| | |
|---|---|
| **Laki julkisen hallinnon tiedonhallinnasta**<br>**Suosituskortti**<br>**Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät ja ylläpitäjät<br>**Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua | |
| 17 § Lokitietojen kerääminen | versio<br>0.95/1.11.2019 |

**17 § Lokitietojen kerääminen**

Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

Hallituksen esitys HE 284/2018
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Lokitietojen perusteella voidaan selvittää virhetilanteita ja valvoa tietojärjestelmien käyttöä muun muassa oikeusturvan toteuttamiseksi ja virkavastuun todentamiseksi sekä häiriöiden ja riskin muodostavien poikkeamien tunnistamiseksi. Lokitiedot ovat tietojärjestelmistä automaattisesti kirjautuvia tapahtumatietoja, jotka muodostavat lokin. Tällaisia lokitapahtumia ovat tietojärjestelmän, sovelluksen tai laitteen muodostamat tapahtumatiedot, jotka kuvaavat esimerkiksi tietojärjestelmään ulos- tai sisäänkirjautumista, tiedon käsittelyä (katselu, lisäys, muutos, poisto) tai palomuurin suorittamaa toimenpidettä.

Lokitietoja tarvitaan sekä normaalitilanteissa että poikkeamatilanteissa. Normaalitilanteissa lokien avulla toteutetaan muun muassa toiminnan häiriöttömyyden seurantaa, käytönvalvontaa, tilastointia ja laskutusta. Poikkeustilanteissa lokeja käytetään muun muassa syiden selvittämiseen, tilanteen normalisointiin sekä tapahtumien ja niiden osapuolten tunnistamiseen. Lokitietojen käsittelyn yhtenä tavoitteena on siis varmistaa tapahtumien osapuolet, kulku ja tapahtumaketjun kiistämättömyys sekä kyetä havaitsemaan ja hallitsemaan tunkeutumisyrityksiä, poikkeamia, häiriöitä ja suorituskykyongelmia. Poikkeamien ja häiriöiden tunnistamisen lisäksi lokitietoja voidaan kuitenkin hyödyntää myös nykytilan seuraamiseen ja visualisointiin, trendien tunnistamiseen ja tulevan ennustamiseen sekä päätöksenteon ja toiminnan tukemiseen.

Lokitiedot eivät ole välttämättä aina tietojärjestelmistä muodostuvia sähköisiä lokitietoja, sillä tietoaineistojen käsittely ja luovuttaminen voi olla myös manuaalista paperisia tietoaineistoja koskevaa käsittelyä. Tällöin samat suositukset on huomioitava soveltuvin osin myös paperiaineistojen käsittelyä koskevan seurannan suunnittelussa ja toteuttamisessa.

**Lokitiedot**
Lokitiedot kuvaavat jonkin tapahtuman toteutumista tiettynä hetkenä ja niiden on kyettävä esittämään tarvittavat tiedot näistä tapahtumista luotettavasti kirjatun tapahtumaketjun (*audit trail*) muodostamiseksi. Lokitietoja kerätään erityyppisistä toimenpiteistä, kuten tietojärjestelmien käytöstä ja tiedon luovutuksista, tietojärjestelmien ylläpidosta sekä niiden teknisestä toiminnasta ja virheistä.

Käytöstä, muutoksista ja luovutuksista kerättävät lokitiedot kuvaavat tietojen käyttöä, niihin tehtäviä muutoksia ja tietojen luovutuksia. Lokitiedot kerätään tietojärjestelmän käytöstä ja tietojen luovutuksista varsinkin, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta

kirjautumista. Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, luovuttavassa järjestelmässä kerätään luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen perusteensa. Lisäksi käyttölokitiedot kerätään ainakin tietojärjestelmistä, joissa käsitellään salassa pidettäviä tietoja. Käyttölokitietojen keräämisen tarvetta arvioidaan erityisesti sillä perusteella, tarvitaanko niitä virheselvittelyjä varten tai yksilön etujen, oikeuksien ja velvollisuuksien sekä oikeusturvan toteuttamiseksi taikka virkavastuun todentamiseksi. Tietojärjestelmien ylläpitotoimista kerättävät lokitiedot kuvaavat tietojärjestelmän toimintaan ja käyttöoikeuksiin tehtyjä muutoksia ja tekniset järjestelmä- ja virhelokit kuvaavat muun muassa teknisiä virheitä ja toimintahäiriöitä.

**Lokienhallinnan suunnittelu ja ohjaus**

Lokien kerääminen ja käsittely perustuvat lakiin. Lokienhallinnan toteuttamista ja lokitietojen käsittelyä organisaatiossa kuvataan ja ohjataan lokiperiaatteissa ja -suunnitelmassa, jotka ottavat kantaa lokien käsittelyyn liittyviin rooleihin ja vastuisiin, lokien käsittelyn elinkaaren vaiheisiin (miten niitä kerätään, käsitellään ja säilytetään), käsittelyn tarpeeseen ja perusteeseen sekä lokienhallinnan tekniseen toteutukseen.

Lokitietoja ei kerätä ja käsitellä summittaisesti, vaan määritetyn tarpeen pohjalta laadittujen lokiperiaatteiden ja -suunnitelman mukaisesti. Ennen tietojärjestelmän ja siihen liittyvien lokijärjestelyiden toteuttamista toteutus, käyttötapa sekä kerättävien ja käsiteltävien tietojen tarpeellisuus selvitetään ja kuvataan. Lainsäädäntö asettaa myös suojausvelvoitteita tietojen, erityisesti henkilötietojen, suojelemiseksi. Tämä tarkoittaa sitä, että tietojen suojaustarpeet tunnistetaan ja huomioidaan lokien käsittelyn, tieto- ja lokijärjestelmien sekä järjestelmähankintojen suunnitteluvaiheessa.

