TIETOTURVAN VAIKUTUS LIIKETOIMINTAAN

Sisällys

Lukijalle

Kyberturvallisuus ja tietoturva-asiat alkavat hiljalleen nostaa päätään monissa johtoryhmän kokouksissa. Vähitellen yritykset meillä Suomessakin alkavat ymmärtää, ettei tietoturvaa voida enää täysin sivuuttaa, mikäli yrityksen toiminnan halutaan pysyvän kilpailukykyisenä. Moni kuitenkin pohtii, millaisia toimenpiteitä tietoturvan tason kohentamiseksi tarvittaisiin? Kuinka varmistutaan siitä, että tietoturvaan laitettavat panostukset ovat juuri oikealla tasolla liiketoimintaan nähden? Tietoturvaan voidaan panostaa myös kustannustehokkaasti, kunhan investoinnit suunnitellaan huolellisesti ja ammattitaidolla. Kun tietoturvaan laitetaan panostuksia, kannattaisi sitä käyttää myös markkinoinnissa, jolloin siitä voi muodostua kilpailuetua tuova tekijä.

Tämä opas on suunnattu niille, jotka pohtivat edellä olevia kysymyksiä ja kaipaavat lisätietoa tietoturvan panostuksien hyötysuhteesta. Oppaan tarkoituksena on avata näkökulmia tietoturvan liiketoiminnallisille vaikutuksille läpi organisaation. Toivottavasti materiaali vastaa myös sinun kysymyksiisi.

Antoisia lukuhetkiä toivottaa,
Xcure Oy

Hyvin hoidetun tietoturvan merkkejä

Tietoturvan tulisi olla jalkautettuna organisaation liiketoimintakulttuuriin ja olla osana päivittäistä toimintaa. Koko henkilökunnan tulisi olla tietoisia tietoturvasta ja sen merkityksestä, sekä puuttua mahdollisiin poikkeamiin. Tämä poikkeavuuksien huomaaminen kertoo myös tietoturvatietoisuudesta.

Myös tietojen luokittelun tulisi olla olennainen osa toimintatapaa. Kaikki yrityksen tieto tulee luokitella sen mukaisesti, kuinka kriittistä kyseinen tieto on. Yritys voi itse määrittää luokittelutasot, mutta esimerkiksi julkishallinnon puolella käytetään neljää tasoa – julkinen, sisäinen, luottamuksellinen ja salainen. Mikäli tietoa ei luokitella, henkilöstö ei voi esimerkiksi tietää, mistä saa puhua julkisesti, ja mikä tieto taas täytyy jättää täysin yrityksen seinien sisälle.

Sen lisäksi, että kaikki tieto tulee luokitella, tiedoilla täytyy olla myös omistaja. Tähän ei kiinnitetä yrityksissä riittävästi huomiota. Kaikella tiedolla tulisi olla omistaja, jonka vastuulla on huolehtia tiedon suojauksesta, käyttöoikeuksista ja luokittelutasosta. Tiedon omistajuus määräytyy sen mukaisesti, ketä tieto eniten koskettaa tai kellä on vankin näkemys tiedon merkityksestä ja käyttötarkoituksista.

Tietoturvaan tarvitaan ennen kaikkea kokonaisvaltaista lähestymistapaa. Kaikista tärkeintä tietoturvallisuuden kannalta on tunnistaa yrityksen toimintaa uhkaavat riskit ja varautua niihin liiketoiminnan luonteen edellyttämällä tavalla - kustannustehokkaasti.

Tiesitkö?

Monet tuudittautuvat tietoturvan olevan hyvällä tasolla, kun esimerkiksi IT-infraan liittyvät palvelut on ostettu ulkopuoliselta palveluntarjoajalta. Ulkoistettujen toimittajien tilat ja työmenetelmät olisi kuitenkin syytä auditoida tietoturvan kannalta, jotta jälkikäteiseltä selvittelyltä vältytään esimerkiksi silloin, jos yrityksen tietoverkkoihin on murtauduttu. Osapuolten vastuut tulisi myös kirjata yhteistyösopimukseen.

