Tietoriskien tärkeitä kysymyksiä

Tässä tietokortissa on koottu joukko tärkeitä tietoriskien hallintaan liittyviä kysymyksiä yrityksessä tapahtuvan keskustelun pohjaksi.

Tiedot ovat tärkeitä yritystoiminnassa

Suunnitelmien, laskelmien, tarjousten, asiakkaiden, tuotekehityksen ja muihin yrityksen toiminnalle tärkeiden tietojen käsittelyyn kiinnitetään liian vähän huomiota. Huolimattomien ja vastuuntunnottomien käsittelytapojen seurauksena **tiedot saattavat muuttua toisiksi, hävitä, kopioitua tai joutua asiattomille**. **Tiedon siirron helppous ja nopeus, uudet sähköiset kauppatavat, tiivis yhteistyö kumppanin kanssa, henkilöstön vaihtuvuus ja rikollisuuden torjunta edellyttävät ennakolta luotuja toimintatapoja**. Tietoriskit hallitaan johtamiskäytännöin, arkipäivän työskentelyrutiinein ja teknisin suojaamiskeinoin.

Tietoja on papereilla ja sähköisessä muodossa useilla tietovälineillä sekä ihmisten mielissä.

Mitkä tilanteet haittaavat toimintaa?

- Jos tietokoneet varastetaan, voiko joku hyödyntää niissä olevia tietoja?
- Jos tapahtuu sähköhäiriö, voiko päivän aikana luodut tiedostot hävitä?
- Jos kiinteistössä syttyy tulipalo, voiko tiedot tai muotit tuhoutua ja liiketoiminta pysähtyä?
- Jos järjestelmään tulee tietokonevirus, voiko tiedot muuttua tai järjestelmä tukkeentua?
- Jos järjestelmä ei tunnista käyttäjää, voiko sitä käyttää petokselliseen toimintaan?
- Jos työntekijä kertoo junassa tutulleen tuotekehityksen tuloksista, voiko tieto olla merkittävä takana istuvalle kilpailijalle?
- Jos yrityksessä työskentelevä ulkopuolinen työntekijä kuljettaa tietoa ulkopuolelle, voiko tiedot joutua niitä hyödyntäville tahoille?
- Jos työntekijä irtisanotaan, voiko hän tuhota tärkeitä tietoja tai viedä ne ja hyötyä niistä?

Onko tällaisten tilanteiden uhka tunnistettu teidän yrityksessänne?

Liiketoiminnan jatkuvuus vaarassa

Liiketoimintaa häiritsevät tapahtumat ja tilanteet edellyttävät valmiutta hallita tilanteet. Tämän vuoksi tarpeelliset varajärjestelyt pitää toteuttaa jo ennalta. Tämä on tärkeää myös liiketoiminnassa tarvittavien tietojen käytettävyyden varmistamisessa.

Yritysturvallisuus ja riskien hallinta

Monenlaisia suojaamiskeinoja ja turvajärjestelyjä on tarjolla. Yrityksessä tulee luoda käsitys liiketoiminnan jatkuvuuden ja turvaamisen tarpeista – tärkeää on luoda näkemys **todellisista riskeistä**.

Tietoturvallisuudesta huolehtiminen on osa turvallisuustyötä. Liiketoiminnan luonne määrittelee turvallisuustyön painopisteet ja suojauskeinot. Toiminnan turvaaminen on nimettävä johtoryhmän jäsenelle ja tietotekninen turvaaminen tietotekniselle osaajalle.

- Onko turvallisuuden kehittämistarpeet tunnistettu ja kirjattu kehittämissuunnitelmaksi? Onko tehtävät vastuutettu?
- Onko kehittämiskustannukset arvioitu?
- Miten toimitaan, jos epäillään väärinkäytöksiä?
- Miltä osin toiminta vakuutetaan?

N. 80% liiketoiminnan turvallisuudesta luodaan valveutuneen henkilöstön arkipäivänrutiineilla ja niiden kehittämisellä, ja n. 20 %:sesti voidaan tukeutua erilaisiin teknisiin suojaamiskeinoihin.

Lait velvoittavat luomaan käytäntöjä

Tietoturvarikkomuksissa yritys varmistaa etunsa, kun se pystyy osoittamaan tietojen suojaamistahdon eli

- Tietojen tunnistamismenettelyn
- Tietojen käsittelyn ohjeet ja käytännöt sekä
- Henkilöstön koulutuskäytännöt .

Henkilötietolaki velvoittaa huolehtimaan mm. etteivät työntekijöitä tai -hakijoita koskevat tiedot, kuten terveys-, osaamis- ja palkkatiedot, paljastu, muutu tai joudu asiattomille.

Arvopaperimarkkinalaki ja pörssisäännöt velvoittavat täsmentämään mm. sisäpiiriin kuuluvat henkilöt ja heitä koskevan vaitiolovelvoitteen merkityksen.

Pelastustoimi-, työsuojelu-, kirjanpito- ja valmiuslait vaikuttavat osaltaan myös tietojen oikeellisuuden ja käytettävyyden varmistamiseen.

ESR
Työsuojelurahasto

Tietoturvallisuuden tavoitteet

Tietoturvatyön tavoite on taata, että yrityksen liiketoiminnan tiedot ovat **oikeita ja säilyvät oikeina**, että ne ovat **tarvittaessa saatavilla ja käytettävissä**, ja että ne ovat **luotettavien ihmisten käsiteltävinä ja oikein toimivien järjestelmien ylläpidettävinä**.

- Mitkä tiedot pitää olla aina oikein? Miten havaitaan tietojen virheet tai puutteet?
- Mitkä tiedot ja järjestelmät pitää olla aina käytettävissä?

