Tietoturvakartoitus yrityksen Internet-palveluja tuottavassa yksikössä

Antti Nilsson

9.1.2008

Valvoja Prof. Jukka Manner

Esityksen sisältö

- Kohdeorganisaation esittely
- Työn tausta ja tavoitteet
- Kirjallisuus
- Tietoturvakartoitus kohdeorganisaatiossa
- Päähavainnot ja kehitysehdotukset
- Jatkotutkimuksen aiheet

Kohdeorganisaatio 1/2

- Suuren kustannusalan yrityksen sisäinen yksikkö
- Pienikokoinen organisaatio toimii itsenäisesti ja erillään emoyrityksen ICT-yksiköstä
- Tekee läheistä yhteistyötä emoyrityksen kustantaman aikakauslehden kanssa
- Omat tietojärjestelmät, ylläpitäjät, sovelluskehittäjät ja asiakaspalvelija

Kohdeorganisaatio 2/2

- Organisaation tehtävänä on tuottaa Internet-palveluja sekä yrityksille että kuluttajille
- Tietoturvallisuuteen kohdistuvat haasteet koostuvat ensisijaisesti Internet-toiminnasta sekä asiakasrajapinnoista

Työn lähtökohdat

- Kohdeorganisaatio haluaa kasvattaa kykyään puuttua mahdollisiin tietoturvaongelmiin ennaltaehkäisevästi
- Tavoitteena ehkäistä mahdollisista tietoturvapoikkeamista aiheutuvia haitallisia vaikutuksia

Tutkimuskysymykset

- Mitä on tietoturvallisuus ja mikä on sen merkitys yrityksille?
- Miten yritysten tietoturvallisuutta voidaan hallita?
- Mikä on kohdeorganisaation tietoturvallisuuden nykytila?
- Miten kohdeorganisaation tietoturvallisuutta tulisi kehittää?

Kirjallisuus 1/2

- Kohdeorganisaation tietoturvallisuuden kehittämisen kannalta oleellisia aiheita
- Mitä on tietoturvallisuus ja mikä on sen merkitys yrityksille?
  - Tietoturvallisuuden määritelmä
  - Tietoturvallisuuden tarve
  - Tietoturvallisuuden osa-aluejako
  - Tietoturvatietoisuuden ja -kulttuurin vaikutus

Kirjallisuus 2/2

- Miten yritysten tietoturvallisuutta voidaan hallita?
  - Tehtävät ja vastuunjako
  - Tietoturvapolitiikka, -suunnitelma ja -ohjeet
  - Tietoturvallisuuden prosessi
  - Riskienhallinta
  - Tietoturvallisuuden kontrolleja
  - ISO 17799 -standardi

Tietoturvakartoitus 1/2

- Mikä on kohdeorganisaation tietoturvallisuuden nykytila?

  => Tietoturvakartoitus

- Miten kohdeorganisaation tietoturvallisuutta tulisi kehittää?

  => Tietoturvakartoituksen tulosten analyysi ja kehityssuunnitelma

Tietoturvakartoitus 2/2

- Pohjana käytettiin ISO 17799 -standardia
- Tutkimusmenetelmät
  - Puolistrukturoitu haastattelu (7 kpl)
  - Tietojärjestelmien, dokumentaation ja toimitilojen läpikäynnit
  - Työ- ja toimintatapatarkastelu
- Tulokset ryhmiteltiin itse muodostetun osa-aluejaottelun mukaisesti

Päähavainnot

- Monet asiat toteutettu hyvin
  - mm. tekniset suojaukset, jokapäiväinen toiminta ja erikoistilanteiden hallinta
  - etenkin tiedon saavutettavuuteen on panostettu
- Suurimmat ongelmakohdat kohdistuvat pääasiassa hallinnolliselle puolelle
  - tietoturvatyön organisoiminen ja vastuunjako
  - strateginen suunnittelu ja dokumentointi
  - tietoturvahäiriöiden ja parannuskohteiden hallinnan organisoiminen

Kehitysehdotukset 1/2

- 13-kohtainen kehityssuunnitelma, joka sisältää
  - tarvittavat toimenpiteet
  - perustelut kunkin toimenpiteen tärkeydestä
  - aikatauluehdotuksen
  - arvion kunkin toimenpiteen läpiviemiseen tarvittavista resursseista

Kehitysehdotukset 2/2

- Ehdotettuja toimenpiteitä muun muassa
  - tietoturvatyön organisointi
  - dokumentoinnin ja koulutuksen parantaminen
  - liiketoiminnan vaatimusten määrittäminen
  - tietoaineistoturvallisuuden kehittäminen
- Kehitysehdotukset on suunniteltu siten, että kohdeorganisaatio pystyy realistisesti toteuttamaan ne

Jatkotutkimuksen aiheita

- Tietoturvallisuuden hallinnan kehittäminen pienissä organisaatioissa
- Tasapaino luottamuksellisuuden, eheyden ja saavutettavuuden välillä
- Tietoturvallisuuden prosessin mittareiden valinta
- Kansainvälisen toiminnan tietoturvallisuudelle tuomat haasteet

Kysymyksiä?