Riippumatta siis siitä, ostetaanko palveluita yrityksen ulkopuolelta vai hoidetaanko toimintaa itse, yrityksen vastuulla on itse varmistua, että tietoturva- ja tietosuoja-asiat ovat asianmukaisella tasolla. Kaikilla osapuolilla tulee olla selkeä näkemys omista vastuistaan ja vastuun rajoituksista.

XCURE

Uhkien ennakointi jatkuvuuden mahdollistajana

Useimmilla yrityksillä on sellaista tietoa, jota ei missään olosuhteissa haluta jakaa muiden, etenkään kilpailijoiden kanssa. Kaikella yrityksen kriittisimmällä tiedolla on usein liiketoiminnan kannalta jopa merkittävää taloudellista arvoa, ja tällöin se lähes väistämättä kiinnostaa muita. Jos tieto on riittävän arvokasta, siihen pyritään pääsemään käsiksi keinolla millä hyvänsä. Tietojen varastaminen ei nykypäivän teknologian avulla ole edes valtavan haasteellista, ellei yritys ole varautunut tietomurtoihin etukäteen. Muista myös, että murtautumiseen ei välttämättä tarvita edes verkkoa – tietoturvallisuus on ennen kaikkea yhdistelmä fyysistä ja teknistä turvallisuutta. Tietojen varastamisen lisäksi hyökkäykset voivat aiheuttaa toiminnan kannalta kriittisten tietojen menettämisen.

Käytännössä yksikään yritys ei ole täysin turvassa hyökkäyksiltä. Hyvä uutinen kuitenkin on, että vaikka erilaiset tietomurrot ja hyökkäykset ovat lisääntyneet valtavasti, hyvällä suunnittelulla ja ennakoinnilla niiden vaikutukset liiketoimintaan pystytään minimoimaan. Kun yritykselle on tehty tietoturvan kypsyysanalyysi ja laadittu jatkuvuudenhallintasuunnitelma, jota noudatetaan, yritys yleensä pystyy jatkamaan toimintaansa normaalisti, vaikka pahin tapahtuisi ja järjestelmät joutuisivat hyökkäyksen kohteeksi.

Tietoturvan kypsyysanalyysi

Tietoturvaan liittyvä kypsyysanalyysi suoritetaan koko yrityksen toiminnan näkökulmasta. Kypsyyden arvioinnissa hyödynnetään yrityksen tarpeen mukaisia viitekehyksiä, kuten ISO27k. Kypsyysanalyysiin sisältyy tietoturvan tarkastelua ja analysointia työvälineiden, prosessien ja ihmisten näkökulmista.

Työvälineillä tarkoitetaan tässä yhteydessä fyysisiä sijainteja, tietoinfrastruktuuria (tietoverkot ja tietojärjestelmät palvelinympäristöineen ja päätelaitteineen) ja IoT-ympäristöä. **Prosesseja** tarkastellessa kiinnitetään huomiota kaikkiin sovittuihin tai ennalta sopimattomiin toimintatapoihin ja työmenetelmiin, joita yrityksessä vallitsee, sekä erilaisiin sopimuksiin, kuten lainsäädännöllisiin ohjeistuksiin. **Ihmisten** analyysi taas käsittää esimerkiksi yrityksen työntekijät, yhteistyökumppanit ja asiakkaat sekä niihin liittyvät toimintatavat. Esimerkiksi, onko yhteistyökumppanillamme pääsy joihinkin järjestelmiimme? Kuinka kirjautumisten ja pääsyoikeuksien valvonnasta on huolehdittu?

Kuten edelläkin jo mainitsimme, pohdi tietoturvallisuutta myös verkon tai järjestelmien ulkopuolelta. Onko esimerkiksi henkilöstön tai yhteistyökumppaneiden pääsyä rajattu tiettyihin tiloihin, tai onko ulkopuolisella henkilöllä minkäänlaista mahdollisuutta päästä luottamuksellisiin aineistoihin käsiksi? Pohdi tätä asiaa huolellisesti ja tunnista mahdolliset riskit myös muutoin, kuin verkon tai järjestelmien suojauksen osalta.

Heikon tietoturvan vaikutukset liiketoimintaan

Maineen menetys. Sana tietoturvan pettämisestä leviää nopeasti, haluttiin sitä tai ei. Myös ”puskaradio” levittää tietoa kulovalkean lailla, niin hyvässä kuin pahassa. Vaikka tietomurto ei koskettaisikaan asiakkaan tietoja, voi se silti heikentää luottamusta yritykseen. Tämä voi johtaa asiakkaiden ja työntekijöiden menettämiseen kilpailijoille. Myös toimittajasuhteet voivat vaarantua ja aiheuttaa yhteistyön päättymisen.

Liikesalaisuuksien varastaminen. Yrityksen liikesalaisuuksien, tuotekehitystietojen ja muiden luottamuksellisten tietojen varastaminen voi johtaa kilpailevan yrityksen perustamiseen markkinoille ja viedä merkittäviä markkinaosuuksia.

Lainsäädännölliset seuraukset. Heikosti hoidettu tietoturva voi aiheuttaa seurauksia mm. tietosuojalain puitteissa. Viranomainen voi määrätä yritykselle sakkoja tai jopa estää liiketoiminnan harjoittamisen.

Liiketoiminnan keskeytykset. Laitteiston tai järjestelmien kaatuminen voi tehdä yrityksen täysin toimintakyvyttömäksi pidemmäksikin aikaa. Järjestelmiä ja prosesseja voidaan joutua rakentamaan uudelleen, mikä aiheuttaa viivästyksiä ja taloudellista vahinkoa.

Taloudelliset tappiot. Tietoturvaloukkaukset voivat aiheuttaa suoria taloudellisia menetyksiä yritykselle. Tietoturvan rikkoutumisesta voi aiheutua mm. korvausvaatimuksia, sakkoja ja oikeudenkäyntikuluja. Lisäksi ne voivat vaikuttaa esim. yrityksen tuottavuuteen ja rahoituksen saatavuuteen.

Liiketoiminnan kaatuminen. Vakavat tietoturvaloukkaukset voivat johtaa jopa koko yrityksen kaatumiseen. Jos kaikki yrityksen toiminnan kannalta oleellinen tieto katoaa esim. kiristyshaittaohjelman vuoksi, voi toiminnan jatkaminen muodostua mahdottomaksi. Lisäksi maineen menetys voi estää uusien asiakkaiden hankkimisen ja olemassa olevien menettämisen, mikä lopulta johtaa konkurssiin sekä työpaikkojen ja sijoitusten menettämiseen.

Tietoturvan jatkuva kehitys

Kun yritys huolehtii tietoturvastaan hyvin, kaikki edellä mainitut uhkakuvat kääntyvät päälaelleen. Hyvin hoidetulla tietoturvalla voidaan turvata liiketoiminnan jatkuvuus yllättävissäkin tilanteissa ja turhalta vaivalta ja ylimääräiseltä työltä vältytään. Myös asiakkaiden ja kumppaneiden luottamus yrityksen toimintaan kasvaa, kun tietoturvasta huolehditaan ja se myös tuodaan julki.

Toki tietoturvan tason parantaminen ja ylläpito vaativat investointeja. Jos tietoturvatason säilyttämiseksi vaaditaan esimerkiksi järjestelmien kahdentamista, tarkoittaa se helposti myös kaksinkertaisia kustannuksia. On hyvä kuitenkin miettiä, otetaanko riski tietojen menetyksille, varkauksille tai toiminnan häiriöille, vai kärsitäänkö investointien vaatimat kustannukset ja varmistetaan toiminnan jatkuvuus.

On syytä myös muistaa, että tietoturva ei ole koskaan 100 % valmis. Yrityksen tulee jatkuvasti ylläpitää tilannekuvaa oman organisaation tietoturvan tilasta. Uusia järjestelmiä ja teknologioita kehitetään ja otetaan käyttöön jatkuvasti, mikä taas synnyttää täysin uusia tietoturva-aukkoja ja uhkia. Kyberrikollisuus on käytännössä aina pienen askeleen edellä suojautumismenetelmiä, mutta mikäli tietoturva-asioihin panostetaan ja kiinnitetään yrityksessä riittävästi huomiota, uudetkaan uhkat eivät suorilta käsin uhkaa liiketoiminnan jatkuvuutta.

