VALTIOVARAINMINISTERIÖ

Lokiohje

Valtionhallinnon tietoturvallisuuden johtoryhmä

3/2009 VAHTI

VALTIOVARAINMINISTERIÖ

Lokiohje

Valtiovarainministeriön julkaisuja

3/2009 VAHTI

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi

ISSN 1455-2566 (nid.)
ISBN 978-951-804-957-2 (nid.)
ISSN 1798-0860 (PDF)
ISSN 978-951-804-958-9 (PDF)

YMPÄRISTÖMERKKI
MILJÖMÄRKT
441 002
Painotuote

Edita Prima Oy
Helsinki 2009

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM/720/00.00.00/2009

OHJE
28.4.2009

Ministeriöille, virastoille ja laitoksille

LOKIOHJE

Valtiovarainministeriön lokiohjeen tavoitteena on parantaa ja tehostaa suunnitelmallista ja tietoturvallista lokien hallintaa ja käsittelyä ministeriöissä ja hallinnonalojen organisaatioissa. Ohje on suunnattu johdolle ja tietohallinnolle sekä henkilöstöhallinnosta, arkistotoiminnasta, tietoturvallisuudesta, tietosuojasta, laki- ja sopimusasioista vastaaville.

Lokien käsittely on oleellinen osa tietojärjestelmien ja tietoverkkojen ylläpitämistä sekä tietosuojan varmistamista ja tietoturvallisuuden valvontaa. Lokit ovat työväline järjestelmän eheyden tarkistamiseksi, häiriöiden ja väärinkäytösten havaitsemiseksi ja niiden korjaamiseksi sekä luotettavaksi tapahtumaketjun kirjaamiseksi ja tapahtumien toteamiseksi.

Ohje pyrkii sovittamaan yhteen käyttäjän ja rekisteröidyn oikeudet, organisaatioiden toiminnan tarpeet sekä hyvän tiedonhallintatavan, henkilöstöhallinnon, tietosuojan ja tietoturvallisuuden periaatteet. Ohjeeseen sisältyy lainsäädännön merkittävimmät lokeihin liittyvät vaatimukset ja käsittelyn oikeudet sekä erityyppisten lokien tarkastelu.

Jokaisen organisaation johto päättää ja vastaa riittävien organisaation toimintaan, järjestelmiin ja verkkoihin liittyvien lokien olemassa olosta, kattavuudesta, turvaamisesta sekä lokivaatimusten sisällyttämisestä toimintaan ja hankkeisiin. Organisaatioissa tulee tunnistaa lokien vaatimukset, määritellä lokien suojaustarpeet ja -tavat, laatia tarvittavat rekisteriselosteet, määritellä käsittelyn vastuut sekä auditoida lokien turvallisuus ja suojaus säännöllisesti. Kunkin organisaation tulee selvittää ja varmistua omaa toimintaansa koskevien säädösten sisällöstä ja vaatimusten toteutumisesta. Lokitietojen hallinnan on oltava suunnitelmallista ja katettava lokien koko elinkaari.

Lokien käsittelyn vaatimat laitteisto- ja henkilöresurssit sekä kustannukset on otettava huomioon osana toiminnan, järjestelmän tai hankinnan suunnittelua ja budjetointia. Lokien käsittely tulee järjestää kustannustehokkaasti siten, että lokien keräämisellä ja analysoinnilla saavutetaan sille asetetut tavoitteet ilman turhan tiedon keräämistä. Kustannusten ja riskien hallitsemiseksi järjestelmien kehityksessä ja hankinnoissa tulee alkuvaiheista lukien määritellä, mitä lokitietoja tarvitaan ja missä muodossa.

Lokien käsittelyn perustana ovat selvät roolit ja vastuut sekä ennalta määritellyt ja dokumentoidut toimintatavat lokien käsittelemiseksi. Avoimuusperiaatteen mukaisesti tietojen keräämisestä, käsittelystä ja menetelmistä tulee tiedottaa kaikkia asianomaisia tahoja.

Hallinto- ja kuntaministeri — Mari Kiviniemi

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite: Lokiohje (VAHTI 3/2009)

Esipuhe

Tämä ohje toimii ICT-lokien turvallisen käsittelyn yleisohjeena. Ohje on kirjoitettu valtionhallinnon näkökulmista, mutta se on sovellettavissa myös muissa organisaatioissa.

Ohjeessa on käsitelty erityyppisiä ICT-lokeja, lokien käsittelyn vastuita ja prosessia, järjestelmäkehityksen ja -hankinnan lokinäkökohtia sekä lokien säilytystä, keräämistä ja suojaamista. Ohjeeseen sisältyy myös tarkistuslista, lakiliite ja yhteenveto VAHTI-ohjeistuksen vaatimuksista.

Ohje on valmisteltu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn alaisuudessa ja ohjauksessa. VAHTI päätti ohjeen viimeistelytoimista ja julkaisemisesta kokouksessaan tammikuussa 2009.

Lokiohje julkaistaan VAHTIn verkkosivuilla ja painotuotteena. Ohjeen kaupallinen käyttö ja jäljentäminen ansaitsemistarkoituksessa on kielletty. Muussa hyödyntämisessä tulee tämä ohje mainita lähteenä.

Lyhyesti VAHTIsta

Valtiovarainministeriö vastaa julkishallinnon tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.

VAHTIssa käsitellään kaikki merkittävät valtionhallinnon tietoturvalinjaukset ja tietoturvatoimenpiteiden ohjausasiat. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset sekä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä.

VAHTIn toiminnalla on parannettu valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä, kansalaistoiminnassa ja kansainvälisesti. VAHTIn toiminnan tuloksena muun muassa on aikaansaatu erittäin kattava yleinen tietoturvaohjeisto (www.vm.fi/VAHTI). Valtiovarainministeriön ja VAHTIn johdolla on menestyksellisesti toteutettu useita ministeriöiden ja virastojen tietoturvayhteishankkeita. VAHTI on valmistellut, ohjannut ja toteuttanut laajan valtion tietoturvallisuuden kehitysohjelman, jossa on aikaansaatu merkittävää kehitystyötä yhteensä 26 kehityskohteessa yli 300 hankkeisiin nimetyn henkilön toimesta. VAHTI on saanut kolmena vuotena tunnustuspalkinnon esimerkillisestä toiminnasta Suomen tietoturvallisuuden parantamisessa.

VAHTIn verkkosivuilta löytyy monipuolisesti tietoa VAHTIn toiminnasta, tuloksista, suunnitelmista ja menossa olevista hankkeista sekä voimassa olevista ja valmisteilla olevista julkaisuista.

Sisältö

A Esittely

A.1 Työryhmän kokoonpano

Tämä ohje on laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän, VAHTIn alaisen ja ohjaaman lokiryhmän toimesta. Ryhmän toimintaan osallistuivat:

- Kari Santalahti, Poliisin tietoturvapäällikkö, ryhmän puheenjohtaja
- Sari Kajantie, Keskusrikospoliisi, sihteeri
- Mats Kommonen, Turun yliopisto, sihteeri
- Sami Kilkkilä, Viestintävirasto
- Reijo Aarnio, Tietosuojavaltuutettu
- Ari Mämmi, Poliisin tietohallintokeskus
- Mikko Hakuli, Puolustusvoimat
- Jussi Jääsaari, Verohallinto
- Olli Nieminen, Väestörekisterikeskus
- Kari Keskitalo, valtionvarainministeriö
- Manu Pajuluoma, Lapin yliopisto (29.2.2008 saakka)
- Juha Koivisto, Tampereen kaupunki/Tietotekniikkakeskus
- Heikki Pietilä, Poliisin ylijohto

Ohjeen laadintaan konsultteina osallistuivat KPMG:n asiantuntijat: Mika Laaksonen, Mika Iivari, Kimmo Nikulainen ja Matti Järvinen.

Ohjeen luonnos oli kommenttikierroksella helmikuussa 2008. Saadut kommentit käsiteltiin työryhmän kokouksessa 18.3.2008 ja huomioitiin ohjeen seuraavassa kommenttiversiossa. Ohjeen toinen kommenttiversio oli kommenttikierroksella huhtikuussa 2008. Saadut kommentit käsiteltiin työryhmän kokouksessa 13.6.2008. Ohjeeseen pyydettiin kommentteja myös kuudelta kaupallisia lokijärjestelmiä toimittavalta yritykseltä,joista kommentteja saatiin kahdelta.

VAHTI järjesti syksyllä 2008 ohjetta koskevan laajan lausuntokierroksen, jonka palautteen pohjalta käynnistyi ohjeen viimeistely. Lausuntoja saatiin 19 kappaletta.

VAHTI päätti ohjeen viimeistelytoimista ja julkistamisesta tammikuussa 2009.

1 Johdanto

Lokitieto on dokumentti jonkin tapahtuman toteutumisesta jonakin tiettynä hetkenä.

Loki on olemassa ennalta määriteltyä tarkoitusta varten ennalta määrätyn ajan. Lokeja ja niiden käsittelyä tarvitaan niin poikkeus- kuin normaalitilanteissakin. Normaalitilanteissa lokeja tarvitaan toiminnan häiriöttömyyden seuraamiseen ja käytön tilastointiin. Poikkeustilanteissa lokeja tarvitaan tilanteen normalisointiin sekä tapahtumien osapuolten, vaikutusten laajuuden sekä syiden selvittämiseen.

Lokien tuottama tieto edesauttaa järjestelmän ylläpitäjien ja käyttäjien oikeusturvan toteutumista, järjestelmien ja verkon toiminnan optimointia sekä erilaisten tietoturva- ja muiden poikkeamien selvittämistä.

Tietoturvallisuuden ja tietosuojan kannalta erittäin suuren merkityksensä vuoksi lokitietojen suojaamisen, seurannan ja säilyttämisen tulee olla suunnitelmallista. Hyvään käytäntöön kuuluu lokipolitiikan määrittäminen. Lokipolitiikassa otetaan kantaa lokien säilytystapaan ja aikaan, lokien käsittelyyn liittyviin rooleihin sekä lokien käsittelyyn ja käsittelyn tarpeeseen.

Oikein toteutettuna lokit ja luotettava lokiympäristö mahdollistaa aukottoman tapahtumaketjun[1] kirjaamisen ja tapahtumien todentamisen.

1.1 Lokitietojen määritelmä

Loki dokumentoi tapahtumia, jotka ovat tapahtuneet organisaation järjestelmissä, verkoissa tai muussa ympäristössä ja toiminnassa. Lokitiedot voivat olla automaattisten järjestelmien keräämiä merkintöjä tai manuaalisesti kerättäviä lokitietoja, kuten vierailijaloki.

Riippumatta lokin keräämistavasta tai lokin muodosta, tulee lokien käsittelyssä huomioida samat asiat. Kun tässä ohjeessa puhutaan lokitiedoista, tarkoitetaan lokeja niiden kaikissa muodoissa, ellei erikseen toisin mainita.

[1] Audit trail.

Lokit voidaan luokitella ja tyypitellä monilla eri tavoilla. Tässä ohjeessa lokit on luokiteltu seuraavasti:

- ylläpitoloki
- käyttöloki
- muutosloki
- virheloki.

1.2 Lokien käsittelyn määritelmä

Termi ”lokien käsittely” kattaa lokin koko elinkaareen liittyvät toimenpiteet:

- lokien kerääminen
- lokien analysointi
- lokien säilyttäminen
- lokien luovuttaminen ja
- lokien poistaminen tai arkistointi.

Jokapäiväisessä työssä ja puhekielessä lokien käsittely on erotettu lokien keräämisestä ja säilytyksestä. Tässä suppeammassa merkityksessä lokien käsittely tarkoittaa jo olemassa olevan lokitiedon analysointia. Tässä ohjeessa lokien käsittelyllä tarkoitetaan kaikkia edellä listattuja asioita ja ohjeessa käsitellään lokien koko elinkaari.

Koska kaikkia tietojärjestelmien lokeihin kirjautuneita tapahtumia ei käytännössä voida manuaalisesti tarkastella lokitietojen suuresta määrästä johtuen, on valikoitava olennaisimmat kohteet, tapahtumat, raportointitapa ja tarkastuksen suorittaja. Teknisillä lokien analysointiin tarkoitetuilla työvälineillä on mahdollista tarkastaa kaikki lokiin kirjatut tapahtumat ja niiden yksityiskohdat ja raportoida niistä lokien analysointia suorittavalle henkilölle merkityksselliset asiat.

Lokien käsittelyssä ihminen tekee päätökset automatisoidun tai manuaalisen analysoinnin perusteella.

1.3 Lokien käsittelyn tavoitteet

Lokien käsittely on oleellinen osa tietojärjestelmien ja tietoverkkojen ylläpitämistä ja tietoturvallisuuden valvontaa. Lokit ovat välttämätön työväline järjestelmän eheyden tarkistamiseksi, häiriöiden havaitsemiseksi ja niiden korjaamiseksi sekä luotettavan tapahtumaketjun muodostamiseksi.

Lokitietojen avulla voidaan jäljittää järjestelmän tapahtumia (kuka, mitä, milloin), virheitä, väärinkäyttö- ja tietomurtotilanteita ja niiden yrityksiä.

Lokeja voidaan myös käyttää todistusaineistona rikosprosessissa.

Lokitietojen käsittelyllä pyritään saavuttamaan ja varmistamaan tapahtuman:

Osapuolet. Kuka tai ketkä toimijat liittyvät johonkin tiettyyn tapahtumaan. Lokista riippuen osapuolet voivat olla verkkolaitteita, joiden identiteettiä ei millään tavoin ole varmennettu, mutta tapahtuman osapuolena voi olla myös tunnistettu ja todennettu toimija.

Kiistämättömyys. Tavoitteena on, ettei mikään tapahtuman osapuoli voisi kiistää osallisuuttaan tapahtumaan. Esimerkkinä kiistämättömyydestä ovat pankin järjestelmiin syntyvät lokitiedot koskien käyttäjän verkkopankissa suorittamia maksutapahtumia. Näiden tavoitteiden saavuttamisessa ehdottomana edellytyksenä on tapahtuman suorittajan tunnistaminen henkilö-, järjestelmä- tai prosessitasolla. Tämän tavoitteen saavuttamiseksi tulee lokiin kirjata myös sallitut ja onnistuneet tapahtumat, ei ainoastaan ei-sallittuja tapahtumia.

Kulku. Tapahtumien kulku voidaan dokumentoida keräämällä lokijäljet kronologiseen järjestykseen. Tällöin tietty tapahtuma tai tapahtumasarja saadaan jäljitettyä. Tähän liittyvät tapahtumien lokiin kirjaaminen, kuten esimerkiksi onnistuneet ja epäonnistuneet yhteydenmuodostukset palomuurin pääsynvalvontalokeissa sekä käyttäjän onnistuneet ja epäonnistuneet kirjautumiset sähköisiin palveluihin. Jotta kronologinen kirjaus olisi mahdollista, tulee järjestelmien kellojen olla oikeassa ajassa.

Tunkeutumisten ja poikkeamien havaitseminen. Poikkeavien tai ei-sallittujen tapahtumien tunnistaminen, joka mahdollistaa niihin reagoimisen. Esimerkkinä mainittakoon poikkeavaan kellonaikaan tapahtuva toiminta, valtuuttamaton käyttö, resurssien väärinkäyttö, murtautumisyritykset, epäonnistuneet kirjautumiset tai murtautumista edeltävä tiedustelu.

Suorituskykyongelmien havaitseminen. Lokitietojen avulla voidaan varmistaa järjestelmän, ohjelmiston tai palvelun asianmukainen toiminta ja käytettävyys. Lokitiedot sisältävät tietoja esimerkiksi resurssien käytöstä, syntyneistä tai uhkaavista virhetilanteista sekä epäonnistuneista toimenpiteistä. Tähän liittyvät järjestelmän vika- ja ongelmatilanteiden lokiin kirjaaminen, kuten esimerkiksi palvelimen kovalevyn vikaantumisesta kertova lokimerkintä käyttöjärjestelmän järjestelmälokissa.

Käyttäjien ja rekisteröityjen oikeusturvan varmistaminen. Lokitietojen avulla voidaan luotettavasti osoittaa, kuka on tai ei ole tehnyt jotain tiettyä asiaa tietojärjestelmässä tai muussa ympäristössä, josta lokia pidetään.

Erityyppisten lokien kerääminen ja seuranta auttavat siten järjestelmien ylläpitäjiä ja muita vastuuhenkilöitä suorittamaan seuraavia tehtäviä:

- poikkeamatilanteen havainnointi
- poikkeamatilanteen selvitys
- toipuminen ja ylläpitoprosessin kehittäminen

- jatkuva kuormituksen seuranta
- todisteiden keruu
- tapahtumien kiistämättömyyden varmistaminen
- käyttäjien, rekisteröityjen ja ylläpitäjien oikeusturvasta huolehtiminen.

Asianmukaisella lokien keräämisellä ja tehtävien eriyttämisellä parannetaan järjestelmien ja niiden komponenttien ylläpitoon ja käyttöön osallistuvien henkilöiden ja rekisteröityjen oikeusturvaa.

1.4 Ohjeen tarkoitus, kohderyhmä

Tämä ohje on tarkoitettu avuksi lokijärjestelyiden suunnitteluun sekä tietojärjestelmiin liittyvien lokien keräämiseen ja analysointiin.

Sek ohjeen että lokihankkeen tarkoituksena on kuvata kokonaisvaltaisesti ja käytännöllisesti toteuttamista lokien käsittelyssä.

Ohje pyrkii sovittamaan yhteen käyttäjän ja rekisteröidyn oikeudet, hyvän tiedonhallintatavan, hyvän henkilöstöhallinnon ja tietoturvallisuuden toteuttamisen periaatteet.

Ohjeessa huomioidaan erityyppiset lokit, esimerkiksi käyttöjärjestelmä-, tietoliikenne- ja sovelluslokit sekä tietoaineistojen käsittelyvaiheista syntyneet lokit. Ohje on välineriippumaton yleisohje, mutta esimerkkeinä ohjeessa kuvattujen periaatteiden sovittamisesta käytetään yleisimpiä palveluita, kuten sähköpostia ja www-palvelua.

Ohjeen on tarkoitus olla hyödyllinen niin tietojärjestelmien ja palveluiden suunnittelijoille, tilaajille, käyttäjille kuin omistajille. Järjestelmien kehityksen tai hankinnan yhteydessä tulee määritellä myös mitä lokitietoja järjestelmästä tarvitaan ja missä muodossa tiedot halutaan. Toisaalta järjestelmän omistajan tulee varmistua, että lokeihin ei kerätä turhaa tietoa. Ylimääräinen tieto vaikeuttaa lokien analysointia, eikä henkilöistä ja heidän toimistaan muutenkaan saa kerätä turhaa tietoa.

Ohjeen peruskivenä on kuvaus siitä, mitä loki ja lokitiedot ovat. Ohje kuvaa hyvän tiedonhallintatavan asettamat lokienkäsittelyvaatimukset ymmärrettävässä muodossa ja myös palvelun käyttäjän tai rekisteröidyn näkökulmasta. Ohjeen perusteella laaditut kuvaukset kertovat käyttäjälle, mihin tarkoitukseen ja millä tavalla häneen liittyviä lokitietoja käsitellään.

Ohjeen kohderyhmänä ovat henkilöt, jotka:

- osallistuvat tietojärjestelmien suunnitteluun, määrittelyyn, kehittämiseen ja hankintaan
- osallistuvat tietojärjestelmien ja -verkkojen ylläpitoon
- vastaavat arkistoista ja arkistonmuodostamisesta

- vastaavat organisaation tietoturvallisuudesta
- vastaavat laki-, sopimus- ja yksityisyyden suojaan liittyvistä asioista
- haluavat saada lisätietoja lokeista sekä lokien tallentamiseen ja analysointiin liittyvistä teknisistä ja hallinnollisista tekijöistä.

Ohje antaa myös valtionhallinnon ulkopuolella toimiville, tietoturvallisuuden ja erityisesti lokien käsittelyn kehittämisestä kiinnostuneille henkilöille mahdollisuuden kehittää oman organisaationsa lokien käsittelyn menetelmiä ja toimintatapoja.

Ohjetta ei ole laadittu siten, että eri luvut olisi erityisesti suunnattu jollekin tietylle kohderyhmälle. Sen sijaan ohje on pyritty laatimaan siten, että asiat esitetään siinä järjestyksessä kun ne tyypillisesti tulisi tehdä. Poikkeuksen muodostaa luku 5, joka on erityisen sopiva hankinnoista, ulkoistuksesta tai sovelluskehityksestä vastaaville henkilöille.

Ohjeen luvussa 1 esitetään lokeihin ja niiden käsittelyyn liittyvät määritelmät, lokien käsittelyn tavoitteet sekä ohjeen sisältö, tavoitteet ja kohderyhmä.

Ohjeen luvussa 2 käsitellään lokien käsittelyn tarvetta, vaatimuksia ja rajoituksia. Ohjeen lainsäädäntöliitteessä käsitellään eri lakien vaatimuksia yksityiskohtaisemmin. Ohjeen VAHTI-liitteessä käsitellään tarkemmin aiempien VAHTI-ohjeiden lokien käsittelylle asettamia suosituksia.

Ohjeen luvussa 3 käsitellään eri tyyppisiä lokeja ja näihin lokityyppeihin liittyviä erityskysymyksiä.

Ohjeen luvussa 4 käydään läpi lokien käsittelyyn liittyvät vastuut ja velvollisuudet sekä lokien käsittelyn prosessi.

Ohjeen luvussa 5 käsitellään hankintoihin, ulkoistukseen ja järjestelmäkehitykseen liittyviä erityiskysymyksiä.

Ohjeen luvussa 6 käsitellään lokien säilyttämistä, keräämistä ja suojaamista.

2 Tarve, vaatimukset ja rajoitteet lokien käsittelylle

2.1 Lokien käsittelyn perusperiaatteet

Lokien käsittely vaatii laitteisto- ja henkilöresursseja. Täten lokien käsittelystä aiheutuu kustannuksia, jotka on huomioitava osana toiminnan tai hankinnan suunnittelua ja budjetointia. Lokin käsittelyssä ja sen suunnittelussa huomioidaan tarkoitussidonnaisuus, tarvevaatimus ja suunnitelmallisuus. Lokien käsittely tulee optimoida siten, että lokien keräämisellä ja analysoinnilla saavutetaan sille asetetut tavoitteet ilman, että tuhlataan resursseja turhan tiedon keräämiseen ja analysointiin. Vaikka lokien käsittelystä aiheutuukin kustannuksia, on se välttämätöntä järjestelmien toiminnan, rekisteröityjen ja käyttäjien tietosuojan sekä tietoturvallisuuden varmistamiseksi ja usein myös ulkoisten vaatimusten täyttämiseksi. Huomioimalla lokivaatimukset toiminnan tai järjestelmän suunnitteluvaiheessa saadaan niistä aiheutuvat kustannukset minimoitua.

Lokien käsittelyn 4 tärkeintä perusperiaatetta ovat:

- Käsittelyn tulee perustua määritettyyn tarpeeseen.
- Käsittelyn tulee tapahtua määriteltyjen järjestelmien ja toimintatapojen mukaisesti.
- Lokien analysoinnin tulosten perusteella tehtävät toimet tulee olla ennakolta määritelty.
- Rekisteröityjen, järjestelmän käyttäjien sekä ylläpitäjien tietosuoja ja oikeusturva tulee huomioida kaikessa lokien käsittelyssä.

2.2 Hyvän tiedonhallinta- ja ylläpitotavan vaatimukset lokien käsittelylle

Hyvä tiedonhallintatapa[2] edellyttää, että käsiteltävän tiedon saatavuus, suoja, eheys ja laatu turvataan.

Kunkin tavoitteen saavuttaminen edellyttää, että organisaation tietojärjestelmät tuottavat lokia järjestelmän tapahtumista. Hyvään tiedonhallintatapaan liittyy järjestelmien toiminnan seuraaminen, ei-toivottujen tilanteiden ennakointi, tapahtuneisiin tilanteisiin reagointi sekä toiminnan ja järjestelmän kehittäminen tehtyjen havaintojen perusteella. Organisaation tulee varmistaa, että myös itse lokitiedot ovat turvassa asiattomalta pääsyltä sekä vahingossa tai luvattomasti tapahtuvalta hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta käsittelyltä.

Hyvä ylläpitotapa edellyttää, että hyvän tiedonhallintatavan vaatimat toimenpiteet toteutetaan tavalla, joka takaa mahdollisimman hyvin eri osapuolten oikeusturvan.

Järjestelmän omistajan ja ylläpitäjän tulee tietää, mitä tietojärjestelmä normaalitilanteessa tekee tai mitä se ei tee, mutta järjestelmän seuranta tulee toteuttaa siten, ettei kättäjien oikeuksia – kuten viestinnän luottamuksellisuutta – rikota. Toisaalta ylläpitotapahtumien lokien kirjaus tulee toteuttaa kiistämättömästi siten, etteivät ylläpitäjät pääse poistamaan suorittamiensa tapahtumien lokimerkintöjä.

2.3 Lainsäädännön vaatimukset lokien käsittelylle

Lainsäädäntö asettaa useita erilaisia vaatimuksia lokien käsittelylle. Ohjeessa on käsitelty merkittävimmät lainsäädännön lokien käsittelylle asettamat vaatimukset ja lokien käsittelyyn liittyvät oikeudet. Kunkin hallinnonalan tulee selvittää ja varmistua omaan toimintaansa liittyvien erityislakien sisällöstä, vaatimuksista ja vaatimusten toteutumisesta.

Seuraavat lait ottavat kantaa ja asettavat vaatimuksia tai antavat oikeuksia, jotka liittyvät lokitietojen käsittelyyn:

- Henkilötietolaki (523/1999)
- Julkisuuslaki (621/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004) (”työelämän tietosuojalaki”)
- Sähköisen viestinnän tietosuojalaki (526/2004)
- Eräitä muita lokien käsittelyn säädöksiä

[2] Julkisuuslain 18 §.

- Julkisuusasetus
- Laki sananvapauden käyttämisestä joukkoviestinnässä
- Laki tietoyhteiskunnan palveluiden tarjoamisesta
- Arkistolaki sekä asetus arkistolaitoksesta.

Lainsäädäntö asettaa rajoituksia lokitiedon käsittelyyn erityisesti silloin, kun lokeihin tallentuu joko tunnistamistietoja[3] tai henkilötietoja[4] . Kaikki lokit eivät välttämättä sisällä näitä tietoja. Lokien käsittelyn suunnittelussa onkin ensiarvoisen tärkeää tunnistaa erilaisiin lokeihin tallentuvat tiedot. Lokitiedoista muodostuu henkilörekisteri silloin, jos ne sisältävät henkilöä koskevaa tunnistettavaa tietoa. Tällöin tulee huomioida kaikki henkilörekisteriä koskevat vaatimukset tai vaihtoehtoisesti harkita uudelleen henkilötietojen tallentamisen tarve.

Suunnitteluvelvoite ja käyttötarkoitussidonnaisuus, ovat hyvän tietohallintotavan keskeisiä elementtejä. Ennen järjestelmän ja siihen liittyvien lokijärjestelyiden toteuttamista tulee toteutus, käyttötapa sekä kerättävien ja käsiteltävien tietojen tarpeellisuus selvittää ja kuvata.

Lainsäädäntö asettaa myös suojausvelvoitteita tietojen, erityisesti henkilötietojen, suojelemiseksi. Tämä tarkoittaa sitä, että tietojen suojaustarpeet tulee tunnistaa ja huomioida toiminnan, hankinnan tai tieto- ja lokijärjestelmän suunnitteluvaiheessa.

Jos jonkin lokin tarkoituksena on tuottaa tietoa, jota työantaja voi käyttää työntekijöiden valvontaan, lokin kerääminen tulee käsitellä työelämän tietosuojalain mukaisesti yhteistoimintamenettelyssä. Yhteistoimintamenettelyä säätelevat lait yhteistoiminnasta yrityksissä, valtion virastoissa ja laitoksissa sekä kunnissa.

Muistilista lokien lainmukaisesta käsittelystä:

- Tunnista miksi ja mihin tarkoitukseen kutakin lokia käsitellään.
- Arvioi tallennettavien tietojen tarpeellisuus.
- Tunnista lokeihin tallentuvat tietotyypit, erityisesti henkilötiedot ja tunnistamistiedot.
- Tunnista tallentuvien tietotyyppien suojaustarpeet.
- Varmista, että tietojen suojaustarve toteutuu järjestelmän toteutuksessa ja tietojen käsittelyssä.
- Huomioi tarve YT-menettelylle, mikäli kyseessä on tekninen valvonta.
- Huomioi YT-menettelyn lisäksi muu käyttäjien, rekisteröityjen tai muiden tahojen informointi[5] .

[3] Tunnistamistieto pitää sisällään tietoa viestinnän osapuolista.

[4] Henkilötietoa on kaikki henkilön tunnistamista edesauttava tieto.

[5] Esim. käyttökoulutuksessa, järjestelmädokumentaatiossa tai henkilöstöoppaassa.

- Huomioi henkilörekisteriin liittyvät vaatimukset[6], jos lokeista muodostuu henkilörekisteri.
- Suunnittele ja dokumentoi säilytystarve ja varmista sen toteutuminen käytännössä.
- Huomioi edellä mainitut asiat myös hankinnoissa ja ulkoistuksissa.

Lokien analysointiin liittyen usein esitetään kysymyksiä siitä, saako lokeja käyttää johonkin tiettyyn tarkoitukseen. Lähtökohtaisesti oikeampi lähestymistapa on miettiä, miksi lokia on kerätty ja millaisista käyttötavoista henkilöstölle tai muille tahoille on YT-menettelyn avulla tai muutoin kerrottu. Jos aiottu käyttötapa poikkeaa lokin suunnitellusta ja analysoinnin kohteena oleville tahoille informoidusta tavasta, ei toimiin tule ryhtyä.

Lainsäädäntöä ja sen vaatimuksia on tarkemmin käsitelty ohjeen liitteessä.

2.4 Aikaisempien VAHTI-ohjeiden asettamat lokien käsittelyn suositukset

Lukuisissa VAHTI-ohjeissa käsitellään lokien käsittelyyn liittyviä asioita sekä asetetaan lokien käsittelyyn liittyviä vaatimuksia ja suosituksia. Nämä vaatimukset kohdistuvat niin organisaation omaan kuin ulkoisten toimittajien toimintaan sekä järjestelmiin ja prosesseihin. Kunkin VAHTI-ohjeen aiheesta ja kattamasta alueesta riippuen vaatimuksia asetetaan kehitteillä oleville järjestelmille, olemassa oleville järjestelmille ja käytöstä poistettaville järjestelmille. Usein vaatimukset kohdistuvat järjestelmien lisäksi myös toimintatapoihin ja prosesseihin, sekä myös toiminnan tarkastamiseen ja auditointiin. Vaatimuksia löytyy siten järjestelmäkehityksen ja tiedon elinkaaren kaikkiin vaiheisiin.

Tässä ohjeessa esitetään yhteenveto aikaisempien VAHTI-ohjeiden lokien käsittelylle asettamista vaatimuksista. Vaatimukset ovat tässä selvyyden vuoksi jaoteltu teknisiin, hallinnollisiin ja toiminnan tarkastamiseen liittyviin vaatimuksiin. Kunkin VAHTI-ohjeen asettamat vaatimukset on tarkemmin käsitelty liitteessä.

[6] Lokilla voi olla ja usein onkin itsenäinen käyttötarkoitus suhteessa kulloinkin kyseessä olevaan ydintoiminnon henkilötietojen käsittelyn tarkoitukseen, jolloin lokista/lokijärjestelmästä on laadittava itsenäinen rekisteriseloste.

2.4.1 Tekniset suositukset

Tietojärjestelmien ja ympäristön turvallisuutta tukevien järjestelmien tulee kerätä lokitietoja. Yleensä lokeja kerätään tietojärjestelmissä, mutta lokit voivat olla myös manuaalisesti kerättäviä merkintöjä kuten konesalin kävijäloki.

Lokien pitää pystyä esittämään riittävät tiedot valvottavista tapahtumista. Järjestelmien rakentamisen yhteydessä määritellään mitä tarkoitetaan riittävillä tiedoilla. Tyypillisesti tiedosta tulee käydä ilmi ainakin kyseessä oleva tapahtuma, tapahtuman onnistuminen tai epäonnistuminen, tapahtuman luotettavasti yksilöivä suorittaja ja ajankohta.

Lokien kerääminen tulee järjestää teknisesti niin, että lokit ovat luotettavia sekä riittäviä ja että niitä ei esimerkiksi tietomurtojen yhteydessä ole mahdollista muuttaa.

Lokitiedot tulee suojata käyttövaltuuksin ja lokijärjestelmä on rakennettava niin, että se hälyttää[7] asiattomista lokien käsittely-yrityksistä.

Kaikkien lokiympäristöön kuuluvien laitteiden, kuten lokien lähde- ja keräysjärjestelmien kellojen tulee olla samassa ajassa, jotta tapahtumien tapahtumajärjestys on mahdollista selvittää. Käytännössä tämä tarkoittaa keskitetyn aikapalvelimen (NTP[8]) käyttöä.

2.4.2 Hallinnolliset suositukset

Lokeihin liittyvät vaatimukset tulee määritellä ja edellyttää toteutettavaksi järjestelmäkehityksen, hankinnan tai ulkoistuksen yhteydessä.

Toimittajilla tulee olla kuvaus omalla vastuullaan olevien järjestelmien tai toimintojen lokien keräämiseen, tallennukseen ja analysointiin liittyvistä asioita. Sopimuksen teon yhteydessä tulee määrittää myös lokien käsittelyyn liittyvät vaatimukset sekä lokien omistaja ja omistajan mahdollisuudet saada lokitietoja käyttöönsä tarpeen vaatiessa.

Lokeihin tallennettavien tietojen tyyppi tulee tunnistaa. Vain tarpeellisia tietoja tulee kerätä. Samalla tulee kuitenkin varmistaa, että kerätään riittävästi tietoja, jotta lokien analysointi yleensä olisi mahdollista. Henkilötietojen suojan piirissä olevat tiedot tulee tunnistaa ja suojata sekä käsitellä niiden edellyttämällä tavalla. Silloin kun loki muodostaa henkilörekisterin, tulee lokista laatia rekisteriseloste. Tyypillisesti on järkevämpää laatia seloste koko järjestelmästä ja huomioida selosteessa järjestelmän tuottamat lokitiedot.

---

[7] Tyypillisesti tämä järjestetään tiedosto-oikeuksilla ja näiden oikeuksien ylitysyritysten kirjaamisella erilliseen lokiin ja tämän lokin automaattisella tai manuaalisella seurannalla.

[8] NTP (engl. Network Time Protocol) on UDP-pohjainen protokolla täsmällisen aikatiedon välittämiseen tietokoneiden välillä. Protokolla on suunniteltu ottamaan huomioon verkon vaihtuvat viiveet.

Lokitietojen tarvittava säilytysaika ja paikka tulee määritellä. Tämän jälkeen tulee varmistaa, että lokitiedot säilyvät ja ovat käytettävissä tämän määritellyn ajan. Säilytysajan umpeuduttua vanhentuneet lokitiedot tulee poistaa.

Lokeja kerätään lähes aina valvonta- tai selvitystarkoituksia varten. Täten lokitietoja on säännönmukaisesti seurattava ja analysoitava. Lokien seuraamiseksi ja havaintoihin reagoimiseksi on määritettävä tarpeelliset prosessit sekä tekniset valmiudet. Tämä tulee toteuttaa niin omien kuin ostettujen palveluiden tai järjestelmien osalta.

Aikaisemmissa VAHTI-ohjeissa todetaan, ettei lokeja saa käyttää profiiliyhteenvetojen tekemiseen. Laajemmin ilmaistuna lokeja tulee käyttää vain siihen tarkoitukseen, jota varten niitä kerätään[9] ja mihin niitä on työntekijöille tai muille tahoille kerrottu käytettävän.

Tarkastuksen yhteydessä tulee varmistaa, että lokien kerääminen on teknisesti riittävällä ja luotettavalla tavalla toteutettu, lokeihin liittyvät vaatimukset on tunnistettu ja määritelty, ja että lokeja seurataan ja käytetään suunnitellusti

2.5 Kustannushyötyajattelu

Lokien luotettavaan keräämiseen, tallentamiseen ja tehokkaaseen analysointiin tarvittavat järjestelmät ovat investointeja, joiden tulee olla samalla tavalla perusteltuja kuin muidenkin investointien. Kaikki lokien käsittelyyn liittyvät tekijät eivät ole helposti suoraan rahalla perusteltavissa, vaan lokeja on kerättävä ja analysoitava myös erilaisten vaatimusten täyttämiseksi. Tällöinkin vaatimukset tulee luonnollisesti pyrkiä täyttämään kustannustehokkaalla tavalla. Tunnettu tosiasia tietojärjestelmäprojekteissakin on se, että etukäteen määrittely on huomattavasti kustannustehokkaampaa kuin jälkikäteen toteuttaminen.

Lokihankkeissakin vain osa kustannuksista syntyy itse lokijärjestelmän tai sovelluksen lokiominaisuuksien toteuttamisesta. Yleensä merkittävämpi osa kustannuksista syntyy järjestelmän käytön aikaisista kustannuksista ja erityisesti henkilökustannuksista. Vaikka lokien analysointia on mahdollista helpottaa ja osin automatisoida käyttämällä teknisiä ratkaisuita, tulee lokien analysointi kuitenkin viimekädessä tehdä ihmisen toimesta.

Lokien analysoinnilla voidaan myös saavuttaa kustannussäästöjä, muun muassa seuraamalla järjestelmän kuormitusta ja mitoittamalla käytössä olevat ja kustannuksia aiheuttavat resurssit optimaalisesti. Tällä tavoin sekä vältetään ylikapasiteettia, että voidaan samalla ennakoida kuormituksen kasvu siten, että pullonkaulojen muodostuminen voidaan välttää.

[9] Käyttötarkoitussidonnaisuus.

Lokien käsittelyyn liittyvät vaatimukset tulee tunnistaa hankintojen yhteydessä ennen tarjousten pyytämistä, sillä muutoin saaduissa tarjouksissa välttämättä ei ole riittävästi huomioitu lokeihin liittyviä vaatimuksia ja kustannuksia. Tällöin projektin kustannukset ja aikataulu tyypillisesti ylittyvät, eikä lopputulos välttämättä kaikilta osin vastaa vaatimuksia.

Lokien vaatimusten mukainen suojaaminen aiheuttaa myös kustannuksia. Tarvittavalle suojaukselle vaatimuksia asettavat lainsäädäntö, hyvä tiedonkäsittelytapa sekä mahdollisesti myös sopimukset. Suojausvaatimukset tulee tunnistaa ajoissa, jotta suojaukset voidaan toteuttaa oikeassa laajuudessa ja osana projektia, jolloin myös suojaustoimenpiteiden toteuttaminen on kustannustehokasta.

2.6 Muut vaatimukset lokien käsittelylle

2.6.1 Luottokorttiyhtiöiden PCI-DSS vaatimukset

PCI-DSS[10] on luottokorttiyhtiöiden[11] kehittämä kansainvälinen maksukorttialan tietoturvastandardi, jonka tavoitteena on turvata kortinhaltijoiden tilitiedot ja nostaa kaikkien luottokorttitietoja käsittelevien tahojen tietoturvataso mahdollisimman korkeaksi. Standardin noudattaminen on pakollista kaikille luottokorttitapahtumia vastaanottaville, välittäville tai tallentaville tahoille. Standardi sisältää 12 pääkohtaa, jotka jakautuvat lukuisiin yksittäisiin tietoturvavaatimuksiin. Standardi sisältää vaatimuksia myös lokien käsittelyyn ja sen järjestämiseen korttitietoja käsittelevissä organisaatioissa. Standardia hallinnoi riippumaton, korttijärjestöjen perustama PCI Security Standards Council[12] -toimielin, jonka kotisivuilta on saatavilla standardin uusin versio, yksityiskohtaiset auditointiohjeet sekä muuta standardiin ja sen noudattamiseen liittyvää materiaalia.

PCI-DSS standardin kohdassa 10, ”Seuraa ja valvo kaikkea verkkoresurssien ja kortinhaltijoiden tietojen käyttöä”, on esitetty yhteensä 25 eri vaatimusta lokien käsittelylle. Kohdan kontrollitavoitteessa lokeista ja lokijärjestelmien tarpeellisuudesta mainitaan seuraavasti:

”Lokijärjestelmät ja mahdollisuus seurata käyttäjien toimia ovat kriittisiä. Lokien olemassaolo kaikissa järjestelmissä mahdollistaa valvonnan ja analysoinnin, jos jotain väärinkäyttöä tapahtuu. Väärinkäytön syy on erittäin hankalaa selvittää ilman lokeja järjestelmien käytöstä.”

---

[10] Payment Card Industry (PCI) Data Security Standard, versio 1.1, julkaistu syyskuussa 2006.

[11] Kehittämisessä ovat olleet mukana Visa International, MasterCard Worldwide, American Express, JCB ja Discover Financial Services.

[12] https://www.pcisecuritystandards.org/.

Standardin mukaan organisaatiolla tulee olla prosessi lokien keräämiseen, jotta kaikkien järjestelmäkomponenttien käyttö (erityisesti järjestelmänvalvojan oikeuksilla suoritettu käyttö) voidaan yhdistää yksittäiseen käyttäjään. Standardi määrittää seuraavat toimet, joiden tapahtumaketju (audit trail) pitää pystyä selvittämään kaikkien järjestelmäkomponenttien osalta:

- kaikki yksittäisten käyttäjien pääsy kortinhaltijoiden tietoihin
- kaikki ylläpitäjien tekemät toimet
- pääsy kaikkiin kirjausketjuihin (audit trails)
- epäonnistuneet kirjautumisyritykset
- tunnistus- ja todennusmekanismien käyttö
- auditointilokien käyttöönotto
- järjestelmätason objektien luominen ja poistaminen.

Lisäksi standardi määrittää, mitä kaikkien edellä mainittujen toimien osalta tulee vähintään kirjoittaa lokiin:

- käyttäjän tunnistus
- tapahtuman tyyppi
- päiväys ja kellonaika
- merkintä onnistumisesta tai epäonnistumisesta
- tapahtuman luominen
- järjestelmäkomponentin tai resurssin nimi, johon kyseinen tapahtuma liittyy.

Lisäksi standardi velvoittaa synkronisoimaan kaikkien kriittisten järjestelmien kellot ja turvaamaan kirjausketjut muuttamiselta. Kirjausketjuihin pääsy pitää rajoittaa niihin henkilöihin, jotka tarvitsevat sitä työtehtäviensä hoitamiseksi. Lokitiedot tulee suojata valtuuttamattomilta muutoksilta ja ne tulisi varmistaa keskitetylle lokipalvelimelle tai muulle medialle, jossa niitä ei voida muuttaa. Organisaation sisäverkossa sijaitsevalle keskitetylle lokipalvelimelle tulee kopioida myös langattomien verkkojen lokitiedot. Standardin mukaan organisaation tulee lisäksi käyttää lokitiedostojen eheyden ja muuttumisen valvontaan erillistä tarkkailuohjelmistoa[13] , jotta lokitietoja ei voida muuttaa ilman, että siitä syntyy hälytys.

Standardissa määritellään myös vaatimukset lokien säännölliselle läpikäynnille. Standardin mukaan lokeja tulee tarkastella vähintään päivittäin, ja näiden lokikatselmusten tulee sisältää sellaisten palvelinten lokit, jotka suorittavat tärkeitä tietoturvallisuuteen liittyviä toimintoja. Standardissa mainitaan esimerkkeinä IDS-palveluita ja käyttövaltuuksien tarkastukseen liittyviä palveluita, kuten RADIUS, tuottavat palvelimet. Lokien läpikäyntiin suositellaan käytet-

[13] Esim. Tripwire, AIDE.

täväksi analysointia helpottavia työkaluja. Tapahtumien kulun selvittämiseen (audit trail) liittyvät lokitiedot vaaditaan säilytettävän vähintään vuoden ajan, josta vähintään 3 kuukauden lokitiedot on oltava saatavilla jatkuvasti.

Lisäksi viittauksia lokien käsittelyyn on myös muissa standardin kohdissa, kuten kohdassa 1.4, jossa määritellään, että lokeihin ja lokitietoja sisältäviin korttitietojärjestelmiin ei saa olla suoraa pääsyä ulkoisista verkoista. Standardin kohdassa 3.4 vaaditaan, että korttitietojen tulee olla typistettyjä tai lukukelvottomia myös lokeissa. Kohdassa 5.2 vaaditaan, että myös virustorjuntajärjestelmien tulee pystyä tuottamaan lokitietoja. Kohdassa 9.4 asetetaan vaatimus vierailijalokista korttitietoja sisältävien palvelinten säilytystilaan. Vierailijalokia tulee säilyttää vähintään kolmen kuukauden ajan. Standardin kohdassa 12.2 vaaditaan että organisaatio kehittää ja ottaa käyttöön päivittäiset operatiiviset tietoturvatoimet, joista mainitaan esimerkkinä säännöllinen päivittäinen lokien läpikäynti. Standardin liitteessä vaatimuksessa A.1 vaaditaan, että myös organisaation käyttämien palveluntarjoajien tulee huolehtia PCI-DSS standardin vaatimuksen 10 mukaisesta lokituksesta ja kirjausketjujen tuottamisesta.

2.6.2 Tietoturvastandardien mukaisuus

Myös tietoturvallisuuden hallintaan laaditut ISO 27001[14] ja ISO 27002[15] -standardit sisältävät vaatimuksia lokien hallintaan ja käsittelyyn. Lokien käsittelyyn liittyvät vaatimukset on pääasiassa esitetty standardin luvussa 10.10, monitorointi. Standardin alkusanoissa mainitaan, että kuvatut kontrollit ja niiden toteuttaminen organisaatiossa tulee aina suhteuttaa paikalliseen lainsäädäntöön, jotta asiakkaiden tai työntekijöiden yksityisyyden suojaa ei rikota.

Standardin lokien käsittelyyn liittyvät ohjeet ja vaatimukset kuuluvat lukuun 10, joka antaa vaatimuksia erilaisten tietoturvallisuuden operatiivisten toimien toteuttamiseen. Standardi edellyttää, että tietyille toimille on olemassa dokumentoidut toimintaohjeet, ja tapahtumien kulun selvittämiseen tarvittavien kirjausketjujen ja järjestelmien lokitietojen hallinta on yksi tarkoitetuista operatiivisista toimista.

Kohdan 10.10, monitorointi, tavoitteeksi standardissa määritellään ”valtuudettomien tiedon prosessointitoimien havaitseminen”. Standardin mukaan järjestelmiä tulee valvoa ja tietoturvallisuuteen liittyvät tapahtumat tulee kirjata ylös. Operointilokeja ja virhelokeja tulee kerätä, jotta varmistetaan, että tiedon prosessoinnissa ja järjestelmissä mahdollisesti tapahtuvat virheet havaitaan. Järjestelmien valvonta ja lokien kerääminen tulee standardin mukaan hoitaa myös kaikkien lakien ja asetusten mukaisesti.

---

[14] ISO/IEC 27001 on tietoturvallisuuden hallintajärjestelmän (ISMS) vaatimusmäärittely, jota vastaan tietoturvallisuuden sertifiointi toteutetaan.

[15] I SO/IEC 27002 on tietoturvallisuuden hallintajärjestelmän (ISMS) rakentamisen hyvät käytännöt esittävä standardi.

Standardeissa määritellään ja kuvataan kuusi eri valvontaan ja lokien keräämiseen liittyvää kontrollia, sekä niiden toteuttamiseen liittyvät ohjeet:

- Lokeja tulee kerätä ja säilyttää.
- Lokeja ja järjestelmien käyttöä tulee seurata ja valvoa säännöllisesti.
- Lokeja ja lokien säilytysjärjestelmiä tulee suojata valtuudettomalta käytöltä.
- Järjestelmänvalvojien toimia järjestelmissä tulee valvoa ja niistä tulee kerätä lokia.
- Vikatilanteita tulee seurata ja analysoida.
- Kaikkien järjestelmien kellot tulee synkronisoida, ja niiden tulee olla oikeassa.

Lokien keräämisestä standardissa määritellään tarkasti, mitä tietoja lokeihin tulee kerätä. Lokien seurannasta ja valvonnasta määritellään, mitä kannattaa valvoa ja kuinka usein valvonta tulisi suorittaa. Käytännössä ISO27001 määrittelee lokien osalta kontrolloitavat osa-alueet ja ISO27002 antaa ohjeet näiden kontrollien toteuttamiseen.

Lisäksi standardin muissa kohdissa on lokeihin liittyviä mainintoja, kuten muutoshallintaan liittyvissä kontrolleissa, joissa mainitaan, että muutosten yhteydessä tulee kerätä lokia itse muutoksesta ja siihen liittyvistä asioista. Verkon turvallisuuteen liittyvissä kontrolleissa mainitaan, että verkon turvallisuuteen liittyvistä tapahtumista on kerättävä lokeja ja niitä tulee valvoa. Median käsittelyyn liittyvissä kontrolleissa mainitaan, että tuhottaessa arkaluonteisia tietoja tulee kerätä lokia tapahtumien kulun selvittämisen varmistamiseksi. Standardin kohdassa 15.1.3 kirjoitetaan organisaation tärkeiden tietojen suojaamisesta, ja siellä mainitaan mm. erilaisten lokien säilyttämisestä ja suojaamisesta häviämiseltä, tuhoamiselta ja vääristelyltä lain, määräysten, sopimuksien ja liiketoiminnan vaatimuksien toteuttamiseksi.

COBIT:issa[16] vaatimuksia lokeille ja niiden keräämiselle on sen sijaan vähemmän. Kohdassa DS5.5, tietoturvallisuuden testaus, valvonta ja monitorointi, mainitaan, että lokien keräämis- ja valvontatoiminto auttaa organisaatiota havaitsemaan ja tarvittaessa estämään epänormaalit toimet, joihin tulisi puuttua. Toisaalla kohdassa DS8.2 mainitaan että ongelmien ja muutosten hallintaan tulee luoda järjestelmä, jolla kaikkia ongelmia, tapahtumia ja muutoksia voidaan jälkikäteen seurata. Kohdassa DS9.2 laajennetaan muutostenhallinta koskemaan myös konfiguraation hallintaa.

[16] Control Objectives for Information and related Technology.

3 Lokit ja lokityypit

Lokitiedostojen tulkinta edellyttää usein syvällistä tietämystä kyseessä olevan tietoteknisen ympäristön arkkitehtuurista ja järjestelmätoteutuksesta. Tässä luvussa käsitellään erityyppisiä lokitiedostoja, jotta ohjeen lukija saa kattavan käsityksen siitä, millaisia lokeja on olemassa ja mistä lokitietoja tyypillisesti syntyy. Lokit voidaan jakaa ja luokitella usealla tavalla. Ohjeessa käytetään neljä luokkaa sisältävää lokitietojen luokittelua:

- ylläpitoloki
- käyttöloki
- muutosloki
- virheloki.

Käytännössä kuitenkin monet lokit voivat tietosisällöstä riippuen kuulua moniin edellä mainittuihin luokkiin, eikä erilaisia lokeja voida tyhjentävästi sijoittaa yhteen ainoaan luokkaan.

Lokeja tuottavat tyypillisesti käyttöjärjestelmien varusohjelmistot, sovellukset, tietokannat ja verkkolaitteet. Lokeja tuottavan järjestelmän tai sovelluksen lisäksi lokit voidaan jakaa niiden tyypin, semanttisen sisällön tai käyttötarkoituksen mukaan. Järjestelmälokien[17] ensisijainen tavoite on informoida toimintahäiriöistä ja -virheistä. Haltijalokin[18] tarkoituksena on osoittaa jonkin asian, esimerkiksi ip-osoitteen, haltija tietyllä ajanhetkellä. Pääsynvalvontalokien[19] tehtävänä on auttaa järjestelmän käytön ja turvallisuuden valvonnassa.

Lokin käyttötarkoituksesta riippuu, onko se osa varsinaista järjestelmää ja henkilörekisteriä, vai erillinen rekisteri. Silloin kun lokilla on itsenäinen käyttötarkoitus suhteessa kulloinkin kyseessä olevaan ydintoiminnon henkilötietojen käsittelyyn, on myös lokista laadittava henkilötietolain tarkoittama rekisteriseloste. Kaikki lokit eivät ole henkilörekistereitä. Aina loki ei muodosta ollenkaan henkilörekisteriä, jolloin myöskään rekisteriselosteen tarvetta ei ole.

---

[17] Järjestelmälokin tyypistä ja sisällöstä riippuen järjestelmäloki on tyypillisesti virhe tai käyttöloki.

[18] Haltijaloki ilmaisee jonkin tunnisteen haltijan ja on siten käyttöloki.

[19] Pääsynvalvontaloki ilmaisee onnistuneet tai epäonnistuneet yritykset käyttää järjestelmän suojattuja resursseja ja on siten käyttöloki. Pääsynvalvontaloki voitaisiin luokitella myös virhelokiksi, koska se ilmaisee virheelliset yritykset käyttää suojattuja resursseja.

Jäljitettävyys- ja puuttumiskynnysten kannalta on tarkoituksenmukaista ylläpitää edellä mainittuja lokityyppejä, joiden tiedot voivat teknisesti sijaita yhdessä lokissa, useassa erillisessä lokissa tai mieluiten yhdessä lokien keräämiseen omistetussa järjestelmässä.

Ylläpitoloki sisältää tiedot:

- käyttöoikeuksien muutoksista, poistoista ja lisäyksistä
- rekistereiden käyttöön liittyvien virhetilanteiden hallinnasta
- järjestelmään tehdyistä muutoksista.

Käyttöloki sisältää tiedot:

- sisään- ja uloskirjautumisista käyttäjä-, ryhmä- ja sovellustietotasoilla
- epäonnistuneista kirjauksista
- käyttöoikeuksien vaihdosta erityisesti normaalikäyttäjän oikeuksista etuoikeutettuihin
- tietokannan lukutapahtumista ja kyselytiedoista hakuehtoineen
- tulostuksesta ja tallennuksesta.

Muutoslokin tulee sisältää tiedot:

- järjestelmien tietosisällön muutoksista: poistoista ja lisäyksistä
- järjestelmäparametrien ja asetustiedostojen muutoksista.

Virhelokin tulee sisältää tiedot:

- seurattavassa järjestelmässä tai tapahtumassa havaituista virheistä
- rekisterissä havaituista virheistä ja epäjatkuvuuksista.

3.1.1 Viestinnän loki

Viestinnän loki sisältää tietoja viestintätapahtumista. Lokien ensisijainen tarkoitus on viestintäjärjestelmän vikatilanteiden selvittäminen, mutta viestinnän lokeja voidaan käyttää myös tietoturvapoikkeamatilanteiden hallintaan tai jonkin viestintätapahtuman näyttämiseen toteen.

Esimerkkejä viestinnän lokeista ovat sähköpostiloki ja keskustelujärjestelmän loki. Sähköpostin välitysjärjestelmät kirjaavat lokiin tyypillisesti osapuolten sähköpostiosoitteet, lähettäjän tai välittävän järjestelmän IP-osoitteen, kellonajan, viestin yksikäsitteisen tunnisteen, tilastotietoa toimituksesta, sekä toimituksen tilatiedon tarkennuksineen. Usein esimerkiksi sähköpostijärjestel-

män lokia käytetään sen selvittämiseen, onko viesti, joka ei ole mennyt perille, lähtenyt oman organisaation järjestelmästä.

Huomioitavaa lokin käsittelyssä:

> Lokit sisältävät viestinnän tunnistamistietoja sekä henkilötietoja, joten niiden käsittelyssä on huomioitava sähköisen viestinnän tietosuojalain, henkilötietolain sekä työelämän tietosuojalain velvoitteet.

3.1.2 Haltijaloki

Haltijaloki kertoo, kenen hallussa jokin verkkotunniste, tyypillisesti IP- tai MAC-osoite[20], on ollut tiettynä ajanhetkenä. Haltijaloki voi perustua todennuslokiin, jossa ip-numero liitetään tiettyyn henkilökohtaiseen tunnisteeseen kuten käyttäjätunnukseen, tai DHCP-lokiin[21], jossa IP-numero annetaan tietyn MAC-osoitteen tai liittymätunnisteen käyttöön.

Lokien ensisijaisena tarkoituksena on varmistaa se, että tarvittaessa voidaan selvittää, minkä liittymän käytössä tietty iIP-osoite on ollut nimettynä hetkenä, jotta voidaan selvittää tapahtumien kulku ja osapuolet. Haltijalokia voidaan käyttää rajallisesti myös sen selvittämiseen, onko organisaation verkossa sinne kuulumattomia laitteita. Tämä voidaan saavuttaa vertaamalla lokissa olevia laitteiden MAC-osoitteita laitekirjanpidossa oleviin osoitteisiin. On erittäin tärkeää, että organisaatiolla on ajantasainen laitekirjanpito ja tieto omista liittymistään sekä omien laitteidensa MAC-osoitteista. Koska MAC-osoitteet ovat laite- ja osittain myös valmistajakohtaisia[22] , voidaan lokin avulla erottaa toisistaan myös vaikkapa valmistajan X WLAN-tukiasemat valmistajan Y WLAN-tukiasemista. Kun tiedetään, että käytössä pitäisi olla vain valmistajan X tukiasemia, kaikki muut tukiasemat on yksinkertaista tunnistaa ylimääräisiksi.

---

[20] Media Access Control, verkkolaitteen yksilöivä tunniste. Myös tämä tunniste on väärennettävissä.

[21] Dynamic Host Configuration Protocol. Käytetään tyypillisesti vaihtuvien IP-osoitteiden jakamiseen työasemille.

[22] MAC-osoitteen ensimmäinen puolisko (6 ensimmäistä merkkiä) osoittaa laitteet, yleensä verkkokortin, valmistajan.

Esimerkkejä tarpeellisista haltijalokeista ovat muun muassa:

- DHCP-loki silloin, kun käyttäjien työasemilla tai muilla verkkolaitteilla ei ole käytössä staattista osoitetta.
- Proxy-lokit silloin, kun organisaatiosta liikennöidään esimerkiksi HTTP-protokollalla yhden proxyn kautta. Proxy-lokin avulla on selvitettävissä[23], mistä organisaation sisäisestä IP-osoitteesta tietty yhteys todella tuli.
- Mahdollisten yhteiskäyttöisten työasemien kirjautumisloki, joka voi toimia myös muutoin kuin sähköisesti.

Huomioitavaa lokin käsittelyssä:

> Lokit sisältävät henkilö- tai tunnistamistietoja. Näiden tietojen käsittely on sallittua vain lain sallimissa puitteissa ja tavoilla.
>
> Viestinnän osapuolten oikeusturvan ja lokien hyödynnettävyyden kannalta on keskeistä, että lokia tuottavat laitteet ovat aikapalvelun avulla tarkalleen oikeassa ajassa ja että ylläpitäjä tietää mille aikavyöhykkeelle loki kirjataan. Tämä pätee laajemminkin kaikkiin lokityyppeihin.

Lokit sisältävät henkilö- tai tunnistamistietoja. Näiden tietojen käsittely on sallittua vain lain sallimissa puitteissa ja tavoilla.

Viestinnän osapuolten oikeusturvan ja lokien hyödynnettävyyden kannalta on keskeistä, että lokia tuottavat laitteet ovat aikapalvelun avulla tarkalleen oikeassa ajassa ja että ylläpitäjä tietää mille aikavyöhykkeelle loki kirjataan. Tämä pätee laajemminkin kaikkiin lokityyppeihin.

3.1.3 Sovellustason pääsyvalvontalokit

Sovellustason pääsynvalvontalokit kertovat, mistä (IP-osoitteesta) on muodostettu onnistuneesti yhteys johonkin suojattuun kohteeseen ja millä käyttäjätunnisteella kohteeseen on kirjauduttu. Yleensä sovellukset pitävät kirjaa myös epäonnistuneista yhteysyrityksistä sekä yrityksistä ylittää omat käyttövaltuudet.

Lokien tarkoituksena on mahdollistaa ehjä kirjausketju yhdistämällä käyttöoikeudet ja lähdeosoite tietoturvapoikkeamien selvittämiseksi. Lokien toissijainen tarkoitus on mahdollistaa järjestelmään kohdistuvien sanakirjahyökkäysyritysten seuranta.

Esimerkkejä tarpeellisista pääsyvalvontalokeista ovat muun muassa shell

[23] Mikäli perusteet selvittämiselle on olemassa.

access-lokit (sshd[24], tcp wrapper[25]), sovellusten, kuten taloushallinnon järjestelmien, tilausjärjestelmien, toiminnanohjausjärjestelmien ja muiden vastaavien lokit.

Huomioitavaa lokin käsittelyssä:

> Lokit saattavat sisältää henkilö- tai tunnistamistietoja. Näiden tietojen käsittely on sallittua vain lain sallimissa puitteissa ja tavoilla.
>
> Jos lokia tuottavassa järjestelmässä käsitellään henkilötietoja, turvaluokiteltua tai muuten erityisesti suojattavaa aineistoa, pääsyvalvontalokeista on syytä ohjata automaattisesti kopio myös erilliseen lokipalvelimeen, johon mahdollinen murtautuja ei pääse samalla käsiksi.

3.1.4 Tarjottujen, julkisten verkkopalveluiden sovelluslokit

Tarjottujen verkkopalveluiden sovelluslokit eivät periaatteessa eroa edellisessä kappaleessa esitetyistä sovellustason lokeista. Ero tässä on se, että edellisessä kappaleessa käsiteltiin organisaation sisäisten sovellusten lokeja. Sisäisillä sovelluksilla pitäisi olla rajattu ja tiedossa oleva käyttäjäjoukko, kun taas näillä verkkopalveluiden sovelluksilla ei välttämättä ole.

Verkkopalveluiden sovelluslokista ilmenee, mistä verkko-osoitteesta palveluun on otettu milläkin hetkellä yhteys. Lokista ilmenee myös mahdollinen kirjautumiseen liittyvä käyttäjätunnus sekä tunnistautumisen onnistuminen tai epäonnistuminen silloin, kun palvelu vaatii käyttäjän tunnistusta.

Verkkopalveluiden lokien ensisijaisena tarkoituksena on yhdistää palvelutapahtuma ja lähdeosoite vikatilanteiden tai tietoturvapoikkeamien selvittämiseksi. Lokien perusteella voidaan myös tuottaa tilastollista aineistoa palvelun käytöstä tai jonkin sivuston osan tai muun vastaavan suosiosta sekä siitä, mistä sivustolle tullaan. Monissa tapauksissa on myös tärkeää pystyä lokien avulla toteennäyttämään jonkun tiedon luovuttaminen tai transaktion[26] toteutuminen.

---

[24] Secure Shell, salattu etäkäyttöprotokolla.

[25] Tcp wrapper on pääsynvalvontatoteutus, jonka avulla on laitekohtaisesti mahdollista määritellä, mistä jokin tietty yhteys on sallittua muodostaa.

[26] Kuten viranomaisen dokumentin luovuttaminen tai tiedoksi saattaminen.

Esimerkkejä tarpeellisista pääsyvalvonta- ja verkkopalveluiden sovelluslokeista ovat muun muassa WWW-lokit. WWW-palveluissa tuotetaan tyypillisesti seuraavia lokeja:

- Tapahtumaloki tai käyttöloki, joka luo WWW-palvelimelta haetusta tiedosta lokimerkinnän.
- Virheloki[27] , johon kirjataan sovelluksen virheet selityksineen.
- Selaintyyppiloki, joka kerää tietoja asiakasohjelmistoista eli selaimen tyypeistä sekä versioista.
- Viittausloki, johon kerätään HTTP-yhteyteen liittyviä tietoja ja ne URL-tiedot, mistä asiakasohjelmisto tuli organisaation sivuille.

Tyypillisesti tapahtuma-, käyttö-, selaintyyppi-, ja viittausloki ovat samassa lokitiedostossa ja niiden kerääminen on www-palvelinohjelmiston vastuulla.

Huomioitavaa lokin käsittelyssä:

> Lokit saattavat sisältää henkilö- tai tunnistamistietoja. Näiden tietojen käsittely on sallittua vain lain sallimissa puitteissa ja tavoilla.

3.1.5 Muut käyttöjärjestelmä- ja sovelluslokit

Käyttöjärjestelmät keräävät aina lokia monista järjestelmässä tapahtuvista asioista, ellei tätä ominaisuutta erikseen ole poistettu käytöstä. Myös käyttöjärjestelmän apuohjelmat ja muut sovellukset voivat toteutuksesta riippuen kerätä lokia sovelluksen toiminnasta ja virheistä.

Käyttöjärjestelmän tuottamat lokit vaihtelevat järjestelmästä toiseen, mutta tyypillisesti lokeja on samassakin järjestelmässä useita erilaisia. Esimerkiksi Windows-järjestelmä tuottaa sovellus-, suojaus- ja järjestelmälokeja (application, security ja system lokit). Sovelluslokit sisältävät tietoa muun muassa käynnistyneistä ohjelmista, virheistä käynnistyksessä, ohjelman käynnistysajankohdan sekä tiedon käynnistäjästä. Suojausloki pitää kirjaa määritellyistä onnistuneista ja epäonnistuneista tapahtumista ja niiden toteuttajasta ja kellonajasta. Järjestelmäloki puolestaan sisältää tietoa eräistä järjestelmän sisäisistä tapahtumista, niihin liittyvistä prosesseista ja virheistä. Windows-järjestelmässä sovelluksen lokin tuottaminen on yleensä sovelluksen itsensä vastuulla. Jos jokin sovellus ei erikseen tuota lokia, lokitietoa ei ole saatavilla.

---

[27] Tämä on tyylillisesti sovelluksen vastuulla. Myös www-palvelinohjelmisto voi kerätä virhelokia, mutta tämän virhelokin merkitys on vähäisempi kuin sovelluksen virhelokin.

UNIX-järjestelmät tuottavat tyypillisesti /var/log tai /var/adm-hakemistoihin runsaasti tietoa järjestelmän sisäisistä tapahtumista sekä käyttäjän tekemistä toimista. Kaikki lokit eivät välttämättä sisällä kaikissa ympäristöissä ja toteutuksissa tarpeellisia tietoja. Lokin sisältö ja tarpeellisuus tulee varmistaa tapauskohtaisesti.

Lokin käyttötarkoitus riippuu siitä, mistä lokista on kyse. Tyypilliset käyttötarkoitukset ovat järjestelmän käytön ja oikean toiminnan valvonta, mahdollisten tulevien tai piilevien vikatilanteiden paikallistaminen ja järjestelmän turvallisuuden valvonta sekä tapahtumaketjujen todentaminen (audit trail).

Käyttöjärjestelmät tarjoavat runsaasti mahdollisuuksia säätää ja määritellä, mitä lokeihin kirjoitetaan, kauan lokeja säilytetään ja mitä lokeille tehdään jonkun määrätyn tiedostokoon täyttyessä. Oletusasetukset eivät monesti ole tarkoituksenmukaisia, joten käyttöjärjestelmien lokiasetuksia on syytä säätää järjestelmäkehityksen yhteydessä ja dokumentoida lokimääritykset.

Huomioitavaa lokien käsittelyssä:

Nämä lokit eivät aina sisällä henkilö- tai tunnistamistietoja.

Käyttöjärjestelmät tarjoavat paljon mahdollisuuksia aktivoida tiettyjä lokeja sekä määritellä, mitä lokiin kirjataan. Esimerkiksi kirjataanko tietystä tapahtumasta mitään, kirjataanko tapahtuman onnistuminen tai epäonnistuminen. Näiden parametrien tarpeiden mukainen määrittely on tärkeää. Lisäksi on oleellista määritellä lokitiedostoille riittävä koko ja lokien kierrätysrutiinit, erityisesti jos lokeja ei siirretä keskitettyyn lokijärjestelmään, jossa riittävä levytila on helpompi varmistaa.

Erillisten sovellusten ja erityisesti räätälöityjen sovellusten lokit voivat olla ongelmallisia siirrettäviä keskitettyyn lokijärjestelmään. Usein sovellukset voivat kirjoittaa erillisiä lokeja ympäriinsä levyjärjestelmää ja hakemistorakennetta sekä käyttävät ei-standardeja tiedosto- tai tekstimuotoja lokien tallentamiseen. Hankintojen yhteydessä tulee varmistaa, että lokit saadaan järjestelmästä talteen oikeassa muodossa ja siirrettyä tarvittaessa keskitettyyn lokijärjestelmään.

Tietokannan varmistusloki sisältää kaikkia tietokantaan tallennettavia tietoja, joten sen tietosisältö on sama kuin ao. tietojärjestelmän ja sen käyttötarkoitus on niin suoraan sidoksissa itse kannan käyttötarkoitukseen, että siitä ei yleensä katsota tarpeelliseksi tehdä erillistä rekisteriselostetta.

3.1.6 Verkkotason pääsyvalvonta- ja yhteyslokit

Verkon aktiivilaitteet, kuten reitittimet ja palomuurit, keräävät lokeja niiden kautta kulkevista yhteyksistä. Verkkotason lokit kertovat tyypillisesti mistä osoitteesta on mennyt liikennettä mihin osoitteeseen. Korkeamman protokollatason lokista näkyy myös mihin tietoliikenneportteihin[28] liikennöinti on kohdistunut.

Murrettujen palvelinten levyiltä löytyviä lokeja tunkeutuja voi muuttaa, mikäli niitä ei ole siirretty suojaan keskitettyyn lokijärjestelmään tai kertakirjoitteiselle medialle. Sen sijaan verkkolaitteiden lokit ovat yleensä tunkeutujan ulottumattomissa, ellei tunkeilija ole päässyt murtautumaan itse verkkolaitteille. Myös verkkolaitteiden lokitiedot on suositeltavaa siirtää mahdollisuuksien mukaan keskitettyyn lokijärjestelmään, jolloin myös ne ovat paremmassa turvassa erilaisia hyökkäyksiä vastaan. Palomuuri- ja reititinlokeista selviää mahdollisten hyökkäysten kulkureitit kaikkein luotettavimmin, mutta nämä lokit eivät puolestaan kerro, mitä murretussa palvelimessa on tapahtunut tai että palvelin yleensäkin on murrettu.

Verkkotason pääsynvalvonta- ja yhteyslokien tarkoitus on vikatilanteiden selvittäminen, mutta niitä voidaan käyttää myös tietoturvapoikkeamien dokumentointiin ja selvittämiseen. Monissa tapauksissa on perusteltua kerätä verkkotason pääsynvalvontalokitietoja myös sallituista, ei pelkästään estetyistä yhteyksistä.

Esimerkkejä tarpeellisista verkkotason pääsynvalvonta ja yhteyslokeista ovat muun muassa reititinloki, palomuuriloki ja reititinten tuottama flow-data[29].

Huomioitavaa lokien käsittelyssä:

> Salassapidettävää aineistoa sisältävän palvelimen suojana olevan palomuurin tulee kirjata onnistuneet yhteydet, ei pelkästään epäonnistuneita yhteyksiä. Palomuurien oletusasetuksissa korostetaan tyypillisesti liikaa epäonnistuneita yhteyksiä.
>
> Myös verkkolaitteiden lokit on mahdollista ja suositeltavaa siirtää suojaan keskitetylle lokipalvelimelle.
>
> Lokit sisältävät tunnistamistietoja.

---

[28] Yleensä TCP tai UDP portti. Yleensä tietyt palvelut ovat määrätyssä portissa, kuten salaamaton www-palvelu portissa 80/TCP tai SSH portissa 22/TCP. Sovellusten ei kuitenkaan ole pakko käyttää määritettyjä standardiportteja, vaan ne voivat olla myös järjestelmän rakentajan määräämässä muussa portissa.

[29] Esimerkki flow-datasta on Ciscon NetFlow, joka on avoin, mutta tekijänoikeuksin suojattu protokolla. Siitä ollaan kehittämässä IETF:n standardia; Internet Protocol Flow Information eXport (IPFIX). Tyypillisesti NetFlow data sisältää tiedot versionumerosta, sekvenssinumerosta, SNMP liittymätiedot, aikatiedot verkkoliikenteen kestosta, siirretyn datan määrästä, OSI tason 3 otsikkotiedoista, lähde ja kohde IP osoitteista, lähde- ja kohdeporttiosoitteista, käytetystä IP protokollasta sekä OSI-tason 3 reititystiedoista.

3.1.7 Transaktiolokit

Transaktiolokiin kirjataan tietokantatapahtumia, kuten kirjoitus-, muutos-, poisto- ja lukuoperaatioita. Lokien varsinaisena tarkoituksena on ylläpitää järjestelmän yhtenäisyyttä ja käytännössä transaktioloki on toiminnallinen ja erottamaton osa itse tietokantaa. Lokeja voidaan kuitenkin käyttää myös sen selvittämiseksi, kuka teki jotain tietokantaan, esimerkiksi muutti tai luki[30] tietyn solun arvoa. Tietomurtotapauksissa tietokannat ovat yleensä murron perimmäinen syy ja kohde, sillä juuri tietokannassa säilytetään niitä tietoja, joilla on taloudellista tai muuta arvoa. Siksi tietokannat tulee suojata erityisen hyvin ja niiden käyttöä valvoa tehokkaasti.

Yleisesti transaktiolokilla tarkoitetaan tietokantojen yhteydessä tietokannan hallintajärjestelmän keräämää toimintohistoriaa, joilla pyritään varmistamaan nk. ACID-periaatteen eli tiedon oikeellisuuden säilymisperiaatteet:

- Atomisuus (Atomicity). Jokainen operaatio pitää suorittaa loppuun asti tai peruuttaa kokonaisuudessaan.
- Oikeellisuus (Consistency). Jokaisen tietokantatapahtuman jäljiltä tietokannan tulee olla oikeellisessa ja yhtenäisessä tilassa.
- Eristys (Isolation). Tietokantatapahtumat eivät saa vaikuttaa toisiinsa ja keskeneräinen suoritus ei saa näkyä muille tapahtumille.
- Kestävyys (Durability). Onnistuneiden tietokannan päivitysten pitää säilyä mahdollisen tietokannan virhetilanteen jälkeen.

