

TIETOTURVAPOIKKEAMIIN REAGOIMINEN

Sisällysluettelo:

1	Johdanto.....	1
1.1	Tietoturvapoikkeamien reagointisuunnitelman tarkoitus ja soveltamisala.....	1
1.2	Tietoturvapoikkeamien käsittely.....	2
2	Organisaatio.....	2
3	Reagoiminen tietoturvapoikkeamiin.....	3
3.1	Tietoturvapoikkeamien vakavuuden arviointi ja reagointiryhmän laajentaminen.....	3
3.2	Vastatoimien laajentamisessa huomioitava.....	5
3.3	Toimintavastuu.....	5
3.4	Viranomaisilmoitukset.....	6
3.5	Poikkeaman jälkeinen toiminta.....	6
3.6	Poikkeamista tiedottaminen.....	6
4	Ohjeen päivittäminen.....	6
5	Liitteet.....	7

Suunnittele – Kouluta – Harjoittele

1 Johdanto

1.1 Tietoturvapoikkeamien reagointisuunnitelman tarkoitus ja soveltamisala

Reagointisuunnitelman tavoitteena on, että tietoturvapoikkeamiin reagoiminen on ennakolta suunniteltua, harjoiteltua, poikkeaman vaikutukset minimoivaa ja niistä tehokkaasti palautuvaa. Tämä tapahtuu varmistamalla, että tietoturvapoikkeamat tunnistetaan yliopistossa nopeasti, niihin reagoiminen aloitetaan viipymättä ja se tehdään ennalta sovitun menettelytavan (tämä ohje) mukaisesti.

Tietoturvapoikkeama on tahallinen tai tahaton tapahtuma tai olotila, jonka seurauksena yliopiston vastuulla olevien tietojen ja palvelujen käytettävyydellä ei ole suunnitellulla tasolla tai tietojen eheys² tai luottamuksellisuus³ on vaarantunut.

¹ Käytettävyyttä uhkaavia tilanteita: sähkö-, LVI-, laite- ym. häiriöistä aiheutuva palvelutason lasku sovitusta tasosta kaikille käyttäjille tai palvelutasoa vaarantavat palvelunestohyökkäykset ja muut haittaohjelmistojen toiminnot.

² Eheyttä uhkaavia tilanteita: laitteistojen ja/tai ohjelmistojen virheellinen toiminta, haittaohjelmien toiminnan vaikutuksesta uhkaava tietojen muuttuminen tai tuhoutuminen.

³ Luottamuksellisuutta uhkaavia tilanteita: ohjelmien ja laitteiden virhetoiminnot, ihmisten tarkoituksellinen tai vahingossa tapahtuva luvaton toiminta (hakkerointi), erilaisten haittaohjelmien toiminta ja niiden käyttäminen (esimerkiksi virus, joka lähettää koneeseen talletettuja tiedostoja tai niiden osia).

Reagointisuunnitelmaa on noudatettava kaikkien tietojärjestelmien, myös yksittäisten työasemien hallinnoinnissa.

Jokaisen yksikön tulee laatia palvelinjärjestelmäkohtaiset reagointisuunnitelmat (malli liitteessä 1), vahvistaa ne ja toimittaa tietoturvapäällikölle tiedoksi. Tämä koskee yksiköitä, joilla on omia itsenäisiä palvelinjärjestelmiä.

Jokaisen yksikön tulee myös ylläpitää luetteloa yksikkönsä työasemien ja niissä mahdollisesti käytettävien erityisohjelmistojen pääkäyttäjistä, ylläpitäjistä ja tukihenkilöistä. Nämä henkilöt toimivat työasemien tietoturvapoikkeamia seuraavina henkilöinä yksikkötasolla ja avustavat käyttäjiä työasemien seurannassa.

