VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta

Lautakunnat

Valtiovarainministeriön julkaisuja – 2021:65

Valtiovarainministeriön julkaisuja 2021:65

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta

Lautakunnat

Valtiovarainministeriö Helsinki 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Valtiovarainministeriö

ISBN pdf: 978-952-367-897-2
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2021

Kuvailulehti

8.11.2021

Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta

Valtiovarainministeriön julkaisuja 2021:65		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	suomi	**Sivumäärä**	89

Tiivistelmä

Tämä tiedonhallintolautakunnan antama suosituskokoelma opastaa tiedonhallintalain asettamien erinäisten vaatimusten täyttämisessä.

Tiedonhallintalain luku 4 sisältää tietoturvallisuutta koskevat vaatimukset, jotka kaikkien tiedonhallintalain soveltamisalaan kuuluvien viranomaisten tulee täyttää. Tietoturvallisuusvaatimusten toteuttamiseksi tiedonhallintalautakunta on antanut tietoturvallisuutta koskevia suosituksia.

Tiedonhallintalautakunta hyväksyi suosituskokoelman viimeisimmän version kokouksissaan 11.6. ja 14.10.2021.

Korvaa 1.4.2020 (Valtiovarainministeriön julkaisuja 2020:21) ja 21.9.2020 (Valtiovarainministeriön julkaisuja 2020:61) julkaistut versiot. Tiedonhallintalautakunta hyväksyi suosituskokoelman alkuperäisen version 26.3.2020 ja täydennyksen 23.6.2020.

Asiasanat	lautakunnat, tietoturva, julkinen hallinto, riskienhallinta, elinkaari, lokitiedostot, tiedonhallintalautakunta, tiedonhallintalaki		
ISBN PDF	978-952-367-897-2	**ISSN PDF**	1797-9714
Julkaisun osoite	http://urn.fi/URN:ISBN:978-952-367-897-2		

Presentationsblad

8.11.2021

Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet

Finansministeriets publikationer 2021:65		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämden		
Språk	finska	**Sidantal**	89

Referat

Denna rekommendationssamling som utfärdats av informationsförvaltningsnämnden ger vägledning när det gäller att uppfylla olika krav som ställs i lagen om informationshantering inom den offentliga förvaltningen.

Kapitel 4 i informationshanteringslagen innehåller de krav på informationssäkerhet som alla myndigheter som hör till tillämpningsområdet för informationshanteringslagen ska uppfylla. För att se till att informationssäkerhetskraven uppfylls har informationshanteringsnämnden gett rekommendationer som gäller informationssäkerhet.

Informationshanteringsnämnden godkände den senaste versionen av rekommendationssamlingen på sina möten den 11 juni och den 14 oktober 2021.

Ersätter de versioner som publicerades den 1 april 2020 (Finansministeriets publikationer 2020:21) och den 21 september 2020 (Finansministeriets publikationer 2020:61). Informationshanteringsnämnden godkände den ursprungliga versionen av rekommendationssamlingen den 26 mars 2020 och kompletteringen den 23 juni 2020.

Nyckelord	nämnder, informationshanteringsnämnden, lagen om informationshantering inom den offentliga förvaltningen, nämnder, informationssäkerhet, den offentliga förvaltningen, riskhantering, livscykel, loggfiler		
ISBN PDF	978-952-367-897-2	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-897-2		

Description sheet

8 November 2021

Collection of recommendations on the application of certain information security regulations

Publications of the Ministry of Finance 2021:65		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	Finnish	**Pages**	89

Abstract

This collection of recommendations issued by the Information Management Board provides guidance on the fulfilment of a number of requirements set out in the Information Management Act.

Chapter 4 of the Information Management Act lists the information security requirements that must be met by all authorities covered by the Information Management Act. To ensure that the information security requirements are fulfilled, the Information Management Board has issued various recommendations on information security.

The Information Management Board approved the latest version of the collection of recommendations at its meetings on 11 June and 14 October 2021.

This replaces the versions published on 1 April 2020 (Ministry of Finance publications 20:21) and 21 September 2020 (Ministry of Finance publications 20:61). The Information Management Board approved the original version of the collection of recommendations on 26 March 2020 and a supplement thereto on 23 June 2020.

Keywords	board, Information Management Board, Information Management Act, Boards, information security, public administration, risk management, lifecycle, log files		
ISBN PDF	978-952-367-897-2	**ISSN PDF**	1797-9714
URN address	http://urn.fi/URN:ISBN:978-952-367-897-2		

Sisältö

1 Johdanto

Tämä tiedonhallintolautakunnan antama suosituskokoelma opastaa lain julkisen hallinnon tiedonhallinnasta (906/2019, jatkossa tiedonhallintalaki, TiHL) asettamien erinäisten vaatimusten täyttämisessä.

Tiedonhallintalain luku 4 sisältää tietoturvallisuutta koskevat vaatimukset, jotka kaikkien tiedonhallintalain soveltamisalaan kuuluvien viranomaisten tulee täyttää. Tietoturvallisuusvaatimusten toteuttamiseksi tiedonhallintalautakunta on antanut tietoturvallisuutta koskevia suosituksia.

Yleiset huomiot suositusten sisällöstä:

- Suositukset on laadittu tiedonhallintayksikön ja viranomaisen oman toiminnan kehittämisen tueksi. Suosituksia ei ole tarkoitettu käytettäväksi auditointi- tai arviointikriteeristöinä.
- Suositukset koskevat kaikissa muodoissa olevaa tietoa, sekä analogista että sähköistä.
- Suosituksissa ei viitata mihinkään yleisiin standardeihin tai viitekehyksiin eikä anneta ohjeita teknisistä ratkaisuista, jotka voivat muuttua nopeastikin. Kunkin viranomaisen tulee tapauskohtaisen riskiarvioinnin perusteella valita kuhunkin tapaukseen sopivat, riittävän turvalliset tekniset ratkaisut.
- Suositukset kuvaavat suosituksia ja parhaita käytäntöjä, ne eivät ole velvoittavia kuten lainsäädäntö on.

Turvallisuusluokitellun tiedon käsittelyssä valtionhallinnon viranomaisten tulee huomioida sekä tiedonhallintalakia että valtioneuvoston asetusta asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) koskevat suositukset.

2 Tietoturvallisuuden vähimmäisvaatimukset

Julkisessa hallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset, ja niiden noudattamisesta annetut suositukset ovat seuraavat:

1. Tehtävät, joiden suorittaminen edellyttää henkilöiltä erityistä luotettavuutta on tunnistettu, 12 §
2. Toimintaympäristön tietoturvallisuustilaa seurataan, 13.1 §
3. Tietoturvallisuus varmistetaan tiedon elinkaaren ajan, 13.1 §
4. Tietoriskien hallinta ja siihen perustuvat tietoturvatoimet on järjestetty, 13.1 §
5. Tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettu, 13.2 §
6. Julkisuus ja salassapitorakenne on huomioitu tietovarantojen tietorakenteissa, 13.3 §
7. Hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet 13.4 §
8. Salassa pidettävät tiedot on suojattu yleisessä tietoverkossa tietoja siirrettäessä, 14.1 §
9. Tietoaineistojen turvallisuus on varmistettu, 15 §
10. Tietoaineistoja käsitellään riittävän turvallisissa tiloissa, 15.2 §
11. Käyttöoikeudet on määritelty ja hallittu tietojärjestelmissä, 16 §
12. Tarpeelliset lokitiedot on kerätty tietojärjestelmien käytöstä ja luovutuksista, 17 §
13. Turvallisuusluokiteltavista asiakirjoista ja niiden käsittelystä on huolehdittu, 18 §

Viranomaisen tulee arvioida mitä suunniteltu tiedonhallintamallin muutos tarkoittaisi kunkin yllä luetellun vähimmäisvaatimuksen osalta tai mitä kunkin vähimmäisvaatimuksen osalta on huomioitava kehittämisessä.

Uusia tietojärjestelmäpalveluja hankittaessa tietoturvallisuusvaatimukset muodostuvat yllä olevista vähimmäisvaatimuksista sekä riskiarvioinnin avulla tunnistetuista muista mahdollisista vaatimuksista. Kunkin vaatimuksen toteuttamisen menettely arvioidaan riskiarviointiprosessin avulla.

3 Luotettavuuden varmistaminen (TiHL 12 §)

> ***Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014). Työnantajan oikeudesta selvittää työntekijän luotettavuuden arvioimiseksi häntä koskevat luottotiedot ja käsitellä huumausainetestejä koskevia tietoja säädetään yksityisyyden suojasta työelämässä annetussa laissa (759/2004).***

Erityistä luotettavuutta edellyttäviä tehtäviä voidaan tunnistaa esimerkiksi määrittämällä tilanteet, joissa henkilö käsittelee turvallisuusluokiteltavia tai merkittävässä määrin ja säännöllisesti salassa pidettäviä tietoja tai työskentelee tiloissa, joissa henkilön tietoon voi tulla muutoin kuin satunnaisesti turvallisuusluokiteltavia tai salassa pidettäviä tietoja.

Edellytykset työnhakijaa koskevien henkilöluottotietojen saamiseksi työnhakijan luotettavuuden arvioimiseen on kuvattu yksityisyyden suojasta työelämässä annetun lain 5 a §:ssä. Työnantajan oikeudesta käsitellä huumausainetestejä koskevia tietoja säädetään lain 3 luvussa.

Turvallisuusselvityslain ohella erityissäännöksissä on saatettu täsmentää tiedonhallintalain 12 §:n velvoitetta luotettavuuden varmistamisesta. Esimerkiksi valtion virkamieslain (750/1994) 8 c §:n nojalla voidaan asetuksella säätää, että virkaan nimittämisen edellytyksenä on, että henkilöllä on voimassa oleva turvallisuusselvityslaissa tarkoitettu henkilöturvallisuusselvitystodistus. Turvallisuusselvityslain 16 §:n nojalla taas voidaan asetuksella säätää valtionhallinnon viranomaisen velvollisuudesta hankkia henkilöstä turvallisuusselvitys.

Tiedonhallintayksikkö laatii kuvauksen sellaisista tietoaineistojen käsittelyyn liittyvistä tehtävistä, jotka edellyttävät erityistä luotettavuutta. Näihin tehtäviin nimettävistä henkilöistä haetaan turvallisuusselvitys, mikäli tähän on turvallisuusselvityslain mukaan peruste. Lisäksi tiedonhallintayksikkö ylläpitää luetteloa näistä tehtävistä.

Huomioitavia seikkoja:

- Suojelupoliisilta tulee hakea lupa turvallisuusselvitysten hakemiseen; tätä varten on kuvattava tehtävät, joihin selvityksiä haetaan.
- Turvallisuusselvityksestä on ilmoitettava etukäteen esim. rekrytointi- tai koulutusilmoituksessa.
- Selvityksen kohteelta pitää saada suostumus selvitykseen.
- Selvityksen perusteella käynnistetään nuhteettomuusseuranta, joka on voimassa ainoastaan sen ajan kun henkilö toimii selvityksen kohteena olleessa tehtävässä tai toimeksiannossa.
- Selvitykset laaditaan sekä omista että palvelutoimittajien henkilöistä tarpeen mukaan.
- Suomen kansalaisista kansainvälisiä tehtäviä varten laadittavat PSC-selvitykset pyydetään UM:n NSA-viranomaiselta, pohjalla pitää olla Suomessa tehty turvallisuusselvitys. (PSC on kansallisen turvallisuusviranomaisen (NSA) myöntämä henkilöturvallisuustodistus, joka perustuu Suojelupoliisin tekemään turvallisuusselvitykseen).
- Ulkomaiden kansalaisista selvitysten laatiminen voi olla hankalaa. Niitä pyydetään kansallisten turvallisuusviranomaisten kautta.
- Myös toimittajien alihankkijoiden henkilöstöstä voi olla vaikea hakea selvityksiä.
- Luotettavuutta edellyttävät työtehtävät tulee huomioida käyttöoikeuksien hallinnassa.

4 Elinkaaren huomioiminen tietojen käsittelyssä (TiHL 13 §)

> ***Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.***

Tiedon elinkaari alkaa tiedon tuottamis- tai vastaanottovaiheessa ja päättyy tiedon pysyvään säilyttämiseen arkistossa tai tiedon tuhoamiseen. Tiedon elinkaari kattaa siis kaikki tiedon käsittelyn vaiheet, jotka ovat **tiedon tuottaminen** tai **vastaanotto**, **säilytys**, **käyttö**, **jakaminen**, **siirto** ja **arkistointi** tai **tuhoaminen**. Tiedon elinkaariajattelun lähtökohtana on tiedon suunnitelmallinen ja riskilähtöinen käsittely ja hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietoaineistojen tietoturvallisuuden koko niiden elinkaaren ajan tunnistamalla tietoaineistojen käsittelyyn kohdistuvat riskit ja mitoittamalla tietoturvallisuustoimenpiteet tehdyn riskiarvioinnin mukaisesti. Tietoaineistojen tietoturvallisuuden on täytettävä tiedonhallintalain asettamat vähimmäisvaatimukset.

Tiedon elinkaaren osalta on tärkeää huomioida, että tietoaineistoja käsitellään useassa eri sijainnissa ja tietojärjestelmässä tai laitteistossa, joissa tiedolla voi olla oma elinkaarensa, ja että tiedon elinkaari on yleensä pidempi kuin yksittäisen tietojärjestelmän elinkaari.

4.1 Tietoturvallisuus läpi tiedon elinkaaren

Tietoturvallisuus tietoaineistojen elinkaaressa muodostaa kokonaisuuden, johon kuuluvat **tiedon luokittelu**, **riskien arviointi**, **tietoturvallisuustoimenpiteiden suunnittelu** tunnistettujen riskien perusteella sekä **tietoturvallisuustoimenpiteiden toteuttaminen.** Tiedonhallintayksikön tulee arvioida tietoaineistoihin liittyviä riskejä säännöllisesti tietoaineistojen koko elinkaaren ajan sekä huomioitava muuttuneiden riskien edellyttämättoimenpiteet tietoturvaa koskevissa suunnitelmissa ja toteutuksissa. Ennen tiedon tuottamista tai vastaanottamista tulee huomioida tiedon määrittely, jossa arvioidaan tiedon ominaisuuksiin, turvallisuuteen ja metatietoihin liittyviä ominaispiirteitä. Tiedon määrittelyvaiheen perusteella muodostuvat tiedon käsittelyperiaatteet koko elinkaaren ajalle.

Tiedon osalta tunnistetaan ja määritellään, mihin sen käsittely perustuu ja mikä on tiedon käsittelyn tarkoitus. Lisäksi varmistetaan myös suunnitellun käsittelytarkoituksen toteutuminen läpi tiedon elinkaaren. Kaikissa elinkaaren vaiheissa varmistetaan, että tietoa käsitellään käsittelyperusteen muodostamien vaatimusten, tietoon kohdistuvien riskien ja tiedolle asetettujen tietoturvavaatimusten mukaisesti kaikissa käsittely-ympäristöissä. Tietoturvallisuus on alusta alkaen osa tietoaineistojen käsittelyyn liittyvien käytäntöjen ja käsittely-ympäristöjen suunnittelua ja toteutusta.

Tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt ja muut käsittelyyn liittyvät tekijät ovat tiedonhallintayksikön tiedossa asianmukaisen tiedonhallinnan toteuttamiseksi ja tiedon käsittelyyn liittyvien riskien arvioimiseksi. Tietoa käsitellään tehtyjen suunnitelmien mukaisesti kaikissa elinkaaren vaiheissa. Lisätietoja turvallisuusluokitellun tiedon käsittelystä löytyy mm. ulkoministeriön kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohjeesta.

Tiedon elinkaari alkaa sen käsittelyn käynnistyessä tiedon tuottamis- tai vastaanottovaiheessa ja päättyy sen pysyvään säilyttämiseen arkistoinnin muodossa tai tiedon tuhoamiseen. Tiedon elinkaari kattaa siis kaikki tiedon käsittelyn vaiheet, joita tyypillisesti ovat **tiedon tuottaminen** tai **vastaanotto**, **säilytys**, **käyttö**, **jakaminen** ja **siirto** sekä **arkistointi** tai tuhoaminen. Tiedon elinkaariajattelun lähtökohtana on tiedon suunnitelmallinen ja riskilähtöinen käsittely ja hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietoaineistojen tietoturvallisuuden koko niiden elinkaaren ajan tunnistamalla tietoaineistojen käsittelyyn kohdistuvat riskit ja mitoittamalla tietoturvallisuustoimenpiteet tämän riskiarvioinnin mukaisesti. Tietoaineistojen tietoturvallisuuden on täytettävä tiedonhallintalain asettamat vähimmäisvaatimukset.

Tiedon elinkaaren osalta on tärkeää huomioida, että tietoaineistoja käsitellään useassa eri sijainnissa ja tietojärjestelmässä tai laitteistossa, joissa tiedolla voi olla oma elinkaarensa ja tiedon elinkaari on yleensä pidempi kuin yksittäisen tietojärjestelmän elinkaari.

Alla on listattu keskeisiä tietoaineistojen elinkaareen liittyviä kysymyksiä:

- Onko tietoaineistojen käsittelyn peruste ja käyttötarkoitus tunnistettu ja määritetty?
- Onko tietojen käsittelyssä otettu huomioon tiedon käyttötarkoituksen mahdollinen muuttuminen?
- Onko tiedon käsittelyperusteen, kuten henkilötietojen ja erityisten henkilötietojen muodostamat vaatimukset tunnistettu?
- Onko tietoaineistoihin liittyvät riskit arvioitu koko tiedon elinkaaren ajalta? Seurataanko riskejä säännöllisesti?

- Ovatko tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt sekä muut käsittelyyn liittyvät tekijät tiedonhallintayksikön tiedossa (Tiedonhallintamalli, ministeriöillä lisäksi tiedonhallintakartta)

4.2 Tiedon tuottaminen ja vastaanotto

Tietoaineistojen tuottamisella tarkoitetaan käsittelyvaihetta, jossa tuotetaan uutta tietoa tai tehdään tietoaineistoon päivityksiä. Tietoaineistojen vastaanotolla tarkoitetaan käsittelyvaihetta, jossa tiedonhallintayksikkö vastaanottaa muualla tuotettuja tietoaineistoja.

Tiedon tuottamisen tai vastaanoton yhteydessä tunnistetaan ja kuvataan tiedon käsittelyn perusteet ja tarkoitus. Tuotettavan ja vastaanotettavan tiedon kohdalla tunnistetaan niiden käsittelyä koskevat erityisvaatimukset, jotka voivat tulla lainsäädännöstä tai toisen organisaation tiedon käsittelylle asettamista vaatimuksista. Erityisvaatimuksia asettaa esimerkiksi henkilötietoja koskeva tietosuojalaki ja tietosuoja-asetus. Tiedon tuottamis- ja vastaanottovaiheessa määritellään tiedon alustava säilytysaika, joka voi vielä muuttua tiedon elinkaaren eri vaiheissa.

Alla on listattu tiedon tuottamiseen ja vastaanottoon liittyviä keskeisiä kysymyksiä:

- Onko tietoaineistojen käsittelyn peruste ja käyttötarkoitus tunnistettu ja määritelty?
- Onko käsiteltävää tietoaineistoa koskevat erityisvaatimukset, kuten henkilötietoihin liittyvät vaatimukset tunnistettu?

4.3 Tiedon säilytys

Säilytyksen osalta määritellään ja toteutetaan tiedon riittävä suojaus sille asetettujen vaatimusten ja hallintakeinojen sekä riskitason mukaisesti. Tiedon suojauksen avulla turvataan tiedon luottamuksellisuuden ja eheyden säilyminen ja sen saatavuus. Suojaus kattaa tekniset ja hallinnolliset keinot.

Säilytyksessä varmistetaan tiedon saatavuus ja säilyminen sekä sen säilytysajan mittainen käytettävyys teknologioiden muuttuessa. Tiedon säilytyksen suunnittelussa ja toteutuksessa varaudutaan riskiarvioissa tunnistettuihin uhkatilanteisiin riskien edellyttämällä tasolla muun muassa asianmukaisen salauksen ja jatkuvuuden hallinnan avulla. Tietoaineistoille on määritelty säilytysajat, joiden päättyessä tietoaineistot joko arkistoidaan tai tuhotaan. Tietoaineistojen tuhoamiseen on dokumentoitu prosessi. Lisätietoja salauskäytännöistä löytyy mm. Vahti-ohjeesta 2/2015.

Tietoaineistojen säilytykseen käytetään ainoastaan siihen hyväksyttyjä ja asetettujen vaatimusten mukaisia säilytysympäristöjä, jotka noudattavat luvun 5 periaatteita.

Alla on listattu tiedon säilytykseen liittyviä keskeisiä kysymyksiä:

- Onko säilytettävä tieto luokiteltua (turvallisuusluokiteltua)? Jos on, onko säilyttämiseen liittyvät vaatimukset tunnistettu ja täytetäänkö ne? Onko tietojenluokittelussa huomioitu eri näkökulmat, kuten tietojärjestelmät, tietosuoja, tietoturva, toimintaprosessit ja tietoarkkitehtuuri?
- Säilytetäänkö tietoa siten, että vain oikeutetut tahot pääsevät siihen käsiksi?
- Onko tiedon säilytys suunniteltu siten, että sen käytettävyys ja saatavuus on taattu myös poikkeusoloissa, mikäli riskiarvio näin edellyttää?
- Onko säilytettävälle tiedolle määritetty säilytysaika, jonka päättyessä se joko arkistoidaan tai tuhotaan asianmukaisesti?

4.4 Tiedon käyttö

Tietoaineistojen luvallinen käyttö mahdollistetaan ja luvaton käyttö estetään henkilöiden työtehtäviin perustuvalla roolipohjaisella fyysisten ja loogisten käyttöoikeuksien ja -valtuuksien määrittelemisellä ja hallinnalla. Tietoaineistojen käyttäjän identiteetti todennetaan riskeihin ja käytettävään tietoon nähden riittävällä tavalla.

Tietoaineistojen käyttöä seurataan ja valvotaan tehdyn riskiarvioinnin mukaisesti. Tietojärjestelmien kohdalla vähintään kirjautumisista ja niiden yrityksistä tulee tuottaa lokia, mutta useissa tapauksissa myös järjestelmässä toimimisesta tulee kerätä käyttölokia. Tietoaineistojen käytön lokitus ja valvonta toteutetaan tarpeellisuusarvioinnin perusteella tiedon käyttötarkoituksen ja siihen liittyvien riskien edellyttämällä tavalla. Palvelusta vastaavan vastuulla on selvittää, saako palvelusta kerätä lokitietoja.

Tietoaineistojen käyttö tapahtuu siihen hyväksytyissä ja asetettujen vaatimustenmukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä.

Alla on listattu tiedon käyttöön liittyviä keskeisiä kysymyksiä:

- Onko tietoaineiston käyttöoikeudet ja -valtuudet määritelty henkilön työtehtävien mukaisesti?
- Valvotaanko tietoaineiston käyttöä riskiarvion mukaisesti?
- Voidaanko olla varmoja siitä, että tietoaineistoa käytetään vain siihen tarkoitukseen, johon ne on (alun perin) tarkoitettu?
- Kerätäänkö tietojärjestelmien kirjautumisista lokia?
- Voidaanko olla varmoja siitä, että tietoaineistoa käsitellään vain siihen hyväksytyissä ja asetettujen vaatimusten mukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä?

4.5 Tiedon jakaminen, siirtäminen ja luovuttaminen

Tietoaineistojen jakamisella tarkoitetaan toimia, joiden avulla päätetään tietoaineiston vastaanottajat, varmistetaan vastaanottajien tiedontarve ja oikeus sekä kyky käsitellä jaettavaa tietoaineistoa. Tietoaineistojen siirrolla tarkoitetaan niitä toimenpiteitä, joilla tietoaineistot siirretään määritetyille tahoille tai toisiin tietojärjestelmiin. Siirto voi tapahtua esimerkiksi postin, sähköpostin, sähköisen muistivälineen, tietojärjestelmien välisen tiedonsiirron tai käsittelyoikeuksien myöntämisen avulla. Ei-julkista tai turvallisuusluokiteltua tietoa jakaessa ja siirtäessä tulee muistaa, että tavallinen sähköposti ei lähtökohtaisesti ole salattu ja turvallinen tiedonvälityskanava. Tällaista tietoa siirrettäessä tulee olla erityisen varma, että tiedonsiirrossa käytettävä menetelmä on salattu ja riittävän turvallinen. Tiedon luovuttamisella tarkoitetaan tietojen luovuttamista niitä pyytävälle taholle. Julkista tietoa luovutetaan viranomaisten toiminnan julkisuudesta annetun lain mukaisesti.

Tietoa jaettaessa, siirrettäessä ja luovutettaessa varmistutaan aina riittävän luotettavasti mahdollisen vastaanottajan identiteetistä sekä toteutetaan tiedon siirto tunnistettuihin riskeihin nähden asianmukaista salausta ja suojausta käyttäen. Näin varmistetaan, etteivät tietoon pääse käsiksi siihen oikeudettomat henkilöt ja tietoaineisto jaetaan tai luovutetaan vain henkilöille, joilla on siihen työtehtäviinsä liittyvä oikeus. Lisätietoja salausratkaisujen turvallisuudesta on luvussa 6 sekä Kyberturvallisuuskeskuksen turvallisuusluokitellun tiedon suojaamiseen hyväksymissä salausratkaisuissa, vahvuustaulukoissa, sekä ohjeissa salaustuotteiden arvioinnista ja turvallisesta kehittämisestä.

Kun tietoaineistoja jaetaan tai luovutetaan viranomaisten välillä, huomioidaan (erillinen) suositus Teknisistä rajapinnoista ja katseluyhteyksistä. Alla on listattu keskeisiä tiedon jakamiseen, siirtämiseen ja luovuttamiseen liittyviä kysymyksiä:

- Voidaanko tietoaineistoa jakaessa, siirtäessä ja luovuttaessa varmistua riittävällä tasolla vastaanottajan identiteetistä?
- Käytetäänkö tiedon siirrossa asianmukaista salausta?
- Onko tietoja luovutettaessa varmistuttu siitä, että tiedon luovuttaminen on lain mukaista ja vastaanottajalla on oikeus tietoaineiston käsittelyyn sekä kyky käsitellä sitä vaatimusten mukaisesti?

4.6 Tiedon arkistointi

Tietoaineistojen arkistoinnilla tarkoitetaan niitä menettelyjä, joilla varmistetaan tiedon säilyminen muuttumattomana asetetun elinjakson ajan. Tietoaineistot on tuhottava tai arkistoitava tietoturvallisella tavalla tiedon säilytysajan päätyttyä.

Arkistoinnissa huomioidaan tiedon säilytysaika, -paikka ja -tapa sekä varmistetaan tiedon käyttökelpoisuus ja luettavuus koko säilytysajaksi. Arkistointi perustuu sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin. Lisätietoja arkistoinnin vaatimuksista löytyy Kansallisarkiston ohjaussivulla.

Alla on listattu keskeisiä tiedon arkistointiin liittyviä kysymyksiä:

- Onko arkistoinnissa huomioitu tiedon säilytysaika, -paikka ja -tapa?
- Onko tiedon käyttökelpoisuudesta ja luettavuudesta varmistuttu koko tiedon säilytysajan?
- Perustuuko arkistointi sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin?

4.7 Tiedon tuhoaminen

Tietoaineistojen tuhoamisella tarkoitetaan niitä toimenpiteitä, joiden avulla tietoaineistot tuhotaan tarkoituksella niiden säilytysajan ja käyttötarpeen päättyessä tai niitä sisältävän laitteiston käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä.

Tiedon tuhoaminen tapahtuu määritellyn säilytysajan tai käyttötarpeen päättyessä tunnistettuihin riskeihin nähden riittävän luotettavalla tavalla. Tietoaineistoille määritetyt

säilytysajat huomioidaan tiedon tuhoamisen suunnittelussa. Tietoaineistoista muodostetut kopiot ja luonnokset sekä väliaikaistiedostot tuhotaan niiden käyttötarpeen päätyttyä.

Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen osittain tai kokonaan. Salassa pidettävän tietoaineiston tuhoamiseen voidaan käyttää useita eri menetelmiä ja työvälineitä riippuen muun muassa tiedon olomuodosta ja saatavilla olevista erilaisista ratkaisuista. Esimerkiksi tiedon silppuamisen tai kovalevyn ylikirjoituksen sijaan tai lisäksi silppu voidaan polttaa ja kiintolevy sulattaa.

Erityisesti sähköisten aineistojen luotettavan tuhoamisen menettelyjen tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa. Laitteistojen osien (kiintolevyt, muistit, muistikortit, jne.) sisältämän salassa pidettävän tiedon luotettavasta tuhoamisesta on huolehdittava erityisesti käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä. Mikäli luotettava tyhjennys (esimerkiksi viranomaisen hyväksymä ylikirjoitusmenettely) ei ole mahdollista, salassa pidettävää tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille. Tilanteissa, joissa laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä, tulisi kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa, ja pyrkiä varmistumaan siitä, että salassa pidettävää tietoa ei viedä huoltotoimenpiteen yhteydessä. Mikäli tiedon tuhoaminen tapahtuu palveluntarjoajan toimesta, viranomaisen tulee varmistua luotettavalla tavalla tiedon oikeellinen hävittäminen

Alla on listattu keskeisiä tiedon tuhoamiseen liittyviä kysymyksiä:

- Tapahtuuko tiedon tuhoaminen määritellyn säilytysajan tai käyttötarpeen päättyessä riittävän luotettavalla tavalla? Käytetäänkö tässä menetelmää, jolla estetään tietojen kokoaminen uudestaan tai osittain?
- Kattavatko luotettavan tuhoamisen menettelyt kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa?

4.8 Säädökset ja lisätiedot

EU:n yleinen tietosuoja-asetus

Arkistolaki

Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksynät salausratkaisut

Kyberturvallisuuskeskuksen hyväksymä ylikirjoitusmenettely (Kiintolevyjen elinkaaren hallinta)

Kyberturvallisuuskeskus, Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat

4.9 Yhteenveto suosituksesta

Taulukko 1. Yhteenveto suosituksesta.

Koko elinkaari	Tietoaineistoihin liittyvät riskit arvioidaan säännöllisesti. Tunnistetaan ja määritetään tietoaineistojen käsittelyn peruste ja käyttötarkoitus. Varmistetaan, että tiedon käsittelyperusteen muodostamat vaatimukset, tietoon kohdistuvat riskit ja tiedolle asetetut tietoturvavaatimukset huomioidaan tiedon käsittelyn kaikissa vaiheissa. Varmistetaan, että tietoon, tietoaineistoon ja niiden käsittelyyn liittyvät vaatimukset huomioidaan tietojärjestelmiä ja ympäristöä suunniteltaessa ja ratkaisujen toteuttamisessa. Tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt sekä muut käsittelyyn liittyvät tekijät tulee olla tiedonhallintayksikön tiedossa (Tiedonhallintamalli, ministeriöillä lisäksi tiedonhallintakartta)
Tiedon tuottaminen ja vastaanotto	Tunnistetaan ja kuvataan tiedon käsittelyn perusteet ja käsittelytarkoitus. Tunnistetaan tiedon käsittelyä koskevat erityisvaatimukset (esim. lainsäädännöstä tai toisen organisaation vaatimuksista muodostuvat).
Tiedon säilytys	Säilytettävää tietoa suojataan sille muodostettujen vaatimusten ja hallintakeinojen sekä riskitason mukaisesti. Säilytettävän tiedon säilyminen ja saatavuus on turvattu. Säilytettävän tiedon käytettävyys on varmistettu koko säilytysajan. Tietoaineistolle on määritetty säilytysaika ja sen päättyessä tieto joko arkistoidaan tai tuhotaan. Tietoaineistojen säilytykseen käytetään ainoastaan siihen hyväksyttyjä ja asetettujen vaatimusten mukaisia säilytysympäristöjä.
Tiedon käyttö	Käyttöoikeudet ja -valtuudet tietoaineistoihin perustuvat henkilöiden työtehtäviin. Tietoaineistojen käyttöä lokitetaan riskiperustaisesti. Tietoaineistoja käytetään siihen tarkoitukseen, joihin ne on (alun perin) tarkoitettu. Tietoaineistoja käyttö tapahtuu ainoastaan siihen hyväksytyissä ja asetettujen vaatimusten mukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä.

Tiedon jakaminen, siirtäminen ja luovuttaminen	Tietoa jaettaessa, siirrettäessä ja luovuttaessa varmistutaan riittävällä tasolla vastaanottajan identiteetistä. Tiedon siirrossa käytetään asianmukaista salausta. Tietoa luovutettaessa varmistetaan, että tiedon luovuttaminen on lain mukaista ja vastaanottajalla on oikeus tietoaineiston käsittelyyn sekä kyky käsitellä sitä vaatimusten mukaisesti.
Tiedon arkistointi	Arkistoinnissa huomioidaan tiedon säilytysaika, -paikka ja -tapa. Arkistoinnissa on varmistettu tiedon käyttökelpoisuus ja luettavuus koko säilytysajaksi. Arkistointi perustuu sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin.
Tiedon tuhoaminen	Tiedon tuhoaminen tapahtuu määritellyn säilytysajan tai käyttötarpeen päättyessä riittävän luotettavalla tavalla. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. Sähköisten aineistojen luotettavan tuhoamisen menettelyt kattavat kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassapidettävää tietoa.

5 Tiedon elinkaaren huomioiminen tietojärjestelmissä (TiHL 13 §)

> ***Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.***

5.1 Tietojärjestelmä

Tietojärjestelmällä tarkoitetaan järjestelmää, jonka tarkoitus on tietoja käsittelemällä palvella, helpottaa ja tehostaa jotakin toimintaa. Tietojärjestelmä koostuu ohjelmista, tietovarastoista, laitteista ja palveluista. Tietojärjestelmän elinkaari alkaa siihen liittyvästä tarvekartoituksesta ja päättyy tietojärjestelmän käytöstä poistoon. Tietojärjestelmän elinkaari kattaa kaikki tällä välillä olevat vaiheet, jotka ovat **määrittely** ja **suunnittelu, kilpailutus** ja **hankinta**, **toteutus** ja **kehitys**, käyttöönotto, **ylläpito** sekä **käytöstä poisto**. Tietojärjestelmien elinkaariajattelun lähtökohtana on kussakin järjestelmässä käsiteltävien tietojen elinkaaren huomiointi ja järjestelmien suunnitelmallinen ja riskilähtöinen hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietojärjestelmien tietoturvallisuuden koko niiden elinkaaren ajan tunnistamalla niihin kohdistuvat **riskit** ja mitoittamalla tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Riskienarvioinnissa tunnistetaan olennaiset riskit, jotka voivat vaikuttaa tietojärjestelmien käytettävyyteen ja saatavuuteen tai niissä käsiteltävien tietoaineistojen tietoturvallisuuteen ja oikeellisuuteen.

Tietoturvallisuus tietojärjestelmien elinkaaressa muodostaa kokonaisuuden, johon kuuluvat riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen. Tiedonhallintayksikkö arvioi tietojärjestelmiin liittyviä riskejä säännöllisesti niiden koko elinkaaren ajan sekä huomioi muuttuneiden riskien edellyttämät toimenpiteet tietoturvallisuuden suunnittelussa ja toteutuksessa. Tietojärjestelmien riskien arvioinnissa huomioidaan toimintaympäristö ja järjestelmään liittyvät tietoturvavaatimukset.

5.2 Määrittely- ja suunnitteluvaihe

Ennen määrittely- ja suunnitteluvaiheen aloittamista tehdään tarvekartoitus, jossa tunnistetaan ja määritellään tietojärjestelmä, sekä se mitä uuteen tai uudistettavaan tietojärjestelmään liittyy ja millaisia vaatimuksia siihen kohdistuu. Määrittely- ja suunnitteluvaiheen aikana tunnistetaan tietoturvallisuuden kannalta keskeiset asiat, jotka on huomioitava toteutuksen myöhemmissä vaiheissa. Näihin kuuluvat aina tiedonhallintalaissa asetetut tietoturvallisuuden vähimmäisvaatimukset, jotka on lueteltu luvussa 3.

Määrittely- ja suunnitteluvaiheessa tunnistetaan tietojärjestelmän liittymät muihin järjestelmiin sekä niistä muodostuvat riippuvuudet ja tietovirrat. Nämä dokumentoidaan osaksi arkkitehtuuri- ja integraatiosuunnitelmia, joiden mukaisesti toteutetaan tarvittavat integraatiot muuhun ympäristöön varmistaen myös tietoturvallisuuden toteutuminen niissä. Edellä mainitut asiat voidaan tunnistaa jo tarvekartoituksen aikana, ja ne tarkentuvat kehittämisen edetessä.

Määrittely- ja suunnitteluvaiheessa kuvataan tietojärjestelmän käyttötarkoitus sekä toimintaympäristö, kuten käyttäjät, ohjaava lainsäädäntö ja muut ulkoiset vaatimukset, järjestelmässä käsiteltävät tietoaineistot sekä liittymät muihin tietojärjestelmiin. Näiden pohjalta tehdään riskiarvio sekä määritetään tietojärjestelmään kriittisyys ja edellytetty tietoturvallisuuden taso, joiden perusteella tunnistetaan koko tietojärjestelmän elinkaaren aikana huomioitavat tietoturvavaatimukset. Tietojärjestelmään kohdistuvat toiminnalliset vaatimukset kuvataan ja niiden pohjalta laaditaan tietojärjestelmään kohdistuvat hyväksymiskriteerit. Tämä sisältää myös tietoturvallisuutta koskevat suunnitelmat ja vaatimukset, joiden määrittelyssä käytetään tarvittavaa tietoturvaosaamista. Määrittely- ja suunnitteluvaiheessa huomioidaan luvun 6 tarkennukset hankinnan suunnitteluun ja valmisteluun.

Tietojärjestelmän tai sen osan määrittelyvaiheessa arvioidaan sekä kokonaisuuden että järjestelmän eri osien tietoturvallisen toteuttamisen riskejä. Sellaisten osakokonaisuuksien sisällyttämistä järjestelmään on vältettävä, joiden tietoturvallinen toteuttaminen tai ylläpito vaativat runsaasti resursseja. Keskeistä on kiinnittää myös huomioita tietoriskien arvioinnissa koko palvelu- ja toimitusketjun kaikkien osapuolien ja heidän ympäristöjensä huomioimiseen, jotta tietojärjestelmään kohdistuvat riskit tulee kokonaisvaltaisesti hallittua. Organisaation johto sitoutuu tietoriskien hallintaan perustuvaan tietoturvallisuuden toteuttamiseen jo määrittely- ja suunnitteluvaiheesta lähtien. Johdolle on myös tarkoituksenmukaista antaa realistinen kuva tietoturvallisuuden rakentamisen ja ylläpidon vaatimista resursseista.

Lisäksi ennen hankintaa tai toteutusta suunnitteluvaiheessa laaditaan alustava suunnitelma hankinnan ja toteutuksen aikaisista tietoturvaan liittyvistä tehtävistä, vastuista ja aikataulutuksesta. Määrittely- ja suunnitteluvaiheessa on lisäksi hyvä varmistaa

jasuunnitella riittävät resurssit tietojärjestelmien tietoturvalliselle toiminnalle, kuten tietoturvapäivitysten toteuttamiselle, niiden koko elinkaaren ajalle.

5.3 Kilpailutus- ja hankintavaihe

Kilpailutus- ja hankintavaiheessa suunnitellaan ja toteutetaan tietojärjestelmään liittyvä hankinta luvun Tietoturvallisuus tietojärjestelmähankinnoissa mukaisesti.

Kilpailutus- ja hankintavaiheessa on keskeistä, että hankintavaatimuksiin, tarjouspyyntöihin ja sopimuksiin sisällytetään myös tietoturvaa koskevat vaatimukset. Ne kohdistuvat sekä hankinnan kohteena olevaan tietojärjestelmään, että sen toteuttavaan ja tarjoavaan toimittajaan.

5.4 Toteutusvaihe

Toteutusvaiheen sisältö riippuu hankittavasta tietojärjestelmästä ja sen toteutusmallista. Kyseessä voi olla esimerkiksi täysin räätälöity järjestelmä ja siihen liittyvä laajempi kehitysprojekti tai valmisohjelmisto, johon tehdään toteutusvaiheen aikana ainoastaan tiettyjä konfigurointeja.

Toteutusvaiheessa tehdään uudelleentarkastelu määrittelyvaiheessa laadittuun riskiarviointiin sekä tehdään tarvittavat tarkentavat uhkamallinnukset ja riskiarviot tietojärjestelmään liittyvien riskien ja uhkaskenaarioiden tunnistamiseksi. Määritetyt tietoturvavaatimukset suunnitellaan ja dokumentoidaan tietoturvakontrolleiksi, jotka toteutetaan tämän vaiheen aikana.

Tietojärjestelmät koostuvat usein lukuisista, mahdollisesti hajautetuista ja usean osapuolen tekemistä komponenteista. Tällöin on tietoriskien hallinnassa hyvä kiinnittää huomiota rajapintojen hallintaan sekä palvelujärjestelmän ja taustajärjestelmän välisen tiedonsiirron hallintaan.

Toteutuksen aikana suoritetaan suunnitellut katselmoinnit ja testaukset pohjautuen riskiarvioon ja tarveharkintaan; mm. arkkitehtuurikatselmointi, koodikatselmointi, toiminnallisuuksien testaus, väärinkäyttötapausten testaus/ tietoturvatestaus ja suorituskykytestaus.

Toteutusvaiheessa huomioidaan sille etukäteen laaditut suunnitelmat ja vaiheet. Tavoitteena on, että tarvittavat toimenpiteet tehdään riskilähtöisesti ja suunnitelmallisesti asianmukaisen tietoturvallisuuden sisään rakentamiseksi.

Toteutetut tietoturvakontrollit ja ratkaisut dokumentoidaan osaksi tietojärjestelmän turvallisuuskuvausta ja muuta laadittua dokumentaatiota.

Tietoturvallisuusvastuiden epäselvyydet toteutuksen aikana ovat tavallinen ongelma, etenkin monitoimittajaympäristössä. Tähän voidaan varautua tietoriskien jatkuvalla hallinnalla ja riskien hallintaan tähtäävien toimenpiteiden toteuttamisella, huomioiden erityisesti sopimuksiin kirjatut tavoitteet ja toimenpiteet riskien hallinnan osalta. Sopimuksiin liittyviä tyypillisiä riskejä ovat IPR-kysymykset, tekijänoikeudet, lisenssit ja kaikki vielä tunnistamaton immateriaalioikeuden alla oleva aineisto, omistajan vaihdokset, fuusiot ja toiminnan lopettaminen.

5.5 Käyttöönottovaihe

Käyttöönottovaihetta varten laaditaan käyttöönottosuunnitelma tuotantoon viennin toteuttamiseksi. Osana tietojärjestelmän käyttöönottoa suoritetaan käyttöönottohyväksyntä, jossa varmistetaan aiemmin kuvattujen vaatimusten toteutuminen tietojärjestelmässä. Hyväksyntä edellyttää tarvittavien toiminnallisuuksien ja tietoturvakontrollien todentamista. Tietojärjestelmien, laitteiden ja sovellusten käyttöönottoasennus tehdään määritetyn prosessin ja ohjeistuksen mukaisesti huomioiden esimerkiksi organisaation laatimat arkkitehtuuriperiaatteet, yhteensopivuus muuhun ympäristöön sekä määritetyt suojausvaatimukset ja kovennukset. Näiden toteuttamiseksi on määritetty määrämuotoiset konfiguraatiot eri asetuksille ja parametreille sekä tarpeettomat palvelut poistettu käytöstä. Kovennetun, määritetyt tietoturva-asetukset sisältävän, asennuksen toteuttamisessa voidaan hyödyntää esimerkiksi ylläpidettyä luotettua levykuvaa (golden image), jonka avulla asennus tehdään. Nämä levykuvat katselmoidaan, testataan ja päivitetään säännöllisesti niiden asianmukaisuuden varmistamiseksi. Myös itse tietojärjestelmien, laitteiden ja sovellusten konfiguraatioiden säännöllinen katselmointi ja valvonta suunnitellaan osaksi ylläpitovaihetta.

Tietojärjestelmän tietoturvakuvaus päivitetään tarvittavien muutosten osalta käyttöönottovaiheessa.

5.6 Ylläpitovaihe

Osana ylläpitoa tunnistetaan käsittely-ympäristössä tai vaatimuksissa tapahtuvien muutosten vaikutus tietojärjestelmään sekä niiden edellyttämät muutokset tietoturvakontrolleihin. Tehtävissä muutoksissa noudatetaan määritettyjä muutoshallintamenettelyitä. Tietojärjestelmään kohdistetaan säännöllisiä riskiarvioita ja suojaustason asianmukaisuuteen kohdistuvia arvioita, jotta varmistutaan siitä, että tietojärjestelmään kohdistuvat riskit

ja vaatimukset ovat huomioitu. Arvioinneissa hyödynnetään muun muassa katselmointeja sekä automaattisia ja manuaalisia tietoturvatestauksia. Riippuen toteutustavasta myös tietojärjestelmän palvelutoimittajaan kohdistetaan tarvittavia auditointeja ja heiltä voidaan edellyttää tietojärjestelmän turvallisuustason seurantaa sekä siihen liittyvää raportointia. Ylläpitovaiheen yhtenä tavoitteena on varmistaa määritettyjen tietoturvavaatimusten ja suojauskeinojen ajantasaisuus ja asianmukainen toiminta tehtyihin suunnitelmiin pohjautuen sekä näitä koskevan dokumentaation ja kuvausten ylläpito.

Tietojärjestelmien ylläpidossa noudatetaan organisaatiossa määritettyjä prosesseja ja toimintatapoja, kuten muutoshallinta, poikkeamienhallinta ja riskienhallinta, kun huolehditaan tietojärjestelmien haavoittuvuuksien hallinnasta, päivityksistä, varmuuskopioinnista, konfiguraation hallinnasta ja kovennuksista, haittaohjelmasuojauksesta sekä valvonnasta. Ylläpitovaiheessa pitää huolehtia myös toiminnan jatkuvuuden edellyttämästä tietojärjestelmän toipumissuunnitelmasta ja varmistamisesta harjoittelulla.

Osana tietojärjestelmien ylläpitoa toteutetaan tarvittava valvonta ja seuranta muun muassa tietojärjestelmän toimivuuden, suorituskyvyn ja tietoturvallisuuden seuraamiseksi ja ylläpitämiseksi. Suoritettava valvonta ja seuranta tulee kuitenkin olla suunniteltuna määrittely- ja suunnitteluvaiheen aikana.

Varmuuskopiot otetaan tehdyn suunnitelman mukaisesti huomioiden organisaation toiminnan ja käsitellyn tiedon pohjalta määritetyt varmuuskopioitavat tiedot, varmuuskopiointiin käytetyt menetelmät ja sen tiheys sekä varmuuskopioiden suojaamiseen liittyvät keinot. Varmuuskopiointi toteutetaan

- käyttäen siihen tarkoitettua ratkaisua,
- kirjaten lokiin tiedot varmuuskopioiduista tiedoista, varmuuskopioinnin ajankohdasta ja varmuuskopion kohteesta sekä merkiten varmuuskopiot asianmukaisesti,
- varmistaen varmuuskopioinnin onnistuminen ja palauttaminen esimerkiksi raportein sekä palautustestein, sekä
- suojaten varmuuskopiot vahingoilta ja väärinkäytöksiltä, kuten ylikirjoittamiselta, muuttamiselta tai tuhoutumiselta sekä niiden siirron että säilytyksen aikana.

Ohjelmistohaavoittuvuuksien hallinnassa noudatetaan määritettyä prosessia, jossa määritetään päivitystarpeen tunnistaminen ja havaitseminen, päivitysten asentamiseen liittyvät toimintamallit (huomioiden erityyppiset tietojärjestelmät ja ympäristöt sekä niiden mahdollisesti muodostamat erityistarpeet), päivitysten epäonnistumiseen ja palautumiseen liittyvät käytännöt, päivitystilanteen seurantaan ja siitä raportointiin liittyvät toimintatavat sekä vaihtoehtoiset suojaustavat ja toimenpiteet, kun haavoittuvuutta ei voida korjata

päivityksellä (esimerkiksi päivitystä ei ole vielä julkaistu tai jokin sovellus ei toimi päivitetyssä versiossa).

Haittaohjelmasuojausta koskevat toimintamallit on määritelty kuvaten muun muassa haittaohjelmasuojaukseen käytettyjen ratkaisujen asennus ja konfigurointi sekä päivittämisen käytännöt, ratkaisujen ajantasaisuuden ylläpitäminen sekä niiden toimivuuden varmistaminen.

Ylläpitoyhteydet ja -oikeudet on toteutettu vähimpien oikeuksien periaatteen mukaisesti, jolloin ylläpitotoimiin on käytössä lievimmät mahdolliset tarvittavat oikeudet. Tietojärjestelmien ylläpitoyhteydet tehdään käyttäen salattuja yhteyksiä. Loogista ja fyysistä pääsyä rajoitetaan.

5.7 Käytöstä poisto

Käytöstä poistoa varten laaditaan riskiarviointi, jossa tunnistetut riskit huomioidaan poiston toteuttamisessa. Käytöstä poistolle laaditaan suunnitelma, jossa huomioidaan muun muassa säilytettävän tiedon migraatio, tuhottavien laitteiden ja muistivälineiden sanitointi sekä käytöstä poistuvan tietojärjestelmän osien tuhoaminen.

Käytöstä poiston yhteydessä tietoaineistojen tuhoamisen tulee tapahtua tunnistettuihin riskeihin nähden riittävän luotettavalla tavalla. Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen osittain tai kokonaan. Tietoaineistojen elinkaaren osalta huomioidaan luvun 4 periaatteet.

Tietojärjestelmien käytöstä poistossa järjestelmien sisältämät tiedot voidaan tuhoamisen sijaan arkistoida. Arkistoinnin keskiössä on tiedon säilyvyys, käyttökelpoisuus ja luotettavuus.

5.8 Säädökset ja lisätiedot

JHS 166 Julkisen hallinnon IT-hankintojen yleiset sopimusehdot (JIT 2015)

Tilastoinnin yleinen prosessimalli (GSBPM)

5.9 Suosituksen yhteenveto

Taulukko 2. Suosituksen yhteenveto

Koko elinkaari	Tietojärjestelmiin liittyvät riskit arvioidaan säännöllisesti. Suunnitellaan tiedon elinkaari kokonaisuudessaan, jotta esimerkiksi käytöstä poisto vaihe voidaan toteuttaa suunnitelmien mukaisesti. Suunnitelmia päivitetään kehityksen edetessä elinkaaren aikana.
Määrittely ja suunnittelu	Tunnistetaan tietojärjestelmän merkitys tiedonhallintayksikön toiminnalle ja sen jatkuvuudelle sekä siinä käsiteltävät tiedot ja niiden merkitys. Tunnistetaan tietojärjestelmään kohdistuvat ulkoiset vaatimukset. Arvioidaan tietojärjestelmään kohdistuvat riskit. Määritellään tietojärjestelmän kriittisyys ja tietoturvataso. Määritellään ja kuvataan tietojärjestelmään ulkoisista vaatimuksista, sisäisestä luokituksesta ja tunnistetuista riskeistä muodostuvat tietoturvavaatimukset. Määritellään tietojärjestelmän hyväksymiskriteerit. Suunnitellaan hankinnan ja toteutuksen aikaiset tietoturvaan liittyvät tehtävät ja niiden aikataulutus.
Kilpailutus ja hankinta	Tietojärjestelmään liittyvä hankinta tehdään suunnitelmallisesti. Hankinnassa huomioidaan luvun Tietoturvallisuus tietojärjestelmähankinnoissa periaatteet. Kilpailutukseen- ja hankintaan liittyviin kuvauksiin, vaatimuksiin, tarjouspyyntöihin ja sopimuksiin sisällytetään myös tietoturvaa koskevat vaatimukset. Huomioidaan, että tietoturvavaatimukset kohdistuvat sekä hankinnan kohteena olevaan tietojärjestelmään että sen toteuttavaan ja tarjoavaan toimittajaan.
Toteutus	Tehdään uhkamallinnus ja tunnistetaan tietojärjestelmään liittyvät riskit ja uhkaskenaariot. Valitaan ja dokumentoidaan tietoturvakontrollit. Tunnistetaan tietojärjestelmän liittymät muihin järjestelmiin sekä näihin liittyvät riippuvuudet osana kokonaisarkkitehtuuria. Toteutetaan valitut tietoturvakontrollit osana tietojärjestelmän kehitystä. Toteutetaan määritellyt katselmoinnit ja testaukset (arkkitehtuurikatselmointi, koodikatselmointi, toimin nallisuuksien testaus, väärinkäyttötapausten testaus/ tietoturvatestaus, suorituskykytestaus). Laaditaan tietojärjestelmän turvallisuuskuvaus ja muu dokumentaatio.

Käyttöönotto	Laaditaan käyttöönottosuunnitelma. Toteutetaan tarvittavat integraatiot ja liittymät muuhun ympäristöön ja varmistetaan integraatioiden tietoturvallisuus. Suoritetaan tietojärjestelmän hyväksyntätestaus. Tehdään hyväksyntä tietojärjestelmän käyttöönotosta.
Ylläpito	Riskejä ja suojaustason asianmukaisuutta katselmoidaan ja arvioidaan säännöllisesti. Tunnistetaan käsittely-ympäristössä ja vaatimuksissa tapahtuvien muutosten vaikutuksen tietojärjestelmään sekä niiden edellyttämät muutokset tietoturvakontrolleihin. Muutoksissa noudatetaan määriteltyjä muutos-hallintamenettelyitä. Tietojärjestelmää ylläpidetään tehtyjen suunnitelmien mukaisesti. Tässä yhteydessä huolehditaan muun muassa päivityksistä, varmuuskopioinnista, konfiguraation hallinnasta, kovennuksista ja haittaohjelmasuojauksesta. Tietojärjestelmää koskevaa dokumentaatiota ja kuvauksia päivitetään tehtyjen muutosten mukaisesti. Tietojärjestelmää valvotaan jatkuvasti tunnistettujen riskien mukaisesti.
Käytöstä poisto	Laaditaan ja hyväksytään käytöstä poistolle suunnitelma. Suunnitellaan ja toteutetaan säilytettävän tiedon migraatio. Sanitoidaan tuhottavat laitteet poistaen niissä olevat tiedot luotettavasti. Tuhotaan käytöstä poistuvan tietojärjestelmän osat.

6 Riskienhallinta (TiHL 13 §)

> ***Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.***

6.1 Tietoriskien analyysi ja hallinta

Tiedonhallintayksikön hyvänä käytäntönä on huolehtia tietoaineistojen, tietovarantojen ja tietojärjestelmien riskienhallinnasta (1):

- tunnistamalla ja arvioimalla olennaisia riskejä
- vähentämällä riskien todennäköisyyttä ja vaikutuksia hyväksyttävälle tasolle
- ylläpitämällä saavutettua tasoa tai
- vaihtoehtoisesti hyväksymällä jäännösriskit tai osa niistä.

Riskienhallinnalla pyritään toteuttamaan tietoturvallisuustoimenpiteiden yhdistelmä, jonka avulla varmistetaan tietoaineistojen ja tietojärjestelmien riittävä tietoturvallisuuden taso ja saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Oikeasuhtainen riskienhallinnan taso voidaan saavuttaa, kun tietoihin ja tietojärjestelmiin liittyvät vaikutukset on tunnistettu vaikutusanalyysin avulla ja riskien realisoitumisen todennäköisyys on otettu huomioon. Tietojen ja tietoaineistojen laadun varmistaminen on osa riskienhallintaa, sillä virheellinen tieto voi itsessään olla iso riski.

Tietoriskien hallinta on jatkuvaa toimintaa, johon liittyvät tavoitteet, periaatteet, vastuut ja keskeiset menettelyt tiedonhallintayksikön on hyvä kuvata. Johdon vastuulla on tietoriskien hallinnan organisointi ja resursointi. Hallintaprosessi vaikuttaa tiedonhallintayksikön toiminnan ja tavoitteiden arviointiin ja suunnitteluun. Tietoriskien hallinnassa havaitut riskit vaikuttavat tiedonhallintayksikön toimenpiteisiin koko sen toiminnan ajan.

Tietoriskien hallinnassa käytetään tiedonhallintayksikön tehtävien ja tietoaineistojen laajuuden perusteella valittuja menettelytapoja. Pienissä organisaatioissa tietoriskien

koordinointi voi olla vastuutettu yhdelle henkilölle ja organisoitu tehtäväksi johdon ja muutaman henkilön yhteistyönä. Tietoriskien hallintaan vaadittavien resurssien tarpeeseen vaikuttaa organisaation koon lisäksi tehtävien ja tietoaineistojen luonne. Prosessissa voidaan hyödyntää tavanomaisia toimisto-ohjelmistoja.

Laajemmissa organisaatioissa, ja etenkin ICT-tuotannosta vastaavissa organisaatioissa, riskienhallinnassa tarvitaan sekä useiden asiantuntijoiden ja keskijohdon ja ylemmän johdon työpanosta että erityisiä riskienhallintaohjelmistoja. Kaikissa organisaatioissa johdon tulee käsitellä tietoriskit vähintään kerran vuodessa osana muuta riskienhallintaa.

Tietoriskien käsittelyssä toimenpiteet mitoitetaan organisaation määrittämälle hyväksyttävälle tasolle. Organisaation johdolla on kokonaisvastuu riskienhallinnasta ja hyväksyttävästä riskitasosta. Jäännösriskejä ja tehtyjä tietoturvallisuustoimenpiteitä tulee seurata säännöllisesti. Tietoriskien seurannan tulee jatkua tietoaineistojen ja tietojärjestelmien koko elinkaaren ajan. Seurannassa tarkastetaan riskienkäsittelysuunnitelmien toteutuminen sekä tietoturvallisuustoimenpiteiden vaikuttavuus.

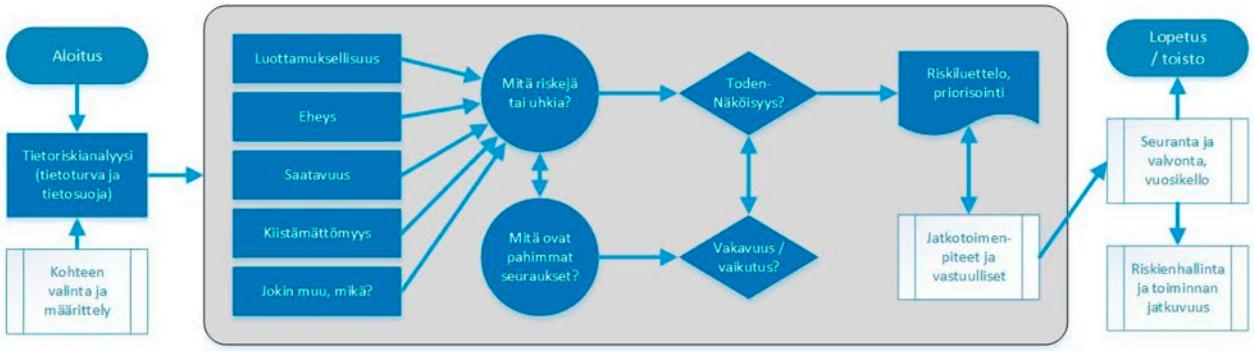
Tietoriskien hallinnassa on tärkeää kirjata **riskirekisteriin** kaikki potentiaaliset tietoriskit ja arvioida niiden todennäköisyys ja vaikutukset. Kaikkien keskeisten henkilöiden olisi hyvä osallistua arvioitavan kohteen tietoriskien selvittämiseen ja riskiarviointiin, jotta riskirekisteristä saadaan kattava ja eri asiantuntijoiden näkemykset tulevat huomioon otetuiksi. Myös tietoriskien syyt ja mahdollisen toteutumisen seuraukset on hyvä kirjata ylös. Usein on helpompaa puuttua riskin syyhyn kuin itse tietoriskiin. Tarkempia ohjeita riskien todennäköisyyden ja vaikutusten arviointiin löytyy julkaisusta Ohje riskienhallintaan (Valtiovarainministeriön julkaisuja 22/2017).

Tietoriskien selvittämisen ja arvioinnin lisäksi riskirekisteriin on hyvä kirjata jo aloitetut tai tehdyt riskienhallintatoimenpiteet sekä potentiaaliset uudet toimenpiteet. Tietoriskin omistaja päättää, mitkä hallintatoimenpiteet toteutetaan ja mitkä riskit voidaan hyväksyä ja kuka vastaa toimenpiteistä ja niiden aikatauluista. Hallintatoimenpiteet tulee suhteuttaa riskiarvioinnin perusteella tietoihin ja tietojärjestelmiin kohdistuviin uhkiin ja seurauksiin.

Riskit ja hallintatoimenpiteet tulee myös ottaa huomioon jatkuvuussuunnittelussa, jonka avulla pyritään takaamaan tietojen tai tietojärjestelmien riittävä saatavuus.

Sovittujen hallintatoimenpiteiden toteutumista ja aikataulujen pitävyyttä on hyvä seurata systemaattisesti, esimerkiksi kerran kuukaudessa tai vähintään neljä kertaa vuodessa. Tietoriskien arviointi on hyvä tehdä uudelleen, kun yksi tai useampia hallintatoimenpiteitä on tehty.

Kuvio 1. Tietoriskianalyysin prosessikaavio



6.2 Jäännösriskien hallinta

Hallintatoimenpiteiden jälkeen voimaan jääviä riskejä, joihin ei voida tai haluta enää vaikuttaa, kutsutaan jäännösriskeiksi. Niitä syntyy esimerkiksi hallintakeinojen ollessa riskin vaikutusten suhteen liian kalliita tai raskaita. Organisaatiolla tulee olla johtoryhmätason hyväksymä menetelmä jäännösriskien käsittelemiseksi ja niiden nostamiseksi tarvittaessa myös johtoryhmän käsiteltäväksi.

6.3 Tietoriskien hallinnassa tarvittavat tietoaineistot

Hyvänä käytäntönä tiedonhallintayksikössä on seurata toimintaympäristön turvallisuustilannetta viranomaislähteistä, viranomaiskontaktien ja mediaseurannan avulla sekä valvomalla jatkuvasti tietojärjestelmiä ja tietovarantoja. Tämä tulee tehdä ottaen huomioon mahdollinen erityislainsäädäntö, käytännesäännöt, muu informaatio-ohjaus, tulosohjaus ja taloudelliset voimavarat. Keskeisiä viranomaistietolähteitä ovat Kyberturvallisuuskeskuksen raportit sekä rikosasioissa Poliisi.

Julkisen hallinnon on hyvä ottaa omassa varautumisessaan huomioon tietoturvallisuudesta annetut VAHTI-ohjeet. Niihin kuuluu muun muassa tietoturvapoikkeamista mahdollisimman nopeasti tehty ilmoitus Kyberturvallisuuskeskukselle, jotta poikkeaman kohteeksi joutunut viranomainen saa apua tilanteesta toipumiseen. Lisäksi on aina suositeltavaa tehdä rikosilmoitus Poliisille, jos rikoksen tunnusmerkit täyttyvät. Oikea-aikainen toiminta koituu sekä julkisen hallinnon että kansalaisten eduksi.

Tietoriskien hallinnassa hyödynnetään tiedonhallintayksikön ylläpitämiä, tietojärjestelmiä koskevia metatietoja sekä tiedonhallintamallista löytyviä metatietokuvauksia tietoaineistoista ja -varannoista ja tietovarantojen ja -järjestelmien tärkeysluokituksista. Erityistä huomiota on kiinnitettävä siihen, missä tietojärjestelmät ja tietovarannot fyysisesti

sijaitsevat ja mitä tietoriskejä siitä mahdollisesti aiheutuu, toiminta ja kyseessä olevat tietoaineistot huomioon ottaen.

Tiedonhallintayksikkö ylläpitää riskiarvioiden tuloksista ja riskienkäsittelysuunnitelmista muodostuvaa tietoaineistoa sekä arvioi säännöllisesti, onko se osin tai kokonaan salassa pidettävä tai turvallisuusluokiteltava. Salassapitosäännösten niin vaatiessa viranomaisen on luokiteltava tietoriskejä koskeva tietoaineisto salassa pidettäväksi sekä turvallisuusluokitteluvaatimusten täyttyessä myös turvallisuusluokiteltava se kokonaan tai osittain.

6.4 Yleisiä vaatimuksia

Seuraavat yleiset vaatimukset tulisi ottaa huomioon riskienhallinnassa:

- Onko viranomainen tunnistanut ja dokumentoinut kaiken tiedon ja kaikki tietojärjestelmät, joista se on vastuussa?
- Onko näitä ylläpitävät ja käyttävät avainhenkilöt tunnistettu?
- Onko tietoihin, tietojärjestelmiin ja avainhenkilöihin mahdollisesti kohdistuvat uhkatekijät tunnistettu?
- Onko tiedoille ja tietojärjestelmille laadittu vaikutusanalyysi, jonka perusteella on mahdollista arvioida riskienhallintatoimenpiteiden oikeasuhtaisuus?
- Ovatko riskienhallintatoimenpiteet oikeasuhtaiset riskin realisoitumisen vaikutukseen ja todennäköisyyteen nähden?
- Ylläpidetäänkö riskirekisteriä ja arvioidaanko riskienhallintatoimenpiteiden toimivuutta säännöllisesti?

6.5 Säädökset ja lisätiedot

ISO 31000 Riskienhallinta

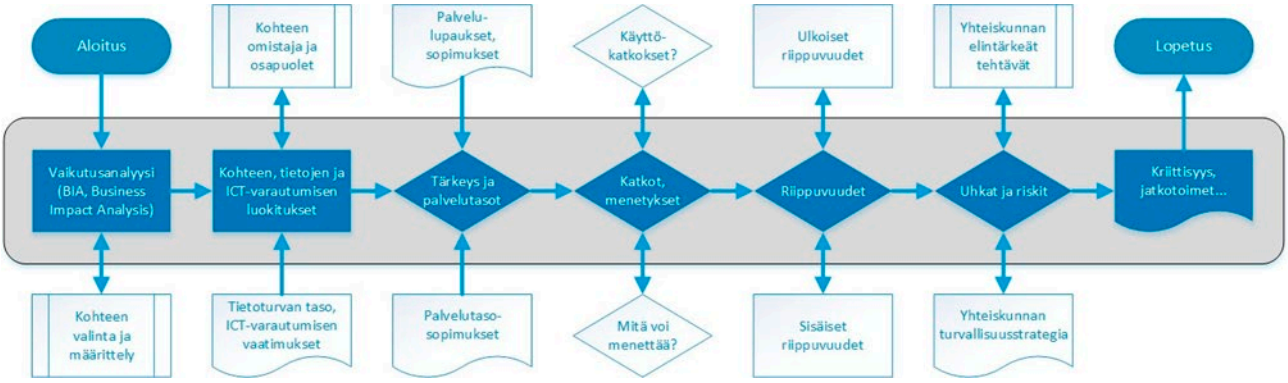
Riskienhallinnan järjestäminen (valtiovarainministeriön sivusto)

Riskienhallintapolitiikkamalli (valtiovarainministeriön sivusto)

VAHTI, Ohje riskienhallintaan (Valtiovarainministeriön julkaisuja 22/2017)

Ohje riskienhallintaan – Liitteet 1-6 (Valtiovarainministeriön julkaisuja 22/2017)

Kuvio 2. Vaikutusanalyysin prosessikaavio



7 Vikasietoisuus ja toiminnallinen käytettävyys (TiHL 13 §)

> ***Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.***

Olennaiset tietojärjestelmät kartoitetaan niitä varten laaditaan kriittisyysluokitus, jota tulee myös ylläpitää. Luokituksessa on huomioitava lakisääteiset tehtävät sekä riippuvuus muista järjestelmistä (oman organisaation sisällä sekä viranomaisten kesken).

7.1 Vikasietoisuus

Vikasietoisuutta varmistetaan esimerkiksi joillakin alla kuvatuista menetelmistä:

- Testaus ennen käyttöönottoa sekä merkittävien ylläpitotoimien yhteydessä
  - Testauksen laajuus ja toteutustapa valitaan järjestelmän riski- ja kriittisyysluokituksen mukaisesti
  - Testataan, että tietoturvallisuus on toteutettu ennalta määritettyjen vaatimusten mukaisesti
- Järjestelmätestaus ja hyväksymistestaus; tietoturvallisuuteen liittyvät käyttötapaukset
- Kuormitustestaus
- Koodikatselmoinnit
- Haavoittuvuusskannaukset tai automatisoidut tietoturvatestaukset
- Vikatilanteesta toipumisen suunnittelu

Testauksista pitää syntyä raportteja, joista selviää, mitä on testattu ja millaisia tuloksia testauksessa on saatu. Testaustulokset huomioidaan järjestelmäkehityksessä.

Tietoturvatestausta voidaan toteuttaa esimerkiksi seuraavia standardeja vasten:

Sovelluksen tietoturvallisuus

- OWASP Application Security Verification Standard (ASVS)
  - Varmuustaso (application security verification level) (1-3) valitaan sovelluksen kriittisyyden tai sensitiivisyyden perusteella

Mobiilisovelluksen tietoturvallisuus

- OWASP Mobile Application Security Verification Standard (MASVS)
  - Varmuustaso (L1 tai L2) ja vaatimus sovelluksen resilienssistä (-R-) valitaan sovelluksessa käsiteltävien tietojen sensitiivisyyden perusteella

IoT-laitteen tietoturvallisuus

- OWASP IoT Security Verification Standard (ISVS)
  - Varmuustaso (1-3) valitaan laitteen kriittisyyden tai siinä käsiteltävien tietojen sensitiivisyyden perusteella

Alustan (Käyttöjärjestelmä ja Middleware) tietoturvallisuus

- Center for Internet Security (CIS) benchmarkit
  - Varmuustaso (1 tai 2) valitaan järjestelmän kriittisyyden tai sensitiivisyyden perusteella

Hankittaessa sovelluksia, järjestelmiä, palveluita tai sovelluskehitystyötä ulkoisilta toimittajilta kannattaa sopimuksessa vaatia asiaankuuluvien edellä mainittujen standardien ja niihin liittyvien varmuustasojen täyttymistä.

Tietoturvatestausta kannattaa lisäksi erityisesti kohdistaa mahdollisessa uhkamallinnuksessa (esim. STRIDE-TRIM, Uhkapuu, tietovuo) tunnistettuihin merkittävimpiin uhkiin.

Tietoturvatestausta voidaan toteuttaa esimerkiksi seuraavien ohjeiden mukaisesti:

- OWASP Web Security Testing Guide
- OWASP Mobile Security Testing Guide
- The Open Source Security Testing Methodology Manual (OSSTMM)
- Open Source Security Testing Methodology Manual
- Secure Coding Guidelines For Java (koodikatselmointi)

Esimerkiksi seuraavat osapuolet voivat toteuttaa tietoturvatestausta:

- Dedikoidut tietoturvatestaajat, esim.
  - Tekninen tietoturvatestaus tietoturvatestaustyökaluja hyödyntämällä (haavoittuvuustestaus)
  - Tunkeutumis-/penetraatiotestaus
  - Red teaming (tunkeutumistestaus laajalla skopella ja aikaikkunalla)

- Ohjelmistotestaajat/ QA, esim.
  - Pääsynhallinnan testaus (tunnistaminen, valtuutus, lokitus)
  - Käyttö- ja väärinkäyttötapaukset
  - Yleisten syötteentarkistusten testaus
  - Businesslogiikan ohitusten testaus

- Automaattinen tietoturvatestaus, CI/CD, esim.
  - Dynaamiset ja staattiset koodiskannerit
  - Automatisoidut käyttö- ja väärinkäyttötapaukset (esim. Selenium, Robot Framework)
  - Automatisoidut haavoittuvuusskannaukset ja -testaukset (proxyt)

Määritettäessä haavoittuvuustestauksen löydösten kriittisyyttä on syytä käyttää standardoitua menetelmää, kuten CVSS (Common Vulnerability Scoring System), ja määritellä palveluntoimittajien sopimuksiin vaatimusten tiukkuus sen perusteella, onko kyseessä matalan, keskitason vai korkean luokan haavoittuvuus. Esimerkiksi korkean luokan haavoittuvuudet on pääsääntöisesti syytä korjata heti, eikä edetä niiden kanssa tuotantoon, kun taas alemman luokan haavoittuvuuksissa voidaan tapauskohtaisesti hyväksyä jonkin asteista riskiä (ainakin väliaikaisesti).

7.2 Toiminnallinen käytettävyys

Toiminnallisen käytettävyyden turvaamiseksi on varmistettava, että

- tietojärjestelmä on helposti opittava
- tietojärjestelmän toimintalogiikka on helposti muistettava
- tietojärjestelmän toiminta tukee niitä työtehtäviä, joissa käyttäjä järjestelmää hyödyntää
- tietojärjestelmä edistää käytön virheettömyyttä.

Edellä mainitut asiat varmistetaan mm. seuraavilla tavoilla:

- Räätälöidyissä järjestelmissä käytettävyys määritellään ja suunnitellaan organisaatiossa hyväksytyn menetelmän mukaan. Käytettävyyttä on testattava jatkuvasti kehittämisen aikana.
- Valmisohjelmistojen käytettävyys on testattava hyväksymistestauksen yhteydessä
- Testaus on toteutettava erilaisten käyttäjäryhmien näkökulmasta
- Käytettävyystestausta voidaan tehdä jo hankintavaiheessa, jolloin voidaan paremmin varmistaa hankittavan järjestelmän soveltuvuus käyttötarpeeseen

7.3 Toiminnallinen käytettävyys ja tietosuoja

Jotta tietojärjestelmän tietosuoja voidaan toteuttaa asianmukaisesti ja käyttäjälähtöisesti, on suunnittelussa hyödynnettävä alusta lähtien oletusarvoisen tietosuojan periaatteita. Niiden mukaan henkilötietojen käsittely tulee suojata ja tietosuojavelvoitteista huolehtia esimerkiksi minimoimalla käsiteltävän tiedon määrä sekä talletusaika ja suojaamalla mahdollisuuksien mukaan tieto salauksen tai pseudonymisoinnin avulla.

Oletusarvoisen tietosuojan turvaamiseksi tietojärjestelmän toteutuksessa on huomioitava, että

- tietosuoja on proaktiivista, ei reaktiivista
- tietosuoja on estävää, ei korjaavaa
- oletusasetukset takaavat tietosuojan toteutumisen
- tietosuoja on sisäänrakennettu järjestelmään (designiin)
- käyttäjälle tarjotaan täysi toiminnallisuus yksityisyydestä tinkimättä
- turvallisuus taataan päästä päähän, tiedot on suojattu koko elinkaaren ajan
- näkyvyys ja läpinäkyvyys taataan – pidetään tietojen käsittely avoimena
- kunnioitetaan käyttäjän yksityisyyttä – pidetään tietojen käsittely käyttäjäkeskeisenä.

Erityisesti on varottava, ettei järjestelmän suunnittelussa hyödynnetä ns. 'Dark patterneita' eli esimerkiksi käyttöliittymätoteutuksia, joilla tietoisesti pyritään ohjaamaan käyttäjän valintoja.

Suunniteltaessa ja testattaessa järjestelmän toiminnallisuutta tietosuojan näkökulmasta on tärkeää huomioida erityisesti seuraavat seikat:

- Hakutoiminnallisuus ei saa vuotaa valtuuttamattomille käyttäjille tietoa, josta voidaan päätellä tai johtaa rekisteröityjen henkilötietoja
- Liitetiedostot (kuvat, videot, toimistodokumentit jne.) pitävät usein sisällään näkymätöntä metadataa (esim. sijaintikoordinaatit, tunnistetiedot) – on syytä arvioida, voidaanko nämä poistaa automaattisesti tai muuten varmistaa, että ne eivät päädy luvattomille tahoille
- Käyttäjän päätelaitteelle voidaan tallettaa ei-välttämätöntä tietoa vain käyttäjän suostumuksella
- Suostumuksen pyytämisen tulee olla yksiselitteinen ja aktiivinen tahdonilmaisu. Suostumus tulee kerätä erikseen eri tarkoituksiin eikä sitä voi yhdistää esimerkiksi käyttöehtojen hyväksymiseen
- Käyttäjää täytyy informoida henkilötietojen käsittelystä läpinäkyvästi ja helposti ymmärrettävää kieltä käyttäen.

Sähköisten palveluiden toiminnallisessa käytettävyydessä pitää huomioida myös EU:n saavutettavuusdirektiivi ((EU) 2016/2102) ja sitä seuraava kansallinen lainsäädäntö (Laki digitaalisten palveluiden tarjoamisesta 306/2019). Saavutettavuusdirektiivin soveltamisalaan kuuluvat julkisen hallinnon ja julkista hallintotehtävää hoitavien organisaatioiden verkkosivustot ja mobiilisovellukset sekä lähes kaikki niiden sisällöt.

7.4 Säädökset ja lisätiedot

Saavutettavuusdirektiivi ((EU) 2016/2102

Laki digitaalisten palveluiden tarjoamisesta 306/2019

CVSS (Common Vulnerability Scoring System)

Open Web Application Security Project (OWASP)

Center for Internet Security (CIS)

ISO/IEC 27001/27002

8 Tietoturvallisuus tietojärjestelmähankinnoissa (TiHL 13 §)

> ***Viranomaisten on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.***

8.1 Tietoturvallisuustoimenpiteiden sääntely hankinnoissa

Tiedonhallintalain 4 luvussa on säädetty tietoturvallisuustoimenpiteiden toteuttamisen vähimmäisvaatimuksista. Ne kohdistuvat keskeisiltä osin tietoaineistoihin ja tietojärjestelmiin. Jotta viranomaistoiminnassa voidaan varmistua tietoturvallisuustoimenpiteiden asianmukaisuudesta, on tietoturvallisuustoimenpiteet määriteltävä jo tietojärjestelmien ja muiden ICT-palvelujen hankintojen valmisteluvaiheessa.

Tiedonhallintalain 13.4 § velvoittaa hankinnasta vastaavan viranomaisen varmistamaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Laissa ei ole säädetty varsinaisesti tietojärjestelmiin tai tietoaineistoihin liittyvistä konkreettisista toimenpiteistä, vaan ne on määriteltävä ja toteutettava kussakin tietojärjestelmässä käsiteltävien tietojen laadun ja luonteen näkökulmasta. Lisäksi tietoturvallisuustoimenpiteiden määrittelyyn ja toteuttamiseen vaikuttaa hankittavan tietojärjestelmän merkitys viranomaisen tehtävien hoidolle, lakisääteisten velvollisuuksien toteuttamiselle ja yhteiskunnan toiminnalle.

Tiedonhallintalain 13.1 §:ssä on säädetty tiedonhallintayksiköille velvollisuus seurata toimintaympäristönsä tietoturvallisuuden tilaa ja varmistaa tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.

Tiedonhallintalain 13.1 §:ssä on myös säädetty tiedonhallintayksikölle velvollisuus selvittää olennaiset tietojenkäsittelyyn kohdistuvat riskit, joiden perusteella tietoturvallisuustoimenpiteet mitoitetaan ja suhteutetaan niihin vaatimuksiin, joita tiedonhallintalaissa tietoturvallisuustoimenpiteille on säädetty. Hankintavaiheessa tulisi myös selvittää, miten tietoturvallisuuden tilaa seurataan tietojärjestelmän käytössä sen tuotantovaiheessa.

Euroopan unionin yleisessä tietosuoja-asetuksessa (EU) 2016/679 on säädetty sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamisesta. Tietosuoja-asetuksen resitaalin 78 mukaan sisäänrakennettu ja oletusarvoinen tietosuoja on otettava huomioon julkisten tarjouskilpailujen yhteydessä. Siksi hankintojen suunnitteluvaiheessa on selvitettävä ne tietosuojavaatimukset, jotka vaikuttavat hankinnassa tietoturvallisuustoimenpiteiden määrittelyyn tarjouspyyntöasiakirjoihin.

Tietosuoja-asetuksen 25 (2) artiklan perusteella rekisterinpitäjän on suunniteltava ja toteutettava henkilötietojen käsittelyyn asianmukaiset tietoturvallisuustoimenpiteet (tekniset ja organisatoriset toimenpiteet), joilla varmistetaan tietosuoja-asetuksessa säädettyjen tietosuojaperiaatteiden toteutuminen henkilötietojen käsittelyssä. Tietoturvallisuustoimenpiteet on toteutettava siten, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, ettei henkilötietoja oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.

Tietojärjestelmän hankinnasta johtuvat tietoturvallisuusjärjestelyjen muutosten arviointi kuuluu tiedonhallintalain 5.3 §:ssä tarkoitetun tiedonhallinnan muutosvaikutusarvioinnin piiriin. Säännöksen mukaan suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikössä on arvioitava näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa muun muassa tiedonhallintalain 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja -toimenpiteisiin. Säännöksessä tietojärjestelmän käyttöönotolla tarkoitetaan joko uuden tietojärjestelmän hankkimista tai käytössä olevan tietojärjestelmän uudistamista siten, että uudistuksella on vaikutusta tiedonhallintamallin sisältöön. Tiedonhallintalaissa tarkoitettu tietojärjestelmän käyttöönotto tarkoittaa jo hankintavaiheessa tehtävää muutosvaikutusarviointia muun muassa tietoturvallisuustoimenpiteiden järjestämisen osalta. Muutosvaikutusarvioinnissa arvioidaan toimintaympäristöön kohdistuvat riskit ja suunnitellaan tarvittavat tietoturvallisuustoimenpiteet suhteessa säädettyihin tietoturvallisuusvaatimuksiin.

Koska tiedonhallintalaissa on säädetty tiedonhallintayksikölle velvollisuus varmistaa sekä tietojärjestelmähankintojen toteuttamisessa että tietojärjestelmän elinkaaren ajan tietoturvallisuustoimenpiteiden asianmukaisuus, on tiedonhallintayksikön suunniteltava sekä hankintamenettelylle, tietojärjestelmän käyttöönoton eri vaiheille että tietojärjestelmän tuotantokäytölle riittävät kontrollit. Hankinnan ja toteutusprojektin turvallisuustoimenpiteiden ja -kontrollien on myös oltava toteutettavan järjestelmän turvallisuusvaatimusten mukaisia.

Tietoturvallisuustoimenpiteiden suunnittelu ja dokumentointi tietojärjestelmähankinnoissa voidaan jakaa osiin:

- Hankintaohjeet
- Tarjouspyyntö
- Tarjousten sisältöjen arviointi
- Hankintasopimuksen laadinta
- Hankintasopimuksen toimeenpano.

8.2 Tietoturvallisuus hankintaohjeissa

Tiedonhallintayksiköillä voi olla useita eri asiakirjoja, joilla ohjataan hankintojen toteuttamista. Tällaisia voivat olla esimerkiksi hankintasäännöt, taloussäännöt, hankintaohjeet, hankintastrategiat sekä tietojärjestelmien arkkitehtuurilinjaukset. Hankintojen toteuttamista ohjaaviin asiakirjoihin tulisi tarkentaa, miten hankintamenettelyssä toteutetaan tiedonhallintalaissa säädetyt vaatimukset hankinta-asiakirjojen tietoturvallisesta käsittelystä. Hankinnan kohteen tietoturvallisuustoimenpiteiden suunnitteluun vaikuttavat hankintojen toteutuksen yhteiset periaatteet kuuluvat myös asianmukaiseen hankintoja ohjaavaan dokumentaatioon. Tiedonhallintayksikössä noudatettavat tietoturvallisuusperiaatteet voivat olla määriteltyinä tiedonhallintamallissa, joten nekin vaikuttavat hankintojen suunnitteluun.

Hankintoja ohjaaviin asiakirjoihin tulisi sisällyttää:

- hankinta-asiakirjojen käsittelyä koskevat ohjeet, joista ilmenee, mitä tietoturvallisuustoimenpiteitä hankinta-asiakirjojen käsittelyssä on noudatettava tiedonhallintayksikössä
- tarjouspyynnön mallipohja, joka sisältää tiedot tiedonhallintayksikössä noudatettavista yleisistä tietoturvallisuustoimenpiteistä riippumatta hankintakohteesta
- sopimusmallin, jonka perusteella hankintakohdekohtaisesti hankintaan suunnittelevan vastuuhenkilön on kuvattava asianmukaiset tietoturvallisuusvaatimukset ja -toimenpiteet tarvittavilta osin niin henkilö-, tietoliikenne-, tietojärjestelmä-, tietoaineisto- kuin toimitilaturvallisuuden osalta.

Julkisia hankintoja toteutettaessa on myös eri toimijoiden roolien oltava selkeät. Tiedonhallintayksiköstä on säädetty tiedonhallintalaissa. Se on viranomaisorganisaatio, kuten valtion virasto tai kunta. Tiedonhallintayksikkö voi koostua useammasta viranomaisesta, joista kukin voi olla hankintalaissa tarkoitettu hankintayksikkö. Tässä suosituksessa käytetään tiedonhallintayksikön käsitettä, koska tiedonhallintayksikkö toimii pääsääntöisesti

viime kädessä hankintasopimuksen sopimusosapuolena, kuten kunta oikeushenkilönä, jota voi edustaa hankinnan tehnyt kunnallinen viranomainen hankintayksikkönä.

8.3 Tietoturvallisuusvaatimukset tarjouspyynnössä

Tiedonhallintayksikössä tarjouspyyntöasiakirjoihin sisällytettäviä tietoturvallisuusvaatimuksia ja -toimenpiteitä määriteltäessä on hankinnan kohteesta riippuen otettava huomioon julkisista hankinnoista ja käyttöoikeussopimuksista annetun lain (1397/2016) 3 §:ssä, julkisista puolustus- ja turvallisuushankinnoista annetun lain (1531/2011) 2 §:ssä sekä hallintolain (434/2003) 6 §:ssä säädetyt periaatteet. Tietoturvallisuusvaatimukset ja niitä toteuttavat toimenpidevaatimukset on suhteutettava hankittavan tietojärjestelmän tietosisältöihin ja tietojärjestelmän merkitykseen viranomaisen toiminnan kannalta. Määriteltäessä tietoturvallisuusvaatimuksia tarjouspyyntöön on huolehdittava siitä, että vaatimukset liittyvät hankinnan kohteena olevaan tietojärjestelmään sekä siihen liittyviin hankittaviin muihin palveluihin. Tietoturvallisuusvaatimuksissakin on huomioitava edellä mainituista laeista johtuvat vaatimukset tarjoajien tasapuolisesta ja syrjimättömästä kohtelusta. Lisäksi lainsäädäntö edellyttää vaatimusten olevan kohtuullisia suhteessa hankittavaan tietojärjestelmään.

Tarjouspyynnön laadinnassa on suositeltavaa käyttää erilaisia valmiita tietoturvallisuustoimenpiteiden toteuttamisen vaatimuslistoja tai -kriteeristöjä, mutta niiden sisältö on sovitettava yhteen hankittavan tietojärjestelmän ja siinä käsiteltävien tietojen kanssa. Tiedonhallintalain asettamien vähimmäisvaatimusten ylittäviä vaatimuksia määriteltäessä on arvioitava niiden soveltuvuus ja suhteutettava ne hankinnan kohteeseen, koska ylimitoitetut ja turhat vaatimukset voivat aiheuttaa lisäkustannuksia sekä vaikuttaa hankinnan kohteen käytettävyyteen ja tehokkuuteen. Vaatimusten on oltava perusteltuja ja asianmukaisesti määriteltyjä.

Tarjouspyynnössä on myös selkeästi eroteltava, mitkä ovat tietojärjestelmän tietoturvallisuudelle määriteltäviä ehdottomia vaatimuksia ja mitkä tietoturvallisuustoimenpiteitä sisältävät määritykset ovat tietojärjestelmän laatuun liittyviä kriteereitä, joita käytetään mahdollisesti tarjousvertailussa. Tarjoajille määriteltävät vaatimukset ja tarjousvertailussa käytetyt kriteerit on erotettava selkeästi toisistaan. Epäselvä tarjouspyyntö voi johtaa siihen, että tarjouskilpailu joudutaan toteuttamaan uudestaan.

