Tietoriskien tärkeitä näkökohtia

Tässä tietokortissa on koottu joukko tärkeitä tietoriskien hallintaan liittyviä näkökohtia 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?

- Voiko joku hyödyntää tietokoneissa olevia tietoja, mikäli niitä anastetaan?
- Voivatko päivän aikana luodut tiedostot hävitä sähkökatkon tapahtuessa?
- Voivatko tiedot tai muotit tuhoutua ja liiketoiminta pysähtyä, jos kiinteistössä syttyy tulipalo?
- Voivatko tiedot muuttua tai järjestelmä ylikuormittua tietokoneviruksen iskettyä järjestelmään?
- Voiko tietojärjestelmää käyttää petokselliseen toimintaan käyttäjän jäädessä tunnistamatta?
- Voiko työntekijän junassa tutulleen kertoma tuotekehitystieto olla merkittävä takana istuvalle kilpailijalle?
- Voiko yrityksessä toimiva ulkopuolinen työntekijä viedä yrityksen tietoja yrityksen ulkopuolellle ja luovuttaa niitä kolmansille osapuolille?
- Voiko irtisanottu työntekijä tuhota tai anastaa tietoja 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. Yrityksen on ymmärrettävä liiketoiminnan jatkuvuuden ja turvaamisen tarpeet – tärkeää on tunnistaa **todelliset riskit**.

Tietoturvallisuudesta huolehtiminen on osa turvallisuustyötä. Liiketoiminnan luonne määrittelee turvallisuustyön painopisteet ja suojauskeinot. Toiminnan turvaamisesta vastaa johtoryhmän jäsen ja tietoteknisestä turvaamisesta alan asiantuntija.

- Onko turvallisuuden kehittämistarpeet tunnistettu ja kirjattu kehittämissuunnitelmaksi? Onko tehtävät vastuutettu?
- Onko kehittämiskustannukset arvioitu?
- Miten toimitaan epäiltäessä 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 kykenee osoittamaan tietojen suojaamistahdon eli

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

Henkilötietolaki velvoittaa huolehtimaan mm. etteivät työntekijöitä tai –hakijoita, asiakkaita tai yhteistyökumppaneita 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.

Pelastus-, 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 1. **oikeita ja säilyvät oikeina**, 2. **tarvittaessa saatavilla ja käytettävissä**, 3. **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 on tunnistettava.

Tiedot luokitellaan merkityksen mukaan 1. elintärkeiksi, 2. tärkeiksi 3. tarpeellisiksi sekä sisällön mukaan 1. salaisiksi, 2. luottamuksellisiksi, 3. sisäisesti käsiteltäviksi 4. julkisiksi tiedoiksi. Luokittelut ohjaavat tietojen käsittelykäytäntöjen, -ohjeiden ja turvaamismenettelyjen 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 asiakirjat, levykkeet, CD:t, DVD:t ja varmuuskopiot?
- Käyttääkö jokainen omaa käyttäjätunnustaan ja siihen liitettyä henkilökohtaista salasanaa?
- Miten toimitaan virustartuntatilanteessa?
- Onko työntekijöillä oikeus kopioida omaan käyttöön yrityksen virustentorjuntaohjelmisto?
- Onko huomioitu etätyön erilaiset riskit?

Jos osoiterekisteri on ainoastaan kännykässä, miten pärjäät puhelimen kadotessa?

Toimitilojen turvallisuus

- Onko liikkuminen toimitiloissa rajattu eri alueisiin?
- Annetaanko vierailijoille vierailijakortit?
- Onko erilliset neuvottelutilat?
- Miten työ- ja tekniset tilat suojataan? Miten työasemat, palvelimet, henkilöt, tietoliikenneyhteydet, ristikytkentäkaapit, etätyöpisteet on suojattava?
- Valvotaanko tiloissa kulkemista?
- Miten toimitaan rikostilanteissa?
- Kuinka usein toteutetaan tiloista poistumisharjoituksia?
- Miten jatketaan toimintaa tulipalon jälkeen?

Tietotekniset 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, ja onko niitä testattu?
- Miten huolehditaan tärkeiden tehtävien varahenkilöjärjestelyistä?
- Saako jokainen työntekijä käyttöoikeudet vain työtehtävissään tarvittaviin tietoihin?
- 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 kumppanit saavat ja miten ne siirretään?
- Voiko kumppani saada vain itselleen hyödyllisiä tietoja?
- Onko kumppanin työntekijöiden kanssa käsitelty yrityksen ja kumppanin vaitiolositoumusten ja tietojen käsittelysääntöjen merkitys?
- Onko kumppanilla omaa tietoturvapolitiikkaa?

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, Johannes Halmevuo. Työvälinesarjan ovat pääosin rahoittaneet Euroopan sosiaalirahasto ja sosiaali- ja terveysministeriön työsuojeluosasto sekä Työsuojelurahasto. Versio 2.0. 17.9.2004. Tiedosto: kor-tie-kysymyksia.doc