ROVANIEMEN KOULUTUSKUNTAYHTYMÄ Tietoturvapoikkeamiin reagoiminen v.2006

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 Rovaniemen koulutuskuntayhtymässä nopeasti, niihin reagoiminen aloitetaan viipymättä ja se tehdään ennalta sovitun menettelytavan (= tämä ohje) mukaisesti.

Tietoturvapoikkeamiksi määritellään tilanteet, joissa Rovaniemen koulutuskuntayhtymän vastuulla olevien tietojenkäsittelytoimintojen ja –palvelujen käytettävyyttä[1] ei voida hoitaa suunnitelmien mukaan tai joissa tietojen eheys[2] tai luottamuksellisuus[3] on uhattuina.

Reagointisuunnitelmaa on noudatettava kaikkien tietojärjestelmien, myös yksittäisten työasemien hallinnoinnissa.

Jokaisen yksikön tulee laatia keskeisistä/kriittisistä palvelinjärjestelmäkohtaiset reagointisuunnitelmat (malli liitteessä 1), vahvistaa ne ja toimittaa tietoturvapäällikölle tiedoksi.

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] 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).

1.2. Tietoturvapoikkeamien reagointiryhmä

Tietoturvapoikkeamien reagointiryhmän tehtävänä on varmistaa, että tapahtumiin reagoidaan suunnitelmien mukaan, ja että kaikissa tilanteissa on mukana riittävästi asiantuntemusta ja vastuuhenkilöitä.

Reagointiryhmän kokoonpano määräytyy poikkeaman perusteella, ja sen muodostuminen on kuvattu kohdassa 3.2 Laajentaminen.

1.3. Tietoturvapoikkeamien käsittely

Tietoturvapoikkeamien käsittely jaetaan kolmeen vaiheeseen:

1. havainnointi
2. reagointi
3. palautuminen

1. Havainnointi: käsittää normaalin käytettävyysvalvonnan sekä tietoturvallisuusvalvonnan.

2. Reagointi: tähän toimintaan ryhdytään, jos näyttää ilmeiseltä, että sovitussa käytettävyystasossa 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 vakavuus ja vaikutukset arvioidaan ja sen mukaisesti määritetään vastatoimien laajuus ja tarvittavat henkilöt kytketään toimintaan mukaan.

Tietoturvapoikkeamien vastatoimista vastaavan reagointiryhmän kokoonpano määräytyy poikkeaman vakavuuden ja laajuuden perusteella. Reagointiryhmän kokoonpano eri vakavuus- ja laajenemistasoilla on kuvattu kohdassa 3.2 Laajentaminen.

Vakavuudeltaan merkittävissä tietoturvapoikkeamissa (= vakavuusluokat 2 ja 3) toimintaan kytketään mukaan alla kuvatut perusryhmä sekä tapauskohtaiset tahot.

Perusryhmään kuuluvat:

- Tietohallintopäällikkö
- Tietoturvavastaava
- Tapauskohtaiset ryhmän lisäjäsenet ○ Järjestelmien vastuuhenkilöt ○ Kiinteistöpäällikkö
  - Henkilöstöpäällikkö
  - Yksikön johtaja
  - lakimies
  - luottamusmies
  - ulkoistetun palvelun vastuuhenkilö
  - muu perusryhmän kutsuma henkilö

3. Reagoiminen tietoturvapoikkeamiin

3.1. Tietoturvapoikkeamien vakavuuden arviointi

Tietoturvapoikkeamat luokitellaan kolmeen vakavuusluokkaan.

Vakavuus-luokka	Kuvaus
Vähäinen	Pääsääntöisesti poikkeama jonka vaikutus on suppea ja ei vaikuta mitenkään koko järjestelmän toimintaa ja josta voidaan palautua nopeasti normaalitilaan. Esimerkiksi, eristetty virustartunta, yksittäisen sovelluksen tilapäinen käyttökatkos, lyhytaikainen/paikallinen tietoliikenne katkos virustorjunnan ja tietoturvapäivitysten laiminlyönti, resurssien tuhlaus.
Merkittävä	Poikkeama joka vaikuttaa määrällisesti useiden käyttäjien toimintaan tai jonka arvioidaan ylittävän sovitun sallitun käyttö-katkoajan. Myös merkittävä tietoliikennekatkot, sähköpostikatkot, kriittisten sovellusten katkot, joiden kestoaika 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.

Vakava	Vakavaksi poikkeamaksi luokitellaan 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.

Taulukossa arvioidut poikkeamat koskevat koko Rovaniemen koulutuskuntayhtymän tietojärjestelmää. Yksikkökohtaisesti voidaan tietojärjestelmä tai – palvelu luokitella suurempaan vakaavuusluokkaan.