Fyysisesti transaktioloki on tiedosto tietokantatapahtumista, jotka on tehty tietokantaan (esim. edellisen täysvarmistuksen jälkeen) ja sitä säilytetään erillään tietokannasta. Virhetilanteissa transaktiolokia voidaan käyttää palauttamaan tietokanta virhetilannetta edeltäneeseen tilaan. Tällöin tietokannan hallintajärjestelmä vertaa transaktiolokia tietokannan tilaan ja tekee transaktiolokiin merkityt tietokantatapahtumat uudelleen tietokantaan.

Transaktiolokin lokimerkintä koostuu seuraavista osista:

- Lokimerkinnän numero (LSN, Log Sequence Number): Jokaisella transaktiolokin lokimerkinnällä tulee olla uniikki tunnistetieto.
- Tieto edellisen lokimerkinnän numerosta (LSN), jotta lokimerkintöjen keskinäinen järjestys voidaan selvittää.
- Tietokantatapahtuman tunnistetieto, jotta tiedetään, mikä tietokantatapahtuma aiheutti lokimerkinnän.

[30] Salassapidettävien tietojen osalta on perustelua kirjata lokiin myös tietojen luku, ei ainoastaan muutokset solujen arvoihin.

- Lokimerkinnän tyyppi, joka kertoo tietokantatapahtuman tyypin.
- Tieto itse tietokantatapahtuman generoimasta muutoksesta, joka tietokantaan tehtiin ja jonka vuoksi transaktiolokin merkintä kirjoitettiin.

Esimerkkejä transaktiolokeista ovat erilaiset operatiivisten tietokantajärjestelmien tietokantalokit, kuten toiminnanohjausjärjestelmien tietokantojen transaktiolokit. Esimerkiksi toiminnanohjausjärjestelmästä voidaan ottaa päivittäin täysi tietokantavarmistus. Tämän jälkeen tulee jokaisesta transaktiosta kirjoittaa transaktiolokia varmistuksen jälkeisistä tietokantatapahtumista seuraavaan täysvarmistukseen asti. Näin ollen tietokanta voidaan päivän aikana palauttaa täysvarmistuksesta ja transaktiolokista takaisin siihen tilaan, missä se oli mahdollisen virhetilanteen tapahtuessa.

Transaktiolokin lisäksi tietokannat pitävät tai voivat[31] pitää muita lokeja. Tyypillisesti tietokannat ovat kykeneviä kirjaamaan lokitietoja

- kirjautumisista ja uloskirjautumisesta
- tietokantojen käynnistyksestä, uudelleen käynnistämisestä ja sammuttamisesta
- järjestelmävirheistä ja vioista
- käyttöoikeuksien muutoksista
- tietokannan rakenteen muutoksista
- tietokannan ylläpitäjän toimista[32]
- tietokannan tietojen luvusta ja muutoksista.

Erityisesti tunnettujen tietokantavalmistajien uusimmat tietokantaversiot sisältävät erittäin kehittyneet loki ja auditointiominaisuudet, jotka eivät kuitenkaan välttämättä ole oletuksena käytössä. Vanhemmissa tietokannoissa on rajoittuneemmat mahdollisuudet muun muassa tietokannan ylläpitäjien toimien seurantaan ja kirjaamiseen sekä tehtävien eriyttämiseen.

---

[31] Tyylillisesti monet tietokannan tietoturvallisuuden ja käytön seurannan kannalta keskeiset lokiasetukset ovat oletuksena pois päältä, jolloin tietokanta pitää vain pakollisia transaktiolokeja, joiden avulla varmistetaan kannan oikea toiminta.

[32] Tämä on erityisen tärkeää tietokannan turvallisuuden varmistamiseksi. DBA (tietokannan ylläpitoloki) loki tulee olla suojattu tietokannan ylläpitäjän muutoksilta.

Huomioitavaa lokien käsittelyssä:

Jos järjestelmässä käsitellään salassapidettävää aineistoa, myös transaktiolokit tulisi kopioida automaattisesti suojattuun lokipalvelimeen.

Myös luku- ja pääsyvalvontatapahtumista tulee kirjata lokia.

Tietokannoissa tapahtumien kirjaamisella lokiin voi olla konkreettiseia vaikutuksia järjestelmän suorituskykyyn. Tämä on huomioitava järjestelmän suunnittelussa.

3.1.8 Muiden lokien käsittelylokit

Muiden lokien käsittelyloki pitää kirjaa siitä, kuka on lukenut, muuttanut, poistanut tai muutoin käsitellyt jotain tiettyä lokitietoa tai lokitiedostoa. Vaatimus lokienkäsittelyn lokien keräämisestä liittyy erityisesti teleyritysten hallussa olevien viestinnän lokien käsittelyyn, mutta hyvin rakennetussa lokiympäristössä kaikesta lokien käsittelystä pidetään kirjaa ja seuranta on erotettu järjestelmien operoinnista ja ylläpidosta.

Käsittelyloki ei tyypillisesti synny automaattisesti, vaan lokia tuottavan organisaation tulee itse rakentaa sellainen järjestelmä ja lokiympäristö, että tarvittava lokienkäsittelyn kirjaaminen ja seuranta on mahdollista.

Sähköisen viestinnän tunnistamistietojen käsittelylokin käsittely on hyvä tehdä erityisesti siihen tarkoitukseen luodulla käyttäjätunnuksella[33]. Nämä tunnukset tulee myöntää vain rajoitetulle ja nimetylle joukolle ihmisiä. Mahdollisuuksien mukaan järjestelmien ylläpito tulee erottaa käytön valvonnasta. Lokien sisältämää tietoa voidaan luovuttaa vain Sähköisen viestinnän tietosuojalain 33 § mukaisesti tietyissä tapauksissa ohjaus- ja valvontaviranomaisille. Kaikista tunnistamistietojen käsittelykerroista tulisi tallentaa ainakin:

- käsittelyn aloitus- ja lopetusaika ja päivämäärä
- käsittelijän koko nimi tai yksilöllinen käyttäjätunnus, joka on yhdistettävissä yksittäiseen henkilöön
- mitä tunnistamistietoja on käsitelty
- minkä ajankohdan tunnistamistietoja on käsitelty
- käsittelyn peruste, eli miksi kyseistä lokia on katsottu tai muuten käsitelty
- mahdollinen kuvaus käsittelystä.

[33] Myös tämän tunnuksen tulee olla henkilökohtainen, niin kuin kaikkien muidenkin luotettavaan lokiympäristöön liittyvien käyttäjätunnusten.

Huomioitavaa lokien käsittelyssä:

> Lokien käsittelyn loki voidaan tuottaa esimerkiksi ohjaamalla tärkeät lokit erilliseen lokipalvelimeen, jonne kirjaudutaan omalla tunnuksella ja käsittelemällä lokeja omilla tunnuksilla.

3.1.9 Automaattisesti raakalokia tulkiten tuotettu aineisto

Raakalokista tulkiten tuotettu aineisto perustuu olemassa oleviin lokeihin ja lokimerkintöihin ja sitä voidaan pitää raporttina lokeista. Esimerkkejä tällaisista raporteista on erilaisin analyysimenetelmin muodostetut poikkeavien lokimerkintöjen listat, kuten IDS[34] ja palomuuriraportit. Tällaisten lokitiedosta muodostettujen raporttien tarkoituksena on etsiä hyökkäykseen viittaavia ennalta tunnettuja sormenjälkiä. Käyttö ja analysointi tulee olla linjassa lokin keräämistarkoituksen kanssa.

Huomioitavaa raporttien käsittelyssä:

> Ylläpitäjän on ymmärrettävä automaattista lokitietojen analysointia suorittavan ohjelman / järjestelmän rajoitukset. IDS-järjestelmä ei pysty havaitsemaan kuin pienen osan poikkeamista. IDS-järjestelmät havaitsevat tapahtumia ennalta määriteltyjen hyökkäyssormenjälkien perusteella. Tosin monet järjestelmät voivat tehdä myös heuristista analyysiä tapahtumista ja niiden merkityksestä.
>
> Analysointi tulee perustua lokien alkuperäiseen keräämistarkoitukseen ja olla linjassa tämän kanssa.
>
> Lokien tiivistys on usein tarpeellista valtavan tietomäärän hallitsemiseksi ja tallennustilan säästämiseksi.

3.1.10 Kuormitusraportit

Kuormitusraportti osoittaa määritetyn palvelimen, järjestelmän tai verkon kapasiteetin ja kuormituksen kehityksen. Kuormitusraportteja käytetään nk. pullonkaularesurssien etsimiseen, jotta kapasiteetti ja kuormitus saadaan

[34] Intrusion Detection System, tunkeutumisen havaitsemisjärjestelmä.

optimoitua. Kuormitusraportteja käytetään laite- ja verkkoresurssien suunnitteluun, muutosten tarkistamiseen ja optimointiin sekä kuormantasaukseen[35].

3.1.11 Tilastot

Erilaiset sovellukset (esim. web-sovellukset) keräävät tilastotietoja sovellusten ja sivustojen käytöstä, käyttäjistä jne. Tilastoinnilla selvitetään web-sovellusten ja sivustojen käytön määrää ja voidaan esimerkiksi analysoida kävijöiden etenemistä palvelussa, jolloin voidaan optimoida sovelluksen käyttäjäystävällisyyttä ja käytettävyyttä. Tilastointi voidaan toteuttaa muun muassa evästeitä[36] hyödyntäen, joiden perusteella käyttäjä tunnistetaan tämän palatessa uudelleen samaan www-palveluun. Näin palvelujen käytöstä saadaan tilastoja lokianalyysia käyttäen. Näiden tilastojen avulla voidaan suorittaa esim. palvelun käyttäjien tyypittelyä. Lokitietoja analysoimalla voidaan esim. selvittää käyttäjien kiinnostusta tiettyihin aiheisiin tai käyttäjien ajankäyttöä palvelussa / sivustolla. Systemaattinen käyttäjien yksilöllinen seuraaminen ja yhdistely henkilötietoihin aiheuttavat henkilön tietosuojan loukkauksen, mutta anonyymissä analyysissä käytettynä tilastojen lokianalyysi on hyödyllinen tapa www-palveluiden kehittämiseksi.

---

[35] Kuormantasauksella tarkoitetaan tietyn tehtävän suorittamisen aiheuttaman kuorman jakamista usealle palvelimelle ja sitä käytetään suurta tehokkuutta vaativissa järjestelmissä sekä toteutuksen mahdollistamiseksi, että kustannustehokkuuden aikaansaamiseksi

[36] Cookie eli eväste on dataa, jonka web-palvelin tallentaa käyttäjän tietokoneelle. Selain lähettää evästeet vain kyseiselle palvelimelle. Evästeet ovat ratkaisu HTTP-protokollan tilattomuuteen. Jokainen HTTP-kutsu on täysin riippumaton toisistaan. Tämä vaikeuttaa istunnon seuraamista ja käyttäjän yksilöimistä: Käyttäjätunnus pitää piilottaa piilotettuihin CGI-kutsujen kenttiin. Evästeen avulla palvelin voi tallentaa dataa käyttäjälle joko tilapäisesti kyseisen istunnon ajaksi, tai pitemmäksi aikaa.

4 Lokien käsittelyn vastuut ja käsittelyprosessi

Lokien käsittely ja käsittelyn sisältö määriteltiin jo luvussa 1.2 ”Lokien käsittelyn määritelmä”. Yleisesti ottaen lokien käsittely kattaa lokin koko elinkaareen liittyvät toimenpiteet. Tietosuojasäännösten ja ohjeistusten yhteydessä puhutaan avoimuuden periaatteesta. Avoimuusperiaatteella tarkoitetaan sitä, että tietojen keräämisestä tai käsittelystä ja menetelmistä tiedotetaan kaikkia asianomaisia tahoja. Tätä periaatetta on luontevaa soveltaa myös lokitietoihin ja niiden käsittelyyn. Lokitietojen käsittelyn tulee olla tarpeeseen perustuvaa sekä ennalta määrätyllä ja sovitulla tavalla toteutettua.

Keskeisessä asemassa lokien käsittelyssä ovat selvät roolit ja vastuut sekä ennalta määritellyt ja dokumentoidut toimintatavat sekä prosessit lokien käsittelemiseksi. Käsittelyn perusperiaatteet tulee hyvän tiedonhallintatavan mukaisesti saattaa niin rekisteröityjen kuin järjestelmien käyttäjien ja ylläpitäjien tietoisuuteen. Monet lokien käsittelyyn liittyvät käytännön ongelmat ja haasteet ovat parhaiten vältettävissä juuri hyvällä suunnittelulla, dokumentoinnilla ja avoimella tiedottamisella.

Tässä luvussa käsitellään erityisesti lokien käsittelyyn liittyviä rooleja, vastuita sekä hallinnollisia prosesseja.

4.1 Vastuut lokien käsittelyssä

Asemavastuun perusteella henkilön asema organisaatiossa tai organisaation asema suhteessa toisiin organisaatioihin määrittelee pitkälti lokien käsittelyyn liittyvät vastuut. Lokien käsittelyyn liittyvien vastuiden ja velvollisuuksien määrittely ja dokumentointi on lokien keräämiseen liittyvien teknisten asioiden ja määrittelyiden ohella aivan keskeisessä roolissa lokien käsittelyssä.

Lainsäädäntöä ja muuta vaatimusympäristöä käsitelleissä ohjeen kappaleissa tuotiin jo esille, että:

- lokien keräämiselle tulee olla peruste
- lokeihin tallentuu erilaisia tietoja, joilla on erilaiset suojaustarpeet.

- nämä tietotyypit ja niiden suojaustarve tulee tunnistaa
- kaikkien henkilöiden ei tule päästä näkemään kaikkia lokissa olevia tietoja
- useimpien käyttäjien ei tule päästä näkemään mitään lokitietoja
- jotta lokeihin voidaan luottaa, niitä ei tule olla mahdollista oikeudettomasti muuttaa tai tuhota.

Kaikista edellä mainituista syistä johtuen lokien keräämiseen ja käsittelyyn liittyy myös erilaisia vastuita ja velvollisuuksia, joita käsitellään seuraavaksi.

4.1.1 Ylimmän johdon rooli ja vastuut

Riittävien ja toisaalta turhia tietoja sisältämättömien lokien olemassaolosta vastaa organisaation ylin johto. Organisaation johdon tulee täten varmistaa, että kaikissa hankkeissa huomioidaan myös toiminnan tai järjestelmien lokivaatimukset. Johdon tulee omalta osaltaan varmistua myös siitä, että lokit ja niiden sisältämät tiedot on suojattu tietoihin kohdistuvien vaatimusten ja käyttäjien sekä rekisteröityjen oikeusturvan edellyttämällä tavalla. Käytännössä tämä tarkoittaa vähintään että:

- vaatimukset tunnistetaan
- suojaustarpeet ja tavat määritellään
- tarvittaessa laaditaan rekisteriselosteet ja informoidaan asianomaisia
- käsittelytavat ja vastuut määritellään ja että
- lokien turvallisuutta ja suojauksen riittävyyttä auditoidaan säännöllisesti.

4.1.2 Tietohallinnon/ylläpitäjien rooli ja vastuut

Ylläpitäjien tulee tehtäviensä hoitamiseksi seurata sellaisia lokitietoja, joiden avulla voidaan havaita ylläpitäjän vastuulla olevien järjestelmien tai komponenttien oikea toiminta ja kapasiteetti.

Ylläpitäjien ei sen sijaan kuulu seurata lokeja, jotka liittyvät järjestelmän ylläpitäjien tekemien toimien seuraamiseen tai järjestelmän asianmukaisen ylläpidon seuraamiseen. Lokit tulee suojata myös ylläpitäjien tekemiltä muutoksilta

Ylläpitäjien tulee osana jokapäiväisiä tehtäviään varmistaa, että määritellyt lokit syntyvät suunnitellusti ja että niille on järjestelmissä riittävästi tilaa.

4.1.3 Tietoturvavastaavan tai -organisaation rooli ja vastuut

Tietoturvaorganisaation vastuulla on seurata lokeja tietoturvallisuudesta huolehtimiseksi sekä tietoturvarikkomusten selvittämiseksi. Tietoturvaorganisaa-

tio on myös oikea taho seuraamaan ylläpitäjien tekemiä toimia sen varmistamiseksi, että ylläpitäjät hoitavat tehtävänsä asianmukaisesti. Tietoturvaorganisaatiolla puolestaan ei tule olla järjestelmien ylläpidollista roolia.

Tietoturvaorganisaatio avustaa ylintä johtoa tietosuoja ja -turvavaatimusten tunnistamisessa ja määrittämisessä sekä varmistaa omalta osaltaan vaatimusten toteutumisen hankintojen tai toimittajavalintojen yhteydessä.

Tietoturvaorganisaatio myös tekee tai teettää tarvittavat auditoinnit lokien asianmukaisen suojauksen todentamiseksi sekä järjestelmien tietoturvallisuuden kehittämiseksi.

4.1.4 Henkilöstöhallinnon/identiteetinhallintavastuullisten rooli ja vastuut

Yksi lokien suojaamisen tärkeistä elementeistä on lokitietojen suojaaminen käyttöoikeuksin. Henkilöstöhallinnon (HR) rooli ja vastuut lokien käsittelyssä liittyvät usein lähinnä käyttöoikeuksien hallintaan. Kaikissa organisaatioissa HR ei ole osallisena käyttöoikeuksien hallinnassa. HR on usein kuitenkin luonteva identiteetinhallintajärjestelmien omistaja ja HR usein käynnistää prosessin käyttöoikeuksien myöntämiseksi tai poistamiseksi. Käyttöoikeudet puolestaan hyväksyy kunkin järjestelmän tai tiedon omistaja ja toteuttaa järjestelmän tai sovelluksen pääkäyttäjä.

4.1.5 Roolit ja vastuut ulkoistuksissa

Ulkoistetuissa palveluissa vastuut perustuvat sopimukseen ja sen määrittelyihin. Hankinnoissa kannattaa lokivaatimuksiin kiinnittää huomiota jo tarjouspyyntövaiheessa, jotta palveluiden tarjoajat voivat tarjouksessaan huomioida nämä vaatimukset ja mitoittaa palvelunsa oikein myös lokien käsittelyn osalta. Huomiota tulee kiinnittää niin teknisiin kuin hallinnollisiin vaatimuksiin sekä lokien luovutusoikeuteen sekä omistajaan, jotta omistajalle jää oikeus saada lokitiedot haltuunsa esimerkiksi poikkeamatilanteen selvittämiseksi. Hankintoja ja ulkoistusta käsitellään vielä tarkemmin ohjeen myöhemmissä luvuissa.

4.2 Lokien käsittelyn prosessit ja periaatteet

Järjestelmien ja niihin liittyvien lokiasetusten ja tiedostojen suunnittelussa tulee ottaa huomioon ja miettiä erityisesti sitä, miksi lokeja halutaan kerätä ja analysoida. Myös lainsäädäntö lähtee siitä, että turhia tietoja henkilöistä ei saa kerätä ja kerättäville tiedoille tulee olla perusteltu tarve. Silloinkin kun ei puhuta henkilö- tai tunnistamistiedoista, ei turhia tietoja kannata kerätä,

koska siitä aiheutuu ylimääräisiä kustannuksia ja lokien analysointi vaikeutuu. Lokien käsittelyyn tulee olla riittävä oikeutus, joka tyypillisesti perustuu henkilön toimenkuvaan ja rooliin, joita käsiteltiin aikaisemmin.

4.2.1 Käsittelyoikeudet omassa organisaatiossa

Lokien käsittelyoikeus perustuu lakiin. Koska lokeja on hyvin erityyppisiä, on niiden käsittelyn tarve ja käsittelyoikeus riippuvainen siitä, millaista tietoa loki sisältää ja mihin tarkoitukseen lokia on alun perin kerätty. Tietojärjestelmän omistaja on myös järjestelmästä syntyvien lokitietojen omistaja. Tietojärjestelmän omistaja valtuuttaa jonkun huolehtimaan tietojärjestelmän toiminnasta, käytettävyydestä ja turvallisuudesta, jolloin samalla myöntää oikeuksia seurata tietojärjestelmän tilaa lokitietoja seuraamalla.

Kaikkien henkilöiden tai oikeammin yksittäisiä tehtäviä hoitavien henkilöiden ei tarvitse nähdä kaikkia lokeja tai kaikkia yksittäisen lokin tietoja. Lokien käsittelyoikeudet tulee rajata roolipohjaisesti käyttöoikeuksin, vastaavasti kuin muidenkin järjestelmien ja tietojen käsittelyn oikeudet.

Silloin kun kyseessä on sellaisten lokien käsittely, jotka sisältävät sähköiseen viestintään liittyviä tunnistamistietoja, määräytyy lokien käsittelyoikeus sähköisen viestinnän tietosuojalain luvun 3 mukaan. Käsittely on tällöin sallittua lain rajaamissa puitteissa:

- palvelujen toteuttamiseksi ja käyttämiseksi
- laskutusta varten
- markkinointia varten
- teknistä kehittämistä varten
- lähinnä maksullisen palvelun käyttöön liittyvissä väärinkäytöstapauksissa
- teknisen vian tai virheen havaitsemiseksi
- tietoturvallisuudesta huolehtimiseksi.

4.2.2 Toimenpiteet tietoturva- ja tietosuojarikkomuksissa

Organisaatiossa on oltava riittävä ohjeistus ja valtuutukset tietoturva- ja tietosuojarikkomusten selvittämiseksi. Tässä yhteydessä on määriteltävä menettelyt virhetilanteiden sekä tietoturva- ja tietosuojaloukkausten varalta. Ohjeistuksen tulee ottaa kantaa siihen, kuka tekee ja mitä tehdään, jos tietorikkomuksia epäillään. Tähän liittyvät lokien käyttöoikeudet on määriteltävä ja toteutettava sekä asianomaiset henkilöt koulutettavasiten, että he ymmärtävät rooliinsa liittyvät oikeudet ja velvollisuudet. Ylläpitohenkilökunnalla tulee olla tiedossa henkilö - esimerkiksi organisaation lakimies - jolta saa tarvittaessa neuvoja.

Viestinnän lokitietoja voi käyttää vain sähköisen viestinnän tietosuojalain sekä työelämän tietosuojalain säätämällä tavalla. Työnantajalla ei siten ole oikeutta käyttää viestinnän tunnistamistietoa esimerkiksi työtehtävien laiminlyöntien eikä edes salassapitorikosten selvittämiseen. Viestiliikenne johonkin tiettyyn vahingolliseen kohteeseen voidaan kuitenkin estää työelämän tietosuojalain edellyttämän yhteistoimintaprosessin jälkeen.

4.2.3 Tarve yhteistoimintamenettelylle (YT)

Teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestäminen työpaikalla kuuluvat yhteistoimintamenettelyn piiriin. Käytännössä edellä mainittu tarkoittaa sitä, että silloin kun lokia tai yleensä laajemmassa mielessä teknistä järjestelmää, joka myös tuottaa lokia, on tarkoituksena käyttää henkilöstön toimien tekniseen valvontaan, tulee asia käsitellä YT-menettelyn mukaisesti.

Jos lokissa on henkilötietoa, tulee huomioida henkilötietolain pykälän 24 mukaiset vaatimukset rekisterinpitäjän tiedonantovelvollisuudesta.

4.2.4 Lokitietojen analysointi

Lokitietojen analysoinnissa tulee huomioida edellä esitetyt rajoitukset sekä lokien käsittelyn tarvesidonnaisuus. Lokitietojen tehokas analysointi on usein lokitietojen hallinnan ja käsittelyn vaativin mutta toisaalta usein myös tärkein osa-alue. Vaikka lokitietojen analysointi nähdään työläänä ja tehottomana toimenpiteenä, voidaan hyvillä lokien hallintatyökaluilla ja ympäristöllä automatisoida lokitietojen käsittely ja analysointi, jolloin se vie vähemmän aikaa. Lokitietojen analysoinnissa tulee kuitenkin ymmärtää tiettyjä perusasioita lokeista ja lokimerkintöjen luokittelusta ja priorisoinnista, joita selvitetään seuraavissa kappaleissa.

Tehokkain tapa käsitellä lokeja ja niiden sisältämiä lokimerkintöjä on lokitietojen analysoinnin säännöllisyys (esimerkiksi joka päivä). Tavoitteena on saada käsitys normaaleista lokimerkinnöistä, jotta saadaan vertailukohta epätavallisille lokimerkinnöille. Säännöllisen lokien läpikäynnin ja analysoinnin tuloksena saadaan analysoitua suurin osa lokimerkinnöistä, koska yleensä muutaman tyyppiset lokimerkinnät muodostavat suurimman osan järjestelmän tekemistä lokimerkinnöistä ja mahdolliset poikkeamat pystytään tunnistamaan helpommin. Ajan kuluessa opitaan tunnistamaan järjestelmän normaali toiminta ja pystytään tunnistamaan epätavalliset lokimerkinnät, jolloin päivittäiseen lokien analysointiin menee vähemmän aikaa.

