SUOSITUKSIA IT- JA TIETOTURVAPALVELUIDEN PALVELUNTARJOAJILLE

ARVIOI UHKIA JA YMMÄRRÄ RISKIT

- Tiedosta, mitä tietoja asiakas haluaa palveluun tallentaa, miten tieto on asiakasyrityksessä luokiteltu ja mikä sen merkitys on asiakkaan toiminnan kannalta.
- Tunnista tietojen käsittelyyn ja tallennukseen liittyvä lainsäädäntö ja vaatimukset, esim. henkilötietojen osalta tietosuojalaki ja -asetus.
- Varmista, että asiakasyrityksen tietojen eheys sekä saatavuus pystytään turvaamaan ja että asiakkaan vaatima taso on selkeästi määritelty.
- Sovi asiakasyrityksen kanssa lokien pääsyn hallinnasta ja lokien käytön toimenpiteistä.
- Varmista, että yhteys lokeihin on toteutettu niin, että lokituskäytännöt ovat lainsäädännön mukaiset ja että lokituksen osalta on määritetty, mitä lokitetaan ja kuinka kauan.

- Varmista, että oikeudet järjestelmiin on annettu käyttäjän roolin ja tarpeen mukaisesti, tarvittaessa myös muulle palveluntarjoajalle tai viranomaiselle. Huomioi lokitietojen hyödyntämisessä niiden siirrettävyys sekä luottamuksellisuus.
- Varmista, että lokien hallintaan liittyvät tarpeet, esimerkiksi datan luovuttamisen määräajat viranomaispyyntöjen vuoksi, on katettu sopimuksessa. Huomioi myös tarjottava palveluympäristö.
- Varmista, että asiakkaan varautumisessa on huomioitu mahdolliset auditointivaatimukset, esim. ennakkoilmoitukset, auditointikriteeristö ja kustannusjako.

SUOJAA ORGANISAATIOSI TOIMINTA JA TURVAA JATKUVUUS

- Huolehdi siitä, että yrityksesi henkilöstöllä on selkeät toimintaohjeet asiakasyritykseen kohdistuvan häiriö- tai poikkeustilanteen varalle.
- Huomioi tietoturvaohjeissa ja käyttäjille annetuissa ohjeissa se, käytetäänkö eri laitteita sisäisissä verkoissa vai ulkoisissa, julkisissa verkoissa. Huomioi myös mobiililaitteet.
- Harjoittele toimintatavat häiriötilanteiden varalle ja huomioi harjoittelu sekä harjoittelukustannukset sopimuksessa.

REAGOI NOPEASTI JA TOIMI SUUNNITELMALLISESTI

- Selvitä etukäteen, mitä tietoja asiakasyrityksesi häiriö- tai loukkaustapauksessa voidaan käsitellä, kenen toimesta ja millä perusteella.
- Varmista, että asiakasyritykseen tai omiin järjestelmiin kohdistettu tietoturvaloukkaus tai sen uhka on mahdollista havaita.
- Varmista, että saastunut tunnus, laite ja/tai järjestelmä pystytään yksilöimään ja että kyberloukkaukseen pystytään reagoimaan mahdollisimman nopeasti.
- Määrittele prosessit asiakkaille, sidosryhmille sekä eri viranomaisille tehtäviä ilmoituksia varten. Esim. henkilötietoihin kohdistuvasta tietosuojaloukkauksesta tulee tehdä ilmoitus rekisteröidylle viipymättä ja tietosuojavaltuutetun toimistolle 72 tunnin kuluessa.

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI