TIETO- JA KYBERTURVALLISUUS

DIGITAALINEN TURVALLISUUS ON YHÄ TÄRKEÄMPÄÄ

Digitaalisella turvallisuudella on yhä keskeisempi osa yritysturvallisuuden kokonaisuutta ja se käsittää tietoturvallisuuden, kyberturvallisuuden sekä jatkuvuuden hallinnan ja varautumisen.

Tietoturvassa on järjestelmien, ohjelmistojen, laitteiden ja verkkojen suojaamisen lisäksi kyse myös liiketoimintaprosesseista sekä ihmisten käyttäytymisestä ja asenteista. Hyvin rakennettu digitaalinen turvallisuus suojaa merkittävästi yrityksen toimintakykyä.

Digitaalisen omaisuuden turvaamisella on myös tärkeä osa toimintakyvyn varmistamisessa. Varmuuskopioista, tiedon eheydestä ja sen saavutettavuudesta on huolehdittava kaikissa olosuhteissa. Olennaista on lisäksi hallita pääsyoikeuksia, jotta henkilöillä on pääsy oikeisiin järjestelmiin ja oikeudet päivittyvät työsuhteen elinkaaren mukaan.

KYBERUHAT OVAT MONINAISIA

Kyber-termi viittaa sähköisessä muodossa olevan informaation käsittelyyn eli tietotekniikkaan ja -järjestelmiin sekä tiedonsiirtoon. Kyberriskit ovat eri organisaatioissa erilaisia.

Kyberuhat ovat haitallisia tapahtumia tai kehityskulkuja, jotka voivat vaikuttaa organisaation toimintaan, talouteen, sen hallussa olevaan tietoon ja pahimmillaan jopa liiketoiminnan jatkuvuuteen.

Tyypillisiä haavoittuvuuksia ovat:

Tietojenkalastelun tavoitteena on saada rikollisten haltuun käyttäjätunnus- ja salasanapareja tai muita käyttäjälle tai organisaatiolle arvokkaita tietoja.

Haittaohjelmat ovat tietokoneohjelmia, jotka aiheuttavat ei-toivottuja tapahtumia tietojärjestelmässä tai sen osissa.

Kiristyshaittaohjelmat lukitsevat tiedostoja tai koko laitteen vaatien lunnaita näiden lukkojen avaamiseksi.

Palveluestohyökkäyksessä verkkoa kuormitetaan ylimääräisellä tietoliikenteellä. Tavoitteena on lamaannuttaa jokin palvelu- tai tietojärjestelmä.

KYBERTURVALLISUUSKYVYKKYYS ON KILPAILUETU

Digitalisaatio avaa mahdollisuuksia, joiden avulla yritykset voivat tehostaa toimintaansa ja säästää kustannuksissa. Samaan aikaan on huolehdittava tietoturvallisuudesta. Tietoturvallisuus on kriittinen menestystekijä kasvulle, kehittämiselle ja uusien liiketoimintamallien toteuttamiselle.

Hyvin järjestetty, laatujärjestelmään kiinnitetty kyberturvallisuuskyvykkyys on selkeä kilpailuetu, sillä liikekumppanit ja asiakkaat arvostavat ja edellyttävät tietojensa pysymistä turvassa. Samaa kyvykkyys tulee varmistaa myös alihankkijoiden ja toimittajien osalta.

Kyberturvallisuus vaikuttaa yleisemmin myös yrityksen operatiivisiin, juridisiin ja taloudellisiin riskeihin. Yrityksen on yhä useammin osoitettava turvallisuusasioidensa ja -kulttuurinsa asianmukainen hallinta myös viranomaisille.

TIETOTURVALLISUUS ON YKSI LIIKETOIMINNAN TAVOITTEISTA

Tietoturvallisuuden kehittäminen lähtee liikkeelle riskien arvioinnista: mitä salassa pidettävää tietoa yrityksellä on ja missä. Samoin on keskeistä valita turvallisuuden hallintakeinot, asettaa tavoitteet ja kirjata toimenpiteet.

Toimiva tietoturva tarvitsee johtamista, jossa keskitytään luottamuksen ylläpitämiseen ja vahvistamiseen. Yrityksen on hyvä kytkeä turvallisuus osaksi strategiaa ja liiketoiminnan tavoitteita. Turvallisuus nähdään liian kapeasti, jos asia siirretään erilliseen turvallisuustoimintoon ja siellä keskitytään vain uhkien ehkäisemiseen ja säännösten noudattamiseen.

Inhimilliset virheet ovat suuri osa kyberhyökkäyksiä, ja henkilöstö on usein tahattomasti kyberturvan heikoin lenkki. Selkeät ja yhdessä määritellyt tietoturvaohjeet selkeyttävät jokaisen toimintaa. Tahalliset hyökkäykset voidaan välttää, jos tietoa käsitellään turvallisemmin.

Tietoturvapolitiikka linjaa tietoturvanhallintaan liittyvät tavoitteet, organisoinnin ja vastuut. Vastuu tietoturvasta ei ole pelkästään IT-osaston asia, vaan jokaisella on oma roolinsa noudattaa yrityksen tietoturvapolitiikkaa.

Joitakin käytännön toimenpiteinä tietoturvallisuuden edistämiseksi:

- Selvitä ensin, mitkä tietoteknisen ympäristön osat ovat kriittisiä liiketoimintatavoitteiden saavuttamiseksi.
- Tee tilannekuvatietoon perustuva kartoitus yritykseen kohdistuvista uhista tarpeellisten kyberturvallisuustoimenpiteiden ja -investointien toteuttamiseksi.
- Varaudu uhkia vastaan luomalla myönteinen, tietoturvallisuuteen sitouttava turvallisuuskulttuuri. Organisaation toimintatavat ja asenne eivät saa johtaa oikoteiden tai epävirallisten työtapojen etsimiseen.
- Huolehdi turvallisuuskulttuurin ylläpitämiseksi riittävästä osaamisesta, ohjeistuksesta ja sen jalkauttamisesta sekä kommunikaatiosta. Jatkuva valvonta, arviointi ja kehittäminen ovat luonnollisesti myös avaintekijöitä.
- Arvioi tarve kansainvälisen tietoturvastandardin ISO 27001 mukaisen, sertifioidun tietoturvallisuuden hallintajärjestelmän toteuttamiselle. Laadukas johtamisjärjestelmä on usein edellytys yrityksen hyväksymiselle osaksi toimittajaverkostoa.
- Pidä tietoturvallisuus keskiössä tehtäessä yhteistyötä palveluntarjoajien ja kumppaneiden kanssa.

TIETOTURVAN KOMPASTUSKIVIÄ

- Olettamus, ettei joudu hyökkäyksen kohteeksi
- Lähestyä kyberturvaa vain tietotekniikan parantamisella ja luottamalla pelkästään virustorjuntajärjestelmiin
- Puutteet tiedon käytettävyydessä ja eheydessä
- Päätelaitetyöskentelyn huolimattomuus
- Henkilöstön kouluttamisen laiminlyönti
- Ohjelmistopäivitysten huomiotta jättäminen
- Varmuuskopioinnin toimivuus ja palautusprosessi testaamatta
- Puutteellinen toimintasuunnitelma kyberhyökkäystä vastaan Laadukas johtamisjärjestelmä on usein edellytys yrityksen hyväksymiselle osaksi toimittajaverkostoa.
- Pidä tietoturvallisuus keskiössä tehtäessä yhteistyötä palveluntarjoajien ja kumppaneiden kanssa.