Laajojen ympäristöjen osalta manuaalinen analysointi muodostuu helposti työlääksi, ellei mahdottomaksi. Kun on tunnistettu ja määritetty, mitkä loki-

merkinnät ovat tärkeitä ja mitkä eivät, voidaan lokimerkinnöille rakentaa automatisoitua suodattamista. Tämän avulla on mahdollista toteuttaa epätavallisten ja haitallisten toimien automatisoitu tunnistaminen sekä niihin reagointi (esim. hälyttää järjestelmänvalvojia tai aktivoida muita turvakontrolleja). Lokimerkintöjen suodattamisen toinen tarkoitus on mahdollistaa järjestelmänvalvojien manuaalisen analysoinnin järkevä priorisointi. Manuaalinen analysointi on huomattavasti tehokkaampaa, helpompaa ja vähemmän aikaa vievää, kun lokimerkinnöistä on suodatettu kaikki tavalliset tapahtumat pois. Yksi tehokas keino suodattamiseen on suorittaa se siten, että tuotetaan automaattisen analysoinnin tuloksena kaksi raporttia, toinen lokimerkinnöille, jotka on tunnistettu tärkeiksi ja toinen merkinnöille, joita ei vielä täysin ymmärretä. Luonnollisesti molemmat raportit tulee käydä läpi säännöllisesti ja priorisoida tärkeiden merkintöjen raportti korkeammalle kuin uusien merkintöjen, joita ei vielä ymmärretä. On kuitenkin tärkeää käydä uusien lokimerkintöjen raportti läpi, jotta saadaan laajennettua tunnistettujen lokimerkintöjen joukkoa.

Lokimerkintöjen analysoinnin priorisointi voi olla haastavaa johtuen eri järjestelmien tuottamien lokimerkintöjen toisistaan poikkeavista priorisointiluokitteluista. Ne ovat usein epäyhtenäisellä skaalalla toisiinsa verrattuna (esim. high-medium-low tai 1-5). Lisäksi lokia tuottavien järjestelmien priorisointisäännöt eivät välttämättä istu organisaation omiin sääntöihin. Tämän vuoksi organisaatiossa olisi hyvä määritellä oma priorisointi lokimerkinnöille, jossa tulisi huomioida useita eri asioita, kuten:

- lokimerkinnän tyyppi (esim. luokka: kriittinen tai tiedon luvaton muuttaminen/muuttamisyritys)
- lokimerkinnän harvinaisuus tai uutuus (uudet lokimerkinnät tulisi analysoida)
- lokimerkinnän lähde (esim. kriittinen järjestelmä)
- lähde- tai kohde-ip-osoite (lähdeosoitteen oleminen mustalla listalla tai tapahtuman kohdeosoite kuuluu kriittiselle järjestelmälle)
- kellonaika ja viikonpäivä (tietyn tyyppisten merkintöjen ilmaantuminen väärään aikaan)
- lokimerkintöjen ilmaantumisen tiheys (esim. x kertaa y sekunnissa).

Lokimerkintöjen analysoinnin tulisi myös sisältää korrelaatio toisiin lokimerkintöihin tai toisiin järjestelmiin. Tietyn tyyppinen lokimerkintä voi esimerkiksi antaa viitteitä mahdollisesta hyökkäyksestä, jolloin vastaavien lokimerkintöjen tai havaintoa tukevien merkintöjen etsiminen muista lokeista voi auttaa antamaan vahvistuksen havainnon oikeellisuudesta.

Lokien analysoinnissa ja ymmärtämisessä on tärkeää ymmärtää jokaisen lokia tuottavan järjestelmän normaali, tyypillinen toiminta. Suurin osa lokimerkinnöistä on helppoja ymmärtää, mutta osa voi olla vaikeaselkoisia, johtuen lähinnä asiayhteyden puutteesta tai epäselvistä merkinnöistä. Jokaisen

lokimerkinnän merkitys riippuu asiayhteydestä Asiayhteys selviää yleensä vertaamalla lokimerkintää muihin saman järjestelmän tuottamiin lokimerkintöihin ja järjestelmän muihin asetuksiin. Asiayhteys vaaditaan, jotta voidaan varmistua siitä, onko lokimerkintä poikkeava vai ei. Esimerkki asiayhteyden tärkeydestä on IDS-järjestelmien tai muiden tietoturvalaitteiden/-ohjelmistojen tuottamat raportit, jossa yksittäisiä raportointimerkintöjä tulee verrata alkuperäisiin lokeihin, jotta erotetaan nk. väärät positiiviset havainnot oikeista, merkityksellisistä raportoinneista. Lokimerkinnässä voi olla myös kryptinen virheilmoitus tai koodia, joka on ymmärrettävissä järjestelmän toimittajalle, mutta ei lokin analysoijalle. Tällaisten lokimerkintöjen selvittämiseksi tarvitaan järjestelmän toimintaan perehtyneen asiantuntijan apua, jotta saadaan selvitettyä merkintöjen sisältö.

Lokien ja lokimerkintöjen analysoinnissa tulisi organisaatiossa päättää ainakin seuraavista asioista:

- kuinka usein ja miten eri lokitietoja pitää analysoida
- kenen pitää päästä käsiksi lokitietoihin, ja kuinka tämä lokien käsittely pitää kirjata lokienkäsittelyn lokiin
- mitä tehdään, kun huomataan lokimerkinnöissä poikkeamia
- kuinka mahdollisen luottamuksellisen tiedon tahaton paljastuminen (esim. salasanat, sähköpostien sisältö) käsitellään.

4.2.5 Rekistereiden käytön poikkeamatapaukset ja puuttumiskynnykset

Kaikista esiin tulleista rekisterien väärinkäyttötapauksista on erikseen ja viivytyksettä ilmoitettava rekisterinpitäjälle sekä oman organisaation valvonnasta vastaavalle jatkotoimenpiteiden käynnistämiseksi. Jos lokiseuranta-asia siirretään esimerkiksi organisaation sisällä jonkin muun yksikön käsiteltäväksi, on huolehdittava myös siitä, että rekisterinpitäjä saa tällöinkin informaation asiasta ja sen etenemisestä.

Laillisuusvalvonnassa tai muutoin havaittuihin laiminlyönteihin ja virheisiin tulee puuttua viipymättä. Vaikka menettely ei olisikaan nimenomaisesti säännösten, määräysten tai ohjeiden vastaista, siihen on syytä puuttua, jos näin voidaan edistää hyvän hallinnon periaatteiden tai perusoikeuksien toteutumista taikka muutoin parantaa viranomaistoiminnan laatua sekä luottamusta viranomaisiin.

Virkamiehen oikeuksiin puututtaessa asia käsitellään hallintolain säännöksiä soveltaen siinäkin tapauksessa, ettei asiassa ole meneteltävä esimerkiksi valtion virkamieslain 24 §:n tarkoittamalla tavalla. Virkamiehiä ei saa asettaa keskenään eriarvoiseen asemaan, vaan puuttumisen tulee olla johdonmukaista niin osapuolten sisällä kuin välilläkin.

Virheen tai laiminlyönnin vakavuuden mukaan toimenpiteenä voidaan käyttää suullista tai kirjallista huomautusta tai kirjallista varoitusta. Seuraamusten valinnassa tulee kiinnittää huomiota menettelyn vahingollisuuteen ja vaarallisuuteen, sen vaikuttimiin, mahdolliseen toistuvuuteen ja muihin olosuhteisiin, jotka vaikuttavat menettelyn kokonaisarviointiin. Virhe tai laiminlyönti voi täyttää myös rangaistavan teon tunnusmerkistön. Mahdollinen esitutkinta tai asian saattaminen esitutkintaan on rekisterinpitäjän tai muun asianomistajan harkinnassa. Kuitenkin on huomioitava erityinen lainsäädäntö ja ohjeistus.

4.3 Lokitietojen luovutusoikeudet

Organisaatiolle voi tulla tarve luovuttaa sen hallussa olevia lokitietoja toiselle organisaatiolle esimerkiksi silloin kun:

- Organisaatio on ylläpitänyt järjestelmää ja siihen liittyviä lokeja toisen organisaation lukuun. Tällöin luovutusoikeus perustuu sopimukseen ja luovutuksen osapuolten asemaan tietojen tosiasiallisena omistajana.
- Organisaatiot tekevät viranomaistoimintaan liittyvää yhteistyötä.
- Organisaatio on joutunut tai epäilee joutuneensa tietoturvapoikkeaman kohteeksi. Tällöin organisaatio voi luovuttaa lokitietoja sähköisen viestinnän tietosuojalain puitteissa viestintävirastolle tai muille saman tapahtuman kohteeksi joutuneille organisaatioille.

Poliisi voi tarvita organisaation hallussa olevia lokitietoja rikoksen selvittämiseksi tai ennaltaehkäisemiseksi. Viestinnän tietoja kuvaavien lokien luovutusoikeudet ja -velvollisuudet vaihtelevat riippuen lokia hallussaan pitävän organisaation roolista eli siitä, onko organisaatio viestinnässä osapuolena vai ei.

4.3.1 Rikoksen uhrin oikeudet luovuttaa lokitietoja esitutkintaviranomaiselle

Rikoksen uhriksi joutuneella organisaatiolla on lähtökohtaisesti oikeus luovuttaa itseensä kohdistuneen rikoksen selvittämiseksi tarpeellinen lokiaineisto rikosta tutkivalle poliisille. Poliisilain 35 § säätää oikeudesta tietojen saantiin viranomaiselta ja 36 § oikeudesta tietojen saantiin yksityiseltä yhteisöltä tai henkilöltä. Lain mukaan poliisilla on oikeus saada ”teleyritykseltä ja yhteisötilaajalta tai teknisellä laitteella yhteystiedot sellaisesta teleliittymästä, jota ei mainita julkisessa luettelossa, tai teleliittymän, sähköpostiosoitteen, muun teleosoitteen tai telepäätelaitteen yksilöivät tiedot”, jos niitä tarvitaan yksittäistapauksessa poliisille kuuluvan tehtävän suorittamiseen. Tällöin kyseessä on liittymän haltijatiedot.

Tällä hetkellä poikkeuksen muodostaa kuitenkin yksityiseksi ja luottamukselliseksi tarkoitetun viestinnän lokitiedot. Organisaatio voi yhä luovuttaa lokitiedot, jos organisaatio selkeästi on viestinnässä osapuolena. Jos sen sijaan organisaatio on viestinnässä välittäjän roolissa, organisaatiolla ei sähköisen viestinnän tietosuojalain puitteissa ole oikeutta käsitellä lokitietoja viestinnän sisältöön liittyvien semanttisten kriteerien perusteella eikä poliisi voi ottaa lokitietoja vastaan ilman tuomioistuimen määräänmä televalvontalupaa. Niinpä viestinnän lokitietoja ei tällä hetkellä voi lainkaan käsitellä esimerkiksi salassapitorikosten selvittämiseksi.

Jos on syytä olettaa, että ”data, jolla voi olla merkitystä tutkittavana olevan rikoksen selvittämiselle häviää tai sitä muutetaan”, poliisi voi pakkokeinolain takavarikkopykälien perusteella määrätä organisaation säilyttämään sen muuttumattomana. Poliisilla ei ole oikeutta saada tietoonsa datan säilyttämismääräyksen nojalla viestin tai liikennetiedon sisältöä. Jos viestin välittämiseen on osallistunut useampia palveluntarjoajia, on poliisilla oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot. Tällainen datan säilyttämismääräys annetaan määräajaksi, enintään kolmeksi kuukaudeksi. Sitä voidaan jatkaa aina kolme kuukautta kerrallaan, jos rikoksen tutkinta sitä edellyttää. Säilytysmääräyksen saanut on velvollinen pitämään salassa saamansa määräyksen.

4.3.2 Sivullisen oikeudet ja velvollisuudet luovuttaa lokitietoja esitutkintaviranomaiselle

Vaikka organisaatio itse ei olisi rikoksen uhri, sillä voi olla hallussaan rikoksen selvittämistä edesauttavia lokitietoja. Tällainen tilanne syntyy esimerkiksi, jos organisaation järjestelmiä tai yhteyksiä on käytetty rikoksen toteuttamiseen.

Muiden kuin viestinnän lokien osalta organisaatiolla on pääsääntöisesti oikeus luovuttaa lokitietoja rikoksen selvittämiseksi ja usein myös ennaltaehkäisemiseksi. Kaikelle poliisin toiminnalle on kuitenkin oltava toimivaltuussäännös, joten poliisin tulee lokitietoja pyytäessään selventää, mihin tiedonluovutuspyyntö tai -määräys perustuu.

Viestinnän lokitietojen luovutus poliisille edellyttää tuomioistuimen päätöstä, ellei luovuttava organisaatio ole viestinnän osapuoli. Tutkittavasta rikoksesta riippuen päätös voi perustua joko pakkokeinolain 5a §:n mukaiseen televalvontaan tai sananvapauslain (laki sananvapauslain käyttämisestä joukkoviestinnässä) mukaiseen tunnistamistietojen saantiin.

4.3.3 Käyttäjän tai rekisteröidyn tiedonsaantioikeus

Silloin kun loki muodostaa henkilörekisterin, tulee lokista tehdä rekisteriseloste. Rekisteröidyllä on oikeus tarkistaa ja vaatia korjattavaksi itseään koskevat merkinnät henkilörekisteristä. Järjestelmän ja lokin tyypistä ja sisällöstä riippuen tämä tarkastusoikeus voi ulottua myös lokitietoihin. Rekisteröidyllä on oikeus saada itseään koskevat tiedot myös muilta kuin teleyrityksiltä, tarkastaakseen tietonsa henkilörekisteristä. Tiedot tulee kuitenkin yksilöidä. Pyyntö ei voi olla liian yleinen, esimerkiksi: ”haluan kaikki minua koskevat lokimerkinnät”. Tietojen toimittamisesta voidaan periä kustannukset kattava maksu.

5 Lokit hankintojen, ulkoistusten ja järjestelmäkehityksen yhteydessä

Jotta järjestelmät tuottaisivat tarvittavat lokit, jotka täyttävät niin organisaation kuin lainsäädännön vaatimukset, tulee lokeihin liittyvät vaatimukset selvittää ja määrittää hyvissä ajoin hankinnan tai järjestelmäkehityksen alkuvaiheessa. Tässä luvussa käsitellään hankintoihin, ulkoistukseen ja järjestelmäkehitykseen liittyviä lokiasioita, hankinnan elinkaaren mukaisesti.

5.1 Lokit järjestelmähankinnan tai -kehityksen yhteydessä

5.1.1 Määrittely- ja tarjouspyyntövaihe

Määrittelyvaiheessa määritellään hankittavan tai kehitettävän järjestelmän toiminnalliset ja muut vaatimukset. Tässä yhteydessä tulee määritellä myös loki- ja tietoturvavaatimukset, jotka ovat aivan yhtä olennainen osa laadukasta ja toimivaa tietojärjestelmää kuin muutkin vaatimukset. Lokien käsittely tulee suunnitella ja toteuttaa tämän ohjeen lokien käsittelyn periaatteiden mukaisesti. Määrittelyssä tulee huomioida lokien koko elinkaari, joka kattaa seuraavat toimenpiteet: kerääminen, säilyttäminen, prosessoiminen, luovuttaminen ja poistaminen tai arkistointi. Samoin määrittelyssä tulee huomioida lokien eri tasot, sillä järjestelmä voi tuottaa lokeja esimerkiksi sovellus, käyttöjärjestelmä, tietokanta ja verkkotasoilla. Määrittelyvaiheessa on syytä pohtia:

- mitä lokitietoa järjestelmästä halutaan kerätä ja miksi
- millä tarkkuudella tietoa kerätään
- mihin tiedot kerätään ja miten
- millaiset käyttöoikeudet ja käyttäjäryhmät lokitietojen käsittelyyn tarvitaan
- millainen arkistointitarve lokeilla on ja miten lokit varmistetaan.

Yllä olevat vaikuttavat hankinnan kustannuksiin ja ovat usein vaikeasti hahmoteltavissa. Siksi tarjouspyynnössä tulee tarjouspyynnön kohteesta ja laajuudesta riippuen riittävällä tasolla tuoda esille myös hankittavalta järjestelmältä edellytettävät lokit ja niiden suojaustarpeet, jotta toimittaja voi huomioida nämä vaatimukset ehdottamassaan tuotteessa, ratkaisussa tai palvelussa.

5.1.2 Sopimusvaihe

Sopimusvaiheessa tulee varmistaa, että vaatimukset sisältyvät toimitukseen ja siihen liittyvään sopimukseen. Tyypillisesti lokeihin liittyvät vaatimukset on määritelty sopimuksen liitteissä, osana muita vaatimusmäärittelyitä.

5.1.3 Toteutus- ja käyttöönottovaihe

Toteutusvaiheessa toimittajan tai oman sisäisen projektiryhmän tulee toteuttaa järjestelmä vaatimusten mukaisesti. Oleellista toteutusvaiheessa on toteutuksen vaatimusten mukaisuuden varmistaminen projektista riippumattomien tahojen toimesta. Näin varmistutaan, että lopputuotoksesta tulee sovittujen vaatimustenmukainen. Vaatimusten mukaisuus voidaan varmistaa projektin eri vaiheissa tehtävien sisäisten tai ulkoisten auditointien avulla. Auditointeja voi ja kannattaa tehdä ainakin seuraavasti.

- Dokumentaation perusteella – varmistutaan, että määritellyt vaatimukset ovat riittävän kattavat ja linjassa tarpeiden kanssa.
- Eri kehitysvaiheiden testauksen perusteella – varmistutaan, että toteutusta ollaan tekemässä vaatimusten mukaisesti.
- Ennen tuotantoon siirtoa tehtävän testauksen avulla – varmistutaan, että toteutus vastaa kaikilta osiltaan vaatimuksia ja on valmis siirrettäväksi tuotantoon.
- Tuotantoon siirron jälkeen tehtävän testauksen avulla – varmistutaan, että järjestelmän asetukset tai muu toteutus ei ole muuttunut tuotantoon siirron yhteydessä.
- Tuotannon aikaisten testausten avulla – varmistetaan, että järjestelmä on muuttunut hallitusti ja vastaa edelleen vaatimuksia tai mahdollisia uusia/muuttuneita vaatimuksia.

Lokien kannalta tarkastus kohdistuu määriteltyihin lokivaatimuksiin.

5.1.4 Tuotantokäyttö

Tuotantokäytön aikana on oleellista varmistua siitä, että järjestelmään tehdyt muutokset ovat olleet hallittuja ja että järjestelmä edelleen vastaa vaatimuksia. Tässä yhteydessä tulee huomata, että vaatimukset tyypillisesti muuttuvat ja kehittyvät järjestelmän elinkaaren aikana, joten järjestelmän tulee vastata näitä uusia vaatimuksia.

Tuotantokäytön aikana lokeja tulee kerätä ja analysoida sekä muutenkin käsitellä ennalta määriteltyjen käytäntöjen edellyttämällä tavalla.

5.1.5 Käytöstä poisto

Käytöstä poistettu järjestelmä ei enää tuota uusia lokeja, mutta se tai keskitetty lokijärjestelmä tyypillisesti sisältää kyseisen järjestelmän käytön aikanaan tuottamia lokitietoja. Kun järjestelmä poistetaan käytöstä, lakkaa yleensä samalla tarve analysoida tämän järjestelmän tuottamia lokeja.

Tiettyjen tietojen, kuten henkilötietojen tallentaminen on sallittua ja hyvän käytännön mukaista vain jotakin tiettyä tarvetta ja tarkoitusta varten. Jos tallentamisen tarve lakkaa, tulee tiedot tuhota luotettavasti. Toisaalta tietyt lokitiedot tulee arkistoida ja säilyttää todistusaineistona tiettyjen tapahtumaketjujen todentamiseksi tai muusta määritellystä syystä. Lokien arkistointitarve tulee olla määritelty jo suunnitteluvaiheessa. Lokien säilytystä käsitellään tarkemmin toisaalla tässä ohjeessa.

5.2 Ulkoistuksiin liittyvät erityiskysymykset

Edellä käsiteltyjen hankinnan tai järjestelmäkehityksen vaiheiden osalta ulkoistuksiin liittyy tiettyjä erityiskysymyksiä, joita tarkastellaan lokien käsittelyn osalta seuraavaksi. Käsiteltyjen asioiden on tyypillisesti havaittu olevan haasteellisia ja puutteellisesti hoidettuja. Ulkoistusten yhteydessä tulee siten varmistaa, että seuraavat asiat on riittävästi huomioitu ja että niistä on sovittu, mieluummin kirjallisesti osana sopimusta.

- Lokitietojen omistajuus ja luovutusoikeudet sekä –velvollisuudet.
- alassapitosopimukset ja tarvittaessa myös turvallisuusselvitykset, erityisesti silloin kun kyseessä on viranomaisten järjestelmä tai muuten kriittistä tietoa sisältävä järjestelmä.

- Toimittajan käyttöoikeuksien rajaaminen: esimerkiksi ei ole hyväksyttävää, että toimittaja käyttää yhteiskäyttöisiä[37] tunnuksia tai että ylläpitotunnus on turhan laajan joukon tiedossa.
- Toimittajan henkilöstön tekemät järjestelmäoikeuksien ja asetusten muutokset. Näistä on pidettävä kirjaa eli lokia vastaavasti kuin kyseessä olisi oman organisaation työntekijöiden tekemä työ. Erityisesti:
  - käyttöoikeuksien lisäykset tai muutokset
  - järjestelmän objekteihin kohdistuvat toimenpiteet.
  - järjestelmässä suoritettujen eräajojen lokitiedot
  - asiakirjojen jakelu esimerkiksi sähköpostikanavan kautta
  - muutokset prosessi/työnkuvamäärityksiin
  - tietokantojen lokitiedot ja tietomalliin tehdyt muutokset
  - järjestelmien parametrien tai komponenttien muutokset esimerkiksi unixin kernel-tason muutokset tai Windows-verkon toimialueen politiikan asetusten muutokset.
- Versiopäivitykset.

[37] Yhteiskäyttöiset tunnukset katkaisevat luotettavan kirjausketjun.

6 Lokien säilytys, kerääminen ja suojaaminen

Koska lokit sisältävät tietoa järjestelmien ja verkon tietoturvallisuuteen liittyvistä asioista sekä usein myös henkilö- tai tunnistamistietoja, tulee lokien suojaamiseen kiinnittää erityistä huomiota. Lokit tulee suojata niiden luottamuksellisuuden ja eheyden rikkomuksilta. Reaaliaikaisen saatavuuden varmistaminen ei yleensä ole tarpeellista, lukuun ottamatta häiriöselvitystilanteita. Saatavuuteen tulee kuitenkin kiinnittää huomiota siinä mielessä, että monien lokien maksimikoko on rajattu, esimerkiksi lokimerkintöjen määrään, tai lokitiedoston kokoon. Kun lokin maksimikoko saavutetaan, lokijärjestelmä voi ylikirjoittaa vanhoja lokimerkintöjä uusilla lokimerkinnöillä tai lopettaa lokien kirjoittamisen kokonaan. Tällöin vanhojen lokitietojen saatavuus on menetetty[38]. Lokien versiointi on tämän ongelman korjaamisen kannalta keskeistä.

Jotta pystytään vastaamaan organisaation tietojen säilytys- ja luovutusketjujen todentamisvaatimuksiin, organisaatio voi joutua säilyttämään lokitietoja pidempään kuin alkuperäinen lokitietojen tuottajasovellus tukee. Tällöin syntyy tarve lokitietojen arkistoinnille ja käytännöille arkistoinnin toteuttamiseksi. Lokien määrästä ja suuruudesta johtuen voi olla järkevää suodattaa kerättäviä lokitietoja siten, että jätetään kirjoittamatta lokiin sellaisia tietoja, joita ei tarvitse arkistoida. Luottamuksellisuuden ja eheyden toteutuminen tulee varmistaa myös lokitietoja varmistettaessa tai arkistoitaessa.

Lokit, joita ei ole suojattu riittävillä keinoilla säilytyksessä tai siirrossa, ovat alttiita sekä tahalliselle että tahattomalle muuttamiselle ja tuhoutumiselle. Esimerkiksi monet haittaohjelmat ja automaattiset tunkeutumistyökalut on suunniteltu siten, että ne muuttavat lokitietoja poistamalla tiedot haittaohjelman asennuksesta ja sen tekemistä muutoksista. Tällöin lokit eivät täytä tehtäväänsä aukottoman kirjausketjun[39] dokumentoinnissa.

---

38 Ellei vanhoja lokeja ole mahdollista palauttaa varmistuksilta.

39 Audit trail.

6.1 Lokien säilytys

Lokien säilytyksen optimointiin liittyvät seuraavat tekniikat ja toimenpiteet, joilla varmistetaan lokitietojen eheys ja täydellisyys.

6.1.1 Lokien arkistointi

Lokikierrolla tarkoitetaan lokitiedoston sulkemista ja uuden avaamista, kun lokitiedoston katsotaan olevan täynnä. Lokikierto voidaan ajoittaa tietyn aikataulun (tunneittain, päivittäin, viikoittain jne.) mukaan tai suorittaa, kun lokitiedosto saavuttaa ennalta määritellyn koon (lokimerkintöjen lukumäärä tai tiedoston koko). Lokikierron tärkeimpiä hyötyjä on kaikkien lokitietojen suojaaminen ja lokitiedostojen koon pitäminen helposti käsiteltävinä. Kun lokikierto on käytössä, täydet lokitiedostot voidaan siirtää arkistoon ja pakata/tiivistää, jotta säästetään tilaa. Lokikierron toteutuksessa käytetään usein komentojonoja, joilla lokitiedot siirretään arkistoon ja tiivistetään. Samaan komentojonoon voidaan rakentaa logiikkaa, jolla lokitiedoston sisältämät tiedot voidaan suodattaa ja ainoastaan halutut lokimerkinnät arkistoida. Käytettyyn komentojonoon voidaan toteuttaa myös analysointi, jolla voidaan myös tunnistaa mahdollisia haitallisia tai rikollisia toimia lokimerkintöjen perusteella. Vaikka monet järjestelmät, jotka tuottavat lokia, tarjoavat lokikiertoon työkaluja, komentojonoilla ja erillisillä ohjelmilla voidaan toteuttaa monipuolisia toimintoja lokikierron yhteydessä.

Lokien arkistoinnilla tarkoitetaan lokien säilyttämistä pidennetyn ajan. Lokit voidaan arkistoida tyypillisesti irrotettaville tallennusvälineille, SAN-verkkoon, erilliselle lokipalvelimelle tai lokien arkistointiin tarkoitetulle laitteelle. Lokeja tulee usein säilyttää lainsäädännöstä tai muusta säätelystä johtuen määrätty aika. Lokien arkistointi tapahtuu periaatteessa kahdella tavalla; normaalin lokikierron osana, sekä erityisistä vaatimuksista johtuvana varsinaisena arkistointina, jolloin säilytetään myös sellaista lokitietoa, joka normaalin lokikierron mukaan hävitettäisiin.

6.1.2 Lokien tiivistäminen

Lokien tiivistämisellä tarkoitetaan lokin säilyttämistä siten, että säilytykseen vaadittu tila minimoidaan ilman, että tiedoston sisältö muuttuu. Lokien tiivistäminen tapahtuu yleensä lokikierron tai lokien arkistoinnin yhteydessä. Koska lokitiedot ovat tyypillisesti tekstiä, voidaan niitä pakata tehokkaasti.

6.1.3 Lokien supistaminen

Lokien supistamisella tarkoitetaan ylimääräisten lokimerkintöjen poistamista lokista, jotta lokitiedoston kokoa saadaan pienennettyä. Lokeja voidaan supistaa poistamalla kokonaisia lokimerkintöjä tai poistamalla yksittäisistä lokimerkinnöistä tarpeettomia tietokenttiä. Lokien supistaminen tapahtuu yleensä lokien arkistoinnin yhteydessä, jolloin lokimerkinnöistä arkistoidaan ainoastaan ne tiedot, jotka ovat tarpeellisia arkistoida.

6.1.4 Lokimuunnokset

Lokimuunnoksilla tarkoitetaan lokitietojen uudelleen muotoilua ja tallentamista toiseen muotoon. Esimerkki lokimuunnoksesta on tietokantaan talletetun lokin uudelleenmuotoilu XML-muotoiseen tekstitiedostoon. Monet lokien tuottajat pystyvät tekemään muunnoksen, mutta myös erillisiä ohjelmia voidaan käyttää lokimuunnoksien tekoon. Lokimuunnoksiin liittyvät myös lokitietojen suodattaminen, yhdistely ja normalisointi.

6.1.5 Lokien normalisointi

Lokien normalisoinnissa kaikki lokitiedoston tietokentät muunnetaan tiettyyn esitysmuotoon ja luokitellaan yhdenmukaisesti. Käytännössä yleisin normalisointiin liittyvä toimenpide on lokien sisältämän aikatiedon esittäminen tietyssä muodossa. Lokia tuottavat ohjelmat voivat tuottaa lokien aikaleiman eri muodossa, esimerkiksi 12 ja 24 tunnin muodoissa. Samoin aikavyöhykkeeseen liittyy erilaisia esitystapakäytäntöjä. Lokien normalisoinnilla saadaan hyötyä ja tehokkuutta erityisesti lokitietojen analysointiin ja raportointiin, kun eri lokien tuottajien tuottama tieto on samassa muodossa. Lokien normalisointiin voi kuitenkin liittyä myös ongelmia ja se voi viedä paljon resursseja, varsinkin kun normalisoitavaa lokitietoa on paljon, ja lokimerkinnät ovat monimutkaisia. Lokitietojen esitysmuotoon kannattaa uusien tai hankittavien järjestelmien osalta kiinnittää huomiota jo määrittelyvaiheessa.

6.1.6 Lokien säilytysajat

Lokien säilytysajan määrittelyyn voidaan käyttää useita eri tapoja. Lokien säilyttämiseen ja säilytysaikoihin voi tulla ja lokin tyypistä riippuen usein tuleekin vaatimuksia eri säädöksistä ja standardeista. Säilytysaika tulee aina johtaa käyttötarkoitussidonnaisuudesta eli siitä, miksi lokia ja sen tietoja kerätään.

Esimerkiksi Arkistolaki[40] edellyttää, että lokitietojen säilytysaikaa määriteltäessä on otettava huomioon lokien merkitys asiakirjallisen tiedon alkuperäisyyden, eheyden ja luotettavuuden varmistamisessa. Sen takia asiankäsittelyjärjestelmään tallentuvat, näitä ominaisuuksia tukevat lokitiedot ovat pakollisia metatietoja, jotka on säilytettävä niin kauan kuin järjestelmä on organisaatiossa käytössä ja on siirrettävä siirtotiedostossa arkistolaitoksen vastaanotto- ja palvelujärjestelmään. Muutoin lokitietoja on säilytettävä ainakin niin kauan kuin rekisteröity voi esittää rikosperusteisia vaatimuksia henkilötietojen käsittelijää tai sivullista vastaan. Käytännössä tällöin loki tulee säilyä vähintään yhtä pitkään kuin siinä mainitut asiakirjat, tiettyjen tietojen osalta pidempään, koska asiankäsittelyjärjestelmästä hävitettävien asiakirjojen hävityksen jälkeen asiakirjan tilatiedoksi on muututtava ”hävitetty” ja tämä tulee käydä luotettavasti ilmi lokitiedoista. Samalla hävitetyn asiakirjan metatietoihin on tallennuttava asiakirjan hävittämisaika ja hävityksen tekijä, hävittämisperuste, hävittämistapa sekä hävittämisen auktorisointi. Hävitetyn asiakirjan metatietojen on jäätävä järjestelmään. Järjestelmän on voitava tuottaa raportti hävitetyistä asiakirjoista.

Tärkeää on kuitenkin määritellä lokien säilytysaika siihen vaikuttavien vaatimusten mukaan[41], ja määritellä lokikierto ja arkistointi sen mukaan. Seuraavissa kappaleissa annetaan muutamia esimerkkejä erilaisista lokityypeistä ja niiden säilytysajoista.

Tietojärjestelmän testauksessa ja usein tuotantokäytössäkin mahdollisten virhetilanteiden selvittämistä varten ja järjestelmän kuorman seuraamiseksi kerätään teknistä lokia. Tällaisia lokeja ei yleensä talleteta kovinkaan kauan ja niitä selataan ja analysoidaan yleensä yksinkertaisilla ohjelmoijan työkaluilla. Toisaalta kuormituksen pitkäaikaisvaihteluiden seuraamiseksi tarvitaan tietoja pitkältä ajalta.

Tietokantojen varmistamiseksi tietokantaa päivittävät tapahtumat kerätään talteen ja niitä talletetaan vähintäänkin varmistusvälin ajan eli niin kauan, että käytettävissä on koko tietokannasta otettu varmuuskopio ja siihen edellisen varmistuksen jälkeen tehdyt muutostapahtumat. Tavallinen säilytysaika riippuu varmistusjärjestelmästä ja se voi olla esim. 1-2 vuotta.

Laskutustietojen keräämiseksi lokiin kerätään tapahtumat, joista tilastoidaan eri tapahtumaluokkiin kuuluvat erihintaiset tapahtumat asiakkaittain. Lokitietojen säilytysaika riippuu laskutusvälistä ja maksuperusteen vanhenemisajasta.

Järjestelmän tai käyttäjien käyttömäärän tilastoimiseksi voidaan käyttää lokitietoja. Lokitietojen talletustarve riippuu tilastointimenetelmästä, yleensä maksimina pidetään yhtä kalenterivuotta.

---

[40] kts. Arkistolaitoksen sähköisten asiakirjallisten tietojen käsittelyä koskeva määräys (1486/40/2005).

[41] ml. arkistonmuodostussuunnitelma.

Kun lokitietojen säilytysaika umpeutuu, eli kun lokitietoja ei enää tarvita, tulee lokitiedot tuhota. Lokitietojen tyhjentäminen voidaan automatisoida siten, että kaikki lokimerkinnät, jotka ylittävät määritetyn päivämäärän, siirretään arkistoon ja poistetaan alkuperäisestä lokista. Tässä yhteydessä tulee huomata, että lokeja on tyypillisesti myös tallennettu varmistusnauhoille tai muille vastaaville tallennus ja arkistointivälineille, joista tiedot tulee vaatimusten mukaan myös poistaa[42].

6.2 Aikatietojen synkronointi

Lokia tuottavien järjestelmien kellojen synkronointiin tulee kiinnittää erityistä huomiota. Jotta eri järjestelmien tuottamat lokitiedot ovat keskenään yhtenäisiä ja jotta niitä voidaan yhdistellä esim. tietyn tapahtuman tai tapahtumaketjun selvittämiseen, on tärkeää, että lokien aikaleimat ovat yhtenäiset. Eri lokeja tuottavien järjestelmien aika on mahdollista synkronoida NTP:n (Network Time Protocol) avulla.

6.3 Lokien suojaus

Koska lokit ovat yleensä todisteena jostakin tapahtumasta, on erittäin tärkeää, että lokeja ei voi oikeudettomasti tuhota tai muuttaa niiden sisältöä. Pääperiaatteena voidaan todeta, että olemassa olevia tietojärjestelmien lokimerkintöjä ei pidä koskaan pystyä muuttamaan. Lokit pitää ainoastaan voida tuhota niiden määritellyn säilytysajan päätyttyä. Poikkeuksen muodostavat sellaiset lokitiedot, joiden tietoja on perustellusta syystä pystyttävä muuttamaan tai korjaamaan, mikäli jonkun lokissa olevan asian tila on muuttunut. Tällöin kyseessä on tyypillisesti jokin viranomaisen jotain asiankäsittelyä tai tilaa koskeva loki, ei esimerkiksi tietojärjestelmän audit- tai security-loki. Tällöinkin on suositeltavampaa kirjata lokiin uusi arvo ja säilyttää vanha, jolloin tietojen muutoksista muodostuu oma selkeä audit trail.

6.3.1 Käyttöoikeudet

Lokien kirjoitusoikeus tulee olla vain sillä prosessilla, joka lokia tuottaa. Järjestelmän käyttäjillä, mukaan lukien ylläpitäjät, ei tule olla kirjoitusoikeuksia

[42] Käytännössä tämä voi olla vaikeaa järjestää muutoin kun siten, että tiedot poistuvat varmistusmedioiden normaalin kierron yhteydessä. Kuitenkin on syytä miettiä mitä tietoja (lokeja) mihinkin medialle tallennetaan ja miten tämän median kierto ja käytöstä poisto on toteutettu. Kiertoja järjestelemällä turhien tietojen poistamista varmistusmedioilta voi helpottaa.

lokitiedostoihin. Myös lokimerkintöjen tuottamisprosessit tulee suojata luvattomien tahojen ja manipuloinnin varalta. Tällä tarkoitetaan, että kaikki lokien tuottamiseen käytetyt prosessit, ajettavat tiedostot, konfigurointitiedostot ja muut komponentit, jotka voivat vaikuttaa lokien tuottamiseen, pitää suojata luvattomilta muokkauksilta. Lokien suojaaminen pelkästään käyttöoikeuksin on kuitenkin vaikeaa, koska järjestelmän ylläpitäjillä on mahdollisuus ohittaa määritellyt käyttövaltuudet. Niinpä luotettava tapa lokien muuttumattomuuden varmistamiseksi on kirjoittaa lokit sellaiselle medialle, joka on kertakirjoitteinen, esimerkiksi CD-levy, paperi tai kehittyneempänä vaihtoehtona kertakirjoitteinen tiedostojärjestelmä[43].

6.3.2 Keskitetty lokijärjestelmä

Hyvä käytäntö on siirtää lokitiedostot niiden lähdejärjestelmistä keskitettyyn lokijärjestelmään joko reaaliaikaisesti tai jos se ei ole mahdollista niin eräajona. Lähdejärjestelmien ylläpitäjillä ei pidä olla mitään käyttöoikeuksia keskitetyssä lokijärjestelmässä. Keskitetyt lokijärjestelmät käyttävät usein lokitietojen keräämiseen vanhaa syslog-toteutusta, joka ei oletusarvoisesti ole turvallinen sillä,

- se käyttää UDP-protokollaa, joka ei varmista tietojen perille menoa
- sen käyttämä tietoliikenne ei ole salattua
- tietojen lähettäjää ei varmisteta eli keskitettyyn järjestelmään voi lähettää turhaa tai väärennettyä lokitietoa.

Sen sijaan on syytä käyttää jotakin turvallista syslog-toteutusta, esimerkiksi ”secure syslog”.

6.3.3 Lokitietojen katselu ja katselun suojaaminen

Myös lokitietojen katselusta eli määriteltyjen käyttöoikeuksien käytöstä on pidettävä omaa lokia. Luonnollisesti myös oikeuksien ylitysyrityksistä tulee pitää kirjaa. Monet lokijärjestelmät sisältävät toiminnallisuuden, jolla lokitietojen katselusta ja tietoihin tehdyistä hauista voidaan pitää kirjaa. Mikäli lokitietoja on mahdollista katsella lähdejärjestelmässä, on tästä vaikeampi pitää kirjaa. Sekin onnistuu, mutta ei aukottoman luotettavasti, käyttämällä tiedosto-oikeuksia ja järjestelmän kirjautumistoiminnallisuutta ja sen pitämää lokia esimerkiksi seuraavasti:

[43] write-once, read-many (WORM).

- Luodaan yksi tunnus, jolla on haluttujen lokien lukuoikeus. Millään muulla tunnuksella ei ole lukuoikeuksia.
- Estetään järjestelmään kirjautuminen tällä lokien lukuun tarkoitetulla tunnuksella
- Otetaan käyttöön su-login toiminnallisuus ja pidetään sen käytöstä kirjaa
- Pidetään kirjaa siitä, kuka on kirjautunut järjestelmään (omalla henkilökohtaisella tunnuksella).

Tällöin yhdistämällä tieto siitä, kuka on kirjautunut järjestelmään omalla tunnuksellaan ja kuka on ”ottanut käyttöönsä” lokien lukuun tarkoitetun tunnuksen käyttöoikeudet su-komennolla saadaan tieto siitä, kuka on lokitietoja lukenut. Edellä esitetty ratkaisu ei välttämättä ole mahdollista kaikilla laitteilla, kuten Windows-laitteilla ja verkon laitteilla, joten parempi tapa on siirtää lokit keskitettyyn järjestelmään ja pitää oikeuksien käytöstä kirjaa tämän järjestelmän ominaisuuksilla.

6.3.4 Tarkastussummat ja lokien eheyden varmistaminen

Lokitiedostojen eheyden varmistamiseen liittyy tarkistussumman laskeminen ja turvallinen säilyttäminen. Tarkistussumman laskemisella pyritään siihen, että arkistoituihin lokeihin tehdyt muutokset havaitaan. Tarkistussumma on tiedoston digitaalinen allekirjoitus, jonka avulla voidaan havaita pienikin bittitason muutos tiedostossa, jonka jälkeen laskettu tarkistussumma on erilainen kuin alkuperäisessä. Yleisimmin käytettyjä tekniikoita tarkistussumman laskemiseen ovat MD5[44] ja SHA-1[45] algoritmit. Mikäli lokitiedostoa muokataan ja sen tarkistussumma lasketaan uudelleen, se ei enää täsmää alkuperäiseen ja osoittaa, että lokitiedosto on muuttunut. Tämän vuoksi on tärkeää, että myös lokitiedostojen tarkistussummat säilytetään siten, että niitä ei päästä muuttamaan tai poistamaan. Sekä MD5 että SHA-1 algoritmeissa on havaittu tietoturvapuutteita, jotka ainakin teoriassa mahdollistaisivat lokitietojen muuttamisen siten, että tarkistussumma edelleen täsmää. Mikäli käytetyt tuotteet mahdollistavat, kannattaa käyttää vahvempia tiivistefunktioita, esimerkiksi SHA-512/384.

6.4 Järjestelmien virhetilanteet ja lokit

Jokainen lokitietoa tuottava järjestelmä tulee suojata. Lokia tuottavat järjestelmät tulee konfiguroida siten, että ne tuottavat tarvittavaa lokia myös virhe-

[44] message-digest-algorithm.

[45] Secure Hash Algorithm.

tilanteissa. Mikäli lokia tuottavan järjestelmän tapahtumien seuraaminen on todella tärkeä, voi olla tarpeellista, että itse järjestelmä ajetaan alas, mikäli se ei enää pysty tuottamaan lokia. Tällöin järjestelmä ei lokien kirjaamiseen liittyvissä virhetilanteissa toimi lainkaan.

Liite 1

Tässä liitteessä esitetään esimerkki lokien syntymisestä ja niiden käsittelyiden vastuista. Skenaarioksi on valittu tilanne, jossa organisaatiolla on webpohjainen sähköpostipalvelu, jota käyttäjä käyttää selaimella. Organisaatio on ulkoistanut palvelinten ylläpidon (tunnistamis- ja sähköpostipalvelin), verkon ylläpidon ja sähköpostipalvelun kehittämisen.

Esimerkissä käydään läpi, mitä lokeja sähköpostin lähettämisen yhteydessä kirjoitetaan ja karkealla tasolla vastuut, joita lokien käsittelyyn liittyy. Tämä esimerkki ei sisällä kaikkia mahdollisia lokeja, joihin merkintöjä syntyy, eikä myöskään yksityiskohtaisia vastuita. Lisäksi vastuut voi tilanteesta riippuen olla jaettu myös eri tavalla.

Eri toimijat ja vastuut

On tärkeää, että eri toimijoiden vastuut ja roolit on määritelty tarkasti, jotta lokien seurantaan ja tallentamiseen ei jää niin sanottuja 'mustia aukkoja', eli lokeja, joita kukaan ei käsittele. Lokien käsittely tulee määritellä jo sopimusvaiheessa, sillä myöhemmin niistä sopiminen voi olla haastavaa.

Alla on määritelty tyypillinen tilanne vastuiden osalta:

- Organisaatio (1)
  - Määritellä vaatimukset kaikille lokituksen osa-alueille ja sopimusten kautta saada ulkoistuskumppanit toimimaan vaatimusten mukaisesti.
  - Määritellä käytännöt ja vastuut hätätilanteessa toimimiseksi. Toimittajat on hyvä velvoittaa siihen, että niiden tulee hälyttää, mikäli havaitsevat epäilyttäviä lokimerkintöjä.
  - Mikäli jokin ulkoinen standardi koskee lokitusta (kuten PCI-DSS), varmistaa, että oman lokienkäsittelyn lisäksi ulkoistuskumppanit käsittelevät lokeja standardin vaatimusten mukaisesti.
  - Määritellä lokien omistajuus ja toiminta tilanteissa, joissa tarvitaan lokeja useammalta toimijalta.
  - Käsitellä sovelluslokeja.

- Infraylläpidosta vastaava yritys (2)
  - Kerätä käyttöjärjestelmän ja tietokannan tekemiä lokeja ja turvata ne asiakkaan vaatimusten mukaisesti.
  - Seurata lokeja asiakkaan vaatimusten mukaisesti.

- Verkon ylläpidosta vastaava yritys (3)
  - Kerätä verkon laitteiden tekemää lokia ja turvata ne asiakkaan vaatimusten mukaisesti.
  - Seurata lokeja asiakkaan vaatimusten mukaisesti.

- Sähköpostiohjelmaa kehittävä yritys (4)
  - Kehittää ohjelman lokitoimintoja asiakkaan vaatimusten mukaisesti.

- Käyttäjä (5)
  - Suojata omaa yksityisyyttään poistamalla tarvittaessa selaimen kirjoittama loki.

Eri paikkoihin syntyvä loki

Kunkin kohdan perässä suluissa kyseisestä lokista vastaava taho yllä olevan numeroinnin mukaisesti.

1. Käyttäjä siirtyy selaimellaan www-pohjaisen sähköpostipalvelun etusivulle

- Selaimen lokiin jää tieto vierailtavasta sivustosta. (5)
- Palomuuri pääsynvalvontaloki (fw.log): käyttäjän yhteydenavaus työasemalta www- palvelimelle. (3)
- WWW-palvelimen yhteyden salausohjelmiston loki (ssl_engine_log): Käyttäjän selaimen palvelimelle avaaman SSL-suojatun yhteyden muodostuminen. (2)
- WWW-palvelimen virheloki (error_log): Käyttäjän selain pyytää www-palvelimelta automaattisesti tiedostoa, jota kyseisellä sivustolla ei ole. Tästä syntyy virhemerkintä lokitiedostoon. (2)
- WWW-palvelimen sovellusloki (access_log): Käyttäjän selaimen http-pyynnöt vastauskoodeineen. Kaikki www-palvelimelta asiakkaan selaimeen toimitettujen web-sivujen ja web-sivuilla olevien elementtien kuten kuvien URL-osoitteet päätyvät lokitiedostoon. (2)
- WWW-palvelimen web-sähköpostisovelluksen sovellusloki (horde.log): Tieto kirjautumissivun käynnistämisestä. (1)

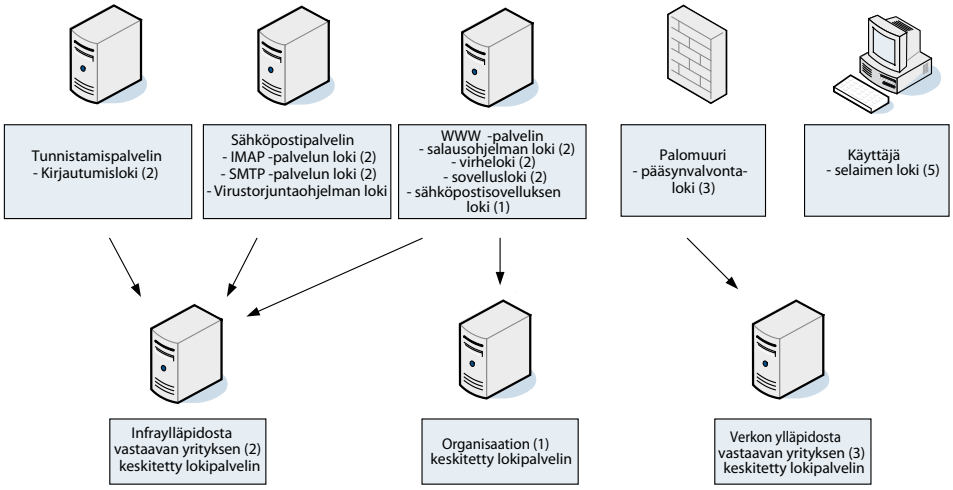
2. Käyttäjä syöttää käyttäjätunnuksensa ja salasanansa www- selaimensa kautta www-sivulle ja kirjautuu www-pohjaiseen sähköpostipalveluun

- WWW-palvelimen sovellusloki (access_log): Käyttäjän selaimen http-pyynnöt vastauskoodeineen. (2)
- Palomuuri pääsynvalvontaloki (fw.log): www-palvelimen yhteydenavaus sähköpostipalvelimelle. (3)
- Sähköpostipalvelimen IMAP-palvelun loki (syslog): yhteyden avauspyyntö www- palvelimelta ohjataan eteenpäin tunnistamispalvelimelle. (2)
- Palomuuri pääsynvalvontaloki (fw.log): sähköpostipalvelimen yhteydenavaus tunnistamispalvelimelle. (3)
- Tunnistamispalvelimen kirjautumisloki (krb5kdc.log): Kirjautumistiketti annettu sähköpostipalvelimen käyttöön. (2)
- Sähköpostipalvelimen IMAP-palvelun loki (syslog): Käyttäjä tunnistettu ja kirjautuminen sähköpostipalvelimelle on onnistunut. (2)
- WWW-palvelimen web-sähköpostisovelluksen sovellusloki (horde.log): Käyttäjä tunnistettu ja kirjautuminen www-sovellukseen on onnistunut. (1)
- WWW-palvelimen sovellusloki (access_log): Käyttäjän selaimen http-pyynnöt vastauskoodeineen. (2)

3. Käyttäjä avaa sähköpostin lähettämiseen tarvittavan näkymän, kirjoittaa viestin ja lähettää sen eteenpäin

- WWW-palvelimen sovellusloki (access_log): Käyttäjän selaimen http-pyynnöt vastauskoodeineen. (2)
- WWW-palvelimen SMTP-palvelun sovellusloki (maillog): Merkintä käyttäjän sähköpostin jakeluun ottamisesta sekä merkintä sähköpostin lähetyksestä salatussa yhteydessä erilliselle sähköpostipalvelimelle. (2)
- Palomuuri pääsynvalvontaloki (fw.log): WWW- palvelimen yhteydenavaus sähköpostipalvelimelle. (3)
- Sähköpostipalvelimen SMTP-palvelun sovellusloki (maillog): Merkintä sähköpostin vastaanottamisesta www-palvelimelta edelleen välittämiseksi. (2)
- Sähköpostipalvelimen virustorjuntapalvelun sovellusloki (syslog): Merkintä sähköpostin virus- sekä roskapostitarkistuksen suorittamisesta. (2)
- Sähköpostipalvelimen SMTP-palvelun sovellusloki (maillog): Merkintä sähköpostin välittämisestä edelleen vastaanottajalle. (2)
- Palomuuri pääsynvalvontaloki (fw.log): Sähköpostipalvelimen yhteydenavaus sähköpostin kohdeorganisaation sähköpostipalvelimelle. (3)

Lokien synty www-pohjaisessa sähköpostipalvelussa



Yllä olevassa kuvassa on esitetty esimerkin lokien muodostuminen eri laitteissa sekä niiden kerääminen keskitettyihin lokipalvelimiin eri organisaatioissa. Nyt kuvattujen lokien lisäksi tavallisesti tilanne on vielä monimutkaisempi ja lokien hallinnassa pitää ottaa huomioon vielä useampia erilaisia laitteita, kuten seuraavat:

- organisaation sisäverkossa olevat loppukäyttäjän työasemat
- DNS -palvelimen lokit
- muut kuin sähköpostipalveluun liittyvät palvelut, joita käyttäjät käyttävät.

Edellä mainitut lisäelementit pystytään kuitenkin hallitsemaan, kun lokien käsittelyyn liittyvät prosessit otetaan käyttöön kokonaisvaltaisesti, eikä unohdeta sitä, että palvelua tarjoava organisaatio on kokonaisvastuussa tuotetusta palvelusta ja sen lokeihin liittyvistä prosesseista.

Haasteita lokien keräämisessä ja analysoinnissa:

- Esimerkissä eri järjestelmien lokitiedot päätyvät eri toimijoiden analysoitaviksi. Tällöin niiden käyttö hyökkäysten havaitsemiseksi on haastavampaa kuin jos kaikki lokit olisivat saman tahon analysoitavissa.
- Esimerkissä olevien lokitietojen käsittelyssä tarvitaan mm. http-, Kerberos-, IMAP4-, SMTP-, SSL/TLS-protokollien toiminnan tuntemusta sekä ymmärrystä tietoliikenneverkon ja sen palveluiden toiminnasta.

Lokitietojen pohjalta käyttäjän ja järjestelmien toiminta on selvitettävissä tarvittaessa melko tarkasti. Samalla myös virhetilanteet ovat tunnistettavissa.

Tietoturvapoikkeamiin reagointi

Edellä kuvatussa esimerkissä lokeja syntyy moniin eri paikkoihin eri organisaatioiden toimesta. Lokien analysointi ja niihin reagointi on esimerkissä jaettu usean eri organisaation kesken, joten vastuu poikkeamien reagointiin on kaikilla. Tässä kuvataan esimerkkitilanne, kun infraylläpidosta vastaava yritys (2) havaitsee hyökkäyksen omista lokeistaan. Tilanne etenee seuraavalla tavalla

1. Infraylläpidosta vastaava yritys (2) havaitsee lokeja analysoidessaan, että palveluun kohdistuu hyökkäys muutamasta ip-osoitteesta.
2. Infrayllläpidosta vastaava yritys (2) ilmoittaa heti asiakkaan (1) yhteyshenkilölle, että he havaitsivat hyökkäyksen ja kertoo hyökkäyksen olennaiset tiedot (millainen hyökkäys on ja mistä ip-osoitteista se kohdistuu heihin)
3. Organisaation (1) yhteyshenkilö ottaa yhteyttä verkon ylläpidosta vastaavan tahon (3) yhteyshenkilöön ja ilmoittaa tilanteesta ja kysyy, havaitsevatko he lokeissa vastaavaa toimintaa. He vahvistavat hyökkäyksen ja yhdessä sovitaan, että palomuurissa estetään liikennöinti kyseisistä osoitteista.

Edellä kuvatussa esimerkissä ripeä ja oikea toiminta perustuu

- säännöllisiin (mielellään reaaliaikaiseen) lokien seurantaan
- ennalta sovittuihin vastuisiin ja yhteyshenkilöihin.

Edellisten puuttuessa onnistuneella hyökkäyksellä olisi voitu aiheuttaa vahinkoa, mikäli sitä ei olisi havaittu tai mikäli siihen reagointi olisi kestänyt liian kauan.

Tarkastuslista

Jokaisessa palvelussa ja organisaatiossa on infrastruktuurin tuomia erityispiirteitä sekä liiketoiminnan tuomia vaatimuksia, joten kattavan tarkastuslistan tekeminen on mahdotonta ja palvelua rakennettaessa onkin syytä miettiä oman toiminnan lähtökohtien perusteella vaatimuksia lokitukselle. Alla on kuitenkin listattu yleisiä vaatimuksia, joita tulisi jokaisen järjestelmän kehityksessä ottaa huomioon:

- onko lokituksen tavoite ja tarkoitus määritelty
- onko sovellusten tuottama lokitieto määritelty
- pystytäänkö lokeihin merkitty toimenpiteen tekijä aina yhdistämään oikeaan henkilöön, vai käytetäänkö yhteiskäyttöisiä tunnuksia
- mikäli joitakin toimintoja on ulkoistettu, onko lokien omistajuus hyvin määritelty
- miten hoidetaan tilanne, jossa loki tai lokipalvelin täyttyy lokitiedoista
- onko sovelluksen tuottamassa lokissa kaikki tarpeellinen tieto, kuten käyttäjä, kellonaika ja selitys tapahtumasta
- miten pääsynvalvonta lokijärjestelmään on järjestetty ja miten se estää oikeudettoman pääsyn lokeihin
- onko lokien muuttumattomuus varmistettu
- onko lokien säilytysaika määritetty ja miten säilytys on hoidettu
- onko prosessit lokien käsittelyyn hyvin määritelty ja vastuutettu
- onko prosessit lokeissa havaittujen poikkeamien hallintaan hyvin määritetty
- pysyvätkö eri järjestelmien kellot samassa ajassa
- onko yritysten välillä sovittu yhteyshenkilöt, joihin otetaan yhteyttä, kun lokeista selviää jotain epäilyttävää.

Liite 2

Lokiohjeen lainsäädäntöliite

HENKILÖTIETOLAKI (523/1999)

Henkilötietolain tarkoituksena on turvata yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.

Lokien käsittelyyn liittyy kaksi keskeistä käsitettä: henkilötieto ja henkilörekisteri.

Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä eli ihmistä, hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskevaksi. Tyypillisiä henkilötietoja ovat nimi ja osoite. Tässä yhteydessä kyseeseen voi tulla esimerkiksi sähköpostiosoite tai IP-osoite, josta voidaan jäljittää yksittäinen tietokoneen käyttäjä.

Henkilörekisterillä puolestaan tarkoitetaan käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuvaa henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta. Sähköisen tietojärjestelmän sisältämä lokitiedosto muodostaa käytännössä lain määritelmän mukaisen henkilörekisterin, mikäli sinne on tallentunut vaikkapa käyttäjän sähköpostiosoite tai IP-osoite.

Soveltamisala

Henkilötietolaki on yleislaki, jota sovelletaan aina henkilötietoja käsiteltäessä, mikäli kyseiseen tilanteeseen ei ole säädetty erityislakia

Millaista lokia laki koskee:

Laki koskee jollekin alustalle talletettua henkilötietoja sisältävää lokia. Laki koskee henkilötietoa käsittelevää virastoa, yritystä, järjestöä tai muuta yhteisöä.

Käsittelyn periaatteet

Lain mukaan henkilötietojen käsittelyä on henkilötiedon kerääminen, tallentaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen, suojaaminen, poistaminen, tuhoaminen sekä muu henkilötietoihin kohdistuva toimenpide.

Laki edellyttää henkilötietojen käsittelijän noudattavan useita yksityisyyden suojaksi säädettyjä periaatteita. Ennen kuin henkilötietoja saa alkaa keräämään henkilörekisteriksi, tulee käsittelijän määritellä henkilötietojen käsittelyn tarkoitus. Määrittely on tarpeen sen vuoksi, että laki edellyttää käsittelyn olevan

asiallisesti perusteltua organisaation toiminnan kannalta. Määrittely tuleekin tehdä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamisen vuoksi kyseistä henkilörekisteriä pidetään.

Edellä mainittuun suunnitteluvelvoitteeseen liittyy kiinteästi lain asettama käyttötarkoitussidonnaisuus. Henkilötietoja saa käsitellä vain tavalla, joka on yhteensopiva rekisterinpitäjän määrittelemän tarkoituksen eli organisaation toiminnan kannalta perustellun tarpeen kanssa.

Laki edellyttää käsittelijältä myös yksittäisten henkilötietojen laaduntarkkailua. Tällä tarkoitetaan sitä, että rekisterissä olevan henkilötiedon on oltava tarpeellinen organisaation tehtävän kannalta. Esimerkiksi osoiterekisteriin ei liene tarpeen tallettaa henkilötunnusta. Toinen laaduntarkkailuun liittyvä vaatimus on henkilötiedon virheettömyys. Rekisterinpitäjän tulee huolehtia siitä, ettei rekisteri sisällä virheellisiä tai vanhentuneita henkilötietoja.

Rekisterinpitäjän tulee suojata pitämänsä rekisteri teknisesti siten, että henkilötiedot ovat turvassa asiattomalta pääsyltä sekä vahingossa tai laittomasti tapahtuvalta hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta käsittelyltä. Edellä mainitut vaatimukset koskevat luonnollisesti myös lokitietoja silloin kun lokeissa on henkilötietoja.

Lokin sisältö

Lokitiedoston sisältämän henkilötiedon voi luokitella julkisuusasteen mukaan julkiseksi tai salassa pidettäväksi. Viranomaisten toiminnan julkisuudesta annetun lain (julkisuuslaki) pääsäännön mukaisesti viranomaisten asiakirjat ovat julkisia. Saman lain 24 §:n luettelon tai jonkin erityislain määräyksen perusteella useat henkilötietoja sisältävät asiakirjat ovat puolestaan salassa pidettävä.

Henkilötietolaissa on säädetty arkaluontoisten henkilötietojen käsittelykielto (11 §) ja poikkeukset siitä (12 §).

Huomiot

Lakia tulkitseva viranomaisia ovat tietosuojavaltuutettu ja tietosuojalautakunta, jotka valvovat henkilötietojen käsittelyä ja antavat henkilötietojen käsittelyä koskevaa ohjausta ja neuvontaa.

LAKI VIRANOMAISTEN TOIMINNAN JULKISUUDESTA (621/1999)

Lain tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan.

Soveltamisala

Laissa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan henkilön vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista.

Käsittelyn periaatteet

Käsittely on avointa, ellei julkisuuslaissa tai muussa laissa toisin säädetä.

Lokin sisältö

Julkisuuslaki kattaa kaikenlaiset lokitiedostoihin sisältyvät tiedot silloin kun kyse on viranomaisen tietojärjestelmään kuuluvasta lokista, eli viranomaisen asiakirjasta.

Huomiot

Laki koskee ainoastaan viranomaisten toimintaa.

LAKI YKSITYISYYDEN SUOJASTA TYÖELÄMÄSSÄ (759/2004)

Laki yksityisyyden suojasta työelämässä on säädetty toteuttamaan yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Kyseessä on erityislaki, jonka vaietessa jostakin kysymyksestä sovelletaan yleislakia eli henkilötietolakia. Tässä laissa työntekijällä tarkoitetaan myös virkasuhteessa olevaa henkilöä.

Soveltamisala

Lakia sovelletaan työntekijää koskevien henkilötietojen käsittelyyn, työntekijälle tehtäviin testeihin ja tarkastuksiin sekä niitä koskeviin vaatimuksiin, tekniseen valvontaan työpaikalla sekä työntekijän sähköpostiviestin hakemiseen ja avaamiseen.

Teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestäminen työpaikalla kuuluvat yhteistoiminnasta yrityksissä annetussa laissa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin.

Käsittelyn periaatteet

Lain mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät palvelussuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai heille tarjottuihin etuuksiin taikka johtuvat työtehtävien erityisluonteesta.

Työnantajan on kerättävä työntekijää koskevat henkilötiedot ensi sijassa tältä itseltään. Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, on tältä hankittava suostumus tietojen keräämiseen.

Työnantajan on ilmoitettava työntekijälle etukäteen tätä koskevien tietojen hankkimisesta luotettavuuden selvittämistä varten. Jos työntekijää koskevia tietoja on kerätty muualta kuin tältä itseltään, työnantajan on ilmoitettava saamistaan tiedoista ennen kuin niitä käytetään työntekijää koskevassa päätöksenteossa.

Työnantajalla on oikeus hakea esille tai avata työntekijän sähköpostiviestejä ainoastaan silloin, jos hän on järjestänyt työntekijälle tämän nimellä lähetettyjen ja tämän lähettämien sähköpostiviestien suojan toteuttamiseksi tarpeelliset toimenpiteet. Lain vaatimia toimenpiteitä ovat automaattinen vastaustoiminto työntekijän poissaolotapauksissa, saapuvien viestien ohjaaminen kollegalle tai työnantajan hyväksymään työntekijän toiseen (yksityiseen) sähköpostiosoitteeseen. Työntekijä voi myös antaa suostumuksensa siihen, että työnantajan hyväksymä henkilö työpaikalla voi vastaanottaa viestit sen selvittämiseksi, onko kyseessä työtehtävien hoitamiseksi tarkoitettu viesti.

Työnantajalla on oikeus tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla ottaa viestin lähettäjää, vastaanottajaa tai viestin otsikkoa koskevien tietojen perusteella selville, onko poissaolevalle työntekijälle lähetetty viestejä, joista työnantajan on toimintansa vuoksi välttämätöntä saada tieto, jos:

1. työntekijä hoitaa tehtäviä itsenäisesti työnantajan lukuun eikä työnantajan käytössä ole järjestelmää, jonka avulla työntekijän hoitamat asiat ja niiden käsittelyvaiheet kirjataan tai saadaan muutoin selville;
2. työntekijän tehtävien ja vireillä olevien asioiden vuoksi on ilmeistä, että työnantajalle kuuluvia viestejä on lähetetty tai vastaanotettu;
3. työntekijä on estynyt tilapäisesti suorittamasta työtehtäviään eikä työnantajalle kuuluvia viestejä siitä huolimatta, että työnantaja on huolehtinut edellä mainituista velvollisuuksistaan, voida saada työnantajan käyttöön; ja
4. työntekijän suostumusta ei voida saada kohtuullisessa ajassa ja asian selvittäminen ei kestä viivytystä.

Jos sähköisen viestin lähettäjää tai vastaanottajaa taikka viestin otsikkoa koskevan tiedon perusteella on ilmeistä, että työntekijälle lähetetty tai työntekijän lähettämä viesti on selvästi työnantajalle kuuluva viesti, jonka sisällöstä työnantajan on toimintaansa liittyvien neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai toimintojensa turvaamiseksi välttämätöntä saada tieto, eikä viestin lähettäjään tai vastaanottajaan saada yhteyttä viestin sisällön selvittämiseksi tai sen lähettämiseksi työnantajan osoittamaan osoitteeseen, työnantaja saa avata viestin tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla toisen henkilön läsnä ollessa.

Lokin sisältö

Laki koskee työnantajan tietojärjestelmään kuuluvaa lokia, jonka sisältämästä henkilötiedosta voidaan tunnistaa yksittäinen työntekijä, esimerkiksi kulunvalvontaloki työpaikalla. Mikäli työnantaja hakee esille tai avaa työntekijälle kuuluvan viestin edellä esitetyin perustein, tulee tästä toimesta pitää kirjaa, eli tehdä lokimerkintä.

Huomiot

Lain noudattamista valvovat työsuojeluviranomaiset ja tietosuojavaltuutettu. Työnantajan tulee pitää tämä laki työntekijöiden nähtävillä työpaikalla. Tähän riittänee se, että työntekijällä on mahdollisuus lukea lakia internetin välityksellä.

SÄHKÖISEN VIESTINNÄN TIETOSUOJALAKI (526/2004)

Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.

Soveltamisala

Lakia sovelletaan yleisissä viestintäverkoissa tarjottaviin verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin ja palveluihin, joissa käsitellään palvelun käyttöä kuvaavia tietoja. Lisäksi lakia sovelletaan suoramarkkinointiin yleisissä viestintäverkoissa sekä tilaajaluettelopalveluihin ja numerotiedotuspalveluihin.

Käsittelyn periaatteet

Tietojärjestelmien toiminnasta ja käytöstä tallentuu lokeja, joiden käsittely on mahdollista tämän lain säätelemissä puitteissa seuraavia tarkoituksia varten:

- palvelun toteuttamiseksi, kehittämiseksi ja sen tietoturvasta huolehtimiseksi
- mahdollisten ongelmien ja teknisten vikojen havaitsemiseksi ja korjaamiseksi

Tietojärjestelmien toiminnasta ja käytöstä tallentuu lokia sekä lokiin tunnistamistietoja. Tunnistamistietojen käsittely on viestinnän välittäjän mahdollista seuraavia tarkoituksia varten:

- palvelun toteuttamiseksi, kehittämiseksi ja sen tietoturvasta huolehtimiseksi
- mahdollisten ongelmien ja teknisten vikojen havaitsemiseksi ja korjaamiseksi
- palveluun kohdistuvien laskutuksen ohittamiseen liittyvien tai siihen rinnastettavien väärinkäytösten havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.

Lokin sisältö

Tunnistamistietoja.

Huomiot

Lain ja sen nojalla annettujen määräysten noudattamista valvoo pääasiassa Viestintävirasto kun taas esim. paikkatietojen käsittelyä ja automatisoitujen järjestelmien avulla tapahtuvaa suoramarkkinointia koskevien säädösten noudattamista valvoo tietosuojavaltuutettu.

JULKISUUSASETUS (1030/1999)

Edellä käsitellyn julkisuuslain sisältämän delegointisäännöksen nojalla on annettu julkisuusasetus, jonka tavoitteena on edistää viranomaistoiminnan julkisuutta ja hyvää tiedonhallintatapaa.

Soveltamisala

Asetuksella täydennetään julkisuuslain 5 luvussa säädettyä viranomaisen velvollisuutta edistää tiedonsaantia ja hyvää tiedonhallintatapaa.

Käsittelyn periaatteet

Asetuksessa määritellään käsite erityissuojattava tietoaineisto. Sen mukaan salassa pidettävät asiakirjat voidaan luokitella kolmeen eri luokkaan sen mukaan, millaisia tietoturvavaatimuksia on lokitiedostoja käsiteltäessä noudatettava..

Ensimmäiseen luokkaan kuuluu tietoaineisto, jonka oikeudeton paljastuminen ja käyttö aiheuttaisi vakavaa vahinkoa julkisuuslain 24 §:n kohdissa 1,2,5 sekä 8–11 tarkoitetuille yleisille eduille.

Toiseen luokkaan kuuluu tietoaineisto, jonka oikeudeton paljastuminen ja käyttö loukkaisi merkittävästi niitä etuja, joiden vuoksi rajoitukset on säädetty.

Kolmanteen luokkaan kuuluu tietoaineisto, jonka paljastuminen ja käyttö vaarantaisi viranomaisen toimintaedellytyksiä tai liike- ja ammattisalaisuuksia tai henkilötietojen suojaa.

Lokit kuuluvat tyypillisesti salassa pidettäviin asiakirjoihin ja lokin tyypistä ja sisällöstä riippuen johonkin edellä mainituista luokista.

Erityissuojattavaa tietoaineistoa koskevat asetuksessa annetut yleiset tietoturvallisuustoimenpiteet. Lokitiedostoja käsiteltäessä on toteutettava luokitusta vastaavat asianmukaiset toimenpiteet siten, että

- tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
- tietojärjestelmiin pääsy on valvottua sekä luvaton tunkeutuminen niihin estetään käytettävissä olevin keinoin;
- tietoaineistoja käsittelevät vain ne, joiden tehtäviin asian käsittely kuuluu;
- tietoja luovuttavat vain ne, joiden tehtäviin siitä huolehtiminen kuuluu;
- tietoverkoissa siirrettävä tieto salataan tarpeen mukaan.

Lokin sisältö

Julkisuusasetus kattaa kaikenlaiset lokitiedostoihin sisältyvät tiedot silloin kun kyse on viranomaisen tietojärjestelmään kuuluvasta lokista, eli viranomaisen asiakirjasta

Huomiot

Asetus koskee ainoastaan viranomaisen toimintaa.

LAKI SANANVAPAUDEN KÄYTTÄMISESTÄ STA JOUKKOVIESTINNÄSSÄ (460/2003)

Lailla turvataan perustuslain mukaisen sananvapauden toteutuminen joukkoviestinnässä. Lakia sovellettaessa ei viestintään saa puuttua enempää kuin on välttämätöntä ottaen huomioon sananvapauden merkitys kansanvaltaisessa oikeusvaltiossa.

Soveltamisala

Lakia sovelletaan Suomessa harjoitettavaan julkaisu- ja ohjelmatoimintaan.

Käsittelyn periaatteet

Julkaisijan tulee määrätä aikakautiselle julkaisulle ja verkkojulkaisulle vastaava toimittaja. Ohjelmatoiminnan harjoittajan tulee määrätä ohjelmaa varten vastaava toimittaja.

Julkaisijan on huolehdittava siitä, että julkaisussa, aikakautisessa julkaisussa ja verkkojulkaisussa on tieto julkaisijasta. Julkaisijan ja vastaavan toimittajan on huolehdittava siitä, että aikakautisessa julkaisussa ja verkkojulkaisussa on tieto myös vastaavasta toimittajasta.

Ohjelmatoiminnan harjoittajan ja vastaavan toimittajan on huolehdittava siitä, että ohjelmatoiminnassa tiedotetaan ohjelmatoiminnan harjoittajasta ja vastaavasta toimittajasta.

Tietojen käsittelyä joukkoviestinnässä koskee vastine- ja oikaisuoikeudet:

Vastineoikeus tarkoittaa, että yksityisellä henkilöllä, jolla on perusteltu syy katsoa aikakautisessa julkaisussa, verkkojulkaisussa tai niihin rinnastettavassa, toistuvasti lähetettävässä ohjelmassa esitetyn viestin loukkaavan itseään, on oikeus saada vastine julkaistuksi samassa julkaisussa tai ohjelmassa.

Oikaisuoikeus tarkoittaa, että yksityisellä henkilöllä, yhteisöllä ja säätiöllä sekä viranomaisella on oikeus saada aikakautisessa julkaisussa, verkkojulkaisussa tai ohjelmassa esitetty itseään tai toimintaansa koskeva virheellinen tieto oikaistuksi samassa julkaisussa tai asianomaisen ohjelmatoiminnan harjoittajan ohjelmassa, jollei tiedon oikaiseminen virheen vähäisyyden vuoksi ole ilmeisen tarpeetonta.

Lain soveltamisalaan kuuluu esimerkiksi sanomalehdet, aikakauslehdet, televisio- ja radio-ohjelmat sekä yleiseen käyttöön tarkoitetut internet-sivustot.

Lokin sisältö

Tunnistamistietoja.

LAKI TIETOYHTEISKUNTAPALVELUIDEN TARJOAMISESTA (458/2002)

Laki sääntelee tietoyhteiskunnan palvelujen tarjoamiseen liittyviä seikkoja, erityisesti sähköistä kaupankäyntiä Euroopan talousalueella.

Soveltamisala

Lain soveltamisalaan kuuluu palvelujen tarjoamisen vapaus, palvelun tarjoajien velvollisuus antaa tietoja, sopimusta koskevien muotovaatimusten täyttäminen sähköisesti sekä välittäjänä toimivien palvelun tarjoajien vastuuvapauskysymykset.

Käsittelyn periaatteet

Palvelujen tarjoajien tulee pitää asiakkaidensa saatavilla laissa määritellyt tiedot itsestään ja toiminnastaan. Palvelun tarjoajien täytyy myös antaa asiakkailleen ohjeita ja tietoja palvelun sisällöstä ennen sähköisen tilauksen tekemistä sekä järjestää kuluttajien käyttöön menettelyt, joiden avulla mahdolliset virheet tilauksissa voidaan etukäteen havaita ja korjata. Käytännössä tämä tarkoittaa käyttäjän antamien tietojen muototarkistuksia ja mahdollisten virheiden jälkikäteistä selvittelyä varten myös tapahtumien kirjaamista lokiin.

Lokin sisältö

Sähköisissä tilauksissa lokitiedostoihin sisältyy tyypillisesti henkilötiedoiksi katsottavia nimi- ja osoitetietoja samoin kuin henkilöiden pankkiyhteystietoja.

Huomiot

Lain noudattamista valvoo Viestintävirasto ja kuluttaja-asiamies omaan toimivaltaansa kuuluvissa asioissa.

ARKISTOLAKI (831/1994)

Laki sääntelee julkista tehtävää hoitavan tahon arkistoja ja arkistonmuodostusta.

Soveltamisala

Laki koskee valtion ja kuntien viranomaisia, muita itsenäisiä julkisoikeudellisia laitoksia, valtion ja kuntien liikelaitoksia, ortodoksista kirkkoa sekä muita yhteisöjä ja yksityisiä niiden hoitaessa julkista tehtävää. Eduskuntaan ja sen viranomaisiin lakia sovelletaan eräin osin. Arkistoon kuuluvat asiakirjat, jotka ovat saapuneet arkistonmuodostajalle sen tehtävien johdosta tai syntyneet arkistonmuodostajan toiminnan yhteydessä.

Arkistoon kuuluvat asiakirjat, jotka ovat saapuneet arkistonmuodostajalle sen tehtävien johdosta tai syntyneet arkistonmuodostajan toiminnan yhteydessä.

Käsittelyn periaatteet

Arkistonmuodostajan on määrättävä tehtävien hoidon tuloksena kertyvien asiakirjojen säilytysajat ja -tavat sekä ylläpidettävä niistä arkistonmuodostussuunnitelmaa. Asiakirjojen säilytysaikoja määrättäessä on otettava huomioon, mitä niistä on erikseen säädetty tai määrätty.

Arkiston muodostamiseen ja käsittelyyn liittyviä lokitietoja on säilytettävä ainakin niin kauan kuin rekisteröity voi esittää rikosperusteisia vaatimuksia henkilötietojen käsittelijää tai sivullista vastaan. Käytännössä tämä loki tulee säilyä vähintään yhtä pitkään kuin siinä mainitut asiakirjat, tiettyjen tietojen osalta pidempään, koska asiankäsittelyjärjestelmästä hävitettävien asiakirjojen hävityksen jälkeen asiakirjan tilatiedoksi on muututtava ”hävitetty”. Samalla hävitetyn asiakirjan metatietoihin on tallennuttava asiakirjan hävittämisaika ja hävityksen tekijä, hävittämisperuste, hävittämistapa sekä hävittämisen auktorisointi. Hävitetyn asiakirjan metatietojen on jäätävä järjestelmään. Järjestelmän on voitava tuottaa raportti hävitetyistä asiakirjoista.

Lokin sisältö

Loki sisältää tietoa arkiston alkuperäisyyden eheyden ja luotettavuuden varmistamiseksi sekä käsittelyn todentamiseksi. Käsittelyoikeuksista ja niiden muutoksista on ylläpidettävä lokia. Järjestelmässä tulee olla mahdollista erilaisin lokitietojen lajittelukriteerein seurata ja valvoa järjestelmätapahtumia. Lokitietoja on voitava lajitella ainakin kohteittain (tapahtumatyyppi), tekijöittäin (käyttäjä) ja tapahtuma-ajoittain

Huomiot

Arkistolaitoksen tehtäviin kuuluu myös arkistotoimen ohjaaminen, kehittäminen ja tutkiminen.Arkistolaitos määrää, mitkä asiakirjat tai asiakirjoihin sisältyvät tiedot säilytetään pysyvästi.

Liite 3

Olemassa olevan VAHTI-ohjeistuksen asettamat vaatimukset

VAHTI 3/2007 - Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan

Ohje asettaa seuraavat lokien käsittelyyn liittyvät vaatimukset:

- Lokien kerääminen ja tallentaminen tulee järjestää niin, että niitä ei päästä muuttamaan tai poistamaan tietomurtojen yhteydessä.
- Osa lokien sisältämästä tiedosta on säädösten mukaan luottamuksellista ja suojataan valtuuttamattomalta käsittelyltä.

VAHTI 2/2007 - Älypuhelimien tietoturvallisuus

- Push-Mail-ratkaisuiden yhteydessä tulee selvittää millaiset oikeudet, mahdollisuudet ja menettelytavat palveluntarjoajan ylläpitohenkilökunnalla on käsitellä organisaation käyttäjätietoja, lokitietoja ja erityisesti yksittäisiä sähköposteja.

VAHTI 9/2006 - Käyttövaltuushallinnon periaatteet ja hyvät käytännöt

- Silloin kun järjestelmän käytöstä jää merkintä siitä, kuka ko. järjestelmää tai sen tietoja on käyttänyt, myös nämä lokit muodostavat henkilörekisterin, josta tulee myös laatia rekisteriseloste.
- Käyttövaltuushallintoon liittyvien tietojen ja asiakirjojen sekä järjestelmän lokitietojen säilytysajat on määriteltävä arkistolain (831/94) säännösten mukaisesti.
- Lupaprosessin kaikki tapahtumat samoin kuin kaikki hallintajärjestelmään suoraan tehdyt tapahtumat ja kohdejärjestelmiin välitetyt tapahtumat kirjataan lokitiedostoihin, joiden perusteella käyttäjätietojen ja käyttö valtuuksien muutoksia voidaan seurata.

VAHTI 8/2006 - Tietoturvallisuuden arviointi valtionhallinnossa

Ohje käsittelee tietoturvallisuuden auditointia ja siinä tuodaan esille seuraavat lokien käsittelyyn liittyvät auditoinnissa tarkastettavat kohteet:

- Arvioinnissa tulee selvittää eritasoisten lokien käyttö ja niiden kattavuus käytön seurannassa. Erityistä huomiota tulee kiinnittää siihen, että henkilö- ja tunnistetietoja sisältävien lokien käsittely ja suojaaminen on toteutettu lainsäädännön mukaisesti.
- (Tarkastuskohteeseen liittyen) lokien osalta arvioidaan niiden riittävyys ja käyttökelpoisuus.
- Onko tietojärjestelmien käytöstä kertyvät lokit, joita voidaan käyttää henkilöstön tekniseen valvontaa luetteloitu?
- Onko tällaisista lokitiedoista asianmukaiset rekisteriselosteet, joissa myös tekninen valvonta on mainittu yhtenä käyttötarkoituksena?
- Onko tällaisten lokitietojen käyttö ohjeistettu ja niitä käsittelemään pääsevät henkilöt asianmukaisesti koulutettu?
- Onko käytössä lokien hallintajärjestelmä?
- Muodostetaanko lokit tarkoituksenmukaisesti kansainvälisten sopimusten, lakien ja muiden säädösten mukaisesti?
- Onko lokien käyttö hallittua?
- Onko pääsy tietoihin rajattu hallitusti vain niille, joiden tarvitsee päästä tietoihin?
- Onko sähköisen viestinnän tietosuojalain määräysten noudattaminen kunnossa?
- Muodostuuko lokitietojen käytöstä merkintä?
- Valvotaanko lokitietojen käyttöä?
- Varmistetaanko lokitiedot?
- Onko lokitietojen säilytys ja poisto säilytysajan umpeuduttua hoidettu?

VAHTI 7/2006 - Muutos ja tietoturvallisuus - alueellistamisesta ulkoistamiseen - hallittu prosessi

Ohje tuo esille seuraavat ulkoistuksen yhteydessä huomioitavat lokien käsittelyyn liittyvät vaatimukset/kysymykset:

- Onko tietojärjestelmässä erillinen lokijärjestelmä?
- Onko lokijärjestelmä eri palvelimella kuin tietojärjestelmä?
- Voidaanko lokijärjestelmästä ajaa raportteja näytölle?
- Voidaanko lokijärjestelmästä tulostaa käyttäjän määrittelemiä raportteja?
- Voidaanko lokijärjestelmästä tulostaa valmiiksi määriteltyjä raportteja paperille?
- Voidaanko lokijärjestelmästä viedä tietoja muihin järjestelmiin jatkojalostusta varten?

Kuvaa kaikki lokiin kirjautuvat tiedot (erilliselle liitteelle).

VAHTI 5/2006 - Asianhallinnan tietoturvallisuutta koskeva ohje

- Asioiden valmistelijoilla tulee olla oikeus muuttaa arkistonmuodostussuunnitelmasta oletusarvoina tallentuvia asioiden ja asiakirjallisten tietojen julkisuutta ja salassapitoa koskevia metatietoarvoja. Salassa pitoon liittyviin metatietoarvoihin tehtävien muutosten on tallennuttava järjestelmän tapahtuma- ja muutoslokiin.
- Asiakirjan omistajalla pitää olla oikeus poistaa luonnosasiakirja. Poistoista tallentuu tieto lokimerkintöihin.
- Tietoaineistojen käytön seurantaa ja valvontaa varten tietojärjestelmiin on tallennuttava automaattisesti lokitietoja tietojen käsittelyyn liittyvistä tapahtumista.
- Järjestelmien on kerättävä lokitietoja, jotta tietojärjestelmien ja niiden tietosisällön käytettävyys, eheys ja luottamuksellisuus voidaan turvata ja jotta mahdolliset luvattomat toiminnot voidaan havaita. Myös sähköisten asiointipalvelujen käytöstä, kuten oman asian käsittelyn seurannasta, on tallennuttava lokitietoja.
- Arkistonmuodostussuunnitelmaan tehtävistä muutoksista on tallennettauva loki- ja muutoshistoriatietoja.
- Lokitietoja on säännönmukaisesti seurattava. Lokijärjestelmä on rakennettava niin, että se hälyttää asiattomista käsittely-yrityksistä.
- Pääsyoikeudet järjestelmän lokitietoihin on määriteltävä valvontakohteiden mukaisesti.
- Lokitietoja ei saa käyttää profiiliyhteenvetojen tekemiseen.
- Lokitietojen säilytysaika määritellään lokin käyttötarkoituksen mukaan.
- Lokitietojen säilytysaikaa määriteltäessä on otettava huomioon myös niiden merkitys asiakirjallisen tiedon alkuperäisyyden, eheyden ja luotettavuuden varmistamisessa. Sen takia asianhallintajärjestelmään tallentuvat näitä ominaisuuksia tukevat lokitiedot ovat pakollisia metatietoja, jotka säilytetään niin kauan kuin järjestelmä on organisaatiossa käytössä ja jotka tulevaisuudessa siirretään pysyvästi sähköisessä muodossa säilytettävien asiakirjallisten tietojen mukana arkistolaitoksen vastaanotto- ja palvelujärjestelmään.
- Käyttövaltuuksien antaminen, muuttaminen ja poistaminen on dokumentoitava ja niiden hallinnasta on tallennuttava tietojärjestelmään valvontalokitietoa.

VAHTI 3/2005 - Tietoturvapoikkeamatilanteiden hallinta

- Poikkeamatilanteiden päätöksentekovastuut on määriteltävä vastaavasti kuin organisaation sisälläkin. Lisäksi sopimuksiin tulee määritellä, että tilaajalla on oikeus saada tarvittaessa käsiteltäväksi toimitta-

jalle kertyneet tilaajaa koskevat loki- tai muut tiedot poikkeamatilanteiden selvittämiseksi (ellei laki toisin määrää).
- Monet tietojärjestelmien käytöstä kerättävät lokitiedot ovat osa teknistä valvontaa ja siten TETSL:n piirissä.

Määrittele kaikki työasemat ja palvelimet käyttämään keskitettyä lokipalvelinta.

VAHTI 2/2005 - Valtionhallinnon sähköpostien käsittelyohje

- Lokit ovat lain yksityisyyden suojasta työelämässä 21 §:ssä säädeltyä teknisin menetelmin toteutettua valvontaa. Niiden käsittelyn periaatteista tulee sopia yhteistoimintamenettelyssä.
- Henkilörekisteri muodostuu myös lokitiedostojen osalta, jos ne sisältävät tunnistettavaa henkilöä koskevia merkintöjä.
- Työnantajan on yhteistyössä henkilöstön kanssa laadittava selkeät säännöt sähköpostin ja lokitietojen käytöstä (sähköisen viestinnän käyttöpolitiikka).
- Lokitietoja ei saa käyttää profiiliyhteenvetojen tms. tekemiseen.
- Lokitietoja saa käyttää vaitiolovelvollisen ylläpitohenkilöstön teknisluontoisiin tehtäviin sekä muihin sähköisen viestinnän tietosuojalain sallimiin tarkoituksiin (esim. laskutukseen ja tilastointiin verrattavaa yhteenvetoa, joissa ei näy yksityiskohtaista käyttöä).
- Työnantajan on määriteltävä lokitietojen säilytysaika ja –paikka.

Ohjelmisto- ja laitetoimittajalta tulee pyytää selvitys siitä, mitä lokitiedostoihin tallentuvat merkinnät kuvaavat ja voidaanko ne yhdistää tiettyyn henkilöön

VAHTI 2/2003 - Turvallinen etäkäyttö turvattomista verkoista

- Kirjautumisyritysten – sekä onnistuneiden että epäonnistuneiden – kirjaaminen pääsynvalvontalokiin. Loki on syytä tallettaa palvelimella, joka on erityisen hyvin suojattu tunkeutumisyrityksiä vastaan. Se ei saa näkyä ulos sisäverkosta.
- WLAN-yhteyksien ja työasemien henkilökohtaisten palomuurien osalta pidetään lokia.
- Kaikki onnistuneet ja epäonnistuneet yhteydenottoyritykset tulee kirjata hyvin suojatun palvelimen lokiin.

Palomuurin loki tulee kirjoittaa hyvin suojatulle palvelimelle.

VAHTI 1/2003 - Valtion tietohallinnon internet-tietoturvallisuusohje

- (IDS) Järjestelmän käyttöä voidaan harkita vasta, kun tietoliikenteen seuranta ja muut tietoliikennejärjestelmien lokien käsittelyt on järjestetty ja seuranta on säännöllistä.
- Järjestelmien käyttöönoton suunnittelussa pitää huomioida lokien käsittelyyn liittyvät vaatimukset.
- Lokitietojen kerääminen ja analysointi vaatii etukäteissuunnittelua ja aina tulee selvittää:
    - lokitietojen sisältö
    - lokitietojen seurantamekanismi
    - lokitietojen keräämisen sijainti
    - lokitiedostojen tallennuspaikka.
- Muista järjestelmistä saatavien lokitietojen merkitys asennettavalle järjestelmälle.
- Kuinka kauan lokitietoja saa tai tarvitsee säilyttää.
- Palomuurin tai muun palvelimen lokitiedot tulee kopioida säännöllisin väliajoin laitteesta sisäisessä verkossa olevalle palvelimelle tai muutoin järjestää niiden säilyminen siten, että niitä ei voida muuttaa tai lukea järjestelmästä itsestään. Lokitiedot voidaan ohjata suojatun yhteyden läpi erilliselle lokipalvelimelle, jonka tehtävänä on ainoastaan kerätä lokitietoja.
- Lokitiedoille tulee varata riittävästi tilaa ja määritellä, mitä tehdään, jos lokitiedoille varattu tila täyttyy.
- Lokitiedot eivät saa olla yleisesti saatavilla, vaan pääsy niihin tulee rajoittaa ylläpitohenkilöstölle. Ylläpitohenkilöstö saa käyttää lokitietoja vain teknisiin ylläpitotehtäviin ja muihin tietoturvapolitiikan edellyttämiin toimiin, kuten verkon turvallisuuden seuraamiseen.
- Lokitietoja seurattaessa on pyrittävä kiinnittämään huomiota normaalista poikkeaviin tapahtumiin esimerkiksi järjestelmien toiminnassa tai tietoliikenteessä.

Ylläpitäjien toimenkuvaan kuuluu seurata järjestelmien lokitietoja järjestelmähäiriöiden havaitsemiseksi.

VAHTI 4/2002 - Arkaluonteiset kansainväliset tietoaineistot

- Turvaluokitellun sähköisen asiakirjan käsittelyn tulee kirjautua sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai itse asiakirjaan. Sähköisen käsittelyn suositeltava kirjaamispaikka on loki tai vastaava sähköinen apuväline.

VAHTI 3/2002 - Valtionhallinnon etätyön tietoturvallisuusohje

- Kaikki tärkeimpien ohjelmistojen käytön tapahtumatiedot, esimerkiksi sisäänkirjaantuminen, poistuminen järjestelmästä ja konfiguroinnin muutokset, tulee kirjata suojattuun lokitiedostoon tietosuojasäädökset huomioon ottaen. Erityisesti epäonnistuneet tapahtumat tulee kirjata.
- Tietokoneen kello on pidettävä oikeassa ajassa transaktiohallinnan, lokitiedostojen ja muiden tarkkaa aikaa edellyttävien toimintojen vuoksi.

VAHTI 1/2002 - Tietoteknisten laitetilojen turvallisuussuositus

- Hävitettäväksi tarkoitettu paperimateriaali (esimerkiksi lokitulostimen tulosteet) on käsiteltävä eri osastossa olevalla silppurilla ja poistettava (laite) tiloista päivittäin.
- IT-laitetiloissa käyvien omien henkilöiden kulku tulee järjestää siten, että jokaisella on omana työaikanaan pääsy vain niihin tiloihin, joissa hänen työtehtäviensä takia tarvitsee oleskella. Henkilöstön käyntejä on seurattava säännöllisesti kulunvalvontajärjestelmän lokitiedostoista.
- Ohjelmistojen asennuksista on pidettävä kirjaa sekä lokitietojen tarkastuksen yhteydessä seurattava onko ohjelmistomuutoksia tehty.

VAHTI 6/2001 - Valtion tietotekniikkahankintojen tietoturvallisuuden tarkistuslista

Ohjeessa esitetään seuraavat lokienkäsittelyyn liittyvät kysymykset:

- Etähallinta ja sen turvallisuus - Muodostuuko etähallintatoimenpiteistä erillinen loki? Voidaanko näitä toimenpiteitä muuten valvoa?
- Tietoturvaominaisuudet ja niiden vahvuus. Ovatko lokit hyvin suojattu? Voidaanko helposti järjestää lokitiedostojen automaattinen siirto sellaiselle tietovälineelle, jota ei voida uudelleen kirjoittaa?
- Turvallisuuden hallinta ja seuranta - Mistä käyttäjien ja järjestelmän toimista muodostuu lokitietoja? Mitä lokitiedot sisältävät ja voidaanko niistä muodostaa tapahtumaketjuja (audit trail), jotka sitovat toisiinsa toimenpiteen ja käyttäjän?
- Käyttöoikeudet ja pääsyvaltuudet - Valvontaanko fyysistä ja loogista pääsyä (pääosin ympärivuorokautisesti) vartiointi- ja valvontajärjestelyin (esim. valvontakameroin), kulunvalvonnalla, loogisella pääsyvalvonnalla ja lokikirjauksilla, automaattisilla valvontalaitteilla (murtovalvonta ja tietomurtovalvonta), automaattihälytyksillä, raportoinnilla ja raporttien analysoinnilla ym?

- Operoinnin ja järjestelmänhallinnan turvamenettelyt ja lokit - Mistä käyttäjien ja järjestelmän toimista muodostuu lokitietoja? Mitä lokitiedot sisältävät ja voidaanko niistä muodostaa tapahtumaketjuja, jotka sitovat toisiinsa toimenpiteen ja käyttäjän?
- Operoinnin ja järjestelmänhallinnan turvamenettelyt ja lokit - Miten tilaajalla mahdollisuus saada käyttöönsä omien järjestelmiensä lokitiedot?
- Operoinnin ja järjestelmänhallinnan turvamenettelyt ja lokit - Mitä tietoja tietoturvalokeihin kerätään? Miten lokit suojataan, säilytetään, arkistoidaan ja hävitetään?

VAHTI 4/2001 - Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

- Palomuurin lokitietoja ja palvelun kuormitusta tulee seurata jatkuvasti ja automaattisesti.
- Lokitiedot on säilytettävä siten, ettei niitä päästä asiattomasti muuttamaan.
- Riskienhallinnan keskeinen väline on tietoturvallisuuden seuranta. Tähän kuuluvat lokitietojen kerääminen, analysointi ja raportointi, sekä tietoturvallisuuden eri osa-alueille tehtävät auditoinnit.
- Järjestelmän on kyettävä tarjoamaan seuranta suoritetuista toimenpiteistä ja palvelutapahtumista (lokitiedot).
- Auditoinneissa tulee kiinnittää huomiota myös lokitietojen sisältöön, käsittelyyn ja arkistointiin

VAHTI 2/2001 - Valtionhallinnon lähiverkkojen tietoturvallisuussuositus

- Kulunvalvontaan liittyvät lokit ja mahdolliset muut raportit tulee tarkistaa säännöllisesti turvallisuusloukkausten ja niiden yrittämisen havaitsemiseksi. Lokien säilytysaika ja –tapa tulee määritellä riittäväksi suhteessa arvioituihin riskeihin ja käytössä oleviin menettelytapoihin.
- Kaikki lähiverkon valvontaan liittyvät lokit ja mahdolliset muut raportit tulee seurata säännöllisesti turvallisuusloukkausten ja niiden yrittämisen havaitsemiseksi. Lokien säilytysaika ja –tapa tulee määritellä riittäväksi suhteessa arvioituihin riskeihin ja käytössä oleviin menettelytapoihin.
- Lokitietoja on konekielisessä muodossa pyrittävä säilyttämään sen järjestelmän ulkopuolella, mistä niitä kerätään. Tämä vähentää hakkereiden mahdollisuuksia päästä peittämään tietomurron/yrityksen jälkiä.

VAHTI 3/2000 - Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus

- Kriittisten aineistojen saantikerroista tehdään merkinnät tietoturvallisuuslokiin. (Järjestelmäkehityksen tietoteknisen ympäristön pääsynvalvontakäytännöt.)
- Tarkistetaan tietoturvallisuuslokit ja analysoidaan havaitut poikkeamat ja ”läheltä piti” –tilanteet. (Järjestelmän tarkastus määrävälein)

VAHTI 2/2000 - Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje

- Asiakirjan ja tietojen tulostamisesta tulee pitää lokitietoja. Lisävaatimuksia II turvaluokalle (salainen) ja I turvaluokalle (erittäin salainen) ja eräille salassa pidettäville henkilötiedoille).
- Asiakirjan tai tietojen käsittelyn tulee kirjautua sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai itse asiakirjaan. Sähköisen käsittelyn suositeltava kirjaamispaikka on loki tai vastaava sähköinen apuväline. (Yleiset vaatimukset kaikille salassa pidettäville tietoaineistoille (Koskevat III turvaluokkaa "luottamuksellinen", II turvaluokkaa, I turvaluokkaa, muita salassa pidettäviä kuten salassa pidettävät EU-asiakirjat ja henkilötiedot).

Liite 4

Voimassa olevat VAHTI-julkaisut

VAHTI 3/2009	Lokiohje
VAHTI 2/2009	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin, yleisohje
VAHTI 1/2009	VAHTIn toimintakertomus vuodelta 2008
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 6/2008	Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008	Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys
VAHTI 4/2008	Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008	Salauskäytäntöjä koskeva tietoturvaohje
VAHTI 2/2008	Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 1/2008	Toimintakertomus 2007
VAHTI 3/2007	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 2/2007	Älypuhelinten tietoturvallisuus
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 10/2006	Henkilöstön tietoturvaohje
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006	Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006	Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006	Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 1/2006	VAHTIn toimintakertomus vuodelta 2005

VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004	Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002	Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002	Etätyön tietoturvaohje
VAHTI 1/2002	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001	Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 2/2001	Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 3/2000	Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000	Valtion tietoaineistojen käsittelyn tietoturvaohje

Ohjeisto löytyy VAHTIn Internet-sivuilta http://www.vm.fi/vahti. Ohjeita saa tilattua laatikoittain edullisesti painotalo Editasta. Yllämainittujen julkaisujen lisäksi VAHTIn toiminnasta kertovia raportteja löytyy VAHTIn verkkosivuilta.

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin (09) 160 01
Telefaksi (09) 160 33123
www.vm.fi

3/2009
VAHTI
Toukokuu 2009

ISSN 1455-2566(nid.)
ISBN 978-951-804-957-2 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-951-804-958-9 (pdf)