M72 valmistelumuistio 2021: Tunnistusjärjestelmän tekniset tietoturvavaatimukset, häiriötilanteiden ja tietoturvallisuuden hallinta

Sisällys

1 Kuva

Kuva: tunnistusjärjestelmän tietoturvallisuus koostuu monesta osatekijästä

2 Säännös ja perustelut (voimassa olevat)

Tähän on koottu voimassa olevasta määräyksestä **Viestintävirasto 72/2018 M sähköisistä tunnistus- ja luottamuspalveluista** säännökset, joiden muutostarvetta muistiossa arvioidaan.

Tähän on koottu myös säännösten perustelut ja soveltamisohjeet **perustelumuistiosta MPS72.** Perustelumuistion 14.5.2018 päivätyssä versiossa ovat mukana vuoden 2016 perustelut ja 2018 osittaismuutoksen perustelut. Perustelut päivitetään muutoksen yhteydessä.

Koko määräys ja perustelumuistio Finlexissä https://www.finlex.fi/fi/viranomaiset/normi/480001/42947

2.1 Säännös 4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset

4 § Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset

Tunnistuspalveluntarjoajan on käytettävä tunnistusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään.

Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet

1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;

2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;

3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;

4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;

5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja

6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.

2.1.1 Perustelumuistio

Pykälässä määrätään yleisellä tasolla siitä, mitä tunnistusjärjestelmän tietoturvallisuuden hallinnassa täytyy ottaa huomioon. Tunnistuspalvelun tarjonnalla tarkoitetaan koko tunnistusjärjestelmää, joka kattaa koko tunnistuspalvelun kokonaisuuden.

EU:n varmuustasoasetuksen [2] liitteen 1 kohdassa 2.4.3 edellytetään, että tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten. Tunnistuslain 8.1 §:n 5 alakohdassa säädetään tietoturvallisuuden hallinnasta ja viitataan mm. varmuustasoasetuksen kohtaan 2.4.3.

Pykälän 1 momentissa tarkennetaan tunnistus- ja luottamuspalvelulain ja EU:n varmuustasoasetuksen vaatimusta. Ainakin ISO/IEC 27001 -standardi [8] on yleisesti tunnettu ja pätevä tietoturvallisuuden hallinnan standardi. Myös muuta standardia tai standardien yhdistelmää voi käyttää, edellyttäen, että standardi todella kohdistuu tietoturvallisuuden hallintaan. Standardi voi olla kansainvälinen, kuten ISO, mutta myös kansallinen kuten KATAKRI [15].

Pykälän 2 momentissa luetellaan toiminnan osa-alueet, jotka tietoturvallisuuden hallinnan täytyy kattaa. Vaatimukset vastaavat pitkälti aikaisemman määräyksen 8 2 §:ää tietoturvallisuuden hallinnasta. Vaatimuksia on nyt tiivistetty käyttäen apuna ISO/IEC 27001 vaatimusten ylätason ryhmittelyä.

Pykälän vaatimukset liittyvät ISO/IEC 27001 -standardiin seuraavasti

Määräys 4 § ja soveltaminen	***ISO/IEC 27001***

1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena *- olennaisten sisäisten ja ulkoisten teknisten, oikeudellisten ja yhteisön hallinnollisten vaatimusten, tarpeiden ja asioiden tunteminen ja huomioiminen*	*4 organisaation toimintaympäristö*
2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito *- dokumentoidaan tietoturvapolitiikassa tai vastaavissa ohjausasiakirjoissa*	*5 johtajuus* *9.2 sisäinen auditointi* *9.3 johdon katselmus* *10 hallintajärjestelmän parantaminen*
3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta	*6 suunnittelu*
4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta	*7 tukitoiminnot*
5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi	*8 toiminta*
6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi *- eli miten hyvin tietoturvallisuuden hallinta tehoaa/vaikuttaa niihin tekijöihin, prosesseihin ja ongelmiin, jotka vaikuttavat tunnistusjärjestelmän tietoturvallisuuteen*	*9.1 seuranta, mittaus, analysointi, arviointi*

2.2 Säännös 5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

5 § Tunnistusjärjestelmän tekniset tietoturvatoimenpiteet

Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän

1) tietoliikenneturvallisuus
- *a) verkon rakenteellinen turvallisuus*
- *b) tietoliikenneverkon vyöhykkeistäminen*
- *c) suodatussäännöt vähimpien oikeuksien periaatteilla*
- *d) suodatuksen ja valvontajärjestelmien hallinnointi koko elinkaaren ajan*
- *e) hallintayhteydet*

2) tietojärjestelmäturvallisuus
- *a) pääsyoikeuksien hallinta*
- *b) järjestelmien käyttäjien tunnistaminen*
- *c) järjestelmien koventaminen*

d) haittaohjelmasuojaus
e) turvallisuuteen liittyvien tapahtumien jäljitys
f) poikkeamien havainnointikyky ja toipuminen
g) kansainvälisesti tai kansallisesti suositellut salausratkaisut muutoin kuin 7 §:ssä säädetyltä osin

3) käyttöturvallisuus
a) muutosten hallinta
b) salassa pidettävän aineiston käsittely-ympäristö
c) etäkäyttö ja -hallinta
d) ohjelmistohaavoittuvuuksien hallinta
e) varmuuskopiointi

Tuotantoverkko ja sen edellä 1 momentin 1) e) ja 3) c) alakohdissa tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on
a) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja
b) korkealla varmuustasolla kokonaisuutena arvioiden estetty.

2.2.1 Perustelumuistio

1 momentin 1 e alakohdan hallintayhteydet voivat olla sekä organisaation sisäisiä että ulkoisia tietoliikenneyhteyksiä.

1 momentin 2 b alakohdan käyttäjien tunnistaminen tarkoittaa käytännössä sitä, että käyttäjätunnusten täytyy olla henkilökohtaisia, eivätkä ne voi olla yhteiskäyttöisiä.

1 momentin 2 g alakohdassa tarkoitettuja salausratkaisuja löytyy esimerkiksi seuraavista lähteistä:

a) ENISA [16],

b) Viestintäviraston kyberturvallisuuskeskuksen NCSA:n (National Communications Security Authority, NCSA-FI) tuottama aineisto [17],

c) NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) [18] tai

d) SANS (The SANS Institute) [19].

2 momentin kannalta internetiä ja toimistoverkkoa pidetään ei-luotettuna verkkona, ellei toimistoverkko kuulu vaatimustenmukaisuuden arvioinnin piiriin. Tiedonsiirtokanavan täytyy siis olla etäkäytössä suojattu ja toimistoverkon aiheuttamat riskit täytyy huomioida. Korotetun varmuustason vaatimukset ovat tavanomaisia ja ne katetaan jo esimerkiksi ISO 27001 -vaatimusten kautta, jos sovelletaan sitä.

Korkealla varmuustasolla 2 momentin vaatimukset voi toteuttaa ainakin siten, että etäkäytössä olevasta työasemasta estetään pääsy muihin organisaation palveluihin kuten sähköpostiin ja poistetaan työasemasta mahdollisuus käyttää muita kuin hallintaverkon käytön kannalta välttämättömiä toimintoja. Käytännössä tämä tarkoittaa siis erillistä työasemaa hallintakäyttöä varten.

Korkealla varmuustasolla edellytetty kokonaisarvio tarkoittaa sitä, että jos käytettään muuta kuin edellä kuvattua kovennettua työasemaa, otetaan toteutuksessa huomioon tuotantojärjestelmän eriyttäminen ja muut järjestelyt, joilla tietoturvauhkat voidaan hallita. Lähtökohtaisesti tällöin edellytetään virtualisoitua terminointia tai kvm-periaatteeseen (etätyöpöytä) perustuvaa ratkaisua.

Olennaista on, mitä tehdään sillä päätelaitteella, josta virtualisoitua yhteyttä otetaan ja siten esimerkiksi two-factor VPN-yhteys virtualisoituun työasemaan ei yksin riitä ratkaisuksi. Riittävää ei ole myöskään, että käytetään virustorjuntaa ja web-proxya.

Välttämättömien tiedostojen siirrossa koneelta toiselle on myös huomioitava haittaohjelmien riski mm. pitämällä huolta siitä, että käytetään vain luotettavia lähteitä ja varmistetaan tietoturvallisuus (eheys) kaikilla tarpeellisilla menetelmillä.

2.3 Määräyksen perustelumuistio 2016 C-osa kohta 1: Suositus tunnistusjärjestelmän kellonajan luotettavuudesta

Suositellaan, että tunnistuspalveluntarjoaja hankkii luotettavan aikalähteen, jonka kanssa ne synkronoivat tunnistusjärjestelmässään käytetyn kellonajan. Kellonaikaa tarvitaan tapahtuma-aikojen luotettavaa osoittamista varten. Suositeltava virhetoleranssi on 0,5 sekuntia. Synkronointia toimijoiden välillä ei tarvittane.

Aiheeseen liittyy suositus ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority [51].

Mahdollisia aikalähteitä ovat esimerkiksi VTT:n/MIKESin NTP tai PTP, joista jälkimmäiseen liittyy myös saatavuustakuu. Muitakin on tarjolla.

2.4 Säännös 11 § Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle

11 § Tunnistuspalveluntarjoajan häiriöilmoitukset Viestintävirastolle

Viestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot:

1) *tunnistusväline tai välityspalvelu, johon häiriö vaikuttaa;*
2) *kuvaus häiriöstä ja sen tiedossa olevista syistä;*
3) *kuvaus häiriön vaikutuksista, mukaan lukien vaikutus uusien tunnistusvälineiden myöntämiseen, käyttäjiin, luottaviin osapuoliin, muihin luottamusverkoston toimijoihin ja rajat ylittävään käyttöön;*
4) *kuvaus korjaustoimenpiteistä; sekä*
5) *kuvaus häiriöstä tiedottamisesta luottaville osapuolille, tunnistusvälineiden haltijoille, luottamusverkostolle ja tieto ilmoittamisesta muille viranomaisille.*

Häiriön merkittävyyden arvioinnissa merkittävyyttä lisää se, että häiriö liittyy sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittävyyttä lisää myös se, että häiriöllä on vaikutuksia luottamusverkostoon.

2.4.1 Perustelumuistio

Pykälän 1 momentissa säädetään niistä tiedoista, jotka tunnistusvälineen tai tunnistusvälityspalvelun tarjoajan on annettava Viestintävirastolle tehtävässä häiriöilmoituksessa. Ilmoituksessa edellytetään häiriökuvauksen lisäksi tietoa vaikutuksista eri tahoihin.

Ilmoituksen tarkoitus on tukea Viestintäviraston tilannekuvaa tunnistuspalveluiden luotettavuudesta, uhkista ja häiriötilanteista. Tiedon perusteella Viestintävirasto

arvioi, onko vaatimuksia noudatettu ja onko tilanteesta tarvetta tiedottaa laajemmin kuin palveluntarjoaja on tehnyt. Viestintävirasto voi myös tarjota tietoa tilanteesta toipumiseksi, jos sellaista on käytettävissä.

Ilmoitus täytyy lain 16 §:n mukaan tehdä ilman aiheetonta viivästystä. Koska täydellisiä tietoja häiriöstä ei aina ole käytettävissä siinä vaiheessa, kun häiriö havaitaan ja sitä ryhdytään korjaamaan, ensi vaiheessa voi ilmoittaa tiedossa olevat seikat ja ilmoitusta voi täydentää myöhemmin. Määräyksessä ei määritellä ilmoituksen toimitusajankohtaa, mutta mitä vakavampi häiriö on, sitä nopeammin Viestintävirastolle tulisi ilmoittaa.

Ilmoituksesta tulisi käydä ilmi häiriön tapahtumisen ja havaitsemisen ajankohta ja kesto, jos se on tiedossa.

Häiriön teknisestä tapahtumakuvauksesta tulisi käydä ilmi, mihin osaan tunnistusjärjestelmästä häiriö on vaikuttanut, havainnot tapahtumien etenemisestä, kuvaus mahdollisista toisten palveluntarjoajien osallisuudesta tapahtumiin ja tiedot tapahtuman aiheuttajasta. Ilmoituksesta tulisi käydä ilmi häiriön pohjasyy eli onko häiriö syy inhimillinen virhe, järjestelmä- tai ohjelmistovirhe, laiterikko, hyökkäys tai muu ulkoinen uhka tai luonnonilmiö.

Jos häiriö on johtunut tietoturvauhasta, ilmoituksesta tulisi käydä ilmi, onko kyseessä esimerkiksi palvelunestohyökkäys, haittaohjelma, tietomurto tai luvaton käyttö, liikenteen muuttaminen tai väärentäminen tai muu vastaava.

Häiriön ja sen vaikutusten kuvauksesta täytyy käydä ilmi mm., onko häiriö vaikuttanut tietojen luottamuksellisuuteen, eheyteen tai käytettävyyteen ja ovatko henkilötiedot vaarantuneet.

Ilmoituksessa tulisi myös kertoa, millaiseen määrään käyttäjiä ja asiointi-palveluita häiriö on vaikuttanut. Ilmoituksessa on hyvä kertoa, jos on tiedossa, että häiriö on vaikuttanut yhteiskunnan kannalta keskeiseen tai kriittiseen palveluun tai toimintoon.

Edelleen ilmoituksesta täytyy käydä ilmi lyhyen ja pitkän tähtäimen korjaustoimenpiteet, joihin on ryhdytty tai aiotaan ryhtyä häiriön vaikutusten poistamiseksi, lieventämiseksi ja vastaavien häiriöiden ennalta ehkäisemiseksi.

Ilmoituksesta täytyy käydä ilmi, miten asiointipalveluille, käyttäjille ja muille luottamusverkostoon kuuluville tunnistusvälineen ja tunnistusvälityspalvelun tarjoajille on tiedotettu häiriöstä. Tiedotuskynnys ja tiedottamisen sisältö ja ajankohta eri osapuolille voi luonnollisesti vaihdella. Tiedottamisessa täytyy tiedon saajan mahdollisuus ja tarve suojautua häiriön vaikutuksilta ja häiriön vaikutusten minimointi. Luottamusverkoston sisällä välitetyn häiriötiedon käytölle on säädetty lain 16.4 §:ssä erityisiä rajoituksia, joiden tarkoitus on madaltaa tiedottamisen kynnystä tunnistuspalveluntarjoajien välillä.

Pykälän 2 momentissa määritellään yleisellä tasolla niitä tekijöitä, jotka ovat olennaisia häiriön merkittävyyden eli ilmoituskynnyksen kannalta. Tällaisia merkittäviä häiriöitä ovat muun muassa:
- tunnistusvälineen myöntäminen väärälle henkilölle
- sellaiset sulkulistojen toimivuuteen liittyvät häiriöt, joissa ajantasaista sulkulistaa ei ole saatavilla
- tunkeutumiset palveluntarjoajan järjestelmiin
- tunnistusvälineen tarjoajan varmenteiden allekirjoitusavaimien paljastumiset

- tunnistusvälineiden vakavat väärinkäytökset kuten tapaukset, jotka liittyvät tunnusten ketjuttamiseen
- vakavat sisäiset väärinkäytökset.

Sähköisen henkilöllisyyden virheitä tai väärinkäytöksiä pidetään merkittävinä hyvin matalalla kynnyksellä, samoin esimerkiksi haavoittuvuuksia tai virheitä, jotka vaarantavat tunnistamistiedon oikeellisuuden. Sen sijaan käytettävyys- tai laatuongelmien ilmoituskynnys on lähtökohtaisesti korkeampi ja niiden merkittävyyttä lisää lähinnä se, että ongelma vaikuttaa muihin luottamusverkoston toimijoihin.

Viestintäviraston verkkosivuilla on lomake, jolla tiedot häiriötilanteesta voi ilmoittaa. Ilmoituksen toimittamisen käytännöistä ohjeistetaan sen yhteydessä.

Yleisesti Viestintävirasto arvioi, että häiriöilmoituksia tulisi tehdä viranomaiselle matalammalla kynnyksellä kuin tähän asti on tehty, sillä toimijoiden menettelyissä on tässä suhteessa paljon eroja.

Tunnistuspalveluiden häiriöilmoitusvaatimukset pyritään laatimaan mahdollisimman yhdenmukaisiksi niiden ohjeiden kanssa, joita ENISA laatii luottamuspalveluiden häiriöistä ilmoittamista varten [22].

Viestintävirastolle tehdyssä ilmoituksessa annettuja tietoja käsitellään viranomaisen toiminnan julkisuudesta annetun lain (621/1999) mukaisesti ja tietoa luovutetaan ulkopuolisille tai luottamusverkoston jäsenille vain lain sallimilla edellytyksillä.

Tunnistus- ja luottamuspalvelulaissa säädetään myös toimijoiden välisen ilmoittamisen velvollisuudesta sopimuspuolilleen eli mahdollisesti vain osalle luottamusverkoston jäsenistä. Laissa säädetään myös Viestintäviraston mahdollisuudesta teknisesti välittää toimijoiden välisiä ilmoituksia. Tällä hetkellä Viestintävirastolla ei kuitenkaan ole järjestelmää, jolla olisi mahdollista ilman erityistä teknistä kehitystyötä välittää tietoa automaattisesti toimijoiden välillä salattuna ja siten, että tieto välittyisi vain osalle luottamusverkostosta.

3 Lähteet vaikutusarviointiin

3.1 Yleiskuvaus lähtötilanteesta, viraston arvio kyselyssä 2020

Määräyksen 4 §:ssä määrätään yleisellä tasolla siitä, mitä tunnistusjärjestelmän tietoturvallisuuden hallinnassa täytyy ottaa huomioon. Tunnistuspalvelun tarjonnalla tarkoitetaan koko tunnistusjärjestelmää, joka kattaa koko tunnistuspalvelun kokonaisuuden.

EU:n varmuustasoasetuksen liitteen 1 kohdassa 2.4.3 edellytetään, että *tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.* Tunnistuslain 8.1 §:n 5 alakohdassa säädetään tietoturvallisuuden hallinnasta ja viitataan mm. varmuustasoasetuksen kohtaan 2.4.3.

Pykälän 1 momentissa tarkennetaan tunnistus- ja luottamuspalvelulain ja EU:n varmuustasoasetuksen vaatimusta. Ainakin ISO/IEC 27001 -standardi on yleisesti tunnettu ja pätevä tietoturvallisuuden hallinnan standardi. Myös muuta standardia tai standardien yhdistelmää voi käyttää, edellyttäen, että standardi todella kohdistuu tietoturvallisuuden hallintaan. Standardi voi olla kansainvälinen, kuten ISO, mutta myös kansallinen kuten KATAKRI.

Pykälän 2 momentissa luetellaan toiminnan osa-alueet, jotka tietoturvallisuuden hallinnan täytyy kattaa. Vaatimuksissa on hyödynnetty standardin ISO/IEC 27001 ylätason ryhmittelyä.

Virasto on havainnut käytännön valvontatyössä, että tietoturvallisuuden hallinnan arvioinnin on varsinkin määräyksen soveltamisen alkuaikoina virheellisesti luultu riittävän vaatimustenmukaisuuden arviointiin. Näin ei ole, sillä tietoturvallisuuden hallinta on yksi arvioitava asia ja säännöksissä määriteltyjen teknisten vaatimusten täyttyminen on myös arvioitava. Tätä on selvennetty arviointiohjeessa 211/2019.

Tunnistusjärjestelmän tekniset vaatimukset, varmuustasot ja häiriönhallinta

Tietojärjestelmä-, tietoliikenne- ja käyttöturvallisuus. Tunnistusjärjestelmän vaatimukset 5.1 §:ssä pohjautuvat tietojärjestelmien turvallisuuden yleisesti käytettyyn eri osa-alueiden jäsentelyyn tietojärjestelmä- tietoliikenne- ja käyttöturvallisuuteen. 5.2 §:ssä tarkennetaan etähallinnassa käytettävän päätelaitteen vaatimukset korotetulla ja korkealla varmuustasolla. Järjestelmän toteutus ja kontrollit täytyy suhteuttaa tavoitellun varmuustason mukaan joko kohtuullisen tai vakavan tason tietoturvauhkaan.

Varmuustasot. Korotetun ja korkean varmuustason vaatimuksia ei pääsääntöisesti ole määritelty määräyksessä erikseen. Järjestelmän toteutus ja kontrollit täytyy suhteuttaa tavoitellun varmuustason mukaan joko kohtuullisen tai vakavan tason tietoturvauhkaan.

Eriyttäminen tietoturvatoimenpiteenä. Määräyksen valmistelussa arvioitiin vuonna 2016, onko tietoturvavaatimusten takia tarpeen jokin seuraavista: henkilöstön työtehtävien eriyttäminen, fyysisten työtilojen ja -välineiden eriyttäminen tai teknisen palveluympäristön ja palveluympäristöjen mahdollinen eriyttäminen muusta tuotannosta.

Vaikutusarvioinnissa päädyttiin siihen, että jätettiin eriyttäminen yksityiskohdiltaan pääosin yleisen tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin varaan. Hallintaverkossa ja toimistoverkossa käytettävien työasemien turvallisuusvaatimusten määrittely herätti valmistelussa niin paljon kysymyksiä, että vaatimukset selkeytettiin määräyksessä 5 §:n 2 momentilla ja perustelumuistion soveltamisohjeilla.

Määräyksen 5 §:n 2 momentissa tarkennetaan 1 momentin yleisiä vaatimuksia hallintayhteyksien ja myös niiden etäkäytön osalta. Työntekijöiden päätelaitteet, joilla nämä pääsevät hallintajärjestelmiin, voivat helposti muodostua tietoturvariskiksi, ellei asiaan kiinnitetä erityistä huomiota. Korotetulla varmuustasolla päätelaitteita ei vaadita eriyttämään, mutta korkealla varmuustasolla edellytetään joko dedikoitua päätelaitetta tai virtualisoitua terminointia tai kvm-periaatteeseen (etätyöpöytä) perustuvaa ratkaisua.

Erikokoiset tunnistuspalvelut ja uudet tulokkaat. Tunnistusjärjestelmän ja tunnistusmenetelmän vaatimukset koskevat kaikenkokoisia resursseiltaan erilaisia tunnistuspalveluntarjoajia eli tunnistusvälineen tarjoajia ja soveltuvin osin tunnistusvälityspalveluita. Määräyksen vaatimusten tarkoitus on parantaa turvallisuutta, mutta myös parantaa ennakoitavuutta tunnistuspalveluiden toiminnan helpottamiseksi. Selkeät vaatimukset luovat viraston arvion mukaan myös keskinäistä luottamusta luottamusverkoston nykyisten ja tulevien tunnistuspalveluiden tietoturvallisuuteen.

Alihankkijat. Määräyksessä ei käsitellä erikseen alihankkijoita. Tunnistuspalvelun tarjoaja vastaa tunnistuslain 13 §:n mukaan siitä, että sen alihankintana käyttämät palvelut täyttävät vaatimukset. Tunnistusjärjestelmän ja tunnistusmenetelmän toteuttamisessa käytetään tyypillisesti alihankintaa. Vaatimustenmukaisuuden arvioinnin kannalta alihankintaa käsitellään tunnistuspalvelun arviointiohjeessa 211/2019.

Poikkeamat ja häiriöilmoitukset. Poikkeamien havainnointikyvystä ja hallinnasta ei ole 5 §:n lisäksi tarkennettuja vaatimuksia. Määräyksen 11 §:ssä määrätään häiriöilmoituksista Liikenne- ja viestintävirastolle. Ilmoituskynnystä ei ole tarkennettu määräyksen, mutta määräyksen perusteluissa on soveltamisohjeita eri häiriötilanteista.

Häiriöilmoitusten toimittaminen virastolle on lisääntynyt kiitettävästi vuonna 2019 ja 2020, kun aikaisemmin ilmoituksia ei käytännössä tehty. Määräyksen kannalta viraston arvio on edelleen, että dataa häiriöistä ei ole niin paljon, että sen perusteella voisi määritellä määräystasolla yksiselitteisiä kynnyksiä. Säädettävien kynnysten edellytys olisi myös, että ne olisivat konfiguroitavissa tunnistuspalveluiden teknisiin järjestelmiin ja niiden tulisi olla kohtuullisen pysyviä, jotta tunnistuspalveluille ei aiheudu sääntelyn muutoksista tarpeettomia järjestelmäkustannuksia. Tällaiset määrittelyt tietoturvallisuusuhkissa ja -loukkauksissa ovat viraston valvontakokemuksen perusteella ylipäätään hankalia ja myös muilla valvontasektoreilla (teletoiminta, verkkotunnusvälitys, NIS-direktiivin mukaiset pilvipalvelut) kynnykset ovat laadullisia ja perustuvat soveltamisohjeisiin.

3.2 Vuonna 2016 ja 2018 vaikutusarvioinneissa linjatut asiat

3.2.1 Eriyttäminen

MPS2016 kohta 3.6.1

Arvioitava kysymys: Onko tietoturvavaatimusten takia tarpeen jokin seuraavista: henkilöstön työtehtävien eriyttäminen, fyysisten työtilojen ja -välineiden eriyttäminen tai teknisen palveluympäristön ja palvelinympäristöjen mahdollinen eriyttäminen muusta tuotannosta?

Arvioinnin lähtökohdat

Tunnistus- ja luottamuspalvelulain 8.1 §:n 4 alakohdassa säädetään tunnistusjärjestelmän turvallisuus- ja luotettavuusvaatimuksista. Laissa viitataan myös EU:n varmuustasoasetuksen liitteen kohtiin 2.2.1, 2.3.1 ja 2.4.6. Kohdassa 2.3.1 säädetään todentamismekanismin kyvykkyydestä suojautua ulkoiselta uhalta ja kohdassa 2.4.6. teknisistä tarkastuksista (toimenpiteistä) tietojen, viestintäkanavien ja salaustekniseen aineistoon suojaamiseksi sekä tietoturvallisuuden ylläpitämiseksi ja riskien, poikkeamien ja loukkausten hallitsemiseksi sekä henkilötietoja sisältävistä laitteista huolehtimiseksi.

Viestintävirasto voi määrätä tunnistusjärjestelmän 8 §:n 1 momentin 4 kohdan mukaisista turvallisuutta ja luotettavuutta koskevista vaatimuksista.

Korotettua ja korkeaa varmuustasoa on syytä tarkastella erikseen.

Valmistelussa arvioitavat tekijät on valittu sillä perusteella, että niistä on työryhmätyössä herännyt arviointikriteeristöä valmisteltaessa toimijoiden kysymyksiä.

Linjaukset

Henkilöstön työtehtävien eriyttäminen on tarpeen ainakin siltä osin, ettei sama henkilö voi luoda tunnistusvälinettä ja hallinnoida tunnistusvälineen luomiseen ja käyttöönottoon liittyviä lokitietoja. Tämän oletetaan toteutuvan jo normaalin tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin kautta, eikä asiasta ole tarpeen määrätä erikseen.

Työvälineiden eriyttäminen on tarpeen siltä osin, että hallintaverkkoon ja toimistoverkkoon ei käytetä samaa työasemaa ainakaan korkealla varmuustasolla. Korotetulla tasolla tyydytään siihen, että arvioi-

daan erityisesti tietoturvariskejä, joita liittyy työasemaan, jos sillä pääsee hallintaverkon lisäksi toimistoverkkoon. Asiasta määrätään, koska tarve vaatimusten selkeyttämiseen tässä suhteessa nousi työryhmässä vahvasti esille.

Muilta osin eriyttäminen jätetään tässä vaiheessa yksityiskohdiltaan yleisen tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin varaan.

Määräyksen 5 § ja erityisesti sen 2 momentti on laadittu näiden linjausten mukaisesti.

