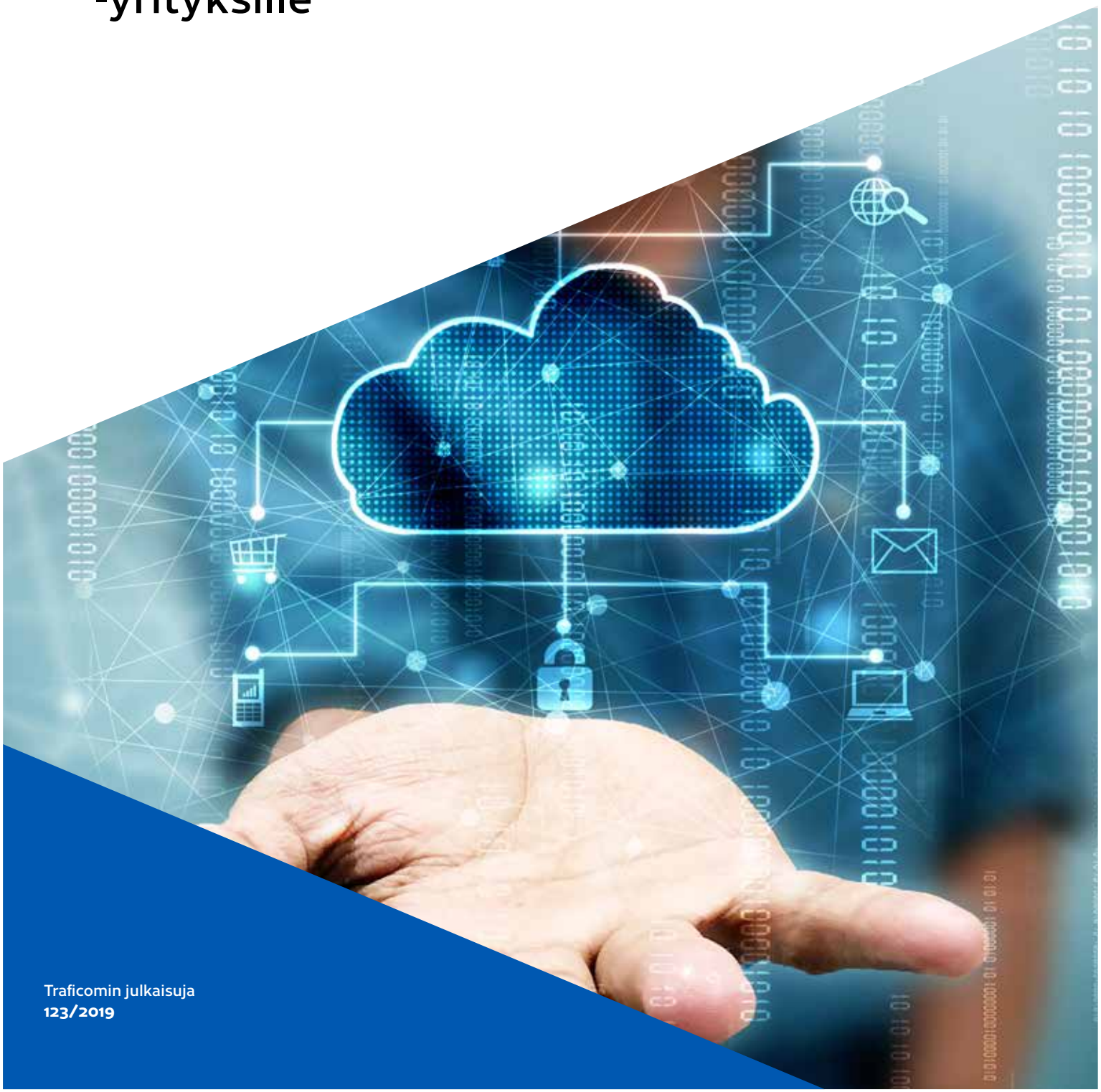
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille



Traficomin julkaisuja
123/2019

Sisältö

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-460-9
ISSN 2669-8757

Johdanto

Kulunut vuosikymmen on vakauttanut pilvipalvelut osaksi yksityishenkilöiden, pienyhteisöjen ja -yritysten tavallista tietojenkäsittelyä. Helppokäyttöisyys, kustannustehokkuus ja kyky vastata vaihtuviin tarpeisiin tukevat monia käyttötarpeita. Kehitys on herättänyt perustellusti kysymyksiä myös siitä, millaista tietoa pilvipalveluissa voi ja kannattaa käsitellä, sekä millaisia riskejä erilaisiin käyttötapauksiin liittyy. Tämä ohje pureutuu yleisimpiin tietoturvallisuusnäkökulmiin, joita yksityishenkilöiden, pienyhteisöjen ja -yritysten kannattaa pilvipalvelujen käyttöä pohtiessaan huomioida.

Tässä ohjeessa käsiteltyjä aiheita on kuvattu yksityiskohtaisemmin PiTuKrissa, Pilvipalveluiden turvallisuuden arviointikriteeristössä[1]. PiTuKri on suunnattu ensisijaisesti viranomaisten salassa pidettävän tiedon suojaamistarpeisiin, mutta siihen kootut pilvipalvelujen turvallisuuteen ja sen arviointiin liittyvät hyvät käytännöt ovat myös yksityishenkilöiden, pienyhteisöjen ja -yritysten hyödynnettävissä.

Tunnista tietosi

Suojattavien tietojen ja niiden merkityksen tunnistaminen on tärkeää, jotta suojaukset voidaan mitoittaa suojaustarpeiden mukaisesti. Tietojen tunnistamisessa ja niiden merkityksen pohdinnassa voi auttaa erilaisiin kysymyksiin vastaaminen. Mitä tietoa käsittelet? Sisältävätkö käsittelemäsi tiedot henkilötietoja? Sisältävätkö ne esimerkiksi valokuvia, ihmisten nimiä tai vaikkapa sähköpostiosoitteita? Sisältävätkö käsittelemäsi tiedot pienyhteisösi tai -yrityksesi toiminnan kannalta kriittistä tietoa? Ovatko tiedot luottamuksellisia, tai onko niihin tarve päästä myös tilanteissa, joissa Internet-yhteys ei toimi? Erilaisiin tietoihin voi kohdistua erilaisia riskejä, joita voi pohtia myös tietoturvallisuuden ulottuvuuksien, käytettävyyden, luottamuksellisuuden ja eheyden kautta.

Käytettävyys

Mikäli kyseiset tiedot eivät olisi käytettävissä, aiheutuisiko tästä sinulle tai pienyhteisöllesi/-yrityksellesi millaista haittaa tai vahinkoa? Onko esimerkiksi valokuva-arkistosi sellainen, että et haluasi sen katoavan? Millaista vahinkoa aiheutuisi, jos pienyrityksesi asiakasrekisteri ei olisi käytettävissä pariin viikkoon, tai jos se tuhoutuisi kokonaan? Miten harrasteseurasi jäsenmaksut kerättäisiin, jos jäsenten yhteystiedot katoaisivat?

Luottamuksellisuus

Mikäli kyseisten tietojen luottamuksellisuus menetettäisiin, ja tiedot joutuisivat ulkopuolisten käsiin, aiheutuisiko tästä sinulle tai pienyhteisöllesi/-yrityksellesi millaista haittaa tai vahinkoa? Onko esimerkiksi valokuva-arkistossasi jotain sellaista, mitä et haluaisi joutuvan kuin lähipiirisi nähtäväksi? Onko pienyrityksesi tulevaisuuden suunnitelmissa tai esimerkiksi tuotekehityksessä jotain sellaista, joka voisi kilpailijoille päätyessään vahingoittaa pienyrityksesi toimintaa? Aiheutuisiko joidenkin tietojen luottamuksellisuuden menetyksestä vain vähäistä harmia, jolloin niiden suojaamiseenkaan ei kannata panostaa merkittävästi?

Eheys

Mikäli kyseisten tietojen eheys tai muuttumattomuus menetettäisiin, ja tiedot eivät enää pitäisikään paikkaansa, millaista vahinkoa tästä voisi seurata? Pystyisitkö selvittämään pienellä vaivalla esimerkiksi ystäviesi puhelinnumerot, mikäli matkapuhelimesi osoitekirja menisi sekaisin? Miten pienyrityksesi laskutus toimisi, mikäli asiakasrekisterin sisältämät yhteystiedot eivät pitäisi paikkaansa?

Näihin kysymyksiin vastaamalla pystyt todennäköisesti haarukoimaan jo joitain suojaustarpeita tietojenkäsittely-ympäristölle, jossa näitä tietoja käsitellään.

1 Kyberturvallisuuskeskus. 2019. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) - v1.0. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf.

Millainen pilvipalvelu voi soveltua juuri sinun tiedoillesi?

Mikäli käsittelemäsi tiedot ja niiden käyttötavat sen mahdollistavat, pilvipalvelun käyttö voi olla useistakin syistä hyvä ratkaisu. Esimerkiksi nopeus, kustannustehokkuus ja kyky vastata muuttuviin tarpeisiin voivat olla perusteltuja syitä valita pilvipalvelu perinteisemmän tietojenkäsittely-ympäristön sijaan.

Kannattaa kuitenkin huolehtia, että tietosi ovat pilvipalvelussa riittävän hyvin suojattuja. Pilvipalvelua valittaessa kannattaakin varmistaa, että pilvipalveluntarjoajalla on tietoturvallisuuden hyvät käytännöt tiedossa ja myös käytäntöön jalkautettuna. Seuraavassa luvussa kuvataan yleisiä tietoturvallisuuden hyviä käytäntöjä, joiden tulisi jokaisella pilvipalveluja tarjoavalla organisaatiolla olla kunnossa.

Tietoturvallisuuden hyviä käytäntöjä

1. Turvallisuuden vastuut

Vähimmäissuojaukset

1. Pilvipalvelun turvallisuuden hoitamisen tehtävät ja vastuut on määritelty ja dokumentoitu.
2. Pilvipalvelun tarjoamiseen ja käyttöön liittyvä vastuunjako asiakkaan ja palveluntarjoajan välillä on kuvattu.
3. Pilvipalvelun tietoturvallisuudesta vastaava henkilö on nimetty.

