Katakri 2015

Tietoturvallisuuden auditointityökalu viranomaisille

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

PL 31, 00131 HELSINKI

www.defmin.fi

Taitto: Tiina Takala/puolustusministeriö

ISBN: 978-951-25-2681-9 painettu
ISBN: 978-951-25-2682-6 pdf

Sisällysluettelo

1. Esipuhe **2**

2. Johdanto **3**

3. Osa-alue T: Turvallisuusjohtaminen **5**

Hallinnollinen turvallisuus 6

Henkilöstöturvallisuus 13

4. Osa-alue F: Fyysinen turvallisuus **16**

Tiloja ja laitteita koskevat vaatimukset 17

Luvattoman pääsyn estäminen 24

Suojaaminen salakatselulta ja salakuuntelulta 27

Toiminnan jatkuvuuden hallinta 28

5. Osa-alue I: Tekninen tietoturvallisuus **29**

Tietoliikenneturvallisuus 30

Tietojärjestelmäturvallisuus 36

Tietoaineistoturvallisuus 53

Käyttöturvallisuus 60

Liite I: Yritysturvallisuusselvitys 66

Liite II: Tietojärjestelmien arviointi 69

Katakrin uudistamistyötä on koordinoinut ohjausryhmä, johon kuuluvat:

Maarit Jalava, ulkoasiainneuvos, ulkoasiainministeriö (pj.)
Aku Hilve, tietoturvallisuusasiantuntija, valtiovarainministeriö (vpj.)
Kai Knape, puolustushallinnon apulaisturvallisuusjohtaja, puolustusministeriö
Laura Vilkkonen, yksikönpäällikkö, liikenne- ja viestintäministeriö
Richard Wunsch, komentajakapteeni, Pääesikunta
Tapio Aaltonen, tietohallintojohtaja, sisäministeriö
varajäsen **Samuli Bergström**, tietoturvapäällikkö, sisäministeriö
Juha Ilkka, tietoturvallisuuspäällikkö, valtioneuvoston kanslia
Rauli Paananen, apulaisjohtaja, Viestintävirasto
Lauri Holmström, tarkastaja, Suojelupoliisi
Aki Tauriainen, päällikkö, Viestintävirasto
Pekka Ylitalo, insinöörimajuri, Pääesikunta
Jyrki Hollmén, johtava asiantuntija, Elinkeinoelämän keskusliitto
(1.1.2015 alkaen asiantuntija **Mika Susi**)
Kari Santalahti, turvallisuuspäällikkö, Poliisihallitus
Mikko Viitasaari, turvallisuusjohtaja, UPM
Tuomas Hyvärinen, lakimies, ulkoasiainministeriö (siht.)
(1.8.2014 alkaen lakimies **Johanna Erkkilä**)
Kimmo Janhunen, erityisasiantuntija, valtiovarainministeriö (siht.)
(1.8.2014 alkaen eritysasiantuntija **Kirsi Janhunen**)

Tämän lisäksi Katakrin eri osa-alueita on valmisteltu erillisissä alatyöryhmissä. Katakri auditointityökalu on hyväksytty käyttöön NSA:n yhteistyöryhmässä 26.03.2015. Katakrista on pyritty tekemään paremmin aikaa kestävä, jotta vältetään usein toistuvat kokonaisuudistukset. Ajantasainen Katakri on saatavilla sähköisenä.

1. Esipuhe

Ensimmäinen Katakri eli kansallinen turvallisuusauditointikriteeristö valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Katakri valmisteltiin puolustusministeriön johdolla viranomaisten ja elinkeinoelämän yhteistyössä. Tämän jälkeen vastuu Katakrin jatkohallinnoinnista ja päivityksestä siirrettiin sisäministeriölle, jonka koordinoimana Katakrin ensimmäinen päivitysversio valmistui vuonna 2011.

Elokuussa 2012 sisäministeriö asetti neuvoa antavan työryhmän, jonka tehtävänä oli vuoden 2013 loppuun mennessä sekä Katakrin päivittäminen että Katakria koskevien vastuiden selvittäminen valtionhallinnossa. Katakrin päivittämistä ei kuitenkaan ollut mahdollista saattaa valmiiksi työryhmälle asetetun määräajan puitteissa. Työryhmän esityksestä keskeiset ministeriöt (VM, UM, LVM, SM, PLM, VNK) päättivät tammikuussa 2014, että päävastuu Katakrin ylläpidosta ja hallinnoinnista siirtyy ulkoministeriössä toimivalle Kansalliselle turvallisuusviranomaiselle (NSA).

Katakrin uudistamistyö ja hallinnointi on NSA:n yhteistyöryhmän alatyöryhmäksi perustetun ohjausryhmän vastuulla. Ohjausryhmässä ovat edustettuina toimivaltaisten viranomaistahojen lisäksi elinkeinoelämän edustajat. Lähtökohtana Katakrin uudistamisessa on ollut käytettävyyden lisääminen, skaalautuvuus, riskiperusteisuus, vaatimusten läpinäkyvyyden parantaminen sekä osittaisten auditointien mahdollistaminen. Koska uudistukset ovat mittavia ja ne ovat johtaneet Katakrin rakenteen muuttumiseen, ei enää voida puhua Katakrin päivitysversiosta. Katakri-nimi on kuitenkin käytössä jo niin vakiintunut ja tunnettu että se on päätetty säilyttää jatkossakin tämän viranomaisten auditointityökalun nimenä.

2. Johdanto

Katakri on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata *viranomaisen salassa pidettävää tietoa*. Katakriin on koottu kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset. Katakri itsessään ei aseta tietoturvallisuudelle ehdottomia vaatimuksia, vaan siihen kootut vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Keskeisin kansalliseen lainsäädäntöön perustuva vaatimuslähde on valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), jäljempänä tietoturvallisuusasetus, jota noudatetaan Suomessa niin kansallisen kuin kansainvälisenkin salassa pidettävän tiedon suojaamisessa. Kansainvälisenä lähteenä on käytetty EU:n neuvoston turvallisuussääntöjä (2013/488/EU), jotka sisältävät EU:n turvallisuusluokitellun tiedon suojaamista koskevat vähimmäisvaatimukset ja perusperiaatteet. Katakrissa esitettyjen vaatimusten yhteyteen on merkitty lähdeviittaus läpinäkyvyyden varmistamiseksi.

Katakrin rakenne

Katakriin kirjatut vaatimukset on jaettu kolmeen osa-alueeseen. Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on riittävät turvallisuusjohtamisen valmiudet sekä kyvykkyys. Turvallisuusjohtamisen osa-alueessa on kuvattu perustaso, jonka vaatimukset kohdeorganisaation tulee täyttää. Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan salassa pidettävien tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Organisaation tilat voidaan salassa pidettävien tietojen käsittely- ja säilyttämistarpeen perusteella jakaa kolmeen alueeseen: hallinnollinen alue, turva-alue ja tekninen turva-alue. Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset. Tämä osa-alue jakautuu kolmeen käsiteltävän tiedon mukaiseen suojaustasoon (ST IV, ST III, ST II).

Vaatimukset on kuvattu niin, että ne mahdollistavat erilaisia toteutustapoja. Vaatimusten yhteydessä oleviin lisätietokenttiin on kirjattu toteutustavoista esimerkkejä, jotka eivät kuitenkaan ole sitovia. Niissä kuvataan suosituksia ja parhaita käytäntöjä, joita löytyy muun muassa VAHTI-ohjeista ja EU:n turvallisuussääntöjä täydentävistä suuntaviivoista ja ohjeasiakirjoista. Lisätietokenttiä voidaan täydentää auditointiprosessien yhteydessä.

Katakrin käyttö

Katakria voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Sitä voidaan käyttää myös apuna yrityksien, yhteisöjen sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä.
Katakrin käytöllä pyritään varmistamaan, että kohdeorganisaatiolla on riittävät turvallisuusjärjestelyt viranomaisen salassa pidettävien tietojen oikeudettoman paljastumisen ehkäisemiseksi kaikissa niissä ympäristöissä, joissa tietoja käsitellään. Tavoitteena on lisäksi varmistaa turvallisuusvaatimusten huomioon ottaminen turvallisuuden hallinnassa.

Turvallisuusjärjestelyjen suunnittelun ja toteutuksen avulla pyritään varmistamaan uhkiin nähden hyväksyttävä turvallisuustaso. Kohdeorganisaation tulee pystyä osoittamaan turvallisuusjärjestelyjen riittävyys luotettavasti. Turvallisuusjärjestelyjen riittävyyden arvioinnin tulee pohjautua järjestelmälliseen riskienarviointiin. Turvallisuusriskien hallinnalla on pyrittävä toteuttamaan turvatoimien yhdistelmä, jolla saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä.

Katakrin avulla arvioidaan kohdeorganisaation yleistä kykyä suojata viranomainen salassa pidettävää tietoa. Näin ollen Katakrin avulla tehtyä yritysturvallisuusselvitystä voidaan käyttää niin kotimaisissa kuin kansainvälisissäkin hankkeissa.

Vaikka Katakrissa kuvatut EU:n neuvoston turvallisuussääntöjen vaatimukset koskevat vain EU:n turvallisuusluokiteltujen tietojen suojaamista, ne edustavat EU:n jäsenvaltioiden yhteisesti hyväksymiä ja käyttämiä salassa pidettävän tiedon suojaamista koskevia perusperiaatteita ja vähimmäisvaatimuksia Euroopassa ja luovat sen vuoksi hyvän perustan salassa pidettävien tietojen suojaamiseksi myös Suomessa. Jäsenvaltiot noudattavat EU:n turvallisuussääntöjä kansallisen lainsäädäntönsä mukaisesti, joten Suomessa EU:n salassa pidettävien tietojen suojaamisessa noudatetaan EU:n vaatimusten lisäksi tietoturvallisuusasetusta. Tietoturvallisuusasetuksen ja EU:n neuvoston turvallisuussääntöjen vaatimukset eivät merkittäviltä osin poikkea toisistaan. Mikäli Katakriin kirjattu vaatimus koskee pelkästään EU:n salassa pidettävää tietoa, se ilmenee lähdeviitteistä.

Katakrin osa-alueet on laadittu erillisiksi kokonaisuuksiksi, joten osa-alueita voidaan käyttää myös erikseen. Esimerkkinä on osittainen yritysturvallisuusselvitys, joka voidaan tehdä yrityksen toiminnan muuttuessa tai silloin kun auditointi kohdistuu rajattuun osa-alueeseen. Organisaation tulee kuitenkin täyttää T-osion vaatimukset osittaisenkin yritysturvallisuusselvityksen yhteydessä.

Katakria ei ole tarkoitettu käytettäväksi sellaisenaan julkisen hankinnan turvallisuusvaatimuksena. Julkisessa hankinnassa tarkat turvallisuusvaatimukset tulisi määrittää erikseen ottaen huomioon hankintaa koskevat riskit ja erityistarpeet. Yksittäiseen hankkeeseen voi sisältyä muitakin kuin Katakriin koottuja salassa pidettävän tiedon käsittelyä ja suojaamista koskevia vaatimuksia. Näiden vaatimusten toteutumista ei arvioida Katakrin avulla, vaan kohdeorganisaatio sitoutuu noudattamaan niitä sopimusperusteisesti.

3. osa-alue T

TURVALLISUUS-JOHTAMINEN

Turvallisuusjohtamisen osa-alueessa käsitellään niitä menetelmiä, joilla turvallisuus ja sen hallinta jalkautetaan osaksi koko organisaation toimintaa. Turvallisuusjohtamisen osa-alue kattaa hallinnollisen turvallisuuden ja henkilöstöturvallisuuden. Turvallisuusjohtamisen vaatimuksilla pyritään siihen, että organisaatiolla on toimiva turvallisuuden hallintajärjestelmä sekä riittävät menettelyt sen varmistamiseksi, että viranomaisen salassa pidettäviä tietoja käsittelevä henkilöstö toimii asianmukaisesti.

Lisätietokenttään on tulkinnan tueksi koottu toteutusesimerkkejä, joissa kuvatuilla menettelyillä voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojausten vähimmäistaso. Toteutusesimerkit voivat olla korvattavissa myös muilla vastaavan tasoisilla suojauksilla. Vaatimuksissa tai toteutusesimerkeissä ei kuvata kaikkiin ympäristöihin tai erikoistapauksiin riittäviä suojauksia.

Turvallisuusjohtamiseen liittyviä prosesseja tulee käsitellä kokonaisuuksina. Turvallisuuden hallintamenettelyt tulee suhteuttaa riskienarvioinnin perusteella suojattavaan tietoon ja kohdeorganisaation toimintaan.

Turvallisuusjohtamisen osa-alueen tarkoituksenmukainen käyttö edellyttää arvioinnin kohdentamista siihen osaan organisaatiosta, jolla on suora tai epäsuora vaikutus salassa pidettävän tiedon käsittelyyn. Tarkoituksenmukaisena kohdentamisena voi olla tietojenkäsittely-ympäristöä hallinnoiva organisaation osa, esimerkiksi tytäryhtiö tai vastaava. Erityisesti henkilöstöturvallisuuden vaatimusten arvioinnissa tulee huomioida, että riittävä toteutustapa voi vaihdella kohdekohtaisesti. Esimerkiksi suojaustason II käsittely-ympäristön henkilöstön ohjeistuksen sisältö eroaa yleensä merkittävästi koko organisaatiota koskevista yleisistä ohjeistuksista.

Toimivaltaisella viranomaisella tarkoitetaan sitä viranomaista, joka kyseisessä Katakrin käyttötapauksessa voi myöntää kohteelle hyväksynnän tai todistuksen.

Hallinnollinen turvallisuus

T 01

Turvallisuusjohtaminen

Turvallisuusperiaatteet

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan. 2) Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. 3) Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan ja niiden toteutumista seurataan säännöllisesti.	4 §, 6 §	9 artiklan 1 kohta

Lisätietoja

Yleistä

Organisaation turvallisuusperiaatteilla tavoitellaan sitä, että johto sitoutuu organisaation turvallisuustyöhön ja että turvallisuustyö tukee organisaation toimintaa. Turvallisuusperiaatteet viestitään henkilöstölle ja tarvittaville sidosryhmille. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana organisaation ohjeistokokonaisuutta.

Muita lisätietolähteitä

ISO/IEC 27002:2013 5.1.1; ISO/IEC 27001:2013 5.1; ISO/IEC 27001:2013 5.2; ISO/IEC 27001:2013 5.3; ISO/IEC 27001:2013 9.3; VAHTI 2/2010

T 02

Turvallisuusjohtaminen

Turvallisuustyön tehtävien ja vastuiden määrittäminen

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Organisaatio on määritellyt turvallisuuden hoitamisen tehtävät ja vastuut.	5 §:n 1 mom. 3 kohta	7 artiklan 5 kohta

Lisätietoja

Toteutusesimerkki

1) Organisaatio on määritellyt turvallisuuden hoitamisen tehtävät ja vastuut ainakin seuraavilta osin:
   a) turvallisuuden hallinta
   b) henkilöstöturvallisuus
   c) fyysinen turvallisuus
   d) tietotekninen turvallisuus
2) Vastuumäärittely sisältää salassa pidettävän tiedon käyttöympäristön omistajan sekä turvallisuuteen liittyvät vastuut.
3) Turvallisuusdokumentaation kattavuuden ja ajantasaisuuden säännöllinen seuranta on vastuutettu. Turvallisuusdokumentaatio kattaa salassa pidettävään tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta, ja se on tarvittavien tahojen saatavilla.

Yleistä

Turvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa.

Muita lisätietolähteitä

ISO/IEC 27002:2013 6.1.1; ISO/IEC 27001:2013 5.1; ISO/IEC 27001:2013 5.2; ISO/IEC 27001:2013 5.3; VAHTI 2/2010

T 03

Turvallisuusjohtaminen

Turvallisuustyön resurssit

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Organisaatiolla on käytössään riittävä asiantuntemus tietoturvallisuuden varmistamiseksi.	5 §:n 1 mom. 2 kohta	IV liitteen 4 kohta

Lisätietoja

Riittävällä asiantuntemuksella pyritään varmistamaan, että tietoturvallisuustyön tarkoitus toteutuu ja toimet mitoitetaan kustannustehokkaasti. Resurssien riittävyyttä arvioidaan säännöllisesti.

Muita lisätietolähteitä

ISO/IEC 27001:2013 7.1; ISO/IEC 27001:2013 7.2; ISO/IEC 27001:2013 5.1; VAHTI 2/2010

T 04

Turvallisuusjohtaminen

Turvallisuusriskien hallinta

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Organisaatiolla on käytössä riskienhallintaprosessi. Riskienhallinnan on oltava säännöllinen ja jatkuva, dokumentoitu prosessi. 2) Riskien analysoinnissa on käytettävä vakiintunutta, avointa ja ymmärrettävää järjestelmällistä menetelmää. 3) Riskienhallintaan osallistuvat tarvittavat tahot organisaation sisältä ja ulkopuolelta. 4) Riskienhallinnan on katettava vähintään turvallisuusjohtamisen, tila- ja tietoturvallisuuden osa-alueet. Tunnistetut riskit on otettava huomioon tarvittavien sidosryhmien osalta. Organisaation tulee varmistaa, että salassa pidettäviä tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. 5) Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation turvallisuustavoitteiden asettamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa, turvatoimien suunnittelussa, muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä. 6) Turvatoimet on mitoitettu ottaen huomioon muun muassa tiedon suojaustaso, määrä, muoto, luokittelu-peruste ja sijoitustilat suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan. 7) Organisaatio dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet.	1) 4 §, 5 §, 6 § 2) 3) 4 §, 5 §, 6 § 4) 4 §, 5 §, 6 § 5) 4 §, 5 §, 6 § 6) 4 §, 5 §, 6 § 7) 4 §, 5 §, 6 §	1) 5 artikla, IV liitteen 4 kohta 2) IV liitteen 4 kohta 3) IV liitteen 4 kohta 4) IV liitteen 4 kohta 5) IV liitteen 4 kohta 6) 5 artikla, IV liitteen 4-7 kohdat 7) 5 artiklan 2 kohta 8) IV liitteen 12 kohta

Lisätietoja

Toteutusesimerkkejä

1) Riskienhallinnan periaatteet on kuvattu.
2) Suojattavat kohteet on tunnistettu.
3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö.
4) Suojattaviin kohteisiin liittyvät riskit on tunnistettu ja arvioitu.
5) Suojausmenetelmät on suhteutettu tunnistettuihin riskeihin.
6) Riskienhallintaan ja analysointiin käytetään jotain järjestelmällistä menetelmää.
7) Organisaatiossa ylläpidetään kuvausta turvallisuusjärjestelyistä. Riskienhallintaprosessin johtopäätökset on huomioitu organisaation turvallisuusdokumentaatiossa.

Yleistä

Riskienhallinta on organisaation johdon ja muun henkilöstön toteuttama organisaation johtamiseen ja toimintaan sisältyvä prosessi, jota sovelletaan riittäväksi katsottavissa määrin kaikessa organisaation toiminnassa (esimerkiksi prosessit, asiakassuhteet). Riskienhallinnan tavoitteena on tunnistaa ja hallita organisaation toimintaedellytyksiä mahdollisesti vaarantavia tekijöitä ja pitää toimintaan kohdistuvat riskit sellaisissa rajoissa, etteivät organisaation toiminta ja tavoitteet ole uhattuna.

Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.

T 04

Riskienhallinta on epäedullisten ja haitallisten tapahtumien välttämistä (vaikutetaan tapahtuman todennäköisyyteen) tai tapahtumien seurausten pienentämistä (vaikutetaan seurauksen suuruuteen). Riskienhallinta on myös potentiaalisten mahdollisuuksien tunnistamista, analysointia ja hyödyntämistä. Kaikki nämä toiminnat tähtäävät organisaatioiden tavoitteiden saavuttamiseen.

Riskienhallinnan kohdentaminen viranomaisen salassa pidettävien tietojen näkökulmasta

Riskienhallintatoimet tulee kohdentaa siihen ympäristöön, jossa salassa pidettäviä tietoja on tarkoitus käsitellä. Tietojenkäsittely-ympäristöön sisältyy yleensä sekä henkilöstöön, toimitiloihin että tietojärjestelmiin liittyviä kokonaisuuksia.

Monitasoisen suojaamisen huomiointi riskienhallinnassa

Riskienhallinnassa tulee huomioida turvallisuusjärjestelyjen monitasoisuus (defence in depth). Riskienarvioinnissa tulee huomioida, että täydellistä suojausta ei pystytä toteuttamaan millään turvallisuusjärjestelyillä. Yksittäisiin riskeihin nähden riittävän suojauksen voi toteuttaa yksittäisillä luotettavilla turvatoimilla, tai useampia turvatoimia yhdistelemällä. Esimerkiksi rakenteellisen turvallisuuden vaikuttavuutta voidaan parantaa teknisten turvallisuusjärjestelmien käytöllä, ja siten saavuttaa riskeihin nähden riittävä turvallisuusjärjestelyjen yhdistelmä.

Riskien hallinnan ja analysoinnin menetelmiä

Riskienhallintaan ja analysointiin on olemassa useita eri menetelmiä, joilla kullakin on omat vahvuutensa ja heikkoutensa. Useissa järjestelmällisissä menetelmissä toiminta perustuu uhkien ja haavoittuvuuksien tunnistamiseen, todennäköisyyksien ja vaikuttavuuden arviointiin, tarvittavien riskejä pienentävien toimenpiteiden määritykseen, jäännösriskien arviointiin sekä korjaavien toimien seurantaan.

Riskienhallinta toimivaltaisen viranomaisen hyväksyntää edellyttävissä tilanteissa

Organisaation turvallista toimintaa uhkaavien riskien hallinta on perustana turvallisuusjärjestelyjen oikealle mitoitukselle. Toimivaltainen viranomainen suhteuttaa vaatimuksensa lähtökohtaisesti siihen uhkaympäristöön ja niihin turvatoimiin (kontrolleihin), jotka organisaatio esittää. Toimivaltaisen viranomaisen käsitys uhkista saattaa kuitenkin poiketa siitä, mihin organisaatio on omista lähtökohdistaan päätynyt.

Tilanteissa, joissa organisaation tavoitteena on saada viranomaisen myöntämä hyväksyntä tai todistus, organisaation on huomioitava jo riskienhallintaprosessissa ennen toteutusmallin laadintaa toimivaltaisen viranomaisen määrittämät uhkatekijät tai arvio turvallisuusjärjestelyjen riittävyydestä. Organisaation tulee pystyä riskienhallintaprosessinsa kautta osoittamaan toimivaltaiselle viranomaiselle perusteensa valituille turvatoimille ja niiden riittävyydelle. Yritystä suositellaan keskustelemaan riskiensä määrittelystä ja turvatoimisuunnitelmistaan toimivaltaisen viranomaisen kanssa jo varhaisessa vaiheessa, jotta sekä organisaation että toimivaltaisen viranomaisen arviot kyseisen ympäristön riskeistä pystytään huomioimaan jo turvatoimia suunniteltaessa. Toimivaltaisen viranomaisen arvioimilla uhkatekijöillä voi olla vähimmäisvaatimuksista poikkeava korottava vaikutus suojausvaatimuksiin.

