Finnish

FI | EN

Funet CERT

Funet CERT (Finnish University and Research Network, Computer Emergency Response Team) koordinoi tietoturvapoikkeamia sekä tukee ja palvelee tietoturvariskien pienentämisessä.

Palvelemme ensisijaisesti Funetin jäsenorganisaatioita.

Funet CERT välittää tietoturvapoikkeamatilanteessa tietoa osapuolten välillä ja tarjoaa tarvittaessa tukea.

Pyrimme myös auttamaan tietoturvahaavoittuvuuksiin ja IT-palveluihin kohdistuviin hyökkäyksiin varautumisessa. Toimimme aktiivisesti tietoturvayhteistyön edistämiseksi Funetin jäsenorganisaatioiden kesken sekä välitämme tietoa yhteistyökumppaneiltamme.

Lisäksi tarjoamme Funetin jäsenorganisaatioiden nimetyille tietoturvavastaaville mahdollisuuden tutkia oman verkkonsa haavoittuvuuksia. Kyseinen palvelu on kuvattu info.funet.fi:ssä.
Funet CERT päivystää toimistoaikana. Meihin voi ottaa yhteyttä soittamalla tai sähköpostitse. Luottamuksellisen aineiston salaaminen on mahdollista PGP-avaimellamme.

Käsittelemme saamaamme tietoa luottamuksellisesti ja kunnioitamme käyttäjän oikeutta tietosuojaan. Välitämme tietoja eteenpäin ainoastaan asianomaisen pyynnöstä ja luvalla, ellei laki toisin määrää. Tietoturvapoikkeaman määritelmä on ohjeen VAHTI 3/2005 mukaan: "tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut."

Funet CERT käsittelee tietoturvapoikkeamia ilmoitusten ja oman verkonvalvonnan perusteella. Saamme ilmoituksia useasta muustakin lähteestä, esim. Kansalliselta tietoturvaviranomaiselta (NCSC-FI), luotetuilta yhteistyökumppaneilta, hyökkäyksen kohteelta jne. Myös jäsenorganisaatioiden tietoturvavastaavat raportoivat poikkeamista, jotka voivat vaikuttaa muiden tietoturvallisuuteen.

Ilmoituksen voi tehdä sähköpostitse, puhelimitse, kirjeitse tai faksilla. Ilmoituksessa on hyvä kertoa paitsi mitä on tapahtunut, myös lähde- ja kohdeosoite, mahdollisesti porttinumerot ja käytetty protokolla sekä päivämäärä ja aika (myös aikavyöhyke). Usein asian selvittelyä helpottaa, jos mukaan voi liittää pätkän lokitietoa.

Kun ilmoitus tehdään sähköpostitse pyytäen vastausta, ilmoitamme heti, kun olemme aloittaneet tapauksen käsittelyn. Ensimmäisen vastauksen otsikkorivillä on käsittelynumero. Mahdollisiin lisätietoihin tai -kysymyksiin kannattaa otsikkoriville liittää mukaan tuo tunnus, koska silloin osaamme kytkeä viestin oikeaan asiaan ja tapahtumaan.

Käsittelemme palvelupyyntöjä tapauskohtaisesti. Joskus riittää pelkkä ilmoitus asian osapuolille, mutta toisinaan asia vaatii laajempaa käsittelyä ja pidemmän ajan. Kun asia on selvitetty ja tapaus käsitelty, se arkistoidaan ja tilastoidaan.
Tietoturvapoikkeamien havaitseminen ja hoitaminen perustuu luotettujen verkostoihin. Tämän vuoksi Funet CERT panostaa vahvasti sekä kotimaiseen että kansainväliseen yhteistyöhön.

Teknisen tietoturvan osalta seuraamme tietoturvan välineistön ja menetelmien kehittymistä sekä Suomessa että maailmalla. Tällaisia ovat esimerkiksi tietoliikenteen analysointiin tai tietoturvapoikkeamien tutkimiseen liittyvät menetelmät.

Hallinnollisen tietoturvan osalta olemme aktiivisesti mukana tietoturvasääntöjen ja ohjeiden valmistelussa. Voimme tarvittaessa antaa lausuntoja tietoturvaan liittyvistä laeista ja asetuksista. Pidämme säännöllisesti yhteyttä Funetin jäsenorganisaatioiden tietoturvavastaaviin sekä muihin tietoturva-alan toimijoihin niin Suomessa kuin kansainvälisesti.