Digi Turku – Tietoturvakäytännöt ja NIS2-valmius

Tila: Voimassa oleva

Tämä dokumentti kuvaa Digi Turun (digiturku.fi) tietoturvakäytänteet, infrastruktuurin turvallisuuden sekä datan hallinnan periaatteet. Toimintamme on suunniteltu vastaamaan modernin kyberturvallisuuden vaatimuksia, ja tuemme täten osaltamme asiakkaidemme NIS2-direktiivin ja GDPR-tietosuoja-asetuksen mukaisia toimitusketjun turvallisuusvaatimuksia.

1. Palvelininfrastruktuuri ja Hosting-palvelut

Tarjoamme asiakkaillemme luotettavaa ja turvallista palvelintilaa EU:n sisällä kahdella eri toimintamallilla, jotka jakavat kyberturvallisuusvastuut selkeästi:

- **Oma jälleenmyyntiympäristö (Jaettu vastuu):** Digi Turku hallinnoi itsenäisesti jälleenmyyntipalvelinta, jonka fyysisestä konesaliturvallisuudesta, verkkotason suojauksesta (mm. DDoS-estot) ja laitteistopäivityksistä vastaa ruotsalainen Miss Hosting AB. Digi Turku vastaa oman hallintaympäristönsä (cPanel/WHM) loogisesta turvallisuudesta, asiakastilien eristämisestä toisistaan, pääsynhallinnasta (MFA) ja resurssien valvonnasta.
- **Välitetyt palvelut (Suora asiakkuus):** Toimiessamme välittäjänä (affiliate) kumppaneillemme (esim. team.blue / Hostingpalvelu.fi tai Miss Hosting), asiakkaan palvelininfrastruktuuri ja sen NIS2-yhteensopivuus ovat suoraan kyseisen palveluntarjoajan vastuulla. Digi Turku toimii näissä asiantuntijana ja suosittelijana.

2. Verkkosivutuotanto ja Ylläpito

Verkkosivujen tietoturva riippuu valitusta palvelumallista:

- **Projektiluovutus:** Kun sivusto rakennetaan ja luovutetaan asiakkaalle ilman jatkuvaa ylläpitosopimusta, Digi Turku takaa, että ohjelmistot ja lisäosat ovat luovutushetkellä ajan tasalla ja perussuojaukset (esim. palomuuri, vahvat salasanat) on asennettu. Luovutuksen jälkeen vastuu päivityksistä siirtyy asiakkaalle.
- **Jatkuva ylläpito:** Kun asiakas valitsee Digi Turun ylläpitopalvelun, vastaamme sivuston kriittisten päivitysten (ydin, teemat, lisäosat) säännöllisestä asentamisesta, haavoittuvuuksien seurannasta sekä säännöllisestä varmuuskopioinnista.

3. Sisäinen tietoturva ja Datan hallinta

Digi Turku käsittelee asiakastietoja, tunnuksia ja lähdeaineistoja ehdottoman luottamuksellisesti.

- **Työkalut ja Pilvipalvelut:** Operatiivinen tiedonhallinta, asiakirjat ja taulukot on keskitetty Microsoft 365 / OneDrive -ympäristöön. Tiedostojen jakamiseen asiakkaiden ja sidosryhmien kanssa hyödynnetään suojattua Google Drivea. Molemmissa ympäristöissä on käytössä pakotettu monivaiheinen tunnistautuminen (MFA) ja käyttöoikeudet on rajattu tiukasti.

- **Päätelaitteiden turvallisuus:** Kaikki työlaitteet on suojattu levynsalauksella, automaattisella ruudunlukituksella sekä ajantasaisella virustorjunnalla ja käyttöjärjestelmäpäivityksillä.

4. Tekoälyn turvallinen käyttö

- **Sisäinen käyttö:** Tuotannon ja kehityksen tukena käytettävään tekoälyyn (Google AI Pro) ei syötetä asiakkaiden henkilötietoja, tietokantadumppeja, salasanatietoja tai liiketoimintasopimuksia, jotta arkaluonteinen tieto ei päädy kielimallien opetusdataan.
- **Asiakasratkaisut:** Asiakkaiden verkkosivuille rakennettavat AI Engine Chatbotit konfiguroidaan siten, että ne keräävät vain toiminnan kannalta välttämättömän tiedon ja ne suojataan yleisimpiä manipulointiyrityksiä (prompt injection) vastaan.

5. Poikkeamien hallinta ja Lokitus (Incident Response)

- Seuraamme palvelinympäristömme kirjautumis- ja virhelokeja luvattoman toiminnan havaitsemiseksi.
- Mahdollisen tietoturvaloukkauksen tai tietovuodon sattuessa Digi Turku eristää vaarantuneen ympäristön välittömästi. Raportoimme tapahtuneesta ensitilassa kosketetuille asiakkaille, jotta NIS2-direktiivin ja GDPR:n alaiset asiakkaamme voivat täyttää omat lakisääteiset ilmoitusvelvollisuutensa määräajassa.