T 04

Toimivaltaisen viranomaisen arvio uhkatekijöistä

Arvioissaan toimivaltainen viranomainen ottaa huomioon muun muassa tiedon luokitteluperusteen, suojaustason, käsittelymuodon ja merkittävyyden sekä arvion siitä, onko tieto kiinnostavaa valtiollisille toimijoille tai rikollisille toimijoille. Toimivaltainen viranomainen hyväksyy organisaation valitsemat turvatoimet ja toteutusmallit arvionsa perusteella.

Muita lisätietolähteitä

ISO/IEC 27001:2013 6.1.2; ISO/IEC 27001:2013 6.1.3; ISO/IEC 27001:2013 6.2; ISO/IEC 27001:2013 8.2; ISO/IEC 27001:2013 8.3; ISO/IEC 27001:2013 9.1; ISO/IEC 27001:2013 9.3; ISO/IEC 27001:2013 10.1; ISO/IEC 27002:2013 8.1.1; ISO/IEC 27002:2013 8.1.2; ISO/IEC 27002:2013 18.1.1; ISO/IEC 27002:2013 18.2.2; ISO/IEC 27002:2013 18.2.1; ISO/IEC 27005:2011; ISO 31000:2009; OCTAVE Allegro; SRHY-riskienhallinta; VTT - Riskianalyysimenetelmät; VAHTI 2/2010.

T 05

Turvallisuusjohtaminen

Jatkuvuuden hallinta

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1. Toipuminen ja jatkuvuuden varmistaminen toimintavaatimuksiin nähden riittävässä ajassa on huomioitu suunnittelussa. 2. Toiminnan jatkuvuussuunnitelmiin on sisällytettävä ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset salassa pidettävien tietojen käsittelyyn ja säilyttämiseen. 3. Poikkeamista tehdyt havainnot tuodaan osaksi riskienarviointia ja tarpeen mukaan näiden pohjalta päivitetään toipumis- ja jatkuvuussuunnitelmia. 4. Jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa, jotta estetään luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai käytettävyyden menettäminen.	1) 5 §:n 1 mom. 4 kohta 4 § 2) 5 §:n 1 mom. 4 kohta, 4 § 3) 5 §:n 1 mom. 4 kohta, 4 § 4) 5 §:n 1 mom. 4 kohta, 4 §	1) 5 artiklan 4 kohta 2) 5 artiklan 4 kohta 3) 4) 5 artiklan 3 kohta

Lisätietoja

Yleistä

Organisaatiossa on tunnistettu riippuvuudet ulkoisista tekijöistä, ja niiden vaikutuksista omaan toimintaan. Organisaatiossa on tunnistettu oman toiminnan vaikutus muihin.

Muita lisätietolähteitä

ISO/IEC 27002:2013 17.1.1; ISO/IEC 27002:2013 17.1.2; ISO/IEC 27002:2013 17.2.1; ISO/IEC 27002:2013 12.3.1; ISO/IEC 27002:2013 16.1.2; ISO/IEC 27002:2013 16.1.6; VAHTI 2/2009; VAHTI 2/2010

T 06

Turvallisuusjohtaminen

Turvallisuuspoikkeamien hallinta

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Organisaatiolla on menettelytavat turvallisuuspoikkeamien asianmukaiseen käsittelyyn. 2) Organisaatio on määrittänyt henkilöt/tahot, joille turvallisuuspoikkeamista tai niiden epäilyistä tulee ilmoittaa.	5 §:n 1 mom. 4 kohta	5 artiklan 4 kohta, 14 artiklan 3 kohta

Lisätietoja

Toteutusesimerkki

Turvallisuuspoikkeamien hallinta on
1) suunniteltu,
2) ohjeistettu/koulutettu,
3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla,
4) harjoiteltu, ja erityisesti
5) viestintäkäytännöt ja vastuut on sovittu.

Yleistä

Turvallisuuspoikkeamien hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa tilanteissa, minimoiden vahingot ja palauttaen tilanteen normaaliksi. Tehokas poikkeamienhallinta edellyttää myös riittävää resursointia.

Useat tiedon omistajat (esimerkiksi EU) sekä myös voimassa olevat viranomaishyväksynnät tai -todistukset edellyttävät välitöntä ilmoitusta salassa pidettävän tiedon vaarantaneista poikkeamista tai niiden epäilyistä.

Muita lisätietolähteitä

ISO/IEC 27002:2013 16.1.1; ISO/IEC 27002:2013 16.1.2; ISO/IEC 27002:2013 16.1.4; ISO/IEC 27002:2013 16.1.5; ISO/IEC 27002:2013 6.1.3; VAHTI 2/2010

T 07

Turvallisuusjohtaminen

Tietojen luokittelu

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tiedot on luokiteltu lakisääteisten vaatimusten perusteella: a) Tietosisällöltään salassa pidettävät aineistot ja asiakirjat (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä. b) Asiakirja merkitään asiakirjan osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä. c) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi asiakirjasta.	3 luku 8 §, 9 §	III liitteen 2, 6 ja 7 kohdat

Lisätietoja

Yleistä

Luokittelun tavoitteena on tunnistaa ja mitoittaa turvatoimet tiedon suojaustarpeen perusteella. Luokituksen voi ilmaista eri tavoin riippuen tietoaineistosta, käsittely-ympäristöstä ja käyttäjistä. Luokittelemalla tietojenkäsittely-ympäristöt tietoaineiston mukaisesti, pystytään selkeämmin osoittamaan ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät turvatoimet.

Muita lisätietolähteitä

ISO/IEC 27002:2013 8.2.1; ISO/IEC 27002:2013 8.2.2; VAHTI 2/2010

Henkilöstöturvallisuus

T 08	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Henkilöstöturvallisuus Työsuhteen elinkaaren huomioiminen	Organisaatiossa on käytössä turvallisuuden huomioon ottava menettely työsuhteen elinkaaren eri vaiheissa. Erityisesti tulee huomioida toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä.	5 §:n 1 mom. 8 kohta, 13 §	I liitteen 29 ja 31 kohdat
	Lisätietoja		
	Yleistä Turvallisuustekijät huomioon ottava menettely edellyttää tyypillisesti menettelyohjeita, jotka on koulutettu ja saatavilla tarvittavilla henkilöstöryhmillä. Menettelyohjeet voidaan jakaa esimerkiksi työsuhteen elinkaaren mukaisiin kokonaisuuksiin. Ohjekokonaisuuksia voivat olla esimerkiksi rekrytointiohjeet, perehdyttämisohjeet, työsuhteen aikaisten muutosten ohjeet, työsuhteen päättymisen ohjeet ja ohjeet yksityiskohtaisempiin toimiin kuten esimerkiksi ohjeet käyttö- ja pääsyoikeuksien muutoksiin. *Muita lisätietolähteitä* ISO/IEC 27002:2013 7.1; ISO/IEC 27002:2013 7.2; ISO/IEC 27002:2013 7.3; VAHTI 2/2008; VAHTI 2/2010		

T 09	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Henkilöstöturvallisuus Henkilöstön luotettavuuden arviointi	Salassa pidettävien aineistojen käsittelyyn liittyvien henkilöiden luotettavuus selvitetään tarvittaessa asianmukaisen tason turvallisuusselvitysmenettelyin.	5 §:n 1 mom. 8 kohta	I liitteen 2c, 2b ja 29 kohdat
	Lisätietoja		
	Yleistä EU:n ja Naton turvallisuusluokiteltujen tietojen käsittely edellyttää CONFIDENTIAL-tasosta lähtien henkilön luotettavuuden varmistamista turvallisuusselvityksellä. *Muita lisätietolähteitä* ISO/IEC 27002:2013 7.1.1; laki turvallisuusselvityksistä 726/2014; laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004		

T 10

Henkilöstöturvallisuus

Salassapito- ja vaitiolositoumukset

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Salassapito- tai vaitiolositoumusmenettely on käytössä.	5 §:n 1 mom. 8 ja 9 kohdat	I liitteen 29 kohta

Lisätietoja

ISO/IEC 27002:2013 7.1.2; ISO/IEC 27002:2013 13.2.4

T 11

Henkilöstöturvallisuus

Turvallisuuskoulutus ja -tietoisuus

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Turvallisuusohjeet kattavat salassa pidettävään tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta 2) Henkilöstölle annetaan ohjeet ja koulutusta salassa pidettävien tietojen asianmukaisesta käsittelystä. 3) Salassa pidettävien tietojen käsittelyä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneet henkilöt dokumentoidaan. 4) Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti.	1) 4 §, 5 §, 6 § 2) 5 §:n 1 mom. 9 kohta 3) 5 §:n 1 mom. 10 kohta 4) 5 §:n 1 mom. 10 kohta	I liitteen 29-31 kohdat, IV liitteen 21-22 kohdat

Lisätietoja

Toteutusesimerkki

1) Mikäli henkilö käsittelee salassa pidettäviä tietoja, hänelle on selvitetty tietojen suojaamista koskevat turvallisuussäännöt ja -menettelyt. EU:n ja Naton turvallisuusluokiteltujen tietojen käsittely edellyttää, että henkilö antaa lisäksi tietojen suojaamista koskevan vakuutuksen.
2) Turvallisuuskoulutus ja -ohjeistus toteutetaan henkilöstön työtehtävien tarpeet huomioiden.
3) Turvallisuusohjeiden kattavuutta ja ajantasaisuutta seurataan säännöllisesti ja se on tarvittavien tahojen saatavilla.
4) Turvallisuuskoulutuksen sisältö dokumentoidaan.

Yleistä:

Turvallisuusdokumentaatiolla pyritään muun muassa siihen, että turvallisuuden kannalta keskeiset menettelytavat ovat asianmukaisia ja yhdenmukaisia. Dokumentoimalla turvallisuuden kannalta keskeiset asiat pyritään varmistumaan myös siitä, että toiminta ei ole henkilöriippuvaista. Vrt. dokumentaation rooli muutoksenhallinnassa ja poikkeamien havainnointikyvyssä (I 20).

Muita lisätietolähteitä:

ISO/IEC 27002:2013 7.2.2; ISO/IEC 27002:2013 5.1.1; ISO/IEC 27002:2013 5.1.2; ISO/IEC 27002:2013 12.1.1; ISO/IEC 27001:2013 7.5; VAHTI 4/2003; VAHTI 2/2008; VAHTI 2/2010

T 12 Henkilöstöturvallisuus Tiedonsaantitarve ja käsittelyoikeudet	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
	1) Organisaatiossa ylläpidetään luetteloa salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä. 2) Pääsy salassa pidettävään tietoon voidaan myöntää vasta, kun henkilön työtehtävistä johtuva tiedonsaantitarve on selvitetty. 3) Organisaatiossa ylläpidetään luetteloa salassa pidettävien tietojen käsittelyoikeuksista suojaustasoittain.	13 §	I liitteen 2a kohta
	Lisätietoja		
	Yleistä: Tiedonsaantitarpeen määrittämistä helpottaa se, että organisaatio on kuvannut periaatteet, jolla organisaation henkilöt pääsevät salassa pidettäviin tietoihin, sekä prosessin tai menettelytapaohjeet, joilla työtehtäväperusteisesti pääsy myönnetään ja hallinnoidaan muutostilanteissa. Käsittelyoikeusmäärittelyissä sekä työtehtävä- ja roolimäärittelyissä tulisi ottaa huomioon, ettei synny vaarallisia työ- tai rooliyhdistelmiä. *Muita lisätietolähteitä:* ISO/IEC 27002:2013 9.1.1; ISO/IEC 27002:2013 9.1.2; ISO/IEC 27002:2013 6.1.2; VAHTI 2/2008; VAHTI 2/2010		

4. osa-alue F

FYYSINEN TURVALLISUUS

Katakrissa tarkastellaan fyysistä turvallisuutta viranomaisen salassa pidettävän tietoaineiston suojaamisen näkökulmasta. Lähtökohtana on varmistaa, että salassa pidettävät tiedot ovat suojassa oikeudettomalta paljastumiselta. Fyysisten turvatoimien tarkoituksena on estää tunkeutuminen salaa tai väkisin, ehkäistä, estää ja havaita luvattomat toimet ja mahdollistaa henkilöstön luokitus ja pääsy salassa pidettäviin tietoihin sen perusteella, mikä heidän tiedonsaantitarpeensa on. Tällaiset turvatoimet on määriteltävä riskienhallintaprosessin perusteella. Osa-alueessa F tilat ja tilaryhmät jaetaan alueisiin: hallinnollinen alue, turva-alue ja tekninen turva-alue. Tarve kunkin alueen perustamiseksi riippuu siitä, minkä tasoista salassa pidettävää tietoa alueella säilytetään tai käsitellään. Aluejako perustuu EU:n neuvoston turvallisuussääntöihin, mutta vastaavanlainen turvallisuusvyöhykkeisiin perustuva jako on käytössä myös kansallisesti.

Fyysiset turvatoimet valitaan ja mitoitetaan uhkakartoitukseen ja riskienarviointiin pohjautuen. Vaatimukset voidaan täyttää erilaisilla toteutusmalleilla. Fyysisten turvatoimien vaikuttavuutta tulee seurata osana organisaation riskienhallintaa. Tilanteissa, joissa organisaation tavoitteena on saada tiloilleen toimivaltaisen viranomaisen myöntämä hyväksyntä tai todistus, tulee organisaation toteuttamien turvatoimien olla riittäviä sekä organisaation oman että toimivaltaisen viranomaisen riskienarvioinnin havaintoihin nähden.

Lisätietokenttään on tulkinnan tueksi koottu toteutusesimerkkejä, joissa kuvatuilla menettelyillä voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojausten vähimmäistaso. Toteutusesimerkit voivat olla korvattavissa myös muilla vastaavan tasoisilla suojauksilla. Vaatimuksissa tai toteutusesimerkeissä ei kuvata kaikkiin ympäristöihin tai erikoistapauksiin riittäviä suojauksia.

Fyysisen turvallisuuden perusta on suunnittelussa. Tilojen ja rakennusten suunnittelussa ja käytössä on syytä ottaa huomioon seuraavat seikat:

1) Missä tiloissa suojattavia tietoja käsitellään ja minkä suojaustason tiedoista on kyse.
2) Missä ympäristössä ja rakennuksen osassa suojattavia tietoja käsitellään.
3) Rakennuksen tai tilan turvajärjestelyt ja rakenteet.
4) Salassa pidettävien tietojen suojaaminen tilassa (luominen, vastaanottaminen, käyttäminen, säilyttäminen ja hävittäminen).
5) Millä tietojenkäsittelyvälineillä ja järjestelmillä tietoja tilassa käsitellään.
6) Tietojen määrä; suojattavien tietojen kasautuminen saattaa edellyttää tiukempien turvallisuusvaatimusten soveltamista (esimerkiksi suuri määrä suojaustason IV tietoa saattaa muodostaa suojaustason III kokonaisuuden).
7) Tietoja käsitellään muuten kuin satunnaisesti sellaisissa tiloissa, joiden turvallisuus on käsiteltävän tiedon suojaustason huomioon ottaen riittävä.
8) Suunnittelu- ja ylläpito-organisaation kanssa on sovittu rakennuksen turvallisuusdokumentaation luottamuksellisuudesta.

Tiloja ja laitteita koskevat vaatimukset

F 01

Tiloja koskevat vaatimukset

Fyysiset turvatoimet

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Fyysiset turvatoimet on toteutettu monitasoisen suojaamisen periaatetta noudattaen.	14 §	II liitteen 4 kohta

Lisätietoja

Monitasoisella suojaamisella tarkoitetaan sitä, että toteutetaan joukko toisiaan täydentäviä turvatoimia. Mikäli mahdollista, tilat muodostavat keskenään sisäkkäisiä vyöhykkeitä, joissa korkeamman suojaustason tilat ovat sisimpinä. Vyöhykkeiden välinen liikenne on hallittua. Turvatoimet suunnitellaan kokonaisuutena, jossa otetaan huomioon salassa pidettävien tietojen suojaustaso, määrä, rakennusten ympäristö ja rakenne. Tämän lisäksi otetaan huomioon riskienhallintaprosessin kauttatunnistetut uhkat, kuten sabotaasi, terrorismi, tiedustelu ja rikokset.

Fyysiset tietoja suojaavat ominaisuudet muodostuvat rakennusten ja tilojen suunnittelusta, rakenteellisista suojaratkaisuista, turvajärjestelmistä ja –laitteista sekä turvallisuutta ylläpitävistä menettelytavoista. Turvaratkaisut suunnitellaan eri turvakontrollien yhdistelminä perustuen riskiarviointiin.

Esimerkki monitasoisesta suojauksesta:
Rakennus suunnitellaan niin, että sen ulkoseinät ja kuori muodostavat ensimmäisen turvallisuustason. Kulku rakennuksen sisään valvotaan ja hallitaan. Korkeamman suojaustason tietoa käsitellään rakennuksen sisemmissä osissa siten, että tunkeutuminen tiloihin on estetty. Turvallisuustekniset ratkaisut täydentävät rakenteellisia ratkaisuja. Suunnittelussa otetaan huomioon ikkunat, ovet ja muut aukot.

F 01

Organisaation on monitasoisen turvallisuuden käsitettä soveltaen riskienhallintaprosessin perusteella määriteltävä asianmukainen fyysisten turvatoimien yhdistelmä jotka voivat sisältää:

a) kehäsuojauksen: fyysinen este, jolla suojattava alue rajataan ja lukitaan;
b) säilytysyksikön tai säilytystilan: lukittava toimistokaluste, turvakaappi, kassakaappi, holvi;
c) murtohälytysjärjestelmä: kehäsuojauksen parantamiseksi sekä huoneissa ja rakennuksissa turvallisuushenkilöstön sijasta tai sen tueksi.
d) kulunvalvonnan: sähköinen tai sähkömekaaninen, turvallisuushenkilöstön ja/tai vastaanottovirkailijan toimesta tai muunlaisin fyysisin keinoin toteutettu;
e) pääsyoikeuksien hallinnan; asiakirjojen suoja varmistetaan antamalla henkilölle pääsy asiakirjoihin vain tiedonsaantitarpeen perusteella;
f) turvallisuushenkilöstön: koulutettua ja valvottua ja tarvittaessa asianmukaisesti turvallisuusselvitettyä turvallisuushenkilöstöä voidaan ottaa palvelukseen muun muassa tunkeutumista suunnittelevien henkilöiden aikeiden torjumiseksi;
g) kameravalvonnan: turvallisuushenkilöstö voi käyttää kameravalvontaa tilanteiden ja murtohälytysjärjestelmien hälytysten todentamiseksi laajoilla aluilla tai rajatuilla alueilla;
h) turvavalaistuksen: jonka ansiosta turvallisuushenkilöstö voi myös valvoa aluetta tehokkaasti joko suoraan tai kamerajärjestelmän välityksellä; ja
i) muun asianmukaisen fyysisen turvatoimen;

joiden tarkoituksena on luvattoman pääsyn estäminen ja havaitseminen tai salassa pidettävien tietojen katoamisen tai vahingoittumisen ehkäiseminen.

Muita lisätietolähteitä

ISO/IEC 27002:2013 11.1.3; VAHTI 2/2013

F 02	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Alueita koskevat vaatimukset Tietojen fyysiseksi suojaamiseksi tarvittavat alueet Hallinnolliset alueet, turva-alueet ja tekniset turva-alueet	1) Alueet, joissa säilytetään tai käsitellään salassa pidettäviä tietoja, on suojattu asianmukaisella lukituksella, kulunvalvonnalla tai muilla toimenpiteillä luvattoman pääsyn estämiseksi tiloihin ja siellä oleviin asiakirjoihin. 2) Asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja 3) Tietojen fyysiseksi suojaamiseksi on perustettu tarvittavat fyysisesti suojatut alueet (ks. I 21). *Hallinnollinen alue* 4) Alueella on selkeästi määritellyt näkyvät rajat, joilla henkilöt ja mahdollisuuksien mukaan ajoneuvot voidaan tarkastaa. 5) Alueelle on pääsy ilman saattajaa vain henkilöillä, joilla on lupa tulla alueelle. Kaikilla muilla henkilöillä on aina oltava saattaja tai heille on tehtävä vastaavat tarkastukset. 6) Mikäli alueella säilytetään salassa pidettäviä tietoja, alueella on kyseisen tiedon säilyttämiseen hyväksytty tila tai säilytysratkaisu. 7) Mikäli alueella käsitellään salassa pidettäviä tietoja, sivullisten pääsy tietoihin on estetty. *Turva-alue* 8) Alueella on selkeästi määritellyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla. 9) Alueelle on pääsy ilman saattajaa vain henkilöillä, joilla on asianmukainen turvallisuusselvitys ja erityinen lupa tulla alueelle tiedonsaantitarpeensa perusteella. Kaikilla muilla henkilöillä on aina oltava saattaja tai heille on tehtävä vastaavat tarkastukset. 10) Aluetta rajaavat rakenteet muodostavat kokonaisuuden, joka tarjoaa riskeihin nähden riittävän suojan asiattoman pääsyn estämiseksi. 11) Mikäli alueella säilytetään salassa pidettäviä tietoja, tulee siellä olla kyseisen tiedon säilyttämiseen hyväksytty tila tai säilytysratkaisu. 12) Mikäli alueelle ei ole asennettu murtohälytysjärjestelmää ja alueella ei ole henkilöstöä palveluksessa ympäri vuorokauden, se on tarvittaessa tarkistettava normaalin työajan päätteeksi ja satunnaisin ajankohdin sen ulkopuolella.	1) 14 § 2) 5 §:n 1 mom. 7 kohta	3) II liitteen 12 kohta 4) II liitteen 14a kohta 5) II liitteen 14b-c kohdat 6) II liitteen 24 kohta 7) II liitteen 23b kohta

F 02	Jos alueelle tulo merkitsee käytännössä välitöntä pääsyä sillä oleviin salassa pidettäviin tietoihin, sovelletaan lisäksi seuraavia vaatimuksia: 13) On varmistettu, että alueella tavanomaisesti säilytettyjen tietojen korkein suojaustaso tai turvallisuusluokka on tiedon käsittelijän tiedossa. 14) Kaikilla vierailijoilla on oltava erityinen lupa tulla alueelle. Heillä on aina oltava saattaja ja asianmukainen turvallisuusselvitys, paitsi jos on tehty toimia, joilla varmistetaan, ettei henkilöllä ole pääsyä sellaisiin tietoihin, joihin tällä ei ole oikeutta. Alueelle on laadittu turvallisuusmenettelyt, joissa on määräykset seuraavista: 15) Korkein suojaustaso- tai turvallisuusluokka, jota alueella voidaan käsitellä. 16) Sovellettavat valvonta- ja suojatoimenpiteet. 17) Henkilöt, joilla on pääsy alueelle ilman saattajaa tiedonsaantitarpeensa ja turvallisuusselvityksensä perusteella. 18) Henkilön saattamiseen liittyvät menettelyt. 19) Muut asiaan kuuluvat toimenpiteet ja menettelyt. *Tekninen turva-alue* Turva-alueen vaatimusten lisäksi: 20) Alueella on murtohälytysjärjestelmä. 21) Alue pidetään lukittuna silloin, kun se ei ole käytössä, ja vartioituna silloin, kun se on käytössä. 22) Avaimia valvotaan. 23) Alueelle tulevia henkilöitä ja aineistoja valvotaan. 24) Alue tarkastetaan säännöllisesti mahdollisten luvattomien tietoliikenneyhteyksien ja viestintävälineiden sekä muiden elektronisten laitteiden löytämiseksi. 25) Alueella ei ole luvattomia tietoliikenneyhteyksiä tai laitteita.		8) II liitteen 15a kohta 9) II liitteen 15b-c kohdat 10) II liitteen 22 11) II liitteen 22, 24 ja 26 kohdat 12) II liitteen 19 kohta 13) II liitteen 16a kohta 14) II liitteen 16b kohta 15-19) II liitteen 21 kohta 20-25) II liitteen 17 kohta
	Lisätietoja Alueella voidaan tarkoittaa mm. huonetta, laitetilaa, varastoa, arkistotilaa, niiden muodostamaa kokonaisuutta tai muuta rakennuksen osaa. Rakennuksissa sekä toimitiloissa voi olla useita eri turvallisuusvyöhykkeisiin kuuluvia alueita. Turvallisuusalue voi muodostua useasta tilasta. Turva-alue voidaan muodostaa ilman hallinnollista aluetta. Suojaustason IV-II tietoja voidaan käsitellä turva-alueella. Suojaustason IV-II tietoja voidaan käsitellä myös hallinnollisella alueella, jos sivullisten pääsy tietoihin on estetty. Suojaustason IV tietoja voidaan säilyttää hallinnollisella alueella. Suojaustason III-II tason tietoja tulee säilyttää turva-alueella. Ks. I 21 ja I 14.		

F 02

Hallinnollisen alueen raja:

Aluetta rajaavan aidan tai kuoren seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteilta ei vaadita erityisiä ominaisuuksia.
Hallinnollisen alueen raja ja salassa pidettävän tiedon käsittely- sekä säilytysyksikön rajaava tila tulisi olla lukittavissa lukolla, jonka avainten kopiointi on estetty patenttisuojalla.

Turva-alueen raja:

- Suojaustaso III

Mikäli suojattavaa tietoa säilytetään tilassa hyväksytyssä säilytysyksikössä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden antaa sellainen rakenteellinen suoja, että niiden kautta alueelle tunkeutuminen on hidasta ja vaikeaa.

Mikäli suojattavaa tietoa säilytetään tilassa ilman hyväksyttyä säilytysyksikköä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden olla kyseisen suojaustason tiedon säilyttämiseen hyväksyttyä säilytysyksikköä vastaava. Tällainen säilytysyksikkö on SFS-EN-14450 luokan S2 turvakaappi tai vastaava. Tällaiseksi suojaksi voidaan katsoa myös esimerkiksi SFS-EN-1627 luokkaa 4 vastaava rakenteellinen suoja.

- Suojaustaso II

Mikäli suojattavaa tietoa säilytetään tilassa hyväksytyssä säilytysyksikössä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden antaa sellainen rakenteellinen suoja, että niiden kautta alueelle tunkeutuminen on erittäin hidasta ja vaikeaa.

Mikäli suojattavaa tietoa säilytetään tilassa ilman hyväksyttyä säilytysyksikköä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden olla kyseisen suojaustason tiedon säilyttämiseen hyväksyttyä säilytysyksikköä vastaava. Tällainen säilytysyksikkö on SFS-EN-1143-1 luokan EII kassakaappi tai vastaava. Tällaiseksi suojaksi voidaan katsoa myös esimerkiksi SFS-EN-1627 luokkaa 5 vastaava rakenteellinen suoja. Vastaava rakenteellinen suoja voidaan toteuttaa myös siten, että turva-aluetta rajaavat rakenteet muodostavat SFS-EN-1627 luokkaa 3 vastaavan suojan ja sen lisäksi säilytysyksikköä rajaavan tilan rakenteet muodostettavat SFS-EN-1627 luokkaa 4 vastaavan suojan.

F 02

Murtohälytysjärjestelmä (vaatimuskohta 11):

Turva-alueiden tulisi olla riittävästi valvottuja tunkeutumiseen liittyvät riskit huomioiden. Toteutusesimerkkejä:

a) murtohälytysjärjestelmä ja hälytyksiin reagoiva yksikkö; tai
   - murtohälytysjärjestelmän on katettava turva-alueen suojatun rajan
   - murtohälytysjärjestelmä ja ilmoituksensiirto testataan kerran kuukaudessa
   - suojaustason II tietoaineistoa valvovan murtohälytysjärjestelmän hallinta on organisaatiosta nimetyn vastuuhenkilön hallinnassa

b) säilytystilan välittömässä yhteydessä on 24/7 miehitys.

Muita lisätietolähteitä

ISO/IEC 27002:2013 11.1.1; ISO/IEC 27002:2013 11.1.2; VAHTI 2/2013

F 03

Tietojen fyysiseen suojaukseen tarkoitetut turvallisuusjärjestelmät ja laitteet

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojen fyysiseen suojaamiseen tarkoitetut turvallisuusjärjestelmät ja laitteet (kuten turvakaapit, kassakaapit, kulunvalvontajärjestelmät, murtohälytyshälytysjärjestelmät ja valvontajärjestelmät) ovat hyväksyttyjen teknisten standardien tai vähimmäisvaatimusten mukaisia. Järjestelmiä ja laitteita tulee testata ja pitää käyttökuntoisina.	14 §, 6 §	II liitteen 8 ja 10 kohdat, IV liitteen 8 kohta

Lisätietoja

Säilytysratkaisujen ja turvallisuusjärjestelmien tulisi täyttää seuraavien standardien tai vaadituilta ominaisuuksiltaan vähintään sitä vastaavan muun Euroopan talousalueella hyväksytyn standardin vaatimukset:

- Kassakaapit: esimerkiksi SFS-EN 1143-1 tai muun vastaavan standardin mukaan testattu ja sertifioitu;
- Elementtiholvi: esimerkiksi SFS-EN 1143-1 tai muun vastaavan standardin mukaan testattu ja sertifioitu;
- Turvakaapit: esimerkiksi SFS-EN-14450 tai muun vastaavan standardin mukaan testattu ja sertifioitu;
- Lukot heloineen: esimerkiksi standardin SFS 7020 / SFS 5970 mukaan tai muun vastaavan standardin mukaan testattu ja luetteloitu sekä sertifioitu;
- Ovet ja aukot: esimerkiksi standardin SFS-EN 1627 mukaan tai muun vastaavan standardin mukaan testattu ja sertifioitu;
- Hälytysjärjestelmien (murto- ja ryöstöilmaisujärjestelmät) järjestelmävaatimukset ja soveltamisohjeet: esimerkiksi standardien SFS-EN 50131-1 + A1, SFS-EN 50131-1/A1 ja SFS-CLC/TS 50131-7 tai vastaavien mukaan.
- Hälytysjärjestelmien (Ilmoituksensiirtojärjestelmät ja laitteet) yleiset vaatimukset ja soveltamisohjeet: esimerkiksi standardien SFS-EN 50136-1 ja SFS-CLC/TS 50136-7 tai vastaavien mukaisesti
- Kulunvalvontajärjestelmien järjestelmä- ja komponenttivaatimukset sekä soveltamisohjeet: esimerkiksi standardien SFS-EN 50133-1 + A1, SFS-EN 50133-1/A1, SFS-EN 50133-2-1 ja SFS-EN 50133-7 tai vastaavien mukaisesti
- Kameravalvontajärjestelmien järjestelmävaatimukset ja soveltamisohjeet: esimerkiksi standardien SFS-EN 50132-1, SFS-EN 50132-7, SFS-EN 62676-1-1 ja SFS-EN 62676-1-2 tai vastaavien mukaan.
- Kameravalvontajärjestelmän käyttöönotto ja luovutustarkastus voidaan tehdä esimerkiksi finanssialan keskusliiton K-menetelmän mukaan.
- Paperisilppurit: ks. I 19.

Lisäksi:

- Mikäli suojaustasolle IV luokitellun tietoaineiston säilytysyksikkönä käytetään lukittavaa kaappia, on varmistuttava siitä, että tunkeutumisesta jää jälki.
- Suojaustaso III luokiteltu tieto on säilytettävä SFS-EN 14450 luokan S2 turvakaappi tai vastaavassa.
- Suojaustaso II luokiteltu tieto on säilytettävä SFS-EN 1143-1 luokan EII kassakaapissa tai vastaavassa.

Muita lisätietolähteitä

ISO/IEC 27002:2013 11.1.1; VAHTI 2/2013

Luvattoman pääsyn estäminen

F 04

Luvattoman pääsyn estäminen

Kulkuoikeuksien hallinta

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Kulkuoikeuksien hallinta on järjestetty niin, että luvaton pääsy salassa pidettäviin tietoihin on estetty. 2) Pääsy salassa pidettäviä tietoja sisältäviin tiloihin sallitaan ainoastaan työtehtävistä johtuvan tiedonsaanti-tarpeen perusteella.	14 §	II liitteen 2 kohta

Lisätietoja

Suositus kulunvalvonnan toteuttamisesta:

- Organisaatiossa käytetään kuvallisia henkilökortteja tai vastaavia näkyviä tunnisteita.
- Hallinnollisen alueen ja turva-alueen (myös tekninen turva-alue) kulkuoikeudet myöntää nimetty vastuuhenkilö organisaatiossa
- Kulunvalvonnan hallintajärjestelmän menettelytavat on ohjeistettu ja dokumentoitu:
    - Myönnetyistä kulkuoikeuksista laaditaan dokumentti ja sitä ylläpitää nimetty vastuuhenkilö.
    - Henkilöllä on vain ne kulkuoikeudet, joita hän tarvitsee työtehtäviensä hoitamiseksi.
    - Kulkuoikeuden myöntämisperuste kirjataan dokumenttiin ja vain nimetyillä henkilöillä on kulkuoikeudet alueelle.
    - Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa kulkuoikeuksiin.
    - Organisaatioon kuuluvan henkilöstön ja ulkopuolisten henkilöiden luettelot pidetään erillään.
    - Kulkuoikeudet katselmoidaan säännöllisin väliajoin esimerkiksi 6kk:n välein organisaatiosta nimetyn vastuuhenkilön toimesta.
    - Kulunvalvontajärjestelmän hallinta voi olla ulkoistettu. Peruskäyttäjän työasemalta tapahtuva oven avaus turva-alueelle pitää olla estetty.

- Turva-alueelle kulkuoikeus on vain alueelle oikeutetulla henkilöllä. Kulku alueelle pitää olla myöhemmin todennettavissa.
- Suojaustasolle II luokitellun tiedon käsittely- ja säilytystilaan on kulkuoikeus vain alueelle oikeutetulla henkilöllä ja kulunvalvonnassa on käytettävä tilaan mentäessä sekä tilasta poistuttaessa tunnistusta. Kulku tilaan pitää olla myöhemmin todennettavissa.

Käytännöt vierailijoiden osalta:

- Henkilöistä on koulutettu vierailijoita koskevien hallintatapojen ja menettelytapojen osalta ja näitä ylläpitää nimetty vastuuhenkilö organisaatiossa:
    - Vierailijoiden isännän on kuuluttava organisaation henkilöstöön.
    - Vieraat eivät koskaan jää valvomatta tiloihin ilman isäntää tai hänen edustajaansa.
    - Vierailijat käyttävät näkyvää tunnistetta esimerkiksi vierailijakorttia.
    - Henkilökunta on ohjeistettu reagoimaan ilman tunnistetta liikkuviin henkilöihin.

F 04

Hallinnollisen alueen ja turva-alueen huoltotoimenpiteiden osalta

- Hallinnollisella alueella tehtävät huoltotoimenpiteet tapahtuvat vain alueelle valtuutettujen toimesta tai organisaatioon kuuluvan henkilökunnan valvonnassa.
- Turva-alueella tehtävät huoltotoimenpiteet tapahtuvat vain niiden henkilöiden toimesta joilla on erityinen lupa ja turvallisuusselvitys alueelle tai organisaatioon kuuluvan henkilökunnan valvonnassa.
- Suojaustasolle III luokitellun tiedon säilytystilan tai sitä rajaavan tilan murtohälytysjärjestelmän, kulunvalvontajärjestelmään ja muihin valvontajärjestelmiin liittyvien laitetilojen ja sen laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat vain niiden henkilöiden toimesta, joilla on erityinen lupa ja turvallisuusselvitys alueelle tai organisaatioon kuuluvan henkilökunnan valvonnassa.
- Suojaustasolle II luokitellun tiedon käsittely- ja säilytystilan sekä sitä rajaavan turva-alueen murtohälytysjärjestelmän, kulunvalvontajärjestelmään ja muihin valvontajärjestelmiin liittyvien laitetilojen ja sen laitteistojen huolto-, asennus- ja siivoustoimet toteutetaan vain niiden henkilöiden toimesta, joilla on erityinen lupa ja turvallisuusselvitys alueelle sekä organisaatioon kuuluvan henkilökunnan valvonnassa.

Salassa pidettävän tiedon käsittely huoltotoimenpiteiden ja vierailujen aikana:

Suojaustasolle IV-II luokitellun tiedon käsittely tilassa on huolto-, asennus- ja siivoustoimien aikana kielletty.

Muita lisätietolähteitä

ISO/IEC 27002:2013 11.1.5; VAHTI 2/2013

F 05

Luvattoman pääsyn estäminen

Avainten ja numeroyhdistelmien hallinta

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Toimistojen, huoneiden, kassaholvien ja turvasäilytysyksiköiden avainten ja avaustunnisteiden hallintamenettelyt ovat riittävät luvattoman pääsyn estämiseksi. 2) Avaustunnisteet on annettu mahdollisimman harvoille sellaisille henkilöille, joiden on tarpeen tietää ne ja henkilöt osaavat numeroyhdistelmät ulkoa. 3) Turvasäilytysyksiköiden ja kassaholvien avaustunnisteiden numeroyhdistelmät vaihdetaan a) uuden turvallisen säilytyspaikan vastaanoton yhteydessä b) aina kun avaustunnisteen tunteva henkilö vaihtaa tehtäviä tai poistuu organisaation palveluksesta c) aina kun tiedot ovat vaarantuneet tai kun niiden epäillään vaarantuneen d) kun jokin lukoista on huollettu tai korjattu ja vähintään 12 kuukauden välein.	1) 5 §:n 1 mom. 7 kohta, 14 §:n 1 mom.	2) 1) II liitteen 30 kohta 3) 2) II liitteen 31 kohta 4) 3) II liitteen 31 kohta

Lisätietoa

Avainten hallintajärjestelmä:

- Avainten hallintajärjestelmän menettelytavat on ohjeistettu ja dokumentoitu
    - Avainten hallintaan on nimetty vastuuhenkilö organisaatiossa ja hänellä on luettelo jaetuista ja hallussaan olevista avaimista sekä alueen lukostokaavio ja avainkortti.
        - Avaimen luovutusperuste kirjataan dokumenttiin.
        - Avaimet voidaan luovuttaa vain kulkuoikeuden omaavalle henkilölle.
        - Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa avainten hallintaoikeuteen.
        - Avainten hallintaoikeus katselmoidaan säännöllisesti.
- Hallinnolliselle alueelle ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. Yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos tiloista on kielletty. Yleisavainta säilytetään turvallisesti ja suljettuna sinetöityyn, sulkemispäiväyksellä ja kuittauksella varustettussa säilytyskuoressa.
- Turva-alueelle ei saa päästä alemman luokan tilaan sopivalla yleisavaimella. Yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos tiloista on kielletty. Yleisavaimen tai vastaavan kulkutunnisteen vieminen ulos tiloista on kielletty. Yleisavainta säilytetään turvallisesti ja suljettuna sinetöityyn, sulkemispäiväyksellä ja kuittauksella varustettuun säilytyskuoreen. Yleisavain luovutetaan työtehtävään liittyen ja kuittausta vastaan. Menettely on kuvattu turvallisuuden hallintaohjeissa.
- Turva-alueelle vartiointi-, kiinteistönhoito- ja huoltohenkilöstölle jaettavat avaimet tulee olla sinetöitynä poikkeuksellisien tilanteiden hoitamista varten, mikäli vartiointi-, kiinteistönhoito- ja huoltohenkilöstö on ulkoistettu. Hälytystilanteessa tilaan edellytetään saapuvan kaksi henkilöä samanaikaisesti.
    - Salassa pidettävän tiedon säilytystilaan sopivia avaimia ei luovuteta poikkeuksellisten tilanteiden hoitamista varten ulkoistetulle vartiointi-, kiinteistöhoito- ja huoltohenkilökunnalle.

F 05	
	Pääsyoikeuksien hallintajärjestelmä (tietojärjestelmäturvallisuus ks. I 06, I 07 ja I 08) ■ Pääsyoikeuksien hallintajärjestelmän menettelytavat on ohjeistettu ja dokumentoitu ● Myönnetyistä pääsyoikeuksista (avaimet ja numeroyhdistelmät) salassa pidettävän tietoaineiston (asiakirjat, dokumentit) säilytystilaan tai säilytysyksikköön (turvakaapit, kassakaapit, kassaholvit sekä palvelintilat) laaditaan dokumentti ja sitä ylläpitää nimetty vastuuhenkilö organisaatiossa. • Pääsyoikeus voidaan myöntää, jos henkilöllä on turvallisuusselvitys ja oikeus salassa pidettävään tietoon tai jos tilaan on muu tarve ja sinne pääsy merkitsee käytännössä välitöntä pääsyä sillä oleviin salassa pidettäviin tietoihin. • Pääsyoikeuden myöntämisperuste kirjataan dokumenttiin. • Henkilöstössä tapahtuvat muutokset välittyvät tarvittaessa pääsyoikeuksiin. • Pääsyoikeudet katselmoidaan säännöllisin väliajoin. *Muita lisätietolähteitä* VAHTI 2/2013

Suojaaminen salakatselulta ja salakuuntelulta

F 06	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
	Tietojen salakatselua vastaan on suojauduttu.	14.§:n 1 mom. 5§:n 5 mom.	II liitteen 6 kohta
Tiedon suojaaminen	Lisätietoja		
Salakatselulta suojautuminen	*Salakatselun estäminen:* ■ Tiedon esiintymismuodosta riippumatta salassa pidettävää tietoa käsitellään siten, ettei tieto näy asiattomille. ■ Kannettavissa tietokoneissa on sivusta katselun estävä näyttösuoja. ■ Tilan ikkunat on varustettu näköestesuojalla, esimerkiksi sälekaihtimilla. Tilaan ei saa olla näköyhteyttä ulkopuolelta silloin, kun tilassa käsitellään suojausta-solle IV tai sitä korkeammalle luokiteltua tietoa. Teknisellä turva-alueella tehdään lisäksi tekninen tilaturvatarkastus ennen tilan käyttöönottoa. (vrt. F 02 kohta 24). Ks. I 14. *Muita lisätietolähteitä* ISO/IEC 27002:2013 11.1.3; VAHTI 2/2013		

F 07	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tiedon suojaaminen Salakuuntelulta suojautuminen	Tietojen salakuuntelua vastaan on suojauduttu.	14 §:n 1 mom. 5§:n 5 mom.	II liitteen 17 kohta
	Lisätietoja		
	Tilojen ääneneristys hallinnollisella alueella ja turva-alueella: Salassa pidettävästä tiedoista käytävä keskustelu ei saa välittyä viereisiin tiloihin niille, joilla ei ole tietoon oikeutta. Teknisellä turva-alueella tehdään lisäksi tekninen tilaturvatarkastus ennen tilan käyttöönottoa. (vrt F 02 kohta 24) *Muita lisätietolähteitä* ISO/IEC 27002:2013 11.1.3; VAHTI 2/2013		

Toiminnan jatkuvuuden hallinta

F 08	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Toiminnan jatkuvuuden varmistaminen	Toiminnan jatkuvuussuunnitelmiin on sisällytetty ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutuksen salassa pidettävien tietojen käsittelyyn ja säilyttämiseen.	5 §:n 1 mom. 4 kohta	5 artikla
	Lisätietoa		
	Kriittisten palvelin- ja laitetilojen toimintavaatimukset: ■ Kriittiset palvelimet ja laitteet on tunnistettu ja varmennettu toimintavaatimusten mukaisesti. • Mikäli järjestelmän toimintavaatimukset ovat korkeat, on järjestelmien käytettävyys varmennettava murtoa, ilkivaltaa, paloa, lämpöä, kaasuja, pölyä, tärinää, vettä ja sähkönkäytön katkoksia vastaan. • Kriittisiä palvelin- ja laitetiloja ohjaavan LVI-automaationhallinnan etäkäyttö on estetty. • Kriittisten palvelin- ja laitetilojen olosuhdesensoreja suojataan ja valvotaan. *Muita lisätietolähteitä* ISO/IEC 27002:2013 11.2.1; ISO/IEC 27002:2013 11.2.2; VAHTI 2/2013		

5. osa-alue I

TEKNINEN TIETOTURVALLISUUS

Katakrin teknisen tietoturvallisuuden osa-alueessa kuvataan vaatimukset, joita soveltamalla pyritään varmistamaan turvallisuusjärjestelyjen riittävyys viranomaisen salassa pidettävän tiedon sähköisissä käyttöympäristöissä. Osa-alueessa täydennetään myös Katakrin muiden osa-alueiden kuvauksia paperimuotoisen aineiston suojausvaatimuksista. Vaatimukset on jaettu tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuuden osioihin. Osa-alue koostuu vaatimuksista, niiden tulkinnan tueksi laadituista toteutusesimerkeistä sekä muista taustoittavista lisätiedoista. Tiettyihin asiakokonaisuuksiin (esimerkiksi hallintayhteydet, langattomat verkot, etäkäyttö ja varmuuskopiointi) on ryhmitelty niihin liittyvät vaatimukset.

Teknisen tietoturvallisuuden osa-alueen tarkoituksenmukainen käyttö edellyttää kyseiseen ympäristöön kohdistetun riskienarvioinnin pohjalta tapahtuvaa vaatimusten tulkintaa. Lisätietokenttään on tulkinnan tueksi koottu toteutusesimerkkejä, joissa kuvatuilla menettelyillä voidaan useimmissa ympäristöissä saavuttaa hyväksyttävä suojausten vähimmäistaso. Toteutusesimerkit voivat olla korvattavissa myös muilla vastaavan tasoisilla suojauksilla. Vaatimuksissa tai toteutusesimerkeissä ei kuvata kaikkiin ympäristöihin tai erikoistapauksiin riittäviä suojauksia.

Tilanteissa, joissa organisaation tavoitteena on saada tietojärjestelmälle toimivaltaisen viranomaisen myöntämä hyväksyntä tai todistus, tulee organisaation toteuttamien suojausten olla riittäviä sekä organisaation oman että toimivaltaisen viranomaisen riskienarvioinnin havaintoihin nähden. Erityisesti tilanteissa, joissa suojauksille käytetään korvaavaa menettelyä, tulee kohdeorganisaation pystyä osoittamaan, että näillä menettelyillä saavutetaan riittävä suojausvaikutus.