Tiesitkö?

Organisaatioiden suurimmat kyberuhat

1. Kiristysohjelmahyökkäykset
Hyökkäykset, joissa kyberrikolliset ottavat haltuunsa kohteen ja vaativat lunnaita sen saatavuuden palauttamiseksi.

2. Palvelunestohyökkäykset
Hyökkäykset, joissa käyttäjiltä estetään pääsy tarvittaviin tietoihin tai palveluihin.

3. Haittaohjelmat
Haittaohjelmilla pyritään vahingoittamaan tai häiritsemään laitetta tai hankkimaan siihen luvaton pääsy.

4. **Käyttäjän manipulointi**
Hyökkäykset, joissa yritetään käyttää hyväksi inhimillistä virhettä tietoihin pääsemiseksi.

5. Dataan kohdistuvat hyökkäykset
Hyökkäykset, joilla pyritään saamaan laittomasti dataa.

(Lähde: EU:n kyberturvallisuusvirasto)

XCURE

Tietoturvan onnistumisen mittaaminen

Tietoturvan onnistumista on haastavaa mitata suoranaisesti taloudellisilla tai muilla määrällisillä mittareilla. Kuitenkin mittaaminen voi joissain tapauksissa onnistua, jos pystytään esittämään, kuinka paljon tietoliikennekatkoksista on koitunut aiemmin haittaa toiminnalle. Esimerkiksi, jos edellisvuonna tietoliikennekatkokset ovat aiheuttaneet saamattomina myyntituloina tappiota 50 000 euroa ja tietoliikenteen kahdentaminen maksaa 20 000 euroa vuodessa, niin kahdentamisen jälkeenkin hyödytään vielä 30 000 euroa. Tämä on kuitenkin vain karkea esimerkkilaskelma. Usein erilaisia panos-hyöty – laskelmia voidaan tehdä asiakas- ja tapauskohtaisesti, mutta ne vaativat jo hieman enemmän ajatusta.

Toisaalta tietoturvan mittaamista voidaan tehdä myös takaisinmaksuajan kautta. Takaisinmaksuaika määritetään laskemalla jokaiselle tietojen menetykselle riskianalyysin kautta hinta, eli jokainen riski arvioidaan euroissa: ”Miten tämän tiedon menetys näkyisi liiketoiminnassamme?”. Menetykset työajassa, brändin maineessa ja toimituksissa summataan yhteen, ja summaa verrataan tietoturvaan vaadittaviin panostuksiin. Usein tietojen menetyksestä aiheutuvat kustannukset ovat huomattavasti suuremmat kuin niiden suojaamiseen vaadittavat panostukset, jolloin panostukset on helppo perustella yrityksen sisällä.

Perusasiat kuntoon

Vaikka kyberhyökkäykset ovat esillä yhä enenevissä määrin, ei perustavanlaatuisia tietoturvaan liittyviä käytäntöjä pidä unohtaa: esimerkiksi papereita ei tulisi heittää suoraan paperinkeräykseen, vaan ne tulisi tuhota esimerkiksi silppuamalla. On olemassa jopa esimerkkitapauksia, joissa yrityksiä on haastettu oikeuteen, kun niiden paperiroskien seasta on löytynyt salassa pidettäviä tietoja.

Pohdi myös, onko yrityksessä sovittu mitään tietojen tallentamisesta liikuteltaville laitteille ja miten niiden tietoturvasta on huolehdittu? Onko yrityksellä prosessit tietojen hävittämiseksi käytöstä poistuvilta laitteilta?

Edellä olevien esimerkkien kautta on hyvä muistaa, että myös tulostettujen ja liikuteltavilla muistivälineillä olevien tietojen suojaus on tärkeää, eikä tietoturvallisuudessa aina ole kyse pelkästään verkkoon liittyvistä asioista.

Kolme merkittävää uhkaa ja toimintaohjeet

1. Päivittämättömät ohjelmistot

Haavoittuvuudet ovat avoin ovi rikollisille ja niitä hyväksikäytetään yhä nopeammin. Päivittäkää laitteet ja ohjelmistot mahdollisimman pian, mieluiten heti korjausten ilmestyttyä.

