SISÄMINISTERIÖ
INRIKESMINISTERIET

Viestintävirasto

EK

Yritys – miten olet suojannut tietopääomasi?

Sisällysluettelo

Liitteet

Yritys – miten olet suojannut tietopääomasi?

Mitä on yrityksen tietopääoma?

Yritysten toiminta perustuu yhä enemmän uuden tiedon syntymiseen, jalostamiseen, jakamiseen ja kierrättämiseen. Yritysten tietopääoman merkitys on korostunut erityisesti nopeasti kehittyvän tieto- ja viestintäteknologian sekä toimintojen kansainvälistymisen seurauksena.

Lähes jokaisella yrityksellä on jotain toimintansa kannalta olennaista tietoa, joka halutaan pitää liiketoiminnallisista syistä salassa. Tällaisen tiedon paljastuminen ulkopuolisille tarkoittaisi yritykselle taloudellisia vahinkoja ja kilpailuedun menettämistä. Usein puhutaan yritys- tai liikesalaisuuksista.

Tällaisia voivat olla esimerkiksi:

- **Tuotekehitystiedot**
- **Strategia- ja liiketoimintasuunnitelmat**
- **Valmistus- ja tuotantopiirustukset**
- **Lähdekoodit**
- **Prototyypit**
- **Testitulokset**
- **Kauppasopimukset**
- **Asiakasrekisterit**
- **Hinnastot**
- **Henkilöstöä koskevat tiedot**

Yrityssalaisuuksia on nykyisin yhä vaikeampi pitää varmuudella turvassa. Siksi yritysten on tärkeää panostaa toimintaansa ja tietopääomiinsa kohdistuvien uhkien tiedostamiseen, tunnistamiseen ja haitallisen toiminnan ennalta estämiseen.

Mitä seurauksia tietopääoman menettämisellä voi olla?

Pahimmillaan yrityksen keskeisen tietopääoman menetys tarkoittaa yrityksen koko toiminnan vaarantumista. Vähintään se voi aiheuttaa taloudellisia tappioita, kuten tuotekehitysinvestointien hyötyjen tai kilpailuaseman menettämisen.

Yritysvakoilu ja ulkovaltojen tekemä taloudellinen tiedustelu ovat suomalaisiin yrityksiin ja koko kansantalouteen kohdistuvia uhkia. Yritysten ja yhteiskunnan tietopääomiin kohdistuvilla haitallisilla toimilla arvioidaan nykyisin olevan huomattavia kansantaloudellisia haittavaikutuksia.

Tutkimukseen ja tuotekehitykseen panostavissa kehittyneissä talouksissa tappiot ovat kaikkein suurimpia. Laajasti arvioituna taloudellisen tiedustelun ja yritysvakoilun aiheuttamat tappiot voivat olla Suomen kaltaisissa kehittyneissä talouksissa jopa 1–3 % bruttokansatuotteesta. Arvioiden mukaan Suomessa puhutaan jopa satojen miljoonien eurojen suuruisista tappioista vuosittain. Tämä voi tarkoittaa pahimmillaan myös teknologisen etumatkan menettämistä ja kilpailukyvyn heikentymistä.

Mikä voi uhata yritykseni tietopääomaa?

Yrityksesi tietopääoma voi kiinnostaa esimerkiksi kilpailijoitasi. He voivat pyrkiä saamaan salaisia tietoja haltuunsa kyetäkseen kilpailemaan markkinoilla kanssasi. Kilpailijat voivat pyrkiä anastamaan tuotekehitystietojasi ja pääsemään markkinoille ennen sinua, kopioimaan tuotteesi tai palvelusi sekä tuottamaan ja myymään niitä sinua edullisemmin. Myös asiakkaidesi tiedot, hinnoittelutietosi ja tulevaisuuden suunnitelmasi voivat kiinnostaa heitä.

Joidenkin yritysten tietopääoma voi kiinnostaa myös ulkomaisia tiedustelupalveluita. Ne toimivat usein hyödyttääkseen oman maansa yrityksiä ja ovat usein kiinnostuneita erityisesti:

- **Tulevaisuuden mahdollisista kasvualoista**
- **Korkeasta teknologiasta**
- **Uusista innovaatioista**
- **Yhteiskunnan kriittisestä infrastruktuurista**

Tämän lisäksi yrityksesi tietopääoma voi tuhoutua tai sen luotettavuus voi muutoin vaarantua esimerkiksi tiedon tahallisen manipuloinnin seurauksena. Viime aikoina myös erilaiset tietoverkoissa leviävät kiristyshaittaohjelmat ovat hävittäneet yritysten tietoja.

