitä tulee suojata. Yrityksen johdon hyväksymän tietoturvapolitiikan alle laaditaan alemman tason politiikat, joista johdetaan yksityiskohtaiset toimintaohjeet ja järjestelmien turvamääritykset.

Alemman tason politiikat ovat yksittäisille osa-alueille määriteltyjä tietoturvaperiaatteita, jotka ohjaavat tietoturvan toteutusta.

Tietoturvaperiaatteet ovat sääntöjä ja määritelmiä, jotka ohjaavat tietoturvapolitiikkojen toteutusta.

Toimintaohjeet ovat yksityiskohtaisia soveltamisohjeita. Ne kertovat, miten politiikoissa suojattaviksi määritellyt kohteet turvataan. Toimintaohjeissa kuvataan vaihe vaiheelta, miten tietyssä toiminnossa säilytetään haluttu tietoturvan taso.

Ohjenuorat, oppaat, ovat yleisiä suosituksia tai ehdotuksia tietoturvapolitiikkojen ja standardien käyttöönotosta. Ne eivät ole pakollisia. Niitä noudatetaan, ellei ole erityistä syytä niistä poikkeamiseen.

5. Tietoturvapolitiikkojen laatimisen periaatteet

Turvapolitiikoissa on pohjimmiltaan kysymys luottamuksen ja valvonnan välisestä tasapainosta. Kehen luotetaan ja milloin. Luotetaanko kaikkiin, ei kehenkään vai joihinkin joissakin tilanteissa. Tietoturvapolitiikat koskettavat jokaista työntekijää. Kaikkien osapuolten, niin käyttäjien, ylläpitäjien kuin yritysjohdonkin, yksimielisyyttä on vaikea saavuttaa. Liian rajoittavia politiikkoja on vaikea toteuttaa: niistä joko ei välitetä tai keksitään keinot niiden kiertämiseksi. Politiikkojen tekeminen vaatii sovittelua ja erilaisten vaihtoehtojen vertailua.

Turvapolitiikat voivat olla myös keskenään ristiriitaisia tai tietyissä olosuhteissa yhden säännön noudattaminen rikkoo toista sääntöä. Siponen [Sip00] esittää viisi lähtökohtaa turvaohjeiden laatimiseksi siten, että ristiriidat voidaan välttää:

1. Kiellettyä on kaikki, mikä ei ole erikseen sallittua
2. Sallittua on kaikki, mikä ei ole erikseen kiellettyä

3. Yhtä tietoturvaohjetta voidaan muodollisesti rikkoa, jos se tuo enemmän hyötyä tietoturvallisuudelle tai liiketoiminnalle kuin ohjeen noudattaminen
4. Ohjeet ovat suosituksia, joita ei ole pakko noudattaa
5. Yleistettävyyden malli, jossa toiminnan hyväksyttävyyden mittarina on käyttäjän kuvitelma siitä, sallittaisiinko toiminto kaikille muillekin.

6. Tietoturvapolitiikkojen käyttöönotto

Tietoturvapolitiikat on otettava käyttöön koko yrityksessä. ”Yritys muodostuu työntekijöistä, joten työntekijät ovat ensisijaisia myös silloin, kun määritellään yrityksen tietoturvan taso”, toteaa Virtanen [Vir2002]. Turvapolitiikkojen ja toimintaohjeiden noudattaminen riippuu työntekijöiden tietoturvaosaamisen tasosta ja vallitsevasta yrityskulttuurista. Yrityskulttuuri määrää myös sen, millä tasoilla tietoturvapolitiikkojen noudattamista valvotaan.

Jatkuva koulutus ja tietoturvatietoisuuden lisääminen ovat välttämättömiä edellytyksiä hyvän tietoturvatason saavuttamiseksi.

7. Tietoturvapolitiikkojen elinkaari

Howard [How03] on esitellyt elinkaarimallin tietoturvapolitiikkojen laatimisen ja ylläpidon helpottamiseksi. Howardin [How03] mukaan turvapolitiikkojen elinkaari muodostuu politiikan kehittämisestä, käyttöönotosta, ylläpidosta ja käytöstä poistamisesta. Kukin vaihe jakaantuu tehtäviin. Kehittämistehtäviä ovat politiikan luominen, tarkistaminen ja hyväksyminen. Käyttöönottovaiheeseen kuuluu tiedottaminen, politiikan käyttöönotto ja poikkeusten käsittely. Ylläpitovaiheen tehtäviä ovat politiikasta muistuttaminen, käytön valvonta, rikkomusten käsittely ja politiikan ajantasaisuudesta huolehtiminen. Politiikka poistetaan käytöstä silloin, kun yrityksessä ei enää käytetä tekniikkaa, johon politiikka on liittynyt tai kun on otettu käyttöön korvaava politiikka.

8. Esimerkkejä tietoturvapolitiikoista

9. Lähteet

Dav03 Davidson, K.,A framework for certification testing. Teoksessa *Information Security Management Handbook*, vol 4, 4th edition, toim. Tipton, H., Krause, M., Auerbach Publications, USA, 2003, sivut 509-539.

Har03 Hare, C., Firewalls, ten percent of the solution: a security architecture primer. Teoksessa *Information Security Management Handbook*, vol 4, 4th edition, toim. Tipton, H., Krause, M., Auerbach Publications, USA, 2003, sivut 699-781.

HoP03 Hoefelmeyer, R., Phillips, T., Malicious code: the threat, detection and protection. Teoksessa *Information Security Management Handbook*, vol 4, 4th edition, toim. Tipton, H., Krause, M., Auerbach Publications, USA, 2003, sivut 541-563.

How03 Howard, P., The security policy life cycle: functions and responsibilities. Teoksessa *Information Security Management Handbook*, vol 4, 4th edition, toim. Tipton, H., Krause, M., Auerbach Publications, USA, 2003, sivut 297-311.

Lan01 Landwehr, C., Computer Security. *International Journal of Information Security*, vol 1, issue 1, Springer-Verlag, 2001. [Myös http://link.springer.de/link/service/journals/10207/ tocs/t1001001.htm]

Sip00 Siponen, M., Policies for Construction of Information Systems´ Security Guidelines, Five approaches*, Proc. IFIP TC11 16th Annual Working Conference on Information Security: Information Security for Global Information Infrastructures*, Beijing, China, elokuu 2000, sivut 111-120.

SmN00 Smith, G.,Newton, R., A taxonomy of organisational security policies, *Proc. 23rd National Information Systems Security Conference*, Baltimore, MD, USA, lokakuu 2000, sivut 225-233. [Myös http://csrc.nist.gov/nissc/2000/proceedings/ papers/052.pdf]

Val99 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuudesta, VM 0024:00/02/99/1998, Helsinki, 1999. [Myös http://www.vm.fi/tiedostot/pdf/fi/6294.pdf]

Vir02 Virtanen, T., *Four views on security*. Väitöskirja, Teknillisen korkeakoulun tietoliikenneohjelmistojen ja multimedian julkaisuja, Otamedia Oy, Espoo 2002. [Myös http://www.tml.hut.fi/~tpv/ opiskelijat/tpv.pdf]