

Pk-yrityksen tietoturvasuunnitelman laatiminen

Matti Laakso, Turun ammattikorkeakoulu

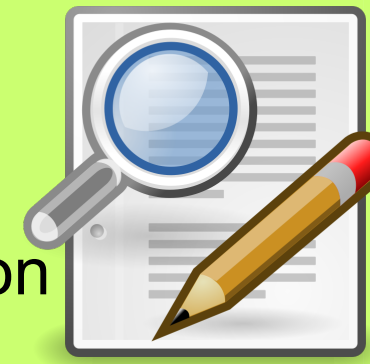
Joko sinun yritykselläsi on tietoturvasuunnitelma?

Tietoturvasta huolehtiminen on yhä tärkeämpi osa yrityksen päivittäistä liiketoimintaa. Lainsäädännön vaatimukset ja asiakkaiden muuttuvat tietoturvatarpeet kannustavat yrityksiä parantamaan toimintatapojaan. Laadukas tietoturvatyöskentely edellyttää asianmukaista ja ylläpidettyä dokumentaatiota.

Onko yritykselläsi jo sellainen?

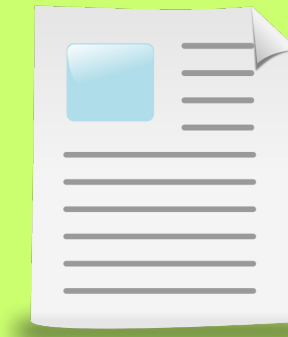
Suojattavien kohteiden määrittely

Tietoturvasuunnitelman laatiminen kannattaa aloittaa listaamalla yritykselle tärkeät suojattavat kohteet. Niitä voivat olla esimerkiksi fyysiset tai sähköiset dokumentit sekä erilaiset tietojärjestelmät. Määrittelyn tarkoituksena on tunnistaa liiketoiminnan kannalta tärkeimmät asiat. Yrityksen tulee pohtia myös tietojen kriittisyyttä. Tärkeimmät tiedot tulee suojata ensimmäisenä.



Tietoturvapoliitiikka

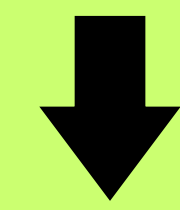
Riskianalyysistä paljastuvien epäkohtien korjaaminen aloitetaan tekemällä tietoturvapoliitiikka. Se on yritysjohton laatima dokumentti, joka sisältää yleisellä tasolla tietoturvalinjaukset ja -tavoitteet. Asiakirja ei sisällä mitään teknisiä ohjeistuksia tai toimenpiteitä. Ne sijoitetaan erilliseen dokumenttiin, tietoturvasuunnitelmaan.



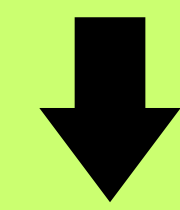
Lopullinen dokumentaatio voidaan toteuttaa monella tavalla. Eräs hyväksi havaittu keino on kirjata asiat tietoturvan eri osa-alueiden näkökulmasta. Yleisesti käytetyssä jaottelussa niitä on kahdeksan. Oheisessa taulukossa on listattuna eri osiot sekä esimerkkitapaukset kyseisen osa-alueen aihepiiristä. Tietoturvaperiaatteet ja -käytännöt -dokumentaatioon kirjataan kaikki oleelliset toiminnot sekä toteutetut suojaustoimenpiteet, jotka liittyvät eri osa-alueisiin.

Hallinnollinen	Tietoturvapoliitiikan laatiminen, tietoturvatyöskentelyn johtaminen
Fyysinen	Toimitilojen yleinen turvallisuus ja suojaaminen esimerkiksi varkauksilta
Henkilöstö	Tietoturvaosaaminen ja yleinen ohjeistaminen
Tietoaineisto	Sähköisten ja fyysisten dokumenttien salaaminen ja turvallinen käsittely
Tietoliikenne	Tietoverkkojen turvallisuuden varmistaminen esimerkiksi palomuuereilla
Ohjelmisto	Haittaohjelmilta suojautuminen ja ohjelmien luvattoman käytön estäminen
Laitteisto	Laitteiden fyysinen suojaaminen sekä luvattoman käytön estäminen
Käyttöturvallisuus	Salasanakäytännöt ja muut käyttöoikeuksiin liittyvät asiat

