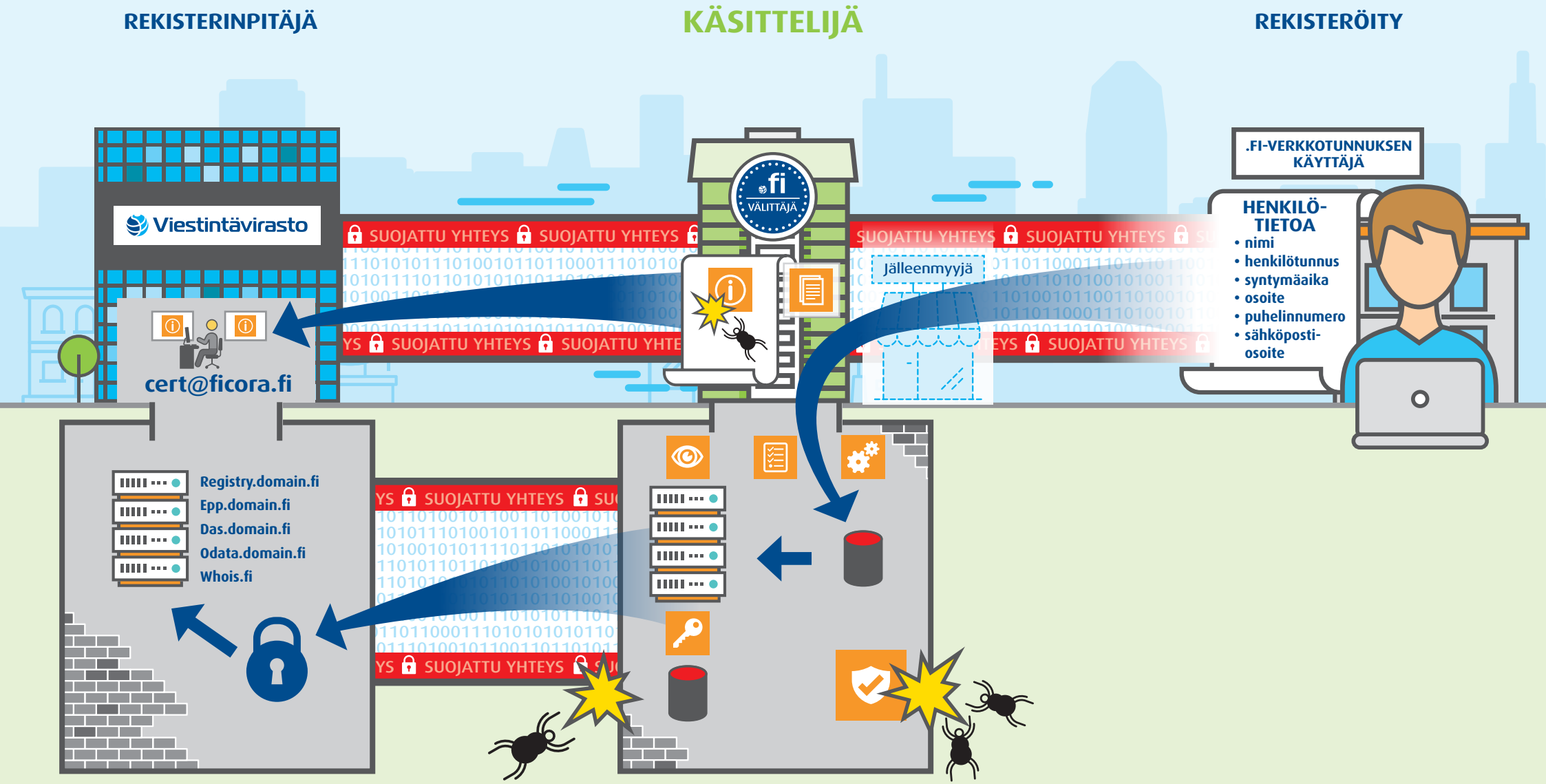
Tietoturvavelvoitteet .FI-verkkotunnusten välittäjille



Miksi tietoturvaa?

