Tietoriskit

Tietoriskejä on pitkään aliarvioitu, eikä niiden hallinta ole vielä aina kunnossa. Yritys voi huolehtia tietoriskeistä pitkälti itse, mutta esimerkiksi tietoverkkojen suojaus vaatii monasti asiantuntija-apua. Olennaista on tiedostaa yrityksen keskeiset tiedot, kehittää toimintaa lähtökohdiltaan turvalliseksi ja soveltaa monipuolisia turvajärjestelyjä. Tekninen suojaus on tässä vain yksi elementti.

Tieto on tärkeä tuotantotekijä

Jokaisessa yrityksessä on sen toiminnalle kriittisiä tietoja, esimerkiksi asiakastiedot, tuotannonohjauksen tiedot, tuoteideat, markkinointisuunnitelmat. Tietoa on **paljon monessa eri muodossa**: henkilökohtainen osaaminen ja kokemustieto; asiakirjat, sopimukset, ohjeet, suunnitelmat ja muut paperidokumentit sekä asiakas-, tilaus- ja palkkatiedot yms. tietojärjestelmien sisältämä tieto.

Monessa pk-yrityksessä **tieto on suurin pääoma**. Silti tietojen hallintaan ja suojaamiseen ei aina kiinnitetä riittävästi huomiota. Yrityksen toiminnan kannalta on tärkeätä, että

- Tiedot oikeita, luotettavia ja ajantasalla
- Tiedot ovat aina oikeutettujen henkilöiden saatavilla
- Tiedot eivät joudu ulkopuolisille, asiaankuulumattomille henkilöille.

Tieto lisää tuskaa – tietohävikit ja -vuodot lisäävät sitä vielä enemmän!

Tietoriskien luonne muuttuu

Tietoriskien luonne muuttuu jatkuvasti. Yritysten elämä on kaikilla toimialoilla yhä enemmän tietojen käsittelyä – dokumentteja ja tietämystä siirretään ja käsitellään koko ajan, yhä monipuolisemmilla tavoilla ja yhä monimutkaisemmissa verkostoissa

- Yritysverkostoissa tieto liikkuu uudella tavalla
- Työsuhteet lyhenevät — väheneekö henkilöstön sitoutuminen?
- Erilaiset virukset, madot, muut haittaohjelmat ja tiedostojenjako-ohjelmat aiheuttavat ongelmia
- Maahanmuuttajien tai uuden vientimaan tavat voivat poiketa siitä, mihin yrityksessä on totuttu
- Tiedonsiirtotavat monipuolistuvat ja nopeutuvat
- Missä puhut matkapuhelimeesi?
- Ovatko kannettavasi tiedot suojattuja?
- Internetissä koko maailma on naapurinasi
- Elektroninen kauppa uudistaa kauppaa ja maksuliikennettä, sekä asettaa haasteita tietoturvalle
- Roskaposti kuormittaa tietojärjestelmiä

Hallinta vaatii monipuolisia keinoja

Tietoriskien hallinnan perusta on tunnistaa tietoihin liittyvät keskeiset riskit. Tunnistamisen helpottamiseksi tämän kortin kääntöpuolella on tietoriskien riskikartta, jonka avulla voidaan selvittää keskeiset tietoriskien alueet. Niiden parissa ryhdytään tarkempaan tunnistamis- ja hallintatyöhön välinesarjassa olevilla työkorteilla. Riskejä hallittaessa on otettava lähtökohdaksi toiminnan kehittäminen – toimintatavat, osaaminen, johtaminen – ja vasta sen jälkeen tulevat tekniset suojauskeinot.

Pahimmat tietovuotojen lähteet
1. Keskustelut
2. Paperidokumentit
3. Tietojärjestelmät

Lisätietoja

- Tietoturvallisuus, tietosuoja, normit, ohjeet, säädökset, tietoturvallisuusviitteet. Valtionhallinnon tietoturvallisuuden johtoryhmä. http://www.vm.fi/vm/liston/page.lsp?r=3115&l=fi (Sisältää keskeisiä koti- ja ulkomaisia linkkejä)
- Käytännön tietoturvallisuusopas PK-yrityksille. Ovatko yrityksesi tietoriskit hallinnassa. Teollisuus ja työnantajat. Saatavana myös PDF-muodossa osoitteesta http://www.ytnk.fi/tietoturva.pdf
- Viestintäviraston tietoturvasivut. Asiaa tietoturvasta ja uusimmat haavoittuvuudet yms. http://www.cert.fi

Laatija: Matti Vuori, VTT Automaatio, Johannes Halmevuo. Copyright © 2004 VTT. Työvälinesarjan ovat pääosin rahoittaneet Euroopan sosiaalirahasto ja sosiaali- ja terveysministeriön työsuojeluosasto sekä Työsuojelurahasto. Versio 3.0. 17.9.2004. Tiedosto: kor-tie-aloituskortti.doc

Tietoriskikartta

Yritys:	Ryhmä/arvioija:
Tarkastelun kohde:	Päiväys:

Johtaminen

- ❑ Johdon tietoisuus tietoriskien merkityksestä
- ❑ Tärkeimpien tietojen tunnistaminen
- ❑ Suurimpien riskien tunteminen
- ❑ Tietoturvapolitiikka ja käytäntö
- ❑ Tietoturvallisuus osana laatujärjestelmää
- ❑ Hankittu käyttöön riittävä osaaminen
- ❑ Tietoturvatoiminnan kehittäminen

Toimitilat

- ❑ Alttius onnettomuuksille
- ❑ Yrityksen tilojen erottaminen kiinteistössä
- ❑ Kulunvalvonta
- ❑ Vartiointi ja rikostorjunta
- ❑ Tilojen erottaminen toisistaan ja kulkuoikeudet
- ❑ Arkisto ja dokumenttien käsittely
- ❑ Faksit, kirjoittimet, tms.
- ❑ Asiakastilat
- ❑ Vierailijat, ulkopuoliset toimijat (siivoojat, konsultit yms.)

Tietojärjestelmien suojaus

- ❑ Vastuut järjestelmistä
- ❑ Paperin käsittely
- ❑ Käyttöoikeudet
- ❑ Etätyö (puhelimet, PDA:t, tietokoneet yms.)
- ❑ Toiminnan seuranta (häiriöt, käyttö, levytila)
- ❑ Arkistot ja dokumenttien käsittely
- ❑ Muutosten hallinta
- ❑ Käytöstä poisto
- ❑ Ohjelmistohankinnat ja asennukset
- ❑ Varmistukset ja palauttaminen
- ❑ Salasanat
- ❑ Intranet, Extranet ja WWW
- ❑ Virukset, haittaohjelmat, roskaposti yms.
- ❑ Sähkön- ja energiansyötön häiriöt

Henkilöstön toiminta

- ❑ Koulutus tietoriskien hallintaan
- ❑ Tietoturvaperiaatteet
- ❑ Selkeät toimintaohjeet
- ❑ Rekrytointi ja taustaselvitykset
- ❑ Salassapitositoumukset
- ❑ Toimet työsuhteen päättyessä
- ❑ Käyttöoikeuksien hallinta
- ❑ Varautuminen häiriöihin ja onnettomuuksiin
- ❑ Suojaratkaisut henkilöstön välineissä (virustentorjuntaohjelmat yms.

Tietoriskit

Kehittäminen ja toiminnan jatkuvuus

- ❑ Dokumentointi ja järjestelmäkuvaukset
- ❑ Jatkuvuus- ja toipumissuunnittelu
- ❑ Muutosten hallinta
- ❑ Avainhenkilöt
- ❑ Riskienhallinta

Suhteet sidosryhmiin

- ❑ Yhteistyökumppanien luokittelu
- ❑ Yhteiset pelisäännöt
- ❑ Alihankkijoiden aiheuttamat riskit
- ❑ Eri osapuolten katselmointi
- ❑ Sopimukset
- ❑ Järjestelmien käyttöoikeudet
- ❑ Neuvottelutilojen yms. tietoturvallisuus
- ❑ Yhteistyön tietojen suojaus muilta asiakkailta
- ❑ Taustaselvitykset

Täyttöesimerkki

☒ Sopimukset *- Merkittävä riski;* OK☐ Asiakkaat *- Asia kunnossa;* ☐ ~~Laiterikot~~ *- Ei koske meitä*

Johtaminen. Johdon tietoisuus tietoriskeistä on tietoriskien hallinnan kivijalka. Johtamisen käytännön välineitä ovat hallittu tietoturvatyö, osaamisen hyödyntäminen ja riskienhallinnan muiden perustelähtökohtien luominen.

Henkilöstö. Henkilöstön käytännön toimissa tietoriskit joko hallintaan tai ne toteutuvat. Osaaminen ja suunnittellut toimintatavat luovat pohjan onnistumiselle. Henkilöstön käyttöön on luotava laadukkaat välineet riskien hallitsemiseksi, esimerkiksi automaattisesti toimivat virustentorjuntaohjelmistot.

Toimitilat. Onnettomuudet ja varkaudet ovat keskeisiä riskejä. Tilojen kulunvalvonta, erottaminen yms. ovat perustoimia tietoriskienkin hallitsemiseksi.

Tietojärjestelmien suojaus. Sähköisten tietojärjestelmien suojaus on keskeisiä tietoriskien hallinnan haasteita. Mutta paperilla toimivien järjestelmien hallinta on aivan yhtä tärkeää.

Suhteet sidosryhmiin. Liikesuhteiden tietoriskit korostuvat verkottumisen ja alihankinnan myötä. Eri osapuolten valmiudet yhteistoimintaan on selvitettävä, ja kouluttamalla ja katselmoimalla varmistuttava, ettei yhteistoimintaan jää heikkoja lenkkejä. Luottamuksen on toimittava yhtä hyvin jokaiseen suuntaan!