Taustatietoa

Turvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa. Turvallisuusvastuiden määrittely on oleellista, jotta vastuuhenkilöt voivat käytännössäkin toteuttaa heidän vastuullaan olevat turvallisuustehtävät. Mikäli muuta ei ole kuvattu, ovat kaikki turvallisuusvastuut organisaation johdolla. Pilvipalvelupolitiikan (tai/ja vastaavien kuvausten) määrittelyn tavoitteena on tuoda selkeästi esille, mitkä turvallisuusasioista ovat asiakkaan vastuulla ja mitkä palveluntarjoajan.

Ota selvää

Onko pilvipalvelusta saatavilla selvä kuvaus siitä, mitä palvelun käyttöön liittyvä turvallisuuden vastuujako käytännössä tarkoittaa? Saatko selville sen, mistä sinun tulee pilvipalvelun asiakkaana huolehtia, ja mikä on palveluntarjoajan vastuulla? Onko pilvipalveluntarjoajan oma turvallisuustyö vastuutettu selkeästi?

Huom: Muista huomioida pilvipalveluihin liittyvä turvallisuuden vastuujako myös omalta osaltasi! Olethan ottanut käyttöön kaksivaiheisen tunnistautumisen? Muistaahan pienyrityksesi huolehtia turvallisuuspäivityksistä myös pilvipalveluihin sijoitettujen järjestelmien osalta?

Lisätietoja: PiTuKri TJ 02

2. Turvallisuusriskien ja muutosten hallinta

Vähimmäissuojaukset

1. Palvelun turvallisuutta valvotaan.
2. Palveluun kohdistuvia riskejä arvioidaan säännöllisesti.
3. Merkittävät palveluun kohdistuvat riskit saatetaan hyväksyttävälle tasolle.
4. Palveluun liittyviin muutoksiin on käytössä turvallisuuden huomioiva muutosten hallintamenettely. Oleelliset muutokset ovat jäljitettävissä.

Taustatietoa

Riskienhallinnan tavoitteena on tunnistaa ja hallita toimintaedellytyksiä mahdollisesti vaarantavia tekijöitä ja pitää toimintaan kohdistuvat riskit sellaisissa rajoissa, etteivät toiminta ja tavoitteet ole uhattuna. Muutostenhallinnan tavoitteena on, että pilvipalvelussa käsiteltävien tietojen luottamuksellisuus, eheys tai käytettävyys ei vaarannu palveluun tehtävien muutosten seurauksena.

Ota selvää

Kuinka pilvipalveluntarjoaja valvoo palvelun turvallisuutta? Arvioiko pilvipalveluntarjoaja palveluun liittyviä riskejä säännöllisesti, ja miten tämä näkyy käytännön tasolla pilvipalveluntarjoajan toiminnassa? Kuinka pilvipalveluun liittyvät muutokset toteutetaan? Kuinka muutoksiin liittyvät riskit huomioidaan?

Lisätietoja: PiTuKri TJ 03 ja MH 01

3. Turvallisuuspoikkeamien hallinta

Vähimmäissuojaukset

1. Pilvipalveluntarjoajalla on menettelytavat turvallisuuspoikkeamien asianmukaiseen käsittelyyn.
2. Pilvipalveluntarjoajalla on käytössään selkeät prosessit turvallisuuspoikkeamien ilmoittamisesta. Pilvipalveluntarjoajalla on määritettynä henkilöt/tahot, joille turvallisuuspoikkeamista tai niiden epäilyistä tulee ilmoittaa.
3. Turvallisuuspoikkeamien määrää ja tyyppejä seurataan. Toteutuneiden poikkeamien uusiutuminen pyritään estämään korjaussuunnitelmissa.
4. Asiakastiedon käsittelyyn liittyvät poikkeamat tai niiden epäilyt ilmoitetaan kyseiselle asiakkaalle.

Taustatietoa

Turvallisuuspoikkeamien hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa tilanteissa, minimoiden vahingot ja palauttaen tilanteen normaaliksi. Ilmoitusvelvollisuus asiakkaalle tukee asiakkaan riskienarviointia ja muun muassa vahinkojen minimointia.

Ota selvää

Kuinka pilvipalveluntarjoaja käsittelee havaitut poikkeamat? Kenelle pilvipalveluntarjoajan työntekijät ilmoittavat poikkeamista ja miten niiden käsittelyprosessi etenee käytännössä? Kuinka asiakkaan tietoihin kohdistuvat poikkeamat ilmoitetaan asiakkaalle?

Lisätietoja: PiTuKri TJ 04

4. Vaatimustenmukaisuus ja tietosuoja

Vähimmäissuojaukset

1. Pilvipalveluntarjoajan on tunnistettava, dokumentoitava ja päivitettävä säännöllisesti pilvipalveluun sovellettavien lakien ja säädösten määräykset sekä menettelyt näiden noudattamiseksi.
2. Pilvipalvelun toimintaan kohdistetaan vähintään vuosittain ulkoinen tai/ja sisäinen tarkastus, jonka tavoitteena on selvittää kuinka palvelu kokonaisuutena vastaa turvakäytäntöjensä ja sopimus- sekä lainsäädännöllisten vastuiden täyttämiseen.
3. Ylin johto vastaa siitä, että havaitut poikkeamat priorisoidaan ja korvaavat suojaukset tai korjaukset toteutetaan riittävän nopeasti.