Osana lokienhallinnan suunnittelua ja sitä ohjaavan dokumentaation laatimista:

- Tunnistetaan lokitietoihin ja lokien käsittelyyn liittyvät ulkoiset vaatimukset lainsäädännöstä, määräyksistä ja mahdollisista sopimuksista
- Määritetään toimintatavat lokienhallinnalle ja käsittelylle
- Määritetään lokien käsittelyprosessi ja –tavat sekä käsittelyyn liittyvät roolit ja vastuut
- Määritetään prosessi lokienhallinnan ja käsittelyn asianmukaisuuden ja lainmukaisuuden säännölliseksi arvioimiseksi
- Tunnistetaan miksi ja mihin tarkoitukseen kutakin lokia käsitellään
- Tunnistetaan tietojärjestelmät ja laitteet, joiden tulisi tuottaa lokitietoja (esim. kriittiset tietojärjestelmät ja salassa pidettävän tiedon käsittelyyn tarkoitetut tietojärjestelmät)
- Arvioidaan tallennettavien tietojen tarpeellisuus
- Tunnistetaan lokeihin tallentuvat tietotyypit, erityisesti henkilötiedot ja tunnistamistiedot.
- Tunnistetaan tallentuvien tietotyyppien suojaustarpeet.
- Määritetään suojaustarpeet ja tavat (kuten salaus, varmuuskopiointi, pääsynhallinta) lokien suojaamiseksi
- Varmistaa, että tietojen suojaustarve toteutuu järjestelmän toteutuksessa ja tietojen käsittelyssä.
- Huomioida tarve lain yksityisyyden suojasta työelämässä mukaiselle yhteistoimintamenettelylle, mikäli kyseessä on tekninen valvonta.

- Huomioida yhteistoimintamenettelyn lisäksi muu käyttäjien, rekisteröityjen tai muiden tahojen informointi.
- Huomioida henkilötietojen käsittelyä koskevat lainsäädännön (kuten tietosuoja-asetus ja tietosuojalaki) asettamat vaatimukset, jos lokit sisältävät henkilötietoja.
- Suunnitella ja dokumentoida säilytystarve ja varmistaa sen toteutuminen käytännössä.
- Määrittää lokien keräämiseen liittyvät konfiguraatiot tietojärjestelmille ja laitteille

Lokeihin liittyvät vaatimukset määritellään ja edellytetään toteutettavaksi myös järjestelmäkehityksen, hankinnan tai ulkoistuksen yhteydessä lisäämällä ne osaksi näitä koskevia vaatimusmäärittelyitä, suunnitelmia ja sopimuksia. Toimittajilta edellytetään kuvausta omalla vastuullaan olevien järjestelmien tai toimintojen lokien keräämiseen, tallennukseen ja analysointiin liittyvistä asioista. Sopimuksen teon yhteydessä määritetään myös lokien käsittelyyn liittyvät vaatimukset ja käytännöt sekä lokitiedot omistava organisaatio ja omistajan mahdollisuudet saada lokitietoja käyttöönsä tarpeen vaatiessa. Organisaatio voi kerätä lokitietoja myös käyttämistään tietojärjestelmistä ja palveluista, jotka eivät ole sen itsensä hallussa, vaan palveluntarjoajan omistamia.

Lokitietojenkäsittelyyn sekä etenkin keräämiseen ja säilyttämiseen ja säilytysaikoihin voi kohdistua vaatimuksia erityislainsäädännöstä sekä määräyksistä ja standardeista, jotka ohjaavat säilytysaikojen määrittämistä. Tällaisten on tunnistettava ja huomioitava osana lokienhallintaa.

**Lokitietojen kerääminen**
Lokitietoja tuotetaan ja kerätään tietojärjestelmän käytöstä ja tietojen luovutuksista, mutta missä laajuudessa ja mitä lokitietoja, perustuu tiedonhallintalain mukaiseen tarpeellisuusarviointiin. Tähän arviointiin pohjautuvat lokitietojen keräämisen peruste ja laajuus (mitä lokitietoja kerätään) sekä lokitietojen käyttötarkoitus ja käsittelyn laajuus (miten ja kenen toimesta niitä käsitellään). Tarpeellisuusarviointiin vaikuttaa myös yleisessä tietosuoja-asetuksessa säädetyt vaatimukset teknisten ja organisatoristen toimenpiteiden toteuttamiseksi henkilötietojen suojaamiseksi. Tarpeellisuusarvioinnin tekee tietojärjestelmästä vastuussa oleva viranomainen.

Lokitietojen käyttötarve määrittelee sen, mitä tietoja lokitietoina kerätään tietystä tietojärjestelmästä. Tarpeellisuusarviointiin perustuen, jokaisen kerättävän lokitiedon tulee sisältää riittävät tiedot tarvittavan luotettavan tapahtumaketjun muodostamiseksi sekä tapahtumien valvomiseksi ja analysoimiseksi. Lokin käyttökelpoisuus riippuu siihen kerättävien tietojen riittävyydestä lokin käsittelytarkoitusta varten. Lokitiedot kuvaavat lokeille aina riittävässä laajuudessa jokaisen tapahtuman osalta sen, milloin, missä, kuka ja mitä:

- Milloin (milloin tapahtuma oli?)
    - Lokitiedon aikaleima eli päivämäärä ja kellonaika
    - Tapahtuman aikaleima päivämäärä ja kellonaika (lokitiedon ja tapahtuman aikaleima voivat joskus myös erota toisistaan)
    - Tapahtuman tunniste
- Missä (mihin tietoon ja/tai järjestelmään tapahtuma ja toiminta kohdistuivat?)

