Matti Laakso / Tietoturvapäivä 8.2.2011

PK-yrityksen tietoturvasuunnitelman laatiminen

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

Tietoturvasuunnitelma 1/3

Toimenpiteiden ja dokumentoinnin lopputuloksena syntyvä kokonaisuus

”-- kirjallinen tietoturvasuunnitelma on KTM:n tutkimuksen mukaan vain 14 prosentilla yrityksistä --”

Kauppa- ja teollisuusministeriön tutkimus vuodelta 2007
- http://www.huoltovarmuus.fi/ajankohtaista/uutisarkisto/news.mpl?id=59

Tietoturvasuunnitelma 2/3

Kysymys: Onko sellaista pakko olla?

Vastaus: Miksi et sellaista tekisi?

Tietoturvasuunnitelma 3/3

Ajatellaan edelliset kysymykset toisella tavalla:

Ostaisitko palvelun/tuotteen yritykseltä, jolla ei ole tietoturva-asiat kunnossa?

Haluatko, että oma yrityksesi menettää asiakkaita huonon maineen johdosta?

Esimerkkitapaus

Suojattavien kohteiden määrittely

Mitkä asiat ovat tärkeimpiä yrityksesi liiketoiminnan kannalta?

- Esim. Palvelimet, tietojärjestelmät, tuotantolaitteet, salaiset asiakirjat jne.
- Määrittele tärkeysjärjestys ja kriittisyys
  - Tuotantopalvelin vs testipalvelin
  - Salainen vs luottamuksellinen dokumentti

Mieti alustavasti miten kohteita kannattaa suojata

- Sisäinen testipalvelin: perussuoja
- Tuotantopalvelin: kovennettu suojaus
- Sidosryhmille lähetettävät materiaalit: salaus tai kirjattu kirje

Dokumentoi!

Riskienhallinta 1/3

Mitkä tekijät uhkaavat tärkeitä suojattavia kohteitasi?

- Tietomurrot
- Laiteviat
- Fyysiset uhat
  - Varkaus
  - Hajoaminen
  - Sähkökatkos
  - Luonnonilmiö
- Yllättävät tahot
  - Ulkoistetut palvelut

Dokumentoi!

Riskienhallinta 2/3

Yksi riskitekijä ylitse muiden:

Henkilöstö

”Selvityksen mukaan yritykset suojautuvat huolellisemmin ulkoapäin tulevia uhkia vastaan, vaikka tietoon ja innovaatioihin kohdistuvista väärinkäytöksistä ja rikoksista 47 % oli oman henkilökunnan tai entisten työntekijöiden tekemiä.”

Helsingin kauppakamari 2010: Innovaatioiden ja tiedon suojaaminen 2010
http://helsinki.chamber.fi/index.phtml?1137_m=3210&s=229

Riskienhallinta 3/3

Arvioi riskien tapahtumistodennäköisyys

Esim:

Riski	Todennäköisyys	Vaikutus liiketoimintaan	Riskikerroin
Palvelin hajoaa	1	2	3
Tietomurto	2	3	5
Tuotantotyöntekijä irtisanoutuu	1	1	2
Avaintyöntekijä irtisanoutuu	3	3	6

Dokumentoi!

Tietoturvapolitiikka

Dokumentti, joka kertoo yleisesti yrityksen suhtautumisesta tietoturvaan

- Yleisellä tasolla tietoturvalinjaukset ja –tavoitteet
- Ei teknistä ohjeistusta
- Yritysjohdon hyväksymä dokumentti
- Sisältää myös yritysjohdon kannanoton tietoturvatyöskentelyyn

Dokumentoi!

Suojamekanismien toteuttaminen ja dokumentointi 1/2

Tällä hetkellä pitäisi olla tiedossa:

1. **Mitä suojataan**
2. **Mitä riskitekijöitä on olemassa**
3. **Miten halutaan suojata**

Suojataan yrityksen tärkeät dokumentit, järjestelmät ja toiminnot.