Mitä suojaa lainsäädäntö antaa yritykselleni?

Suomessa yritys- ja liikesalaisuuksien suoja perustuu eri aikakausina säädettyihin lakeihin, joiden välisiä suhteita voi olla joskus hankala hahmottaa. Yrityssalaisuuden suojasta on säädetty sopimattomasta menettelystä elinkeinotoiminnassa annetussa laissa (SopMenL), työsopimuslaissa ja rikoslaissa. Yleinen salassapitovelvollisuus liikesuhteissa asetetaan SopMenL:ssa, työsopimuslaki taas kieltää työntekijää loukkaamasta työnantajan yrityssalaisuuksia ja rikoslaki puolestaan mahdollistaa rangaistuksen antamisen yrityssalaisuutta loukkaavasta toiminnasta. Suomeen ollaan myös säätämässä EU:n liikesalaisuusdirektiivin toimeenpaneva liikesalaisuuslaki, jonka tarkoituksena on parantaa mahdollisuuksia liikesalaisuuksien loukkauksiin puuttumiseen. Lain on tarkoitus tulla voimaan kesällä 2018.

Tekijänoikeuksilla, patentilla ja yrityssalaisuuksilla on yhtymäkohtia. Tekijänoikeussuoja tarkoittaa tietyn ilmaisumuodon suojaa, mutta se ei suojaa teoksen varsinaista sisältöä, teemaa, motiivia, periaatteita tai tutkimustyön tuloksia. Patentissa suoja taas syntyy julkistamalla ja rekisteröimällä keksintö. Tämä puolestaan tarkoittaa tuotteen yrityssalaisuussuojan menettämistä.

Oletko tunnistanut riskitilanteet?

Yritysvakoilun kohteena on yleensä yritysten tieto ja osaaminen. Tekijät pyrkivät hankkimaan luvatta kohdeyrityksen luottamuksellisia tietoja, suunnitelmia ja muuta vastaavaa materiaalia.

Poliisin rikostilastojen mukaan tyypillisimmin yritysten tietopääoma vaarantuu tilanteessa, jossa työntekijä vie luottamuksellista tietoa mukanaan ja perustaa kilpailevan yrityksen tai luovuttaa tiedot muutoin eteenpäin käytettäväksi. Tällöin puhutaan yrityssalaisuuden rikkomisesta tai väärinkäytöstä.

Toimintatavat voivat olla samankaltaisia riippumatta siitä, onko tekijänä ulkomainen tiedustelupalvelu tai kilpaileva yritys. Joskus ulkomaisilla yrityksillä voi myös olla kytköksiä maansa tiedustelu- ja turvallisuusviranomaisiin. Käytännössä yrityksistä pyritään anastamaan tai kopioimaan valmiita suunnitelmia, palveluita ja innovaatioita toisen valtion elinkeinoelämän hyödyksi ja oman kilpailukyvyn edistämiseksi. Esimerkiksi tiedot suomalaisen yrityksen liikkumavarasta kauppaneuvotteluissa tarjoavat selkeän neuvotteluedun vastapuolelle.

Yritysvakoilu ja taloudellinen tiedustelu ovat piilorikollisuutta. Yrityksillä ja viranomaisilla on kuitenkin säännöllisiä havaintoja suomalaisyrityksiin Suomessa ja ulkomailla kohdistuvasta tietojen urkkimisesta, kopioinnista, epäilyttävistä henkilökontakteista sekä erilaisista haittaohjelmahyökkäyksistä. Epäilyjä on usein vaikea todentaa ja poliisin esitutkintaan asti eteneviä tapauksia on siksi vuosittain varsin vähän.

Miten yritysvakoilua voi tapahtua?