Taustatietoa

Pilvipalveluntarjoajan tulee huolehtia esimerkiksi henkilötietojen käsittelyn turvallisuudesta yleisen tietosuoja-asetuksen (EU) 2016/679 32 artiklan mukaisesti. Henkilötietojen luokittelu ja luokittelun mukainen käsittely voi olla tarpeen, mikäli erilaisten henkilötietojen suojaustarpeet (oikeudelliset vaatimukset, arvo, arkaluonteisuus) eroavat tai/ja mikäli niitä käsitellään eroavasti suojattuna pilvipalveluntarjoajan eri toiminnoissa tai järjestelmissä.

Ota selvää

Kuinka pilvipalveluntarjoaja varmistaa sen, että tietosuoja toteutuu palvelussa? Kuinka pilvipalveluntarjoaja on tunnistanut siihen kohdistuvat lakisääteiset velvoitteet, sekä sopimuspohjaiset sitoumukset? Kuinka pilvipalveluntarjoaja varmistaa, että se täyttää toiminnassaan sekä lakisääteiset velvoitteet, että sopimuspohjaiset sitoumukset?

Lisätietoja: PiTuKri TJ 07

5. Työsuhteen elinkaari ja turvallisuus-tietoisuus

Vähimmäissuojaukset

Pilvipalveluntarjoajalla on käytössä turvallisuuden huomioon ottava menettely työsuhteen elinkaaren eri vaiheissa. Erityisesti huomioidaan toimenpiteet **a)** rekrytoitaessa, **b)** työtehtävien muutoksissa ja **c)** työsuhteen päättyessä.

Taustatietoa

Suojaustavoitteena on henkilöstöön liittyvien riskien pienentäminen työsuhteen elinkaaren aikana. 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.

Ota selvää

Kuinka pilvipalveluntarjoaja huomioi turvallisuuden henkilöstönsä työsuhteen elinkaaren eri vaiheissa? Kuinka turvallisuus huomioidaan esimerkiksi rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä? Kuinka pilvipalveluntarjoajan henkilöstön riittävästä turvallisuustietoisuudesta varmistutaan käytännön tasolla?

Lisätietoja: PiTuKri HT 01, HT 02, HT 03, HT 04

6. Tietojen ja toiminnan fyysinen turvallisuus

Vähimmäissuojaukset

1. Suojattavan tiedon fyysinen sijainti on kuvattuna koko tiedon elinkaaren ajalta.
2. Suojattavaan tietoon pääsy suojataan fyysisen turvallisuuden menetelmin. Suojattava tieto säilytetään lukitussa tilassa. Tilaan ei ole pääsyä palvelun tuottamiseen kuulumattomilla henkilöillä.
3. Siirrettäessä suojattavaa tietoa fyysisesti suojattujen tilojen ulkopuolella tai matalamman turvallisuustason verkon kautta, suojattava tieto siirretään käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia.

Taustatietoa

Oikeudeton fyysinen pääsy laitetiloihin tai epäsuora pääsy tietoon voi vaarantaa tiedon eheyden, luottamuksellisuuden ja saatavuuden. Asiakastiedon luottamuksellisuus tai eheys voi vaarantua myös tilanteissa, joissa asiakastietoa siirretään fyysisen pääsynhallinnan ulottumattomissa, tyypillisesti esimerkiksi Internetissä ja muissa turvattomissa tietoverkoissa. Suojattavaan asiakastietoon ei tule olla loogista tai fyysistä pääsyä ulkopuolisilla suoraan, tai tiedon käsittelyyn käytettävän laitteiston kautta epäsuoraan.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistanut sen, että asiakkaan palvelussa käsittelemä tieto on suojattu riittävin fyysisen turvallisuuden menetelmin? Kuinka palveluntarjoajan konesalien fyysinen turvallisuus on järjestetty? Onhan pilvipalveluntarjoajalla täsmällisesti tiedossa kaikki fyysiset ja loogiset sijainnit, minne asiakkaan tieto voi elinkaarensa aikana palvelussa kulkeutua? Onhan kaikki fyysisen turvallisuuden suojaamattomat yhteydet (esimerkiksi konesalien välillä) salattuja käyttötilanteeseen soveltuvalla menetelmällä?

Lisätietoja: PiTuKri FT 01, FT 02, FT 03, FT 04, JT 08, TA 01

7. Tietoliikenneverkon rakenne

Vähimmäissuojaukset

1. Pilvipalveluympäristö on erotettu muista ympäristöistä.
2. Pilvipalveluympäristö on ulkoreunan sisäpuolella jaettu erillisiin alueisiin (vyöhykkeet, segmentit, mikrosegmentit tai vastaavat).
3. Liikennöintiä rajoitetaan ja valvotaan siten, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan (default-deny) pilvipalveluympäristön ulkoreunalla ja sisäisten alueiden välillä.