Määräykselle vaihtoehtoiset ohjauskeinot

Suositus/ohje. *Yksityiskohtia toiminnan tietoturvallisuudesta huomioidaan ohjeessa 211/2016 O tunnistuspalvelun arvioinnin mallikriteeristöön liitettävissä esimerkeissä hyvistä käytännöistä.*

Yhteissääntely. *Viestintävirasto tai toimijat voivat tuoda tietoturvallisuuden toteutuksiin liittyviä kysymyksiä luottamusverkoston yhteissääntelyryhmään tiedonvaihtona hyvistä käytännöistä. Häiriötilanteisiin liittyvään tiedonvaihtoon säädetään tunnistus- ja luottamuspalvelulain 16 §:ssä velvoite ja toisaalta myös tiedon väärinkäyttökielto.*

Informaatio-ohjaus. *Tiedon julkaiseminen ei lähtökohtaisesti tietoturva- ja liikesalaisuussyistä sovellu yritysten yksityiskohtaisten toteutusten ohjaamiseen.*

3.3 Lähteet/referenssit/standardit

- [1] Laki vahvasta sähköisestä tunnistamisesta ja sähköistä luottamuspalveluista (617/2009 muutoksineen, tunnistus- ja luottamuspalvelulaki)
- [3] * EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta (nk. eIDAS-asetus)
- [2] EU:n komission täytäntöönpanoasetus (EU) 2015/1502 (nk. varmuustasoasetus) teknisten vähimmäiseritelmien ja -menettelyjen vahvistamisesta sähköisen tunnistamisen menetelmien varmuustasoja varten sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 910/2014 8 artiklan 3 kohdan mukaisesti
- [10] "LOA guidance" EU:n varmuustasoasetuksen epävirallinen soveltamisohje
  - https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Guidance+documents
  - Suomennos https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/LOA_Guidance_Final_suomeksi.pdf
- ISO/IEC 27001:2013 Information security management (tai uudempi)
- Häiriönhallinnan ISO/IEC (myös SFS) [tarkenna]
  - x
- Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta (SFS-ISO/IEC 27005)
- ETSI
  - varmennestandardit tunnistusvarmenteen kannalta

- [18] NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) www.nist.gov
- [19] SANS (The SANS Institute) www.sans.org
- [15] KATAKRI 2020, Tietoturvallisuuden auditointityökalu viranomaisille
    - https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille
- Pilvipalveluiden turvallisuuden arviointikriteeristö, PiTuKri
    - https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf
- [51] ITU-R TF.1876 (03/2010) Trusted time source for time stamp authority
    - https://www.itu.int/dms_pubrec/itu-r/rec/tf/R-REC-TF.1876-0-201004-I!!PDF-E.pdf
- Haavoittuvuuksien seurantalähteet, mitkä olisivat relevantteja:
    - Määräyksen 5 §:n turvallisuuden ylläpitoon liittyen
    - NIST, SOGIS -päivitykset, NCSA
    - CVE https://cve.mitre.org/ ja https://cwe.mitre.org/
- Liikenne- ja viestintäviraston ohje 211/2019 O tunnistuspalvelun arvioinnista

3.4 Toimialakysely 2020 muutostarpeista

Seuraavaan on koottu viraston elokuussa 2020 tekemästä muutostarvekyselystä aiheeseen liittyviä kysymyksiä ja vastauksia. Vastauksia on tässä koosteessa osittain niputettu ja anonymisoitu.

3.4.1 Kysymykset tietoturvallisuudesta

5) **Tietoturvallisuuden hallinta.** Virasto arvioi, että ainakin määräyksen perusteluja pitää täydentää ja selventää tietoturvallisuuden hallinnan suhde teknisiin vaatimuksiin. Oletteko samaa mieltä?

- *Yleinen kriteeristö tietoturvallisuuden osalta perustuu yleiseen ISO/IEC 27001 -standardiin ja erityiset turvallisuustasoa määrittävät osa-alueet on säännelty asetuksin ja voimaanpanoasetuksin.*
- *Käytännön arviointityössä on esiintynyt epätietoisuutta sovellettavasta kriteeristöstä erityisesti tunnistuspalvelun osalta. Lienee tarkoituksenmukaista todeta käytettävissä olevista kriteereistä esim. nykyistä kuvaavammalla tekstillä, mitä arvioinnin kriteeristöjä on mahdollista käyttää, toteuttaen eIDAS-asetuksen vaatimukset.*
- *vaatimuksenmukaisuuden arvioinnin osalta määräyksen perusteluja on syytä selventää tietoturvallisuuden hallinnan suhteesta teknisiin vaatimuksiin.*
- *viranomaisen järjestämä testiympäristö auttaisi osapuolia paremmin ymmärtämään vaatimuksenmukaisuuden eri osa-alueet ja etenkin tekniset edellytykset.*

- *…verkoston osapuolien tekniset valmiudet eivät ole samantasoisia. Joitain osapuolia jouduttiin käyttöönotoissa tukemaan enemmän kuin muita*

6) **Tietoturvallisuuden hallinta.** Olisiko tietoturvallisuuden hallinnan vaatimuksia mielestänne muutettava, lisättävä tai vähennettävä jollain tavalla ja millä perusteella?

- *Määräykseen kirjatut vaatimukset ovat riittäviä.*
- *nykyinen tietoturvallisuuden auditointimalli on hyvä ja sitä on sellaisena hyvä yllä pitää.*
- *myös omaa tietoturvallisuuden hallintamallia tukeva prosessi. Auditointi antoi lisähavaintoja ja tarjosi lisämahdollisuuden kehittyä tietoturvallisuutensa hallinnassa edelleen*
- *M72A hyväksyy ISO 27001:n tai muun tunnetun standardin mukaisen tietoturvallisuuden hallintajärjestelmän täyttävän 4 § vaatimuksen tietoturvan hyvästä hallinnasta. Olemme asiasta pääosin samaa mieltä, mutta hieman varovaisempia kuin Traficom. Sanamuoto ”on käytettävä” sallii varsin paljon. On perusteltua edellyttää joko ”standardin noudattamista” tai ”sertifioitua noudattamista”.*
- *Olisi hyvä tarkentaa, mitkä standardit täyttävät vaatimuksen. PCIS DSS, ISF SOGP ja Katakri (T-osa) käsittelevät tietoturvan johtamisen asioita, mutta onko niistä 4§ vaatimuksen täyttäjiksi?*

3.4.2 Kysymykset teknisten vaatimusten kattavuudesta

7) **Kattavuus.** Kattaako teknisten vaatimusten sääntely mielestänne oikeat asiat? Ovatko 5 §:n luettelon asiat relevantteja?

- *Kattavuus yleisellä tasolla hyvä. Erityisesti on hyvä korostaa korotetun ja korkean vaatimustason eroja vaatimuksissa, jottei tarvitse tehdä toteutusvaiheessa erillistä tulkintaa.*
- *Nykyinen taso tietoturvallisuuden hallinnan vaatimuksien erittelyssä määräyksen pykälissä 5-6 on riittävällä tasolla ja erillistä tarkentamisen tarvetta ei ole etenkin, kun vaatimuksenmukaisuuden arvioinnista on erillinen arviointikehys.*

8) **Tarpeettomat vaatimukset.** Onko määräyksessä teknisiä vaatimuksia, jotka ovat tarpeettomia? Miksi? Miten näette mahdollisesti tarpeettomina pitämänne vaatimukset suhteessa Suomen markkinoille tuleviin kokonaan uusiin tunnistuspalvelun tarjoajiin?

- *Toivotaan, että välityspalvelun korotetun ja korkean tason eroa voitaisiin tarkastella ja mahdollisuuksien mukaan määrätä kansallisesti luottamusverkostossa toimivat välityspalvelut toimimaan korkean tason vaatimusten mukaisesti. Välityspalvelun rooliin kuuluu välittää useita eri välineitä, jolloin välityspalvelulta on perusteltua edellyttää jopa yksittäistä välinettä korkeampaa tietoturvaa.*

9) **Puuttuvat vaatimukset.** Onko tunnistusjärjestelmän tai tunnistusmenetelmän toteutuksessa osa-alueita, jotka puuttuvat kokonaan määräyksestä ja joista olisi tarpeellista määrätä? Voisiko mahdollisesti puuttuvia asioita edistää ohjeella tai suosituksella?

- *Ohjelmistohaavoittuvuuksien hallinnan osalta on hyvä vaatia säännöllisiä haavoittuvuusskannauksia sekä ulko- että sisäverkon osalta, kuten luottamuspalveluiden sääntelyn puolella vaaditaan.*

3.4.3 Kysymykset varmuustasoista ja eriyttämisestä

10) **Varmuustasot.** Pitäisikö määräyksessä määritellä erikseen korkean varmuustason teknisiä vaatimuksia? Miltä osin ja miten?

- *Kevään tulkintamuistion osalta eriytys korotetun ja korkean tason vaatimuksiin ei ole yksiselitteisen selkeä. Aihepiiri on vielä varsin uusi ja aiheuttaa tulkintaa, erityisesti uudistetun TunnL 17 §:n osalta. Tältä osin olisi tarkoituksenmukaista avata nykyistä konkreettisemmin, miten korotettu ja korkea vaatimustaso eroavat toisistaan tunnistusvälineen myöntämisen toteutuksissa ja prosesseissa. Emme näe tarvetta eritellä korkean tason teknisiä vaatimuksia.*

11) **Varmuustasot.** Voiko eri varmuustasojen vaatimusten soveltamista ennakoida määräyksen sijaan kehittämällä neuvontaa ja tulkintaohjeita tunnistuspalvelun arviointiohjeessa 211/2019 O?

- *Määräys ja ohje ovat eritasoisia sitovuudeltaan, on perusteltua kirjata asiat määräykseen sovellettavaksi jokapäiväisessä palveluntarjonnassa. Arviointiohjeen ensisijainen käyttötarkoitus lienee on, että se toimii ns. tarkistuslistana määräajoin toteutettavien auditointien yhteydessä.*

12) **Eriyttäminen.** Onko mielestänne tarpeen tarkentaa järjestelmien tai työtehtävien eriyttämistä joltain osin määräyksellä tai ohjeella?

- *Emme näe tarvetta erilliselle määräykselle tai ohjeelle.*

- *ei ole tarpeen erikseen määräyksessä tarkentaa järjestelmien tai työtehtävien eriyttämisestä. Määräyksen pykälässä 4 viitataan jo tietoturvallisuuden hallinnassa käytettäviin standardeihin. Näissä määritellään riittävällä tarkkuudella eriyttämisestä ja olisi tarpeetonta päällekkäisyyttä tuoda tällaista määrittelyä erikseen M72-määräykseen.*

3.4.4 Kysymykset uhkien ja häiriöiden hallinnasta

23) Häiriöt. Onko tietoturvauhkien, tietoturvaloukkausten ja häiriöiden havainnoinnissa, hallinnassa ja häiriöilmoituksissa asioita, joita olisi arvioitava määräysvalmistelussa?

- *Nykyinen määräys menettelyineen on riittävä*
- *Käytännön menettelynä Traficomin sivusto on ollut toimiva eIDAS tunnistus- ja luottamuspalveluiden häiriöiden sähköisine ilmoituslomakkeineen, Auditointiraporttien ja poikkeamakorjausten ilmoittamista varten toivoisi sivustolle oman lomakelajinsa.*
-
- *häiriöistä ilmoittaminen ei liene toivotulla tasolla.*
- *Olemme havainneet, että yleisesti katsottuna tunnistuspalvelut antavat varsin vähän häiriöilmoituksia suhteessa monitoroinnissa havaittuihin häiriötilanteisiin. Vaikuttaa siltä, että joko luottamusverkostossa on puutteita häiriöiden havaitsemisessa tai niistä ei raportoida. Kokonaisuutena häiriöt ovat olleet siinä määrin vähäisiä ja vaikutukseltaan rajattuja, että verkoston luotettavuus ei ole vaarantunut. Verkoston maine on hyvällä tasolla.*

- *Häiriöistä ilmoittamisen tulisi olla vakiintunut käytäntö, osa FTN-verkostoon osallistuvien yritysten toimintaprosesseja ja toimintakulttuuria. …epäilee, että viranomainen on nykyisellään osapuolille vieras ja ulkopuolinen.*
-
- *Häiriöistä ilmoittamisen aiheuttamia seurauksia todennäköisesti pelätään etenkin, kun organisaatioiden työntekijät ovat ennestään kovin kuormitettuja. Häiriöiden ilmoittamisen kynnyksen madaltuminen vakiintuneeksi kulttuuriksi edellyttää viranomaiselta aktiivista läsnäoloa ja parempaa tunnettuutta.*
- *Erityisen tärkeää viranomaisen rooli olisi mahdollisten tietoturvaloukkausten tai tietovuotojen selvittämisen koordinoinnissa.*
- *…joutunut kertaalleen omaan seurantaansa ja riskinarvioonsa perustuen sulkemaan tunnistuspalvelustaan erään verkoston osapuolen verkoston kolmannen osapuolen esille nostaneiden tietovuotoepäilyjen takia. Viranomainen ei tässä yhteydessä ottanut kantaa tapahtuneeseen…*
- *Mikäli tietoja häiriöistä olisi saatavilla riittävällä tasolla, olisi viranomaisen hyvä julkaista tilannekuvaa verkoston luotettavuudesta, häiriöalttiudesta ja tyypillisistä ongelmatilanteista, jotta niistä voitaisiin verkostossa oppia ja kehittyä.*
- *Häiriöiden hallinnan osalta verkoston operoinnissa tulisi parhaimmillaan olla saatavilla yleistä tilannekuvaa julkaiseva sivusto, josta kansalainen tai verkoston osapuoli voisi käydä tarkistamassa verkoston eri toimijoiden tilan. Tämän valvontatehtävän olisi hyvä olla viranomaisen operaattorina toimivan osapuolen keskeisimpiä tehtäviä sen lisäksi, että operaattori toimisi välittäjänä verkostossa kommunikoimassa tietoa häiriön osapuolien välillä etenkin silloin, jos nämä eivät keskenään pääse eteenpäin häiriön selvittämisessä.*

3.4.5 Kysymykset toteutettavuudesta ja vaikuttavuudesta

25) Toteutettavuus. Onko määräyksessä teknisiä vaatimuksia, jotka on vaikea toteuttaa teknisesti? Mitkä vaatimukset ja missä toteutustilanteissa? Miten asia pitäisi ratkaista, onko esimerkiksi kompensoivia kontrolleja?

- *Emme ole tunnistaneet tällaisia vaatimuksia.*

- *teknisen toteutuksen suosituksessa 213/2018 S on puutteita ja määrityksiä, jotka ovat ristiriidassa OIDC:n keskeisten määritysten kanssa (OIDC-Core). Näiden löytämiseen ja korjaamiseen on kuitenkin konteksti erikseen, kun verkoston teknisessä työryhmässä on käynnissä erillinen linja ko. suosituksen uudistamiseksi.*

- *Määräyksen 5§2 b) edellyttää, että "korkealla varmuustasolla [hallintayhteyksien, etäkäytön, sähköpostien ja web-selailun aiheuttamat tietoturvauhat ovat] kokonaisuutena arvioiden estetty". Vaatimus on tosiasiallisesti mahdoton noudatettavaksi: minkään uhan toteutumista ei käytännössä voida poistaa. Kohtaa on syytä lieventää niin, etteivät kaikki korkean tason palvelut ole määräyksen vastaisia. Lisäksi on niin, että uhka itsessään on usein palveluntarjoajasta täysin riippumaton, jolloin itse uhkaan ei voida vaikuttaa, mutta uhan toteutumiseen sen sijaan kyllä.*

26) Toteutettavuus. Onko määräyksessä teknisiä vaatimuksia, jotka ovat ristiriidassa keskenään tai joiden toteuttaminen on teknisesti mahdotonta tai vaikeaa jossain käyttötapauksissa? Miten ristiriidat tai toteutettavuusongelmat voisi mielestänne korjata?

- *Emme ole tunnistaneet tällaisia vaatimuksia.*

27) Soveltaminen. Onko määräyksessä vaatimuksia, joiden tulkinta ja soveltaminen on epäselvää?

- Emme ole tunnistaneet tällaisia vaatimuksia, muistio on erittäin kattava.

28) Palvelut. Onko määräyksessä vaatimuksia, joita on vaikea sovittaa yhteen käyttäjille tai asiointipalveluille tarjoamiinne tunnistuspalveluihin tai jotka hankaloittavat niiden kehittämistä?

- Emme ole tunnistaneet tällaisia vaatimuksia.

29) Vaikuttavuus. Miten määräys on vaikuttanut omaan tunnistusjärjestelmäänne ja tunnistusvälineenne ylläpitoon ja sen turvallisuuteen?

- vaikutukset ovat olleet vähäisiä, sillä järjestelmämme ja välineemme ylläpito ja turvallisuus olivat jo määräystä edeltävänä aikana hyvällä tasolla.

30) Vaikuttavuus. Mikä on käsityksenne määräyksen vaikutuksesta muiden luottamusverkostoon rekisteröityjen vahvojen tunnistuspalveluiden tekniseen turvallisuuteen? Luotatteko siihen, että muiden luottamusverkoston jäsenen tunnistusjärjestelmät ovat yhtä turvallisia kuin omanne?

- *oma väline on LoA-tasoa korkea, kun taas muiden välineiden LoA-taso on korotettu. Tekninen turvallisuus on tämän myötä välineellämme korkeammalla tasolla kuin muilla vahvoilla välineillä. Luottamusta muiden toimijoiden välineiden turvallisuuteen voidaan lisätä painottamalla nykyistä vahvemmin ulkoisien auditointilaitosten käyttöä. Ulkoisten auditointilaitosten auditoidessa eri toimijoiden järjestelmiä, kasvaa todennäköisyys sille, että kerran tunnistetut puutteet tulevat korjatuksi myös muiden välineiden kohdalla.*

- *verkoston käynnistymisen yhteydessä kävi ilmi, että verkoston osapuolien tekninen kyvykkyys ei ollut tasaista*

67) Arviointikriteerit. Olisiko kriteereitä tai arviointiperusteita tarkasteltava määräysvalmistelussa? Olisiko niitä tarkennettava joltain osin?

- Tietoturvallisuuden hallinnassa on kiinnitetty huomiota vaatimukseen siitä, että yksi henkilö ei pysty toiminnallaan tahattomasti tai tahallisesti aiheuttamaan vakavaa turvallisuuspoikkeamaa (vaaralliset työyhdistelmät). Vaarallisten työyhdistelmien hallinnassa oleellista on se, että tavanomaisessa prosessissa pyritään eliminoimaan yksin suoritettavia työvaiheita siellä missä se on mahdollista ja varmistamaan audit-jäljen syntyminen ja valvonta siellä missä se ei ole mahdollista. Olisi suotavaa, että vaatimuksenmukaisuuden arvioinnin kriteereissä tunnustettaisiin pääkäyttäjän oikeuksien dilemma, ja arvioitaisiin ovatko operoinnin valvonta ja mitigaatiokeinot tarkoituksenmukaisella tasolla.

4 Muutosvaihtoehdot ja vaikutusarviointi

4.1 Tietoturvallisuuden hallinnan vaatimusten selkeyttäminen (4 §)

Arvioitava kysymys:
a) Kattaako 4 § selvästi tarpeelliset tunnistusjärjestelmän hallinnan osa-alueet? Vaatiiko määräyksen tai perustelujen selventämistä?
b) Onko vaatimusta tietoturvallisuuden hallinnan standardien noudattamisesta/käyttämisestä tarkasteltava/tarkennettava/tiukennettava?
c) Mitkä standardit ovat relevantteja tietoturvallisuuden hallinnan kannalta ISO 27001 lisäksi? (PCIDSS, …)?

4.1.1 Sääntelyehdotus

4 kohta Tunnistuspalvelun tarjoajan tietoturvallisuuden hallinnan vaatimukset

4.1 Tietoturvallisuuden hallinnan standardi

Tunnistuspalveluntarjoajan on noudatettava/käytettävä tunnistusjärjestelmän tietoturvallisuuden hallinnassa ISO/IEC 27001 -standardia tai muuta yleisesti tunnettua vastaavaa tietoturvallisuuden hallinnan standardia. Tietoturvallisuuden hallinta voi perustua myös useamman standardin yhdistelmään.

4.2 Tietoturvallisuuden hallinnan kattavuus

Tietoturvallisuuden hallinnan tulee kattaa seuraavat tunnistuspalvelun tarjontaan vaikuttavat osa-alueet
1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;
2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;
3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta;
4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;
5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi; ja
6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.

4.1.2 Perustelut ja soveltaminen

4.1 Tietoturvallisuuden hallinnan standardi

2016 pohdittiin, mitä standardeja määräyksessä voidaan asettaa referenssiksi. Tuolloin päädyttiin siihen, että ISO 27001 on ainoa riittävän kattava standardi. Arvioinneissa on käytännössä tullut esille ainakin finanssialan standardeihin (kuten PCI DSS) tukeutuminen osana tietoturvallisuuden hallintaa.

Virasto arvioi, että edelleenkään ei ole esitetty relevantteja kokonaisvaltaisia vaihtoehtoja ISO 27001:lle. Se ei ole ainoa vaihtoehto, mutta vaikuttaa olevan ainoa toimialariippumattomasti laajalti käytetty nimenomaan tietoturvallisuuden hallintaan liittyvä standardi.

Määräysmuutostarvekyselyssä annetussa palautteessa ehdotettiin, että säännöksen sanamuotoa tiukennettaisiin tai tarkennettaisiin siten, että edellytetään standardin noudattamista tai sertifiointia. Liikenne- ja viestintävirasto arvioi, että ehdoton sertifiointivaatimus olisi taloudellisesti raskas ja soveltuisi huonosti siihen tilanteeseen, että tietoturvallisuuden hallinnasta huolehditaan usean standardin yhdistelmällä.

Virasto harkitsee kuitenkin sanamuotoa tarkennettavaksi siten, että valittua tai valittuja tietoturvallisuuden hallinnan standardeja on noudatettava. Olisiko tarkoituksenmukaista huomioida varmuustaso?

4.2 Tietoturvallisuuden hallinnan kattavuus

- Kokonaisuutena:
- tunnistuspalvelun tarjoajan tietoturvallisuuden hallinta on kattavaa, johdonmukaista, organisoitua, suunnitelmallista ja jatkuvasti seurattua
- alihankkijoiden tietoturvallisuuden hallinta täyttää vaatimukset

4.2.1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena;

- Tietoturvallisuuden hallintajärjestelmä kattaa tunnistusjärjestelmään vaikuttavat olennaiset sisäiset ja ulkoiset tekniset, oikeudelliset ja hallinnolliset vaatimukset ja tarpeet.
- Tunnistuspalvelussa tulee mm. noudattaa ajantasaisia lainsäädäntöjä ja määräyksiä, kuten tunnistus- ja luottamuspalvelulakia, määräystä 72 ja yleistä tietosuoja-asetusta.

4.2. 2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito;

- Tietoturvallisuuden hallintajärjestelmä kattaa hallinnan johtamisen, organisoinnin ja ylläpidon.
- Käytössä on ajantasainen ja johdon hyväksymä **tietoturvapolitiikka**. Turvallisuusperiaatteet ja politiikat ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset.
- Henkilökunnan ja alihankkijoiden tietoturvallisuuteen liittyvät vastuut on kuvattu.

4.2.3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta

- Tietoturvallisuuden hallintajärjestelmä kattaa tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinnan.
- Riskienhallinta on säännöllinen ja jatkuva, dokumentoitu prosessi.
- Tunnistetut riskit luokitellaan ja priorisoidaan.
- Riskienhallintaprosessi tunnistaa tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kohdistuvat riskit.
- Riskienhallintaprosessia ja sen tuloksia hyödynnetään tunnistuspalvelun/tunnistusjärjestelmän turvatoimien suunnittelussa.

On syytä huomata, että tietoturvallisuuden ja riskien hallinta ei riitä täyttämään tunnistusjärjestelmän vaatimuksia, vaan tunnistusjärjestelmän on kaikilta osin täytettävä tekniset vaatimukset, joista säädetään tunnistuslaissa, EU:n komission varmuustasoasetuksessa ja muualla tässä määräyksessä.

Vaatimustenmukaisuuden arvioinnin kannalta tämä tarkoittaa sitä, että pelkkä tietoturvallisuuden hallinnan arviointi ei riitä osoittamaan säädettyjen vaatimusten täyttämistä, vaan on nimenomaisesti arvioitava, täyttääkö järjestelmä esimerkiksi tietoliikenteen salausvaatimukset.

Vrt. LOA guidance

Riskienhallinnassa yleisenä periaatteena on, että organisaation on itsensä valittava, minkä tasoista riskiä se pitää hyväksyttävänä. Kohdan 2.4 vaatimuksella muutetaan tätä yleistä periaatetta, sillä sen mukaan organisaation turvatoimenpiteiden on oltava suhteutettuja riskeihin kulloisellakin tasolla.

4.2.4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;

- Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden resursoinnin, pätevyysvaatimukset, henkilöstön tietoisuuden tieto-turvallisuudesta, viestinnän ja dokumentoinnin sekä dokumentoidun tiedon hallinnan.
- Ajantasaiset tietoturvaohjeet ja käytännöt ovat kaikkien sähköisen tunnistamisen tehtäviin osallistuvien saatavilla ja tiedossa
- Henkilöstön turvallisuuskoulutus on säännöllistä ja dokumentoitua. Koulutuksen tehokkuutta seurataan

4.2.5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi

- Tietoturvallisuuden hallintajärjestelmässä huolehditaan tunnistuspalvelun tarjonnan suunnittelusta ja ohjauksesta siten, että tunnistuspalvelulle säädetyt tietoturvavaatimukset täyttyvät.

- tunnistuspalvelun vaatimukset (TunnL, eIDAS LOA-asetus ja viraston määräys 72) on huomioitu hallintajärjestelmässä
-

4.2.6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi.

- Tietoturvallisuuden hallintajärjestelmä kattaa tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden säännöllisen arvioinnin.

4.2 kohdan vaatimukset liittyvät ISO/IEC 27001 -standardiin seuraavasti

Määräys 4 kohta § ja soveltaminen	***ISO/IEC 27001***
1) tunnistuspalveluntarjoajan toimintaympäristö kokonaisuutena *- olennaisten sisäisten ja ulkoisten teknisten, oikeudellisten ja yhteisön hallinnollisten vaatimusten, tarpeiden ja asioiden tunteminen ja huomioiminen*	*4 organisaation toimintaympäristö*
2) tietoturvallisuuden hallinnan johtaminen, organisointi ja ylläpito *- dokumentoidaan tietoturvapolitiikassa tai vastaavissa ohjausasiakirjoissa*	*5 johtajuus* *9.2 sisäinen auditointi* *9.3 johdon katselmus* *10 hallintajärjestelmän parantaminen* A.5.1.1 Tietoturvapolitiikat A.6.1.1 Tietoturvaroolit ja -vastuut A.15.1.1 toimittajasuhteiden tietoturvapolitiikka
3) tunnistuspalvelun tarjontaan liittyvien tietoturvallisuusriskien hallinta	*6 suunnittelu*
4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta	*7 tukitoiminnot*
5) tunnistuspalvelun tarjonnan suunnittelu ja ohjaus tietoturvavaatimusten täyttämiseksi	*8 toiminta* A.18.1.1 vaatimustenmukaisuus/lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen: sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen
6) tietoturvallisuuden hallinnan tehokkuuden ja toimivuuden arviointi	*9.1 seuranta, mittaus, analysointi, arviointi*

- eli miten hyvin tietoturvallisuuden hallinta tehoaa/vaikuttaa niihin tekijöihin, prosesseihin ja ongelmiin, jotka vaikuttavat tunnistusjärjestelmän tietoturvallisuuteen	

4.1.3 Tunnistuspalveluiden kehitys, turvallisuusvaikutukset, taloudelliset vaikutukset

Säännökseen ja perusteluihin ehdotetut muutokset selkeyttävät soveltamiskäytäntöä.

Mitä vaikutuksia standardin noudattamisvaatimuksesta aiheutuu?

4.1.4 Muut ohjauskeinot

Ohje
Suositus
Yhteissääntely
Informaatiolla ohjaaminen

4.2 Tunnistusjärjestelmän tekniset vaatimukset 5 §

Arvioitava kysymys:
a) Varmuustasojen vaatimusten eriyttäminen? Kautta linjan tai yksittäisten vaatimusten kannalta - minkä vaatimusten?
b) Perustelumuistion täydentäminen ja esimerkkien lisääminen (esim. tunnistusjärjestelmän arviointiohjeen, katakrin ja/tai pitukrin avulla)?
c) Vaatimusten tarkentaminen?
- **Prosessivaatimusten, kuten haavoittuvuusskannausten lisääminen säädettyihin vaatimuksiin**
- **Pääsyoikeuksien hallinnan ja minimoinnin tarkennustarpeet, pääkäyttäjäteemat yms.?**

4.2.1 Alustava säännösehdotus

5 kohta Tunnistusjärjestelmän tekniset vaatimukset

5.1 Tunnistusjärjestelmän turvallisuuden laatu

Tunnistusjärjestelmän tietoliikenne, tietojärjestelmät ja niiden käyttö on suunniteltava, toteutettava ja jatkuvasti ylläpidettävä koko elinkaaren ajan siten, että tunnistuspalvelun eheys ja luottamuksellisuus on suojattu tunnistuspalvelun varmuustason mukaista [komission varmuustasoasetuksen liitteen kohdassa 2.3 tarkoitettua] kohtuullista tai korkeaa uhkaa ja hyökkäyspotentiaalia vastaan.

5.2 Tietoliikenneturvallisuus

Tunnistusjärjestelmän tietoliikenteessä on oltava

~~*Tunnistusjärjestelmä on suunniteltava, toteutettava ja ylläpidettävä siten, että huomioidaan järjestelmän tietoliikenneturvallisuus*~~

a) verkon rakenteellinen turvallisuus
b) tietoliikenneverkon vyöhykkeistäminen

c) suodatussäännöt vähimpien oikeuksien periaatteilla
d) suodatuksen ja valvontajärjestelmien hallinnointi ~~koko elinkaaren ajan~~
e) hallintayhteydet

5.3 Tietojärjestelmäturvallisuus

Tunnistusjärjestelmän tietojärjestelmissä on oltava

~~➢ tietojärjestelmäturvallisuus~~
a) pääsyoikeuksien hallinta
b) järjestelmien käyttäjien yksilöity tunnistaminen
c) järjestelmien koventaminen
d) haittaohjelmasuojaus
e) turvallisuuteen liittyvien tapahtumien jäljityskyky- ja ennalta määritelty prosessi
f) poikkeamien havainnointikyky ja ennalta määritelty prosessi poikkeamien korjaamiseen ~~toi-puminen~~
g) kansainvälisesti tai kansallisesti suositellut salausratkaisut sen lisäksi, mitä määrätään ~~muu-toin kuin~~ 7 ja 9 kohdassa ~~§:ssä~~ säädetyltä osin

5.4 Käyttöturvallisuus

Tunnistusjärjestelmän käytössä on toteutettava

1) käyttöturvallisuus
a) muutosten suunnitelmallinen hallinta
b) tiedon suunnitelmalliseen luokitteluun perustuva salassa pidettävän aineiston käsittely-ympäristö ja säilytys
c) etäkäyttö ja -hallinta, jossa tunnistusjärjestelmä suojataan etäkäyttöympäristön uhkilta
d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien suunnitelmallinen hallinta
e) varmuuskopiointi

5.5 Tunnistusjärjestelmän tuotantoverkon hallinta- ja etäyhteydet
*Tuotantoverkko ja sen edellä ~~1 momentin 1) e)~~**5.2.e** ja **5.4.c** alakohdissa~~edellä 1 momentin 1) e) ja 3) c) alakohdissa~~ tarkoitetut hallintayhteydet ja etäkäyttö- ja etähallinta on toteutettava siten, että organisaation muiden palveluiden kuten sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat on*
c) korotetulla varmuustasolla erityisesti arvioitu ja minimoitu ja
d) korkealla varmuustasolla kokonaisuutena arvioiden estetty.

4.2.2 Perustelut ja soveltaminen

Lainsäädäntöpohja

5 kohdassa tarkennetaan tietoturvallisuuden toteuttamisessa tarvittavia toimenpiteitä.

Vaatimuksista säädetään yleisellä tasolla tunnistus- ja luottamuspalvelulain 8.1 §:n 4 alakohdassa, jossa viitataan EU:n varmuustasoasetuksen liitteen kohtiin 2.2.1, 2.3.1 ja 2.4.6. Kohdassa 2.3.1 edellytetään korotetulla varmuustasolla todentamismekanismille tietoturvatoimenpiteitä vakavuusasteeltaan kohtuullisten tietoturvauhkien (arvaaminen, salakuuntelu, toisto, manipulointi) estämiseksi.

Kohdassa 2.4.6 säädetään toimenpiteistä tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi, sähköisen viestinnän kanavien suojaamisesta salakuuntelua, manipulointia ja toistoa vastaan, salausteknisen aineiston suojaamisesta, valmiudesta reagoida riskin muutoksiin, poikkeamiin ja tietoturvaloukkauksiin sekä laitteiden ja välineiden tietoturvallisuudesta.

5 kohdan 1-5 alakohdissa tarkennetaan tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuutta, jotta säädännössä vaadittu tietoturvallisuus toteutuisi.

5.1 Tunnistusjärjestelmän turvallisuuden vaatimustaso

Kohdassa 5.1 määritellään yleisellä tasolla tunnistusjärjestelmän turvallisuuden osa-alueet ja turvallisuuden vaatimustaso. Tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuus ovat tietoturvallisuuden arvioinnissa vakiintuneita käsitteitä. Alueet eivät sulje toisiaan pois, vaan ovat pikemminkin eri näkökulmia samaan tunnistusjärjestelmän kokonaisuuteen.

Varmuustasot. Korotetun ja korkean varmuustason vaatimuksia ei pääsääntöisesti ole määritelty määräyksessä erikseen.

Järjestelmän toteutus ja kontrollit täytyy suhteuttaa tavoitellun varmuustason mukaan joko kohtuullisen tai vakavan tason tietoturvauhkaan. Turvallisuuden vaatimustaso perustuu siihen, että tunnistusjärjestelmän eheys ja luottamuksellisuus on pystyttävä kokonaisuutena suojaamaan ulkoisilta ja sisäisiltä tietoturvauhkilta.

Riski- ja uhka-arviota ohjaa laissa säädetty taso, joka on määritelty hyökkäyspotentiaalin perusteella. Korotetun varmuustason järjestelmän on siedettävä kohtuullista (engl. moderate) hyökkäyspotentiaalia ja korkean varmuustason korkean kyvykkyystason hyökkäyspotentiaalia. Uhka- ja riskiarvioon ei ole tarkempaa kriteeristöä, vaan arvion on perustuttava hyvään toimialaosaamiseen ja uhkien, haavoittuvuuksien ja teknisen kehityksen seurantaan.

> LOA Guidance todentamismekanismin 2.3.1 soveltamisohje (ote)
>
> …
>
> *Varmuustasossa eri vakavuusasteista käytettävät termit ovat ”korkeampi perustaso” (enhanced-basic), ”kohtuullinen” (moderate) ja ”korkea” (high). Nämä termit on lainattu standardeista ISO/IEC 15408 ”Information technology – Security techniques – Evaluation criteria for IT security” ja ISO/IEC 18045 ”Information technology – Security techniques – Methodology for IT security evaluation”. Standardien teksti on vapaasti luettavissa osoitteessa www.commoncriteriaportal.org/cc (CCPART1-3 vastaa standardia ISO/IEC 15408 ja CEM standardia ISO/IEC 18045).*
>
> *Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismia] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.*
>
> *Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.*
>
> *Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.*
>
> *Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.*

5.1 Tunnistusjärjestelmän kokonaisuus (arkkitehtuuri)

Tunnistusjärjestelmä (engl. eID scheme) tarkoittaa järjestelmää, jonka puitteissa sähköisen tunnistamisen menetelmiä eli tunnistusvälineitä myönnetään ja tuotetaan käyttäjille. Tunnistusjärjestelmä kattaa tunnistuspalvelun tarjoajan tekniset järjestelmät, tietoturvallisuuden hallinnan ja muut säädetyt luotettavuusvaatimukset. Tunnistusjärjestelmä kattaa myös kaikki alihankitut osat ja toiminnot, jotka liittyvät tunnistuspalvelun tuottamiseen. Tunnistuslain termi on *sähköisen tunnistamisen järjestelmä***.**

Tunnistusjärjestelmään sisältyvät esimerkiksi seuraavat:
- Konesalit ja muut tilat
- tunnistustapahtumaan liittyvät palvelimet ja ohjelmistot
- tunnistamiseen liittyvät järjestelmäkomponentit
- tunnistusjärjestelmän osien väliset yhteydet/yhdyskäytävät/kytkennät, ml. hallintayhteydet
- yhteyksien suojauskäytännöt, järjestelmän osien väliset rajapinnat ja muut seikat - ml. ulkoisten toimijoiden yhteyksien turvallisuuskontrollit
- verkon tietoturvallisuuskomponentit, kuten palomuurit
- tietovarannot

Alihankkijat. Määräyksessä ei käsitellä erikseen alihankkijoita. Tunnistuspalvelun tarjoaja vastaa tunnistuslain 13 §:n mukaan siitä, että sen alihankintana käyttämät palvelut täyttävät vaatimukset. Tunnistusjärjestelmän ja tunnistusmenetelmän toteuttamisessa käytetään tyypillisesti alihankintaa. Vaatimustenmukaisuuden arvioinnin kannalta alihankintaa käsitellään tunnistuspalvelun arviointiohjeessa 211/2019.

Jos tunnistusjärjestelmässä käytettään pilvipalveluiden tuotteistettuja komponentteja tai tuotteita (Amazon Web Services, Google, Microsoft Azure jne.), tunnistusjärjestelmän vaatimukset koskevat näitä komponentteja ja ne täytyy sisällyttää myös vaatimustenmukaisuuden arvioinnin piiriin. Tunnistusjärjestelmässä voi käyttää vain komponentteja, jotka täyttävät vaatimukset ja joiden vaatimustenmukaisuudesta pystytään varmistumaan.

Eriyttäminen tietoturvatoimenpiteenä. Määräyksen valmistelussa arvioitiin vuonna 2016, onko tietoturvavaatimusten takia tarpeen jokin seuraavista: henkilöstön työtehtävien eriyttäminen, fyysisten työtilojen ja -välineiden eriyttäminen tai teknisen palveluympäristön ja palvelinympäristöjen mahdollinen eriyttäminen muusta tuotannosta. Vaikutusarvioinnissa päädyttiin siihen, että jätettiin eriyttäminen yksityiskohdiltaan pääosin yleisen tietoturvallisuuden hallinnan, suunnittelun ja auditoinnin varaan. Tätä arviota ei ole muutettu 2021.

5.2 Tietoliikenneturvallisuus

5.2 vastaa pitkälti määräyksen aikaisempaa sanamuotoa 5.1 §:n 1 alakohdassa.

5.2 kohdassa määrättyjen vaatimusten lisäksi määräyksen 14 kohdassa määrätään tietoliikenneprotokollasta ja kohdissa 7-9 tietoliikenteen suojaamisesta tunnistuspalveluiden välillä ja tunnistuspalveluiden ja niihin luottavien asiointipalveluiden välillä. Tunnistusvälineen käyttäjän ja tunnistusvälineen tarjoajan välisen yhteyden turvallisuus on osa todentamismekanismin vaatimuksia.

5.2.a) *verkon rakenteellinen turvallisuus*

Verkon rakenteellisella turvallisuudella edellytetään, että *henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta*

- dokumentoitava

- tunnistusjärjestelmän tietoliikennelaitteet ja -järjestelmät on tunnistettu ja dokumentoitu
- koskee tunnistusjärjestelmän osien välisiä tietoliikenneyhteyksiä ja niiden suojauskäytäntöjä
- eri turvatason verkkoalueet, sekä niiden välissä toimivat suodatus- ja valvonta-järjestelmät
- myös kaikki relevantit tietoliikenneyhteydet alihankkijoihin (infra, ohjelmistot, käyttöpalvelut, korttitehdas jne.)

5.2. b) tietoliikenneverkon vyöhykkeistäminen

Tällä pyritään vähentämään tietoliikenneyhteyksien kautta aiheutuvia riskejä verkkojen eheydelle, luottamuksellisuudelle ja käytettävyydelle.

- tuotantoverkon, ylläpito- ja hallinnointiverkon sekä muun toimistoverkon tulee olla eriytettynä toisistaan.
- Lisäksi käytössä on oltava tuotannosta eriytetty kehitysympäristö

5.2. *c) suodatussäännöt vähimpien oikeuksien periaatteilla*

- Kaikki muut kuin toiminnalle tarpeelliset yhteydet pitää kieltää tai sulkea.
- Tuotantoverkon yhteyksien julkiseen verkkoon tulee olla riskiperusteisia, vain palvelun toiminnallisuudet mahdollistavia yhteyksiä.

5.2 d) suodatuksen ja valvontajärjestelmien hallinnointi

Ei esimerkkejä soveltamisesta.

5.2.*e) hallintayhteydet*

- Alakohdassa tarkoitetut hallintayhteydet voivat olla sekä organisaation sisäisiä että ulkoisia tietoliikenneyhteyksiä.
- Hallintaan käytettävä tietojenkäsittely-ympäristö tulee olla erotettu muista ympäristöistä.

Ks. myös erityisesti 5.5 Tunnistusjärjestelmän (tuotantoverkon) etäkäytössä ja etähallinnassa pitää olla estetty sähköpostin tai web-selailun kautta aiheutuvat tietoturvauhat, sekä hallinnassa käytettävän päätelaitteen muiden kuin hallinnassa välttämättömien toimintojen aiheuttamat tietoturvauhat.

5.3 Tietojärjestelmäturvallisuus

5.3 vastaa pitkälti määräyksen aikaisempaa sanamuotoa 5.1 §:n 2 alakohdassa.

5.3.a) *pääsyoikeuksien hallinta vähimpien oikeuksien periaatteella*

- pääsy myönnetään vain tietojärjestelmän luokitteluun ja käyttäjän tehtäviin perustuen.
- Pääsyoikeuksien hallinnoinnin avulla rajoitetaan pääsy tietoon ja tiedonkäsittely-ympäristöihin suunnitelmallisesti ja dokumentoidusti.
- tarpeettomien käyttöoikeuksien säännöllinen poistaminen
- Pääkäyttäjien oikeuksien määrittelyssä on käytettävä järjestelmien eriyttämistä ja lokien muuttumattomuuden varmistamista ja muita tarkoituksenmukaisia keinoja.

5.3.b) *järjestelmien käyttäjien yksilöity tunnistaminen*

- alakohdassa edellytetään, että käyttäjätunnusten täytyy olla henkilökohtaisia, eivätkä ne voi olla yhteiskäyttöisiä.
- Tunnistusjärjestelmän tietojärjestelmien käyttäjät tunnistetaan tunnetulla ja turvallisena pidetyllä menetelmällä …pääsääntöisesti MFA…jos käyttäjätunnusta ja salasana arvioidaan kokonaisuutena muiden suojakeinojen jossain kohdin riittäväksi, edellytetään riittävän vahvoja salasanoja

Tunnistamisella varmistetaan, että vain oikeat käyttäjät pääsevät järjestelmiin ja toisaalta, että voidaan jäljittää tapahtumat.

5.3.*c) järjestelmien koventaminen*

- järjestelmien koventamisella tarkoitetaan, että tunnistusjärjestelmässä käytetään vain sen toiminnan kannalta tarvittavia palveluita, toimintoja, prosesseja, laitteita ja komponentteja.
- Niiden käyttö tulee määritellä siten, että asennuksesta on poistettu kaikki tarpeettomat oikeudet ja toiminnot.
- Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.

5.3.*d) haittaohjelmasuojaus*

- alakohdan mukaan tulee tunnistusjärjestelmässä huolehtia haitta-ohjelmien aiheuttamien haittojen ja uhkien havaitsemisesta, ennaltaehkäisystä, estämisestä ja korjaamisesta.

5.3.e) *turvallisuuteen liittyvien tapahtumien jäljitys*kyky- ja ennalta määritelty prosessi

- alakohdassa edellytetään, että olemassa on ennalta määritelty menettely, jota noudatetaan mahdollisen turvallisuuspoikkeaman jäljittämisessä ja korjaamisessa.
- Seuraavassa kohdassa kuvatut lokitukset ovat osa tapahtumien jäljityskykyä.

5.3.*f) poikkeamien havainnointikyky ja* ennalta määritelty prosessi poikkeamien korjaamiseen ~~toipuminen~~

- alakohdassa edellytetään, että tunnistusjärjestelmän poikkeamien havaitsemiseen on kyvykkyys ja ennalta määritellyt prosessit.
- Määrittelyissä tulee huomioida järjestelmän tietoliikenneyhteyksien ja tietojärjestelmien komponenttien ja prosessien kriittisyys ja luokittelu ja se, että turvallisuuteen vaikuttavat tapahtumat kyetään jäljittämään myös jälkikäteen.
- Tunnistusjärjestelmässä kerätään ja tallennetaan tapahtumalokeja järjestelmän toiminnasta ja tietoturvaan vaikuttavista tapahtumista ja poikkeamista.
- Tunnistusjärjestelmän toimintaa, muutoksia ja tapahtumalokeja monitoroidaan poikkeamien ja tietoturvaloukkausten havaitsemiseksi.
- Lokien eheydestä huolehditaan mm. pääsyn- ja käyttöoikeuksien hallinnalla ja ympäristön suojaamisella.
- Tunnistusjärjestelmän poikkeamat ja häiriöt käsitellään ja analysoidaan ja niiden vakavuus luokitellaan suunnitelmallisesti.
- Kaikki havainnot käsitellään ja niiden vaikuttavuus luokitellaan sovittujen menetelmien mukaan.
- Poikkeamat korjataan vakavuusluokittelun edellyttämällä tavalla.

3.*g) kansainvälisesti tai kansallisesti suositellut salausratkaisut* sen lisäksi, mitä ~~muutoin kuin~~ *7 ja 9 kohdassa* ~~*§:ssä*~~ määrätään~~säädetyltä osin~~

alakohdassa tarkoitettuja salausratkaisuja löytyy esimerkiksi seuraavista lähteistä:
- ENISA [16],
- Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen NCSA:n (National Communications Security Authority, NCSA-FI) tuottama aineisto [17],
- NISTin (National Institute of Standards and Technology) FIPS-standardit (Federal Information Processing Standards) [18] tai
- SANS (The SANS Institute) [19].

Vaatimus kohdistuu esim. tunnistusjärjestelmän sisäisiin elementteihin, yhteyksiin alihankkijan järjestelmiin jne.

5.4 Käyttöturvallisuus

5.4.a) *muutosten suunnitelmallinen hallinta*

- suunnitelmallisuus
- dokumentointi
- katselmoinnit, testaaminen
- jäljitettävyys…tunnistusjärjestelmän hallintalokeihin tallennetaan tiedot tunnistusjärjestelmässä tehtävistä muutoksista, lokit on eriytetty muista lokeista ja niiden eheydestä on huolehdittu.

5.4.b) tiedon suunnitelmalliseen luokitteluun perustuva salassa pidettävän aineiston käsittelyympäristö ja säilytys

Alakohtaan on lisätty/siirretty säilytettävien tietojen suojaus entisestä 7 § 4 kohdasta
Tunnistusjärjestelmässä säilytettävien tietojen eheydestä ja luottamuksellisuudesta on huolehdittava. Jos tiedon suojaaminen perustuu ainoastaan niiden salaukseen, sovelletaan kohdan 7.1 allekirjoittamisen, symmetrisen salaamisen ja tiivistefunktioiden vaatimuksia.

- tiedon ja aineistojen luokittelu ottaen huomioon…esim. kryptografiset salaisuudet, henkilötiedot, liikesalaisuudet jne. …
- turvatoimet on mitoitettu ottaen huomioon muun muassa tiedon luokitteluperuste, määrä, muoto ja sijoitustilat suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan.
- säilytettävien tietojen eheys ja luottamuksellisuus ottaen huomion tiedon luokittelu, pääsynhallinta ja salaus…
- mm. salaukseen käytettävien avainten huolellinen hallinta
- Tunnistusjärjestelmän tietojärjestelmät pitää olla luokiteltu huomioiden niissä käsiteltävä tieto ja niiden mahdollistamat toiminnot.
- Järjestelmien luokittelussa tulee huomioida suojattavan tiedon koko elinkaari.

5.4.c) etäkäyttö ja -hallinta

Ei esimerkkejä soveltamisesta.

5.4.*d) ohjelmistokehityksen ja ohjelmistohaavoittuvuuksien suunnitelmallinen hallinta*

- alakohdassa edellytetään, että organisaatiolla tulee olla menetelmä yleisten haavoittuvuuksien seurantaan ja sen tulee kattaa tunnistusjärjestelmän turvallisuuteen vaikuttavat ohjelmistot
- tunnistusjärjestelmässä käytettävien ohjelmistojen tulee noudattaa turvallisen ohjelmoinnin periaatteita…mukaan lukien kehitysympäristön turvallisuus

- Kirjastot, tunnistussovellukset jne.

- salausalgoritmien ja menetelmien haavoittuvuuksien seuranta
- Tiedotteiden seuranta
- Järjestelmät tarkastetaan automaattisesti

Ks. Pitukri

Pilvipalvelun koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmisto-haavoittuvuuksien hallitsemiseksi.
Erityisesti huomioitava:
a) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja riskiperusteisesti tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti (vrt. MH-01).
b) Järjestelmät tarkistetaan tunnettujen haavoittuvuuksien varalta automaattisesti vähintään kuukausittain. Jos suunnitelluista asetuksista tai turvapäivitystasosta on poikettu, syyt analysoidaan, ja poikkeamat korjataan tai dokumentoidaan poikkeamahallintaprosessin mukaisesti (ks. TJ-04).

Haavoittuvat algoritmit, vrt. Määräyksen 7 kohta

Määräyksessä listattujen algoritmien tai arvojen muuttuminen haavoittuviksi ja siitä aiheutuva tarve luopua niiden käytöstä?

…tarkoituksenmukainen tapa huomioida haavoittuvuudet on seurata niitä koskevia tiedotuskanavia ja luopua omaehtoisesti haavoittuvien menetelmien käytöstä. Tunnistuspalveluilla on mahdollisuus ja määräyksen 5 §:n mukaan velvollisuus ylläpitää tunnistuspalveluidensa tietoliikenne-, tietojärjestelmä- ja käyttöturvallisuutta. Haavoittuvuuksien seurannan tarkentamista arvioidaan 5 §:n yhteydessä ja soveltamiskäytäntöä voidaan tarkentaa sen perusteluissa. Haavoittuvuuksiin reagoimista voidaan tarvittaessa ohjata viraston suosituksella.

5.4.*e) varmuuskopiointi*

- tunnistusjärjestelmän varmuuskopioinnista huolehditaan suunnitelmallisesti ja
- varmuuskopioinnissa huomioidaan tiedon luokittelu (henkilötiedot, salaustekniset tiedot jne.), järjestelmien palautettavuus ja varmuuskopioiden säilytys.
- Varmuuskopioiden fyysinen sijoituspaikka tulee olla riittävän eriytetty varsinaisesta järjestelmästä.

5.5

5.5 alakohdassa tarkennetaan edeltävien kohtien yleisiä vaatimuksia hallintayhteyksien ja myös niiden etäkäytön osalta.

Kohdassa tarkennetaan etähallinnassa käytettävän päätelaitteen vaatimukset korotetulla ja korkealla varmuustasolla.

Työntekijöiden päätelaitteet, joilla nämä pääsevät hallintajärjestelmiin, voivat helposti muodostua tieto-turvariskiksi, ellei asiaan kiinnitetä erityistä huomiota. Jos päätelaitteella on käytössä esimerkiksi sähköpostiohjelmisto tai muita vastaavia ohjelmistoja, sen saastumisen riski haittaohjelman takia on todellinen ja tämä altistaa myös tunnistusjärjestelmän hallinnan.

Käytettävyys- ja käytännöllisyyssyyt toisaalta puoltavat sitä, että työntekijä voi hoitaa kaikkia työtehtäviään samalla päätelaitteella. Siksi korotetulla varmuustasolla edellytetään vain sitä, että tehdään huolellinen riskiarvio ja luonnollisesti huolehditaan erilaisilla toimenpiteillä siitä, että päätelaitteen saastumisen riski on hallittavissa.
Korkealla varmuustasolla edellytetään, että hallintaverkkoon pääsee vain päätelaitteella, josta on poistettu kaikki hallintaverkon hallinnan kannalta tarpeettomat yhteydet ja toiminnot.

5 alakohdan kannalta internetiä ja toimistoverkkoa pidetään ei-luotettuina verkkoina, ellei toimistoverkko kuulu vaatimustenmukaisuuden arvioinnin piiriin. Tiedonsiirtokanavan täytyy siis olla etäkäytössä suojattu ja toimistoverkon aiheuttamat riskit täytyy huomioida. Korotetun varmuustason vaatimukset ovat tavanomaisia ja ne katetaan jo esimerkiksi ISO 27001 -vaatimusten kautta, jos sovelletaan sitä.
Korkealla varmuustasolla 5 alakohdan vaatimukset voi toteuttaa ainakin siten, että etäkäytössä olevasta työasemasta estetään pääsy muihin organisaation palveluihin kuten sähköpostiin ja poistetaan työasemasta mahdollisuus käyttää muita kuin hallintaverkon käytön kannalta välttämättömiä toimintoja. Käytännössä tämä tarkoittaa siis erillistä työasemaa hallintakäyttöä varten.

Korkealla varmuustasolla edellytetty kokonaisarvio tarkoittaa sitä, että jos käytetään muuta kuin edellä kuvattua kovennettua työasemaa, otetaan toteutuksessa huomioon tuotantojärjestelmän eriyttäminen ja muut järjestelyt, joilla tietoturvauhkat voidaan hallita. Lähtökohtaisesti tällöin edellytetään virtualisoitua terminointia tai kvm-periaatteeseen (etätyöpöytä) perustuvaa ratkaisua.

Olennaista on, mitä tehdään sillä päätelaitteella, josta virtualisoitua yhteyttä otetaan ja siten esimerkiksi two-factor VPN-yhteys virtualisoituun työasemaan ei yksin riitä ratkaisuksi. Riittävää ei ole myöskään, että käytetään virustorjuntaa ja web-proxya.

Välttämättömien tiedostojen siirrossa koneelta toiselle on myös huomioitava haittaohjelmien riski mm. pitämällä huolta siitä, että käytetään vain luotettavia lähteitä ja varmistetaan tietoturvallisuus (eheys) kaikilla tarpeellisilla menetelmillä.

4.2.3 Tunnistuspalveluiden kehitys, turvallisuusvaikutukset, taloudelliset vaikutukset

Säännöksen vaatimukset eivät muutu, mutta niitä selvennetään. Säännöstä on tarkennettu ja perusteluihin on lisätty esimerkkejä soveltamisesta tunnistuspalveluiden vaatimustenmukaisuuden arvioinnissa ja valvonnassa kertyneen kokemuksen ja soveltamiskäytännön perusteella.

Muutokset ovat omiaan parantamaan tunnistusjärjestelmien turvallisuutta. Vaatimukset eivät ole teknologiariippuvaisia, joten niillä ei ole vaikutusta tunnistuspalveluiden ominaisuuksien kehittämiseen.

4.2.4 Muut ohjauskeinot

Ohje. Arviointiohjeessa 211/2019 on tarkennettu tietoturvallisuuden arvioinnin vaatimuksia.
Suositus. Kyselyssä on toivottu testauspalvelua, mutta virastolla ei ole vahvan sähköisen tunnistamisen valvonnassa säädettyjä operatiivisia tehtäviä kuten testaustoiminnan hankintaa tai ylläpitoa. Olisiko testaussuositus laadittavissa luottamusverkostossa?
Yhteissääntely. Tietoturvallisuuden taso on sääntelyssä ja valvonnassa määritelty asia. Luottamusverkoston yhteistoimintaryhmässä on mahdollisuus vaihtaa salassapitosäännösten estämättä tietoa turvallisuusuhkista ja -toimenpiteistä.
Informaatiolla ohjaaminen. Ei huomioita.

4.3 Häiriöilmoituskynnys

Arvioitava kysymys:
Onko tarpeellista tiukentaa toimivuushäiriöiden ilmoitusvaatimusta viranomaiselle, jotta valvova viranomainen saa kokonaiskuvan toimivuushäiriöistä? Mikä olisi ilmoituskynnys (tunnit, käyttäjämäärät, …)?

4.3.1 Säännösehdotus

11 kohta §~~.~~ Tunnistuspalveluntarjoajan häiriöilmoitukset Liikenne- ja v~~V~~iestintävirastolle

11.1 Ilmoitettavat tiedot

Liikenne- ja v~~V~~iestintävirastolle tunnistus- ja luottamuspalvelulain 16 §:n mukaisesti tehtävässä merkittävää uhkaa tai häiriötä koskevassa ilmoituksessa on annettava vähintään seuraavat tiedot:

1) *tunnistusväline tai välityspalvelu, johon häiriö vaikuttaa;*
2) *kuvaus häiriöstä ja sen tiedossa olevista syistä;*
3) *kuvaus häiriön vaikutuksista, mukaan lukien vaikutus uusien tunnistusvälineiden myöntämiseen, käyttäjiin, luottaviin osapuoliin, muihin luottamusverkoston toimijoihin ja rajat ylittävään käyttöön;*
4) *kuvaus korjaustoimenpiteistä; sekä*
5) *kuvaus häiriöstä tiedottamisesta luottaville osapuolille, tunnistusvälineiden haltijoille, luottamusverkostolle ja tieto ilmoittamisesta muille viranomaisille.*

11.2 Merkittävät häiriöt

Merkittäviä tunnistuspalvelun häiriöitä ovat tapahtumat, jotka ~~Häiriön merkittävyyden arvioinnissa merkittävyyttä lisää se, että häiriö~~ liittyväty~~y~~ sähköisen henkilöllisyyden virheellisyyteen tai väärinkäyttöön tai tietoturvauhkaan tai -häiriöön, joka vaarantaa tunnistamisen eheyden ja luotettavuuden. Merkittäviä ovat myös ennakoimattomat toimivuushäiriöt, joilla on vähäistä suurempia haittaa~~yyttä lisää myös se, että häiriöllä on~~ vaikutuksia luottamusverkostoon.

4.3.2 Perustelut ja soveltaminen

Säännökseen on tehty valvonta- ja soveltamiskäytännön mukaisia selvennyksiä. Ilmoituskynnystä tai ilmoitettavia tietoja ei ole tarkoitus muuttaa, vaan ainoastaan selkeyttää säännöstä.

Viraston kyselyyn määräyksen muutostarpeista annetuissa vastauksissa esitettiin huoli, että kaikki eivät ilmoita häiriöistä virastolle riittävän alhaisella kynnyksellä ja että kaikki tunnistuspalvelut eivät informoi toisiaan häiriötilanteista.

Virasto arvioi, että näihin havaintoihin on vaikutettava ensisijaisesti valvonnalla ja tehostamalla edelleen luottamusverkoston keskinäistä informointia. Jälkimmäinen ei kuulu määräystoimivallan piiriin. Virasto ei myöskään pidä palautteen perusteella tarkoituksenmukaisena tai tarpeellisena laatia määräykseen toimivuushäiriöille uusia ilmoituskynnyksiä. Arviota ei muuteta vuonna 2016 tehdystä arviosta. On myös huomattava, että tunnistuslaissa ei ole nimenomaisia vaatimuksia tunnistuspalveluiden toimintavarmuudesta, varmistamisesta tai varautumisesta eikä siten toimivaltuutta määrätä niistä.

Tunnistamisen eheyteen ja luottamuksellisuuteen liittyvissä poikkeamissa ilmoituskynnys on määräyksen mukaan matala ja esimerkkejä virastolle ilmoitettavista häiriöistä esitetään perusteluissa.

Onko esimerkkejä perusteluissa tarpeellista tarkentaa tai lisätä?

4.3.3 Tunnistuspalveluiden kehitys, turvallisuusvaikutukset, taloudelliset vaikutukset

Tunnistuspalveluiden turvallisuuden kannalta ilmoitukset eheyttä ja luottamuksellisuutta koskevista häiriöistä ovat tärkeitä sekä virastolle että muille luottamusverkoston tunnistuspalveluille. Ilmoitusten havaintojen perusteella voidaan edistää kaikkien tunnistuspalveluiden turvallisuuden parantamista.

Toimintahäiriöt vaikuttavat usein myös muiden luottamusverkoston tunnistuspalveluiden tarjoamiseen ja asiakassuhteisiin. Siksi hyvä häiriönhallinta ja informointi vaikuttavat positiivisesti kaikkien toimintaedellytyksiin.

4.3.4 Muut ohjauskeinot

Ohje. Ei huomioita.
Suositus. Ei huomioita.
Yhteissääntely. Luottamusverkoston yhteistoimintaryhmässä on laadittu käytänne häiriöiden ja uhkien tiedonvaihdosta toimijoiden välillä.
Informaatiolla ohjaaminen. Ei huomioita.

5 Säädäntö

5.1 Määräyksen antamisen perusta

42 § (23.11.2018/1009) Yleinen ohjaus sekä Liikenne- ja viestintäviraston määräykset

Vahvan sähköisen tunnistamisen ja sähköisten luottamuspalveluiden yleinen ohjaus ja kehittäminen kuuluvat liikenne- ja viestintäministeriölle.

Liikenne- ja viestintävirasto voi antaa tarkempia määräyksiä:

1) tunnistusjärjestelmän 8 §:n 1 momentin 4 ja 5 kohdan mukaisista turvallisuutta ja luotettavuutta koskevista vaatimuksista;

…

5.2 Asiaan liittyvät säännökset

5.2.1 Tunnistusjärjestelmän vaatimukset, säännökset

TunnL 8 § (29.6.2016/533) Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

…

4) tunnistusjärjestelmä on turvallinen ja luotettava siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdissa 2.2.1, 2.3.1 ja 2.4.6 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät ottaen huomioon kulloinkin käytettävissä olevaan tekniikkaan liittyvät tietoturvallisuusuhat sekä tunnistuspalvelun tarjoamiseen käytettävät tilat ovat turvallisia sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdassa 2.4.5 säädetyllä tavalla;

…

LOA 2.2.1 Sähköisen tunnistamisen menetelmien ominaispiirteet ja suunnittelu

LOA 2.3.1 Todentamismekanismi

Seuraavassa taulukossa esitetään vaatimukset varmuustasoittain todentamismekanismista, jolla luonnollinen tai oikeushenkilö käyttää sähköisen tunnistamisen menetelmää vahvistaakseen henkilöllisyytensä luottavalle osapuolelle.

…

LOA 2.4.5 Tilat ja henkilökunta

Seuraavassa taulukossa esitetään vaatimukset, jotka koskevat tiloja ja henkilöstöä sekä tarvittaessa alihankkijoita, jotka suorittavat tämän asetuksen soveltamisalaan kuuluvia tehtäviä. Kunkin vaatimuksen noudattaminen on suhteutettava siihen, minkä tasoinen riski tarjottavaan varmuustasoon liittyy.

MATALA, KOROTETTU, KORKEA

…

3. Palvelun tarjoamiseen käytetyt tilat ovat jatkuvasti seurattuja ja suojattuja ympäristötapahtumien aiheuttamilta vahingoilta, luvattomalta käytöltä ja muilta tekijöiltä, jotka voivat vaikuttaa palvelun turvallisuuteen.

4. Palvelun tarjoamiseen käytetyissä tiloissa varmistetaan, että pääsy alueille, joilla säilytetään tai käsitellään henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, rajoitetaan koskemaan valtuutettuja henkilöstön jäseniä tai alihankkijoita.

LOA 2.4.6 Tekniset tarkastukset

MATALA

1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.

2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.

3. Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä.

4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin.

5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.

KOROTETTU

Sama kuin tasolla "matala" lisättynä seuraavalla:

Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.

KORKEA

Sama kuin tasolla "korotettu".

5.2.2 LOA guidance, tunnistusjärjestelmän vaatimukset

2.4.6 Tekniset tarkastukset

MATALA

1. Käytössä on oikeasuhteiset tekniset tarkastukset palvelujen turvallisuuteen kohdistuvien riskien hallitsemiseksi ja käsiteltävien tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamiseksi.

OHJE:

On tärkeää pitää erillään luottamuksellisuuden ja eheyden suojaamista koskevien vaatimusten arviointi. Eheyden (tai aitouden) suojaaminen määräytyy periaatteessa varmuustason mukaan, mutta henkilöihin liittyvän tiedon luottamuksellisuuteen vaikuttavat myös tietojen tyyppi sekä mahdolliset suojaamista koskevat lainsäädännölliset vaatimukset.

Henkilötietojen luottamuksellisuus on suojattava ja käytössä on oltava turvatoimenpiteitä, jotka pohjautuvat riskiperusteista lähestymistapaa hyödyntävään arviointiin valitun tietoturvallisuuden hallintajärjestelmän mukaisesti. Turvatoimenpiteiden kattamia osa-alueita ovat esimerkiksi tietomurrot, väärinkäytökset, palvelunestohyökkäykset ja hajautetut palvelunestohyökkäykset.

Henkilötietojen luottamuksellisuutta ja aitoutta/eheyttä rajat ylittävissä siirroissa käsitellään yhteentoimivuusjärjestelmää koskevassa täytäntöönpanoasetuksessa.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.10 "Cryptography", (saatavuutta koskevan kohdan) A.12 "Operations security", A.17 "Information security aspects of business continuity management" ja A.18.1.5 "Regulation of cryptographic controls" mukaisia turvatoimenpiteitä.

2. Henkilökohtaisten tai arkaluonteisten tietojen vaihtoa varten käytettävät sähköisen viestinnän kanavat on suojattu salakuuntelulta, manipuloinnilta ja toistolta.

OHJE:

On syytä huomata, että viestintäkanavia voi syntyä samaan tunnistamisjärjestelmään osallistuvien osapuolten välille, esimerkiksi tunnistamismenetelmän omistajan ja palvelun tai kunnan ja valmistajan välille.

Yhtenä tapana toteuttaa viestintäkanavien teknistä valvontaa ovat viranomaisen antamat tekniset ohjeet, joissa määritellään käytettäviä salauksia ja turvatoimenpiteitä koskevat vaatimukset. Tässä käytetään yleensä salausprotokollaa, jonka varmennuksen vaiheet on kuvattu erikseen.

eIDAS-yhteentoimivuusjärjestelmän solmupisteiden välisiä viestinnän kanavia koskevat vaatimukset on ilmoitettu järjestelmää koskevassa teknisessä erittelyssä.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.10 "Cryptography", A.13 "Communications security" ja A.18.1.5 "Regulation of cryptographic controls" mukaisia turvatoimenpiteitä. Kohdissa saatetaan myös viitata edellä mainittuihin teknisiin ohjeisiin.

3. Pääsy arkaluonteiseen salaustekniseen aineistoon, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, rajoitetaan tiukasti niihin tehtäviin ja

sovelluksiin, jotka edellyttävät tällaista pääsyä. On varmistettava, ettei tällaista aineistoa koskaan tallenneta pysyväisluonteisesti ilmitekstinä.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.9 "Access control" ja A.10 "Cryptography" mukaisia turvatoimenpiteitä.

4. Käytössä on menettelyt, joilla varmistetaan, että turvallisuus säilyy ja että kyetään vastaamaan muutoksiin riskitasoissa, poikkeamiin ja tietoturvaloukkauksiin.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.14 "Security in development and support processes" ja A.16 "Information security incident management" mukaisia turvatoimenpiteitä.

5. Kaikki laitteet ja välineet, jotka sisältävät henkilötietoja, salattuja tietoja tai muita arkaluonteisia tietoja, säilytetään, kuljetetaan ja hävitetään turvallisella ja varmalla tavalla.

OHJE:

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.8 "Asset management" mukaisia turvatoimenpiteitä

KOROTETTU

Taso "matala" lisättynä seuraavalla:

Arkaluonteinen salaustekninen aineisto, jota käytetään sähköisen tunnistamisen menetelmien myöntämiseen sekä todentamiseen, on suojattu luvattomalta käsittelyltä.

OHJE:

Arkaluonteisella salaustekniselllä aineistolla tarkoitetaan avainaineistoja, joita käytetään sähköisen tunnistamisen menetelmien myöntämisessä, käyttäjien todentamisessa ja vakuutusten myöntämisessä (tarvittaessa). Tällaisten salausavainten suojaaminen on ensiarvoisen tärkeää sähköisen tunnistamisen järjestelmän turvallisuuden kannalta.

Luvattomalta käsittelyltä suojautumiseen tarkoitetuilla mekanismeilla pyritään estämään salausavainaineistojen julkistaminen, muuttaminen tai väärinkäyttö koko niiden elinkaaren ajan. Tätä varten avainten suojaamisessa käytetään sekä fyysisiä että loogisia turvatoimenpiteitä.

Yleisenä käytäntönä on, että turvatoimenpiteet toteutetaan osana laitteiston turvamoduulia (HSM). Tarkoituksen täyttävissä tuotteissa käytettyjen turvamekanismien on oltava läpinäkyviä, ja niiden on oltava parhaiden laatua ja turvallisuutta koskevien standardien mukaisia. Turvallisuussertifiointi toimii lisätodisteena ja on hyvä toimintatapa laitteiston turvamoduulin laadun arvioinnissa. Sertifiointi voidaan tehdä esimerkiksi Criteria Recognition Arrangement (CCRA) -järjestelyn, Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOGIS-MRA) -sopimuksen ja/tai FIPS-140-normin mukaisesti. Tuotteet hankitaan luotetuilta myyjiltä ja alkuperäketjusta huolehditaan tuotteen valmistuksesta aina turvamoduulin tuotantokäyttöön ottamiseen saakka.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohtien A.10 "Cryptography" ja A.11 "Physical and environmental security" mukaisia turvatoimenpiteitä

5.2.3 Tietoturvallisuuden hallinta, säännökset

TunnL 8 § (29.6.2016/533) Sähköisen tunnistamisen järjestelmälle asetettavat vaatimukset

Sähköisen tunnistamisen järjestelmän on täytettävä seuraavat vaatimukset:

…

5) tietoturvallisuuden hallinnasta on huolehdittu siten, että sähköisen tunnistamisen varmuustasoasetuksen liitteen kohdan 2.4 johdanto-osassa ja kohdissa 2.4.3 ja 2.4.7 vähintään korotetulle varmuustasolle säädetyt edellytykset täyttyvät.

LOA 2.4 Hallinto ja organisointi

Kaikilla osallistujilla, jotka tarjoavat sähköiseen tunnistamiseen liittyvää rajat ylittävää palvelua (jäljempänä tässä liitteessä ”palveluntarjoajat”), on oltava käytössä dokumentoidut tietoturvallisuuden hallintakäytännöt, toimintaperiaatteet, lähestymistavat riskien hallintaan ja muut hyväksytyt turvatoimenpiteet siten, että asiaankuuluvilla sähköisen tunnistamisen järjestelmien hallintoelimillä on kyseeseen tulevissa jäsenvaltioissa varmuus siitä, että tehokkaat menettelyt ovat käytössä. Kaikki 2.4 jakson vaatimukset/osatekijät on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.

LOA 2.4.3 Tietoturvallisuuden hallinta

MATALA

Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.

KOROTETTU

Taso ”matala” lisättynä seuraavalla:

Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.

KORKEA

Sama kuin tasolla ”korotettu”.

2.4.7 Noudattaminen ja tarkastus

MATALA

Määräajoin tehdään sisäisiä tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

KOROTETTU

Määräajoin tehdään riippumattomia sisäisiä tai ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

KORKEA

1. Määräajoin tehdään riippumattomia ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

2. Jos järjestelmää hallinnoi suoraan julkinen elin, tarkastukset tehdään kansallisen lainsäädännön mukaisesti.

5.2.4 LOA Guidance, tietoturvallisuuden hallinta

Liite

1. sovellettavat määritelmät

4) 'tietoturvallisuuden hallintajärjestelmällä' tarkoitetaan prosesseja ja menettelyjä, joiden tarkoituksena on pitää tietoturvallisuuteen liittyvät riskit hyväksyttävällä tasolla.

2.4 Hallinto ja organisointi

Kaikilla osallistujilla, jotka tarjoavat sähköiseen tunnistamiseen liittyvää rajat ylittävää palvelua (jäljempänä tässä liitteessä "palveluntarjoajat"), on oltava käytössä dokumentoidut tietoturvallisuuden hallintakäytännöt, toimintaperiaatteet, lähestymistavat riskien hallintaan ja muut hyväksytyt turvatoimenpiteet siten, että asiaankuuluvilla sähköisen tunnistamisen järjestelmien hallintoelimillä on kyseeseen tulevissa jäsenvaltioissa varmuus siitä, että tehokkaat menettelyt ovat käytössä. Kaikki 2.4 jakson vaatimukset/osatekijät on ymmärrettävä suhteutettuina riskeihin kulloisellakin tasolla.

OHJE:

Kaikkiin osallistujiin kuuluvat rajat ylittävän todentamisprosessin osapuolet, mukaan lukien tunnistustietojen tarjoaja ja jäsenvaltion käyttämät validointipalvelut (jos sellaisia on), mutta eivät käytetyt luotettavat lähteet.

Riskienhallinnassa yleisenä periaatteena on, että organisaation on itsensä valittava, minkä tasoista riskiä se pitää hyväksyttävänä. Kohdan 2.4 vaatimuksella muutetaan tätä yleistä periaatetta, sillä sen mukaan organisaation turvatoimenpiteiden on oltava suhteutettuja riskeihin kulloisellakin tasolla.

Suuri(n) osa tämän kohdan vaatimuksista täyttyy, jos

☐ käytössä on standardin ISO/IEC 27001:2013 mukainen auditoitu tietoturvallisuuden hallintajärjestelmä, tai

☐ operatiivisten palveluiden tuottajat ovat eIDAS-asetuksen mukaisia hyväksyttyjä luottamuspalveluiden tarjoajia.

Tämä ei kuitenkaan estä hyödyntämästä muita normeja, esimerkiksi soveltuvia kansallisia järjestelmiä, jotka täyttävät tämän kohdan vaatimukset.

Selvitys standardin ISO/IEC 27001:2013 vaatimuksista sekä hyväksyttyjä luottamuspalveluiden tarjoajia koskevista vaatimuksista annetaan vaatimusten soveltamista koskevien ohjeiden mukana [päätetään myöhemmin]./ A mapping of the requirements to ISO/IEC 27001:2013 and the requirements for qTSPs is provided as part of the guidance of the requirements [TBD]. Standardin ISO/IEC 27001:2013 mukaista tietoturvallisuuden hallintajärjestelmää käytettäessä kyseisen standardin turvatoimenpiteet kattavat kaikki kohtien 2.4.4–2.4.6 vaatimukset.

2.4.3 Tietoturvallisuuden hallinta

MATALA

Käytössä on tehokas tietoturvallisuuden hallintajärjestelmä tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.

OHJE:

Tietoturvaan kohdistuvien riskien hallinta koskee kaikkia sähköisen tunnistamisen järjestelmän osa-alueita. Toimivassa tietoturvallisuuden hallintajärjestelmässä otetaan huomioon järjestelmän kaikkiin osa-alueisiin kohdistuvat riskit.

Sähköisen tunnistamisen järjestelmän organisaatiorakenteen perusteella voi olla tarpeen käyttää useita tietoturvallisuuden hallintajärjestelmiä eri komponenteista vastaaville toimijoille.

KOROTETTU

Taso "matala" lisättynä seuraavalla:

Tietoturvallisuuden hallintajärjestelmässä noudatetaan vakiintuneita standardeja tietoturvaan liittyviä riskien hallintaa ja valvontaa varten.

OHJE:

Standardi ISO/IEC 27001:2013 on tunnettu ja toimivaksi osoittautunut tietoturvaan kohdistuvien riskien hallintaa koskeva normi. Katso myös kohta 2.4.7, jossa käsitellään toimintaperiaatteiden noudattamisesta huolehtimista.

KOROTETTU

Määräajoin tehdään riippumattomia sisäisiä tai ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

OHJE:

Tarkastus, joka hoidetaan sisäisesti organisaation omien normien mukaisesti ja jonka tulokset ilmoitetaan ensisijaisesti organisaation omalle johdolle, on hyväksyttyjen määritelmien mukaisesti sisäinen tarkastus (silloinkin, kun mukana on ulkopuolelta hankittua osaamista). Sisäisen tarkastuksen tekee objektiivisesti riippumaton tarkastustoiminto, ja se voi toimia pohjana organisaation itsensä antamalle vakuutukselle siitä, että sovellettavia määräyksiä on noudatettu. Tarkastus olisi tehtävä siten, että tarkastettavan toiminnon esimiehet eivät osallistu siihen, jotta tulosten vääristymiseltä ja eturistiriidoilta vältytään.

Ulkopuolisella (kolmannen osapuolen suorittamalla) tarkastuksella tarkoitetaan tarkastuksia, jotka tekee riippumaton tarkastusorganisaatio, kuten sääntelyviranomainen tai sertifiointitaho. Tavoitteena on arvioida tarkastettavaa organisaatiota suhteessa tiettyihin periaatteisiin ja kriteereihin ja antaa lausunto siitä, onko johdon vakuutus kyseisten periaatteiden täyttymisestä perusteltu. Ulkopuolisessa tarkastuksessa tarvitaan yleensä tarkastusstandardia, joka voi olla esimerkiksi auditointistandardi SFS-ISO/IEC 27007 tai AICPAn/CICAn kehittämä SysTrust/WebTrust-standardi.

Standardissa SFS-EN ISO 19011 on johtamisjärjestelmien auditointia koskevia ohjeita, mukaan lukien sisäisen ja ulkopuolisen tarkastuksen periaatteet sekä ohjeita siitä, miten tarkastusprosessiin osallistuvien henkilöiden osaamista voidaan arvioida.

KORKEA

1. Määräajoin tehdään riippumattomia ulkoisia tarkastuksia, jotka kattavat kaikki palvelujen tarjonnan kannalta merkitykselliset toimintalohkot, jotta voidaan varmistaa sovellettavien toimintaperiaatteiden noudattaminen.

OHJE:

Tämä vaatimus voidaan täyttää standardin SFS-ISO/IEC 27007 mukaisella auditoinnilla tai todentamisella.

2. Jos järjestelmää hallinnoi suoraan julkinen elin, tarkastukset tehdään kansallisen lainsäädännön mukaisesti.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

4) tietoturvallisuuden resursointi, pätevyys, henkilöstön tietoisuus tietoturvallisuudesta, viestintä ja dokumentointi sekä dokumentoidun tiedon hallinta;

2.4.5 Tilat ja henkilökunta

MATALA

1. Käytössä on menettelyt, joilla varmistetaan, että henkilöstöllä ja alihankkijoilla on riittävä koulutus, pätevyys ja kokemus taidoissa, joita he tarvitsevat suorittaakseen tehtävänsä.

OHJE:

Jos henkilöstöltä edellytetään todistettua osaamista, on käytössä oltava koulutusohjelma, jolla varmistetaan, että henkilöstö pystyy osoittamaan taitonsa ja ylläpitämään niitä.

Esimerkkejä: Fyysisiä asiakirjoja (esimerkiksi passeja ja henkilökortteja) tarkastavaa henkilöstöä koskevien hyvien toimintatapojen mukaisia vaatimuksia voivat olla esimerkiksi seuraavat:

Matala
☐ Tiedostaa, että asiakirjapetoksia tapahtuu.
☐ Kykenee täsmällisesti ja johdonmukaisesti tarkistamaan, onko asiakirjoissa poikkeavuuksia, kuten kirjoitusvirheitä, erilaisia kirjasintyyppejä, puuttuvia sivuja tai epäjohdonmukaisuuksia asiakirjan asettelussa ja kohdentamisessa.
Korotettu
☐ On saanut asiakirjaväärennösten havaitsemista koskevaa koulutusta, jossa on hyödynnetty kansallisesti tunnustettuja, laadukkaita koulutusmateriaaleja.
☐ Kykenee tunnistamaan muutetut asiakirjat/laminointipinnan.
☐ Kykenee tunnistamaan yleisimmät painotekniikat.

Suuri [p.o. korkea]
☐ Tuntee hyvin käytännön tasolla asiakirjojen mallit ja niiden turvaominaisuudet.
☐ On asianmukaisen koulutuksen kautta oppinut tuntemaan erilaiset vesileimat, turvakuidut ja painotekniikat.
☐ Kykenee asiakirjojen tarkastelun perusteella tunnistamaan väärennetyt ja tekaistut asiakirjat.
☐ Kykenee käyttämään tehokkaasti viitemateriaaleja.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.7 ”Human resource security” (vertaa etenkin kohta A.7.2.2) mukaisia turvatoimenpiteitä.

M72 5 §

LOA Guidance todentamismekanismin 2.3.1 soveltamisohje (ote)

…

Varmuustasossa eri vakavuusasteista käytettävät termit ovat ”korkeampi perustaso” (enhanced-basic), ”kohtuullinen” (moderate) ja ”korkea” (high). Nämä termit on lainattu standardeista ISO/IEC 15408 ”Information technology – Security techniques – Evaluation criteria

for IT security" ja ISO/IEC 18045 "Information technology – Security techniques – Methodology for IT security evaluation". Standardien teksti on vapaasti luettavissa osoitteessa www.commoncriteriaportal.org/cc (CCPART1-3 vastaa standardia ISO/IEC 15408 ja CEM standardia ISO/IEC 18045).

Standardissa ISO/IEC 15408-1 hyökkäyksen vakavuusaste määritellään sen työn määräksi, jota [mekanismia] vastaan hyökkääminen edellyttää, ilmaistuna hyökkääjän asiantuntemuksena, resursseina ja motivaationa.

Standardin ISO/IEC 18045 / CEM:n liitteessä B.4 ohjeistetaan, miten lasketaan todentamismekanismin tietyn heikkouden hyväksikäyttämisen edellyttämä hyökkäyksen vakavuusaste.

Täytäntöönpanoasetuksessa säädettyjen vaatimusten täyttäminen edellyttää mahdollisten hyökkäysten sietokyvyn arviointia.

Arvioinnissa olisi otettava huomioon asiaankuuluvat uhat. Standardissa ISO 29115 mainitaan esimerkiksi seuraavat: verkossa ja verkon ulkopuolella tapahtuva arvaaminen, tunnistetietojen toisintaminen, tietojen kalastelu, salakuuntelu, replay-hyökkäys, istuntokaappaus, mies välissä -hyökkäys, tunnistetietojen varastaminen, spoofing-hyökkäys ja toisena esiintyminen.

Tietojen säilyttäminen

2.3.1 todentamismekanismi

MATALA

2. Jos henkilön tunnistetiedot tallennetaan osana todentamismekanismia, nämä tiedot on suojattu niiden menetykseltä ja vaarantamiselta, mukaan lukien analyysi verkkoympäristön ulkopuolella.

OHJE:

Tallennettuihin henkilötietoihin pääsyä on valvottava huolellisesti. Henkilön tunnistetietojen suojaamisessa käytettäviä menetelmiä ovat esimerkiksi Euroopan unionin verkko- ja tietoturvaviraston ENISAn "Algorithms, Key Sizes and Parameters Report" -asiakirjan, kansallisten salausohjeiden tai muiden hyvien toimintatapojen mukainen salaaminen ja tiivistäminen.

Käyttöoikeuksia on aina valvottava

2.4.4 Tietojen säilyttäminen

MATALA

1. Asiaankuuluvat tiedot kirjataan ja säilytetään käyttämällä tehokasta tiedonhallintajärjestelmää ottaen huomioon sovellettava lainsäädäntö ja tietosuojaan ja tietojen säilyttämiseen liittyvät hyvät käytännöt.

OHJE:

Jos tietoja säilytetään, on tiedonhallintajärjestelmällä varmistettava, että tietojen eheys ja luottamuksellisuus säilyvät läpi niiden koko käyttöajan.

Standardin ISO/IEC 27001:2013 mukaisessa tietoturvallisuuden hallintajärjestelmässä tämä vaatimus huomioidaan osana kohdan A.12 "Operational security" (etenkin kohdan A.12.4 "Logging and monitoring") sekä kohdan A.18 "Compliance" mukaisia turvatoimenpiteitä

Varmuustaso

2.3.1 todentamismekanismi

KOROTETTU

2. Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on kohtuullinen ("moderate"), voi heikentää todentamismekanismeja.

OHJE:

Tässä kohdassa ei anneta erityisiä ohjeita.

KORKEA

Taso "korotettu" lisättynä seuraavalla:

Todentamismekanismissa toteutetaan turvatoimenpiteitä sähköisen tunnistamisen menetelmän varmentamiseksi siten, että on erittäin epätodennäköistä, että viestin arvaaminen, salakuuntelu, toisto tai manipulointi hyökkäyksessä, jonka vakavuusaste on korkea ("high"), voi heikentää todentamismekanismeja.

OHJE:

Jos todentamismekanismin suojaamisessa käytetään salausta, on valittava vahvat salausprotokollat ja pituudeltaan riittävät avaimet.

Tärkeitä menetelmiä salausprotokollan vahvuuden varmistamisessa ovat salausanalyysit, kuten salauksen turvallisuutta koskevat todisteet.

Kun tiedossa on, että jokin protokolla ei ole turvallinen (esimerkiksi SSLv3), tämä on otettava huomioon; sama koskee tiettyihin salausprotokolliin kohdistuneita tunnettuja hyökkäyksiä sekä toimenpiteitä, joita hyökkäyksiä vastaan on otettu käyttöön, jos näitä protokollia käytetään.

Kun todentamismekanismissa hyödynnetään salausratkaisua, on huomioon otettava paitsi salausprimitiivit, myös protokollat ja ympäristö, etenkin avainten hallinta.

Esimerkki: Tyypillinen avainten hallinnassa käytettävä mekanismi on julkisen avaimen infrastruktuurin (Public Key Infrastructure, PKI) käyttäminen. Varmenneviranomaisen toiminnan tietoturva vaikuttaa suoraan todentamismekanismin turvallisuuteen paitsi varmenneviranomaisen puhtaasti teknisen tietoturvan, myös organisatoristen näkökohtien osalta.

Jos sähköisen tunnistamisen järjestelmän tiettyjä osia koskevien varmenteiden myöntäjinä on useita luotettuja varmenneviranomaisia, on huomioon otettava kaikkien luotettujen varmenneviranomaisten yleinen tietoturvan taso.

Esimerkkinä viimeksi mainitusta on tilanne, jossa viestinnän alku- ja loppupisteiden tunnistamisessa käytetään internet-PKI:stä peräisin olevia varmenteita eli varmenteita, joiden myöntäneiden varmenneviranomaisten juurivarmenne on käyttäjän selaimen luotettujen varmenteiden luettelossa. Tässä tapauksessa on otettava huomioon kaikkien luotettujen varmenteiden luettelossa olevien varmenneviranomaisten tietoturva. Hyvien toimintatapojen mukaista yleensä on, että jos sähköisen tunnistamisen järjestelmän infrastruktuurissa käytetään internet-PKI:tä, silloin korkea varmuustaso edellyttää, että käyttäjälle suositellaan riittävien turvamekanismien käyttämistä.

Todentamisella olisi suojattava todentamistietoja sellaiselta manipuloinnilta, jonka tarkoitus on saada henkilö uskomaan, että todentaminen annetaan toiselle luottavalle osapuolelle.

5.3 Muu sääntely

…