3.2. Laajentaminen

Kun tietoturvapoikkeama havaitaan, tavanomaisen toiminnan tai järjestelmien vastuuhenkilöiden tulee arvioida poikkeaman laajuus ja välittömien reagointitoimenpiteiden lisäksi laajentaa tarvittaessa toiminta seuraavalle tasolle. Järjestelmien vastuuhenkilöillä tarkoitetaan tässä tapauksessa yksikön nimettyä atk- vastaavaa tai hänen varahenkilöä tai tietojärjestelmälle erikseen nimettyä teknistä vastuuhenkilöä ja hänen varahenkilöä.

Normaali-tila	**Henkilöt**	**Kuvaus**
Työasemat	• Järjestelmän vastuuhenkilö • Käyttäjät • Atk-ylläpitohenkilöstö	Käyttäjät seuraavat työasemiensa toimintaa. Vastuuhenkilöt seuraavat työasemaverkon toimintaa ja varoituksia eri lähteistä.
Palvelimet, järjestelmät, palvelut	• Järjestelmän vastuuhenkilö • Järjestelmän pääkäyttäjä • Atk-ylläpitohenkilöstö	Vastuuhenkilöt ja pääkäyttäjät seuraavat järjestelmien toimintaa ja varoituksia eri lähteistä. Käyttäjät havainnoivat järjestelmän toimintaa.

Laajentamisvastuu ⇒ 1 Järjestelmän vastuuhenkilö ja atk-vastaava

Poikkeaman laajuus	Reagointiryhmän kokoonpano	Kuvaus
1	• Järjestelmän vastuuhenkilö • Järjestelmän pääkäyttäjä • Atk-ylläpitohenkilöstö • Tietoturvavastaava	Uhka on havaittu, vakavuusluokaksi on arvioitu vähäinen. Määriteltävä vaikutukset ja vastatoimenpiteet. Informoitava tarvittaessa henkilöstöä toimenpiteistä. Informoidaan tietoturvavastaavaa.

laajentamisvastuu ⇒ 2 **järjestelmän vastuuhenkilöllä**, sekä oman harkintansa mukaan myös tietoturvavastaavalla.

2	• Perusryhmä • Järjestelmän vastuuhenkilö • Järjestelmän pääkäyttäjä • Atk-ylläpitohenkilöstö	Uhka on kiistaton, vakavuusluokaksi on arvioitu vähäinen tai merkittävä. Määriteltävä toimenpiteet haitan rajoittamiseksi ja poistamiseksi. Informoitava tarvittaessa henkilöstöä toimenpiteistä.

laajentamisvastuu ⇒ 3 **perusryhmän johtajalla (**tietohallintopäällikkö**)**

3	• Perusryhmä • Tapauskohtaiset ryhmän jäsenet • Järjestelmän vastuuhenkilö •	Uhka on laaja tai vaikutus on merkittävä, vakavuusluokaksi on arvioitu vakava. Määriteltävä toimenpiteet haitan rajoittamiseksi ja poistamiseksi. Informoitava henkilöstöä. Valmistaudutaan mahdolliseen rikostutkintaan ja muihin seurauksiin.

3.3. Vastatoimien laajentamisessa huomioitava

Tietoturvapoikkeamiin 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?

3.4. Toimintavastuu

Vastuu toiminnasta on kohdan 3.2. mukaisesti määritellyllä henkilöllä. Hänen tehtävänään on johtaa torjuntatoimia.

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

Tietohallintopäällikkö päättää tiedottamisesta, niin sisäisestä kuin ulkoisesta, tietoturva loukkaus tilanteessa.

Todistusaineisto on suojattava poikkeamissa, joista voi olla odotettavissa jälkiseurauksia.

3.5. Viranomaisilmoitukset

FUNET-CERT:lle ja CERT-FI:n organisaatioon (Viestintävirastossa) ilmoitetaan kaikista laajenemistason 2 ja 3 saavuttaneista poikkeamista.

Ilmoituksen lähettää aina tietohallintopäällikkö tai hänen sijaisenaan tietoturvavastaava.

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, tietohallintopäällikkö tai tietoturvavastaava harkitsee otetaanko yhteys poliisiin. Mahdollisen varsinaisen tutkintapyynnön laatii tietohallintopäällikkö kuntayhtymän johtajan hyväksyttäväksi.

3.6. Poikkeaman jälkeinen toiminta

Toiminnasta kohdan 3.4. 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 hoidon 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

3.7. Poikkeamista tiedottaminen

Tiedottamisen tulee olla informoivaa, ohjaavaa, ohjeistavaa ja rauhoittavaa ja sen perustarkoituksena on ylläpitää tietoisuutta tosiasioista ja toimenpiteistä. Sen tulee ehtiä väärien 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.

Näiden ohjeiden päivittäminen

Sääntöjä päivitetään tarvittaessa tai Rovaniemen koulutuskuntayhtymän yhteisen sääntösuosituksen muuttuessa. Päivitystarvetta seuraa tietoturvavastaava