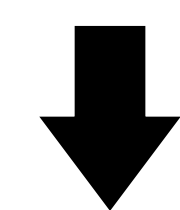
SUOJATTAVIEN KOHTEIDEN MÄÄRITTELY



RISKIENHALLINTA

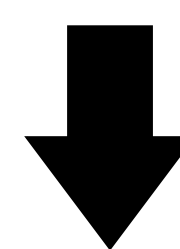


TIETOTURVAPOLITIIKKA



SUOJAMEKANISMIIEN TOTEUTTAMINEN

DOKUMENTOINTI



YRITYKSEN TIETOTURVAPERIAATTEET JA -KÄYTÄNNÖT

Tekijä: Matti Laakso

matti.laakso@gmail.com
www.tietojesiturvaksi.fi

Kuvat:
Taitto- ja julkaisuohjelma:

www.opencipart.com
www.scribus.net

Tutkimustulokset

Tämän tutkimuksen tarkoituksena oli selvittää, mitä asioita pk-yrityksen tulee huomioida tietoturvasuunnitelmaa laadittaessa. Työn lähteinä käytettiin kotimaisia ja ulkomaisia kirjoja, virallisia tietoturvastandardeja sekä sähköisiä materiaaleja. Tutkimustulokset pyrittiin kuvaamaan siten, että lukijan on helppo siirtää teoria käytäntöön.

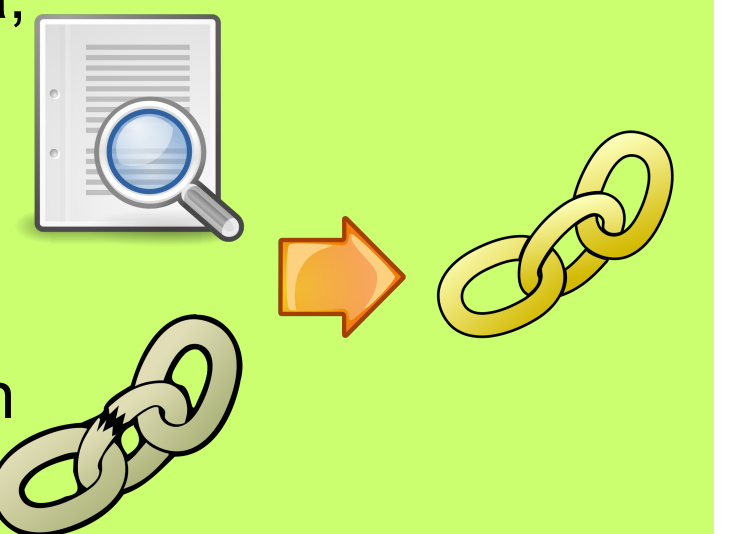
Kuten oheisesta kuviosta on huomattavissa, prosessi on moniosainen ja laaja. Tietoturvasuunnitelman laatiminen ei kuitenkaan ole vaikeaa, mikäli tehtävässä edetään järjestelmällisesti ja loogisesti.

Riskienhallinta

Suojattavien kohteiden määrittelyn jälkeen on pohdittava niitä uhkaavia ongelmatekijöitä. Riskienhallinnaksi kutsutaan kaikkia niitä toimenpiteitä, joilla näitä uhkia pyritään kontrolloimaan.

Yleisimpiä riskitekijöitä ovat erilaiset tietomurrot ja haittaohjelmat. Näiden lisäksi yrityksen tulee miettiä myös mahdollisimman monia muita riskitekijöitä, kuten fyysisiä tai henkilöstöön liittyviä uhkia.

Riskien tapahtumistodennäköisyys pitää arvioida ja vakavimmilta uhilta pyritään suojautumaan ensin.



Suojamekanismien toteuttaminen ja dokumentointi

Määrittelyjen, riskianalyysin ja tietoturvapoliitiikan laatimisen jälkeen tarvittavat suojamekanismit toteutetaan ja kirjataan. Prosessissa syntyvää dokumentaatiota kutsutaan tietoturvasuunnitelmaksi.



Tietoturvasuunnitelma

Tämän dokumentaation tarkoituksena on kuvata yrityksen käytössä olevat tietoturvaratkaisut. Terminä tietoturvasuunnitelma on kuitenkin harhaanjohtava, sillä dokumentti kuvaa nykyisiä tietoturvan ylläpitämiseksi tehtyjä teknisiä ja hallinnollisia toimenpiteitä.

Parempi nimitys on esimerkiksi VAHTI -työryhmän* käyttämä "tietoturvaperiaatteet ja -käytännöt". Varsinaista suunnitelmaosuutta kutsutaan tietoturvan kehittämissuunnitelmaksi.

*Valtiohallinnon tietoturvallisuuden johtoryhmä VAHTI

