Luottamuksellisen tiedon suojaaminen

Organisaatiossa voi sen toiminnan, solmittujen sopimusten tai lainsäädännön vuoksi olla salassa pidettävää tietoa. Asiattomien käsiin päästessään tämä tieto voi aiheuttaa organisaatiolle taloudellista vahinkoa, maineen menetyksen tai vahingonkorvaus- tai jopa rikosoikeudellisen vastuun. Yrityssalaisuuksia suojattaessa on varauduttava sekä ulkoisiin (yritysvakoilu) että organisaation sisältä (yrityssalaisuuden rikkominen) tuleviin uhkiin. Suojaaminen on kuitenkin paljon muutakin kuin tekniikkaa ja lukkoja. Seuravilla toimenpiteillä voidaan pienentää yrityssalaisuuksien paljastumisen riskejä.

Yrityssalaisuus – mikä se on?

Rikoslaki määrittelee yrityssalaisuuden seuraavasti: ”Yrityssalaisuudella tarkoitetaan tässä luvussa liike- tai ammattisalaisuutta taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle.”.

Käytännössä tällaisia asioita voivat olla esimerkiksi:

- Tekniset tiedot kuten: tuotekehitys- ja tutkimustulokset sekä tekniset ratkaisut ja suunnitelmat.
- Taloudelliset tiedot kuten: asiakkuustiedot, hinnoitteluperusteet, katteet, ostotiedot ja sopimukset.
- Toimintasuunnitelmat kuten: liiketoiminta-, markkinointi- ja myyntistrategiat.
- Henkilötiedot kuten: palkka-, sairaus- ja rikosseuraamustiedot.

Suojaamistahto

Jotta tietoja voitaisiin suojata, on organisaatiolla oltava ”suojaamistahto”. Organisaation on toimittava siten, että salassa pidettävät tiedot tosiasiallisesti pyritään suojaamaan. Tätä varten tiedot tulee luokitella. Ilman tietojen luokitusta on vaikea saada lakiin perustuvaa turvaa tiedon suojaamiseksi. Jotta suojaaminen saataisiin kohdistettua oikein ja taloudellisesti, kannattaa pyrkiä systemaattiseen toimintaan:

- Luokittele tietosi ja niitä käsittelevät järjestelmät eri turvallisuusluokkiin (esimerkiksi: salainen, luottamuksellinen ja julkinen).
- Määrittele eri tietoluokille ja tiedoille käsittelysäännöt koko niiden elinkaaren ajaksi (synty – käsittely – säilytys – poisto).
- Tiedota henkilöstölle salassapidosta ja toimintatavoista kunkin tietoluokan suhteen.
- Nimeä ainakin yleisellä tasolla (esimerkiksi ostosopimukset) tiedot, joiden suhteen on toteutettava korostettua turvallisuutta.
- Vastuuta ja ohjeista yrityksen sisäisistä asioista ja tilanteesta tiedottaminen nimetyille henkilöille. Ohjeista henkilöstö ohjaamaan kaikki kyselyt näille henkilöille.
- Tee kriisiviestintäsuunnitelma.

Tietojen kartoitus

- Kartoita suojattavat tietosi. Mitä tietoja, teknisiä laitteita, järjestelmiä ja toimitiloja haluat suojata?
- Ovatko suojattavat tiedot vielä salaisia? Jos tieto on tullut laajalti julkiseksi (esimerkiksi julkaistu lehdessä / netissä), ei se enää voi saada lainsäädännöllistä suojaa.
- Tee uhka-analyysi. Mitä seuraa, jos tämä tieto paljastuu? Miten voidaan rajoittaa paljastumisesta seuraavia haittoja?

Suojauskeinoja – asiattomat henkilöt

- Lukitse kaapit, tilat ja huoneet, joissa on luottamuksellista tietoa. Vahvenna tarvittaessa ovi- ja lukkorakenteita.
- Suurehkoon toimitilaan tulisi tehdä eri kulunvalvontavyöhykkeitä. Erota vyöhykkeet siten, että niiden välillä on lukittu ovi, jonka avaaminen kirjautuu kulunvalvontalokiin tai aiheuttaa murtohälytyksen.
- Talleta salainen aineisto kassakaappiin tai salakirjoita sähköisessä muodossa oleva tieto turvallisella, organisaation tietohallinnon hyväksymällä salausvälineellä.
- Varusta toimitilat vartiointiliikkeeseen hälyttävällä murtohälytyslaitteella sekä tallentavalla kameravalvonnalla. Tiedota kameravalvonnasta kyltein tai tarroin.

Suojauskeinoja – tietoverkkojen uhat

- Kerää ja talleta lokeja palomuureista, järjestelmistä sekä verkon tapahtumista erilliselle lokipalvelimelle. Muista tiedottaa henkilöstöä valvonnasta.
- Asenna kaikille tietoteknisille laitteistoille automaattisesti päivittyvä haittaohjelmien torjuntaohjelmisto.
- Vaihda järjestelmien, ohjelmien ja laitteistojen oletussalasanat. Pidä salasanat riittävän pitkinä (> 14 merkkiä) ja vaikeina arvata. Vaihda salasanoja säännöllisesti.
- Varmista järjestelmien tietoturvapäivitysten säännöllinen asentaminen.
- Huolehdi poistettavan tiedon turvallisesta hävittämisestä (silppuaminen, murskaus, ylikirjoitus).
- Kouluta henkilöstöä tietoverkkojen ja yritysvakoilun riskeistä.

Suojauskeinoja – toimitiloissa työskentelevät

- Rekrytoi turvallisesti. Tarkasta rekrytoitavien taustat lain sallimissa puitteissa.
- Jos salassapidolla on erittäin tärkeä merkitys yritystoiminnalle, pyri viranomaistarkastusten piiriin rekrytoinnissa.
- Tee salassapitosopimukset työntekijöiden sekä tietoa käsittelevien tai muiden toimitiloissa toimivien organisaatioiden ja henkilöiden kanssa.
- Rajaa käyttäjien oikeudet vain työtehtävien kannalta tarvittaviin järjestelmiin, hakemistoihin ja oikeuksiin.
- Ohjaa työntekijät käyttämään tulostimien tietoturva-asetuksia (pääsykoodit / viivästetty tulostus).
- Ohjeista siihen, että luottamuksellinen ja salainen aineisto tuhotaan itse tai viedään itse lukittuun tietosuoja-astiaan.
- Kouluta henkilöstöä ohjaamaan tuntemattomat toimitiloissa oleskelevat henkilöt vastaanottoon tai pois tiloista.
- Työsuhteen päättyessä muista käyttö- ja kulkuoikeuksien poistaminen sekä avainten ja muun työmateriaalin poiskeräys.

Suojauskeinoja – toimitiloissa vierailevat

- Varmista ulkopuolisten vierailijoiden sekä huolto- ja lähettihenkilöstön henkilöllisyys sekä asioinnin oikeellisuus esimerkiksi vierailun isännältä / palvelun tilaajalta.
- Pyri siihen, että vieraat liikkuvat tiloissa vain saatettuina.
- Tilanteen vaatiessa tee salassapitosopimus jo ennen neuvottelujen alkua.
- Suosi työtiloista erotettuja neuvottelutiloja ulkopuolisten kanssa neuvotellessasi.
- Siivoa neuvottelutila tietomateriaalista lähtiessäsi ja varmista sen siisteys tullessasi.
- Estä vierailijoiden pääsy tiloihin (työpisteet, tuotekehitys) ja järjestelmiin (mm. lähiverkko, sisäinen WLAN), joissa luottamuksellista tietoa käsitellään.

Suojauskeinoja – omat työntekijät muualla

- Ohjeista ja kouluta työasioista viestiminen toimipaikan ulkopuolella.
- Älä keskustele julkisella paikalla työasioista.
- Vältä näkyviä työpaikan logolla tai tunnuksella varustettuja asusteita tai varusteita työmatkoilla.
- Käytä salausta kannettavissa tietokoneissa ja muistivälineissä.
- Jos pystyt, poista työmatkan tulosteista logot tai tunnistetiedot. Jos tietoja on käytettävä, suosi koodeja ja lyhenteitä.
- Noudata varovaisuutta työskennellessäsi julkisissa kulkuvälineissä. Tietokoneen näyttö ja asiapaperit voivat näkyä muille.
- Pidä luottamuksellinen materiaali (tietokone / paperit) aina valvonnassasi.

Jos luottamuksellista tietoa kuitenkin pääsee julki…

- Epäillessäsi rikosta ota yhteys poliisiin ja noudata heidän ohjeitaan.

Muussa tapauksessa:

- Tiedota asiasta heti kumppaneille ja asiakkaille, joita asia koskee.
- Kokoa organisaatiosta kriisiviestintäryhmä ja tarkasta kriisiviestintäsuunnitelma. Käytä tarvittaessa asiantuntija-apua.
- Arvioi syntynyt vahinko ja estä vahingon laajeneminen (esim. muuta salasanat, tee tietoturvapäivitykset).
- Ohjeista henkilöstöä tiedottamisesta.
- Jos tiedotusvälineet ottavat asiasta yhteyttä, kerro tosiasioita ja harkitse sanasi! Pahoittele tilannetta. Kerro, että tapausta selvitetään ja vaikutuksia arvioidaan. Lupaa tiedottaa asiasta määräajan kuluttua ja toimi lupauksen mukaisesti.