Tietoturvallisuusvaatimusten on oltava niin selkeitä ja ymmärrettäviä, että alalla ammattimaisesti toimiva ja kohtuullisen valistunut tarjoaja saa niistä selon. Vaatimuksia sisältävät tarjouspyyntöasiakirjat on laadittava tavalla, joka mahdollistaa tarjoajille antaa selkeät ja yksiselitteiset vastaukset niin tarjottavan tietojärjestelmän vaatimusten täyttämisestä, kuin tarjousvertailussa käytettävistä kriteereistä. Epäselvät tarjouspyyntö ja sen liitteenä olevat,

täytettävät lomakkeet voivat johtaa siihen, ettei tiedonhallintayksikkö ei saa vertailukelpoisia tarjouksia. Tarjouksien käsittelyllä tiedonhallintayksikön on pystyttävä todentamaan tarjouksista, että tarjouspyynnössä tietojärjestelmälle määritellyt vaatimukset täyttyvät.

Tietoturvallisuusvaatimusten täyttymisen todentaminen tarjouksista on tärkeää myös tietosuojan toteuttamisen näkökulmasta, koska tietosuoja-asetuksen 28 (1) artiklan mukaan rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu. Tietojärjestelmän hankkivan tiedonhallintayksikön on siis varmistettava, että tietojärjestelmän toimittaja (esimerkiksi henkilötietojen käsittelijänä) täyttää ne vaatimukset, jotka henkilötietojen suojaamiseksi tarjouspyynnössä on määritelty osana tietoturvallisuustoimenpiteitä. Tiedonhallintayksikkö ei voi valita tietojärjestelmän toimittajaksi sellaista tarjoajaa, joka ei varmuudella voi täyttää tietoturvallisuustoimenpiteille määriteltyjä vaatimuksia.

Tarjouspyynnön laadinnassa on tärkeää ottaa huomioon, että tiedonhallintalaissa on säädetty tiettyjä pakollisia tietojärjestelmien tietoturvajärjestelyihin liittyviä vaatimuksia:

1. salassa pidettävien tietojen siirtäminen yleisessä tietoverkossa on toteutettava salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä.
2. tietojärjestelmän käyttöoikeudet on pystyttävä määrittelemään käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja käyttöoikeuksien myöntämistä koskevien toiminnallisuuksien on tuettava käyttäjä- ja käyttöoikeushallinnan ajantasaisena pitämistä.
3. tietojärjestelmän käytöstä ja tietoluovutuksista on pystyttävä keräämään tiedonhallintalain 17 §:n mukaiset tarpeelliset lokitiedot.
4. tietojärjestelmien rajapinnat on toteutettava tavalla, joka täyttää tiedonhallintalain 22 §:ssä säädetyt vaatimukset ja katseluyhteydet tavalla, joka täyttää tiedonhallintalain 23 §:ssä säädetyt vaatimukset.

Valtionhallinnossa tietojärjestelmän tarjouspyynnössä esitettäviin tietoturvallisuustoimenpiteitä koskeviin vaatimuksiin voi sisältyä myös asiakirjojen turvallisuusluokittelusta annetun asetuksen (1101/2019) mukaisia vaatimuksia. Tarjouspyyntö voi myös sisältää turvallisuusluokiteltavia tietoja, jolloin tarjouspyynnön käsittelyssä on otettava huomioon edellä mainitussa asetuksessa säädetyt vaatimukset turvallisuusluokiteltujen asiakirjojen käsittelystä.

Suositus tarjouspyynnön sisällöstä:

- Tarjouspyynnössä esitetään ne tietoturvallisuusvaatimukset, jotka tietojärjestelmään on toteutettava. Vaatimuksiin voi sisällyttää myös kuvaukset toteutettavista toimenpiteistä, kuten teknisistä ratkaisuista, tai antaa tarjoajille mahdollisuus tarjota tietoturvallisuustoimenpiteitä tietoturvallisuusvaatimusten täyttämiseksi. Tällöin tarjoajan on pystyttävä osoittamaan, että esitetty tietoturvallisuustoimenpide täyttää kiistatta määritellyn tietoturvallisuusvaatimuksen. Jos ei haluta vertailla tai arvioida erilaisia teknisiä tietoturvallisuustoimenpiteitä, kannattaa vaatimukset täyttävät tietoturvallisuustoimenpiteet kuvata tarjouspyyntöön. Tietoturvallisuustoimenpiteiden kuvaamisella ei saa edellyttää jonkin tietyn tuotemerkin käyttöä.
- Tietoturvallisuusvaatimuksissa on myös suositeltavaa kertoa, jos tiedonhallintayksikkö teetättää palvelun toimittajasta ja sen alaisuudessa toimivista, nimetyistä henkilöistä turvallisuusselvityksen.
- Tietoturvallisuusvaatimuksiin voidaan kytkeä mahdolliset toimittajan tietoturvallisuuden tietoturvasertifikaatit tai jokin muu tapa (esim. riippumattoman tietoturva-auditoijan auditointi), jolla toimittaja voi antaa vahvistuksen organisaationsa tietoturvallisuustasosta.
- Tietoturvallisuusvaatimuksiin sisältyy myös palvelutasoa koskevat vaatimukset, jotka tulisi kuvata selkeästi tarjouspyyntöön, koska palvelutasolla on vaikutus myös tietojärjestelmän hankintahintaan ja palvelun soveltuvuuteen. Palvelutaso voi vaihdella merkittävästikin eri tietojärjestelmien välillä riippuen tietojärjestelmän käyttötarkoituksesta ja merkityksestä viranomaisen toiminnalle.
- Tarjouspyyntöön on suositeltavaa sisällyttää myös tietoturvallisuusvaatimusten toteutumista mittaavia kriteerejä tietojärjestelmän palvelutuotannon aikana sekä vaatimukset vikasietoisuuden varmistamisesta säännöllisesti ainakin viranomaisen toimintaan olennaisesti vaikuttavan tietojärjestelmän osalta, koska tiedonhallintalain 13.2 § tätä edellyttää.
- Tarjouspyynnössä tulisi myös kuvata, miten tietojärjestelmän tuotantokäyttö turvataan poikkeusoloissa, mikäli tietojärjestelmä on olennainen viranomaisen tehtävien hoidon tai yhteiskunnan toiminnan kannalta katsottuna.
- Tarjouspyyntöön tulisi myös kuvata, millä menettelyillä muun muassa erilaisista poikkeamista ja havaituista tietoturvaloukkauksista raportoidaan tiedonhallintayksikölle, sekä miten ja kuinka nopeasti tällaisissa poikkeavissa tilanteissa toimitaan.
- Tarjouspyynnössä tulisi esittää myös kuvaukset muutoksenhallinnalle riippumatta siitä, koskevatko muutokset tietoturvallisuustoimenpiteiden ajan tasalla pitämistä vai jotain muuta ylläpitoa.

- Tarjouspyynnöstä tulisi myös ilmetä sanktiomenettelyt, jos tietojärjestelmän toimittaja ei ole noudattanut määriteltyjä tietoturvallisuusvaatimuksia.
- Tarjouspyynnössä tulisi esittää myös ehdot ja menettelyt sille, että tiedonhallintayksiköllä on oikeus auditoinneilla varmistaa tietoturvallisuustoimenpiteiden vaatimustenmukaisuus tietojärjestelmän toiminnassa ja tuotannossa. Auditointien osalta tulee kuvata kustannusten jakautumisen periaatteet sekä aika, jonka kuluessa ilmoituksesta auditointi voidaan tehdä. Varmistamiseen liittyvät tarkistuspisteet tulisi kiinnittää käytettävään tietojärjestelmän kehittämis- tai käyttöönottomalliin.
- Tarjouspyyntöön tulisi myös sisällyttää vahingonkorvausperiaatteet, jos tiedonhallintayksikölle aiheutuu vahinkoa toimittajan laiminlyönneistä tietoturvallisuustoimenpiteiden toteuttamisessa. Erityisen merkityksellistä vahingonkorvausperiaatteiden sisällyttämiselle on sellaisiin tarjouspyyntöihin, joissa hankinnan kohteena on henkilötietojen käsittelyyn tarkoitettu tietojärjestelmä. Tietosuoja-asetuksessa ja henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetussa laissa (1054/2018) on säädetty vahingonkorvausvastuut rekisterinpitäjälle, jolloin tiedonhallintayksikön on suositeltavaa varmistaa, että tietojärjestelmän toimittajan toiminnassa henkilötietojen käsittelyn takia aiheutuvat vahingonkorvausvastuut voidaan viime kädessä kohdentaa toimittajalle.
- Tarjouspyyntö voi sisältää myös tietoturvallisuuteen liittyviä laatukriteerejä, joita käytetään tarjousvertailussa. Tällaisten kriteerien asettaminen edellyttää tiedonhallintayksiköltä kuitenkin riittävää osaamista erilaisten tarjottujen tietoturvallisuusratkaisujen arvioimiseksi ja niiden vertailemiseksi. Tästä syystä tietoturvallisuustoimenpiteitä vertailuperusteina tulee harkita aina erikseen ja siihen vaikuttaa myös hankittavassa tietojärjestelmässä käsiteltävien tietojen luonne sekä teknologinen kehitys. Tavoiteltu tietoturvallisuuden minimitaso tulisi kuitenkin olla aina määritelty ehdottomana vaatimuksena.
- Tarjouspyynnössä tai sen liitteenä olevissa sopimuspohjissa tulisi esittää myös menettelyt ja vaatimukset sille, miten hankittavan tietojärjestelmän elinkaaren loppuvaiheessa turvataan tiedonhallintayksikön toiminta sekä tietojärjestelmässä olevien tietojen siirto (mukaan lukien lokitiedot) uuteen järjestelmään tai uudelle asiakkaalle. Lisäksi tulisi esittää myös menettelyt, jolla varmistetaan, että käytöstä poistetussa järjestelmässä ei enää ole käsiteltävissä sen käytöstä muodostuneita tietoaineistoja.
- Ennen tarjouspyynnön tekemistä tulee arvioida tietojärjestelmään liittyvät immateriaalioikeustarpeet (omistus-, muutos- ja luovutusoikeudet) ottaen huomioon tietojärjestelmän turvallisuusvaatimukset ja elinkaaren aikaiset kehitystarpeet. Nämä immateriaalioikeustarpeet kirjataan tarvittaessa tarjouspyyntöön vaatimuksina.

Tarjouspyynnössä esitetyt tietoturvallisuusvaatimukset ovat osa hankintasopimusta. Tarjouspyyntöön on suositeltavaa sisällyttää jo valmiiksi sopimusluonnos liitteineen, jolla varmistetaan niin tiedonhallintalaissa kuin tietosuoja-asetuksessa säädettyjen vaatimusten täyttyminen niin valitun toimittajan toiminnassa kuin hankitussa tietojärjestelmässä. Sopimusluonnoksessa tietoturvallisuusvaatimusten ensisijaisuus tulee varmistaa sopimusliitteiden pätemisjärjestyksessä.

8.4 Tarjousten sisällön arviointi

Tarjousten vastaanottamisen jälkeen tarjouksista on tarkastettava, täyttävätkö ne tarjouspyynnössä esitetyt vaatimukset. Hankintalain (74.1 §, 104.2 §) mukaan tarjoajan tulee tarjouksessaan osoittaa tarjoamansa tavaran, palvelun tai rakennusurakan olevan tarjouspyynnössä ja muissa hankinta-asiakirjoissa esitettyjen vaatimusten mukainen. Hankintayksikön on suljettava tarjouspyyntöä tai tarjousmenettelyn ehtoja vastaamattomat tarjoukset tarjouskilpailusta. Sellaiset tarjoukset, joissa on esitetty puutteellisia tietoja tarjouspyynnössä määritellyistä tietoturvallisuusvaatimuksista, on hankintalain nojalla suljettava tarjousvertailun ulkopuolelle.

Kuitenkin, jos puute on teknisluonteinen, esimerkiksi vaatimuslistassa olevan rastin puuttuminen, voi tiedonhallintayksikkö pyytää tarjoajaa täydentämään tarjousta. Tällöin täydennys voi olla vain havaitun puutteen teknisluonteinen täydentäminen ilman, että tarjous muuten sisällöllisesti muuttuu. Hankintalain (74.2 §, 104.2 §) mukaan hankintayksikkö voi pyytää tarjoajaa tai ehdokasta toimittamaan, lisäämään, selventämään tai täydentämään tarjouksensa tai osallistumisilmoituksensa tietoja tai asiakirjoja hankintayksikön asettamassa määräajassa. Täydentämisessä on kuitenkin otettava huomioon erityisesti tarjoajien tasapuolisen ja syrjimättömän kohtelun vaatimus.

Tarjousten käsittelyssä on suositeltavaa:

- varata riittävät ja asiantuntevat resurssit varmistamaan tarjouksissa esitettyjen tietoturvallisuustoimenpiteiden vastaavuus tarjouspyynnössä määriteltyihin tietojärjestelmän ja sen toimituksen tietoturvallisuusvaatimuksiin.
- käyttää useampaa tietoturva-asiantuntijaa arvioimaan tarjouksissa esitettyjä tietoturvallisuustoimenpiteisiin liittyvä ratkaisuja, jos niitä käytetään tarjousvertailuperusteina. Useamman asiantuntijan käyttö luo perustan asianmukaiselle tarjousten arvioinnille tasapuolisen ja syrjimättömän kohtelun varmistamiseksi. Arvioinnissa on käytettävä ennalta tarjouspyynnössä määriteltyjä kriteereitä ja asteikkoja, jotta tietoturvallisuustoimenpiteitä koskevien ratkaisujen arviointi ei muodosta rajoittamatonta harkintamarginaalia tarjousten arvioimiselle.

8.5 Hankintasopimuksen laadinta ja täytäntöönpano

Hankintamenettely on kumulatiivinen prosessi. Tarjouspyyntö, hankintailmoitus ja saatu tarjous ovat osa hankintasopimuskokonaisuutta. Jos tarjouspyynnössä on esitetty hankintasopimuksen ja sen liitteiden pohjat, voidaan niitä täydentää vain siltä osin kuin ne on jätetty tarjouspyyntövaiheessa avoimeksi tai niiden sisällössä on saatuun tarjoukseen liittyviä muuttujia. Sopimuksesta tai sen liitteistä on ilmettävä ne vaatimukset, jotka tarjouspyynnössäkin on esitetty tietoturvallisuusvaatimuksiksi. Koska tarjous on osa hankintasopimusta, on tarjouksessa esitetyt tietoturvallisuusvaatimuksia vastaavat valitun toimittajan esittämät tietoturvallisuustoimenpiteet toimittajaa sitovia. Hankintasopimukseen voidaan liittää tarvittaessa erikseen turvallisuussopimus, mutta sen on pitänyt joko olla mukana tarjouspyynnössä tai vastaavat vaatimukset on pitänyt esittää tarjouspyynnössä. Turvallisuussopimuksen sisällöllä voi olla vaikutuksia tietojärjestelmän toimittamiseen ja sen hinnoitteluun, jolloin turvallisuussopimusta ei voida pitää hankintamenettelystä irrallisena asiakirjana. Turvallisuussopimuksissa on suositeltavaa käyttää turvallisuussopimusmalleja, mutta niiden tarkoituksenmukaisuus ja sopivuus suhteessa hankittavaan kohteeseen on arvioitava jo tarjouspyynnön laatimisvaiheessa.

Tietojärjestelmähankinnoissa ja asiantuntijapalveluhankinnoissa käytetään tyypillisesti tiedonhallintayksikköjen laatimia vaitiolositoumuksia. Vaitiolositoumukset eivät ole merkityksellisiä muuta kuin sopimusoikeudellisesti määriteltäessä esimerkiksi salassapitovelvollisuuden rikkomisen perusteella sopimussakkoa tai sopimuksen purkuperusteita. Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 23 §:ssä on säädetty vaitiolovelvollisuudesta ja hyväksikäyttökiellosta. Mainitun lainkohdan mukaan vaitiolovelvollisuus ja hyväksikäyttökielto koskevat myös sitä, joka toimii viranomaisen toimeksiannosta tai hoitaa toimeksiantotehtävää. Säännöksellä tarkoitetaan, että esimerkiksi tietojärjestelmän toimittavan toimittajan palveluksessa olevat ja mahdolliset alihankkijat ovat vaitiolovelvollisia suoraan laissa säädetyn velvollisuuden velvoittamina. Jos laissa säädettyä vaitiolovelvollisuutta on rikottu, kuuluu se rikosvastuun piiriin. Jos vaitiolositoumuksia tehdään, on suositeltavaa sitoa ne osaksi varsinaista hankintasopimusta.

Ennen hankintasopimuksen tekemistä tiedonhallintayksikön tulisi vielä varmistaa, että hankintasopimuksessa tai sen liitteissä ovat kaikki ne kuvaukset ja vaatimukset tietoturvallisuustoimenpiteiden toteuttamiseksi, joita tarjouspyyntöasiakirjoissa ja tarjouksessa on esitetty.

8.6 Hankintasopimuksen toimeenpano

Hankinnan kohteena olevan tietojärjestelmän tai tuotteen toteutusvaiheen sekä palveluun liittyvän projekti- ja käynnistysvaiheen aikana varmistetaan prosessin eteneminen ja

tulosten laatu. Tietojärjestelmän kehittämisprosessin tai käyttöönottoprosessin eri vaiheissa tulisi olla tarkistuspisteitä, joissa arvioidaan muun muassa tietojärjestelmän tietoturvallisuustoimenpiteiden vaatimuksenmukaisuutta.

Jos toimintaympäristön tietoturvallisuuden tilassa tapahtuu muutoksia kehittämistyön aikana, tulisi ne ottaa huomioon tarvittaessa muutospyyntöinä toimittajalle, asianmukaisen ja riittävän tietoturvallisuuden varmistamiseksi ennen varsinaista tuotantokäyttöönottoa.

Ennen käyttöönottoa vielä hyväksymistestausvaiheessa tulisi tehdä systemaattinen tietoturvallisuustestaus tarjouspyynnössä esitettyjen tietoturvallisuusvaatimusten täyttämisen varmistamiseksi, sekä suorittaa vielä erikseen eri testausvaiheiden katselmointi sen varmistamiseksi, että tietoturvallisuusvaatimukset on otettu huomioon kaikissa tarpeellisissa testauksen vaiheissa.

Tiedonhallintayksikön ja siinä toimivien viranomaisten toimintaan olennaisesti vaikuttavien tietojärjestelmien osalta on otettava huomioon, että tiedonhallintalain 13.2 §:n mukaan tällaisten tietojärjestelmien vikasietoisuutta ja toiminnallista käytettävyyttä on testattava säännöllisesti. Käytännössä tämä tarkoittaa sitä, että tiedonhallintayksikön ja tietojärjestelmän toimittajan on luotava laadunvarmistusprosessi tuotantokäytössä olevan tietojärjestelmän vikasietoisuuden varmistamiseksi testauksen avulla. Tietojärjestelmien toiminnallinen käytettävyys tulisi varmistaa jo tietojärjestelmän kehittämis- ja käyttöönottovaiheissa sekä tehtäessä tietojärjestelmän toiminnallisuuksiin ja käyttöliittymään olennaisia, tietojärjestelmän käyttäjän toimintaan vaikuttavia päivityksiä. Toiminnallisen käytettävyyden varmistamisessa on suositeltavaa käyttää niin teknisiä käytettävyystestauksia kuin käyttäjillä suoritettavia käytettävyystestejä tai heuristisia asiantuntija-arviointeja.

8.7 Säädökset ja lisätiedot

Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)

Laki julkisista puolustus- ja turvallisuushankinnoista (1531/2011)

Hallintolaki (434/2003)

Laki viranomaisten toiminnan julkisuudesta (621/1999)

ENISA, Security Guide for ICT Procurement

Ohje turvallisuuskriittisiin hankintoihin, Valtiovarainministeriön julkaisuja 2019:7

ISO/IEC 27036

ISO/IEC 28000

ISO/IEC 27001 ja 27002

9 Tietojen siirtäminen yleisessä tietoverkossa (TiHL 14 §)

> ***Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä.***

Yleinen tietoverkko tarkoittaa tiedonhallintalaissa hallintovaliokunnan mietinnön mukaan internetiä, mutta on suositeltavaa käsitellä yleisenä tietoverkkona myös muita oman hallinnan ulkopuolisia verkkoalueita. Tällaisia ovat esimerkiksi operaattorien tarjoamat yritysverkot, joiden turvallisuusratkaisut tulee määritellä riskiarvioon perustuen. Koska yleiset tietoverkot ovat lähtökohtaisesti turvattomia, tulee niissä siirrettävä tieto olla salattua.

Katso salassa pidettävistä tiedoista tarkemmin tiedonhallintalautakunnan suosituksesta Salassa pidettävät tiedot ja asiakirjat (ei vielä julkaistu).

9.1 Tietoliikenteen salaus

Salausratkaisujen tulee perustua salassa pidettävän tiedon luokitteluun ja riskiarvioon. Salaus tulee toteuttaa kulloinkin voimassa olevien viranomaisvaatimusten ja suositusten mukaisesti.

Tietoliikenne tulisi ideaalitilanteessa salata päästä päähän, eli esimerkiksi käyttäjältä tietojärjestelmään tai kahden tietojärjestelmän välillä. Mikäli tämä ei ole mahdollista, voidaan organisaatioiden verkkojen välinen yleisen tietoverkon osuus salata esimerkiksi VPN-ratkaisuilla, jolloin organisaatioiden sisäisten verkkojen osuus jää salaamatta.

Lakitekstissä puhutaan salassa pidettävästä tiedosta ja yleisestä tietoverkosta. Lähtökohtaisesti kannattaa kuitenkin käsitellä kaikkea tietoa niin kuin se olisi salassa pidettävää ja salata tietoliikenneyhteydet aina oletusarvoisesti. Vastaavasti organisaatioiden omia verkkoja kannattaa käsitellä turvattomina verkkoina ja salata liikenne myös siellä samojen periaatteiden mukaan. Esimerkiksi avoimen HTTP-protokollan käyttöä sisäverkon julkistakin tietoa käsittelevissä järjestelmissä tulisi välttää.

9.2 Tietojen salaus ilman tietoliikenteen salausta

Mikäli tietoliikennettä ei kyetä salaamaan, tietojen salaus voidaan toteuttaa siirrettävien tietojen tai tiedostojen tasolla. Esimerkiksi sähköpostiviestin tai sen liitetiedostojen salaaminen mahdollistaa viestinvälityksen myös salaamattomien verkkojen yli. Mikäli salausratkaisuun kuuluu erillisen salasanan toimittaminen vastaanottajalle, salasanan suojaaminen on yhtä tärkeää kuin itse viestinkin. Salasanan toimittaminen vastaanottajalle ei saa tapahtua samaa reittiä pitkin kuin itse salatun tiedon toimittaminen.

9.3 Säädökset ja lisätiedot

Tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä, 18.1.2021

Kyberturvallisuuskeskus, Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen – kansalliset suojaustasot, 28.11.2018

Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät, 6.3.2020

Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut, 1.7.2020

10 Vastaanottajan tunnistaminen (TiHL 14 §)

> ***Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.***

Vastaanottajan tunnistaminen riittävän tietoturvallisella tavalla tulee määritellä käyttötapauskohtaisesti tiedon arvon ja riskiarvioinnin perusteella. Erityisesti, kun käsitellään turvallisuusluokiteltuja tietoja, tulee huomioida tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä.

10.1 Organisaatioiden sisäinen ja niiden välinen tietojensiirto

Lähtökohtaisesti tiedon vastaanottaja (ja pääsääntöisesti myös lähettäjä) tulisi tunnistaa vahvasti. Mikäli kyseessä on tietojärjestelmien välinen tietojensiirto, tapahtuu tämä tyypillisesti varmenteiden (sertifikaattien) avulla.

Käyttäjän tunnistamisessa tietojärjestelmään hyödynnetään tyypillisesti monivaiheiseen tunnistamiseen (Multi-Factor Authentication, MFA) perustuvaa vahvaa tunnistamista, jossa käytetään vähintään kahta seuraavista todentamistekijöistä: 1) tietoon perustuva todentaminen 2) hallussapitoon perustuva todentaminen, 3) luontainen todentaminen eli jokin luonnollisen henkilön fyysinen ominaisuus. Esimerkiksi käyttäjätunnus-salasana-parin lisäksi käytetään yhtä tai useampaa muuta tunnistavaa tekijää, kuten fyysistä laitetta, (verkko)sijaintia tai PIN-koodia matkapuhelinliittymään.

Organisaatioiden välisessä tietojensiirrossa yleisissä tietoverkoissa tulisi käyttää ainoastaan vahvaa tunnistamista.

10.2 Yleisölle tarjottavat digitaaliset palvelut

Laissa digitaalisten palvelujen tarjoamisesta (306/2019) todetaan, että salassa pidettäviä tietosisältöjä käsitelläkseen käyttäjän tulee tunnistautua vahvasti, mutta perustelluista

syistä voidaan riskiperusteisesti käyttää myös muuta tunnistustapaa, kuten käyttäjätunnus-salasana-paria.

Lähtökohtaisesti salassa pidettäviä tietoja käsiteltäessä käyttäjän vahva tunnistaminen tulee toteuttaa vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetun lain (617/2009) mukaisesti, esimerkiksi Suomi.fi-tunnistus-palvelun avulla.

Heikkoja tunnistustapoja ovat esimerkiksi käyttäjätunnus-salasana-pariin tai sosiaalisen median alustojen (esimerkiksi Facebook) tunnistamiseen perustuvat menettelyt.

10.3 Säädökset ja lisätiedot

Tiedonhallintalautakunnan suositus turvallisuusluokiteltavien asiakirjojen käsittelystä, 18.1.2021

Laki digitaalisten palvelujen tarjoamisesta (306/2019)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)

11 Tietoaineistojen turvallisuuden varmistaminen (TiHL 15 §)

> ***Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:***
>
> ***1) tietoaineistojen muuttumattomuus on riittävästi varmistettu;***
> ***2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;***
> ***3) tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;***
> ***4) tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;***
> ***5) tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;***
> ***6) tietoaineistot voidaan tarvittavilta osin arkistoida.***

11.1 Yleiset tietoturvallisuustoimenpiteet

Tietoaineistojen turvaamiseen liittyvät toimenpiteet voidaan jakaa karkeasti kolmeen luokkaan:

- teknisiin
- toiminnallisiin
- hallinnollisiin.

Teknisillä toimenpiteillä tarkoitetaan esimerkiksi palomuureja, salausmenetelmien käyttöä ja järjestelmien vahvistamista. Toiminnalliset tietoturvatoimenpiteet ovat esimerkiksi prosessikuvauksia. Hallinnolliset toimenpiteet ovat esimerkiksi ohjeistuksia, koulutuksia tai käyttöoikeuksien rajauksia.

Tiedonhallintayksiköt voivat hyödyntää edellä mainittuja toimenpiteitä varmistaessaan tietoaineistojensa turvallisuutta. Seuraavissa kappaleissa on tarkennuksia kuhunkin tapaukseen parhaiten sovelutuvista toimenpiteistä.

11.2 Tietoaineistojen muuttumattomuus

Viranomaisen tulee tarpeen mukaan varmistaa tietoaineistojen muuttumattomuus. Se merkitsee tiedon eheyttä, ts. tietoaineistoa ei saa muuttaa luvatta missään tietoaineiston elinkaaren vaiheessa ilman, että muutos voidaan havaita. Tällä pyritään varmistamaan, ettei tieto muutu oikeudetta tai hallitsematta. Muuttumattomuus on tärkeää esimerkiksi tietoaineiston todistusvoimaisuuden kannalta yksilöiden ja yhteisöjen etuja, oikeuksia ja velvollisuuksia määritettäessä.

Tavoitteena on, että tietoaineistoissa olevien asiakirjojen ja muiden tietojen aitous ja alkuperäisyys voidaan todentaa jälkikäteen. Lisäksi asiakirjoihin tehdyt muutokset havaitaan ja muutosvaiheet tunnistetaan sekä jälkikäteen pystytään selvittämään yksilötasolla, kuka muutokset on tehnyt.

11.2.1 Tarpeelliset tietoturvallisuustoimenpiteet

Tietoaineiston muuttumattomuuden varmistamiseen vaikuttaa sen luonne, ja tarpeelliset tietoturvallisuustoimenpiteet määritellään tapauskohtaisesti. Määrittämisessä huomioidaan riskiarvioinnissa saadut tulokset. Riskienhallinnan periaatteet on kuvattu luvussa Riskienhallinta (TihL 13§). Lisäksi on arvioitava, millaisia seurauksia tiedon eheyden vahingoittuminen aiheuttaa toiminnalle, sen jatkuvuudelle ja asiakkaille.

11.2.2 Muuttumattomuus elinkaaren eri vaiheissa

Tietoaineiston muuttumattomuus on otettava huomioon sen elinkaaren eri vaiheissa. Tiedon elinkaari ja käsittelyvaiheet sekä niihin liittyvät käsittelyketjut ja tietovirrat tulee tunnistaa sekä varmistaa tiedon muuttumattomuus ja luotettavuus. Tässä hyödynnetään muun muassa salausmenetelmiä ja eheystarkistuksia sekä sähköisiä allekirjoituksia.

Tietoaineiston luonti- ja vastaanottovaiheessa tulee tunnistaa toiminnan ja sen jatkuvuuden kannalta merkittävät tiedot, joiden kohdalla muuttumattomuudesta on huolehdittava. Tietoaineistot tulee säilyttää ja arkistoida (Kappale 2.6 Tietoaineistojen arkistointi) niin, että ne pysyvät muuttumattomina. Säilytyksessä ja arkistoinnissa tulee lisäksi varmistaa, että tietoaineistojen alkuperäisyys ja sisällön säilyminen muuttumattomana voidaan myöhemmin osoittaa.

Sähköisessä tiedonsiirrossa on huomioitava turvallinen tiedonsiirtotapa, jotta ulkopuoliset eivät pääse muokkaamaan tietoja. Tietojen siirron periaatteet on kuvattu kappaleessa Tietojen siirto tietoverkoissa. Muuttumattomuuden varmistamisen tarkoituksena on

tietoaineiston saapuminen vastaanottajalle lähetetyssä muodossa. Lisäksi vastaanottaja on tunnistettava tietoturvallisella tavalla, mikäli lähetettävä tietoaineisto sisältää salassa pidettävää materiaalia. Tietoturvallisen tunnistamisen periaatteet on kuvattukappaleessa Vastaanottajan tunnistaminen.

11.3 Vahingoilta suojaaminen

Viranomaisella tulee olla varmuus siitä, että käsiteltävä tieto tai järjestelmä on suojattu fyysisiltä vahingoilta, kuten tulipaloilta, vesivahingoilta ja ilkivallalta, sekä sähköisiä menetelmiä käyttäen aiheutetuilta fyysisiltä vahingoilta, kuten laitteiden rikkoutumiselta. Tietoa tai järjestelmää tulee suojata asianmukaisin, mutta riskiarvioinnin perusteella tarkoituksenmukaisin toimin. Lisätietoja järjestelmän vaikutusten ja riskien arvioinnista on luvussa Riskienhallinta (TiHL 13.1§).

Viranomaisen tulisi määritellä kullekin tietoaineistolle hyväksytyt sijainnit, joissa sähköisessä muodossa ja paperisina olevia aineistoja ja tietovarantoja voidaan käsitellä, säilyttää ja arkistoida. Sijaintien määrittelemisessä pitää huomioida palvelujen toteuttamistapa, kuten palveluntuottajat, pilvipalvelut ja tiedon käsittelyn fyysinen sijainti.

Tyypillisesti palveluntarjoajat säilyttävät ja ylläpitävät tietojen ja tietojärjestelmien käsittelyssä tarvittavia fyysisiä tiloja ja laitteita. Tällöin palveluntarjoajien kanssa on varmistettava fyysisen turvallisuuden vaatimusten toteutuminen. Viranomaisen tulee huomioida, että erityyppisiin tietoaineistoihin (esim. salassa pidettävät tai henkilötiedot) kohdistuu erilaisia suojausvaatimuksia, jotka voivat aiheuttaa lisävaatimuksia palveluntarjoajaa tai viranomaista kohtaan.

Viranomaisen tulee huomioida tietojen ja tietojärjestelmien fyysisessä turvallisuudessa seuraavat seikat:

- Rakenteellinen turvallisuus: Tilojen rakenteiden tulee täyttää niihin kohdistuvat vaatimukset. Lisätietoja rakenteellisista suosituksista löytyy Katakrin F-osiosta. Lisätietoja arkistoitujen asiakirjallisten tietojen tiloja koskevista määräyksistä ja vaatimuksista löytyy Kansallisarkiston asiakirjasta ”Määräys ja ohjeet arkistotiloista”.
- Turvallisuusalueet: Mikäli tiloissa säilytettävään tietoon kohdistuvat vaatimukset sitä edellyttävät, tulee toimitilat jakaa turvallisuusalueisiin, joiden tarkoituksena on estää tai riittävästi hidastaa oikeudettomien tahojen pääsyä käsiksi tietoon tai tietojärjestelmään.
- Salassapidettävät tiedot suojataan rakenteellisin, teknisin ja hallinnollisin keinoin. Hallinnollisen suojaamisen keinoja ovat esimerkiksi pääsyoikeuksien

rajoittaminen ja asianmukaiset salassapidettävän tiedon käsittelymenetelmät. Lisäksi kriittisiin tiloihin tai tietoihin pääsyä voidaan rajoittaa esimerkiksi turvallisuusselvitysten ja vaitiolositoumusten avulla.
- Olosuhdevalvonta: Tiloissa tulee olla siellä säilytettävän tiedon ja tietojärjestelmän vaatimuksiin nähden riittävä olosuhdevalvonta esimerkiksi tulipalon, vesivahingon, kaasuvuodon, pölyn ja tärinän varalta. Organisaatio määrittää riittävän tason riskienarvioinnin perusteella.
- Henkilöstöturvallisuus: Henkilöstö tulee kouluttaa tietojen käsittelyyn ja organisaation vierailijakäytäntöihin. Käytännöt sisältävät muun muassa ohjeet siitä, mille alueille ulkopuolisia henkilöitä saa organisaation tiloissa viedä ja miten tulee toimia, jos ulkopuolinen henkilö havaitaan väärissä tiloissa ilman saattajaa.
- Varavoima ja UPS: Tietoteknisissä tiloissa tulisi olla yllättävien virtapiikkien tai sähkökatkosten varalta UPS-ratkaisu. Se mahdollistaa tietojärjestelmän toiminnan, kunnes järjestelmä voidaan ajaa hallitusti alas ja siirtyä jatkuvuussuunnitelman mukaiseen toimintaan.

Lisätietoja toimitilaturvallisuuteen liittyvistä vaatimuksista ja ohjeistuksista löytyy VAHTI 2/2013 -ohjeesta ”Toimitilojen tietoturvaohje”.

Kriittiset järjestelmät tulisi kahdentaa, jotta toimintaa olisi mahdollista jatkaa toisesta konesalista tai sijainnista käsin silloin, kun toiminta ensisijaisessa ylläpitosijainnissa on estynyt. Tietoaineistojen turvaamiseksi tulee huomioida ja toteuttaa asianmukaisesti turvallisuusluokittelusta aiheutuvat tiedon käsittely- ja säilytysvaatimukset.

11.3.1 Yleiset vaatimukset

Seuraavat yleiset vaatimukset tulisi huomioida vahingoilta suojaamisessa:

- Täyttääkö palveluntarjoaja fyysiselle turvallisuudelle asetetut tietoturvallisuusvaatimukset, kun otetaan huomioon käsiteltävän tiedon turvallisuusluokittelu tai tietojärjestelmän kriittisyys?
- Onko pääsy suojattavaan tietoon rajattu vain niihin henkilöihin, joilla on oikeus käsitellä tietoja?
- Onko kriittiset järjestelmät kahdennettu siten, että toimintaa voidaan jatkaa, mikäli ensisijainen ylläpitosijainti ei ole käytössä?
- Mikäli viranomainen ylläpitää tietojärjestelmiä itse, onko tietojen turvallisuusluokituksesta ja järjestelmän kriittisyydestä aiheutuvat vaatimukset huomioitu ja täytetty?
- Onko fyysiset tilat eroteltu turvallisuusvyöhykkeisiin?

- Ovatko tilojen rakenteelliset ratkaisut riittävät?
- Onko tiloissa olosuhdevalvonta esimerkiksi tulipalon ja kosteusvaurioiden varalle?
- Onko käytössä varavoimaratkaisu, joka takaa järjestelmän toiminnan riittävällä tasolla hallitun alasajon aikana?

11.4 Alkuperäisyyden, ajantasaisuuden ja virheettömyyden varmistaminen

Tiedon käsittelyvaiheet on suunniteltava ja toteutettava sekä käsittelytoimenpiteitä valvottava siten, ettei tieto pääse muuttumaan tahallisesti tai tahattomasti tiedon käsittelyn elinkaaren aikana. Näin varmistetaan kunkin käsittelyhetken tarpeisiin riittävä tiedon eheys, virheettömyys, muuttumattomuus ja kiistämättömyys. Tämä on keskeistä tiedon todistusvoimaisuuden kannalta. Todistusvoimaisuus korostuu esimerkiksi silloin, kun käsitellään salassa pidettäviä tietoja tai erityisiä henkilötietoryhmiä ja niitä käytetään hallintopäätöksien perusteena tai kun muutetaan kriittisiä tietoja. Alkuperäisten asiakirjojen ja niiden liitteiden käsittely on suunniteltava siten, että ne ovat tarvittaessa saatavilla.

Tiedon käsittelyä suunniteltaessa, määriteltäessä ja muutettaessa on tarpeen tunnistaa tiedon käsittelyn elinkaaren eri vaiheet ja niihin liittyvät sellaiset käsittelytoimet tai tapahtumat, joihin voidaan luoda riittävät kontrollit tiedon kiistämättömyyden ja eheyden varmistamiseksi sekä tahattomien ja tahallisten virheiden havaitsemiseksi. Käsittelytoimenpiteet tulee kirjata lokeihin silloin, kun jälkikäteen on pystyttävä osoittamaan käsittelytapahtumat (ns. audit trail). Tiedon elinkaaren eri vaiheita käsitellään luvussa Elinkaaren huomioiminen tietojen käsittelyssä (TiHL 13 §).

Esimerkkejä suunniteltavista ja seurattavista kontrolleista ovat tiedon syöttämisen muoto- ja sisältötarkastukset, tiedon eheyden tarkistaminen siirron ja säilytyksen aikana, käyttäjien vahva tunnistaminen, tiedon käsittelijöiden määrän rajaaminen sekä käsittelytoimenpiteiden riittävän kattava kirjaaminen lokiin. Kontrollien toteuttamiseen voidaan käyttää erilaisia teknisiä ratkaisuja, kuten tarkistustoimenpiteitä tai -palveluja, raja-arvoja, aikaleimoja, määrityksiä tai pakotettuja valintoja sekä tarkistussummia.

11.5 Saatavuuden ja käyttökelpoisuuden varmistaminen

Tietojen ja tietoaineistojen saatavuuden tarve ja käyttökelpoisuus sekä niihin liittyvät vaatimukset tulee tunnistaa ja arvioida toiminnallisesta näkökulmasta esimerkiksi keskeytysvaikutusanalyysin (BIA), tietoriskianalyysin tai yhtenäisen kriittisyys- ja

tärkeysluokittelun avulla. Riittävä saatavuuden taso määritellään tietojen kriittisyyden ja luokituksen perusteella. Muun muassa salassa pidettävän tiedon saatavuutta voidaan rajoittaa esimerkiksi käyttöoikeuksin, kuitenkin siten, että asianmukainen tietojenkäsittely varmistetaan.

Kun tiedot ja tietoaineistot, niitä käsittelevät toiminnot sekä mahdolliset tietojärjestelmät luokitellaan toiminnalle kriittisiksi, on niiden saatavuuteen kiinnitettävä erityistä huomioita. Käsittelytoimien suunnittelussa on huomioitava myös erityis- ja poikkeustilanteet. Luokittelussa tulee huomioida tietojen ja tietojärjestelmien merkitys myös ulkoisille sidosryhmille ja asiakkaille.

11.5.1 Tietojen saatavuus

Tietojen saatavuuteen vaikuttavat erilaiset toiminnalliset ja tekniset ratkaisut, kuten kahdennukset sekä tietojen ja tietoaineistojen hajasijoittaminen. Sen arvioinnissa tulee huomioida esimerkiksi oman konesaliratkaisun ja pilvipalveluratkaisun eroavaisuudet.

Olennaisiin kontrolleihinkuuluu tiedon varmistaminen; tietoaineistojen ja tietojärjestelmien varmuuskopiointi siten, että missään häiriötilanteessa alkuperäiset tiedot ja tietoaineistot eivät pääse katoamaan. Valitut toiminnalliset ja tekniset ratkaisut tulee testata asetettujen tavoitteiden varmistamiseksi.

Tietojärjestelmissä (ml. pilvipalvelut), joilta edellytetään korkeaa saatavuutta, on varauduttava palvelinympäristön saatavuusriskeihin. Esimerkiksi kansainvälisten tai paikallisten tietoliikenneyhteyksien katkojen sekä konesalin vaihdon varalle tulisi olla ennakolta sovitut menettelyt, joita voidaan testata ja varmistua tietojen saatavuudesta näissäkin tilanteissa. Erityisesti pitää varmistaa, että tiedot saadaan tarvittaessa palautettua ulkomaisesta konesalista Suomeen.

Tietojen ja tietoaineistojen kriittisyys voi olla myös aikasidonnaista. Tietojärjestelmien toipumisaika (RTO) tulee suhteuttaa aikasidonnaisuuteen. Tietojen ja tietoaineistojen ajantasaisuuden varmistaminen häiriön sattuessa edellyttää tarpeellista varmuuskopiotaajuutta. Jos tiedot ja tietoaineistot muuttuvat nopealla tahdilla ja ajantasaisuus on olennaista, tulee varmuuskopioinnin tai muun tiedon ajantasaisuuden varmistusmenettelyn olla jatkuvaa.

Saatavuuden varmistamisessa tulee huomioida, että poikkeusolosuhteissa normaaleja teknisiä saatavuusratkaisuja ei mahdollisesti ole käytettävissä. Kriittisten tietojen ja tietoaineistojen saatavuus tulee tällöin suunnitella osana tietojärjestelmien toipumissuunnittelua sekä toiminnan jatkuvuus- ja varautumissuunnittelua.

Osana saatavuuden varmistamista tulee tietojenkäsittely-ympäristöissä käyttää sellaisia tiedostomuotoja sekä tietovälineitä, joilla on mahdollisimman laaja kattavuus ja elinkaari. Yleisesti tunnettu ja hyödynnettävä tiedostomuoto on edellytys jaettavuudelle. Mikäli tiedostomuoto tai tietoväline vanhenee, tulee olla menettelyt uudemman ja tuetun ratkaisun käyttöönottoon. Erityisesti tähän tulee varautua silloin, kun tietojen ja tietoaineistojen elinkaarien oletetaan olevan pitkiä. Tietojen saatavuus pitää varmistaa niin kauan kuin tietoa säilytetään siihen tarkoitukseen, mihin se on kerätty.

11.5.2 Tietojen käyttökelpoisuus

Tietojen ja tietoaineistojen tulee olla käyttökelpoisia viranomaisen toiminnan tarpeisiin. Tietoon kohdistuvat tahalliset tai tahattomat muutokset ja poistot tulee voida estää sekä havaita.

Tiedon luotettavuutta ja eheyttä voidaan suojata esimerkiksi käyttövaltuuksilla, tarkistussummilla ja sähköisillä allekirjoituksilla. Lisäksi luotettavuutta ja eheyttä voidaan varmistaa suunnittelemalla, keräämällä ja valvomalla lokitietoja tiedon käsittelystä sekä tietojenkäsittely-ympäristön tapahtumista. Käyttövaltuuksia käsitellään luvussa Käyttövaltuudet (TiHL 16 §) ja lokitietoja luvussa Lokitietojen kerääminen (TiHL 17§).

Tiedon alkuperä tai lähde (autenttisuus) tulee voida varmistaa riittävällä varmuudella. Usein on tärkeää varmistaa tiedon kiistämättömyys ja todistusvoima siltä varalta, että esimerkiksi toinen osapuoli koettaa kiistää tiedon oikeellisuuden. Myös tiedon käsittelytoimiin liittyvät luotettavat aikamerkinnät (esim. ilmoituksen saapumisaika) ovat tärkeitä kiistämättömyyttä arvioitaessa.

Tiedon alkuperästä, lähteestä ja kiistämättömyydestä voidaan varmistua tunnistamalla luotettavasti tiedon vaihdon osapuolet sekä tiedon luojat ja muokkaajat. Esimerkiksi sähköisillä allekirjoituksilla ja varmenteilla voidaan sekä tunnistaa tiedonvaihdon osapuolet ja varmistua heistä että suojella tiedon eheyttä. Tunnistamista käsitellään luvussa Vastaanottajan tunnistaminen (TiHL 14 §).

Tiedon käyttökelpoisuuteen vaikuttavat myös ajantasaisuus (kuinka tuore tieto on), virheettömyys sekä löydettävyys. Tietojen löydettävyyttä voidaan parantaa metadatan ja kattavien hakuratkaisujenavulla. Tiettyjen tietojen ajantasaisuutta voidaan tarpeen mukaan tarkistaa ulkoisesta palvelusta (esim. henkilötiedot väestötietojärjestelmästä) tai asianomaiselta taholta (esim. asiakkaalta itseltään).

Käyttökelpoisuuden varmistamisessa metatietojen ja hakuratkaisujen merkitystä ei voi korostaa liikaa. Suositeltavaa on käyttää koneluettavia tiedostomuotoja, jotka

mahdollistavat erilaiset sisältöhaut, analysoinnin ja kaiken kaikkiaan tiedon tehokkaamman hyödyntämisen eri tarkoituksissa, myös viranomaisen omissa prosesseissa.

Tietojen käyttökelpoisuutta voidaan parantaa hyödyntämällä avoimia, rakenteellisia ja standardoituja tietoformaatteja ja rajapintoja (esim. XML/SOAP, JSON/REST tai PDF/A). Näitä hyödyntäen voidaan tietoja todennäköisemmin yhdistellä ja käsitellä pitkänkin ajan kuluttua sekä edistää samalla tietojärjestelmien yhteentoimivuutta.

11.6 Tietoaineistojen arkistointi

Tässä kuvataan tietoaineistojen arkistoinnissa huomioitavia tietoturva-asioita. Kantaa ei oteta arkistoinnissa tarvittaviin menettelyihin, joista ohjeistetaan erikseen.

Arkistoinnin tarvemäärittely tehdään organisaatiossa noudattaen tiedonohjaus- tai arkistonmuodostussuunnitelmaa tai vastaavaa, jossa kuvataan ne tietoaineistot ja -joukot, jotka arkistoidaan. Arkistoitavat tiedot tulee voida helposti tunnistaa ja niiden arkistointikelpoisuus tulee varmistaa alusta lähtien aineistojen elinkaaren kaikissa vaiheissa käyttämällä soveltuvia tallennustapoja ja menettelyjä (mm. meta- ja kuvailutiedot).

Henkilötiedoissa tulee varmistua siitä, että ne ovat asianmukaisia, olennaisia ja rajoitettuja siihen tarkoitukseen, mikä on olennaista arkistointikäytössä. Henkilötietojen arkistoinnissa tulee ottaa huomioon, että tietosuoja-asetuksen edellyttämät suojatoimet on toteutettava myös arkistointivaiheessa. Kun siirrytään tiedon säilytysvaiheesta arkistointivaiheeseen vaativat henkilötietojen minimointi ja käyttövaltuudet erityistä huomiota. Kuhunkin henkilötietoaineistoon sovellettavat suojatoimet tulee kuvata selkeästi.

Tiedon eheydestä ja muuttumattomuudesta tulee huolehtia niin säilytys- kuin arkistointivaiheessakin. Myös asiakirjojen asianmukainen tuhoaminen on varmistettava säilytysaikojen kuluttua umpeen. Tuhoamisesta tullaan ohjeistamaan tarkemmin mm. tiedonhallintalautakunnan suosituksessa salassa pidettävän tiedon käsittelystä.

Tietoaineiston arkistoinnissa turvallisuusjärjestelyt toteutetaan tietoaineiston luokituksen vaatimalla tasolla. Organisaation tulee varmistaa, että käytettävä arkistointiratkaisu on riittävän tietoturvallinen kaikille sinne tallennettaville tietoaineistoille.

Arkistoitujen tietojen käsittelyprosesseissa tulee ottaa huomioon eri arkistoaineistojen turvallisuusvaatimukset. Salassa pidettävien sekä henkilötietoaineistojen osalta tulee huolehtia siitä, että arkistointijärjestelmä mahdollistaa käsittelytoimien seurannan.

11.7 Säädökset ja lisätiedot

Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/NCSA_salausratkaisut.pdf

Kyberturvallisuuskeskus, ohjeita viestinnän suojaamiseen https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjeita_viestinnan_suojaamiseen.pdf

Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaiselle https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Kyberturvallisuuskeskus, Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

VAHTI 2/2014 Tietoturvallisuuden arviointiohje https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22014-tietoturvallisuuden-arviointiohje

VAHTI 2/2013 Toimitilojen tietoturvaohje https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22013-toimitilojen-tietoturvaohje

VAHTI 2/2012 ICT-varautumisen vaatimukset https://www.suomidigi.fi/vahti-22012-ict-varautumisen-vaatimukset

Kansallisarkisto, Määräys ja ohjeet arkistotiloista https://arkisto.fi/fi/normit/maeaeraeykset/maeaeraeys-ja-ohjeet-arkistotiloista

Turvallisen sovelluskehityksen käsikirja, DVV 19.5.2020 https://www.suomidigi.fi/sites/default/files/2020-05/Turvallisen%20sovelluskehityksen%20k%C3%A4sikirja.pdf

VAHTI 1/2013 Sovelluskehityksen tietoturvaohje https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-12013-sovelluskehityksen-tietoturvaohje

Kansallisarkisto, Julkishallinnon asiakirjahallinnon ja arkistotoimen ohjaus https://arkisto.fi/fi/viranomaisille/Julkishallinnon-asiakirjahallinnon-ja-arkistotoimen-ohjaus

12 Vahingoilta suojaaminen (TiHL 15 §)

> ***Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:***
> ***2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;***

Viranomaisella tulee olla varmuus siitä, että käsiteltävä tieto tai järjestelmä on suojattu fyysisiltä vahingoilta kuten tulipalot, vesivahingot tai ilkivalta sekä sähköisiä menetelmiä käyttäen aiheutetuilta fyysisiltä vahingoilta kuten laitteiden rikkoutuminen. Tietoa tai järjestelmää tulee suojata asianmukaisin, mutta riskiarvioinnin perusteella tarkoituksenmukaisin toimin. Lisätietoja järjestelmän vaikutusten ja riskien arvioinnista on luvussa 2.

Viranomaisen tulisi määritellä kullekin tietoaineistolle hyväksytyt sijainnit, joissa sähköisessä ja paperisina olevia aineistoja ja tietovarantoja voidaan käsitellä ja myös säilyttää. Sijaintien määrittelemisessä pitää huomioida palvelujen toteuttamistapa, kuten palvelun-tuottajat, pilvipalvelut ja tiedon käsittelyn fyysinen sijainti.

Tyypillisesti palvelutarjoajat säilyttävät ja ylläpitävät tietojen ja tietojärjestelmien käsittelyssä tarvittavia fyysisiä tiloja ja laitteita tai näiden hankinnan sopimusta, kuten pilvipalvelut. Tällöin palveluntarjoajien kanssa on varmistettava fyysisen turvallisuuden vaatimusten toteutuminen. Viranomaisen tulee huomioida, että erilaisiin tietoaineistoihin (esim. salassa pidettävät tai henkilötiedot) kohdistuu erilaisia suojausvaatimuksia, jotka aiheuttavat lisävaatimuksia palveluntarjoajaa ja/tai viranomaista kohtaan.

Viranomaisen tulee huomioida tiedon ja tietojärjestelmien fyysisen turvallisuuteen liittyen seuraavat seikat:

- Rakenteellinen turvallisuus: Tilojen rakenteiden tulee täyttää niihin kohdistuvat vaatimukset. Lisätietoja rakenteellisista suosituksista löytyy Kansallisen auditointikriteeristön F-osiosta. Lisätietoa pysyvästi säilytettävien asiakirjallisten tietojen arkistotiloja koskevista määräyksistä ja vaatimuksista löytyy Kansallisarkiston asiakirjasta Määräys ja ohjeet arkistotiloista.
- Turvallisuusalueet: Mikäli tiloissa säilytettävään tietoon kohdistuvat vaatimukset sitä edellyttävät, tulee toimitilat olla jaettu turvallisuusalueisiin, joiden tarkoituksena on estää tai riittävästi hidastaa oikeudettomien tahojen pääsy käsiksi tietoon tai tietojärjestelmään.

- Salassapidettävien tietojen suojaaminen tapahtuu rakenteellisin, teknisin ja hallinnollisin keinoihin. Hallinnollisen suojaamisen keinoja ovat esimerkiksi pääsyoikeudet salassapidettävään tietoon ja asianmukaiset salassapidettävän tiedon käsittelymenetelmät. Lisäksi kriittisiin tiloihin tai tietoihin pääsyä voidaan rajoittaa esimerkiksi turvallisuusselvitysten ja vaitiolositoumusten avulla.
- Olosuhdevalvonta: Tiloissa tulee olla säilytettävän tiedon ja tietojärjestelmä vaatimuksiin nähden riittävä olosuhdevalvonta esimerkiksi tulipalon, vesivahingon, kaasuvuodon, pölyn ja tärinän varalta. Organisaatio määrittää tason riittävälle olosuhdevalvonnalle riskienarvioinnista saatujen tulosten avulla.
- Henkilöstöturvallisuus: Henkilöstö tulee kouluttaa tietojen käsittelyyn ja organisaation vierailijakäytäntöihin. Ne sisältävät muun muassa ohjeet siitä, mille alueille ulkopuolisia henkilöitä saa organisaation tiloissa viedä ja miten toimia, jos ulkopuolinen henkilö havaitaan väärissä tiloissa ilman saattajaa.
- Varavoima ja UPS: Tietojärjestelmillä tulisi olla käytössä UPS-ratkaisu yllättävien virtapiikkien tai sähkökatkosten varalta. Se mahdollistaa järjestelmän toiminnan siksi aikaa, kunnes se voidaan ajaa hallitusti alas ja siirtyä jatkuvuussuunnitelman mukaiseen toimintaan.

Lisätietoja toimitilaturvallisuuteen liittyvistä vaatimuksista ja ohjeistuksista löytyy VAHTI 2/2013 – Toimitilojen tietoturvaohjeesta.

Kriittiset järjestelmät tulisi kahdentaa, niin että toimintaa voidaan jatkaa toisesta konesalista tai sijainnista käsin silloin, kun toiminta ensisijaisessa ylläpitosijainnissa on estynyt. Tietoaineistojen osalta tulee huomioida tiedon turvallisuusluokittelun kautta tulevat tiedon käsittely- ja säilytysvaatimukset ja toteuttaa nämä asianmukaisesti.

12.1 Yleisiä vaatimuksia

Seuraavat yleiset vaatimukset tulisi huomioida vahingoilta suojaamisessa:

- Täyttääkö palveluntarjoaja tietoturvallisuusvaatimukset fyysisen turvallisuuden osalta, kun on huomioitu käsiteltävän tiedon turvallisuusluokittelu tai tietojärjestelmän kriittisyys?
- Onko pääsy suojattavaan tietoon rajattu vain niihin henkilöihin, joilla on oikeus käsitellä tietoja?
- Onko kriittiset järjestelmät kahdennettu siten, että toimintaa voidaan jatkaa, mikäli ensisijainen ylläpitosijainti ei ole käytössä?

- Mikäli viranomainen ylläpitää tietojärjestelmiä itse, onko tietojen turvallisuusluokituksesta ja/tai järjestelmän kriittisyydestä johtuvat vaatimukset huomioitu ja täytetty?
- Onko fyysiset tilat eroteltu turvallisuusvyöhykkeisiin?
- Ovatko tilojen rakenteelliset ratkaisut riittävät?
- Onko tiloissa olosuhdevalvonta tulipalon ja kosteusvaurioiden varalle?
- Onko käytössä varavoimaratkaisu, joka takaa järjestelmän riittävän toiminnan hallitun alasajon ajaksi?

12.2 Säädökset ja lisätiedot

Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaiselle

Kyberturvallisuuskeskus, Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

VAHTI 2/2014 – Tietoturvallisuuden arviointiohje

VAHTI 2/2013 – Toimitilojen tietoturvaohje

VAHTI 2/2012 – ICT-varautumisen vaatimukset

Kansallisarkisto, Määräys ja ohjeet arkistotiloista

13 Tietojärjestelmien käyttöoikeuksien hallinta (TiHL 16 §)

> ***Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja ne on pidettävä ajantasaisina.***

Asianmukaisen käyttöoikeuksien hallinnan avulla mahdollistetaan tietojen luvallinen käyttö ja estetään niiden luvatonta käyttöä.

Ainoastaan oikeutetuille käyttäjille sekä järjestelmille myönnetään pääsy- ja käyttöoikeus tietoihin ja tietojärjestelmiin. Käyttöoikeuksien hallinnan tulee noudattaa vähimpien oikeuksien periaatetta ja sen on katettava järjestelmien koko elinkaari. Vähimpien oikeuksien periaate tarkoittaa, että käyttäjälle annetaan tietojärjestelmiin vain sellaiset käyttöoikeudet ja -valtuudet, jotka ovat työtehtävien kannalta tarpeellisia. Käyttäjätilien hallintaa ja käyttöä seurataan ja valvotaan poikkeamien ja uhkien havaitsemiseksi sekä niihin reagoimiseksi. Seurannassa ja valvonnassa on huomioitava lokitietojen keräämistä ja käyttöä koskevat suositukset (17§).

13.1 Käyttöoikeuksien hallinnan edellytykset

1. Käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).
2. Käyttäjätilien luontiin, hyväksymiseen, ylläpitoon ja poistamiseen tulee olla kuvattu menettely ja käyttöoikeuden tulee perustua tunnuksen saajan kanssa tehtyyn sopimukseen (esim. työsopimus, ostopalvelusopimus).
3. Käyttöoikeuksien käsittely ja myöntäminen tulee ohjeistaa.
4. Järjestelmien käyttäjille annetaan vain ne tiedot, oikeudet tai valtuudet, jotka ovat työtehtävien kannalta tarpeellisia. Käyttöoikeudet on määriteltävä kullekin tietojärjestelmän käyttäjälle hänen tyypillisten työtehtäviensä perusteella ja vähimpien oikeuksien periaatetta noudattaen (Principle of Least Privilege).
5. Jokaiselle käyttäjätunnukselle tulee olla nimetty vastuuhenkilö eli omistaja. Tunnuksen omistajuus on määriteltävä erikseen, jos myönnetään tunnuksia kone- tai palvelutileille, kuten esim. ohjelmistorobotiikan käyttöön.
6. Yhteiskäyttötunnuksia tulee käyttää vain erikseen hyväksytyissä poikkeustapauksissa.

7. Järjestelmään myönnetyistä käyttöoikeuksista tulee olla saatavilla ajantasainen tieto. Jokaisesta myönnetystä käyttöoikeudesta ja siihen tehdyistä muutoksista tulee jäädä merkintä (paperi tai sähköinen).
8. Käyttöoikeuden myöntämisen yhteydessä tulee tarkistaa, että henkilöllä on oikeutus käyttöoikeuden saamiselle sekä riittävä koulutus kyseisen järjestelmän käyttöön.
9. Organisaation ulkoiset ja sisäiset käyttäjät tulee olla eroteltavissa käyttäjätunnuksen perusteella.
10. Tarpeettomat käyttäjätilit ja käyttöoikeudet tulee poistaa, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta, vaihtaessa työtehtäviään tai, kun käyttäjätiliä ei ole käytetty ennalta määritellyn ajanjakson aikana).
11. Organisaatiolla on oltava selkeät ja toimivat menettelyt käyttäjien tehtävien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä niistä aiheutuvien toimenpiteiden tekemiseen.
12. Käyttöoikeudet tulee katselmoida säännöllisesti. Katselmointi tulee dokumentoida.
13. Vaaralliset käyttöoikeusyhdistelmät on tunnistettava, dokumentoitava ja eriytettävä mahdollisuuksien mukaan (Separation of Duties, SoD). Mikäli tehtäviä ei voida eriyttää, tulee niistä syntyviä riskejä hallita riskienhallinnan keinoin. Vaarallinen yhdistelmä on kyseessä, jos henkilö käsittelee yksin väärinkäytös- tai virhealttiissa prosessissa kaikkia tai useita tapahtumaketjun osia.
14. Käyttöoikeuksien hallinnassa tulee kiinnittää huomiota etenkin korkeamman riskiprofiilin rooleihin (kuten pääkäyttäjät, ylläpitäjät ja muut erityistä luotettavuutta edellyttävät työtehtävät) ja niihin liitettyihin käyttöoikeuksiin. Erityisrooleilla tulee olla erillinen haku- ja päätösprosessi.

On suositeltavaa dokumentoida ja ottaa käyttöön riskienarviointiin perustuva käyttövaltuuksien hallintapolitiikka. Politiikka sisältää käyttöoikeuksien ja -valtuuksien määrittelemisen, myöntämisen ja hallinnoinnin periaatteet ja toimintatavat. Tiedonhallintalain ja käyttövaltuuksien hallintapolitiikan lisäksi voimassa oleva tietosuojalainsäädäntö on otettava huomioon käyttöoikeuksien hallinnassa, koska käyttövaltuuksien hallinta on henkilötietojen käsittelyä ja toisaalta käyttöoikeuksien hallinta on myös keino turvata henkilötietojen lainmukainen käsittely.

13.2 Muutosten hallinta

Käyttöoikeuksien muuttamiseen ja poistamiseen on oltava selkeä ja toimiva menettelytapa työtehtävien muuttuessa ja erityisesti työsuhteen päättyessä. Esimerkiksi esimies voi ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan

muutettua tarvittavana ajankohtana. Käyttöoikeuksia voidaan poistaa tai muuttaa joko keskitetystä hallintajärjestelmästä tai erikseen yksittäisistä järjestelmistä.

13.3 Seuranta ja valvonta

Käyttäjätilejä, käyttöoikeuksia ja niihin liittyviä käyttövaltuuksia seurataan ja niiden käyttöä valvotaan dokumentoidusti asianmukaisuuden varmistamiseksi sekä poikkeamien havaitsemiseksi ja niihin reagoimiseksi ennalta määriteltyjen periaatteiden mukaisesti. Valvonnan avulla seurataan, että käyttäjätilit, käyttöoikeudet ja käyttövaltuudet ovat ajan tasalla ja niiden käyttö on asianmukaista ja noudattaa sovittuja käytäntöjä.

Valvonnassa kiinnitetään huomiota etenkin erityistä luotettavuutta edellyttävissä työtehtävissä toimivien käyttäjien oikeuksien asianmukaisuuteen, ajantasaisuuteen ja käyttöön.

Kaikista käyttöoikeuksiin tehtävistä muutoksista on jäätävä lokimerkintä. Myös monista käyttäjän toimista tulee jäädä lokimerkintä. Niistä kerrotaan tarkemmin lokienhallintaa koskevassa osiossa Lokitietojen kerääminen (TiHL 17 §).

13.4 Tunnistaminen ja todentaminen

Luotaessa uutta käyttäjätunnusta järjestelmään, joka sisältää salassa pidettävää tietoa, tulee käyttäjä ensimmäinen kerran tunnistaa virallisen henkilöllisyystodistuksen avulla. Rekisteröidyttäessä sähköiseen palveluun tulee käyttäjä tunnistaa vahvaa tunnistusmenetelmää hyödyntämällä. Lisäksi käyttäjätunnusta luovutettaessa tulee varmistua siitä, että oikea henkilö saa käyttäjätunnuksen.

Kertakirjautumista (Single Sing-On, SSO) suositellaan käytettäväksi mahdollisimman laajasti. Kertakirjautumisella tarkoitetaan sellaista pääsynhallinnan toteutustapaa, jossa käyttäjä pääsee yhdellä riittävän vahvalla tunnistautumisella omien käyttöoikeuksiensa rajoissa kaikkiin saman pääsynhallinnan piirissä oleviin palveluihin ja järjestelmiin. Kertakirjautuminen vähentää riskiä saman salasanan käytöstä useassa eri palvelussa.

Lisäksi suositellaan monivaiheisen tunnistautumisen (Multifactor Authentication, MFA) hyödyntämistä. Siinä käytetään kahta tai useampaa todentamismenetelmää, minkä ansiosta tietomurtoja voidaan ehkäistä tehokkaasti.

Salasanoille on määritettävä riittävät laatuvaatimukset, esimerkiksi salasanan vähimmäispituus ja kompleksisuus. Laatuvaatimusten tulisi olla teknisesti pakotettuja.

13.5 Säädökset ja lisätiedot

Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaiselle (osio I-06)

Kuntasektorin käyttövaltuushallinnan viitearkkitehtuuri

14 Lokitietojen kerääminen (TiHL 17 §)

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

14.1 Lähtökohdat

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

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

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

14.2 Lokitiedot

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

Lokitietojen kerääminen on sidottu tietojen tarpeellisuuteen, jota arvioidaan riskiperusteisesti. Lokitietojen kerääminen tietojärjestelmän käytöstä ja tietojen luovutuksista on tarpeellista erityisesti silloin kun tietojärjestelmässä käsitellään salassa pidettäviä tietoja. Jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja, luovuttavassa järjestelmässä kerätään luovutuslokitiedot sen varmistamiseksi, että tietojen luovuttamiselle on ollut laillinen peruste. Käyttölokitietojen keräämisen tarvetta arvioidaan erityisesti sillä perusteella, tarvitaanko niitä virheselvittelyjä varten tai yksilön etujen, oikeuksien ja velvollisuuksien sekä oikeusturvan toteuttamiseksi tai virkavastuun todentamiseksi. Tietojärjestelmien ylläpitotoimista kerättävät lokitiedot kuvaavat tietojärjestelmän toimintaan ja käyttöoikeuksiin tehtyjä muutoksia ja tekniset järjestelmä- ja virhelokit kuvaavat muun muassa teknisiä virheitä ja toimintahäiriöitä.

14.3 Lokienhallinnan suunnittelu ja ohjaus

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

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

Osana lokienhallinnan suunnittelua ja sitä ohjaavan dokumentaation laatimista:

- Tunnistetaan lokitietoihin ja lokien käsittelyyn liittyvät ulkoiset vaatimukset lainsäädännöstä, määräyksistä ja mahdollisista sopimuksista.

- Määritellään toimintatavat lokienhallinnalle ja käsittelylle.
- Määritellään lokien käsittelyprosessi ja -tavat sekä käsittelyyn liittyvät roolit ja vastuut.
- Määritellään prosessi lokienhallinnan ja käsittelyn asianmukaisuuden ja lainmukaisuuden säännölliseksi arvioimiseksi.
- Tunnistetaan miksi ja mihin tarkoitukseen kutakin lokia käsitellään.
- Tunnistetaan tietojärjestelmät ja laitteet, joiden tulisi tuottaa lokitietoja, kuten kriittiset tietojärjestelmät ja salassa pidettävän tiedon käsittelyyn tarkoitetut tietojärjestelmät.
- Arvioidaan tallennettavien tietojen tarpeellisuus.
- Tunnistetaan lokeihin tallentuvat tietotyypit, erityisesti henkilötiedot ja tunnistamistiedot.
- Tunnistetaan tallentuvien tietotyyppien suojaustarpeet.
- Määritetään suojaustarpeet ja tavat (kuten salaus, varmuuskopiointi, pääsynhallinta) lokien suojaamiseksi.
- Varmistetaan, että tietojen suojaustarve toteutuu järjestelmän toteutuksessa ja tietojen käsittelyssä.
- Huomioidaan tarve lain yksityisyyden suojasta työelämässä mukaiselle yhteistoimintamenettelylle, mikäli kyseessä on tekninen valvonta.
- Huomioidaan yhteistoimintamenettelyn lisäksi muu käyttäjien, rekisteröityjen tai muiden tahojen informointi.
- Huomioidaan henkilötietojen käsittelyä koskevat lainsäädännön (kuten tietosuoja-asetus ja tietosuojalaki) asettamat vaatimukset, jos lokit sisältävät henkilötietoja.
- Suunnitellaan ja dokumentoida säilytystarve ja varmistaa sen toteutuminen käytännössä.
- Määritellään lokien keräämiseen liittyvät konfiguraatiot tietojärjestelmille ja laitteille.

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

Lokitietojen käsittelyyn sekä etenkin keräämiseen, säilyttämiseen ja säilytysaikoihin voi kohdistua vaatimuksia erityislainsäädännöstä sekä määräyksistä ja standardeista. Nämä on tunnistettava ja huomioitava osana lokienhallintaa.

14.4 Lokitietojen kerääminen

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

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

- Milloin (milloin tapahtuma oli?)
  - Lokitiedon aikaleima eli päivämäärä ja kellonaika
  - Tapahtuman aikaleima päivämäärä ja kellonaika (lokitiedon ja tapahtuman aikaleima voivat joskus myös erota toisistaan)
  - Tapahtuman tunniste

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

- Kuka (toimija eli kuka tai mikä teki ja mikä oli tapahtuman lähde?)
  - Tapahtuman lähteen (ihmis- tai laitekäyttäjän) tunnistetiedot, kuten nimi, lähdeosoite, henkilön tai laitteen identiteetti ja tunnistetiedot, sijainti
  - Millä oikeuksilla ja valtuuksilla tapahtuma tehtiin

- Mitä (mitä tapahtui ja onnistuiko tapahtuma?)
  - Tapahtuman tyyppi, kuten objektin luominen, objektin muuttaminen, kirjautuminen tai järjestelmän kaatuminen
  - Tapahtuman tila (onnistuiko vai epäonnistuiko tapahtuma ja miksi se mahdollisesti epäonnistui)
  - Tapahtuman merkitys tai prioriteetti
  - Tapahtuman kuvaus

Lokiin ei lähtökohtaisesti tule kerätä seuraavan kaltaisia tietoja:

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

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

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

Mikäli käytössä on useita lokeja, niin niiden helposti tapahtuva yhdistely analysointitarpeita varten on hyvä mahdollistaa. Lokia tuottavien lokilähteiden kellojen synkronoinnilla varmistetaan, että eri järjestelmien tuottamat lokitiedot ovat keskenään yhtenäisiä ja jotta niistä voidaan muodostaa yhtenäinen tapahtumaketju. Erityisesti lokilähteiden aikaleimojen on tarve olla samassa ajassa. Eri lokeja tuottavien järjestelmien aika on mahdollista

synkronoida NTP:n (Network Time Protocol) avulla. Myös lokien aikavyöhyketiedot on hyvä tallentaa. Suositeltavaa on käyttää UTC-aikaa kaikissa lähteissä.

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

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

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

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

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

Tietojärjestelmän käyttöä koskevien lokitietojen ja keräämisen ja seurannan merkitys korostuu erityisesti, kun tietojärjestelmässä käsitellään salassa pidettäviä tietoja. Lokitietojen tarkoituksena on myös dokumentoida tietojärjestelmistä tehtävät luovutukset ja samalla osaltaan varmistaa, että luovutuksille on ollut olemassa lainmukainen peruste. Tämä korostuu erityisesti silloin, jos tietojärjestelmästä luovutetaan rajapintojen tai katseluyhteyden avulla salassa pidettäviä tietoja tai henkilötietoja.

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

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

14.5 Lokitietojen säilyttäminen

Lokitietojen säilyttämisen suunnittelussa määritellään lokien säilytysaika ja -paikka. Säilytysaika johdetaan aina niiden käyttötarkoituksesta. Viranomaisen on hyvä tunnistaa ne lokitiedot, joiden säilytysaika on tyypillisesti vähintään viisi vuotta rikosoikeudellisten vanhentumisaikojen vuoksi. Erityislainsäädännössä voi olla säädetty erikseen lokitietojen säilytysajoista etenkin, jos lokitietoja säilytetään pitempiä aikoja kuin on tarpeen viranomaisella olevien velvollisuuksien toteuttamiseksi. On tärkeää varmistaa, että lokitiedot säilyvät ja ovat käytettävissä koko määritellyn säilytysajan, jonka jälkeen ne on poistettava.

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

Edellä mainittujen tarpeiden täyttämiseksi keskeisille teknisille lokeille suositellaan yleisesti vähintään 5 vuoden säilytysaikaa.

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

Lokien keräämistä varten on suunniteltu tarvittavat toimintamallit ja infrastruktuuri, jotta lokeille on varattu riittävästi säilytystilaa suhteessa kerättävien lokien määrän ja niiden säilytysaikaan. Säilytystilan suunnittelussa ja toteutuksessa on huomioitu myös se, ettei lokien kerääminen pysähdy lokin tai lokitilan täyttyessä. Lokien säilytyskapasiteettia seurataan ja siihen liittyvistä ongelmista on tärkeä luoda hälytyksiä.

Kun lokitietojen käsittelylle ei ole enää tarvetta ja niiden säilytysaika on umpeutunut, ne joko poistetaan tai anonymisoidaan. Lokitietojen tyhjentäminen on automatisoitu poistamaan alkuperäisestä lokista kaikki lokitiedot, jotka ylittävät määritetyn säilytysajan. Tässä yhteydessä tulee huomata, että lokeja on tyypillisesti myös tallennettu varmistusnauhoille tai muille vastaaville tallennus- ja arkistointivälineille, joista tiedot tulee tarvittaessa myös poistaa. Tietojen poistamisessa tulee huomioida, onko tietojen poistaminen mahdollista vaarantamatta tiedon eheyden säilymistä. Varmistusnauhoille tai muille vastaaville tallennus- tai arkistointivälineille tallennettujen tietojen poistamisessa tulee huomioida varmistusten eheyden säilyminen.

14.6 Lokitietojen seuranta ja analysointi

Tarvittavan havainnointikyvykkyyden luomiseksi ja ylläpitämiseksi lokitietoja on seurattava ja analysoitava säännöllisesti. Lokeja koskevan seurannan, analysoinnin ja hälytysten tuottamisen tarkoituksena on luoda etenkin kriittisten kohteiden ja tietojen kohdalla mahdollisimman reaaliaikainen havainnointikyvykkyys, jotta tarvittaviin toimenpiteisiin on mahdollista ryhtyä nopeasti.

Lokitietojen seuranta ja valvonta palvelevat myös tiedonhallintalain 13.1§ edellytettyä tietoturvallisuuden tilan seurantaa.

Lokien analysoinnissa ja ymmärtämisessä on tärkeää ymmärtää jokaisen lokia tuottavan järjestelmän ja sitä käyttävän käyttäjän normaali, tyypillinen toiminta. Tavoitteena on saada käsitys normaaleista lokitietoja muodostavista tapahtumista, jotta saadaan

vertailukohta epätavallisille lokitapahtumille. Ajan kuluessa opitaan tunnistamaan järjestelmän normaalitoiminta ja kyetään erottamaan siitä eroavat epätavalliset lokitapahtumat.

Lokitietojen seurannan ja analysoinnin osalta on määritetty:

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

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

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

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

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

- tapahtuman poikkeuksellisuuden (esim. tapahtuman normaalista poikkeava ajankohta tai ilmaantumistiheys)

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

14.7 Lokitietojen luovuttaminen

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

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

14.8 Lokitietojen suojaaminen

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

Lokit muodostavat yhden tietojärjestelmään kuuluvan tietoaineiston ja niiden turvallisuus on suositeltavaa varmistaa vähintään samalla tavoin kuin järjestelmän muiden tietoaineistojen turvallisuus. Tämä voidaan toteuttaa esimerkiksi siirtämällä lokitiedot toiseen,

suojattuun järjestelmään, joka on eriytetty lokitiedot luoneesta tietojärjestelmästä. Hyvin toteutettu lokiympäristö onkin muista tietojärjestelmistä erillään oleva tietokanta, jonka eheys on varmistettu estäen lokien muokkauksen.

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

14.9 Säädökset ja lisätiedot

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) 14 §

EU yleinen tietosuoja-asetus

Tietosuojalaki (1050/2018)

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018

VAHTI 3/2009 Lokiohje

Kyberturvallisuuskeskus, Näin keräät ja käytät lokitietoja

Viestintäviraston ohje 04/2016, Lokien keräys ja käyttö

Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaiselle (osio I-10)

15 Sanasto

Kyberturvallisuuden sanasto (Turvallisuuskomitea)

Kokonaisturvallisuuden sanasto (Sanastokeskus TSK ry)

VAHTI 8/2008 Valtionhallinnon tietoturvasanasto

Aikaleima on tapahtumatietoon tai viestiin liitetty tieto lähetys-, saapumis- tai käsittely-ajankohdasta ja mahdollisesti tapahtuman osapuolista. Aikaleimalla saadaan aikaan viestin lähettämisen tai vas-taanottamisen kiistämättömyys.

Alusta on ohjelmiston tai tietojärjestelmän tekninen toimintaympäristö. Alustalla tarkoitetaan yksinkertaisimmillaan laitteistoa ja sen varusohjelmistoa. Yleisemmässä tapauksessa alustalla saatetaan tarkoittaa tiettyä laajempaa sovellusten ajoympäristöä erilaisine tukiohjelmistoineen, tietokantoineen, tietoliikennevalmiuksineen.

Anonymisointi tarkoittaa henkilötietojen käsittelyä niin, että henkilöä ei enää voida tunnistaa niistä. Tiedot voidaan esimerkiksi karkeistaa yleiselle tasolle (aggregoida) tai muuttaa tilastolliseen muotoon siten, etteivät yksittäistä henkilöä koskevat tiedot ole enää tunnistettavassa muodossa. Tunnistamisen täytyy estyä peruuttamattomasti ja siten, että rekisterinpitäjä tai muu ulkopuolinen taho ei voi enää hallussaan olevilla tiedoilla muuttaa tietoja takaisin tunnistettaviksi.

Arviointi on sen selvittäminen, täyttääkö tietty kohde eri osiltaan sille asetetun tavoitetilan (vaatimukset, suositukset ja parhaat käytännöt). Arviointiprosessi on usein hyväksyntäprosessin osaprosessi.

Auditointi on riippumattoman tahon suorittama kohteen, sen toiminnan ja toiminnan tulosten yleensä määräajoin tapahtuva tutkiminen sen selvittämiseksi, vastaako kohde siihen kohdistuvia vaatimuksia.

Haavoittuvuudet ovat alttiuksia turvallisuutta uhkaaville tekijöille, puutteita ja heikkouksia turvatoimissa sekä suojauksissa. Tietoturvahaavoittuvuudet ovat tietojärjestelmän tai sen osan heikkous, joka vaarantaa tietoturvan Haavoittuvuus voi olla seurausta

ohjelmavirheestä tai siitä, että jotakin erityistapausta ei ole otettu huomioon. Haittaohjelmat hyödyntävät levitessään tietoturva-haavoittuvuuksia.

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

Haavoittuvuusskannaus on tietoverkossa kohdejärjestelmän palveluissa olevien tunnettujen haavoittuvuuksien automaattinen haku, esimerkiksi murtokokeilla tai tutkimalla palvelimen ohjelmistoversiota.

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

Hyväksymistarkastus kattaa toimet, joilla todetaan, täyttääkö tuote tai työn tulos asetetut vaatimukset.

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

Immateriaalioikeudet ovat aineettomia oikeuksia, mm. tekijänoikeus, patentti-, malli-, tavaramerkki ja toiminimioikeus.

IPR-kysymykset (Intellectual Property Rights) eli immateriaalioikeuksiin liittyvät kysymykset koskevat tekijänoikeuksia, tavaramerkkejä, patentteja, toiminimiä ja liikesalaisuuksia.

Katselmointi on kohteen tilan arviointi, jonka tarkoituksena on tunnistaa eroavuudet tavoitetilaan ja tuottaa kehitysehdotuksia.

Komponentti on itsenäinen ohjelmistoyksikkö, joka tarjoaa palveluja hyvin määritellyn rajapinnan kautta.

Kontrolli on riskien hallinnan tavoite, keino tai menetelmä, suunnitelmallinen jatkuva toiminta, kertaluonteinen tai toistuva toimenpide, jolla varaudutaan tai suojaudutaan (tieto) turvaloukkauksia tai haitallisia tapahtumia vastaan. Kontrollit ovat ehkäiseviä, havaitsevia (ilmaisevia) tai korjaavia.

Kriteeri on arviointiperuste, jolla todetaan tavoitteen täyttyminen.

Käyttäjä on organisaation työntekijä (sisäinen/ulkoinen), harjoittelija, opiskelija, asiakas tai organisaation toimintaan muulla tavoin liittyvä henkilö (esim. luottamushenkilö), joka käyttää organisaation tarjoamia palveluja.

Käyttäjärooli on joukko käyttäjän ominaisuuksia, jotka liittyvät hänen tietotarpeittensa ja/tai toimintavaltuuksiensa määrittelyyn. Käyttäjäroolia voidaan tarkastella joko käyttäjän toimenkuvan näkökulmasta (työrooli) tai hänellä järjestelmässä olevien valtuuksien näkökulmasta (IT-rooli).

Käyttöoikeus on tietojärjestelmän käyttäjälle tai esimerkiksi tietyn käyttäjäroolin omaavalle käyttäjäryhmälle myönnetyt yksilöidyt oikeudet nimettyjen palveluelementtien tai muiden resurssien käyttöön. Käyttöoikeudet määrittelevät, miten ja millaisilla edellytyksillä käyttäjällä on oikeus käyttää ko. palveluelementtejä.

Käyttövaltuushallintajärjestelmä (Identity Access Management system, IAM) on keskitetty tietojärjestelmä, jolla voidaan toteuttaa ja automatisoida identiteetin ja käyttövaltuuksien hallintaa sekä niiden valvontaa.

Levykuva eli image on massamuistilaitteen koko sisällöstä ja rakenteesta tehty tiedosto.

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

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

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

Lähdekoodi on tietokoneohjelma ohjelmoijien kirjoittamassa ja ylläpitokelpoisessa muodossa.

Muistivälineiden sanitointi tarkoittaa muistivälineiden tyhjentämistä tai puhdistamista halutusta tiedosta tai materiaalista.

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

Palveluelementti on palvelujärjestelmän toiminto tai tieto, jonka käyttöä halutaan erikseen valvoa.

Palvelujärjestelmä on tietojärjestelmä, joka tarjoaa käyttäjille sovelluspalveluja.

Penetraatiotestaus tarkoittaa tietojärjestelmien testaamista tietoturvariskien varalta. Penetraatiotestausta käytetään tietojärjestelmien suojausmekanismien heikkouksien ja haavoittuvuuksien havaitsemiseen.

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

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

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

Rajapinta on yhtymäkohta, joka mahdollistaa tiedon siirron laitteiden, ohjelmien tai käyttäjien välillä.

Riskirekisteriin tallennetaan tunnistetut riskit ja niiden arvioinnit sekä suunnitellut hallintatoimenpiteet.

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

Salattu yhteys on salausmenetelmällä ulkopuolisilta suojattu tietojärjestelmien välinen yhteys.

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

Salausmenetelmä on salaukseen ja salauksen purkamiseen käytettävä menetelmä.

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

Suojattavien kohteiden tunnistamisella ja dokumentoinnilla tarkoitetaan kaiken tiedonhallintayksikön hallinnassa olevan tiedon ja järjestelmien sekä muiden suojattavien kohteiden, kuten avainhenkilöiden tunnistamista.

Suojauksella tarkoitetaan haitallisen ulkopuolisen vaikutuksen torjumista tai ennalta ehkäisyä.

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

Taustajärjestelmä käsittää ne järjestelmät, jotka tukevat varsinaisen järjestelmän toimintaa.

Testaus on järjestelmän toimivuuden, käytettävyyden, suorituskyvyn, määritysten mukaisuuden tai muun ominaisuuden selvittämiseksi tehtävä toimenpidesarja.

Tiedonhallintayksiköitä ovat esimerkiksi valtion ja kuntien organisaatiot, kuten valtiovarainministeriö, Valtion tieto- ja viestintätekniikkakeskus Valtori, Maanmittauslaitos ja Helsingin kaupunki.

Tiedon migraatio on tiedon siirtämistä toiseen järjestelmään aitouden, eheyden, luotettavuuden ja käytettävyyden varmistamiseksi.

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

Tietoriskillä tarkoitetaan tietoon kohdistuvaa tai tiedosta aiheutuvaa, jonkinlaisen haitan tai vaurion todennäköisyyttä ja sen seurauksia. Tietoriski ilmaistaan tavallisesti riskin lähteiden ja mahdollisten tapahtumien sekä niiden seurausten ja todennäköisyyden yhdistelmänä. Tietoriskit voivat aiheutua esimerkiksi inhimillisistä virheistä, annettujen ohjeiden puutteista tai noudattamatta jättämisestä, varkauksista tai ilkivallasta, laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä, haittaohjelmien leviämisestä, tietoaineistojen tuhoutumisesta tai alihankkijan tai kumppanuusverkostoon kuuluvan toimijan virheistä tai laiminlyönneistä.

Tietoturvahaavoittuvuudet ovat tietojärjestelmän tai sen osan heikkous, joka vaarantaa tietoturvan. Haavoittuvuus voi olla seurausta ohjelmavirheestä tai siitä, että jotakin erityistapausta ei ole otettu huomioon. Haittaohjelmat hyödyntävät levitessään tietoturvahaavoittuvuuksia.

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

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

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

Tietoturvapoikkeaman hallinta sisältää toimenpiteet, joilla varaudutaan ja reagoidaan tietoturvahäiriöihin vahinkojen rajoittamiseksi ja niistä toipumiseksi.

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

Tietoturvauhalla tarkoitetaan tietoaineistoihin ja tietojärjestelmiin liittyvää sellaista tahatonta tai tahallista tekijää, joka vaarantaa tietoaineistojen luottamuksellisuutta, eheyttä tai käytettävyyttä tai tietojärjestelmien käyttöä tai vikasietoisuutta. Tietoturvauhat voivat aiheutua esimerkiksi inhimillisistä virheistä, annettujen ohjeiden puutteista tai noudattamatta jättämisestä, varkauksista tai ilkivallasta, laitteiden, järjestelmien tai ohjelmistojen virheistä ja toimintahäiriöistä, haittaohjelmien leviämisestä, tietoaineistojen tuhoutumisesta tai organisaation oman työntekijän, alihankkijan, palveluntoimittajan tai kumppanuusverkostoon kuuluvan toimijan virheistä tai laiminlyönneistä.

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

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

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

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

Turvallisuuskuvaus on kuvaus esimerkiksi järjestelmän turvallisuudesta ja sen toteuttamisesta.

Vaatimus on kohteelle asetettu yksittäinen tavoite, joka kohteen tulee pystyä toteuttamaan.

Vaikutusanalyysillä tarkoitetaan toiminnan keskeyttävien tai jatkuvuutta häiritsevien uhkien sekä toimintaan liittyvien riippuvuuksien tunnistamista. Tieto- ja kyberturvallisuuden näkökulmasta tulee vaikutusanalyysissä, erityisesti valtionhallinnon tai muun julkisen hallinnon organisaation toiminnan kannalta, tarkastella muun muassa:

- vaikutuksia omaan operatiiviseen toimintakykyyn
- vaikutuksia säädösperusteisten tehtävien hoitamiseen (vrt. myös yhteiskunnan elintärkeät tehtävät)
- vaikutuksia yhteiskunnalle
- riippuvuussuhteita ja niiden vaikutuksia:
    - oman organisaation riippuvuutta toisesta osapuolesta tai palvelusta tai toisista organisaatioista tai palveluista
    - toisen organisaation tai palvelun riippuvuutta oman organisaation tuottamasta palvelusta tai toiminnasta.

Viranomaisen tulee kyetä tunnistamaan kaikki tiedot ja tietojärjestelmät, jotka ovat sen vastuulla sekä ottamaan huomioon niitä ylläpitävät ja käyttävät avainhenkilöt. Jokaiseen tunnistettuun kohteeseen liittyvät riskit ja niiden mahdolliset vaikutukset tulee arvioida ja kirjata organisaation itsensä ylläpitämään riskirekisteriin.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-897-2 (pdf)

Marraskuu 2021