- Tapahtuman kohteen (tietojärjestelmän, laitteen, sovelluksen) tunnistetiedot, kuten nimi, kohdeosoite, laitteen identiteetti ja tunnistetiedot, yhteystapa, käytetty protokolla sekä sijainti
- Tapahtuman kohdetta kuvaavat tiedot, kuten missä tietojärjestelmän, sovelluksen tai palvelun osassa ja mihin elementtiin tai tietoon tapahtuma on kohdistunut

- Kuka (toimija eli kuka tai mikä teki ja mikä oli tapahtuman lähde?)
  - Tapahtuman lähteen (ihmis- tai laitekäyttäjän) tunnistetiedot, kuten nimi, lähdeosoite, henkilön tai laitteen identiteetti ja tunnistetiedot, sijainti
  - Millä oikeuksilla ja valtuuksilla tapahtuma tehtiin
- Mitä (mitä tapahtui ja onnistuiko tapahtuma?)
  - Tapahtuman tyyppi, kuten objektin luominen, objektin muuttaminen, kirjautuminen tai järjestelmän kaatuminen
  - Tapahtuman tila (onnistuiko vai epäonnistuiko tapahtuma ja miksi se mahdollisesti epäonnistui)
  - Tapahtuman merkitys tai prioriteetti
  - Tapahtuman kuvaus

Lokiin ei lähtökohtaisesti tule kerätä seuraavan kaltaisia tietoja:

- henkilötunnuksia
- erityisiä henkilötietoja (ns. arkaluonteiset henkilötiedot)
- luottokorttinumeroita
- salasanoja (ei edes tiivistemuotoisia)
- järjestelmien välisiä käyttöavaimia ja salaisuuksia
- valtuutustietoja
- henkilöiden välisen viestiliikenteen sisältöä
- lähdekoodia
- lokienhallintajärjestelmää korkeampaa turvallisuuden tasoa edellyttäviä tietoja

Lokilähteet ovat tietojärjestelmiä, sovelluksia tai laitteita, jotka tuottavat lokitietoja. Lokia tuottavina lokilähteinä voivat toimia muun muassa:

- sovellukset
- käyttöjärjestelmät
- palvelimet
- päätelaitteet
- verkkolaitteet
- palomuurit
- pääsynhallinta
- tunkeutumisenestojärjestelmä (IPS)
- tunkeutumisenhavaitsemisjärjestelmä (IDS)
- virustorjuntaohjelmat

Mikäli käytössä on useita lokeja, niin niiden helposti tapahtuva yhdistely analysointitarpeita varten on hyvä mahdollistaa. Lokia tuottavien lokilähteiden kellojen synkronointiin varmistetaan, jotta eri järjestelmien tuottamat lokitiedot ovat keskenään yhtenäisiä ja jotta niistä voidaan muodostaa

yhtenäinen tapahtumaketju. Erityisesti lokilähteiden aikaleimojen on tarve olla samassa ajassa. Eri lokeja tuottavien järjestelmien aika on mahdollista synkronoida NTP:n (Network Time Protocol) avulla. Myös lokien aikavyöhyketiedot on hyvä tallentaa. Suositeltavaa on käyttää UTC-aikaa kaikissa lähteissä, jotta lokitapahtumien kohdistaminen keskenään onnistuu myöhemmin.

Käyttö- ja luovutuslokien tietosisällön suunnittelu on yleensä järkevää tehdä koko järjestelmän tietosisällön ja käyttötapauksien määrittelyn yhteydessä, kuitenkin niin, että lokitapahtumien lisääminen ja poistaminen on helppoa järjestelmän elinkaaren kaikissa vaiheissa. Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen perusteensa. Jos tietoaineistojen luovutus tapahtuu tietojärjestelmien ulkopuolella, paperimuodossa, on luovutuslokien kirjaaminen suunniteltu myös tämän osalta.

Käyttöä, muutoksia ja luovutuksia koskevien lokitietojen keräämistä määriteltäessä arvioidaan muun muassa seuraavan tyyppisten tietojen tarpeellisuutta:

- tiedot tietojen tallentamisesta, muuttamisesta, poistamisesta, katselusta tai muusta tietoihin kohdistuvasta toimenpiteestä sisältäen tiedot mm.
    - tietosisällön lisäyksistä ja poistoista (voidaan kutsua myös muutoslokiksi),
    - tietosisällön muutoksista ja epäonnistuneista kirjauksista (voidaan kutsua myös muutoslokiksi),
    - tietokannan lukutapahtumista ja kyselytiedoista hakuehtoineen,
    - tulostuksesta ja
    - tietojen luovutuksista
- tiedot sisään- ja uloskirjautumisista käyttäjä-, ryhmä- ja sovellustietotasoilla (voidaan kutsua myös pääsynvalvontalokiksi)