1.2 Tietoturvapoikkeamien käsittely

Tietoturvapoikkeamien käsittely jaetaan kolmeen vaiheeseen:

1. havainnointi
2. reagointi
3. palautuminen

1. Havainnointi: käsittää normaalin käytettävyyssvalvonnan sekä tietoturvallisuusvalvonnan.

2. Reagointi: tähän toimintaan ryhdytään, jos näyttää ilmeiseltä, että sovitussa käytettävyyss-tasossa ei pysytä tai kun on ilmeistä tai mahdollista, että tietojen eheys tai luottamuksellisuus on uhattuna. Reagoinnilla pyritään estämään tai minimoimaan poikkeaman vaikutuksia.

3. Palautuminen: seuraa reagointia ja on sen välitön jatkotoimenpide. Palautumisessa korjataan tietoturvapoikkeaman vaikutukset ja siirrytään toiminnan normaalitilaan.

2 Organisaatio

Tietoturvapoikkeaman vakavuuden ja vaikutuksien arvioinnin mukaisesti määritetään vastatoimien laajuus ja tarvittavat henkilöt kytketään toimintaan mukaan.

Reagointiryhmän kokoonpano määräytyy poikkeaman perusteella aina tapauskohtaisesti, ja sen muodostuminen on kuvattu kohdassa 3.1. Sen tehtävänä on varmistaa, että poikkeamiin reagoidaan suunnitelmien mukaan, ja että kaikissa tilanteissa on mukana riittävästi asiantuntemusta ja asianmukaiset vastuuhenkilöt.

Vähäiseksi todetussa poikkeamatilanteessa ei välttämättä tarvita koko reagointiryhmän toimintaa, vaan järjestelmän vastuuhenkilö voi reagoida poikkeamaan itse, kunhan tiedottaa poikkeamasta tietoturvapäällikölle ja reagointiryhmän jäsenille. Merkittävissä ja vakavissa tietoturvapoikkeamissa toimintaan kytketään mukaan perusr ryhmä sekä tapauskohtaiset tahot.

Perusr ryhmään kuuluvat:

- [Tietohallintopäällikkö/-johtaja] (ryhmän johtaja)
- Tietoturvapäällikkö (sihteeri, koollekutsuja, toimeenpanija, [esittelijä])
- [Tietohallinnon/atk-keskuksen turvaryhmä/CSIRT-ryhmä]
- Tapauskohtaiset ryhmän lisäjäsenet (Liite 5).

Perusr ryhmällä on valmiudet ja valtuudet päättää voimakkaista suojatoimista vakavissa ja yllättävissä tilanteissa. Perusr ryhmä on elin, jonka jäsenet saavat tiedon poikkeamista, tarjoavat tapauskohtaista asiantuntemusta ja ovat parhaiten perillä tietoturvallisuuden kokonaiskuvasta yliopistossa. Yleisimmissä käytännön tilanteissa perusr ryhmä arvioi suositeltavimmat vastatoimet saamiensa tietojen perusteella ja antaa ohjeet henkilölle, joka suorittaa varsinaiset toimenpiteet.

3 Reagoiminen tietoturvapoikkeamiin

3.1 Tietoturvapoikkeamien vakavuuden arviointi ja reagointiryhmän laajentaminen

Kun tietoturvapoikkeama havaitaan, tavanomaisen toiminnan tai järjestelmien vastuuhenkilöiden tulee arvioida poikkeaman ja sen suorien tai potentiaalisten vaikutusten laajuus ja välittömien reagointitoimenpiteiden lisäksi laajentaa tarvittaessa toiminta seuraavalle tasolle. Toiminnan tason laajentuessa reagointiin osallistuvien henkilöiden määrä kasvaa ja merkittävässä tilanteissa myös vastuuhenkilö vaihtuu. Mikäli poikkeama koskettaa koko yliopiston tietoturvallisuutta, lopullisen toimintavastuun täytyy myös olla keskitettyä.

On huomattava, että tiedon luottamuksellisuuden todellinen vaarantuminen on luokiteltava aina vakavaksi poikkeamaksi (esim. tietyt virustartunnat).

Huom: taulukossa tarkoitettu kriittisyys määritellään keskitetysti koko yliopiston kannalta. Yksiköiden ylläpitämien sovelluksien, ohjelmistojen, palvelimien ja palveluiden kriittisyysluokitus riippuu yksikön toiminnoista.

Normaalitila	Henkilöt	Kuvaus
Työasemat	Järjestelmien vastuuhenkilöt Käyttäjät [Lähituki] [Helpdesk]	Käyttäjät seuraavat työasemiensa toimintaa. Vastuuhenkilöt seuraavat työasemaverkon toimintaa ja varoituksia eri lähteistä.
Palvelimet, järjestelmät, palvelut	Järjestelmän vastuuhenkilö Järjestelmän pääkäyttäjä(t) [Lähituki] [Helpdesk] [Tietoturvallisuusasiantuntija]	Vastuuhenkilöt ja pääkäyttäjät seuraavat järjestelmien toimintaa ja varoituksia eri lähteistä. Käyttäjät havainnoivat järjestelmän toimintaa.

Laajentamisvastuu: järjestelmän vastuuhenkilö tai erikseen määritellyissä tilanteissa [lähituki tai helpdesk] arvioi, onko kyseessä normaalitilanne vai poikkeama, ja toimii sen mukaan. Jos kyseessä on poikkeama, toimitaan seuraavasti:

Poikkeaman laajuus ja vakavuus	Reagointiryhmän kokoonpano	Kuvaus ja toimenpiteet

Vähäinen	Järjestelmän vastuuhenkilö Järjestelmän pääkäyttäjä(t) [Lähituki] [Helpdesk] [Yksikkökohtainen tietoturva- asiantuntija] Käyttäjä (jos tarpeen)	Poikkeama, jonka vaikutus arvioidaan vähäiseksi. Esimerkiksi eristetty virustartunta, yksittäisen sovelluksen tilapäinen käyttökatos, lyhytaikainen tietoliikennekatkos, virustorjunnan ja tietoturvapäivitysten laiminlyönti, resurssien tuhlaus jne. Kootaan reagointiryhmä. Määriteltävä vaikutukset ja vastatoimenpiteet. Informoitava tarvittaessa henkilöstöä toimenpiteistä. Informoidaan tietoturvapäällikköä, [ja/tai kirjataan tapahtuma keskitettyyn CERT-järjestelmään].
----------	--	---

Laajentamisvastuu: järjestelmän vastuuhenkilö (sekä oman harkintansa mukaan myös [tietoturvapäällikkö]) arvioi poikkeaman vakavuuden ja tarvittaessa siirtää reagoinnin perusryhmän vastuulle. Tämä tapahtuu [kirjaamalla hälytys/poikkeamaraportti keskitettyyn CSIRT-järjestelmään toimenpiteitä varten. Häätötilanteessa voi myös soittaa tietoturvapäällikölle].

Merkittävä	Perusryhmä Järjestelmän vastuuhenkilö Järjestelmän pääkäyttäjä [Lähituki] [Helpdesk]	Poikkeama, joka vaikutus arvioidaan merkittäväksi. Esimerkiksi sovelluksen toimintahäiriö, joka ylittää tai jonka arvioidaan ylittävän sovitun sallitun käyttökatoajan. Tällaisia ovat esim. kaikki merkittävät tietoliikennekatkot, sähköpostikatkot, kriittisten sovellusten katkot, joiden kesto aika voidaan arvioida, ja haittaohjelmien toiminta, joka häiritsee useampien työasemien/henkilöiden toimintaa tai estää sen kokonaan. Merkittävää voi olla myös, jos käyttäjän hallusta löytyy luvattomia ohjelmia tai materiaalia. Määriteltävä toimenpiteet haitan rajoittamiseksi ja poistamiseksi. Informoitava tarvittaessa henkilöstöä toimenpiteistä.
------------	---	---

Laajentamisvastuu: perusryhmän johtaja (tietohallintopäällikkö) arvioi, onko kyseessä merkittävä vai vakava poikkeama. Äkillisissä tilanteissa myös tietoturvapäällikkö voi suoraan todeta poikkeaman vakavaksi.

Vakava	Perusryhmä Tapauskohittaiset ryhmän jäsenet Järjestelmän vastuuhenkilö [Lähituki] [Helpdesk]	Poikkeama, jonka vaikutus arvioidaan vakavaksi. Esimerkiksi kaikki kriittisten sovellusten häiriöt, jotka ylittävät tai joiden arvioidaan ylittävän sallitun käyttökatkoajan, ja joiden kestoaikaa ei ole arvioitavissa. Haittaohjelmat, jotka tuhoavat tietoja, häiritsevät suuren joukon työasemien/henkilöiden toimintaa tai estävät sen kokonaan. Kaikki tilanteet, joissa tietojen luottamuksellisuus tai eheys on uhattuna, varsinkin onnistuneet tietomurrot tai murron yritykset yliopiston sisältä. Määriteltävä toimenpiteet haitan rajoittamiseksi ja poistamiseksi. Informoitava henkilöstöä. Valmistaudutaan mahdolliseen rikostutkintaan ja muihin seurauksiin.
--------	--	--

3.2 Vastatoimien laajentamisessa huomioitava

Tietoturvapoiikkeamiin reagoitaessa on huomioitava useita vaikuttavia tekijöitä, kun harkitaan toiminnan laajentamista. Tällaisia tekijöitä ovat:

- Miten laaja poikkeama on?
- Mikä sen vaikutus toimintaan on?
- Kuinka vaikeaa on rajoittaa poikkeamaa?
- Miten nopeasti poikkeama laajenee?
- Mikä on sen arvioitu rahallinen vaikutus?
- Mikä on sen arvioitu vaikutus julkisuuskuvaan?

3.3 Toimintavastuu

Vastuu toiminnasta on kohdan 3.1. mukaisesti määritellyllä henkilöllä; normaalitilanteissa ja vähäisissä poikkeamissa järjestelmän vastuuhenkilöllä, merkittävässä ja vakavissa poikkeamissa kohdassa 2 kuvatulla perusryhmän johtajalla. Hänen tehtävänä on johtaa ja ohjata torjuntatoimia tässä ja muissa yliopiston ohjeissa määriteltyjen menettelytapojen mukaan. Toimintaa laajennettaessa vastuu siirtyy vasta silloin, kun seuraava vastuuhenkilö on ilmoittanut ottaneensa vastuun, ei vielä ilmoitushetkellä.

Reagointiin osallistuvat henkilöt ovat omalta osaltaan vastuussa siitä, että päävastuussa olevan ohjeita noudatetaan.

Kaikesta tietoturvapoiikkeamaan liittyvästä toiminnasta pidetään tapahtumapäiväkirjaa, johon kirjataan toimenpiteet, ajankohdat, päätökset jne. Vastuu tapahtumapäiväkirjan pidosta on vastuuhenkilöllä, mutta jokaisen ryhmän jäsenen tulee kirjata päiväkirjaan omat toimenpiteensä.

Reagointiryhmä päättää, kuka poikkeamasta tiedottaa. Reagointiryhmän kokoonpanon muuttuessa (laajentamisen yhteydessä) myös tiedotusvastuu siirtyy vastaavasti. Tiedotus ohjeistetaan tarkemmin ohjeessa Tiedottaminen poikkeamatilanteissa.

Todistusaineisto on suojattava poikkeamissa, joista voi olla odotettavissa jälkiseurauksia.

3.4 Viranomaisilmoitukset

FUNET-CERT:lle ja CERT-FI:n organisaatioon (Viestintävirastossa) ilmoitetaan kaikista merkittävistä ja vakavista poikkeamista. Myös yliopistojen SEC-ryhmälle on hyvä lähettää ilmoitus, jos siitä voidaan arvella olevan hyötyä muille yliopistoille.

Ilmoituksen lähettää aina tietoturvapäällikkö.

Tietotekniikkarikoksen tunnusmerkistö täyttyy, kun tietojenkäsittelyrauhaa loukataan. Tietotekniikkarikokset määräytyvät rikoslain mukaisesti. Kyseessä voi olla esim. tietomurto (Rikoslaki 38:8§), tietokoneen luvaton käyttö (RL 28:7§), vahingontekorikos (RL 35:1§) tai törkeän viestintäsalaisuuden loukkaaminen (RL 38:4§).

Jos on aihetta epäillä jotain edellä mainituista rikoksista, [tietohallinto / -johtaja / tietoturvapäällikkö] harkitsee otetaanko yhteys poliisiin. Mahdollisen varsinaisen tutkintapyynnön laatii [tietohallinto/-johtaja/tietoturvapäällikkö] ja/tai yliopiston lakimies [rehtorin/hallintojohtajan] hyväksyttäväksi.

3.5 Poikkeaman jälkeinen toiminta

Toiminnasta kohdan 3.3. mukaisesti vastuussa oleva henkilö pitää huolen, että välittömästi poikkeaman jälkeen

- Kerätään ja analysoidaan tapahtumapäiväkirjat ja muut kriisin aikana tehdyt muistiinpanot sekä tarvittaessa haastatellaan asianosaisia
- Analysoidaan tapahtumalokit niiltä osin kuin sitä ei ole tehty jo poikkeaman selvittelyn aikana
- Kirjataan keskeiset poikkeaman aikana esiintyneet vaikeudet, ongelmat, resurssipuutteet, jne.
- Tehdään yhteenveto toiminnasta, johon sisältyy arvio lopputuloksen kannalta hyvin ja huonosti sujuneista toimista. Lisäksi yhteenvetoon tulee aina kirjata ehdotukset toiminnan kehittämiseksi
- Päätetään muun kertyneen aineiston käsittelystä
- Yhteenveto toimitetaan [tietoturvapäällikölle ja kirjataan keskitettyyn CSIRT-järjestelmään].

3.6 Poikkeamista tiedottaminen

Tiedottamisen tulee olla informoivaa, ohjaavaa, ohjeistavaa ja rauhoittavaa ja sen perustarkoituksena on ylläpitää tietoisuutta tosiasioista ja toimenpiteistä. Sen tulee ehtiä väärin tietojen edelle. Kaikista toimista informoidaan ainakin niitä henkilöitä, joiden toimintaan ne vaikuttavat. Vahinkotilanteissa tiedottamisen nopeusvaatimus korostuu. Vahinkojen ollessa laajalle ulottuvia tarvitaan tavanomaisten toimenpiteiden lisäksi valmiuksia myös syntyneen tilanteen hoitamiseksi organisaation ulkopuolella tehokkaasti ja mahdollisimman vähin vaurioin.

Poikkeamatilanteiden tiedotusta käsitellään tarkemmin ohjeessa Tiedottaminen poikkeamatilanteissa.

4 Ohjeen päivittäminen

Reagointiohjetta päivitetään tarvittaessa sekä yliopistojen yhteisen suosituksen muuttuessa. Päivitystarvetta seuraa [tietoturvapäällikkö].

5 Liitteet

[HUOM: liitteet ovat vain esimerkkejä erilaisista reagoitiohjeen aihepiiriin liittyvistä asiakirjoista, ne eivät ole valmiita pohjia.]

Liite 1: Järjestelmäkohtainen suunnitelma – palvelimet/palvelut

Liite 2: Ilmoitus tietoturvallisuuteen liittyvästä havainnosta

Liite 3: Suojakeinot

Liite 4: Tapahtumapäiväkirja

Liite 5: Perusryhmän yhteystietoja

Liite 1:

Asiakirjan turvaluokitus (kun täytetty)

JÄRJESTELMÄKOHTAINEN SUUNNITELMA

Turvaluokiteltu (TLL III)
LUOTTAMUKSELLINEN
 JulkL (621/1999) 24.1 §:n 7 ja 8 k

PALVELIMET/PALVELUT

YKSIKKÖ	Yksikkö	Tiedekunta	Vastuualue
Palvelimen vastuuhenkilö (omistaja)	Nimi		
	Asema		
	Toimipaikan osoite		
	Puhelin	Matkapuhelin	Sähköposti
	HUOM: Palvelimen vastuuhenkilöksi katsotaan yleensä yksikön/vastuualueen johtaja ellei toisin ole määrätty tässä tai muussa asiakirjassa.		
Palvelimen käyttö-tarkoitus			
	Seurattavat ominaisuudet, normaalitilan määritelmä		
Järjestelmän kuvaus	Palvelintyyppi		
	Julkinen palvelin	Extranet (rajattu pääsy)	Intranet (sisäinen käyttö)
	Tarkka sijainti		
	kulunvalvonta	Murtohälyttimet	Olosuhdevalvonta
	Laitteistokuvaus (merkki, malli, lisälaitteet)		
	Käyttöjärjestelmä ja versio		
	Ohjelmistosovellukset (versiotietoineen)		

Liite 2:

ILMOITUS TIETOTURVALLISUUTEEN LIITTYVÄSTÄ POIKKEAMASTA

Millaisesta tietoturvapoikkeamasta on kyse (lyhyt kuvaus):

Mihin tietoon tai järjestelmään uhka tai vahinko kohdistuu:

Milloin ja missä vahinko on tapahtunut:

Mitä vahinkoja on aiheutunut/aiheutuu:

Esimerkiksi tietojen tai palvelujen saatavuus, tietojen luottamuksellisuus, tietojen oikeellisuus, taloudelliset vahingot tai vahinkouhkat, vakavammat vahingot.

Muu vaara, millainen:

Kuka on vastuussa tästä tiedosta tai järjestelmästä:

Keneltä saa lisätietoja yllä esitetystä havainnosta (yhteystiedot):

Muuta:

Ilmoittajan nimi:

Ilmoittamisen ajankohta:

Kenelle/keille ilmoitus toimitettiin:

Liite 3:

SUOJAKEINO (esitetään jälkeenpäin, kun tietoturvapoikkeama on korjattu ja tilanteesta on palattu normaalitilaan)

Kuinka edellä kuvattu uhka tai vahinko voidaan jatkossa estää tapahtumasta:

Suojakeinon mahdolliset kustannukset, toteuttamisen aikataulu ja tarpeelliset yhteistyökumppanit:

Millaisilla muilla keinoilla uhkaan voidaan varautua tai on jo varauduttu:

Keneltä saa lisätietoja yllä esitettyihin suojakeinoihin liittyen:

Muuta:

Liite 5:

PERUSRYHMÄN YHTEYSTIETOJA

Organisaatio ja yhteystiedot:

Turvaluokiteltu (TLL IV)
VIRANOMAISKÄYTTÖ
JulkL (621/1999) 24.1 §:n 7 ja 8 k

Perusryhmä

Tietohallintopäällikkö

puh.

Tietoturvapäällikkö

puh.

Atk-keskuksen sec-ryhmä

(Huom: tietohallintopäällikön ja tietoturvapäällikön varahenkilöt on määrättävä poikkeustilanteiden varalta. Varahenkilöluettelo on salainen (TL II).)

Tapauskohtaiset ryhmän jäsenet

[Tämä luettelo voi olla hankala laatia koko yliopistoa palvelevaksi]

Lakimies

Tiedotusyksikön edustaja

Järjestelmäasiantuntija

Tietoliikenneasiantuntija

Järjestelmän kehittäjä

Tietokanta-asiantuntija

Järjestelmän omistaja

Turvallisuuspäällikkö

Valmiuspäällikkö/-ryhmä

Järjestelmäasiantuntija

Teleliikenne, viranomaisverkko

Tietoliikenne, palomuurit, yhdysliikenne

Sähköposti-, virus- ja nimipalvelut

Työasema-palvelinverkko

Järjestelmän kehittäjä

Tilanteen mukaan

Tietokanta-asiantuntija

Tilanteen mukaan

Järjestelmän omistaja

Tilanteen mukaan