Yleisesti puhekielessä yritysvakoilulla voidaan tarkoittaa joko yritysten välistä tietojen anastamista tai valtioiden suorittamaa taloudellista tiedustelua. Suomessa yritysvakoilijoita kiinnostaviksi aloiksi on perinteisesti arvioitu:

- **Teknologia- ja ICT-osaaminen**
- **Puolustus- ja turvallisuusalan yritykset**
- **Laajasti tuotekehitykseen ja innovaatioihin panostavat yritykset**
- **Lääke- ja bioteknologian yritykset**
- **Huoltovarmuuskriittiset yritykset**
- **Luottamuksellista viranomaisyhteistyötä tekevät yritykset**

Yritysvakoilussa ei siis ole kyse ainoastaan suurten korkean teknologian tai puolustus- ja turvallisuusalojen ongelmasta, vaan sitä voi lopulta kohdata minkä tahansa toimialan tai kokoluokan yritys.

Yrityksen henkilöstö kohteena

Luottamuksellisia tietoja voidaan anastaa yrityksistä työntekijöiden kautta. Työntekijä ei välttämättä aina edes tiedosta, että hänellä voi olla tietoja jotka hyödyttäisivät ulkopuolista. Työntekijä ei siksi välttämättä koe luovuttavansa eteenpäin mitään salassa pidettävää.

Joitakin tietoja, esimerkiksi suunnitelmia ja asiantuntija-arvioita, hankitaan helpoiten juuri henkilökohtaisten kontaktien avulla. Tietoja voi olla helpompi saada suoraan henkilöiltä kuin murtautumalla tietojärjestelmiin tai tiloihin. Kohteena voivat olla monenlaisissa työtehtävissä toimiva yrityksen henkilöstö: yrityksen johto, tutkimus- ja tuotekehityshenkilöstö tai muut avaintehtävissä toimivat.

Työntekijöitä voidaan lähestyä henkilökohtaisesti yhteistyösuhteen luomiseksi ja heihin voidaan kohdistaa tiedonkalastelua sähköpostitse tai sosiaalisessa mediassa. Kohteeksi valikoituneeseen henkilöön yritetään rakentaa verukkeen, esimerkiksi kaupallisen yhteistyön, varjolla yhteistyösuhdetta, jota myöhemmin käytetään hyväksi. Toiminta on arkipäiväistä normaalin verkostoitumisen osana tapahtuvaa tiedonhankintaa, joten sitä voi olla joskus vaikea erottaa tavallisesta yhteistyöstä.

ESIMERKKI:

Suomalaisyrityksen työntekijän kontaktia kiinnostaa kaupallinen yhteistyö ja yrityksen tuotteen viennin edistäminen kotimaassaan. Työntekijä ja kontakti tapaavat useasti muun muassa lounailla, jolloin kontakti pyytää työntekijältä yrityksen julkista materiaalia. Tapaamisten jatkuessa kontakti alkaa kysellä työntekijältä yrityksen tuotteisiin ja tuotekehitykseen liittyviä luottamuksellisia raportteja nähtäväkseen. Työntekijästä tämä on outoa ja hän mainitsee asiasta työpaikallaan, josta ollaan yhteydessä viranomaisiin. Ilmenee, että työntekijän kontakti on epäilty ulkomaisen tiedustelupalvelun edustaja, joka pyrki keräämään tietoa yrityksestä työntekijän avulla.

Yrityksen työntekijöitä siis pyritään manipuloimaan ja käyttämään hyväksi heidän luottavaisuuttaan. Tietojen kalasteluun käytettävää ihmisten manipulointia ja harhaanjohtamista kutsutaan myös social engineeringiksi. Apuna manipuloinnissa ja huijaamisessa voidaan käyttää avoimesti verkosta ja sosiaalisesta mediasta löytyviä tietoja yrityksestä ja sen työntekijöistä.

Tiedot ihmisten työtehtävistä, kollegoista, yhteistyökumppaneista ja harrastuksista voivat kohdentaa lähestymisen sopiviin työntekijöihin sekä auttaa toteuttamaan sen huomaamattomasti. Esimerkiksi sähköposti ei välttämättä näytä epäilyttävältä, jos se väärennetään henkilön kollegan nimissä lähetetyksi tai jos sen sisältö näyttää liittyvän työasioihin.

ESIMERKKEJÄ:

Yrityksen avainhenkilöt saavat asiakasyrityksen nimissä sähköpostia. Mukana on liitetiedosto, jota viestissä kehotetaan klikkaamaan. Tarkemmassa selvittelyssä ilmenee, että asiakasyrityksessä ei ole tietoa tällaisesta viestistä, eikä sitä ole lähetetty kyseisestä yrityksestä. Taustalla oli todennäköisesti kohdistettu hyökkäys, jolla pyrittiin asentamaan haitallinen ohjelma yrityksen tietoverkkoon.