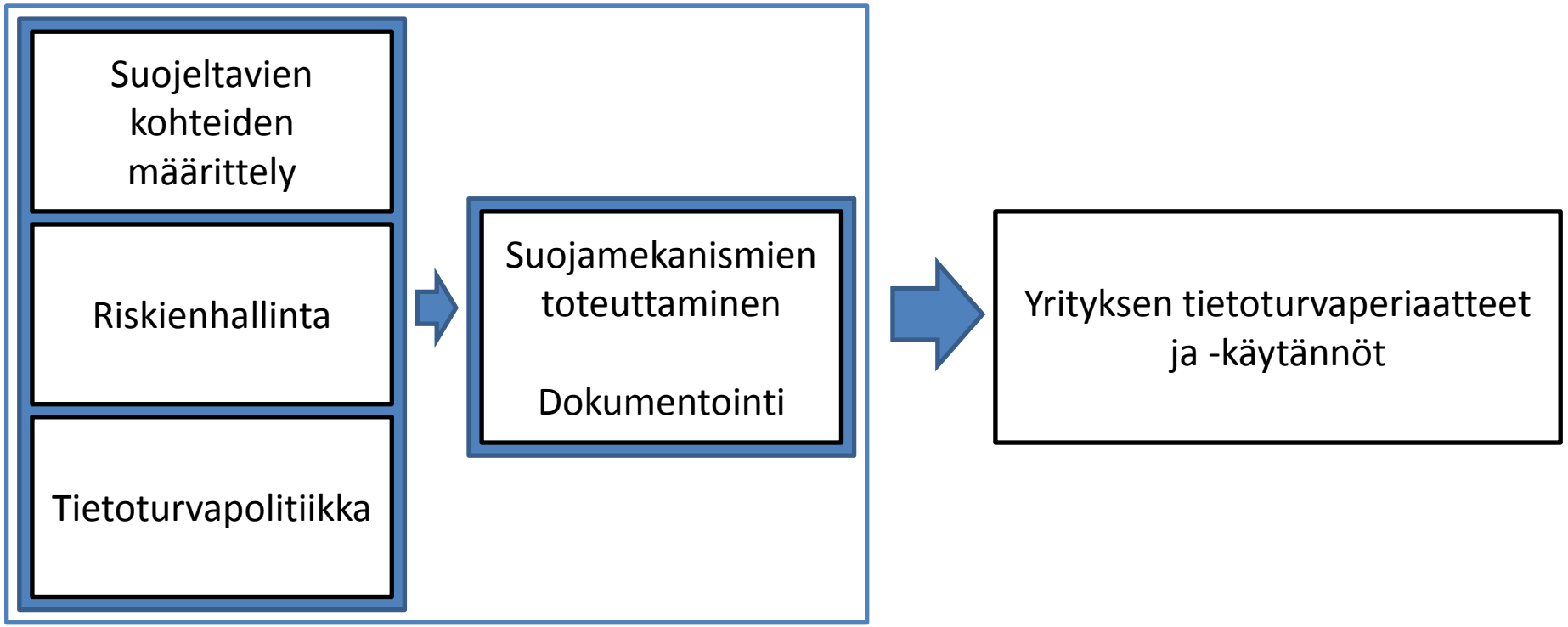
Suojamekanismien toteuttaminen ja dokumentointi 2/2

Mieti asioita esimerkiksi tietoturvan osa-alueiden kautta

- Hallinnollinen tietoturva: Miten esimerkiksi yritysjohto osallistuu tietoturvan johtamiseen
- Fyysinen: Toimitilojen turvaaminen (yleisturvallisuus, varkaudet jne)
- Henkilöstö: Tietoturvaosaaminen ja yleinen ohjeistaminen
- Tietoaineisto: Eri dokumenttien salaaminen ja turvallinen käsittely
- Tietoliikenne: Tietoverkkojen turvallisuuden varmistaminen esimerkiksi palomuureilla
- Ohjelmisto: Haittaohjelmilta suojautuminen ja ohjelmien luvattoman käytön estäminen
- Laitteisto: Laitteiden fyysinen suojaaminen ja luvattoman käytön estäminen
- Käyttöturvallisuus: Käyttöoikeudet ja salasanakäytännöt yms.

Dokumentoi!

Toiminnan ja dokumentoinnin lopputulos



Miten kävi esimerkkitapauksen yritykselle ?

Kysymyksiä?

Kiitos mielenkiinnostanne!

Matti Laakso
www.tietojesiturvaksi.fi

Matti.Laakso @ turkuamk.fi