Turvaamisen lähtökohta: tiedon arvo

Liiketoiminta-, tuotekehitys-, tuotanto-, myynti-, talous-, henkilöstö- ja tietohallinnon ja turvajärjestelyjen tiedot tulee **tunnistaa**.

Tiedot luokitellaan merkityksen mukaan elintärkeiksi, tärkeiksi ja tarpeellisiksi sekä sisällön mukaan luottamuksellisiksi, sisäisesti käsiteltäviksi ja julkisiksi tiedoiksi. Luokittelut ohjaavat tietojen käsittelykäytäntöjen, -ohjeiden ja turvamenettelyjen luomista.

Tietoturvapolitiikka ja -ohjeet

Tietoturvapolitiikka sisältää yrityksen johdon asettamat tavoitteet tietojen huolelliselle käsittelylle sekä tietoja käsittelevien ja turvakäytäntöjen kehittäjien vastuut.

Tietoturvaohjeet sisältävät ohjeita eri vastuutahoille, mm. käyttäjille tarkoitetut tietojen luokittelu-, varmistus-, virusten torjuntaohjeet.

- Kuka huolehtii toimintaohjeiden ylläpidosta?

Henkilöstön tietoisuus ja toimintatavat

Tietoriskien arviointi tulee olla jokaisen työntekijän arkipäivää, osa huolellista tietojen käsittelyä.

- Miten tietoturvaohjeet ja vaitiolositoumus konkretisoidaan työntekijöille?
- Mitkä omassa hallussa olevista tiedoista ovat tärkeitä ja vaativat erityistä huolenpitoa? Mitkä paperit, levykkeet, CD:t ja varmuuskopiot?
- Käyttääkö jokainen omaa käyttäjätunnustaan ja siihen liitettyä henkilökohtaista salasanaa?
- Miten toimitaan virustartuntatilanteessa?
- Onko työntekijöillä oikeus kopioida omaan käyttöön yrityksen virustentorjuntaohjelmisto?

Jos osoiterekisteri on kännykässä, miten pärjäät puhelimen kadotessa?

Toimitilojen turvallisuus

- Onko kulku toimitiloissa rajattu eri alueisiin?
- Annetaanko vierailijoille tunnistelaput?
- Onko erilliset neuvottelutilat?
- Miten työ- ja tekniset tilat suojataan? Miten työasemat, palvelimet, henkilöt, tietoliikenneyhteydet, ristikytkentäkaapit, etätyöpisteet tulee suojata?
- Valvotaanko tiloissa kulkemista?
- Miten toimitaan, jos on tapahtunut varkaus?
- Kuinka usein toteutetaan tiloista poistumisharjoituksia?
- Miten jatketaan toimintaa tulipalon jälkeen?

Tietoteknisen suojaamiskeinot

- Miten virheellinen / asiaton käsittely estetään?
- Kirjautuuko jokainen käyttäjä järjestelmään omalla käyttäjätunnuksellaan?
- Estääkö palomuuriohjelmisto asiattomien pääsyn yrityksen verkkoon?
- Miten toimitaan, jos epäillään hakkerointia?
- Tarkistetaanko tulevat sähköpostiviestit palomuurin virustentorjuntaohjelmistolla?
- Onko kaikilla tietokoneilla ajantasainen virustentorjuntaohjelmisto?
- Onko virustorjuntaohjelmiston päivitys vastuutettu nimetylle henkilölle ja varahenkilölle?
- Mitä ohjelmallisia tarkistuksia tehdään?
- Miten ohjelmistomuutokset hyväksytään ja dokumentoidaan?
- Miten ohjelmisto- ja muut hankinnat hyväksytetään ja rekisteröidään?

Tietojen ja järjestelmien käyttöohjeet

- Kuinka usein varmistetaan varmistusten palautusten ja varajärjestelyjen toimivuus?
- Miten huolehditaan tärkeiden tehtävien varahenkilöjärjestelyistä?
- Saako jokainen työntekijä käyttöoikeudet vain tietoihin, joita työtehtävä edellyttää?
- Salakirjoitetaanko sähköpostiviestit?
- Onko pöytä- ja kannettavien tietokoneiden tiedot salakirjoitettu?
- Säilytetäänkö turvakopiot eri kiinteistössä?

Suojauskeinojen kustannukset eivät saa ylittää suojattavien kohteiden arvoa.

Tietojen suojaaminen liikesuhteissa

- Mitkä alihankkijat ja kumppanit saavat haltuunsa yrityksen tärkeitä tietoja?
- Mitä tietoja heidän kanssaan liikutellaan?
- Voiko kumppani saada sellaisia tietoja, jotka hyödyntävät vaan sen liiketoimintaa?
- Onko kumppanin työntekijöiden kanssa käsitelty yrityksen ja kumppanin vaitiolositoumuksien ja tietojen käsittelysääntöjen merkitys?
- Onko kumppanilla oma tietoturvapolitiikka?

Turvallisuus on yhtä vahva kuin sen heikoin lenkki. Siksi toiminta on turvattava useilla turvatoimilla ja -keinoilla.

Laatijat: Tuija Kyrölä, Tietoturvakoulutus Oy & Matti Vuori, VTT Automaatio.
Copyright © 2000 PK-RH -hanke. Työvälinesarjan ovat pääosin rahoittaneet Euroopan sosiaalirahasto ja sosiaali- ja terveysministeriön työsuojeluosasto sekä Työsuojelurahasto. Versio 1.0. 21.8.2000. Tiedosto: kor-tie-kysymyksia.doc