Kansainvälisesti toimivan yrityksen työntekijöille tulee sosiaalisessa mediassa kontaktipyyntöjä ulkomaisen rekrytointiyrityksen edustajilta. Hyväksytyn pyynnön jälkeen työntekijä saa viestin, jossa kehotetaan tutustumaan rekrytointiyrityksen verkkopalveluun viestissä olevasta linkistä. Todellisuudessa rekrytointiyrityksen nimissä olleet profiilit ovat valeprofiileja, ja profiilien kautta lähetetty linkki sisältää haittaohjelman.

Yrityksen työntekijä saa kollegalta sosiaalisessa mediassa viestin, jossa kehotetaan avaamaan linkki ja katsomaan hauska video. Todellisuudessa kollegan sosiaalisen median tili on kaapattu levittämään haittaohjelmaa kyseisen videolinkin välityksellä.

Yrityksen tieto-järjestelmät kohteena

Kohdistetussa haittaohjelmahyökkäyksessä on kyse huolellisesti suunnitellusta toiminnasta ja usein kohteen mukaan räätälöidystä toimintamallista. Tunkeutujan tavoitteena on siis päästä käsiksi nimenomaisesti tietyn organisaation tietoihin tai järjestelmiin. Kohdeorganisaatiosta voidaan kerätä merkittävä määrä hyödyllisiä tietoja pelkästään julkisia lähteitä käyttämällä. Kiinnostavia tietoja ovat sekä sosiaaliset että tekniset tiedot.

Tavoitteena ei välttämättä ole tehdä näkyviä muutoksia kohdejärjestelmissä, vaan hyökkääjä pyrkii pitkäaikaiseen ja huomaamattomaan läsnäoloon voidakseen seurata yrityksen toimintaa. On tärkeää kiinnittää huomiota yrityksen **havainto- ja reagointikyvyn valmiuksiin**, sillä kaikki järjestelmät sisältävät tietoturva-aukkoja ja tehokkaatkaan tekniset menetelmät eivät välttämättä suojaa esimerkiksi inhimillisiltä erehdyksiltä.

Valmistelussa kerättyjä tietoja hyödynnetään hyökkäyksen seuraavissa vaiheissa. Teknisiä tietoja hyödyntämällä voidaan kyetä ohittamaan verkon havainnointijärjestelmät valitsemalla esimerkiksi kohdeverkossa käytettävien järjestelmien ja ohjelmistojen sisältämät tietoturva-aukot eli haavoittuvuudet tai konfiguraatiovirheet. Haittaohjelma voidaan myös sovittaa toimimaan erilaisten kohdeverkossa olevien laitteiden käyttöjärjestelmien mukaisesti.

Sosiaalisen median tietojen perusteella hyökkääjä voi luoda kohdettaan kiinnostavaa sisältöä, jota voidaan tarjota esimerkiksi sähköpostin tai murrettujen sivustojen kautta. Kun sisältö räätälöidään koskemaan kohteelle muutoinkin ajankohtaisia asioita, ei viesti tai sivusto välttämättä herätä kohteen epäilyksiä.

Mitä voin tehdä kehittääkseni yritykseni tietopääoman suojaa?

Olennaista on pyrkiä mahdollisimman tehokkaasti estämään ennalta haitalliset tilanteet ja yritykselle aiheutuvat taloudelliset tappiot. Tämä tarkoittaa riskitilanteiden tunnistamista sekä tarvittavien suojaustoimien toteuttamista.

Henkilöstölle suunnattu koulutus ja viestiminen vahingollisen tiedonhankinnan arkipäiväisyydestä lisäävät henkilöstön turvallisuustietoisuutta ja vaikeuttavat yritykseen kohdistuvaa tietojenkalastelua.

Tämän lisäksi on myös syytä varautua tilanteeseen, jossa vahinkoja on jo syntynyt. Se tarkoittaa tilanteen nopeaa selvittämistä, syntyvien vahinkojen minimoimista, nopeaa toipumista sekä huolellista viestinnän suunnittelua.

Kehittämismalleja yritysten tietopääoman suojaamiseksi

Elinkeinoelämän järjestöt ja viranomaiset ovat laatineet yhdessä koosteen toimenpiteistä, joiden avulla yritys voi pyrkiä kehittämään tietopääomansa suojaa. Kaikki luetellut toimenpiteet eivät välttämättä aina ole tarpeellisia, vaan antavat yrityksille vinkkejä ja ajatuksia omaehtoisen kehittämisen tueksi.

Yksityiskohtaisia lisätietoja käytännön suojauskeinoista ja testauksesta kannattaa tiedustella alan yrityksistä. Myös viranomaisten julkaisemista materiaaleista löytyy yksityiskohtaisempaa tietoa ja ohjeita viranomaisten luottamuksellisen tiedon suojaamisesta.

Kuka voi auttaa ja miten?

Liikesalaisuuksien suojaan perehtynyt asiamies

Liikesalaisuuksien suojaan perehtynyt asiamies voi selvittää yritykselle parhaiten soveltuvat reagointikeinot eri tilanteissa. Yhdessä voitte harkita, tuleeko asiasta tehdä tutkintapyyntö viranomaiselle ja mitä muita keinoja on käytössä.

Poliisi

Mikäli epäilet yrityksesi joutuneen rikoksen uhriksi, voi ottaa yhteyttä poliisiin rikosilmoituksen tekemistä varten. Yhteydenotto poliisin ei kuitenkaan välttämättä pakota rikosilmoituksen laatimiseen, vaan poliisi voi myös antaa ohjeita ja neuvoja tilanteen ratkaisemiseen. Mikäli kyse on selkeästi tietoverkkorikoksesta, voit olla myös yhteydessä suoraan keskusrikospoliisin kyberrikostorjuntakeskukseen.

Suojelupoliisi

Suojelupoliisi vastaa ulkomaisten tiedustelupalveluiden Suomessa ja Suomen etuja vastaan toteuttaman tiedustelutoiminnan havaitsemisesta ja torjumisesta sekä siten osaltaan suomalaiseen elinkeinoelämään kohdistuvan valtiollisen tiedustelun estämisestä. Suojelupoliisin vastatiedusteluyksikkö käsittelee tilanteet, joissa yrityksessä epäillään tiedustelun kohteeksi joutumista. Kyse voi olla onnistuneesta tai yritykseksi jääneestä tiedonhankinnasta. Lisäksi Suojelupoliisissa tuotetaan tutkimusta, analyysia ja ennalta estävää turvallisuustietoa yritysten käyttöön. Turvallisuusselvitysyksikössä tehdään henkilö- ja yritysturvallisuusselvityksiä.

Viestintäviraston kyberturvallisuuskeskus

Viestintävirasto ylläpitää viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Voit ilmoittaa kyberturvallisuuskeskukseen tietoturvaloukkauksista sekä kysyä ohjausta ja neuvoja ongelmatilanteissa.

Tulli

Tullin tehtäviä ovat tullaukseen- ja verotukseen, valvontaan, yritystarkastuksiin sekä rikostorjuntaan (analyysi ja tutkinta) liittyvät asiat.

Huoltovarmuuskeskus

Huoltovarmuuskeskuksen tehtävänä on maan huoltovarmuuden ylläpitämiseen ja kehittämiseen liittyvä suunnittelu ja operatiivinen toiminta. Tehtävänä on yhteistyössä muiden viranomaisten ja elinkeinoelämän kanssa varmistaa, että yhteiskunnalle kriittisimmät järjestelmät toimivat kaikissa tilanteissa.

Järjestöt

Elinkeinoelämän järjestöt antavat neuvontaa ja julkaisevat ohjeita yrityksille erilaisissa turvallisuusasioissa sekä pyrkivät lisäämään yritysten tietoisuutta ja osaamista ennalta estävistä toimenpiteistä.

JOHTAMINEN JA RISKIENHALLINTA

Yritys tiedostaa, tunnistaa ja hallitsee tietopääomaan kohdistuvia riskejä

Tunnista, luokittele ja merkitse yrityksesi keskeinen tietopääoma

- Tunnista yrityksesi kriittinen suojattava tieto
- Dokumentoi kriittinen tieto, jotta voit osoittaa yrityssalaisuuden olemassaolon ja sisällön tietyllä hetkellä

Muuta

- Muista, että myös merkitsemätön materiaali voi olla luottamuksellista
- Kaikkein sensitiivisimmän tiedon kirjaamista voi olla syytä välttää

Arvioi tietopääomaan kohdistuvat riskit

- Arvioi riskit ja suhteuta suojausmenetelmät riskeihin
- Käytä arvioinnissa säännöllistä, järjestelmällistä ja dokumentoitua menettelyä
- Huomioi arvioinnin tulokset toiminnan tavoitteita asetettaessa ja henkilöstön koulutusta suunniteltaessa
- Arvioi jatkuvasti valittujen suojaustoimenpiteiden vaikutusta ja muodosta käsitys niiden panos-tuotos -suhteesta
- Tunnista tietopääomiin kohdistuvat riskit myös palvelu- ja alihankinnassa

Muuta

- Koita kartoittaa tilannetta esimerkiksi haavoittuvuusanalyysin avulla
- Arvioi huolella minkälaisen jäännösriskin voit hyväksyä
- Riskienarvioinnin avulla voit suunnata ja priorisoida turvallisuustyötä

Viestintä ja vakuutusturva

- Laadi sisäinen ja ulkoinen viestintä-suunnitelma loukkaustapauksia varten
- Muista selvittää vakuutusturva

Laadi yritys- ja liikesalaisuuksien suojaa koskevat säännöt ja ohjeet

- Pidä ohjeisto kaikkien saatavilla, kouluta henkilöstöä ja kannusta raportointiin
- Päivitä ohjeistoa ja sitoudu jatkuvaan kehittämiseen
- Harkitse aina kenelle on tarpeen luovuttaa yrityksen luottamuksellista tietoa (”Need to know” – kuka tarvitsee, mitä ja miksi?)
- Valvo sääntöjen noudattamista ja puutu loukkauksiin. Huomio myös mahdollisten rikkomusten seuraamukset.
- Ohjeista myös luottamuksellisen tiedon vastaanottaminen (onko luovuttajalla oikeus luovuttaa tietoa sinulle ja onko sinulla oikeus luovuttaa sitä edelleen ja millä ehdoilla)
- Tee suunnitelma poikkeamatilanteiden varalle

Muuta

- Muista huolehtia yrityssalaisuuksien suojasta myös mahdollisen viranomaisprosessin aikana
- Harjoittele poikkeustilanteiden varalle

Sisällytä tietopääoman suojaa koskevat asiat sopimuksiin ja tarjouspyyntöihin

- Laadi salassapitosopimus tai ota salassapitoehto henkilöstön työsopimuksiin
- Sovi tiedon salassapidosta sopimuksin yhteistyökumppanien kanssa tilanteissa joissa salaista tietoa luovutetaan yrityksen ulkopuolelle
- Määrittele minkälaisia oikeuksia yhteistyökumppanilla on luovuttaa tietoa edelleen
- Muista salassapitosopimukset palvelu- ja alihankinnassa

HENKILÖSTÖ

Yrityksen henkilöstöpolitiikka tukee tietopääoman suojaa

Laadi ohje yrityksen rekrytointimenettelystä ja sovella sitä rekrytoinnissa

- Työnhakijalta pyydetään aina tiedot vähintään opinto- ja työhistoriasta sekä suosittelijoista
- Hakijan antamien tietojen oikeellisuus pyritään aina vahvistamaan (esimerkiksi haastattelun yhteydessä)
- Huomioi rekrytoitavan aiempien työsuhteiden aiheuttamien mahdollisten luottamuskysymysten vaikutus valintaan
- Muista rekrytoitavan mahdollisten nykyisten yrityskytkentöjen selvittäminen
- Harkitse henkilö- ja soveltuvuusarviointitestauksen käyttöä
- Muista, että tietyissä tapauksissa huumausainetestaus on mahdollista
- Muista, että tietyissä tapauksissa luottotietojen hankkiminen on mahdollista
- Käytä koeaikaa

Muuta

- Selvitä myös mahdollisuus turvallisuusselvitysmenettelyn käyttämiseen (kts. Turvallisuusselvityslaki 723/2014)

Lisää henkilöstön osaamista ja valmiuksia

- Kouluta henkilöstöä tunnistamaan riskitilanteita ja toimimaan niissä oikein
- Kannusta oikeaan toimintaan, anna palautetta ja rohkaise kysymään
- Pyri havaitsemaan ajoissa huomattavat muutokset käytöksessä tai toiminnassa

Muuta

- Muista, että kaikkien käyttäjien valppaus sekä jatkuva raportointi mahdollisista riskitilanteista on tärkeää. Harkitse myös mahdollisuutta anonyymiin raportointiin

Määrittele työntekijän tehtävät, vastuut, oikeudet ja velvollisuudet

- Laadi järjestelmällinen ja dokumentoitu perehdytysprosessi
- Sisällytä henkilön perehdyttämiseen salassapidettäviä tietoja koskeva koulutus
- Pidä salassapitoa koskeva ohjeisto henkilökunnan saatavilla
- Laadi menettelyohjeet epäiltäessä väärinkäytöksiä

Muuta

- Muista salassapito- ja vaitiolosopimukset sekä sopimussakkoehdon käyttö
- Esimerkiksi päihde- tai peliriippuvuudet voivat altistaa väärinkäytöksille
- Arvioi tarve kilpailukieltosopimuksen käytölle

Laadi menettelyohje toimenpiteistä työsuhteen päättyessä

- Muista poistaa välittömästi käyttöoikeudet yrityksen tietojärjestelmiin
- Muista avaimien ja kulkukorttien palautus sekä kulkuoikeuksien poistaminen
- Muista lähtevän työntekijän työvälineiden palautus (esim. puhelin, tietokoneet)
- Käy lähtevän henkilön lähtökeskustelu, jossa muistutetaan yrityksen tietopääoman suojasta

Muuta

- Hyvän toimintatavan noudattaminen työsuhteen päättyessä on tärkeä turvallisuuskysymys

TOIMITILAT

Yritys estää luvattoman tunkeutumisen tiloihinsa

Huomioi yrityksen toimitilojen ja lähialueen ominaisuudet osana yrityksen tietopääoman suojaa

- Huolehdi tilojen ulkokuoren kulkureittien ja aukkojen riittävästä suojauksesta ja lukitsemisesta (ikkunat, ovet, luukut yms.)
- Huomioi rakenteiden materiaalit ja kestävyys
- Huolehdi avaintenhallinnasta järjestelmällisesti (avainluettelot, lukostokaaviot ja avainkortit)
- Säilytä suojattavaa materiaalia huolellisesti. Arvioi tarvitsetko kassakaapin tai holvin suojattavan materiaalin säilyttämistä varten
- Pyri käyttämään sertifioituja ja vakuutusyhtiöiden hyväksymiä tuotteita
- Arvioi tarpeesi yrityksen lähialueen ja ympäristön suojan parantamiseen (aidat, portit ja ajoesteet) (kts. Turvallisuusselvityslaki 723/2014)

Muuta

- Selvitä myös kenellä on yleisavaimia tiloihisi ja mihin tiloihin niillä pääsee
- Muista paloturvallisuus

Kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmän sekä vartiointipalveluiden käyttö

- Hallinnoi tilojen kulkuoikeuksia järjestelmällisesti ja laadi asiasta ohjeistus (oikeuksien myöntäminen ja käsittely)
- Pyri käyttämään vakuutusyhtiöiden hyväksymiä tuotteita
- Testaa järjestelmien ja palveluiden toimintaa säännöllisesti
- Huomioi kameravalvonnan toimivuus eri olosuhteissa (riittävä valaistus pimeällä)
- Muista huomioida kameravalvontaa koskeva lainsäädäntö

Muuta

- Vastuuta kulkuoikeuksien hallinta selkeästi esimerkiksi nimeämällä vastuuhenkilö. Huolehdi myös oikeuksien muuttamisen ohjeistuksesta ja järjestelmällisyydestä
- Rikosilmoitinärjestelmä antaa ilmaisun toiminnasta ja mahdollistaa vastatoimenpiteiden aloittamisen
- Kameravalvonnalla voit nostaa luvattomaan toimintaan ryhtymisen kynnystä tiloissasi
- Muista, että kulunvalvonnan avulla voidaan todentaa henkilöiden liikkumista tiloissa myös jälkikäteen

Laadi toimenpideohjeet vierailijoiden hallitsemiseksi yrityksen tiloissa

- Laadi ohje vierailukäytännöistä yrityksen tiloissa
- Pohdi mihin tiloihin vierailijoita kannattaa päästää
- Pohdi mikä on sopiva tapa tunnistaa vieraat (esim. näkyvillä pidettävä vierailijakortti tai muu vastaava)
- Kouluta vierailijaohje henkilöstölle ja valvo sen noudattamista