Teknisen lokin tietosisältö on tyypillisesti vähemmän tarkasti määritelty kuin käyttölokien, mutta erityistä huomiota on kiinnitettävä siihen, ettei tekniseen lokiin kerry sellaista salassa pidettävää tietoa, joka ei ole välttämätöntä järjestelmän käytön selvittämisen kannalta. Tällaisia voivat olla esimerkiksi tarkemmat kuvaukset käsitellystä tietosisällöstä tai erityisiä henkilötietoryhmiä koskevat tiedot, kuten terveyttä koskevat tiedot. Tietojärjestelmien ylläpitotoimia ja teknisiä järjestelmä- ja virhetietoja koskevien lokitietojen keräämistä määriteltäessä arvioidaan muun muassa seuraavan tyyppisten tietojen tarpeellisuutta:

- tiedot käyttöoikeuksien muutoksista, poistoista ja lisäyksistä,
- tiedot järjestelmään tehdyistä muutoksista,
- tiedot järjestelmien järjestelmäparametrien ja asetustiedostojen muutoksista.
- tiedot seurattavassa tietojärjestelmässä tai tapahtumassa havaituista virheistä,
- tiedot käyttöön liittyvien virhetilanteiden hallinnasta ja
- tiedot havaituista virheistä ja epäjatkuvuuksista.

Tietojärjestelmän käyttöä koskevien lokitietojen ja keräämisen ja seurannan merkitys korostuu erityisesti, kun tietojärjestelmässä käsitellään salassa pidettäviä tietoja. Lokitietojen tarkoituksena on myös dokumentoida tietojärjestelmistä tehtävät luovutukset ja samalla osaltaan varmistaa, että luovutuksille on ollut olemassa lainmukainen peruste. Tästä johtuen, jos tietojärjestelmästä

luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, tulee luovuttavassa järjestelmässä kerätä luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen peruste.

Samaan järjestelmään liittyvät erilaiset lokit on hyvä toteuttaa niin, että niiden tietoja voidaan yhdistää ja erotella. Mikäli erilaiset lokitiedot on kerätty yhteen lokiin, on tietojen suositeltavaa olla sellaisessa muodossa, että kiinnostavia käyttötapahtumia pystytään seuraamaan niin, ettei esimerkiksi teknisen lokiaineiston runsaus hankaloita näiden seuraamista.

Lokitiedot ovat osa viranomaisten tietojärjestelmien tietoturvajärjestelyjä, joten ne ovat salassa pidettäviä julkisuuslain 24 §:n 1 momentin 7 kohdan perusteella, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista.

**Lokitietojen säilyttäminen**
Lokitietojen säilyttämisen suunnittelussa määritetään lokien säilytysaika ja –paikka. Säilytysaika johdetaan aina niiden käyttötarkoituksesta eli siitä, miksi lokia ja sen tietoja kerätään. Viranomaisen on hyvä tunnistaa ne lokitiedot, joiden säilytysaika on tyypillisesti vähintään viisi vuotta viranomaistoiminnassa rikosoikeudellisten vanhentumisaikojen vuoksi. Erityislainsäädännössä voi olla säädettynä erikseen lokitietojen säilytysajoista etenkin, jos lokitietoja säilytetään pitempiä aikoja kuin on tarpeen viranomaisella olevien velvollisuuksien toteuttamiseksi. On tärkeää varmistaa, että lokitiedot säilyvät ja ovat käytettävissä koko määritetyn säilytysajan, jonka jälkeen vanhentuneet lokit on poistettava.

Teknisten lokien säilytysajan tulee olla riittävän pitkä, jotta niitä voidaan käyttää erilaisten järjestelmän toimivuuteen liittyvien ongelmien selvittämiseen. Tietoturvaan liittyvät tapahtumat (kuten erilaiset väärinkäytökset tai tietojen luvaton käyttö), voivat ovat sellaisia tapahtumia, jotka voidaan havaita vasta kauan tapahtuman jälkeen. Tämä huomioidaan lokien säilytyksessä siten, että esimerkiksi teknisiä lokeja, joissa on ainoastaan teknisiä ongelmia koskevia tietoja, suositellaan säilytettäväksi vähintään 6 kuukautta, mutta tietomurtotapausten selvittelyyn edellä mainittu 6 kuukauden säilytysaika on useimmiten sen sijaan riittämätön. Myös käyttö- ja luovutuslokin muuttumattomuudesta voi olla mahdotonta varmistua, mikäli keskeiset tekniset lokit eivät ole käyttölokeja vastaavan säilytysajan piirissä. Edellä mainittujen tarpeiden täyttämiseksi keskeisille teknisille lokeille suositellaan yleisesti vähintään 5 vuoden säilytysaikaa.

Lokien säilyttämistarve voi edellyttää pidempiä säilytysaikoja, kuin mitä esimerkiksi lokia tuottava sovellus tai tietojärjestelmä ja tallennuskapasiteetti tukevat, jolloin syntyy tarve lokien arkistoinnille. Lokien pitkäaikaissäilytyksellä tarkoitetaan lokien säilyttämistä pidennetyn ajan. Lokit voidaan siirtää pidempiaikaiseen säilytykseen esimerkiksi erilliselle lokipalvelimelle tai lokien tähän tarkoitetulle muulle laitteelle, jottei lokia tuhota normaalin lokikierron mukaan säilytysaikaa lyhemmässä ajassa. Lähtökohtaisesti on kuitenkin aina suositeltua toteuttaa keskitetty lokienhallinta, jossa lokit siirretään lähdejärjestelmistä erilliseen keskitettyyn lokienhallintajärjestelmään, mikä mahdollistaa myös tehokkaamman lokien seurannan ja analysoinnin.

