Ilmoita tietoturvapoikkeamasta

Ilmoita tietoturvapoikkeamasta

Ilmoituksessa on hyvä kertoa lyhyesti, mitä on tapahtunut ja miten tapahtuma on käynyt ilmi. Jos mahdollista, ilmoitukseen kannattaa liittää mukaan lokitietoja, joista käy ilmi esimerkiksi lähde- ja kohdeosoite, porttinumerot ja tapahtuma-aika.

On hyvin tärkeää ilmoittaa ajankohta, jolloin poikkeama on tapahtunut. Aikaa ilmoittaessa kannattaa kertoa myös aikavyöhyke, esimerkiksi Suomen aikaa tai UTC (Coordinated Universal Time).

Kun kerätään tietoja ilmoitusta varten, pitää varoa, ettei todistusaineistoa tuhota esimerkiksi muuttamalla tiedostojen aikaleimoja. Jos kyseessä on murrettu tietokone, tietojen kerääminen pitäisi tehdä alkuperäisen kiintolevyn sijasta siitä otetusta levykuvasta (disk image) ja jättää alkuperäinen kiintolevy todistusaineistoksi.

Kun ilmoitus sisältää luottamuksellisia tietoja, kuten henkilötietoja tai järjestelmän konfigurointiin tai turvallisuuteen liittyviä tietoja, suosittelemme, että sähköpostiviestinnässä käytetään salausta.

Kun ilmoitus on tehty sähköpostitse, vastaamme mahdollisimman pian tilanteen edellyttämällä tavalla. Jos vastaamme sähköpostitse, viestin otsikkorivillä on tapahtuman tunniste, jota käyttämällä mahdolliset lisätiedot liitetään automaattisesti edellisiin kyseistä tapahtumaa koskeviin viesteihin.

Funet CERT käyttää tietoturvapoikkeamiin liittyvien palvelupyyntöjen käsittelyyn erityisesti tähän tarkoitukseen suunniteltua ohjelmistoa nimeltä RTIR.

Ilmoitus voi näyttää esimerkiksi tältä:

```
Hei,

Ylläpitämällemme WWW-palvelimelle www.esimerkki.fi (192.0.43.10)
tulee toistuvasti murtoyrityksiä osoitteesta 10.10.10.10.

Yritykset näyttävät tältä (aikaleimat UTC):

Jan 15 10:04:02 example sshd[14523]: Illegal user example from
::ffff:10.10.10.10

Murtoyritysten lukumäärä osoitteesta  10.10.10.10  on melko korkea:

www:/var/log# grep 10.10.10.10 auth.log |wc
2359 23592 187184

-> 2359 yritystä!

Voitteko auttaa lopettamaan nämä murtoyritykset.

Yrjö Ylläpitäjä
```

Muista, että muoto ei ratkaise. Kun teet ilmoituksen Funet CERT:lle, muoto on vapaa.

Sähköpostiviestien salaus

Kun ilmoitukseen liitetään luottamuksellisia tietoja tai henkilötietoja, on poikkeaman käsittelyyn liittyvät sähköpostit hyvä salata. Luottamukselliseen viestintään Funet CERT käyttää PGP-salausta. PGP-salauksen avulla pystyy lähettämään ja vastaanottamaan vahvasti salattuja viestejä julkisen verkon yli niin, että vain lähettäjä ja vastaanottaja voivat lukea viestejä.

PGP perustuu avoimiin ja julkisiin algoritmeihin. Siitä on saatavissa sekä kaupallinen (PGP) että ilmainen ja avoin versio (GnuPG). PGP-salaus perustuu sähköpostiosoitteeseen liitettyyn avainpariin, johon kuuluu julkinen ja salainen avain.

Ohjelmistoa käyttöön otettaessa luodaan sekä julkinen että salainen avain. Salainen avain suojataan salauslauseella ja tallennetaan turvalliseen paikkaan. Julkisen avaimen voi jakaa Funet CERT:n kanssa esimerkiksi www-sivulla tai sähköpostitse. Joka tapauksessa julkinen avain kannattaa julkaista jossakin PGP-avainpalvelussa. Funet CERT:n julkinen avain on saatavissa myös www-sivuiltamme.

Kun haluat lähettää salatun viestin Funet CERT:lle, salaa se julkisella avaimellamme. Sen jälkeen vain me pystymme lukemaan viestin. Kun vastaamme, salaamme viestin sinun julkisella avaimellasi, mikäli meillä on se tiedossamme.

Rikosilmoitukset sekä väärinkäyttötapaukset

Vakavista tapauksista, kuten tietoliikenteen häirintä tai tietomurto, on syytä ilmoittaa myös poliisille. Kyseessä on pääsääntöisesti asianomistajarikos, jolloin ilmoittajan tulee itse tehdä asiasta ilmoitus poliisille. Ilmoituksen voi tehdä paikalliselle poliisille, mutta laajemmissa ja vakavammissa tapauksissa voi ottaa suoraan yhteyttä myös keskusrikospoliisiin.

Mikäli poikkeamassa on kyse yksittäisen käyttäjän lievemmästä rikkeestä, esimerkiksi häiritsevästä tai sääntöjen vastaisesta toiminnasta, voi ottaa myös suoraan yhteyttä väärinkäyttöä valvoviin tahoihin. Yhteysosoite on usein muotoa abuse@organisaatio. Abuse-mailboxia ja muitakin yhteystietoja voi etsiä whois-palvelusta, esim. eurooppalaisen RIPE:n www-palvelun kautta.

Miten Funet CERT käsittelee ilmoituksia?

Saat kuittauksen kun ilmoituksesi on vastaanotettu ja sen käsittely on aloitettu. Tämän jälkeen Funet CERT ottaa tarvittaessa yhteyttä poikkeaman muihin osapuoliin. Jos osapuolia on useita, kukin saa vain itseään koskevia tietoja.

Kun poikkeamasta on ilmoitettu eteenpäin tai sitä on käsitelty muulla tavoin, kuittaamme ilmoituksen hoidetuksi lähettäjälle.

Mikäli toinen osapuoli vastaa tai muuten raportoi tilanteesta, tämä tieto välitetään myös takaisin ilmoituksen tekijälle.

Funet CERT koordinoi

Kun poikkeama koskee useita tahoja, Funet CERT voi koordinoida tiedonkulkua. Mikäli poikkeama koskee vain yhtä tai kahta Funetin jäsenorganisaatioita, osapuolet voivat hoitaa tiedonvälityksen itsekin, mutta myös meitä voi käyttää koordinaattorina. Joka tapauksessa otamme aina mielellämme vastaan tietoa tapahtuneesta.

Miksi poikkeamista tulee ilmoittaa Funet CERT:lle?

Tietoturvapoikkeamista on hyvä ilmoittaa Funet CERT:lle, esimerkiksi koska:

- Hyökkäyksiin kannattaa reagoida yhteisesti, kun niitä halutaan torjua
- Organisaation tietoturvaohjeet edellyttävät ilmoituksen tekemistä
- Ilmoituksen avulla voidaan torjua hyökkäys tai muu haitta
- Tarvitaan lisätietoja tai teknisiä ohjeita
- Kokonaiskuvan saaminen poikkeamista edellyttää yhteistyötä
- Poikkeama saattaa olla osa laajempaa kokonaisuutta
- Ilmoituksen avulla voidaan parantaa tietoisuutta tietoturva-asioista