Teknologiateollisuus

Toimintamalleja yritysturvallisuuden ja riskienhallinnan edistämiseen - kyberturvallisuus

DIGITAALINEN TURVALLISUUS ON YHÄ TÄRKEÄMPÄÄ

Yritysturvallisuus on yrityksen kaikkien toimintojen turvallisuutta. Digitaalinen turvallisuus on yhä keskeisempi osa turvallisuuden kokonaisuutta.

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

Kyberturvallisuus käsittää tietoturvallisuuden sekä jatkuvuuden hallinnan ja varautumisen. Tietoturvassa on järjestelmien, ohjelmistojen, laitteiden ja verkkojen suojaamisen lisäksi kyse myös liiketoimintaprosesseista sekä ihmisten käyttäytymisestä ja asenteesta.

Hyvin rakennettu kyberturvallisuus suojaa yrityksen toimintakykyä.

KYBERUHAT OVAT MONINAISIA

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

Tyypilliset haavoittuvuudet:

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 datan turvallisuudesta. Datan turvallisuus 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.

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

TURVALLISUUS ON YKSI LIIKETOIMINNAN TAVOITTEISTA

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

Toimiva kyberturva tarvitsee johtamista, jossa keskitytään luottamuksen ylläpitämiseen ja vahvistamiseen. Yrityksen tulisi pyrkiä siihen, että sen strategiassa turvallisuus olisi kytketty osaksi liiketoiminnan tavoitteita. Turvallisuus nähdään liian kapeasti, jos asia siirretään erilliseen turvallisuustoimintoon ja siellä keskitytään vain uhkien ehkäisemiseen ja säännösten noudattamiseen.

Inhimilliset virheet ovat isossa osassa 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.

Käytännön toimenpiteinä kyberturvallisuuden edistämiseksi yrityksen tulee mm.

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

TIETOTURVAN KOMPASTUSKIVIÄ

- Olettamus, ettei voi olla hyökkäyksen kohteena
- Lähestyä kyberturvaa vain tietotekniikan parantamisella ja luottamalla pelkästään virustorjuntajärjestelmiin
- Päätelaitetyöskentelyn huolimattomuus
- Henkilöstön kouluttamisen laiminlyönti
- Ohjelmistopäivitysten huomiotta jättäminen
- Varmuuskopioinnin toimivuus ja palautusprosessi testaamatta
- Puutteellinen toimintasuunnitelma kyberhyökkäystä vastaan