- *Varmistutaan siitä, että merkittävät tietoturva-loukkaukset havaitaan ja hoidetaan ajoissa, mieluummin toki ennen asiakkaiden valituksia.*
- *Asiakkaat haluavat valita luotettavan välittäjän, joka pitää hyvää huolta heidän liiketoiminnastaan ja henkilötiedoistaan.*
- *Luvaton pääsy verkkotunnusrekisteriin käyttäen välittäjältä varastettuja tunnuksia vahingoittaa sekä välittäjän että verkkotunnusjärjestelmän toimintaa.*
- *Tietoturvahäiriöiden välttäminen johtaa parempaan toimintavarmuuteen, ja auttaa välttämään myös häiriöiden aiheuttamia odottamattomia kuluja.*

Tietoliikenne- ja tietojärjestelmäturvallisuus

- Suomen laki ja Viestintäviraston määräys edellyttävät, että verkkotunnusvälittäjä huolehtii järjestelmänsä tietoturvasta Viestintäviraston ohjeistamalla tavalla.
- Jos välittäjä käyttää EPP-rajapintaa, järjestelmän on myös toteutettava KATAKRI:n (tason IV) tietoliikenne- ja tietojärjestelmävaatimusosuudet. (Ajantasainen versio KATAKRI 2015, sivut 30-52) http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille.
- Jos välittäjä käyttää selainkäyttöliittymää, tietoturvavelvoitteet ovat vastaavat, mutta KATAKRI:n noudattaminen ei ole pakollista. Suosittelemme silti kaikille välittäjille KATAKRI:in perehtymistä.

Turvallisuusdokumentit

1. Riskienhallinnan prosessit ja tulokset

- Riskien määrittäminen ja toimenpiteet niiden huomioimiseksi on osa normaalia liiketoimintaa erityisesti silloin kun turvalliset ja luotettavat yhteydet ovat välittäjien liiketoiminnan ytimessä. Välittäjä: ovathan riskienhallinnan dokumenttinne ajan tasalla? Valmistautukaa perustelemaan valitsemanne toimenpiteet.

2. Luokittelukriteerit ja arkaluonteisten aineistojen käsittely

- Henkilötiedot ovat arkaluonteista aineistoa. Kuinka säilytätte ja suojelette sitä?
- Pääsytunnukset EPP-rajapintaan tai selainkäyttöliittymään on suojattava huolella.

3. Valvontamekanismit

- Olkaa tietoisia siitä mitä tapahtuu omassa järjestelmässänne, jotta pystytte reagoimaan ajallaan. Ovatko tunkeutumisesto- ja havainnointijärjestelmänne ajan tasalla?

4. Tietoturvaloukkausten käsittely

- Kuinka tietoturvaloukkaukset havaitaan?
- Kuinka tietoturvaloukkauksista toivutaan?
- Tietoturvaloukkauksista ilmoitetaan vapaamuotoisella sähköpostilla osoitteeseen cert@ficora.fi tai Viestintäviraston asiointilomakkeella. Ilmoittamisprosessien tulee olla ohjeistettu henkilökunnalle.

Ilmoitus tietoturvaloukkauksesta

- Arvioitu kesto
- Vaikutukset
- Korjaustoimenpiteet
- Tilanteen toistumisen ennaltaehkäisevät toimenpiteet

5. Muutostenhallinnan prosessit

- Muutostöiden tulee olla suunniteltuja ja huoltoikkunoiden tarpeeksi pitkiä.

Muistettavaa

- Suomen lain edellyttämä välitystoiminnan tietoturva -ohjeistus ”Välitystoiminnan tietoturva” on osoitteessa https://www.viestintavirasto.fi/fiverkkotunnus.html.
- Uuden tietosuojalain vuoksi saatatte joutua muuttamaan toimintatapojanne, hankkimaan uusia ohjelmistoja tai laitteita.
- Viestintävirasto tulee kysymään teiltä yksityiskohtaisempia kysymyksiä valitsemistanne tietoturvatoimenpiteistä, joten pitäkää dokumenttinne ajan tasalla.
- Haluamme olla avuksi! Lähetämme teille sähköpostia tulevista muutoksista. Lisäohjeita ja oppaita on tulossa tietoturvavaatimuksista.

fi-domain-tech@ficora.fi p. 0295 390 100 www.viestintavirasto.fi