Taustatietoa

Palvelun tuottamiseen liittyvän ympäristön liikenteen rajoittamisella vain välttämättömiin yhteyksiin tavoitellaan turvattomista verkoista tulevien hyökkäysten riskien pienentämistä sekä suojattavan ympäristön rajaamista hallittavaan kokonaisuuteen. Sisäisten alueiden välisellä suodatuksella tavoitellaan mahdollisten tietoturvapoikkeamien (ml. tietomurrot) tai niiden yritysten vahinkojen rajaamista sekä poikkeamien havainnointikykyä.

Ota selvää

Kuinka pilvipalveluympäristö on erotettu muista ympäristöistä? Millä periaatteilla pilvipalveluympäristö on ulkoreunan sisäpuolella jaettu erillisiin alueisiin (vyöhykkeet, segmentit, mikrosegmentit tai vastaavat)? Kuinka pilvipalveluntarjoaja varmistaa sen, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan?

Lisätietoja: PiTuKri TT 01

8. Käyttöoikeuksien hallinnointi

Vähimmäissuojaukset

1. Käyttäjätilien luontiin, hyväksymiseen ja ylläpitoon on ennalta määritelty prosessi.
2. Tietojenkäsittely-ympäristön käyttäjille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat tehtävien suorittamiseksi välttämättömiä.
3. Tarpeettomat käyttäjätilit ja oikeudet poistetaan, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta tai kun käyttäjätiliä ei ole käytetty ennalta määritettyyn aikaan).
4. On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen.
5. Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti, vähintään puolivuosittain.

Taustatietoa

Käyttöoikeuksien hallinnan keskeinen tavoite on pystyä varmistumaan siitä, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattavaan tietoon. Kaikkien käyttäjätunnusten osalta on huolehdittava tunnusten elinkaaresta siten, että vain tarpeelliset tunnukset ovat voimassa ja aktiivisia ja että tarpeettomat käyttäjätunnukset poistetaan välittömästi.

Käyttöoikeudet tulee rajata vain välttämättömiin toiminnallisuuksiin, sovelluksiin, laitteisiin ja verkkoihin. Tarpeettoman laajat oikeudet mahdollistavat ko. käyttäjälle, prosessille tai edellä mainitut haltuun saavalle hyökkääjälle tarpeettoman laajat toimintamahdollisuudet. Käyttöoikeuksien rajaamisella vähimpien oikeuksien periaatteen mukaiseksi voidaan pienentää sekä tahallisten että tahattomien tekojen, kuin myös esimerkiksi haittaohjelmista aiheutuvia riskejä. Erityisesti tulee huomioida, että ylläpito-oikeuksia käytetään vain ylläpitotoimiin. Ylläpitotunnuksella varustettua käyttäjätiliä ei tule käyttää esimerkiksi web-selailuun tai sähköpostin käyttöön.

Pääsyoikeuksien ajantasaisuudesta varmistuminen edellyttää yleensä sitä, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esimerkiksi kuuden kuukauden välein. Tehtävänkuvan muutoksissa ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen ja poistamiseen on oltava selkeä, sovittu menettely.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistanut, että vähimpien oikeuksien periaate toteutuu pilvipalvelun tarjoamiseen osallistuvan henkilökunnan osalta? Kuinka pilvipalveluntarjoaja on varmistunut esimerkiksi siitä, että käyttäjätilien luontiin, hyväksymiseen ja ylläpitoon laadittu prosessi toimii käytännössäkin? Kuinka pilvipalveluntarjoaja varmistuu siitä, että ylläpitohenkilöstölle on pääsyoikeudet vain sellaisiin järjestelmiin tai järjestelmäosiin, mitkä ovat välttämättömiä työtehtävien hoitamiseksi? Kuinka on varmistuttu siitä, että pääsyoikeudet pysyvät ajan tasalla myös ylläpitäjien työtehtävien muutoksissa?

Lisätietoja: PiTuKri JT 01

9. Käyttäjätunnistus

Vähimmäissuojaukset

1. Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ja asiakkaan ylläpitäjät sekä palvelun käyttäjät tunnistetaan ja todennetaan luotettavasti ennen pääsyä suojattavaan tietoon:
   - **a)** Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet.
   - **b)** Kaikki käyttäjät tunnistetaan ja todennetaan.
   - **c)** Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti.
   - **d)** Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia[2]
   - **e)** Käyttäjien todennus tehdään vahvasti, vähintään kahteen tekijään nojautuen (esimerkiksi salasana + token). Yhteys on salattu käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia.
   - **f)** Todennus tehdään fyysisesti suojatun alueen sisällä vähintään salasanaa käyttäen.