Lokien keräämistä varten on suunniteltu tarvittavat toimintamallit ja infrastruktuuri, jotta lokeille on varattu riittävästi säilytystilaa suhteessa kerättävien lokien määrän ja niiden säilytysaikaan.

| **Laki julkisen hallinnon tiedonhallinnasta**<br>**Suosituskortti**<br>**Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät ja ylläpitäjät<br>**Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua | |
|---|---|
| 17 § Lokitietojen kerääminen | versio<br>0.95/1.11.2019 |

Säilytystilan suunnittelussa ja toteutuksessa on huomioitu myös se, ettei lokien kerääminen pysähdy lokin tai lokitilan täyttyessä, vaan lokien kerääminen jatkuu häiriöttä. Lokien säilytyskapasiteettia seurataan ja siihen liittyvistä ongelmista on tärkeä luoda hälytyksiä.

Kun lokitietojen käsittelylle ei ole enää tarvetta ja niiden säilytysaika on umpeutunut, ne joko poistetaan tai anonymisoidaan. Lokitietojen tyhjentäminen on automatisoitu poistamaan alkuperäisestä lokista kaikki lokitiedot, jotka ylittävät määritetyn säilytysajan. Tässä yhteydessä tulee huomata, että lokeja on tyypillisesti myös tallennettu varmistusnauhoille tai muille vastaaville tallennus ja arkistointivälineille, joista tiedot tulee tarvittaessa myös poistaa. Lokitietojen poistaminen ja anonymisointi tehdään ennalta määritetyn toimintamallin ja säilytysaikojen mukaisesti.

**Lokitietojen seuranta ja analysointi**

Tarvittavan havainnointikyvykkyyden luomiseksi ja ylläpitämiseksi lokitietoja on seurattava ja analysoitava säännöllisesti. Tämän toteuttamiseksi on luotu tarvittavat prosessit ja tekniset valmiudet, jotka mahdollistavat riittävän havainnointikyvykkyyden. Lokeja koskevan seurannan, analysoinnin ja hälytysten tuottamisen tarkoituksena on luoda etenkin kriittisten kohteiden ja tietojen kohdalla mahdollisimman reaaliaikainen havainnointikyvykkyys, jotta tarvittaviin toimenpiteisiin on mahdollista ryhtyä nopeasti.

Lokien analysoinnissa ja ymmärtämisessä on tärkeää ymmärtää jokaisen lokia tuottavan järjestelmän ja sitä käyttävän käyttäjän normaali, tyypillinen toiminta. Tavoitteena on saada käsitys normaaleista lokitietoja muodostavista tapahtumista, jotta saadaan vertailukohta epätavallisille lokitapahtumille. Ajan kuluessa opitaan tunnistamaan järjestelmän normaalitoiminta ja kyetään erottamaan siitä eroavat epätavalliset lokitapahtumat.

Lokitietojen seurannan ja analysoinnin osalta on määritetty:

- kuinka usein ja mitä lokitietoja seurataan ja analysoidaan
- kenellä on pääsy lokitietoihin ja millaista lokitietoa tuotetaan itse lokitietojen käsittelystä
- miten toimitaan, kun havaitaan lokitiedoissa reagointia vaativia poikkeamia (lokienhallinnan liityntä esimerkiksi poikkeamienhallintaprosessiin)
- miten lokitietoja ja niiden pohjalta muodostettua informaatiota hyödynnetään toiminnassa sekä sen johtamisessa ja kehittämisessä tai tietojärjestelmien ylläpidossa
- miten ennaltaehkäistään luottamuksellisen tiedon, kuten salasanojen, arkaluonteisen henkilötiedon ja viestinnän sisällön paljastumista sekä kuinka käsitellään tällaisen tiedon tahaton paljastuminen.

Koska laajoja ympäristöjä koskevien lokitietojen manuaalinen analysointi on työlästä ja jopa mahdotonta, pyritään lokienhallintaan liittyvillä työkaluilla ja ratkaisuilla automatisoimaan lokitietojen seurantaa ja analysointia. Normaalikäytöstä poikkeavat tapahtumat pyritään automaattisesti tunnistamaan ja suodattamaan, jotta niihin voidaan reagoida hälytyksin ja manuaalisin toimin sekä automaattisin tietoturvakontrollein. Suodattaminen mahdollistaa myös manuaalisen analysoinnin priorisointia, kun siinä voidaan keskittyä tehokkaasti ja helposti ainoastaan merkitykselliseksi tunnistettuihin lokitapahtumiin.

**Laki julkisen hallinnon tiedonhallinnasta**
**Suosituskortti**
**Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät ja ylläpitäjät
**Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua

| 17 § Lokitietojen kerääminen | versio 0.95/1.11.2019 |
|---|---|

Tehokkaamman lokitietojen seurannan, analysoinnin ja suojauksen toteuttamiseksi hyödynnetään keskitettyjä lokienhallintaratkaisuja, jotka tukevat poikkeamien tunnistamista ja suodattamista normaaleista tapahtumista, tietoturvaloukkausten havaitsemista, epäselvän ja harhaanjohtavan datan hallintaa sekä tehokasta reagoimista. Käytetyt ratkaisut hyödyntävät lokitietojen ja tapahtumien analysoinnissa valmiiksi määritettyjä sääntöjä ja raja-arvoja sekä normaalikäytöstä ja ihmisten ja tietojärjestelmien toiminnasta muodostettuja käyttäytymismalleja verran näitä tapahtumista ja toimista muodostettuihin lokitietoihin tunnistaen anomalioita eli poikkeamia ja epätavallisuutta normaalista.

Hälytysten muodostamiseksi ja analysoinnin priorisoimiseksi on määritetty malli lokitietojen suodattamiselle ja priorisoinnille, joka huomioi muun muassa:

- lokimerkinnän tyypin, kuten tapahtumaa kuvaavan luokan
- lokimerkinnän harvinaisuuden tai poikkeuksellisuuden (täysin uuden tyyppinen lokimerkintä)
- lokimerkinnän kohteen (esim. kriittinen tietojärjestelmä tai tieto)
- tapahtuman poikkeuksellisuuden (esim. tapahtuman normaalista poikkeava ajankohta tai ilmaantumistiheys)

Jotta lokitietojen seuraamiseksi ja analysoimiseksi sekä poikkeaviin tilanteisiin reagoimiseksi on tarvittava kyvykkyys, organisaatio on varannut riittävät ja osaavat resurssit toimenpiteiden suorittamiseksi. Lokien seurantaan ja analysointiin ja poikkeamienhallintaan voidaan käyttää sekä sisäisiä että palveluna hankittuja resursseja. Lokien seuranta ja analysointi on liitetty organisaation muihin prosesseihin, kuten poikkeamienhallintaprosessiin, joka käynnistyy esimerkiksi tietoturvapoikkeaman havaitsemisesta lokienhallinnan avulla.

**Lokitietojen luovuttaminen**
Lokitietoja voidaan luovuttaa muun muassa muille viranomaisille tietoturvapoikkeamien ja rikosten selvittelyä varten. Lokitietojen tiedonsaantioikeudet ratkaistaan julkisuuslain tai erityislakien perusteella. Erityislainsäädäntö voi tietyillä toimialoilla mahdollistaa henkilöille muun muassa lokipyyntöjen ja tarkastuspyyntöjen tekemisen, jolloin organisaatiolla on oltava prosessi ja toimintamallit tällaisiin pyyntöihin reagoimiseksi.

Organisaation on varmistettava lokitietojen kerääminen ja saatavuus sopimuksellisesti, jos tietojärjestelmä on toteutettu ostopalveluna ja palvelutoimittaja huolehtii lokitietojen keräämisestä ja hallinnoinnista. Tällöin luovutusoikeus perustuu sopimukseen ja luovutuksen osapuolten asemaan lokitietojen tosiasiallisena omistajana.

**Lokitietojen suojaaminen**
Lokeihin muodostuu erilaisia tietoja, joilla on omat suojaustarpeensa. Tämä tietojen ja lokeihin kohdistuvien riskien muodostama suojaustarve sekä lokeihin kohdistuvat ulkoiset vaatimukset on tunnistettu lokien asianmukaisen suojaamisen toteuttamiseksi koko lokienhallintaympäristöön. Jotta lokitietoihin voidaan luottaa, on niiden eheys eli muuttumattomuus kyettävä turvaamaan estäen lokitietojen oikeudettoman muuttamisen tai tuhoamisen niiden sälytyksen ja siirron aikana. Lisäksi lokien luottamuksellisuus varmistetaan muun muassa asianmukaisen pääsynhallinnan avulla. Lokitietojen saatavuuden turvaamiseksi varmistetaan muun muassa niiden säilyminen ja käytettävyys koko lokien säilytysajan.

**Laki julkisen hallinnon tiedonhallinnasta**
**Suosituskortti**
**Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät ja ylläpitäjät
**Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua

| 17 § Lokitietojen kerääminen | versio 0.95/1.11.2019 |
|---|---|

Lokit muodostavat yhden tietojärjestelmään kuuluvan tietoaineiston ja niiden turvallisuus on suositeltavaa varmistaa vähintään samalla tavoin kuin järjestelmän muiden tietoaineistojen turvallisuus. Tämä voidaan toteuttaa esimerkiksi siirtämällä lokitiedot toiseen, suojattuun järjestelmään, joka on eriytetty lokitiedot luoneesta tietojärjestelmästä. Hyvin toteutettu lokiympäristö onkin muista tietojärjestelmistä erillään oleva tietokanta, jonka eheys on varmistettu estäen lokien muokkauksen.

Lokien käsittelyn suunnittelussa ja toteuttamisessa on varmistettu, että lokien kirjoitusoikeus on vain sillä prosessilla, joka lokia tuottaa. Muilla prosesseilla, tietojärjestelmän käyttäjillä ja ylläpitäjillä ei tule ole kirjoitusoikeuksia lokitietoihin. Lokien käyttöoikeudet poikkeavat tietojärjestelmän varsinaisen tietosisällön käyttöoikeuksista. Lokeja koskevat käyttöoikeudet ja pääsynhallinta on määritelty ja sen noudattamista valvotaan samalla periaatteella kuin järjestelmän muun tietosisällön käyttöoikeuksia. Lokitiedon kohdalla on huomioitava erityisesti vaaralliset työyhdistelmät niin, että järjestelmän käyttäjällä tai ylläpitäjällä ei ole oikeuksia käsitellä omaa käyttölokiaan. Tyypillisesti tämä edellyttää käyttöoikeuksien rajaamista sekä hallinnollisella että teknisellä tasolla. Tämä tarkoittaa muun muassa vaarallisten työyhdistelmien tunnistamista ja määrittämistä ja näiden huomioista rooleja ja käyttöoikeuksia myöntäessä. Vaarallisten työyhdistelmien erottaminen on hyvä saada toteutettua myös teknisesti pakottamalla rajaten vaarallisia työyhdistelmiä muodostavien roolien myöntäminen samalle käyttäjälle.

EU yleinen tietosuoja-asetus ja tietosuojalaki

Lakihenkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018

[1]VAHTI lokiohje
https://www.kyberturvallisuuskeskus.fi/fi/nain-keraat-ja-kaytat-lokitietoja

Viestintäviraston ohje 04/2016, Lokien keräys ja käyttö

**Sanasto**

Kyberturvallisuussanasto
https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf
Kokonaisturvallisuussanasto
http://www.tsk.fi/tiedostot/pdf/Kokonaisturvallisuuden_sanasto_2.pdf
Valtionhallinnon tietoturvasanasto
https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

**Aikaleima** on tapahtumatietoon tai viestiin liitetty tieto lähetys-, saapumis- tai käsittelyajankohdasta ja mahdollisesti tapahtuman osapuolista. Aikaleimalla saadaan aikaan viestin lähettämisen tai vastaanottamisen kiistämättömyys.

**Anonymisointi** tarkoittaa henkilötietojen käsittelyä niin, että henkilöä ei enää voida tunnistaa niistä. Tiedot voidaan esimerkiksi karkeistaa yleiselle tasolle (aggregoida) tai muuttaa tilastolliseen muotoon siten, etteivät yksittäistä henkilöä koskevat tiedot ole enää tunnistettavassa muodossa.

| **Laki julkisen hallinnon tiedonhallinnasta**<br>**Suosituskortti**<br>**Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät ja ylläpitäjät<br>**Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua | |
|---|---|
| 17 § Lokitietojen kerääminen | versio<br>0.95/1.11.2019 |

Tunnistamisen täytyy estyä peruuttamattomasti ja siten, että rekisterinpitäjä tai muu ulkopuolinen taho ei voi enää hallussaan olevilla tiedoilla muuttaa tietoja takaisin tunnistettaviksi.

**Haavoittuvuudet** ovat alttiuksia turvallisuutta uhkaaville tekijöille, puutteita ja heikkouksia turvatoimissa sekä suojauksissa. **Tietoturvahaavoittuvuudet** ovat tietojärjestelmän tai sen osan heikkous, joka vaarantaa tietoturvan Haavoittuvuus voi olla seurausta ohjelmavirheestä tai siitä, että jotakin erityistapausta ei ole otettu huomioon. Haittaohjelmat hyödyntävät levitessään tietoturvahaavoittuvuuksia.

**Haittaohjelma** on ohjelma, joka tarkoituksellisesti aiheuttaa tietojärjestelmän tai laitteen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä t ai sen osassa. Haittaohjelmia ovat esimerkiksi virukset, madot ja troijalaiset sekä näiden yhdistelmät. Kiristyshaittaohjelma on haittaohjelma, joka salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta.

**Havaitseva kontrolli** pyrkii havaitsemaan suojaavan kerroksen läpi päässeen jäännösriskin aiheuttamat vaikutukset. Valvonta ei enää estä vahinkoa tapahtumasta, vaan ainoastaan saattaa sen näkyväksi.

**Häiriö** on tilanne tai tapahtuma, jonka vuoksi järjestelmä ei toimi normaalisti tai toiminnan jonkin osatekijän haitallinen vaihtelu, jonka puitteissa toiminta voi silti pääosin jatkua.

**Kontrolli** on riskien hallinnan tavoite, keino tai menetelmä, suunnitelmallinen jatkuva toiminta, kertaluonteinen tai toistuva toimenpide, jolla varaudutaan tai suojaudutaan (tieto)turvaloukkauksia tai haitallisia tapahtumia vastaan. Kontrollit ovat ehkäiseviä, havaitsevia (ilmaisevia) tai korjaavia. Suojauksella tarkoitetaan haitallisen ulkopuolisen vaikutuksen torjumista tai ennalta ehkäisyä.

**Loki** on tiedosto, johon tehdään aikajärjestyksessä merkinnät tapahtumista ja niiden aiheuttajista. Loki kerätään yleensä automaattisesti ja samaan järjestelmään liittyviä lokeja voi olla useita, esimerkiksi vikaloki, laskutusloki, turvaloki.

**Lokitieto** on tietojärjestelmästä automaattisesti kirjautuva tapahtumatieto. Lokitieto voi sisältää erilaisia tunnistamistietoja ja koskea muun muassa sitä, kuka järjestelmää on käyttänyt tai miten ja milloin järjestelmää on käytetty samoin kuin tietoa erilaisista virhetilanteista.

**Lokitietojenkäsittelyllä** tarkoitetaan lokin koko elinkaaren liittyviä toimenpiteitä lokien keräämisestä niiden säilyttämiseen ja arkistointiin sekä lokien valvonnasta ja analysoinnista niiden luovuttamiseen ja poistamiseen.

**Osapuolen todentaminen** on menetelmä tai prosessi, jolla todennetaan viestinnän osapuoli.

**Protokolla** eli **käytäntö** on yleisesti sovittu menettely kahdenvälistä yhteydenpitoa varten sekä tietoliikenteessä säännöstö, jota lähettävän ja vastaanottavan laitteen tulee noudattaa, jotta datansiirto onnistuisi tarkoitetulla tavalla. **Yhteyskäytäntö** on säännöstö, joka määrittelee datayhteydellä käytettävät yhteydenpitotavat, koodin sekä siirto-, ohjaus- ja toipumismenettelyt.

**Pääsynhallinta** käsittää ne menettelyt, joilla varmistetaan, että käyttäjät, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaisesti.

**Pääsynvalvonta** kattaa ne tiedot, toiminnot ja menettelyt, joiden avulla palvelujärjestelmän tai sen palvelulelementtien käyttö mahdollistetaan vain valtuutetuille käyttäjille.

**Salakirjoittaa** eli käyttää menetelmää tiedon esityksen muuttamiseksi sellaiseksi, että tiedon alkuperäinen sisältö on mahdollista saada selville vain samaa tai soveltuvaa käänteistä menetelmää käyttäen. Salakirjoittaminen tapahtuu salausavainta käyttäen tietyn salausalgoritmin mukaisesti.

**Salattu yhteys** on salausmenetelmällä ulkopuolisilta suojattu tietojärjestelmien välinen yhteys.

**Salaus** on tiedon, esimerkiksi toiselle henkilölle lähetettävän viestin käsittelyä niin, että ulkopuolinen ei saisi haltuunsa tietoa tai viestiä tai sen sisältämää informaatiota. Salaus tarkoittaa myös salakirjoitusta eli salakirjoittamista tai sen tulosta.

**Salausmenetelmä** on salaukseen ja salauksen purkamiseen käytettävä menetelmä.

**Suojattava kohde** on organisaation toiminnan kannalta merkityksellinen kohde, joka halutaan suojata riskien varalta. Suojattava kohde voi olla esimerkiksi tieto, tietojärjestelmä, prosessi, fyysinen tila, yksittäinen asiakirja tai työasema.

**Tapahtumaketju**, **kirjausketju** ja **jäljitysketju** tarkoittavat alkutositteiden, syöttötietojen ja tulosteiden aukotonta ketjua, jonka avulla on mahdollista jäljittää yksittäisen tiedon käsittelyvaiheet.

**Tietojärjestelmä** on ihmisistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi sekä abstrakti systeemi, jonka muodostavat tiedot ja niiden käsittelysäännöt.

**Tietoturvaloukkaus** on oikeudeton puuttuminen tietoon tai tietojärjestelmään. Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto, haittaohjelmatartunta, palvelunestohyökkäys, tietojen varastaminen ja kohdistetut haittaohjelmahyökkäykset.

**Tietoturvaloukkauksen tutkinta** tarkoittaa toimenpiteitä, jotka käynnistetään tietoturvaloukkauksen paljastuttua loukkauksen selvittämiseksi. Tietoturvaloukkauksen tutkinta voi käsittää muun muassa todistusaineiston turvaamista, forensiikkaa, haittaohjelma-analyysia, lokianalyysia tai yleisesti tietoturvaloukkauksen vaikutusten ja laajuuden selvittämistä.

**Tietoturvapoikkeama** on yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu tietoturvatapahtuma, joka vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti. Tietoturvapoikkeamat ovat haitallisia tapahtumia, tahallisia tai tahattomia tapahtumia tai olotiloja, joiden seurauksena organisaation vastuulla olevien tietojen ja palvelujen eheys, luottamuksellisuus tai tarkoituksenmukainen käytettävyystaso on tai saattaa olla vaarantunut.

| | |
|---|---|
| **Laki julkisen hallinnon tiedonhallinnasta**<br>**Suosituskortti**<br>**Kohderyhmä:** Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät ja ylläpitäjät<br>**Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua | |
| 17 § Lokitietojen kerääminen | versio<br>0.95/1.11.2019 |

**Tietoturvapoikkeaman hallintaa** ovat toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi.

**Tietoturvatapahtuma** tai **tietoturvallisuustapahtuma** on tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan. Tietoturvatapahtumia voidaan havaita esimerkiksi tunnistamalla muutoksia tai poikkeamia (engl. anomalies) datassa tai tietojärjestelmän toiminnassa. Muutoksia ja poikkeamia havaitaan pääasiassa teknisiä työkaluja hyödyntävillä seulonnoilla.

**Tietoverkkovalvonta** tai **verkkovalvonta** on toimintaa, jossa seurataan ja analysoidaan omissa tietoverkoissa tapahtuvaa tietoliikennettä. Organisaatiot voivat seurata ja analysoida oman tietoverkkonsa tietoliikennettä esimerkiksi teknisen vian tai virheen havaitsemiseksi tai tietoturvasta huolehtimiseksi.

**Tietoverkkohyökkäys** tai **verkkohyökkäys** on tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön. Tietoverkkohyökkäys voidaan tehdä esimerkiksi palvelunestohyökkäyksenä tai haittaohjelman avulla.

**Toipuminen** kuvastaa toimintakyvyn palautumista kriisin, erityistilanteen, häiriötilan tai poikkeusolojen jälkeen tai elpymistä kriisistä tai katastrofista.

**Toipumissuunnittelua** on toipumissuunnitelman laatiminen ja ylläpito. **Toipumissuunnitelma** on jatkuvuussuunnitelman tai varautumissuunnitelman osa, joka sisältää ohjeet katastrofista toipumiseen, toiminnan jatkamisesta ja paluusta normaaliin toimintaan. Määrittelee tärkeille tietojärjestelmille varajärjestelyvaatimukset, vastuut ja toimet valmiuden luomiseksi sekä antaa ohjeet toiminnasta poikkeustilanteissa. Suunnitelma ei sisällä vain vaatimuksia vaan konkreettisia sovittuja toimenpiteitä / menettelytapoja / teknisiä vararatkaisuja.