2. Inhimillinen tekijä

Henkilöstön osaamattomuus ja kehittyneet, tekoälyn avulla luodut erittäin vaikuttavat huijaukset aiheuttavat suuren uhan. Kouluttakaa henkilöstöänne tunnistamaan huijauksia ja tarkistakaa toimintaprosessejanne.

3. Toimitusketjun haavoittuvuus

Vaikka oman organisaation tietoturva on kunnossa, niin alihankintaketju voi olla haavoittuva. Kartoittakaa kaikki käyttämänne alihankkijat, varmistukaa niiden tietoturvasta ja huolehtikaa sopimusten ajantasaisuudesta.

XCURE

Tietoturva suomalaisissa yrityksissä

Suomalaisten yritysten ymmärrys tietoturvasta vaihtelee paljon toimialasta ja koosta riippuen. Ne yritykset, joilla on liikesalaisuuksia ja kriittisiä tietoja yrityksen toiminnan kannalta, kuten tuotekehitystä koskettavia asioita, ovat yleensä hyvin perillä tietoturvan merkityksestä ja tärkeydestä.

Monissa yrityksissä, etenkin PK-sektorilla, kuitenkin edelleen vähätellään tietoturvan merkitystä ja kuvitellaan haittaohjelmasuojauksen riittävän tietoturvan ylläpitoon.

Yleensä tietoturvan heikkoudet kuitenkin paljastuvat mentäessä syvemmälle prosesseihin, käytäntöihin ja työkaluihin. Vaikka yritys ei omasta mielestään käsittelisi kriittisiä tietoja, tulee sen huomioida toiminnassaan vähintäänkin tietosuojalaki ja sen velvoitteet.

Jokaisen yrityksen velvollisuus on tunnistaa kaikki käsiteltävät henkilötiedot. Henkilötietojen käsittelyä kartoitettaessa ja dokumentoidessa, voidaan samalla helposti kartoittaa myös muut yrityksen toiminnan kannalta tärkeät tiedot ja miettiä niiden suojausta. Tämän osalta on vielä paljon tekemistä kaikissa suomalaisissa yrityksissä.

Tiesitkö?

Suomalaisten yritysten heikkous on myös niin sanottu ”aivovuoto”, eli työhön pätevien ihmisten lähtö yrityksestä.

Kun työntekijä lähtee yrityksestä ja vaihtaa työpaikkaa, seuraukset voivat olla vakavat. Työntekijä vie mukanaan valtavan määrän arvokasta, jopa arkaluonteista tietoa pois yrityksestä.

Tästä syystä myös henkilöstöhallinto olisi syytä ottaa mukaan tietoturvakeskusteluihin ja yhdessä pyrkiä kehittämään keinoja, joilla työntekijöitä sitoutetaan yritykseen vahvemmin. Lisäksi työntekijöiden elinkaaren suunnitteluun tulee panostaa ja miettiä prosessi poistuville työntekijöille.

Lisätietoa aiheesta

Toivottavasti materiaalimme tarjosi sinulle lisätietoa tietoturvaan liittyen ja vastasi sinulla mahdollisesti avoinna olleisiin kysymyksiin. Mikäli jokin jäi vielä askarruttamaan, otathan yhteyttä Xcuren asiantuntijoihin. Autamme mielellämme kaikissa tietoturvaa koskevissa asioissa!

Tutustu myös blogiimme, jossa käsittelemme tietoturvaan, tietosuojaan, kyberturvallisuuteen ja tiedonpalautukseen liittyviä aiheita!

Xcure Oy on tietosuojaan ja tietoturvaan erikoistunut palvelu- ja ohjelmistoyritys. turvapalveluja tuottava ohjelmisto- ja asiantuntijayritys. Olemme auttaneet asiakkaitamme tietoturvan ja tietosuojan haasteissa jo vuodesta 2006. Olemme kehittäneet asiakkaidemme pyynnöstä mm. Tietosuojatyökalun, joka auttaa organisaatioita toimimaan lainsäädännön vaatimalla tavalla.