Taustatietoa

Suojaustavoitteena on tietoihin ja palveluihin pääsyn rajaaminen vain valtuutettuihin käyttäjiin.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistunut siitä, että kaikki käyttäjät, sekä pilvipalvelun tarjoajan, että asiakkaiden, tunnistetaan ja todennetaan luotettavasti, vähintään kahteen todennustekijään pohjautuen? Kuinka pilvipalveluntarjoaja on varmistunut siitä, että kaikki ylläpitäjät ja muut käyttäjät pystytään yksilöimään luotettavasti? Kuinka pilvipalveluntarjoaja on varmistunut siitä, että yhteydet ovat salattuja käyttötilanteeseen soveltuvalla menetelmällä?

Lisätietoja: PiTuKri JT 02, JT 08, TA 01

2 Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille.

10. Hallintayhteydet

Vähimmäissuojaukset

1. Hallintapääsy tapahtuu pilvipalveluympäristössä rajattujen, hallittujen ja valvottujen pisteiden (esimerkiksi hyppykoneet) kautta. Hallintapääsyn mahdollistavat pisteet on eriytetty toisistaan vähintään siten, että pilvipalveluntarjoajan ja eri asiakkaiden hallintapisteet, sekä niiden kautta saavutettavat palvelut, ovat toisistaan luotettavasti eroteltuna.
2. Hallintapääsyn tulee edellyttää vahvaa, vähintään kahteen todennustekijään (esimerkiksi salasana + token) pohjautuvaa käyttäjätunnistusta.
3. Hallintaliikenne on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia.

Taustatietoa

Suojaustavoitteena on hallintayhteyksien suojaus riittävällä tasolla, jotta niitä hyödyntämällä ei ole asiakastietoon tai pilvipalveluun valtuuttamatonta pääsyä.

Ota selvää

Kuinka pilvipalveluympäristön tekniset hallintayhteydet on suojattu? Onhan hallintapääsy mahdollista vain rajattujen, hallittujen ja valvottujen pisteiden (esimerkiksi hyppykoneet) kautta? Edellyttäähän hallintapääsy vahvaa, vähintään kahteen todennustekijään (esimerkiksi salasana + token) pohjautuvaa käyttäjätunnistusta? Onhan myös hallintaliikenne salattua käyttötilanteeseen soveltuvalla menetelmällä?

Lisätietoja: PiTuKri TT 03, JT 08, TA 01

11. Jäljitettävyys ja havainnointikyky

Vähimmäissuojaukset

1. Luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen on toteutettu. Erityisesti:
   a) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen.
   b) Keskeiset tallenteet säilytetään vähintään 3 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa.
   c) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta) vähimpien oikeuksien periaatteen mukaisesti.
2. Luotettavat menetelmät turvallisuuspoikkeamien havaitsemiseksi on toteutettu. Erityisesti:
   a) On olemassa menettely, jolla kerätyistä tallenteista pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan).
   b) Verkkoliikenteen normaali tila on tiedossa.
   c) On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan.
3. On olemassa menettely havaituista poikkeamista toipumiseen.

Taustatietoa

Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitseminen ja selvittäminen, ml. tietomurtojen tutkinta ja korjaavien toimien suunnittelun tukena toimiminen.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistunut siitä, että turvallisuuteen liittyvät tapahtumat ovat jäljitettävissä? Kuinka pilvipalveluntarjoaja on varmistunut siitä, että esimerkiksi tietomurto- tai muut väärinkäytösta-

paukset voidaan jälkikäteen selvittää lokitiedoista? Kuinka pitkään lokitiedot säilytetään? Kuinka pilvipalveluntarjoaja on varmistunut siitä, että se pystyy havainnoimaan turvallisuuspoikkeamat ympäristössään? Millaisia turvallisuuspoikkeamia pilvipalveluntarjoaja on havainnut viimeisen puolen vuoden aikana, ja miten nämä on havaittu?

Lisätietoja: PiTuKri JT 03

12. Järjestelmäkovennus

Vähimmäissuojaukset

1. Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus.
2. Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.

Taustatietoa

Turvallisen ohjelmistokoodin tekeminen on osoittautunut haastavaksi. Mitä enemmän ympäristössä on ohjelmistokoodia, sitä enemmän on mahdollisuuksia ohjelmistovirheille, toisin sanoen haavoittuvuuksille. Mitä enemmän ohjelmistokoodin turvallisuuteen nojaavia palveluja on tarjolla, sitä todennäköisempää on, että palveluissa on myös haavoittuvuuksia. Riskejä voidaan pienentää haavoittuvuuspinta-alaa pienentämällä, toisin sanoen tarjoamalla vain välttämättömiä palveluja alttiiksi hyökkäyksille.

Järjestelmät ovat yleensä tulvillaan ominaisuuksia. Ominaisuudet ovat yleensä oletusarvoisesti päällä ja helppo ottaa käyttöön. Ominaisuudet ovat toisaalta usein myös tarpeettoman turvattomilla asetuksilla. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, nämä ovat myös pahantahtoisen toimijan käytettävissä. Jos välttämättömien palvelujen tarpeettoman turvattomia asetuksia ei muuteta, ovat nämä myös pahantahtoisen toimijan käytettävissä. Järjestelmissä on oletusarvoisesti usein käytössä esimerkiksi ennalta määriteltyjä ylläpitosalasanoja, valmiiksi asennettuja tarpeettomia ohjelmistoja ja tarpeettomia käyttäjätilejä.