Muuta

- Huomioi mitä haluat näyttää yrityksesi toiminnasta. Kaikki vierailijat eivät välttämättä ole vain tutustumassa toimintaasi vilpittömässä mielessä. Älä jätä vieraita valvomatta tärkeisiin tiloihisi. Arvioi myös kuvaamisen rajoittamisen tarvetta
- Muista huomioida myös ulkopuolisten suorittamien huolto- ja siivoustöiden käytännöt ja valvontatarpeet
- Pyydä vierailijoita allekirjoittamaan vierailun aikana havaitsemien liikesalaisuuksien salassapitoa koskeva sitoumus

TIETOLIIKENNE, -JÄRJESTELMÄT JA LAITTEET

Yrityksen tietojärjestelmät ja laitteet ovat riittävän turvallisia

Huolehdi yrityksen arkipäivän tietoturvallisuudesta

- Muista käyttäjien tunnistaminen sekä salasanojen käyttö ja hallinnointi
- Huolehdi palomuuri ja haittaohjelmien torjunta kuntoon
- Muista huolehtia laitteiden asianmukaisesta päivityksestä
- Pidä laite- ja ohjelmistorekisteriä
- Hanki laitteet ja ohjelmistot vain luotetuista ja luvallisista lähteistä
- Määrittele periaatteet ja toimintatavat ohjelmistojen, tietoliikenneyhteyksien ja laitteiden asentamiseen
- Määrittele periaatteet ja ohjeet etä- ja matkatyön aiheuttamia riskejä vastaan
- Muista mobiililaitteiden tietoturvallisuudesta huolehtiminen
- Huolehdi langattoman verkon salauksesta
- Käytä luotettavia salausohjelmistoja
- Muista tyhjentää luottamuksellista tietoa sisältävät laitteet niiden käytöstä poistamisen yhteydessä (joskus myös laitteiden mekaaninen hävittäminen voi olla tarpeen)

Muuta

- Käytä osaavaa henkilöstöä ja osta palvelut luotettavalta palveluntuottajalta. Muista, että vastuusi yrityksesi turvallisuudesta ei siirry palveluiden ulkoistamisesta huolimatta

Seuraa muuttuvaa toimintaympäristöä

- Muista tietoturvaloukkausten ilmoituspiste ja tilannekuvatietojen seuranta
- Tietoturvaloukkausten havainnointi
- Muista haavoittuvuuskoordinointi

Muuta

- Viestintäviraston lyberturvallisuuskeskus:
- Seuraa uutisia ja liity postituslistalle: http://www.viestintavirasto.fi/kyberturvallisuus.html
- Ilmoita Viestintävirastolle: cert@ficora.fi

Kasvata havaintokykyä

- Valvo yrityksen tietoverkkoa ja järjestelmien käyttöä mahdollisimman kattavasti
- Muista lokimenettelyjen käyttö ja säilytys
- Kouluta ja kannusta henkilöstöä raportoimaan havainnoistaan
- Harkitse voitko saada hyötyä ulkopuolisesta vertaisarvioinnista

Muuta

- Muista, että täysin luotettavaa järjestelmää ei ole olemassa
- Harkitse esimerkiksi hackathon-tilaisuutta

Kasvata sietokykyä

- Huomioi ja suunnittele tietojärjestelmien vika- tai poikkeamatilanteesta toipuminen
- Huolehdi varmuuskopioinnista
- Pyri minimoimaan vahingot: älä säilytä kaikkea tietoa yhdessä paikassa

Muuta

- Varaudu häiriöihin ja suunnittele miten toivut niistä mahdollisimman nopeasti
- Halutessasi voit myös eriyttää tietojärjestelmäsi kokonaan muusta verkosta. Se lisää suojausta, mutta muista kuitenkin, että sekään ei ratkaise kaikkea, sillä myös erillisjärjestelmiin voidaan luoda pääsy

Elinkeinoelämän keskusliitto

PL 30 (Eteläranta 10), 00131 Helsinki
Puh. 09 420 20
Fax 09 4202 2299
www.ek.fi

Raportti internetissä:
www.ek.fi

Ulkoasu: Arja Nyholm, Jumo Oy

EK 2017

Lähteet ja lisätietoja:

Sisäministeriön yritysturvallisuuden yhteistyöryhmä

Vapaavuori, Tom:
Yrityssalaisuudet,
liikesalaisuudet ja
salassapitosopimukset,
Talentum Pro, Helsinki 2016