Kustannusten hallitsemiseksi suositellaan erityisesti salassa pidettävän tiedon tarkoituksenmukaista luokittelua, sekä viranomaisen salassa pidettävän tiedon käsittely-ympäristön eriyttämistä ja rajaamista mahdollisimman suppeaksi. Esimerkiksi eriyttämällä suojaustason III käsittely-ympäristöt suojaustason IV käsittely-ympäristöistä, suojaustason III suojausmenetelmiä ei edellytetä toteutettavaksi kuin vain suojaustason III tiedon käsittely-ympäristössä.

Katakrin ensisijaisissa käyttötapauksissa tietojärjestelmien tarkastuksessa viranomaisena toimii Viestintävirasto. Tietojärjestelmätarkastuksen käyttötapauksia on kuvattu yksityiskohtaisemmin liitteessä II.

Arvioitaessa viranomaisen salassa pidettävän tiedon käsittely-ympäristöä kokonaisuudessaan, on arvioinnissa huomioitava kaikki teknisen tietoturvallisuuden osiossa kuvatut vaatimukset. Tilanteissa, joissa arviointi kohdistetaan vain sähköisessä muodossa tietoa käsittelevään tietojärjestelmään, arvioidaan vain sähköiseen tietojenkäsittelyyn liittyvien vaatimusten täyttymistä. Tällöin esimerkiksi paperimuotoista tietojenkäsittelyä koskevia vaatimuksia (erityisesti I 19, I 17, I 16 ja I 18) huomioidaan vain soveltuvin osin. Tiettyjen vaatimusten kohdalla (erityisesti I 12 ja I 14) hyväksyttävissä oleva toteutustapa riippuu siitä, käsitelläänkö kyseisessä järjestelmässä kansallista vai kansainvälistä salassa pidettävää tietoa.

Tietoliikenneturvallisuus

I 01

Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen

-Verkon rakenteellinen turvallisuus

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Suojaustaso IV 1) Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä. 2) Tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä. 3) Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan viranomaisen ko. suojaustasolle hyväksymällä salausratkaisulla (vrt. I 12 ja I 15). *Suojaustasot III-II* Kohtien 1 ja 3 lisäksi: 4) Tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin edellyttää viranomaisen ko. suojaustasolle hyväksymän yhdyskäytäväratkaisun käyttöä.	1) 5 §:n 1 mom. 6 kohta, 16 § 2) 5 §:n 1 mom. 6 kohta, 16 § 3) 5 §:n 1 mom. 6 kohta, 16 § 4) 5 §:n 1 mom. 6 kohta, 16 §19 §	1) IV liitteen 32-35 kohdat 2) IV liitteen 32-35 kohdat 3) 9 artiklan 4 kohta, IV liitteen 25 ja 35 kohdat 4) IV liitteen 32-35 kohdat

Lisätietoja

Yleistä

Tietojenkäsittely-ympäristöjen oletetaan lähtökohtaisesti olevan toisilleen ei-luotettuja myös tilanteissa, joissa yhdistetään eri organisaatioiden hallinnoimia tietojenkäsittely-ympäristöjä toisiinsa. Saman suojaustason käsittely-ympäristöjä voidaan liittää toisiinsa ko. suojaustasolle viranomaisen hyväksymän salausratkaisun avulla (esimerkiksi organisaation eri toimipisteiden ko. suojaustason käsittely-ympäristöjen yhteenliittäminen julkisen verkon ylitse).

Huom: Suojaustason ylitys hallintaliikenteen (vrt. I 04) osalta edellyttää viranomaisen ko. suojaustasolle hyväksymää yhdyskäytäväratkaisua. Käytännössä hallintaliikenne rajataankin lähes poikkeuksetta suojaustasoittain.

I 01

Esimerkkejä

Suojaustason IV tietojenkäsittely-ympäristön yhdistäminen eri suojaustasojen ympäristöihin voidaan toteuttaa palomuuriratkaisuilla ja rajaamalla turvallisuuskriittisten alemman suojaustason ympäristöä käyttävien palvelujen (web-selailu, sähköposti, ja vast.) liikenne kulkemaan erillisten sisältöä suodattavien välityspalvelinten kautta. Suojaustason IV käsittely-ympäristöjä on mahdollista kytkeä Internetiin ja muihin ei-luotettuihin verkkoihin, kunhan suojaustason muut vaatimukset täyttyvät. Tyypillinen käyttötapa suojaustason IV käsittely-ympäristölle on organisaation ”toimistoverkon” tietojenkäsittely-ympäristön osa, joka voi muodostua esimerkiksi työasemista ja asianhallintajärjestelmistä sekä niiden suojaamiseen liittyvistä järjestelyistä (palomuuraus, käyttöoikeushallinto, jne.).

Suojaustasosta III lähtien yhdistäminen eri suojaustasojen ympäristöihin voidaan toteuttaa viranomaisen hyväksymillä yhdyskäytäväratkaisuilla. Hyväksyttävissä olevien yhdyskäytäväratkaisujen suunnitteluperiaatteita ja yleisiä ratkaisumalleja on kuvattu yksityiskohtaisemmin Viestintäviraston ohjeessa ”Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista” (www.ncsa.fi > Asiakirjat > Yhdyskäytäväratkaisuohje).

Suojaustason III käsittely-ympäristöt ovat moniportaisesti loogisesti tai fyysisesti ei-luotetuista verkoista/järjestelmistä eristettyjä kokonaisuuksia. Fyysisellä eristämisellä tarkoitetaan OSI-mallin fyysisen kerroksen tasolla tapahtuvaa erottelua. Suojaustason III käsittely-ympäristöihin ei pääsääntöisesti kytketä mitään muita verkkoja/järjestelmiä. Mikäli loppukäyttäjän työtehtävät edellyttävät pääsyä Internetiin tai muihin eri suojaustason järjestelmiin/verkkoihin, se on yleensä perusteluinta järjestää erillisellä tietokoneella, jota ei kytketä suojaustason III verkkoon. Viranomainen voi tapauskohtaisesti hyväksyä myös suojaustason III käsittely-ympäristön fyysisen kytkemisen erikseen tarkastettuun ja hyväksyttyyn verkkoon/järjestelmään. Tällaiset erikseen hyväksytyt verkot/järjestelmät jakautuvat pääsääntöisesti neljään käyttötilanteeseen:

A. Tiedonsiirtojärjestelmät

Suojaustason III järjestelmä/verkko voi olla tiedonsiirtojärjestelmä kahden tai useamman fyysisen pisteen välillä. Tällöin jokaisen kytketyn pisteen tulisi olla turvallisuustasoltaan vastaavalla tasolla. Verkkotason rajapinta on useimmiten muotoa [fyysisesti eristetty verkko/työasema] - [palomuurilaitteisto/-ohjelmisto] – [suojaustasolle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto] - [Internet] – [palomuurilaitteisto/-ohjelmisto] - [suojaustasolle hyväksytty salauslaite] - [palomuurilaitteisto/-ohjelmisto] - [fyysisesti eristetty verkko/työasema]. Vastaavilla järjestelyillä voidaan toteuttaa myös suojaustason II mukainen ratkaisu.

B. Palvelujärjestelmät

Suojaustason III järjestelmä/verkko voi olla esimerkiksi tietokantapalvelu, jota käytetään useasta fyysisestä pisteestä. Verkkotason rajapinta on tällöin vastaava kuin käyttötilanne A:ssa.

Suojaustason II käsittely-ympäristöt ovat lähtökohtaisesti fyysisesti eristettyjä kokonaisuuksia, joihin sallitaan suojaustason ylittävä liikennöinti vain datadiodien tai vastaavien OSI-mallin fyysisellä kerroksella toimivien yksisuuntaisten yhdyskäytäväratkaisujen kautta.

I 01

C. Yhdyskäytäväratkaisut

C1. Suojaustason III tiedon käsittely-ympäristöön voidaan siirtää tietoa alemman suojaustason ympäristöstä erillisen, vain yksisuuntaisen liikenteen sallivan yhdyskäytäväratkaisun (esim. datadiodi) kautta. Vastaavilla järjestelyillä voidaan toteuttaa myös suojaustason II mukainen ratkaisu.
C2. Suojaustason III tiedon käsittely-ympäristöstä voidaan siirtää matalamman suojaustason tietoa matalamman suojaustason ympäristöön sisältösuodatusratkaisun kautta. Sisältösuodatusratkaisun käyttö edellyttää tiedon tunnistamista ylemmän tason ympäristössä, ja vain matalamman tason tiedon siirtymisen sallimista ylemmän tason ympäristöstä matalamman tason ympäristöön.

D. Muut käsittely-ympäristöt

Muut suojaustason III käsittely-ympäristöt ovat yleisimmin organisaation tuotekehitysverkkoja tai muita suojaustason III tiedon käsittely-ympäristöjä. Tällaisiin järjestelmiin voidaan kytkeä esimerkiksi vain tätä ympäristöä palveleva päivityspalvelin. Päivityspalvelimelta voidaan sallia keskitetty turvapäivitysten ja haittaohjelmatunnisteiden jakelu tietyin rajauksin. Jaeltavat päivitykset ja tunnistekannat voidaan tuoda päivityspalvelimelle ilmaraon yli, tai vaihtoehtoisesti esimerkiksi datadiodin läpi.

Kasautumisvaikutus

Suuresta määrästä tietyn suojaustason tietoa koostuvissa tietojärjestelmissä asiakokonaisuus voi nousta luokitukseltaan yksittäistä tietoa korkeampaan suojaustasoluokkaan. Tyypillisesti kasautumisessa on kysymys IV-tason tiedosta (esimerkiksi suuri määrä suojaustason IV tietoa voi muodostaa yhdistettynä suojaustason III tietovarannon). Kun kohteen keskeisen tietovarannon suojaustaso tulkitaan kasautumisvaikutuksesta johtuen yksittäisten tietoalkioiden tasoa korkeammaksi, tulisi tietovarannon määritellyt suojausmenetelmät toteuttaa korkeamman tason vaatimusten mukaisesti. Määritellyillä suojausmenetelmillä tarkoitetaan menetelmiä, joilla rajataan pääsy vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, ja joilla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä havaitaan. Kun arviointityökaluna käytetään Katakria, tulisi kasautumisvaikutus tulkita siten, että tietovarannon suojauksilta edellytetään korkeamman tason mukaisena tietovarannon fyysisen turvallisuuden lisäksi kohtia I 13 (sovelluskerroksen turvallisuus), I 10 ja I 11 (jäljitettävyys ja havainnointikyky) sekä I 06 (tehtävien eriyttäminen). Onkin huomioitava, että kasautumisvaikutuksen seurauksena yhdellä luokalla noussut tietovarannon suojaustaso ei edellytä hyväksyttävää yhdyskäytäväratkaisua tietovarannon (esim. ST III) ja päätelaitteiden (esim. ST IV) välille.

Muita lisätietolähteitä

Viestintäviraston ohje ”Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista”; SANS Critical Security Controls (v5) / 10; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 13.1.2; VAHTI 3/2012:n luku 2.4

I 02

Vähimpien oikeuksien periaate - Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt ko. suojaustason sisällä

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöstöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti.	5 §:n 1 mom. 6 kohta	IV liitteen 16, 18, 19 ja 33-34 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasoilla IV-II vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Tietoliikenneverkko on jaettu ko. suojaustason sisällä erillisiin verkko-alueisiin (vyöhykkeet, segmentit).
2) Verkko-alueiden välistä liikennettä valvotaan ja rajoitetaan siten, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan (default-deny).
3) Tietojenkäsittely-ympäristössä on varauduttu yleisiin verkkohyökkäyksiin.

Yleistä

Tietoliikenneverkon jakaminen ko. suojaustason sisällä erillisille verkko-alueille (vyöhykkeet ja segmentit) voi tarkoittaa esimerkiksi hankekohtaista työasema- ja palvelinerottelua. Verkkoalueiden välisen liikenteen valvonnan ja rajoittamisen voi toteuttaa suojaustason IV verkon ulkorajalla esimerkiksi siten, että kaikki sisäänpäin tulevat yhteydenavausyritykset estetään ja ulospäin lähtevät yhteydet rajataan vain välityspalvelimen kautta tulevaan web-selailuun sekä sähköpostiliikenteeseen. Kaikkien suojaustasojen verkoissa riittävä vähimpien oikeuksien periaatteen huomiointi edellyttää tyypillisesti myös sitä, että suojaustason sisällä eri verkkoalueiden välillä sallitaan vain tarpeelliset yhteydet (lähde-kohde-protokolla) ja että muut yhteysyritykset havaitaan.

Kaikkia liitettyjä tietotekniikkajärjestelmiä tulisi lähtökohtaisesti käsitellä epäluotettavina ja varautua yleisiin verkkohyökkäyksiin. Yleisiin verkkohyökkäyksiin varautumiseen sisältyy esimerkiksi vain tarpeellisten toiminnallisuuksien pitäminen päällä. Toisin sanoen jokaiselle päällä olevalle toiminnallisuudelle tulisi olla perusteltu toiminnallinen tarve. Toiminnallisuus tulisi rajata suppeimpaan toiminnalliset vaatimukset täyttävään osajoukkoon (esimerkiksi toiminnallisuuksien näkyvyyden rajaus). Lisäksi tulisi ottaa huomioon esimerkiksi osoitteiden väärentämisen (spoofing) estäminen ja verkkojen näkyvyyden rajaaminen. Suojaustasolla IV tulisi myös ottaa huomioon palvelunestohyökkäyksen uhka, mikäli järjestelmä liitetään ei-luotettuun verkkoon.

Suodatusten tulisi perustua vähimpien oikeuksien periaatteeseen ja suodatuksen tulisi sallia vain erikseen hyväksytty liikennöinti (default-deny). Suodatuksissa tulisi huomioida myös eri protokollien (esim. IPv4, IPv6, GRE, VPN-tunnelit, reititysprotokollat) toiminnallisuudet. Tarpeettomat protokollat tulisi poistaa käytöstä kaikista sellaisista järjestelmistä (työasemat, palvelimet, verkkolaitteet, jne.), joissa niille ei ole todellista käyttöperustetta, ja varmistettava liikennöinnin estyminen (verkko-, työasema- ja palvelintason) palomuurien suodatussäännöillä. Mikäli työasemissa, palvelimissa, verkkolaitteissa tai muissa vastaavissa järjestelmissä käytetään esimerkiksi IPv6-toiminnallisuutta, tulisi ottaa huomioon sen vaikutukset erityisesti liikenteen suodatukseen (palomuurauksen tulisi kattaa myös IPv6-liikenne) sekä reititykseen. Myös eri protokollien yhdistämis- ja yhteiskäyttöratkaisujen (esim. IPv4-IPv6-toteutukset, NAT-64, Teredo) vaikutukset tulisi ottaa huomioon verkon/järjestelmien turvallisuuden kokonaissuunnittelussa.

I 02

Muita lisätietolähteitä

BSI IT-Grundschutz-Catalogues - 13th version - 2013; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 11; SANS Critical Security Controls (v5) / 13; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Spear Phishing - Understanding the Threat; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 13.1.2; ISO/IEC 27002:2013 13.1.3; VAHTI 3/2010:n luku 11; VAHTI 2/2010:n liitteen 5 luku 2.5

I 03

Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan - Suodatus- ja valvontajärjestelmien hallinnointi

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan. 2) Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen ja poistaminen on vastuutettu ja organisoitu. 3) Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia. 4) Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.	1) 5 §:n 1 mom. 2 ja 6 kohdat 2) 5 §:n 1 mom. k2 ja 6 kohdat 3) 5 §:n 1 mom. 6 kohta 4) 5 §:n 1 mom. 6 kohta	1) IV liitteen 8-12 kohdat 2) IV liitteen 9 kohta 3) IV liitteen 12 kohta 4) IV liitteen 11 kohta

Lisätietoja

Yleistä

Liikennettä suodattavia ja/tai valvovia järjestelmiä ovat tyypillisesti palomuurit, reitittimet, IDS-/IPS-järjestelmät ja vastaavia toiminnallisuuksia sisältävät verkkolaitteet/palvelimet/sovellukset.
Riittävän dokumentaation toteutus edellyttää yleensä esimerkiksi verkkorakenteen kuvaamista verkkoalueineen (vyöhykkeet ja segmentit) sillä tarkkuudella, että dokumentaation pohjalta voidaan tarkastaa verkon vastaavan viranomaisen hyväksymää rakennetta.
Käytettävyyden ja riittävän dokumentoinnin varmistamisen kannalta tarkoituksenmukainen ratkaisu on usein palomuurisääntöjen sekä palomuurien konfiguraatioiden varmuuskopiointi, ja varmuuskopioiden suojaustason mukainen säilytys.
Asetusten ja halutun toiminnan tarkasteluun hyväksyttävissä oleva tarkastustiheys riippuu erityisesti kohteessa tapahtuvien muutosten tiheydestä ja kohteen laajuudesta. Esimerkiksi organisaation suojaustason IV tietojenkäsittely-ympäristön palomuurisäännöstöt voivat olla laajoja ja muutoksia voi olla tarve tehdä usein. Tällaisissa ympäristöissä riittävä tarkastustiheys voi olla esimerkiksi vuosineljänneksittäin tai puolivuosittain. Toisaalta sellaisissa suppeissa ympäristöissä, missä suodatussäännöstöihin ei ole tarve tehdä muutoksia kuin hyvin harvoin, voi riittää vuosittaiset tarkastukset.

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 10; BSI IT-Grundschutz-Catalogues - 13th version - 2013; ISO/IEC 27002:2013 18.2.1; ISO/IEC 27002:2013 18.2.3; VAHTI 3/2010:n luku 16; VAHTI 2/2010:n liitteen 5 luku 2.5

I 04

Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen - Hallintayhteydet

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Hallintayhteydet on rajattu suojaustasoittain, ellei käytössä ole viranomaisen ko. suojaustasoille hyväksymää yhdyskäytäväratkaisua. 2) Hallintaliikenteen sisältäessä salassa pidettävää tietoa ja kulkiessa matalamman suojaustason ympäristön kautta, salassa pidettävät tiedot on salattu viranomaisen hyväksymällä salaustuotteella. 3) Hallintaliikenteen kulkiessa ko. suojaustason sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella viranomaisen erillishyväksyntään perustuen. 4) Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti.	1) 5 §:n 1 mom. 6 kohta 2) 5 §:n 1 mom. 6 kohta 3) 5 §:n 1 mom. 6 kohta 4) 5 §:n 1 mom. 6 kohta	1) IV liitteen 32-35 kohdat 2) 9 artiklan 4 kohta 10 artiklan 6 kohta, IV liitteen 25 kohta 3) IV liitteen 31 kohta 4) IV liitteen 16 ja 18-19 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasoilla IV-II vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Tietojenkäsittely-ympäristöön ei ole yhteenliitäntää hallintayhteyksille muiden suojaustasojen ympäristöistä ilman viranomaisen ko. suojaustasoille hyväksymää yhdyskäytäväratkaisua (vrt. I 01).
2) Ko. suojaustason hallintatyöasema kytketään laitteeseen/liittymään vain viranomaisen ko. suojaustasolle hyväksymän salausratkaisun (ks. I 12) kautta tilanteissa, joissa hallintaliikenne kulkee matalamman suojaustason ympäristön kautta.
3) Tilanteissa, joissa hallintaliikenne kulkee ko. suojaustason sisällä,
   a) ko. suojaustason hallintatyöasema kytketään laitteeseen/liittymään fyysisesti (esim. konsolikaapeli), tai
   b) ko. suojaustason hallintayhteyden liikennekanava on muuten luotettavasti fyysisesti suojattu (esim. teknisesti suojatun turva-alueen sisäiset kaapeloinnit), tai
   c) ko. suojaustason hallintatyöasema kytketään laitteeseen/liittymään matalamman tason salauksella (esim. SSH, HTTPS, SCP) suojatulla yhteydellä.
4) Laitteisiin/liittymiin sallitaan hallintayhteydenotot vähimpien oikeuksien periaatteen mukaisesti vain hyväksytyistä lähteistä.

I 04	*Yleistä* Laitteilla/liittymillä tarkoitetaan tässä järjestelmiä, joihin pitäisi olla hallintaoikeudet vain ylläpitäjillä tai vastaavilla. Tällaisia ovat tyypillisesti esimerkiksi palomuurit, reitittimet, kytkimet, langattomat tukiasemat, palvelimet, työasemat, ILO-hallintaliittymät ja Blade-runkojen hallintaliittymät. Hallintayhteyksien suojausten arvioinnissa tulisi huomioida erityisesti se, miltä osin ko. hallintayhteyden kautta pystytään vaarantamaan salassa pidettävät tiedot. Useimmat hallintayhteystavat mahdollistavat pääsyn salassa pidettävään tietoon joko suoraan (esimerkiksi tietokantaylläpito pääsee yleensä tarvittaessa tietokannan sisältöön) tai epäsuoraan (esimerkiksi verkkolaiteylläpito pystyy yleensä muuttamaan tietojärjestelmää suojaavia palomuurisääntöjä). Erityisesti tilanteissa, joissa hallintayhteys mahdollistaa suoran tai epäsuoran pääsyn salassa pidettävään tietoon, tulisi hallintayhteys ja siihen käytettävät päätelaitteet rajata lähtökohtaisesti samalle suojaustasolle, kuin mitä ko. tietojenkäsittely-ympäristökin. Matalamman tason ympäristön hallinta voi tietyissä erityistapauksissa olla mahdollista ylemmän suojaustason hallintaympäristöstä käsin, edellyttäen, että suojaustasojen rajoilla on viranomaisen ko. suojaustasoille hyväksymä yhdyskäytäväratkaisu, joka estää ylemmän suojaustason tietojen kulkeutumisen matalamman suojaustason ympäristöön. Ylemmän suojaustason ympäristön hallinta ei lähtökohtaisesti ole hallintaliikenteen turvallisuuskriittisestä luonteesta johtuen mahdollista matalamman suojaustason ympäristöistä. Ylemmän suojaustason ympäristöstä voidaan viranomaisen hyväksymän yhdyskäytäväratkaisun kautta tarjota joissain tapauksessa (read-only) valvontapääsy luokkaa matalamman suojaustason ympäristöön. Riittävän jäljitettävyyden toteuttamisessa voidaan hyödyntää ko. suojaustason sisällä esimerkiksi niin sanottua hyppykone-käytäntöä, jossa kaikki hallintatoimet toteutetaan ja kirjataan (lokitetaan) hyppykoneen kautta. Etähallinnan edellytyksiä on kuvattu tarkemmin vaatimuksessa I 24. *Muita lisätietolähteitä* Viestintäviraston ohje “Ohje hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista”; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 13; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 13.1.2; ISO/IEC 27002:2013 13.1.3; VAHTI 3/2010:n luku 16

I 05

Salassa pidettävien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - Langattomat verkot

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Langattomien verkkojen radiorajapintaa käsitellään kuin julkista verkkoa.	5 §:n 1 mom. 6 kohta	9 artiklan 4 kohta, IV liitteen 33 ja 35 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasoilla IV-II vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
Langattomien verkkojen kautta kulkeva tietoliikenne salataan viranomaisen ko. suojaustasolle hyväksymällä menetelmällä (I 12).

Yleistä Radiorajapinnan käyttö langattomissa verkkoyhteyksissä (esim. WLAN, 3G) tulkitaan poistumiseksi fyysisesti suojatun alueen ulkopuolelle. Toisin sanoen radiorajapinnan käyttö rinnastetaan julkisen verkon kautta liikennöinniksi, mikä tulisi ottaa huomioon erityisesti liikenteen salauksessa (vrt. I 12).

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 7; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0

Tietojärjestelmäturvallisuus

I 06

Vähimpien oikeuksien periaate - Pääsyoikeuksien hallinnointi

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä. 2) Salassa pidettävien tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan sekä tietojärjestelmien asianmukaisilla turvallisuusjärjestelyillä ja muilla toimenpiteillä.	1) 5 §:n 1 mom. 5 ja 6 kohdat 2) 5 §:n 1 mom. 6 kohta	1) IV liitteen 19 kohta 2) IV liitteen 16, 19 ja 32-35 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Järjestelmien käyttöoikeuksien hallintaan on nimetty vastuuhenkilö(t).
2) Järjestelmän käyttäjistä on olemassa lista.
3) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu.
4) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu.
5) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen.
6) Jokaisesta myönnetystä käyttöoikeudesta jää dokumentti (paperi tai sähköinen).
7) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti.
8) Tietojärjestelmissä salassa pidettävät tiedot on eritelty vähimpien oikeuksien periaatteen mukaisesti käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä tai jollain vastaavalla menettelyllä.
9) Tietojärjestelmissä ko. suojaustason tiedot pidetään erillään julkisista ja muiden suojaustasojen tiedoista, tai eri tason tietoja käsitellään korkeimman suojaustason mukaisesti.
10) Tietojärjestelmissä tarkastusoikeuden varaavien tiedon omistajien tiedot säilytetään toisistaan ko. suojaustasolle viranomaisen hyväksymällä menetelmällä eroteltuna.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-10 lisäksi toteutetaan seuraavat toimenpiteet:

11) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi.
12) Palvelimissa, työasemissa ja muissa tallennusvälineissä salassa pidettävät tiedot säilytetään viranomaisen ko. ympäristöön hyväksymällä menetelmällä salattuna (ks. I 12). Viranomainen voi hyväksyä tapauskohtaisesti myös korvaavan menettelyn, jossa salausvaatimus korvataan fyysisen ja loogisen pääsynhallinnan sekä tallennemedioiden hallinnan luotettavalla toteutuksella (ks. F 02, kohdat 6 ja 11). Huom: Korvaava menettely ei sovellu tilanteisiin, joissa salausta käytetään tarkastusoikeuden varaavien eri tiedon omistajien tietojen erotteluun.

I 06

Pääsyoikeuksien ajantasaisuudesta varmistuminen

Pääsyoikeuksien ajantasaisuudesta varmistuminen edellyttää yleensä sitä, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esim. 6 kuukauden välein. Lisäksi muutoksissa, kuten ylennyksissä, alennuksissa, työnkierron yhteydessä ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen/poistamiseen on oltava selkeä ja toimiva menettelytapa. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan pidettyä ajantasaisina. Tämä voi edelleen tarkoittaa sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen.

Tehtävien erottelu

Tehtävien erottelun riittävä toteutus riippuu merkittävästi kyseessä olevan järjestelmän käyttötapauksista. Useimmissa järjestelmissä riittävä tehtävien erottelu on toteutettavissa järjestelmän ylläpitoroolien (ja henkilöiden) ja lokien valvontaan osallistuvien roolien (ja henkilöiden) erottelulla toisistaan. Usein käytettynä valvontamekanismina on myös se, että kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän (”two man rule”).

Tarkastusoikeuden ottaminen huomioon teknisessä toteutuksessa

Salassa pidettävän tiedon omistajat varaavat usein itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti monihankeverkoissa ja muissa vastaavissa ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulisi varmistua siitä, että verkon/järjestelmän rakenne mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä.
Eri omistajien tietojen erottelumenetelmät jakautuvat kolmeen pääluokkaan.

a) Loogisen tason erotteluun (esim. palvelinten virtualisointi ja käyttöoikeuksin rajoitetut verkkolevykansiot) perustuvat menetelmät soveltuvat suojaustason IV tiedoille.
b) Luotettavaan loogiseen erotteluun (esim. hyväksytysti salatut virtuaalikoneet levyjärjestelmän asiakaskohtaisesti dedikoiduilla levyillä, ja tiedon/tietoliikenteen hyväksytty salaus yhteiskäyttöisillä verkkolaitteilla) perustuvat menetelmät soveltuvat suojaustasoille IV ja III.
c) Fyysisen tason erotteluun (dedikoidut fyysiset laitteet) perustuvat menetelmät soveltuvat suojaustasoille IV, III ja II.

Huom: Tietojen erotteluvaatimusta ei IV-tasolla sovelleta työasemiin tai muihin vastaaviin suppeisiin tietovarantoihin, edellyttäen, että käytössä on luotettavaksi arvioidut menetelmät kasautumisvaikutuksen ehkäisemiseksi (ks. I 19, kohta 3). Tarkastusoikeuden varaavien tiedon omistajien tietoja ei edellytetä eroteltavan myöskään tilanteissa, joissa kaikilta tiedon omistajilta on saatu kirjallinen erillishyväksyntä tarkastusoikeuden mahdollistamien riskien hyväksymisestä.

I 06

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 3; SANS Critical Security Controls (v5) / 12; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; Kansallisen turvallisuusviranomaisen ”Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”; ISO/IEC 27002:2013 6.1.2; ISO/IEC 27002:2013 9.1.1; ISO/IEC 27002:2013 9.1.2; ISO/IEC 27002:2013 9.2.1; ISO/IEC 27002:2013 9.2.2; ISO/IEC 27002:2013 9.2.3; ISO/IEC 27002:2013 9.2.4; ISO/IEC 27002:2013 9.2.5; ISO/IEC 27002:2013 9.2.6; ISO/IEC 27002:2013 12.5.1; VAHTI 2/2010:n luku 8.9; VAHTI 2/2010:n liitteen 5 luku 2.7

I 07

Monitasoinen suojaaminen - Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun alueen sisällä

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät tietojenkäsittely-ympäristön toimijoiden tunnistamiseen.	5 §:n 1 mom. 5 ja 6 kohdat, 14 §, 20 §	IV liitteen 16 ja 19 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.
2) Kaikki käyttäjät tunnistetaan ja todennetaan.
3) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestetty luotettavasti.
4) Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin aiheuttaa tunnuksen lukittumisen.
5) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä/sovelluksissa ole teknisesti mahdollista, vaaditaan sovitut ja dokumentoidut salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille.
6) Todennus tehdään vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, a) käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, b) käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-5 lisäksi toteutetaan seuraavat toimenpiteet:

7) Edellytetään vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta.
8) Päätelaitteet tunnistetaan teknisesti (laitetunnistus, 802.1X, tai vastaava menettely) ennen pääsyn sallimista verkkoon tai palveluun, ellei verkkoon kytkeytymistä ole fyysisen turvallisuuden menetelmin rajattu suppeaksi (esim. palvelimen sijoittaminen lukittuun laitekaappiin teknisesti suojatun viranomaisen ko. suojaustasolle hyväksymän turva-alueen sisällä).

I 07

Yleistä

Suojaustason IV ympäristöissä, joissa uhka palvelunestohyökkäyksen aiheuttamiseen (tunnusten lukitseminen esim. Internet-kytkentäisissä tunnistuspalveluissa) arvioidaan merkittäväksi, tunnuksen lukittuminen voidaan korvata jollain riskiä pienentävällä menettelyllä (esim. vastaamisen hidastamiseen, suodattamiseen tai väliaikaiseen lukitsemiseen perustuvat menettelyt). Suojaustasolla IV ei yleensä edellytetä päätelaitteen teknistä tunnistamista, mikäli käyttäjät tunnistetaan.

Suojaustasojen III ja II menetelmät vahvasta käyttäjätunnistuksesta ja päätelaitteen tunnistamisesta voidaan joissain tapauksissa toteuttaa siten, että tietojärjestelmään on mahdollista päästä vain tiukasti rajatusta fyysisesti suojatulta alueelta (yleensä teknisesti suojattu turva-alue, lukittu laitekaappi, tai vastaava), jonka pääsynvalvonnassa käytetään vahvaa, vähintään kahteen tekijään perustuvaa tunnistamista. Tällöin käyttäjän tunnistaminen tietojärjestelmässä voidaan järjestää käyttäjätunnus-salasana -parilla.

Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen ainakin siitä, että i) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), ii) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, iii) todennuksessa käytettävät tunnistamistiedot (todennuskredentiaalit) ovat aina salatussa muodossa jos ne lähetetään verkon yli, iv) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, v) todennusmenetelmä on suojattu brute force -hyökkäyksiä vastaan.

Muita lisätietolähteitä

BSI IT-Grundschutz-Catalogues - 13th version - 2013; SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 12; SANS Critical Security Controls (v5) / 1; SANS Critical Security Controls (v5) / 16; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 9.1.2; ISO/IEC 27002:2013 9.4.1; ISO/IEC 27002:2013 9.4.2; ISO/IEC 27002:2013 9.4.3

I 08

Vähimmäistoimintojen ja vähimpien oikeuksien periaate - Järjestelmäkovennus

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut. 2) Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. 3) Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.	5 §:n 1 mom. 6 kohta	IV liitteen 16, 18 ja 19 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

Verkon aktiivilaitteet

1) Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin.
2) Vain tarpeellisia verkkopalveluita on päällä ja nämä palvelut on rajattu vain tarpeellisiin verkkoliittymiin.
3) Verkkolaitteiden ohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
4) Hallinta ei ole mahdollista ilman käyttäjän tunnistamista ja todentamista.
5) Hallintayhteyksissä tulisi käyttää istuntojen aikakatkaisua.
6) Kovennukset pohjautuvat johonkin luotettavaksi arvioituun kovennusohjeeseen tai suositukseen.

Palvelimet, työasemat ja vastaavat

7) Tarjottavat (erityisesti verkko)palvelut on minimoitu ja rajattu vain välttämättömiin. On lisäksi käytössä verkkoliikenteen vain välttämättömään rajaava (host-based) palomuuriratkaisu.
8) Alusta sisältää vain järjestelmän tarvitsemia ohjelmistokomponentteja. Alustan komponenttien, prosessien (esim. palvelinprosessit), hakemistojen ja lisäohjelmien käyttöoikeudet on asetettu tarkoituksenmukaisiksi vähimpien oikeuksien periaatteen mukaisesti.
9) Käyttöjärjestelmään ja sovellusohjelmistoihin on asennettu tarpeelliset turvapäivitykset.
10) Järjestelmiin asennuksen yhteydessä automaattisesti luoduille tileille (esim. ”administrator” ja ”guest”) on oikeudet rajattu minimiin tai poistettu käytöstä.
11) Oletussalasanat on vaihdettu organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin.
12) Järjestelmä lukittuu automaattisesti, jos sitä ei käytetä vähään aikaan (esim. salasanasuojattu näytönsäästäjä aktivoituu 15 minuutin käyttämättömyyden jälkeen).
13) Käyttöoikeudet asetettu vähimpien oikeuksien periaatteen mukaisesti (vrt. I 06).

I 08

14) Käyttöjärjestelmän tunnettuja turvallisuusuhkia sisältävät automaattisen ohjelmakoodin suorituksen mahdollistavat ominaisuudet on kytketty pois päältä (erityisesti PDF-tiedostojen automaattinen esikatselu sekä ”autorun” ja ”autoplay”-toiminnallisuudet, sekä esimerkiksi USB- ja Firewire-laitteiden automaattisen käynnistymisen estäminen koneen ollessa lukittuna).
15) Ohjelmistot, erityisesti web-selaimet, PDF-lukijat, toimisto-ohjelmistot ja sähköpostiohjelmistot, ovat turvallisesti konfiguroituja.
Ohjelmistojen kovennuksissa tulisi huomioida erityisesti ajettavan koodin (esim. JavaScript sekä makrot) oletusarvoisen suorittamisen estäminen.
16) BIOS-asetuksiin pääsy on suojattu salasanalla (suojaustasolla IV erityisesti Naton turvallisuusluokitellun tiedon osalta)
17) Järjestelmän tukemia lisäturvallisuusominaisuuksia (esimerkiksi DEP/ASLR/Applocker/SELINUX) hyödynnetään.

Suojaustasoilla III-II vaatimus voidaan toteuttaa siten, että kohtien 1-17 lisäksi toteutetaan seuraavat toimenpiteet:

Verkon aktiivilaitteet

18) Tarpeettomat verkkopistokkeet ja muut vastaavat tietoliikenneyhteydet on poistettu käytöstä.

Palvelimet, työasemat ja vastaavat

19) käyttöjärjestelmät ja muut ohjelmistot konfiguroidaan siten, että päivitykset haetaan vain tähän tarkoitukseen tarkoitetuista lähteistä ja kaikki tarpeeton verkkoliikennöinti on poistettu käytöstä (tavoitteena tehokkaamman poikkeamien havainnointikyvyn mahdollistaminen)
20) BIOS-asetukset on asetettu turvallisuutta tehostaviksi ja asetusten muuttaminen on estetty valtuuttamattomilta käyttäjiltä. Salasanasuojauksen lisäksi:
a) On sallittu vain ensisijaiselta kovalevyltä käynnistys. b) Tarpeettomat palvelut ja portit on poistettu käytöstä.

Yleistä

Järjestelmillä tarkoitetaan palvelimia, työasemia, verkon aktiivilaitteita ja vastaavia. Verkon aktiivilaitteilla tarkoitetaan tässä yhteydessä palomuureja, reitittimiä, kytkimiä, langattomia tukiasemia ja vastaavia laitteita/järjestelmiä. Koventamisella tarkoitetaan yleisesti järjestelmän asetusten muuttamista siten, että järjestelmän haavoittuvuuspinta-alaa saadaan pienennettyä. Järjestelmissä on yleisesti otettava käyttöön vain käyttövaatimusten kannalta olennaiset toiminnot, laitteet ja palvelut. Vastaavasti esimerkiksi automaattisille prosesseille on annettava vain ne tiedot, etuoikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä, jotta rajoitetaan onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja. Palvelinten, työasemien ja vastaavien riittävän kovennuksen voi toteuttaa esimerkiksi USGCB:tä tai vastaavaa tasoa (esim. SSLF Microsoft-ympäristöissä) mukaillen. Mikäli salassa pidettävän tiedon käsittelyyn käytetään verkkotulostimia, puhelinjärjestelmiä tai vastaavia, edellä mainittuja periaatteita tulisi soveltaa myös näihin järjestelmiin.

Korvaavia menetelmiä

Mikäli esimerkiksi verkkolaitteen hallinta ei ole teknisesti mahdollista käyttäjän yksilöivällä käyttäjätunnuksella, käyttäjän yksilöivä tunnistaminen voidaan järjestää käyttösäännöillä esimerkiksi siten, että salasanaan pääsy edellyttää kahden henkilön osallistumista. Mikäli ympäristön koko on suurehko, todennuksen järjestämiseen suositellaan kahdennettujen AAA-palvelimien (erityisesti TACACS+, RADIUS, tai Kerberos) hyödyntämistä.

I 08

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 3; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 11; SANS Critical Security Controls (v5) / 13; SANS Critical Security Controls (v5) / 5; SANS Critical Security Controls (v5) / 6; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; The United States Government Configuration Baseline (USGCB); NATO Best Practice Configuration Guidance; IASE Security Technical Implementation Guides (STIGs); NIST Special Publications (800 Series); Microsoft Security Compliance Manager; Apache Security Tips; ModSecurity; Cisco Security Configuration; VAHTI 3/2012:n luku 4.2.1; VAHTI 3/2010:n luku 7

I 09

Monitasoinen suojaaminen - Haittaohjelmasuojaus

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.	5 §:n 1 mom. 6 kohta	IV liitteen 8, 9, 16, 18, 19, 21 ja 22 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartunnoille.
2) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä.
3) Torjuntaohjelmistot tuottavat havainnoistaan lokitietoja ja hälytyksiä.
4) Haittaohjelmatunnisteet (ja vast.) päivittyvät säännöllisesti.
5) Käyttäjiä on ohjeistettu haittaohjelmauhista ja organisaation tietoturvaperiaatteiden mukaisesta toiminnasta.
6) Haittaohjelmahavaintoja sekä hälytyksiä seurataan säännöllisesti ja niihin reagoidaan.
7) Organisaatiossa suodatetaan haittaliikennettä vähintään sähköpostin ja WWW-liikenteen yhdyskäytävissä.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-7 lisäksi toteutetaan seuraavat toimenpiteet:
8) Arvioidaan tarve järjestelmien USB-porttien ja vastaavien liityntöjen käytölle.
9) Tilanteissa, joissa liityntöjen käytölle ei ole kriittistä tarkastelua kestävää perustetta, liitynnät poistetaan käytöstä.
10) Tilanteissa, joissa liityntöjen käytölle on kriittistä tarkastelua kestävät perusteet, arvioidaan tapauskohtaisesti edellytykset ja ehdot, minkä mukaisia laitteistoja ja välineitä (esim. USB-muisteja) järjestelmään voidaan kytkeä.

I 09

Yleistä

Torjuntaohjelmistot voidaan jättää asentamatta ympäristöissä, joihin haittaohjelmien pääsy on muuten estetty (esim. järjestelmät, joissa ei ole mitään tiedon tuonti-/vientiliittymiä, tai joissa tarkasti rajatuissa liittymissä toteutetaan siirrettävän tiedon luotettava validointi/sanitointi).

Julkisista verkoista eristetyt ympäristöt

Järjestelmissä, joita ei kytketä julkiseen verkkoon, haittaohjelmatunnisteiden päivitys voidaan järjestää esimerkiksi käyttämällä hallittua suojattua päivitysten-hakupalvelinta, jonka tunnistekanta pidetään ajan tasalla esimerkiksi erillisestä Internetiin kytketystä järjestelmästä tunnisteet käsin siirtämällä (esim. kerran vuorokaudessa), tai tuomalla tunnisteet hyväksytyn yhdyskäytäväratkaisun (ks. I 01) kautta. Huom: Päivitysten eheydestä varmistumiseen tulisi olla menettelytapa (lähde, tarkistussummat, allekirjoitukset, jne.).

USB-porttien ja vastaavien liityntöjen käytön tapauskohtaisiin ehtoihin voi sisältyä esimerkiksi, että järjestelmään voi kytkeä vain erikseen määritettyjä luotettavaksi todennettuja muistitikkuja (ja vastaavia), joita ei kytketä mihinkään muuhun järjestelmään. Tapauskohtaisiin ehtoihin voi sisältyä esimerkiksi järjestely, jossa vain organisaation tietohallinnon (tai vast.) jakamia muistivälineitä voidaan kytkeä organisaation järjestelmiin, ja että kaikkien muiden muistivälineiden kytkeminen on kielletty ja/tai teknisesti estetty.

Tilanteissa, joissa on tarve tuoda tietoa ei-luotetuista järjestelmistä jotain muistivälinettä käyttäen, tapauskohtaisiin ehtoihin sisältyy usein myös määrittelyt siitä, millä menetelmillä pienennetään tämän aiheuttamaa riskiä. Menetelmänä voi esimerkiksi olla ei-luotetusta lähteestä tulevan muistivälineen kytkeminen eristettyyn tarkastusjärjestelmään, jonne siirrettävä tieto siirretään, ja josta siirrettävä tieto viedään edelleen luotettuun järjestelmään erillistä muistivälinettä käyttäen. Tällaisissa järjestelyissä huomioidaan yleensä suojaustasolla III vähintään muistialueen tarkastaminen, ja suojaustasosta II lähtien myös muistivälineen kontrolleritason räätälöinnin uhat.

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 5; SANS Critical Security Controls (v5) / 17; SANS Critical Security Controls (v5) / 2; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 12.2.1; VAHTI 2/2010:n liitteen 5 luku 2.8

I 10

Monitasoinen suojaaminen - Turvallisuuteen liittyvien tapahtumien jäljitettävyys

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen.	5 §:n 1 mom. 6 kohta, 20 §	IV liitteen 16 kohta, III liitteen 18 ja 21 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen.
2) Keskeiset tallenteet säilytetään vähintään 6 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa.
3) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta).
4) Toimintaan on jalkautettu kirjallinen lokien keräys-, luovutus-, hälytys- ja seurantapolitiikka/-ohje, joka on muodostettu ottaen huomioon toiminnan vaatimukset.

Suojaustasoilla III-II vaatimus voidaan täyttää siten, että kohtien 1-4 lisäksi toteutetaan seuraavat toimenpiteet:
5) Keskeiset tallenteet säilytetään vähintään 2-5 vuotta, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa.
6) Lokitiedot varmuuskopioidaan säännöllisesti.
7) Samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot on synkronoitu sovitun ajanlähteen kanssa.
8) On olemassa menetelmä lokien eheyden (muuttumattomuuden) varmistamiseen.
9) Syntyneiden lokitietojen käytöstä ja käsittelystä muodostuu merkinnät.

Yleistä

Keskeisiä tallenteita ovat tyypillisesti kirjautumistietojen keskeisten verkkolaitteiden ja palvelinten lokitiedot. Myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein. Kattavuusvaatimuksen voi useimmin toteuttaa siten, että varmistaa, että ainakin työasemien, palvelinten, verkkolaitteiden (erityisesti palomuurien, myös työasemien sovellusmuurien) ja vastaavien lokitus on päällä. Verkkolaitteiden lokeista tulisi myös pystyä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. Tapahtumalokeja olisi syytä kerätä järjestelmän toiminnasta, käyttäjäaktiviteeteista, turvaan liittyvistä tapahtumista ja poikkeuksista. Eräs suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot keskitetylle ja vahvasti suojatulle lokipalvelimelle, jonka tiedot varmuuskopioidaan säännöllisesti.

I 10	Toteutus työasemissa/palvelimissa vaatii usein lokituksen päälle laittamista ja oletusarvojen muuttamista säilytysajan/-tilan suhteen. Esimerkiksi joissain Windows-ympäristöissä tämä tarkoittaa yleensä valvontakäytäntöihin (Audit Policy) vähintään seuraavien päälle laittamista (epäonnistuneet ja onnistuneet tapahtumat): ■ Valvo tilien kirjautumistapahtumia (Audit account logon events) ■ Valvo tilienhallintaa (Audit account management) ■ Valvo kirjautumistapahtumia (Audit logon event) ■ Valvo käytäntöjen muutoksia (Audit policy change) ■ Valvo oikeuksien käyttöä (Audit privilege use) ■ Valvo järjestelmätapahtumia (Audit system events) Toteutus työasemissa/palvelimissa edellyttää usein myös sen huomioon ottamista, että lokien säilytystilaa ja -aikaa kasvatetaan riittäviksi. Suositus: lokeille varataan tilaa ympäristössä riittäväksi arvioitava määrä. Riittävän ajan määritys voidaan tehdä esimerkiksi siten, että arvioidaan yhden kuukauden lokikertymän perusteella riittävä tila vaadittavalle säilytysaikajaksolle. Huom: tilalle on syytä varata reilusti ”puskuria”, sillä poikkeavat tilanteet ja myös tietyt hyökkäystyypit kasvattavat lokimäärää merkittävästi. *Muita lisätietolähteitä* SANS Critical Security Controls (v5) / 14; SANS Critical Security Controls (v5) / 16; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2013 12.4.1; ISO/IEC 27002:2013 12.4.2; ISO/IEC 27002:2013 12.4.3; ISO/IEC 27002:2013 12.4.4; ISO/IEC 27002:2013 18.1.3; VAHTI 3/2009

I 11

Monitasoinen suojaaminen - Poikkeamien havainnointikyky ja toipuminen

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne.	5 §:n 1 mom. 6 kohta, 20 §	IV liitteen 16 kohta

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV-II vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Verkkoliikenteen normaali tila (liikennemäärät, protokollat ja yhteydet) on tiedossa.
2) On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan.
3) On olemassa menettely, jolla kerätyistä tallenteista (vrt. I 10) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan).
4) On olemassa menettely havaituista poikkeamista toipumiseen.

Yleistä

Verkkoliikennöinnin osalta tarkkailuun ja havaitun hyökkäyksen vaikutusten rajoittamiseen on useita soveltuvia toteutusmahdollisuuksia keskeisten verkkosolmujen tasolla tapahtuvasta tarkastelusta aina työasema-/palvelinkohtaisiin sensoreihin sekä näiden yhdistelmiin. Riippumatta käytetyistä verkkolaitteista ja toimittajista, verkkotason havainnointikyvyn käytännön toteutus edellyttää tyypillisesti verkkoliikenteen normaalin tilan tuntemista. Suojaustasolla IV verkkoliikennetason havainnointikyvyn tulisi kattaa erityisesti verkon/kohteen ulkorajan, ja III-tasosta lähtien ulkorajan yhdyskäytäväratkaisun sekä verkon/kohteen sisäpuolen liikennöinnin.

Hyökkäyksen/väärinkäyttöyrityksen havaitseminen edellyttää useimmissa ympäristöissä käytännössä automatisoitujen havainnointi- ja hälytystyökalujen käyttöä. Lokitietojen manuaalinen tarkastelu on yleensä riittävä vain ympäristöissä, joissa lokimassat ovat hyvin pieniä ja lokien tarkasteluun on osoittaa riittävät henkilöresurssit.

Tietojenkäsittely-ympäristön palauttaminen takaisin suojattuun tilaan kohtuullisessa ajassa edellyttää yleensä suunniteltuja, kuvattuja, koulutettuja sekä harjoiteltuja prosesseja sekä teknisiä menetelmiä.

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 14; SANS Critical Security Controls (v5) / 16; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 12.4.1; ISO/IEC 27002:2013 13.1.1; ISO/IEC 27002:2013 16.1.4; ISO/IEC 27002:2013 16.1.5; VAHTI 3/2009

I 12

Tietoturvallisuus-tuotteiden arviointi ja hyväksyntä - Salausratkaisut

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Viranomainen on hyväksynyt käytetyt salausratkaisut (ja -tuotteet) ko. suojaustasolle ko. käyttöympäristössä salassa pidettävien tietojen luvattoman paljastumisen ja muuntelun estämiseksi.	5 §:n 1mom. 6 kohta, 16 §, 19 §	10 artiklan 6 kohta, IV liitteen 25 kohta

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV-II vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) On hankittu ko. suojaustasolle a) viranomaisen hyväksymät salausratkaisut ja käytetään niitä hyväksynnän yhteydessä määritellyn käyttöpolitiikan ja -asetusten mukaisesti, tai b) viranomaisen myöntämät tapauskohtaiset hyväksynnät ja käyttöpolitiikat-/asetukset sellaisille salausratkaisuille, joilla ei ollut entuudestaan voimassaolevaa hyväksyntää.
2) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. Salausavaintenhallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Prosessit edellyttävät vähintään a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, f) valtuuttamattomien avaintenvaihtojen estämisen.

Yleistä

Salaustuotteiden arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salaustuotteen oikeellisesta toiminnasta varmistumisen lisäksi huomioidaan muun muassa salaustuotteen käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa merkittävästi tilanteeseen, jossa salausta käytetään liikennöintiin hallitun fyysisen tilan sisällä (esimerkiksi suojaustason II aineiston siirto kahden suojaustason II fyysisen tilan välillä suojaustason III fyysisen turva-alueen läpi). Muihin salaustuotteiden arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi ko. käyttötapauksen vaatimukset tiedon salassapitoajalle ja eheydelle.
Usean kansainvälisen turvallisuusviranomaisen salaustuotehyväksynnät edellyttävät tuotteelta erityisesti näyttöä sen oikeellisesta toiminnasta, ja lisäksi tiettyjen erityisvaatimusten (esim. lähdekoodin luovutus ja tarkastus, peukalointi- ja hajasäteilysuojaukset) täyttämistä. Puhtaasti ohjelmistopohjaiset salausratkaisut ovat tyypillisesti hyväksyttävissä IV- ja joissain tilanteissa erityisehdoilla myös III-tasoille. II-tasolle ja useimmin myös III-tasolle edellytetään tyypillisesti enemmän alustan luotettavuudelta.

Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avainhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään.

Muita lisätietolähteitä

Euroopan unionin neuvoston hyväksyttyjen salaustuotteiden lista; Naton hyväksyttyjen salaustuotteiden lista; Kansallisen salaustuotteiden hyväksyntäviranomaisen hyväksyttyjen salausratkaisujen lista; Kansallisen turvallisuusviranomaisen ”Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”, SANS Critical Security Controls (v5) / 17; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 10.1.1; ISO/IEC 27002:2013 10.1.2; ISO/IEC 27002:2013 18.1.5; VAHTI 3/2010:n luku 12

I 13

Monitasoinen suojaaminen koko elinkaaren ajan - Ohjelmistoilla toteutettavat pääsynhallinta-toteutukset

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Tietojenkäsittely-ympäristön turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimet, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu. 2) Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi ja havaitsemiseksi tietojenkäsittely-ympäristössä järjestetään luotettavat menettelyt ohjelmistoilla toteutettavien pääsynhallintatoteutusten turvallisuudesta varmistumiseksi.	5 §:n 1 mom. 6 kohta, 6 §	1) IV liitteen 8, 9, 10, 16, 19 ja 33 kohdat 2) IV liitteen 10 ja 19 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV-III vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Palvelun/sovelluksen/järjestelmän toteutukselle edellytetään turvallisen ohjelmoinnin periaatteiden täyttämistä, ja toimittajilta vaaditaan selvitys, miten turvallisen ohjelmoinnin periaatteet on käytännössä huomioitu tuotekehityksessä;
2) Palvelun/sovelluksen/järjestelmän toimittaja sitoutetaan turvallisuuspuutteiden korjaamiseen palvelun/sovelluksen elinkaaren ajalle, tai on olemassa jokin muu menettely, jolla havaitut turvallisuuspuutteet pystytään korjaamaan; ja
3) Palvelun/sovelluksen/järjestelmän rajapintojen on kestettävä yleiset hyökkäysmenetelmät ilman, että palvelussa/sovelluksessa käsiteltävien salassa pidettävien tietojen luottamuksellisuus tai eheys vaarantuu.

Suojaustasolla II vaatimus voidaan täyttää siten, että kohtien 1-3 lisäksi toteutetaan seuraava toimenpide:

4) Kaikki ko. palvelun/sovelluksen/järjestelmän turvallisuuteen oleellisesti vaikuttava koodi on tarkastettavissa (esim. mahdolliset takaportit, turvattomat toteutukset).

Yleistä

Vaatimusta sovelletaan erityisesti tilanteisiin, joissa salassa pidettävän tiedon keskeisen pääsynhallintatoteutuksen turvallisuus nojaa ohjelmistoon. Useimmin tilanne esiintyy räätälöidyissä asianhallintajärjestelmissä, web-sovelluksissa ja vastaavissa. Suojaustasolla IV vaatimusta sovelletaan tilanteissa, joissa tiedon suojaamiseen vaikuttava palvelu/sovellus/järjestelmä on saavutettavissa ei-luotetusta verkosta (esim. Internet), tai palvelussa/sovelluksessa/järjestelmässä ilmenee kasautumisvaikutus (tyypillisesti esim. asianhallinta- tai dokumentinsäilöntäjärjestelmät). Suojaustasosta III lähtien vaatimusta sovelletaan myös luotetuista verkoista käsin saavutettaviin palveluihin.

I 13

Ohjelmistotoimittajalta voidaan edellyttää esimerkiksi seuraavia:

1) Ohjelmistokehittäjien riittävä tietoturvatietous on varmistettu.
2) Ohjelmistokehityksen aikana on suoritettu tietoturvauhka-analyysi ja havaitut riskit on joko kontrolloitu tai nimenomaisesti hyväksytty.
3) Rajapinnat (ainakin ulkoiset) on testattu viallisilla syötteillä sekä suurilla syötemäärillä.
4) Riippuen ohjelmointiympäristöstä, helposti ongelmia aiheuttavien funktioiden ja rajapintojen käyttöön on määritelty politiikka ja sitä valvotaan (esim. Microsoftilla on listat kielletyistä funktioista).
5) Arkkitehtuuri ja lähdekoodi on katselmoitu.
6) Ohjelmakoodi on tarkastettu automatisoidulla staattisella analyysillä.
7) Ohjelmakoodin versionhallinnan ja kehitystyökalujen eheys on varmistettu.

Hankittavista ohjelmistoista suositellaan yleensä edellytettäväksi myös dokumentaatio, josta selviää ainakin sovelluksen käyttämät verkkoportit sekä riippuvuudet muista ohjelmistokomponenteista (esimerkiksi ohjelmiston käyttämät kirjastot). Suotavaa on myös, että

1) sovellukset käyttävät pientä määrää määriteltyjä portteja,
2) dynaamisia portteja käyttävät sovellukset käyttävät vain pientä porttiavaruutta, ja
3) ohjelmistot eivät vaadi laajoja käyttöoikeuksia toimiakseen (ts. ohjelmistojen on toimittava ”peruskäyttäjän» oikeuksilla).

Sovellusten suodatustoiminnallisuutta voidaan tukea ja/tai toteuttaa myös esimerkiksi sovelluspalomuureilla (WAF, web application firewall), vrt. I 08.

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 6; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Development and Implementation of Secure Web Applications; CPNI - Security Questions to Ask Your Vendor; OWASP Top Ten Project; OWASP Application Security Verification Standard Project; CWE/SANS TOP 25 Most Dangerous Software Errors; The Building Security In Maturity Model; Software Assurance Maturity Model; ModSecurity; ISO/IEC 27002:2013 14.1.1; ISO/IEC 27002:2013 14.1.2; ISO/IEC 27002:2013 14.1.3; ISO/IEC 27002:2013 14.2.8; ISO/IEC 27002:2013 14.2.9; VAHTI 1/2013

I 14

Monitasoinen suojaaminen - Hajasäteily (TEMPEST)

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Turvatoimia toteutetaan salassa pidettäviin tietoihin liittyvässä tietojenkäsittely-ympäristössä viranomaisen ko. suojaustasolle hyväksymillä menetelmillä niin, että tahattomat sähkömagneettiset vuodot eivät vaaranna tietoja (TEMPEST-turvatoimet). Nämä turvatoimet on suhteutettava tiedon hyväksikäytön riskiin ja suojaustasoon.	16 §, 5 §:n 1 mom. 6 kohta	10 artiklan 5 kohta

Lisätietoja

Yleistä

Suojaustasolla IV ei ole erityisiä vaatimuksia. Suojaustasolla III-II raja-arvot ylittävän hajasäteilyn osalta suojautuminen toteutetaan ko. suojaustasolle viranomaisen hyväksymillä menettelyillä.

EU:n turvallisuusluokitellun tiedon tapauksessa viranomaisena toimii kansallinen TEMPEST-viranomainen (NTA, National TEMPEST Authority, Suomessa Viestintäviraston NCSA-toiminto). Suojaustason III osalta on laajemmat mahdollisuudet hyväksyä korvaavia menettelyjä riittävän suojauksen saavuttamiseksi.

Kohteen hajasäteilyn vastatoimien riittävyys voidaan todentaa vyöhykemittauksella (facility zoning measurement) tai suojatun tilan mittauksella (shielded enclosure measurement).

Muita lisätietolähteitä

Viestintäviraston ohje ”Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet”; BSI IT-Grundschutz-Catalogues - 13th version - 2013; ISO/IEC 27002:2013 11.2.3; VAHTI 2/2010:n luku 4.4; VAHTI 3/2012:n luku 3.2; VAHTI 2/2013:n luku 3.1.3

I 15

Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä - Aineiston sähköinen välitys

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Kun salassa pidettävää aineistoa siirretään hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolella, aineisto/liikenne salataan viranomaisen ko. suojaustasolle hyväksymällä menetelmällä. 2) Kun salassa pidettävää aineistoa siirretään hyväksyttyjen fyysisesti suojattujen alueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella viranomaisen erillishyväksyntään perustuen.	1) 5 §:n 1mom. 6 kohta, 19 § 2) 5 §:n 1 mom. 6 kohta	1) 9 artiklan 4 kohta 2) IV liitteen 31 kohta

Lisätietoja

Toteutusesimerkki

Suojaustasoilla IV-II vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Siirrettäessä salassa pidettävää aineistoa ko. suojaustasolle hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolella verkon kautta tulee ottaa huomioon I 21 ja I 12.
2) Tilanteissa, joissa salassa pidettävää aineistoa siirretään fyysisesti suojattujen alueiden sisäpuolella,
   a) ko. suojaustason liikennekanava on fyysisesti suojattu (esimerkiksi kaapelointi, joka kulkee kokonaisuudessaan suppean, esimerkiksi vain yhden huoneen kattavan ko. suojaustason fyysisesti suojatun alueen sisällä), tai
   b) aineisto suojataan viranomaisen erillishyväksyntään perustuen matalamman tason salauksella (esim. HTTPS).

Yleistä

Kattaa puhelimen, telekopion (faksi), sähköpostin, pikaviestimet ja muut vastaavat tietoverkon kautta toimivat tiedonsiirtomenetelmät. Salassa pidettävää tietoa sisältävien tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) suojaamisperiaatteet kuvataan vaatimuksessa I 22.

Radiorajapinnan käyttö langattomissa verkkoyhteyksissä (esim. WLAN, 3G) tulkitaan poistumiseksi fyysisesti suojatun alueen ulkopuolelle. Langattomien verkkojen radiorajapintaa tulisi toisin sanoen käsitellä kuin julkista verkkoa. Vrt. I 05.

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 15; SANS Critical Security Controls (v5) / 17; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; Kansallisen turvallisuusviranomaisen ”Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”; ISO/IEC 27002:2013 11.2.3; ISO/IEC 27002:2013 13.2.1; ISO/IEC 27002:2013 13.2.3; VAHTI 3/2010:n luku 12

I 16

Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä - Aineiston välitys postilla ja kuriirilla

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojen siirtämisessä yksiköiden ja tilojen välillä fyysisesti suojattujen alueiden ulkopuolella on noudatettava seuraavaa: 1) Yleisenä sääntönä on, että salassa pidettävät tiedot siirretään tietoverkon yli sähköisesti viranomaisen hyväksymillä salaustuotteilla suojattuna. 2) Jos edellä mainittua menettelyä ei käytetä, salassa pidettävät tiedot kuljetetaan joko a) viranomaisen hyväksymillä salaustuotteilla suojatuilla sähköisillä välineillä (kuten USB-muistitikut, CD-levyt, kiintolevyt); tai b) kaikissa muissa tapauksissa, viranomaisen antamia ohjeita noudattaen.	5 §:n 1 mom. 6 kohta, 6 §, 18 §	9 artiklan 4 kohta, III liitteen 28-41 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasolla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Aineisto pakataan suljettavaan kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää suojaustasosta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän salassa pidettävää aineistoa (kirjekuoren tai vastaavan on oltava läpinäkymätön).
2) Aineisto toimitetaan kotimaassa tavallisena postina, kirjattuna kirjeenä tai viranomaisen ko. suojaustasolle hyväksymän kuriirimenettelyn mukaisesti. Ulkomaille toimitus postin välityksellä vain viranomaisen erillishyväksyntään pohjautuen.
3) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä.
4) Organisaatiossa on tunnistettu vaatimukset ja toteutettu menettelyt erityissuojattavien tietoaineistojen (esimerkiksi salausavaimet) välittämiseksi.

Suojaustasolla III vaatimus voidaan täyttää siten, että kohdan 4 lisäksi toteutetaan seuraavat toimenpiteet:

5) Aineisto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää suojaustasosta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän salassa pidettävää aineistoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä).
6) Aineisto toimitetaan kotimaassa viranomaisen erillishyväksyntään pohjautuen kirjattuna kirjeenä tai viranomaisen ko. suojaustasolle hyväksymän kuriirimenettelyn mukaisesti. Ulkomaille toimitus postin välityksellä voi tapahtua vain viranomaisen erillishyväksyntään pohjautuen.
7) Organisaation sisäiseen postin käsittelyketjuun kuuluu vain hyväksyttyä turvallisuusselvitettyä henkilöstöä.

Suojaustasolla II vaatimus voidaan täyttää siten, että kohtien 4 ja 7 lisäksi toteutetaan seuraavat toimenpiteet:

8) Aineisto pakataan suljettavaan kaksinkertaiseen kirjekuoreen tai vastaavaan. Pakkauksen ulkokuoressa ei saa olla merkintää suojaustasosta eikä pakkaus saa ulkoisesti muuten paljastaa sen sisältävän salassa pidettävää aineistoa (kirjekuorien tai vastaavien on oltava läpinäkymättömiä). Sisäkuoren on oltava sinetöity. Vastaanottaja on ohjeistettava tarkistamaan sinetöinnin eheys ja ilmoitettava välittömästi, mikäli eheyden vaarantumista epäillään.
9) Aineisto toimitetaan kotimaassa ja ulkomaille viranomaisen ko. suojaustasolle hyväksymän kuriirimenettelyn mukaisesti.

I 16	*Yleistä* Aineistot voidaan toimittaa perille myös henkilökohtaisesti, edellyttäen että aineistot kuljetetaan fyysisesti suojattujen alueiden välillä ko. suojaustason mukaisesti (kuvattu yksityiskohtaisemmin I 22:ssa.) Osaa kansainvälisistä tai kansallisista suojaustason III aineistoista ei välitetä koskaan postin välityksellä, hyväksyttävät menettelyt tarkistettava viranomaiselta tapauskohtaisesti. Esimerkiksi Naton CONFIDENTIAL-tason selväkielistä aineistoja ei lähetetä postitse edes kirjattuna, vaan lähetys toimitetaan perille joko henkilökohtaisesti tai viranomaisen hyväksymän kuriirimenettelyn välityksellä. Tarvittavia ohjeita antaa kansallinen turvallisuusviranomainen. Mikäli käytetään tiedon suojaustasolle hyväksyttyä salausta, voidaan ko. suojaustason ympäristössä salattu ja tietovälineelle (esim. CD-ROM) siirretty salattu aineisto toimittaa sekä Suomen sisällä että ulkomaille vapaavalintaisella (posti, kaupallinen kuriiri, henkilökuriiri, sotilaskuriiri, tai vast.) menettelyllä. *Muita lisätietolähteitä* BSI IT-Grundschutz-Catalogues - 13th version - 2013; Kansallisen turvallisuusviranomaisen ”Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje”; ISO/IEC 27002:2013 13.2.1

I 17

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Salassa pidettävien tietojen jäljentäminen - Tulostus ja kopiointi

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Suojaustaso IV-III 1) Jäljennöksiin ja käännöksiin sovelletaan alkuperäistä asiakirjaa koskevia turvatoimia. *Suojaustaso II* Kohdan 1 lisäksi 2) Suojaustason II aineiston kopiot on luetteloitava.	1) 5 §:n 1 mom. 6 kohta, 6 §, 13 §, 16 §, 17 § 2) 17 §	1) III liitteen 27 kohta, 9 artiklan 1 kohta, 7 artiklan 1 kohta 8 artiklan 5 kohta 2) III liitteen 18 ja 19 kohdat

Lisätietoja

Toteutusesimerkki:

Suojaustasoilla IV-III vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:
1) Kopioita käsitellään kuten alkuperäistä asiakirjaa.
2) Kopion voi luovuttaa edelleen vain henkilölle, jolla on käsittelyoikeus aineistoon ja tarve tietosisältöön.
3) Kopion/tulosteen saa ottaa vain ko. suojaustason vaatimukset täyttävällä laitteella.

Suojaustasolla II vaatimus voidaan täyttää siten, että kohtien 1-3 lisäksi toteutetaan seuraava toimenpide:
4) Kopiointi merkitään diaariin/rekisteriin tai luetteloidaan jollakin muulla vastaavalla menettelyllä.

Yleistä

Tulostimet ja kopiokoneet tulkitaan tietojärjestelmiksi ja niiden tulisi siten täyttää ko. suojaustason vaatimukset sekä teknisen, fyysisen että hallinnollisen tietoturvallisuuden osalta.

Muita lisätietolähteitä

BSI IT-Grundschutz-Catalogues - 13th version - 2013; VAHTI 2/2010:n luku 8.4

I 18

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Turvallisuus-tarkoituksia varten tapahtuva salassa pidettävien tietojen kirjaaminen

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Suojaustaso IV 1) Tietojenkäsittely-ympäristössä toteutetaan hallinnolliset ja tekniset toimenpiteet, jotka koskevat salassa pidettävien tietojen valvomista koko niiden elinkaaren ajan, jotta autetaan estämään ja havaitsemaan tällaisten tietojen tahallinen tai tahaton vaarantuminen tai katoaminen. *Suojaustaso III-II* Kohdan 1 lisäksi 2) Salassa pidettävää tietoa käsitteleville organisaatioyksiköille on määritelty kirjaamo/rekisteröintipiste. Kirjaamot/rekisteröintipisteet on perustettu fyysisille ko. suojaustason vaatimukset täyttäville turva-alueille. 3) Salassa pidettävä tieto kirjataan/rekisteröidään sille tarkoitetuissa kirjaamoissa/rekisteröintipisteissä, kun aineisto saapuu organisaatioyksikköön tai lähtee siitä. 4) Asiakirjojen käsittely kirjataan sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai asiakirjaan.	1) 20 §, 5 §:n 1 mom. 6 ja 7 kohdat, 6 §, 14 §, 15 §, 17 § 2) 20 §, 5 §:n 1 mom. 6 ja 7 kohdat, 6 §, 14 §, 15 §, 17 § 3) 20 §, 5 §:n 1 mom. 6 ja 7 kohdat, 6 §, 14 §, 15 §, 17 § 4) 20 §	1) III liitteen 1 kohta 2) III liitteen 17 kohta 3) 9 artiklan 2 kohta, III liitteen 18, 19, 21 kohdat 4) IV liitteen 16 kohta, III liitteen 18 ja 21 kohdat

Lisätietoja

Yleistä

Kirjaamisella/rekisteröinnillä tarkoitetaan sellaisten menettelyjen soveltamista, joilla rekisteröidään aineiston elinkaari, mukaan lukien sen jakelu ja hävittäminen. Jos kyseessä on tietojärjestelmä, kirjaamismenettelyt voidaan suorittaa järjestelmän omien prosessien avulla. Suojaustasolla IV turvallisuustarkoituksia varten tapahtuvaa kirjaamista ei edellytetä, ellei käsitellä suojaustasoon IV kuuluvia arkaluonteisia henkilötietoja tai biometrisiä tietoja sisältäviä henkilörekisteriin talletettuja aineistoja.

Aineiston elinkaaren rekisteröinnin käytännön toteutukset edellyttävät tyypillisesti muun muassa tapahtumien jäljitettävyydestä varmistumista. Käsiteltäessä salassa pidettävää tietoa tietojärjestelmällä, tulisi erityisesti ottaa huomioon käyttäjien tunnistaminen ja todentaminen (vrt. I 07) sekä tilivelvollisuuden (accountability) toteuttaminen (lokitus, vrt. I 10) luotettavasti.

Muita lisätietolähteitä

BSI IT-Grundschutz-Catalogues - 13th version - 2013; SANS Critical Security Controls (v5) / 14; SANS Critical Security Controls (v5) / 16; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0

I 19	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan –Salassa pidettävää tietoa sisältävien tietoaineistojen hävittäminen	*Suojaustaso IV* 1) Ei-sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. 2) Sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. 3) Tietojärjestelmien käytön yhteydessä syntyvät tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti, jolleivät ne poistu tietojärjestelmästä automaattisesti. *Suojaustaso III* Kohtien 1-3 lisäksi 4) Sekä kirjaajan että todistajan, jos jälkimmäisen läsnäoloa vaaditaan, on allekirjoitettava hävittämistodistus, joka tallennetaan kirjaamoon/rekisteröintipisteeseen. Kirjaamon/rekisteröintipisteen on säilytettävä aineistojen hävittämistodistukset vähintään viiden vuoden ajan. *Suojaustaso II* Kohtien 1-4 lisäksi 5) Aineiston hävittäminen on suoritettava todistajan läsnä ollessa. Todistajalla on oltava vähintään hävitettävän aineiston turvallisuusluokkaa vastaava turvallisuusselvitys.	1) 6 §, 21 § 2) 6 §, 21 § 3) 6 §, 21 § 4) 5) 6 §, 21 §	1) II liitteen 8 kohta 8, III liitteen 46 kohta IV liitteen 8 kohta 2) IV liitteen 8 ja 37-38 kohdat 3) IV liitteen 16 kohta 4) III liitteen 45 kohta ja IV liitteen 8 ja 37-38 kohdat 5) III liitteen 44 kohta ja IV liitteen 8 ja 37-38 kohdat
	Lisätietoa		
	Hävittäminen silppuamalla Suojaustasolla IV aineistojen silppuaminen voidaan toteuttaa esimerkiksi siten, että ■ paperiaineistojen silppukoko on enintään 30 mm² (DIN 66399 / P5 tai DIN 32757 / DIN 4), ■ magneettisten kiintolevyjen silppukoko on enintään 320 mm² (DIN 66399 / H-5), ■ SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm² (DIN 66399 / E-5), ja ■ optisten medioiden silppukoko on enintään 10 mm² (DIN 66399 / O-5). Suojaustason III aineistojen silppuaminen voidaan toteuttaa esimerkiksi siten, että ■ paperiaineistojen silppukoko on enintään 30 mm² (DIN 66399 / P5 tai DIN 32757 / DIN 4), ■ magneettisten kiintolevyjen silppukoko on enintään 10 mm² (DIN 66399 / H-6), ■ SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm² (DIN 66399 / E-5), ■ optisten medioiden silppukoko on enintään 5 mm² (DIN 66399 / O-6).		

I 19

Suojaustason II aineistojen silppuaminen voidaan toteuttaa esimerkiksi siten, että

- paperiaineistojen silppukoko on enintään 10 mm² (DIN 66399 / P6),
- magneettisten kiintolevyjen silppukoko on enintään 10 mm² (DIN 66399 / H-6),
- SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 1 mm² (DIN 66399 / E-6),
- optisten medioiden silppukoko on enintään 5 mm² (DIN 66399 / O-6).

Käytettäessä edellä mainittuja silppukokoja, voidaan silppuamisesta/tuhoamisesta syntyvä jäte hävittää normaalin toimistojätteen mukaisesti. Esimerkiksi DIN 66399 / P5:n mukaista paperisilppua ei siten suojaustasolla III edellytetä hävitettävän esimerkiksi ulkoistettujen ”tietosuojalaatikoiden” hävitysprosessin mukaisesti.

Hävittäminen eri menetelmiä yhdistäen

Hävittämiseen voidaan käyttää silppuamisen korvaavana tai sitä tukevana suojauksena myös muita menetelmiä, joilla tietojen kokoaminen estetään luotettavasti (esimerkiksi silpun polttaminen tai kiintolevyn sulattaminen). Tietojen kokoamismahdollisuuksiin vaikuttaa myös ulkopuolisille luovutettavan silpun määrä (esimerkiksi yhden paperin silppu vs. suuret määrät paperisilppua). Myös salauksella pystytään pienentämään huomattavasti salassa pidettävään tietoon kohdistuvia riskejä tiedon ja laitteistojen elinkaarten eri vaiheissa. Sähköisten aineistojen hävittämistä on kuvattu yksityiskohtaisemmin Viestintäviraston ylikirjoitusohjeessa (www.ncsa.fi > Asiakirjat > Ylikirjoitusohje).

Sähköisten aineistojen hävittämisessä huomioon otettavaa

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

Väliaikaistiedostojen hävittämisessä huomion otettavaa

Väliaikaistiedostojen hävityksessä tulisi huomioida käyttöjärjestelmän ja sovellusten tilapäistiedostojen tallennuskansioiden, sekä esimerkiksi roskakorin sisällön hävitys ylikirjoittamalla. Tilapäistiedostojen ylikirjoitus voidaan toteuttaa esimerkiksi järjestelmän käynnistyksen tai sammutuksen yhteydessä automatisoiduin komentojonoin (logon-/logoff-skriptit). Palvelimiin ja muihin vastaaviin järjestelmiin, joita ei käynnistellä päivittäin, suositellaan, että väliaikaistiedostojen ylikirjoitus automatisoidaan ja ajastetaan tapahtumaan säännöllisesti, esimerkiksi kerran vuorokaudessa.
Hävittämisen dokumentoinnista löytyy lisätietoja kohdasta I 18.

Muita lisätietolähteitä

Viestintäviraston ylikirjoitusohje; Secure destruction of sensitive items - CPNI standard - 2014, BSI IT-Grundschutz-Catalogues - 13th version - 2013; ISO/IEC 27002:2013 8.3.2; ISO/IEC 27002:2013 11.2.4; ISO/IEC 27002:2013 11.2.7

Käyttöturvallisuus

I 20

Salassa pidettävän tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Muutos-hallintamenettelyt

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
1) Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen. 2) Turvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä. 3) Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.	1) 4 §, 5 §:n 1 mom. 6 kohta, 6 § 2) 4 §, 5 §:n 1 mom. 6 kohta, 6 § 3) 4 §, 5 §:n 1 mom. 6 kohta, 6 §	1) IV liitteen 8 kohta 2) IV liitteen 11 ja 16 kohdat 3) IV liitteen 12 kohta

Lisätietoja

Toteutusesimerkki

Suojaustasoilla IV-III vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Tietojenkäsittelyyn liittyviin muutoksiin tulisi olla käytössä muutoksenhallintamenettely. Muutokset ovat jäljitettävissä.
2) Verkot, järjestelmät ja niihin liittyvät laitteet, ohjelmistot ja asetukset on dokumentoitu siten, että muutokset hyväksyttyyn kokoonpanoon pystytään havaitsemaan vertaamalla toteutusta dokumentaatioon.
3) Tietojenkäsittely-ympäristöjä tarkkaillaan luvattomien muutosten tai laitteistojen havaitsemiseksi.

Suojaustasolla II vaatimus voidaan täyttää siten, että kohtien 1-3 lisäksi toteutetaan seuraavat toimenpiteet:

4) Laitteistot suojataan luvattomien laitteiden (näppäilynauhoittimet ja vastaavat) liittämistä vastaan.

Yleistä

Dokumentaatioon tulisi tyypillisesti sisältyä vähintään verkkokuvat, laite- ja ohjelmistorekisterit, sekä tiedot laitteistojen/ohjelmistojen konfiguraatioista.

Laitteiston suojauksessa luvattomien laitteiden kytkemistä vastaan voidaan hyödyntää esimerkiksi

a) laitteiden sijoittamista sinetöityyn ja/tai hälytyslaitteella varustettuun turvakehikkoon tai vastaavaan,
b) peukalointia vastaan suojattujen laitteiden käyttämistä, tai
c) jotain vastaavaa menettelyä (esim. käytettävien laitteiden sinetöintiä). Käytettäessä sinetöintiin perustuvaa menetelmää, tulisi sinettien eheyden tarkastamiseen olla säännöllinen prosessi.

Luvattomien muutosten tai laitteistojen tarkasteluun hyväksyttävissä oleva tarkastustiheys riippuu kyseessä olevassa kohteessa toteutetuista menetelmistä, joilla rajoitetaan ja valvotaan kohteeseen (tietojärjestelmä, fyysinen tila) pääsyä. Useimmissa ympäristöissä voi riittää tarkastukset esimerkiksi puolivuosittain tai vuosittain.

I 20

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 1 (); SANS Critical Security Controls (v5) / 2; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Hardware Keyloggers; Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje"; ISO/IEC 27002:2013 8.1.1; ISO/IEC 27002:2013 12.1.1; ISO/IEC 27002:2013 12.1.2; ISO/IEC 27002:2013 12.5.1; ISO/IEC 27002:2013 14.2.2; ISO/IEC 27002:2013 14.2.8; ISO/IEC 27002:2013 14.2.9; ISO/IEC 27002:2013 18.2.3; VAHTI 2/2010:n liitteen 5 luku 2.4

I 21

Salassa pidettävien tietojen käsittely fyysisesti suojattujen alueiden sisällä - Fyysinen turvallisuus

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Suojaustaso IV 1) Fyysiset turvatoimet toteutetaan kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa tietoja käsitellään tai säilytetään, tietojenkäsittely-ympäristöjen sijoitusalueet mukaan luettuina. 2) Tietojen käsittely on mahdollista turva-alueilla, hallinnollisella alueella tai viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella. 3) Tietojen säilytys on mahdollista turva-alueilla ja hallinnollisella alueella soveltuvissa lukittavissa toimistokalusteissa, tai tilapäisesti myös viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella. *Suojaustaso III-II* 1 kohdan lisäksi: 4) Tietojen käsittely on mahdollista viranomaisen hyväksymillä turva-alueilla. Tietojen käsittely on mahdollista myös hallinnollisilla alueilla, jos pääsy salassa pidettäviin tietoihin on suojattu sivullisilta. 5) Tietojen säilytys on mahdollista viranomaisen hyväksymillä turva-alueilla turvasäilytysyksikössä tai kassaholvissa.	1) 5 §:n 1 mom. 7 kohta, 14 §, 15 § 2) 5 §:n 1 mom. 7 kohta, 14 §, 15 § 3) 5 §:n 1 mom. 7 kohta, 14 §, 15 § 4) 5 §:n 1 mom. 7 kohta, 14 §, 15 § 5) 5 §:n 1 mom. 7 kohta, 14 §, 15 §	1) 8 artiklan 3 kohta 2) II liitteen 23 kohta, 8 artiklan 3 kohta 3)II liitteen 24 kohta, 8 artiklan 3 kohta, 9 artiklan 4 kohta 4) II liitteen 25 kohta, 8 artiklan 4 kohta 5) II liitteen 22 ja 26 kohdat, 8 artiklan 4 kohta

Lisätietoja

Yleistä

Tilanteissa, joissa suojaustasojen III tai II aineistoa käsitellään tilapäisesti luokkaa matalamman tason tilassa, tulisi esimerkiksi hajasäteilysuojaus (vrt. I 14) toteuttaa ko. aineiston suojaustason mukaisesti. Toteutuksessa huomioitava myös esimerkiksi toiminta työskentelytaukojen aikana (aineisto vietävä esimerkiksi turva-alueen kassakaappiin tauon ajaksi), näkyvyyden rajaus tilaan (esim. mahdollisten ikkunoiden peittäminen) ja käsittelytilaan pääsyn rajaaminen vain hyväksyttyihin henkilöihin. Hallinnolliselle alueelle, turva-alueille sekä esimerkiksi kassakaapeille asetettavat vaatimukset on kuvattu yksityiskohtaisemmin Katakrin F-osiossa (ks. F 02 ja F 03).

Muita lisätietolähteitä

BSI IT-Grundschutz-Catalogues - 13th version - 2013; CPNI - Security Advice - Physical Security; ISO/IEC 27002:2013 11.1.1; ISO/IEC 27002:2013 11.1.3; ISO/IEC 27002:2013 11.1.5; ISO/IEC 27002:2013 11.2.1

I 22

Salassa pidettävien tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä - Etäkäyttö ja etähallinta

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Suojaustaso IV 1) Tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä on mahdollista vain viranomaisen ko. suojaustasolle hyväksymien korvaavien menettelyjen mukaisesti. 2) Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan. 3) Elleivät hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolelle viedyt suojaustason IV tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu viranomaisen ko. suojaustasolle hyväksymällä menetelmällä, tietovälineet säilytetään vastaavantasoisesti suojaten, kuin hallinnollisen turva-alueen lukittavissa toimistokalusteissa säilytettynä, tai tietovälineitä ei jätetä valvomatta. 4) Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää viranomaisen ko. suojaustasolle hyväksymää liikenteen salausta. *Suojaustaso III-II* Kohtien 1-2 ja 4 lisäksi: 5) Hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolelle viedyt salassa pidettävää tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ovat koko ajan kuljettajansa hallussa, ellei niitä ole salattu viranomaisen ko. suojaustasolle hyväksymällä menetelmällä. Salassa pidettäviä tietoja ei avata matkalla eikä lueta julkisilla paikoilla. 6) Järjestelmien etäkäyttö/-hallinta rajataan viranomaisen hyväksymälle fyysisesti suojatulle alueelle.	1) 5 §:n 1 mom. 7 ja 9 kohdat, 14 §, 15 §, 16 §, 19 § 2) 5 §:n 1 mom. 9 kohta 3) 5 §:n 1mom. 6 kohta 4) 5 §:n 1 mom. 6 kohta, 16 §, 19 § 5) 5 §:n 1 mom. 6 kohta 6) 5 §:n 1 mom. 6 kohta, 14 §, 15 §	1) 8 artiklan 3 kohta, 9 artiklan 4 kohta 2) IV liitteen 22 kohta 3) 9 artiklan 4 kohta, III liitteen 28, 30 ja 33 kohdat 4) 10 artiklan 6 kohta 5) 9 artiklan 4 kohta, III liitteen 28, 30 ja 33 kohdat 6) II liitteen 25-26 kohdat, 8 artiklan 4 kohta

Lisätietoja

Yleistä

Etäkäytöllä/-hallinnalla tarkoitetaan perinteisessä merkityksessään organisaation toimitilojen ulkopuolelta tapahtuvaa tietojärjestelmien käyttöä/hallintaa tätä tarkoitusta varten hankitulla päätelaitteella. Normaalisti päätelaitteena toimii organisaation henkilön käyttöön antama kannettava tietokone. Turvallisuusluokitellun tiedon osalta etäkäyttö/-hallinta soveltuu perinteisessä merkityksessään vain suojaustasolle IV. Suojaustasolta III lähtien aineiston käsittely edellyttää viranomaisen hyväksymää fyysisesti suojattua aluetta, ellei viranomainen ole hyväksynyt korvaavia menettelyjä, joilla saavutetaan vastaavat fyysisen turvallisuuden olosuhteet (esimerkiksi tietyissä viranomaisoperaatioissa).

I 22

Vaatimuksessa 1 tarkoitettuihin viranomaisen hyväksymiin korvaaviin menettelyihin sisältyvät suojaustasolla IV seuraavat:

a) Vain käyttöympäristöön hyväksyttyjä laitteita ja etäyhteyksiä käytetään.
b) Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta.

Suojaustasoilla III ja II korvaavana menettelynä edellytetään lisäksi käytön teknistä sitomista hyväksyttyyn etäkäyttölaitteistoon (esim. laitetunnistus). Hallintayhteyksien suojaus on eräs kriittisimmistä tietojärjestelmien turvallisuuteen vaikuttavista tekijöistä (vrt. I 04). Erityisesti suojaustason IV järjestelmiä voi kuitenkin olla perusteltua pystyä hallinnoimaan myös fyysisesti suojattujen alueiden ulkopuolelta. Tilanteissa, joissa etähallinta nähdään perustelluksi, suositellaan se suojattavan etäkäyttöä kattavammilla turvatoimilla. Esimerkiksi suojaustason IV järjestelmän etähallintayhteydet voidaan rajata yksittäisiin fyysisiin ja loogisiin pisteisiin.

Muita lisätietolähteitä

CPNI - Personnel Security in Remote Working; CPNI - Configuring & managing Remote Access for Industrial Control Systems; SANS Critical Security Controls (v5) / 13; SANS Critical Security Controls (v5) / 17; SANS Critical Security Controls (v5) / 10; SANS Critical Security Controls (v5) / 9; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Security Advice - Physical Security; ISO/IEC 27002:2013 6.2.1; ISO/IEC 27002:2013 6.2.2; ISO/IEC 27002:2013 7.2.2; ISO/IEC 27002:2013 8.3.1; ISO/IEC 27002:2013 8.3.3; ISO/IEC 27002:2013 11.1.1; ISO/IEC 27002:2013 11.1.3; ISO/IEC 27002:2013 11.1.5; ISO/IEC 27002:2013 11.2.1; ISO/IEC 27002:2013 11.2.3; ISO/IEC 27002:2013 11.2.5; ISO/IEC 27002:2013 11.2.6; ISO/IEC 27002:2013 12.1.1

I 23

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - Ohjelmisto-haavoittuvuuksien hallinta

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi.	5 §:n 1 mom. 6 kohta, 6 §	IV liitteen 8, 11 ja 16 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasoilla IV vaatimus voidaan toteuttaa siten, että toteutetaan alla mainitut toimenpiteet:

1) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti.
2) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan vähintään (haavoittuvuusskannaus, CMDB, jne.) vuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. Lisäksi säännöllisesti (esim. kuukausittain) tarkastellaan keskitetyistä päivityksenjakopalveluista päivitysten asentumisen onnistumista.

Suojaustasoilla III ja II vaatimus voidaan toteuttaa siten, että kohdan 1 lisäksi toteutetaan seuraava toimenpide:

3) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan vähintään (haavoittuvuusskannaus, CMDB, jne.) puolivuosittain ja aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. Lisäksi säännöllisesti (esim. kuukausittain) tarkastellaan keskitetyistä päivityksenjakopalveluista päivitysten asentumisen onnistumista.

Yleistä

Ohjelmistohaavoittuvuuksien hallintaa voidaan toteuttaa esimerkiksi siten, että

1) Sähköpostiin on tilattu CERT-toimijoiden sekä valmistajien tiedotukset. Tiedotuksista poimitaan sellaiset, jotka vaikuttavat organisaation järjestelmien turvallisuuteen. Ladattujen ohjelmistojen ja päivitysten eheys tarkistetaan (tarkistussummat, haittaohjelmatarkistus) ennen niiden jakamista tuotantoympäristöön. Päivitysten vaikutukset tulisi mahdollisuuksien mukaan testata ennen tuotantoympäristöön asennusta. Testaus voidaan suorittaa esimerkiksi eristetyssä testiympäristössä tai pienellä käyttäjäjoukolla.
2) Verkko ja sen palvelut, palvelimet sekä verkkoon kytketyt työasemat, kannettavat tietokoneet ja vastaavat tarkastetaan (haavoittuvuusskannaus, CMDB, jne.) säännöllisesti aina merkittävien muutosten jälkeen päivitysmenettelyjen korjauskohteiden löytämiseksi. Lisäksi säännöllisesti (esim. kuukausittain) tarkastellaan keskitetyistä päivityksenjakopalveluista päivitysten asentumisen onnistumista.

”Merkittäviin muutoksiin” voidaan laskea esimerkiksi verkkotopologian muutokset, uusien järjestelmien käyttöönotot ja/tai vanhojen service pack -tason päivitykset, palomuurien ja vastaavien suodatussääntöjen merkittävät muutokset, jne.

Muita lisätietolähteitä: SANS Critical Security Controls (v5) / 4; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; CPNI - Good Practice Guide - Patch Management; ISO/IEC 27002:2013 12.6.1; VAHTI 2/2010:n liitteen 5 luku 2.4

I 24

Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - varmuuskopiointi

Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Salassa pidettävää tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto.	5 §:n 1mom. 6 kohta, 6 §, 20 §	III liitteen 18 ja 27 kohdat, IV liitteen 8 ja 16 kohdat

Lisätietoja

Toteutusesimerkki

Suojaustasoilla IV vaatimus voidaan täyttää siten, että toteutetaan alla mainitut toimenpiteet:

1) Varmuuskopiot käsitellään ja säilytetään niiden elinkaaren ajan vähintään ko. suojaustason järjestelmissä.
2) Käsiteltäessä samalla varmistusjärjestelmällä tarkastusoikeuden varaavien eri omistajien tietoja, tarkastusoikeuden (vrt. I 06) mahdollistavat erottelumenettelyt on toteutettava ko. suojaustason mukaisesti varmistusjärjestelmän liittymien ja tallennemedioiden osalta.
3) Mikäli varmuuskopioita siirretään ko. suojaustason fyysisesti suojatun alueen ulkopuolelle, menettelyt kuin I 15:ssa (sähköinen välitys) ja/tai I 16 sekä I 22 (kuljetus fyysisesti suojatun alueen ulkopuolelle).
4) Varmistusmediat hävitetään ko. suojaustason mukaisesti (I 19).

Suojaustasolla III-II vaatimus voidaan toteuttaa siten, että kohtien 1-4 lisäksi toteutetaan seuraava toimenpide:

5) Varmuuskopioista on rekisterit ja varmuuskopioiden käsittely tulisi kirjata sähköiseen lokiin, tietojärjestelmään, asianhallintajärjestelmään, manuaaliseen diaariin tai asiakirjaan. (Vrt. I 18)

Yleistä

Varmuuskopiointi suositellaan aina mitoitettavan toimintavaatimuksiin. Toimintavaatimuksiin nähden riittävä varmuuskopioinnissa tulisi huomioida ainakin seuraavat:

1) Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO).
2) Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO).
3) Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti.
4) Palautusprosessin dokumentointi on riittävällä tasolla.
5) Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä, jne.). Huom: Varmuuskopiot tulisi suojata fyysisen ja loogisen pääsynhallinnan menetelmin vähintään tiedon (mahdollisesti kasautumisvaikutuksen nostaman) suojaustason mukaisesti.
6) Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, tarkastusoikeuden (vrt. I 06) mahdollistavat erottelumenettelyt on toteutettava varmistusjärjestelmän liittymien ja tallennemedioiden osalta (esim. omistaja-/hankekohtaiset eri avaimilla salatut nauhat, joita säilytetään asiakaskohtaisissa kassakaapeissa/kassakaappilokeroissa).

Muita lisätietolähteitä: SANS Critical Security Controls (v5) / 8; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; ISO/IEC 27002:2013 12.3.1; VAHTI 2/2010:n liitteen 5 luku 2.10

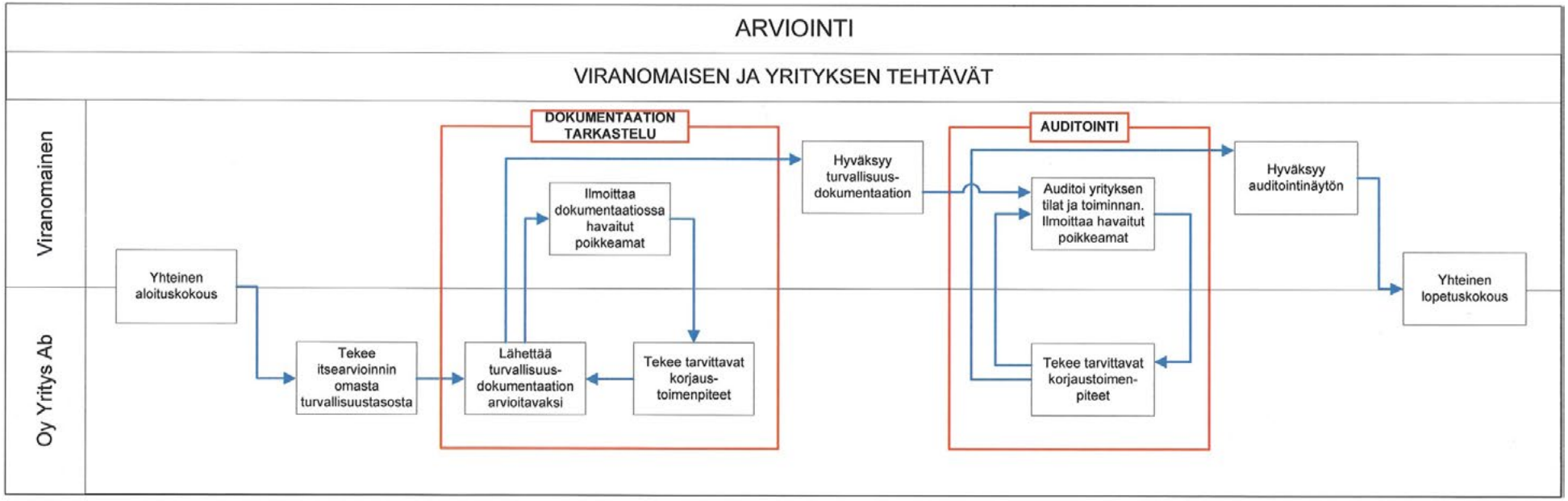
LIITE I: Yritysturvallisuusselvitys

Katakrin käyttö osana yritysturvallisuusselvitystä

Yritysturvallisuusselvityksistä säädetään turvallisuusselvityslaissa (726/2014). Yritysturvallisuusselvityksessä toimivaltainen viranomainen voi selvittää laissa mainittujen tietolähteiden, yritysten vastuuhenkilöiden henkilöturvallisuusselvitysten sekä yritykseen ja sen toimitiloihin kohdistuvan tarkastusten avulla, miten yritys kykenee huolehtimaan tietoturvallisuutta koskevista turvallisuusvelvoitteistaan. Tarkasteltavia turvallisuusjärjestelyjä ovat muun muassa salassa pidettävien tietojen suojaaminen oikeudettomalta paljastumiselta, asiattoman pääsyn estäminen tiloihin, joissa salassa pidettäviä tietoja käsitellään, sekä henkilöstön ohjeistaminen ja kouluttaminen. Katakria voidaan käyttää työkaluna, kun arvioidaan yrityksen toimitiloihin ja tietojärjestelmiin kohdistuvan tarkastuksen avulla yrityksen kykyä huolehtia tietoturvallisuusjärjestelyistä.

Yritysturvallisuusselvitykseen liittyvä arviointiprosessi on esitetty kuvassa 1. Prosessikaaviossa kuvataan viranomaisen ja yrityksen tehtävät arvioinnin eri vaiheissa. Arviointiin sisältyy yrityksen tietojärjestelmien auditointiprosessi silloin, kun se tehdään osana yritysturvallisuusselvitystä.

Kuva 1 Arviointiprosessi.



Yritysturvallisuusselvitys voidaan laatia osittaisena. Jos yritysturvallisuusselvityshakemuksessa yritykseltä ei edellytetä kykyä suojata viranomaisen salassa pidettävää tietoa toimitiloissaan (”FSC without safeguards”), arvioinnissa voidaan käyttää pelkästään turvallisuusjohtamisen osa-aluetta. Jos yritysturvallisuusselvityspyynnössä edellytetään myös kykyä suojata viranomaisen salassa pidettäviä tietoja yrityksen toimitiloissa (”FSC with safeguards”), arvioinnissa voidaan käyttää turvallisuusjohtamisen osa-alueen lisäksi fyysisen turvallisuuden osa-aluetta ja niitä teknisen tietoturvallisuuden osa-alueen vaatimuksia, jotka koskevat paperiasiakirjojen käsittelyä. Tietojärjestelmiin kohdistuva arviointi osana yritysturvallisuusselvitystä on kuvattu tarkemmin liitteessä II.

Valmistautuminen auditointiin

Ennen varsinaisen viranomaisarvioinnin aloittamista yrityksen tulee saattaa tietojenkäsittely-ympäristönsä turvallisuusjärjestelyt ja jäännösriskit sellaisella tasolle, että ne ovat yrityksen riskienhallinnassa hyväksyttävissä. Yrityksen tulee toimittaa viranomaiselle arvioitavaksi riskienhallintatuloksensa sekä kuvaus turvallisuusjärjestelyjen vaatimustenmukaisuudesta. Riskienhallintatuloksille ja turvallisuusjärjestelyjen vaatimustenmukaisuuden kuvaukselle ei edellytetä tietyn määrämuotoisen lomakemallin käyttämistä.

Yrityksen riskienhallinta

Yrityksen turvallista toimintaa uhkaavien riskien hallinta toimii perustana turvallisuusjärjestelyjen oikealle mitoitukselle. Toimivaltainen viranomainen suhteuttaa vaatimuksensa lähtökohtaisesti siihen uhkaympäristöön ja niihin turvatoimiin (kontrolleihin), jotka yritys esittää. Viranomaisen käsitys uhkista saattaa kuitenkin poiketa siitä, mihin yritys on omista lähtökohdistaan päätynyt.
Tiedon suojaamiseen tähtäävä turvallisuusriskien hallintaprosessi voidaan kuvata yksinkertaistetusti neljään vaiheeseen:

1) riskien tunnistaminen,
2) riskien analysointi vaikutusten ja todennäköisyyksien määrittämiseksi,
3) riskien arviointi tarkoituksenmukaisten turvatoimienvalitsemiseksi, ja
4) riskien toteutumiseen varautuminen riskienhallintaprosessin seurantamenettelyjen kautta

Riskienhallinnan kattavuutta ja muita sille asetettuja vaatimuksia käsitellään yksityiskohtaisemmin osa-alueella T (erityisesti T 04).
Yrityksen tulee pystyä riskienhallintaprosessinsa kautta osoittamaan toimivaltaiselle viranomaiselle perusteensa valituille turvatoimille ja niiden riittävyydelle. Yritystä suositellaan keskustelemaan riskiensä määrittelystä ja turvatoimisuunnitelmistaan toimivaltaisen viranomaisen kanssa jo varhaisessa vaiheessa, jotta sekä yrityksen että toimivaltaisen viranomaisen arviot kyseisen ympäristön riskeistä pystytään huomioimaan jo turvatoimia suunniteltaessa.

Kuvaus yrityksen turvallisuusjärjestelyjen vaatimustenmukaisuudesta

Yrityksen turvallisuusjärjestelyjen vaatimustenmukaisuuden kuvauksen tavoitteena on esittää kootusti ne turvallisuusjärjestelyt, joilla yritys pyrkii täyttämään turvallisuusvaatimukset. Kuvausta hyödynnetään erityisesti viranomaisen auditoinnin suunnittelussa ja toteutuksessa. Esimerkkiote turvallisuusjärjestelyjen vaatimustenmukaisuuden kuvauksesta on esitetty taulukossa 1.

Taulukko 1. Esimerkkiote turvallisuusjärjestelyjen vaatimustenmukaisuuden kuvauksesta.

T 11 Henkilöstöturvallisuus Turvallisuuskoulutus ja -tietoisuus	1) Turvallisuusohjeet kattavat suojattavaan tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta 2) Organisaation henkilöstö on koulutettu suojattavien tietojen käsittelyn keskeisten vaatimusten osalta. Henkilöstölle annetaan ohjeet ja koulutusta suojattavien tietojen asianmukaisesta käsittelystä. 3) Suojattavien tietojen käsittelyä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneista henkilöistä pidetään listaa. 4) Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti.	Uusille henkilöille annetaan heti taloon tultua yleinen turvallisuuskoulutus sekä -ohje. Päivitetty yleinen turvallisuuskoulutus annetaan myös koko henkilöstölle vuosittain. Turvallisuuskoulutukseen osallistuminen on pakollista koko henkilöstölle. Osaamista mitataan vuosittain intranetin testeillä, jotka tulee läpäistä käyttöoikeuksien saamiseksi ja ylläpitämiseksi. Yleisen turvallisuuskoulutuksen järjestelyt on vastuutettu riskienhallintapäällikölle. Suojattavan tiedon käsittelyn tehtäväkohtainen turvallisuuskoulutus annetaan henkilöstölle, joka käsittelee työssään suojattavia tietoja. Tehtäväkohtainen koulutus on räätälöity eri tehtäväryhmittäin. Koulutus on pakollinen käydä läpi *ennen* pääsyoikeuksien saamista suojattavan tiedon käsittely-ympäristöön. Koulutukseen osallistumista seurataan koulutusrekisterillä. Koulutus uusitaan vuosittain, ja kunkin vuoden koulutuspaketin läpikäynti tulee olla toteutettuna Q1:n aikana. Tehtäväkohtaisen turvallisuuskoulutuksen järjestelyt on vastuutettu riskienhallintapäällikölle sekä kunkin tehtäväkohtaisen toiminnon turvallisuusvastaavalle. Turvallisuusohjeiden ylläpito on vastuutettu riskienhallintapäällikölle, jota tukee tehtäväkohtaisten ohjeistuksien osalta kunkin tehtäväkohtaisen toiminnon turvallisuusvastaava.

Viranomaisen arviointi turvallisuusjärjestelyjen riittävyydestä

Viranomaisen arvioinnissa huomioidaan muun muassa tiedon suojaustaso, määrä, muoto ja luokitteluperuste suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan. Katakrin eri osioissa kuvattujen turvatoimien soveltamisessa tulee huomioida, että kuvatut toteutusesimerkit voivat olla korvattavissa myös muilla vastaavan tasoisilla suojauksilla. Esimerkiksi vahvan käyttäjätunnistuksen toteutus on mahdollista ratkaista tietoteknisen tai fyysisen turvallisuuden menetelmin. Toisaalta esimerkiksi tietoliikenteen salaukselle ei yleensä pystytä toteuttamaan riittäviä korvaavia turvatoimia tilanteissa, joissa liikenne kulkee fyysisesti suojatun vyöhykkeen ulkopuolella.
Tilanteissa, joissa kohteessa ei arvioida ilmenevän vaatimusten tai toteutusesimerkkien taustalla olevia uhkia, viranomainen voi arvioida kyseisen vaatimuksen täyttämättä jättämisen olevan perusteltua. Esimerkiksi työasemiin, joista on fyysisesti luotettavasti poistettu kaikki verkkoliikennöintiin kykenevät rajapinnat, ei yleensä ole perusteltua edellyttää palomuurin tai sen säännöstön ylläpitomenettelyä.
Viranomainen arvioi riskienarvioinnissaan soveltuviksi valittujen suojausvaatimusten täyttymisen Katakrissa kuvattuja toteutusesimerkkejä hyödyntäen. Viranomaisen arviointi perustuu yleensä hallinnollisen ja teknisen todentamisen menetelmiin. Tietojärjestelmien turvallisuusjärjestelyjen arvioinneissa käytettyjä todennusmenetelmiä on kuvattu yksityiskohtaisemmin Viestintäviraston ohjeessa tietoturvallisuuden arviointilaitoksille[1].

1 Viestintäviraston ohje tietoturvallisuuden arviointilaitoksille. URL: https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf.

LIITE II Tietojärjestelmien arviointi

Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista[2] mukaisesti viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjensä tietoturvallisuuden arvioinnissa Viestintävirastoa tai Viestintäviraston hyväksymää tietoturvallisuuden arviointilaitosta[3]. Katakria voidaan käyttää työkaluna selvitettäessä, miten viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tietoturvallisuudesta on huolehdittu suhteessa kansallisiin tai kansainvälisiin suojausvaatimuksiin. Myös viranomaisten tietojärjestelmien turvallisuuden arvioinnissa Katakrin käytön tulee perustua järjestelmälliseen riskienarviointiin, sen pohjalta soveltuviksi valittaviin suojausvaatimuksiin ja niiden täyttymisen arviointiin toteutusesimerkkejä hyödyntäen. Tässä liitteessä kuvataan Katakrin eri käyttötapauksia tietojärjestelmätarkastuksissa. Kuvauksessa keskitytään yritysturvallisuusselvityksen ja viranomaisten tietojärjestelmien arvioinnin käyttötapauksiin, joissa toimivaltaisena viranomaisena on Viestintävirasto. Kuvaus on jaoteltu käyttötapausten, arviointi- ja hyväksyntäprosessien sekä hyväksynnän ja todistuksen esittelyyn. Kuvauksessa ei käsitellä muita käyttötapauksia, esimerkiksi käyttöä osana organisaation sisäistä turvallisuustyötä.

Käyttötapaukset

Viestintäviraston NCSA-toiminnon suorittamissa tietojärjestelmätarkastuksissa Katakrin käyttötapaukset on jaettavissa viiteen kokonaisuuteen:

1. Viranomaisen määräämisvallassa olevat tai hankittavaksi suunnittelemat järjestelmät, joista viranomainen on tehnyt Viestintävirastolle arviointipyynnön (L 1406/2011).
    - Järjestelmää arvioidaan tällöin viranomaisen tekemän pyynnön mukaisesti joko kansallisen, kansainvälisen tai sekä kansallisen että kansainvälisen salassa pidettävän tiedon näkökulmasta.
2. Valtiovarainministeriön pyynnöstä tehtävät selvitykset valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta (L 1406/2011).
    - Järjestelmää arvioidaan tällöin Valtiovarainministeriön tekemän pyynnön mukaisesti joko kansallisen, kansainvälisen tai sekä kansallisen että kansainvälisen salassa pidettävän tiedon näkökulmasta.
3. Valtionhallinnon toimijoiden järjestelmät siltä osin, kun ne liittyvät kansainvälisten tietoturvavelvoitteiden täyttämiseen (L 588/2004[4]).
    - Järjestelmää arvioidaan tällöin kansainvälisen salassa pidettävän tiedon näkökulmasta.
4. Kansainväliseen yritysturvallisuusselvitysprosessiin hakeutuneiden yritysten järjestelmät siltä osin, kun ne vaativat kansallisen tietoturvallisuusviranomaisen (NCSA) hyväksyntää (L 588/2004 ja/tai 726/2014[5]).
    - Järjestelmää arvioidaan tällöin kansainvälisen salassa pidettävän tiedon näkökulmasta.
5. Kansalliseen yritysturvallisuusselvitysprosessiin hakeutuneiden yritysten järjestelmät siltä osin, kun ne vaativat kansallisen tietoturvallisuusviranomaisen (NCSA) todistusta vaatimustenmukaisuudesta (L 726/2014).
    - Järjestelmää arvioidaan tällöin kansallisen salassa pidettävän tiedon näkökulmasta.

Tietojärjestelmätarkastusten käyttötapauksia on mahdollista myös yhdistellä arvioinnin tilaajan toiveiden mukaisesti.

---

2 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), https://www.finlex.fi/fi/laki/alkup/2011/20111406.

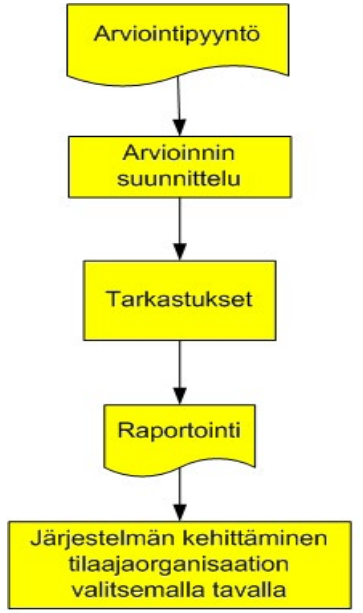
3 Laki tietoturvallisuuden arviointilaitoksista (L 1405/2011), https://www.finlex.fi/fi/laki/ajantasa/2011/20111405.

4 Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), https://www.finlex.fi/fi/laki/alkup/2004/20040588.

5 Turvallisuusselvityslaki (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.

Arviointiprosessi

Tietojärjestelmien turvallisuuden arviointiprosessi (L 1406/2011) alkaa, kun arvioinnin kohde toimittaa Viestintävirastolle arviointipyynnön. Arviointiprosessin keskeisiä muita vaiheita ovat arvioinnin suunnittelu, tarkastukset sekä raportointi. Arviointiprosessia on havainnollistettu yksinkertaistetussa muodossaan kuvassa 1. Arviointiprosessia voidaan hyödyntää esimerkiksi kohdeorganisaation sisäisen turvallisuustyön tukena, jättäen muun muassa jäännösriskien käsittelyn täysin kohdeorganisaation vastuulle. Arviointiprosessia kuvataan yksityiskohtaisemmin ohjeessa ”Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma”[6].



Kuva 1. Arviointiprosessi yksinkertaistettuna.

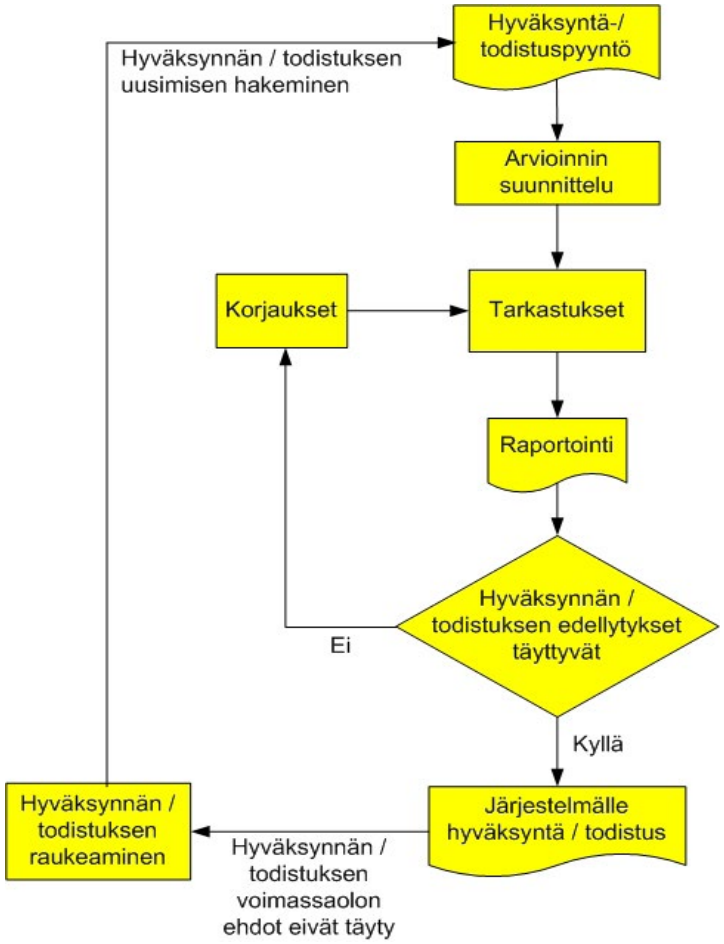
6 Ohje “Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma”. URL: https://www.viestintavirasto.fi/attachments/Viestintaviraston_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

Hyväksyntäprosessi

Viestintäviraston hyväksyntään tai todistukseen tähtäävä hyväksyntäprosessi (L 588/2004, L 726/2014 tai 1406/2011) alkaa, kun arvioinnin kohde toimittaa Viestintävirastolle hyväksyntä- tai todistuspyynnön. Hyväksyntäprosessi mukailee arviointiprosessia sillä keskeisellä erolla, että tarkastuksissa mahdollisesti havaittujen poikkeamien tulee olla todennetusti korjattuja ennen, kuin hyväksyntä tai todistus voidaan myöntää. Hyväksyntäprosessia on havainnollistettu yksinkertaistetussa muodossaan kuvassa 2. Hyväksyntäprosessia voidaan hyödyntää esimerkiksi silloin, kun arvioinnin kohde haluaa osoittaa tietojärjestelmänsä suojausten vaatimustenmukaisuuden Viestintäviraston hyväksynnällä tai todistuksella. Hyväksyntäprosessissa riskienarviointi toteutetaan hyödyntäen sekä kohdeorganisaation, että Viestintäviraston arvioita. Hyväksyntäprosessia kuvataan yksityiskohtaisemmin ohjeessa "Viestintäviraston NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma".

Hyväksyntä ja todistus

Viestintävirasto voi myöntää vaatimukset täyttävälle kansainvälistä suojattavaa tietoa käsittelevälle järjestelmälle hyväksynnän (accreditation). Vaatimukset täyttävälle kansallista suojattavaa tietoa käsittelevälle järjestelmälle Viestintävirasto voi myöntää todistuksen vaatimustenmukaisuudesta. Sekä hyväksynnän että todistuksen myöntäminen edellyttää, että tarkastuksen kohde sitoutuu turvallisuuden tason säilyttämiseen.
Sekä hyväksynnän että todistuksen voimassaolo raukeaa, mikäli tarkastetussa kohteessa tapahtuu merkittävä sen turvallisuuteen vaikuttava muutos. Tällaisia voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten esimerkiksi ohjelmistojen turvapäivitysten asennukset, eivät aiheuta voimassaolevan hyväksynnän tai todistuksen raukeamista. Tapauskohtaiset ehdot hyväksynnän tai todistuksen raukeamiselle määritellään hyväksynnän tai todistuksen myöntämisen yhteydessä. Merkittävät muutokset tulee hyväksyttää etukäteen Viestintävirastolla.
Viestintävirastolla on mahdollisuus myöntää järjestelmälle todistus tai hyväksyntä pohjautuen hyväksytyn arviointilaitoksen suorittamaan arviointiin (L 1405/2011). Myöntämisen keskeisinä ehtoina ovat tehtyjen tarkastusten rajausten yhteneväisyydet haettavan todistuksen tai hyväksynnän rajauksiin sekä toimitettujen arviointiraporttien sisältämien tietojen riittävyys. Todistusta tai hyväksyntää varten Viestintävirasto suorittaa tarvittaessa tarkentavia arviointeja tai pyytää tilaajaorganisaatiolta lisäselvitystä sen selvittämiseksi ja varmistamiseksi, että kohde täyttää soveltuvat tietoturvallisuusvaatimukset.



Kuva 2. Hyväksyntäprosessi yksinkertaistettuna.