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, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä, jotta rajoitetaan onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistanut, että pilvipalveluympäristö ei ole haavoittuva tarpeettomien toiminnallisuuksien tai palvelujen heikkouksien takia? Millaiset menettelytavat pilvipalveluntarjoajalla on käytössään sen varmistamiseksi, että järjestelmät on kovennettu järjestelmällisesti ja sisältävät vain välttämättömät toiminnallisuudet?

Lisätietoja: PiTuKri JT 04

13. Tiedon erottelu

Vähimmäissuojaukset

Asiakkaiden tiedot säilytetään luotettavasti toisistaan eroteltuna yhteiskäyttöisissä virtuaalisissa ja fyysisissä järjestelmissä.

Taustatietoa

Jos samaa laitteistoa käytetään useiden asiakkaiden tiedon käsittelyyn samanaikaisesti, tulee varmistua siitä, että tietojen erottelu on riittävän turvallinen, eikä asiakkaan tietoihin ole pääsyä muilla asiakkailla. Erottelu on toteutettava riittävän luotettavasti, joko loogisen tai/ja fyysisen erottelun menetelmillä. Eräs yleinen käytössä oleva erottelumenetelmä esimerkiksi yhteiskäyttöisten verkkolaitteiden ja tallennusjärjestelmien osalta on salaus. Asiakaskohtaisilla avaimistoilla toteutettavaa tietoliikenteen salausta (data-in-transit) ja salausta tallennettaessa (data-at-rest) voidaan hyödyntää myös muiden turvatavoitteiden, esimerkiksi laitteistojen turvallisen hävittämisen, tukevana suojauksena.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistanut, että eri asiakkaat eivät pääse käsiksi toistensa tietoihin? Kuinka on varmistuttu siitä, että yhden asiakkaan järjestelmän kautta ei ole pääsyä muiden asiakkaiden järjestelmiin tai tietoihin esimerkiksi tilanteessa, jossa yhden asiakkaan omalla vastuulla olevassa järjestelmäosassa on turvallisuuspuutteita?

Lisätietoja: PiTuKri JT 05

14. Suojattavien tietojen ja laitteistojen turvallinen hävittäminen ja uusiokäyttö

Vähimmäissuojaukset

1. Tietoaineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
2. Hävittäminen kattaa koko asiakkaan tiedon elinkaaren siltä osin, kun tieto on ollut pilvipalvelussa.

Taustatietoa

Asiakkaan tietojen luottamuksellisuuden ei tule vaarantua tilanteissa, joissa sen käsittelyyn käytetyt tallennemediat ja vastaavat järjestelmät poistetaan käytöstä, tai kyseinen asiakastieto tulee muista syistä johtuen poistaa pilvipalvelusta.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistunut siitä, että asiakkaan tiedot hävitetään palvelusta luotettavasti silloin, kun asiakas pyytää tietojensa hävittämistä (esimerkiksi lopettaessaan palvelun käytön) ja silloin, kun asiakastiedon käsittelyyn käytetty laite poistetaan käytöstä, tai esimerkiksi vioittunut laitteisto vaihdetaan toiseen?

Lisätietoja: PiTuKri TA 03

15. Jatkuvuuden varmistaminen

Vähimmäissuojaukset

1. Pilvipalveluntarjoajan jatkuvuudenhallinnan prosessit ja menettelyt on suunniteltu, toteutettu, testattu ja kuvattu siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin.
2. Järjestelyissä huomioidaan erityisesti, että **a)** toipuminen ja jatkuvuuden varmistaminen toimintavaatimuksiin nähden riittävässä ajassa on huomioitu suunnittelussa, ja että **b)** asiakkaan tiedot ovat palautettavissa riittävän kattavasti.

Taustatietoa

Jatkuvuudenhallinnan tavoitteena on varmistaa palvelun jatkuvuus siten, että pystytään vastaamaan siihen kohdistuneisiin käytettävyys-, eheys- ja luottamuksellisuusvaatimuksiin. Esimerkiksi laiterikot tai konfigurointivirheet voivat johtaa asiakastiedon käsittelyn estymiseen.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistunut siitä, palvelu ja asiakkaan palveluun tallentavien tietojen käytettävyys (saatavuus) varmistetaan? Kuinka palvelu on suojattu esimerkiksi laitteistorikkojen tai virhekonfiguraatioiden varalta? Kuinka asiakkaan tiedot ja keskeiset järjestelmäkonfiguraatiot on varmuuskopioitu, kuinka varmuuskopiot on suojattu, ja kuinka varmistuttu siitä, toipuminen häiriötilanteesta on mahdollista riittävän nopeasti?

Lisätietoja: PiTuKri TJ 05, FT 05, KT 01, KT 03

16. Haavoittuvuuksien hallinta

Vähimmäissuojaukset

Pilvipalvelun koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi. Erityisesti huomioitava:

a) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja riskiperusteisesti tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti.

b) Julkiseen verkkoon tarjottavien palvelujen/sovellusten rajapintojen on kestettävä yleiset hyökkäysmenetelmät ilman, että palvelussa/sovelluksessa käsiteltävien tietojen luottamuksellisuus, eheys tai käytettävyys vaarantuu.

Taustatietoa

Turvallisen ohjelmistokoodin tekeminen on osoittautunut haastavaksi. Ohjelmistovirheiden, toisin sanoen haavoittuvuuksien, hyödyntäminen on useissa hyökkäystyypeissä jossain vaiheessa mukana. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Riskejä voidaan pienentää korjausten asennuksilla.

Haavoittuvuuksien hallintaan liittyy ohjelmisto- ja järjestelmäympäristön jatkuva seuranta ja kehittäminen siten, että ohjelmistotoimittajien haavoittuvuuskorjaukset voidaan asentaa mahdollisimman nopeasti. Lisäksi on syytä seurata käytettävien ohjelmistoversioiden tukea niiden toimittajalta. Vanhentuneisiin ohjelmistoversioihin ei julkaista aktiivisesti päivityksiä, jolloin myös tietoturvahaavoittuvuuksien korjaaminen voi olla mahdotonta. Palvelujen/sovellusten rajapintojen turvallisuussuunnittelussa ja -arvioinnissa voidaan hyödyntää esimerkiksi OWASP-yhteisön[3] suosituksia.

Ota selvää

Kuinka pilvipalveluntarjoaja on varmistunut, että ohjelmistohaavoittuvuuksien hallintaprosessit toimivat käytännössäkin? Kuinka on varmistuttu siitä, että tunnettuja haavoittuvuuksia sisältävät ohjelmistot tulevat päivitetyiksi korjatuilla versioilla riittävän nopeasti? Kuinka on varmistuttu siitä, että pilvipalveluntarjoajan mahdolliset itsekehitetyt ohjelmistot ovat riittävän hyvin suojattuja?

Lisätietoja: PiTuKri KT 04, MH 02

3 The Open Web Application Security Project (OWASP) Foundation. 2019. URL: https://www.owasp.org/.

Kuinka varmistua, että hyvät käytännöt toteutuvat

Pilvipalvelujen tietoturvallisuuskäytäntöjen riittävyydestä varmistumiseen liittyy useita haasteita. Yksityishenkilöillä, pienyhteisöillä tai -yrityksillä ei yleensä ole mahdollisuuksia esimerkiksi pilvipalveluntarjoajan tietoturvallisuuskäytäntöjen syvälliseen arviointiin. Joskus tietojen suojaamisen arvioinnissa saattaakin olla mahdollista nojautua esimerkiksi vain pilvipalveluntarjoajan tuottamaan itsearviointiin, mahdollisiin muihin sertifiointeihin sekä sopimusteknisiin sitoumuksiin.

Edellisissä luvuissa kuvatut tietoturvallisuuden hyvät käytännöt sisältyvät useisiin tietoturvallisuuden viitekehyksiin joko sellaisinaan, tai vain pienin eroavaisuuksin. Mikäli pilvipalveluntarjoaja toteuttaa toiminnassaan esimerkiksi ISO27001[4]- ja ISO27017[5]-standardien, CSA-pilviturvallisuusyhteisön suojausmatriisin[6], PiTuKrin tai Katakri-kriteeristön[7] mukaisia suojauksia, myös yleisimmät hyvät käytännöt saattavat olla pilvipalveluntarjoajalla jo toteutettuina. Erilaisiin viitekehyksiin ja niiden mukaisen toiminnan arviointiin liittyy kuitenkin useita tekijöitä, jotka voivat vaikuttaa siihen, millainen varmuus esimerkiksi sertifiointien luotettavuudella todellisuudessa on[8].

Kyberturvallisuuskeskus on käynnistänyt selvityksen siitä, kuinka yksityishenkilöiden, pienyhteisöjen ja -yritysten pilvipalveluiden tietoturvallisuustarpeita voitaisiin paremmin tukea. Eräänä selvityksessä tutkittavana vaihtoehtona on pilvipalveluiden kevytsertifiointijärjestely, joka tuottaisi yksityishenkilöille, pienyhteisöille ja -yrityksille helposti hyödynnettävän tavan valita hyvillä tietoturvallisuuskäytännöillä suojattuja pilvipalveluja. Kevytsertifiointijärjestely pyrkisi hyödyntämään palveluntarjoajien jo tekemää tietoturvallisuustyötä, sekä huomioimaan muun muassa EU-laajuiset pilvipalvelujen käyttöön ja sertifiointiin liittyvät hyödyntämismahdollisuudet. Osana selvitystä tullaan julkaisemaan myös ristiinvertailutaulukko tässä ohjeessa kuvattujen tietoturvallisuuskäytäntöjen ja yleisimpien muiden viitekehysten vastaavuuksista.

4 ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.
5 ISO/IEC 27017:2015 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
6 Cloud Security Alliance. 2018. The Cloud Security Alliance Cloud Controls Matrix (CCM). URL: https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix.
7 Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. URL: http://www.defmin.fi/Katakri.
8 Lisätietoa pilvipalvelujen arvioinnista: PiTuKri, luku Arviointimenetelmät.

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000
traficom.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus