

SUOSITUKSIA KYBERTURVALLISUUDESTAAN HUOLEHTIVILLE YRITYKSILLE

ARVIOI UHKIA JA YMMÄRRÄ RISKIT

- Ymmärrä, mitä olet palveluntarjoajalta hankkimassa.
- Varmistu siitä, että palvelun toimittaja pystyy käytännössä toimimaan siltä edellytetyllä tavalla.
- Varmista, että yrityksen sopimuskäytännöissä huomioidaan lainsäädännön vaatimukset.
- Ota sopimuksissa huomioon, millaisia standardeja organisaatiossasi tulee noudattaa.
- Tiedosta, mitä tietoja palveluun ollaan tallentamassa, miten tieto on luokiteltu ja mikä sen merkitys on yrityksesi toiminnan kannalta.
- Tunnista tietojen käsittelyyn ja tallennukseen liittyvät vaatimukset ja lainsäädäntö.
- Varmista, että palveluntarjoaja pystyy turvaamaan tietojen eheyden ja saatavuuden.

- Sovi lokien pääsyn hallinnasta ja lokien käytön toimenpiteistä.
- Varmista, että yhteys lokeihin on toteutettu niin, että käytännöt ovat lainsäädännön mukaiset.
- Varmista, että oikeudet järjestelmiin on annettu työntekijän roolin ja tarpeen mukaisesti, tarvittaessa myös ulkopuoliselle palveluntarjoajalle tai viranomaiselle.
- Varmista, että lokien hallintaan liittyvät tarpeet, esimerkiksi datan luovuttamisen määräajat viranomaispyyntöjen vuoksi, on katettu sopimuksessa.
- Huomioi hankintaprosessissa myös edellä mainittujen seikkojen varmistus ja esimerkiksi integraatioiden rakentaminen palveluntarjoajan lokitietoihin.
- Huomioi sopimuksessa mahdolliset auditointivaatimukset, kuten ennakoilmoitukset, auditointikriteeristö sekä kustannusjako.

SUOJAA ORGANISAATIOSI TOIMINTA JA TURVAA JATKUVUUS

- Viestitä henkilöstöllesi, miten häiriö- tai poikkeamatilanteessa tulee toimia. Sen voi tehdä esimerkiksi tietoverkon käytöstä annetulla erillisellä ohjeella tai YT-menettelyssä.
- Huomioi tietoturvaohjeistuksessa ja käyttäjille annetuissa ohjeissa myös mobiililaitteet sekä se, käytetäänkö eri laitteita yrityksen sisäisissä vai ulkoisissa, julkisissa verkoissa.
- Harjoittele toimintatavat häiriötilanteiden varalle ja huomioi harjoittelu sekä harjoittelukustannukset palveluntarjoajan kanssa tehtävässä sopimuksessa.
- Seuraa palvelun tietoturvaa esimerkiksi pitämällä säännöllisiä palvelunseurantakokouksia.

REAGOI NOPEASTI JA TOIMI SUUNNITELMALLISESTI

- Selvitä etukäteen, mitä tietoja yritykseen kohdistuvassa häiriö- tai loukkaustilanteessa voidaan käsitellä, kenen toimesta ja millä perusteella.
- Varmista, että yrityksessäsi on kyky havaita siihen kohdistettu tietoturvaloukkaus tai sen uhka.
- Varmista, että saastunut tunnus, laite tai järjestelmä pystytään yksilöimään ja että kyberloukkaukseen pystytään reagoimaan mahdollisimman nopeasti.
- Määrittele prosessit asiakkaille, sidosryhmille, palveluntarjoajille sekä eri viranomaisille tehtäviä ilmoituksia varten.

