VALTIOVARAINMINISTERIÖ

Sovellus-kehityksen tieto-turva-ohje

1/2013 VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä

VALTIOVARAINMINISTERIÖ

Sovelluskehityksen tietoturvaohje

Valtionhallinnon tietoturvallisuuden johtoryhmä

1/2013 VAHTI

Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila /VM-julkaisutiimi

ISSN 1455-2566 (nid.)
ISBN 978-952-251-417-2 (nid.)
ISSN 1798-0860 (PDF)
ISBN 978-952-251-418-9 (PDF)

Juvenes Print – Suomen Yliopistopaino Oy, 2013

VALTIOVARAINMINISTERIÖ
Julkisen hallinnon ICT-toiminto

Ohje

VM/144/00.00.00/2013
VM047:14/2007

31.1.2013

Ministeriöille, virastoille ja laitoksille

Sovelluskehityksen tietoturvaohje

Valtionhallinnon tietoturvallisuusasetuksen (681/2010) mukaan valtionhallinnon organisaatioiden tulee saavuttaa tietoturvallisuuden perustaso 30.9.2013 mennessä. Sovellusten tietoturvallisuudella on keskeinen merkitys tietojärjestelmissä käsiteltävien tietojen suojaamisessa ja kyberuhkiin varautumisessa. Kyberturvallisuuden yksi edellytys on turvallinen ICT-infrastruktuuri. Tämä on otettava huomioon sovelluksia kehitettäessä.

Nyt julkaistava Sovelluskehityksen tietoturvaohje on tarkoitettu esimiehille, hankkeiden vetäjille, sovelluskehittäjille sekä tietoturvallisuudesta vastaaville. Ohjeen tavoitteena on opastaa sovelluskehittäjiä ottamaan tietoturvavaatimukset huomioon kaikissa vaiheissa. Tietoturvallisuuden ottaminen huomioon sovelluskehityksen alusta lähtien on olennaista niin turvallisuuden toteuttamisen kuin kustannustehokkuudenkin näkökulmasta.

Sovelluskehitysohjeessa on otettu huomioon muun muassa tietoturvallisuusasetuksen ja siihen liittyvien toteutusohjeiden sovelluskehitykselle esitettyjä tietoturvavaatimuksia. Ohjeeseen on myös sisällytetty kansainvälisten tietoturvavelvoitteiden todentamiseen käytettävän kansallisen turvallisuusauditointikriteeristön sovelluskehitystä koskevat vaatimukset.

Hallinto- ja kuntaministeri — Henna Virkkunen

Yksikön päällikkö — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liitteet — Sovelluskehityksen tietoturvaohje (VAHTI 1/2013)

Tiedoksi — Kunnat

Valtiovarainministeriö
Snellmaninkatu 1 A, Helsinki
PL 28, 00023 Valtioneuvosto
www.vm.fi

Puh 0295 16001 (vaihde)
Faksi 09 160 33123
valtiovarainministerio@vm.fi
Y-tunnus 0245439-9

Tiivistelmä

Sovellusten tietoturvallisuudella on keskeinen merkitys tietojärjestelmissä käsiteltävien tietojen suojaamisessa. Yhteiskunnan toiminta on yhä verkottuneempaa ja palveluja tarjotaan yhä enemmän internetin kautta, missä sovellukset ovat lisääntyvässä määrin alttiita haavoittuvuuksille ja verkosta tuleville uhkille. Kyberturvallisuus rakentuu pitkälti turvallisen ICT-infrastruktuurin päälle. Tämä on otettava huomioon sovelluksia rakennettaessa. Haittaohjelmat hyödyntävät verkossa käytettävien sovellusten tietoturva-aukkoja ja voivat levitä myös organisaation sisäverkon järjestelmiin, jolloin myös sisäiset palvelut ja salassa pidettävät tiedot voivat olla uhattuina.

Valtionhallinnon normit asettavat organisaatioille velvoitteita kehittää hallinnollista ja teknistä tietoturvallisuuttaan. Tietoturvallisuusasetuksen (681/2010) mukaan organisaatioiden tulee saavuttaa tietoturvallisuuden perustaso 30.9.2013 mennessä. Sovelluskehitysohjeessa on otettu huomioon muun muassa tietoturvallisuusasetuksen ja siihen liittyvän toteutusohjeen VAHTI (2/2010) vaatimuksia sekä tietohallintolaissa (634/2011), VAHTIn Keskeisten tietojärjestelmien tietoturvaohjeessa (5/2004) ja muissa VAHTI-ohjeissa sovelluskehitykselle annettuja tietoturvavaatimuksia. Ohjeeseen on myös sisällytetty kansallisen turvallisuusauditointikriteeristön (KATAKRI II) sovelluskehitystä koskevat vaatimukset. Ne tulee huomioida, jos kehitettävän sovelluksen avulla käsitellään kansainvälisiä turvallisuusluokiteltuja tietoaineistoja tai käyttö liittyy Suomen valtion turvallisuuteen.

Ohjeen tavoitteena on opastaa sovelluskehittäjiä ottamaan tietoturvavaatimukset huomioon kaikissa vaiheissa jo sovelluskehityksen alusta lähtien. Ohjeesta löytyvät sovelluskehityksen eri vaiheisiin liittyvät tietoturvavaatimukset, jotka suositellaan liitettäväksi organisaation käytössä olevaan systeemityömalliin, perustui tämä sitten lineaariseen tai iteratiiviseen toimintatapaan. Ohjeessa eri vaiheiden tietoturvavaatimukset on esitetty lineaarisen eli ”vesiputousmallin” mukaisesti, mutta samat vaatimukset tulee ottaa huomioon ja toteuttaa myös iteratiivisessa toimintamallissa. Ohjetta voidaan soveltaa myös tarjouspyyntöjen vaatimusmäärittelyihin kun toimittajilta tilataan räätälöityjä sovelluksia. Ohje perustuu vahvasti tietoturvatasoajatteluun ja tietoturvatasoissa esitettyihin vaatimuksiin. Alkuosassa on esitetty myös sovelluskehitysympäristön yleisiä vaatimuksia ja suosituksia huomioiden kehityshankkeeseen osallistuvien henkilöiden roolit ja tehtävänjako.

Ohje on tarkoitettu esimiehille, hankkeiden vetäjille, sovelluskehittäjille sekä tietoturvallisuudesta vastaaville. Sovelluskehityksestä vastaavien esimiesten on hyvä lukea erityisesti alkukappaleet. Koko ohje on tarkoitettu sovelluskehityshankkeisiin osallistujille. Sovel-

luskehittäjiä varten ohjeeseen on otettu mukaan tarkennettuja teknisiä ohjeita ja linkkejä hyviin käytäntöihin. Esitetyt tietoturvavaatimukset on koottu ohjeen lopussa olevaan liitetiedostoon, jossa esitetään myös vaatimusten velvoittavuus.

Ohjeen tavoitteena on toimia sovelluskehitysprosessin tietoturvaohjeena ja edesauttaa tietoturvallisten, tietoturvatasojen vaatimukset täyttävien, sovellusten ja palveluiden kehittämistä. Ohje koskee uusia, kehitettäviä järjestelmiä, ei jo olemassa olevia järjestelmiä.

Ohje on laadittu VAHTIn alaisessa hankeryhmässä, jonka jäseninä ovat toimineet Pirkko Kilpeläinen (pj), Tuomo Ahjokannas, Hellevi Huhanantti, Lauri Karppinen, Terja Ketola, Topi Laamanen ja Pasi Rouvinen. Ohjeen kirjoittajina ovat toimineet KPMG:n konsultit Antti Alestalo, Matti Järvinen ja Tuomo Makkonen.

Sisältö

1 Johdanto

1.1 Yleistä

Sovellusten hyvällä tietoturvallisuudella on yhä tärkeämpi merkitys organisaatioiden tietojärjestelmien ja tietoaineistojen suojaamisessa. Organisaation tärkeitä tietoja käsitellään lähes pelkästään sovellusten kautta ja verkottuneessa yhteiskunnassa monien sovellusten ja palvelujen tulee olla käytettävissä internetin välityksellä, jolloin ne ovat alttiita uhkille ja haavoittuvuuksille.

Järjestelmien tietoturvallisuuden toteuttaminen vaatii sovellusten turvallisuudesta huolehtimista, jotta sovellusten avulla käsiteltävät salassa pidettävät tiedot eivät päädy ulkopuolisten käsiin tai muutu hallitsemattomasti. Sovelluksen ja tietoaineiston tulee myös tarvittaessa olla käytettävissä.

Tämän ohjeen tavoitteena on auttaa valtionhallinnon organisaatioita toteuttamaan sovelluskehityksessä vaaditut tietoturvatehtävät heti kehityksen alkuvaiheesta lähtien, ja auttaa myös sovellushankintojen vaatimusmäärittelyjen tekemisessä.

1.2 Ohjeen tausta, tarkoitus ja kohderyhmät

Sovelluskehitys on mullistunut viime vuosina merkittävästi. Nopeaan käyttöönottoon perustuvat kehitysmenetelmät ovat korvanneet monessa organisaatiossa ja sovelluskehitysprojektissa perinteisen vesiputousmallin. Organisaatioissa on myös otettu käyttöön avoimen lähdekoodin ohjelmistoja ja ohjelmakirjastoja. Lisäksi organisaatiot ovat ulkoistaneet sovelluskehitystä siihen keskittyneille kumppaneille.

Myös sovellusten suojaamisen tarve on muuttunut. Aiemmin monet sovellukset suunniteltiin vain sisäverkkokäyttöön, jolloin palomuurin vastuulla oli merkittäväkin osa sovelluksen turvallisuudesta. Nykyään sovelluksia tarjotaan enemmän näkyviin myös julkisiin verkkoihin. Vaikka myös organisaatioiden verkkorakenteet ovat kehittyneet, niin perinteisten palomuurien suojaus ei yksin riitä. Sovellukset on rakennettava sellaisiksi, että ne itsessään kestävät toistuvia verkkohyökkäyksiä ilman verkon ja erillisten sovelluspalomuurien tarjoamaa suojaa.

Tämän ohjeen tarkoituksena on

- Tukea sovelluskehitystä niin, että sovellukset saavuttavat riittävän tietoturvallisuuden tason suhteessa sovelluksen käyttökohteisiin
- Tukea julkishallinnon organisaatioita sovelluskehityshankkeiden läpiviennissä, valmisohjelmistojen hankinnoissa sekä ylläpitoon liittyvissä tietoturvatehtävissä
- Varmistaa julkishallinnon sovellusten tietoturvallinen toteutus niin, että tietoturvatoimenpiteillä suojataan tietoaineistojen luottamuksellisuutta ja eheyttä,
- Turvata organisaatioiden toiminnan jatkuvuus kaikissa olosuhteissa niin, että tietojärjestelmät ovat käytettävissä
- Mahdollistaa sovelluskehityksen arviointi tietoturvatasojen mukaisesti
- Toimia vaatimusmäärittelyn tukena sovelluskehitystyötä hankittaessa

Ohjeen laatimisessa tavoitteena on ollut, että sitä pystyvät käyttämään organisaatiot, joka tekevät itse sovelluskehitystä sekä organisaatiot, jotka tilaavat sovelluskehityksen kumppaneiltaan. Ohje on kirjoitettu vahvasti vaatimusmuotoon perustuen Tietoturvallisuusasetuksesta (681/2010) valtionhallinnolle tuleviin tietoturvatasojen vaatimuksiin, jolloin ohjetta voidaan käyttää myös kumppaneiden ohjaukseen.

Ohje on suunnattu julkishallinnon sovelluskehittäjille ja heidän esimiehilleen. Muita kohderyhmiä ovat johto, sovelluksia hankkivat ja tilaavat henkilöt, sovelluskehityksen projektipäälliköt, sovelluskehitysmallien suunnittelijat, tietohallintovastaavat ja tietoturvavastaavat.

Johdon ja tietohallintovastaavien sekä niiden, jotka haluavat saada yleiskuvan tietoturvallisuuden toteuttamisesta osana sovelluskehitystä, kannattaa lukea kappaleet 1 3.2. Niiden, jotka haluavat saada syvällisemmän kuvan ohjeen vaatimuksista, kuten sovelluskehitysmallien suunnittelijat, on syytä lukea myös ohjeen muut osat.

Sovelluskehityksellä tässä ohjeessa tarkoitetaan ohjelmoinnin lisäksi sovelluksen elinkaaren kaikkia vaiheita, alkaen esitutkimuksesta ja päättyen käytöstä poistamiseen. Yksittäisen sovelluksen kehityksen lisäksi ohjeessa käsitellään organisaatioon liittyviä yleisiä vaatimuksia, jotka vaikuttavat sovelluskehityksen turvallisuuteen. Tätä ohjetta täydentää Valtionhallinnon keskeisten tietojärjestelmien turvaaminen -ohje (VAHTI 5/2004).

Ohjeessa kuvataan erilaisia tehtäviä ja vaatimuksia, joilla organisaation sovelluskehitysmallin tietoturvallisuutta voidaan parantaa. Ohjetta käyttävien organisaatioiden vastuulle jää ohjeen integroiminen omaan sovelluskehitysprosessiinsa. Tehtävät ja vaatimukset on määritelty tietoturvatasojen mukaisesti. **Ohje on tarkoitettu sovellettavaksi jokaisen valtionhallinnon organisaation omaan toimintaan.**

Tehtävät ja vaatimukset on jaettu ympäristön vaatimuksiin (organisaation tietoturvallisuuden hallinta) sekä sovelluskehityksen osa-alueisiin (projektin aikaiset vaatimukset) seuraavasti:

Ympäristön vaatimukset:
- Strategia ja resursointi
- Politiikat
- Riskienhallinta
- Osaaminen ja koulutus
- Tekninen sovelluskehitysympäristö
- Jatkuvuuden hallinta

Sovelluskehityksen osa-alueet:
- Esitutkimus
- Vaatimusmäärittely
- Suunnittelu
- Toteutus
- Testaus
- Käyttöönotto
- Ylläpito
- Käytöstä poistaminen

Eri tehtävien toteuttamiselle tulee määritellä organisaatiossa vastuuhenkilöt, jotta niiden toteutuminen voidaan varmistaa. Osan tehtävistä voi toteuttaa kolmas osapuoli. Kuitenkaan vastuuta tietoturvallisesta sovelluskehityksestä ei voida siirtää kolmannelle osapuolelle, vaan organisaation tulee itse varmistua tehtävien ja vaatimusten toteuttamisesta.

Ohjeessa ei käsitellä soveltuvuusselvitystä (feasibility study), jossa tarkastellaan hankkeen kannattavuutta ja järkevyyttä. Kullakin organisaatiolla tulee olla siitä omat ohjeistuksensa. Ohjeessa ei myöskään käsitellä mitään tiettyä sovelluskehitysmallia tai -menetelmää muuten kuin esimerkkimielessä.

Tässä ohjeessa käytetään seuraavia termejä kuvaamaan kontrollien tärkeyttä ja toteuttamisvelvollisuutta eri tietoturvatasoilla:
- Pakollinen vaatimus: Organisaation täytyy ottaa käyttöön tämän ohjeen mukainen toiminto. Poikkeuksen voi tehdä vain siinä tapauksessa, että kirjallisen riskianalyysin mukaan siitä seuraa vain pieni riski ja toiminnon toteuttaminen vaatii runsaasti resursseja. Sovelluksen tai sovelluskehitysprosessin omistaja hyväksyy toteutettavan ratkaisun etukäteen. Kansainvälisen turvallisuusluokitellun aineiston osalta Viestintäviraston NCSA-FI-yksikön on kirjallisesti hyväksyttävä toteutettava ratkaisu etukäteen. Riskianalyysiin on saatavilla Valtion IT-palvelukeskuksen Tietoturvapalveluista prosessiohje ja työväline.
- Vahva suositus: Organisaatio voi tehdyn kirjallisen riskianalyysin perusteella olla ottamatta suosituksen mukaista toimintoa käyttöön.
- Suositus: Hyvä käytäntö, jonka organisaatio voi halutessaan ottaa käyttöön.

Tämä luokittelu on luettavuuden vuoksi ainoastaan ohjeen liitteenä olevassa Excel-taulukossa.

Ohjeessa käytetyt termit löytyvät ohjeesta Valtionhallinnon tietoturvasanasto (VAHTI 8/2008).

2 Sovelluskehityksen tietoturvallisuus ja hallinnointi

Sovelluskehitystä tekevän organisaation tulee yleisellä tasolla selvittää mitkä lait, asetukset ja muut vaatimukset koskevat sen toimintaa ja sovelluskehitystä. Lisäksi organisaation on selvitettävä mahdolliset sovelluskohtaiset vaatimukset ja varmistaa niiden toteutuminen sovelluskehityksen aikana.

Sovelluksen tietoturvavaatimuksia tulee kartoittaa tietoturvallisuuden eri osa-alueiden näkökulmasta:

- Luottamuksellisuus – Tietoa voivat käsitellä vain sellaiset henkilöt, joilla on siihen oikeus
- Eheys – Tieto ei saa muuttua tahattomasti tai hyökkäyksessä, ja jos tieto muuttuu niin se pitää ainakin havaita
- Saatavuus – Tieto tai tiedon saantiin tarvittava palvelu on saatavilla ja käytettävissä, kun sitä tarvitaan
- Jäljitettävyys – Tarvittaessa tulee olla selvitettävissä, mitä järjestelmässä on tehty, kuka toimenpiteen on tehnyt ja milloin se on tehty

Sovelluskehityksen tietoturvavaatimusten lähtökohta on sovelluksen kriittisyys ja sovelluksessa käsiteltävän tiedon merkitys organisaation toiminnalle.

Tietoaineistoja käsitellään lähes aina jonkin sovelluksen avulla. Tietoaineiston luottamuksellisuuden säilyminen riippuu siitä, kuinka luotettava ja tietoturvallinen sovellus on. Käsiteltävän tiedon perusteella sovellus pystytään luokittelemaan, sekä rakentamaan siten, että se sopii käytettäväksi aiottuun tarkoitukseen. Tietoturvavaatimuksia laadittaessa pitää ottaa huomioon edellä mainitut luottamuksellisuus, eheys, saatavuus ja jäljitettävyys. Se, mitä tietoturvallisuuden osa-alueita painotetaan, riippuu kehitettävästä sovelluksesta ja sen aiotusta käyttötarkoituksesta. Tämän ohjeen vaatimuksia tulee soveltaa laadittavassa sovelluksessa käsiteltävän tiedon julkisuusasteen mukaan. Esimerkiksi jos sovellusta käytetään vain julkisen tiedon katseluun, ei käyttäjien tunnistusta välttämättä tarvitse toteuttaa.

Sovelluskehitystä tehtäessä tulee erottaa toisistaan termit palvelu, tietojärjestelmä ja sovellus:

- **Sovellus** on ohjelma, jota suoritetaan jonkin alustan käyttöjärjestelmän, sovelluspalvelimen yms. päällä.
- **Tietojärjestelmä** on ihmisistä, laitteista ja sovelluksista muodostuva kokonaisuus, jonka avulla pyritään kehittämään tai tehostamaan toimintaa.
- **Palvelusta** puhutaan yleensä, kun tarkoitetaan käyttäjän rajapintaa johonkin tietojärjestelmään.

Tässä ohjeessa keskitytään tietoturvallisuuteen nimenomaan sovelluksen kehittämisen näkökulmasta.

Sovelluskehityshankkeessa on eri tehtäville omat roolit ja tietoturvavastuut. Hankekohtaisesti tulee arvioida, onko tarvetta henkilöiden taustatarkistusten tekemiselle tai vaitiolositoumuksille. Hankkeen käynnistyessä tulee arvioida soveltuvien kehitystyövälineiden, ympäristön ja työtilojen turvallisuus, tehdäänkö työ omissa vai toimittajan tiloissa sekä tilojen maantieteellinen sijainti. Sovelluskehitystä tekevän ryhmän lisäksi tietoturvallisuuden kannalta hyvin olennaista on, että organisaatiossa on tietoturvallisuuden asiantuntijataho, kuten tietoturvaryhmä tai tietoturva-asiantuntija, joka tarjoaa ohjeita sekä konsultoivaa apua sovelluskehitykseen liittyvissä tietoturva-asioissa.

2.1 Arkkitehtuuri

Kokonaisarkkitehtuuri on suunnitelma organisaation muodostaman kokonaisuuden ja sen osien rakenteesta ja osien välisistä suhteista. Kokonaisarkkitehtuuri kuvaa, kuinka organisaation toimintaprosessit, tiedot, järjestelmät ja niiden tuottamat palvelut toimivat kokonaisuutena. Kokonaisarkkitehtuurisuunnittelun avulla löydetään ja jäsennetään tarvittavat elementit sekä kuvataan niiden väliset suhteet ja riippuvuudet.

Kokonaisarkkitehtuuri tuo välineen organisaation johtamiseen liittyvän suunnittelun ja päätöksenteon kokonaisuuden hallintaan. Kytkemällä kokonaisarkkitehtuurisuunnittelu osaksi hanke- ja projektitoimintaa, varmistetaan lopputulosten tarkoituksenmukaisuus kokonaisuuden kannalta.

Kokonaisarkkitehtuurin näkökulmat ovat siis toiminta, tiedot, tietojärjestelmät ja teknologia. Jokaiseen näistä näkökulmista sisällytetään tarvittavat tietoturvaratkaisut. Tietoturva-arkkitehtuuri koostuu näiden eri näkökulmien sisältämistä tietoturvaratkaisuista. Jotta sovellusten tietoturvallisuutta ei tehtäisi pelkästään päälle liimattuna osa-alueena, tietoturva-arkkitehtuurin huomioon ottaminen sovelluskehitystyössä sekä tietoturvallisuuden integrointi sovelluksiin ovat tämän ohjeen keskeisiä tavoitteita.

Sovelluskehitys perustuu monitasoarkkitehtuuriratkaisuihin varsinkin silloin, jos sovelluksia tullaan käyttämään internetin kautta. Sovellusympäristön arkkitehtuuriratkaisuilla on myös oleellinen vaikutus siihen, kuinka sovellusten avulla käytettävän tietoaineiston tietoturvallisuus toteutuu. Tietoturvaratkaisuissa tulee ottaa huomioon muun muassa verkkorakenteiden osittaminen, tiedonsiirron salaaminen, laitteiden, sovellusten ja käyttäjien

tunnistaminen, salaustuotteiden käyttö ja turvalliset etäkäyttöratkaisut. Arkkitehtuurivaatimuksia on käsitelty tarkemmin kappaleessa 3.3.3 Suunnittelu.

2.2 Sovelluskehitys ja tietoturvahaasteet

Tietojärjestelmien tietoturvallisuuden keskeinen tekijä on sovellusten tietoturvallisuus. Monet kehitettävät sovellukset asennetaan siten, että niihin on pääsy internetistä, jolloin tietoturvallisuuden hyvä toteuttaminen korostuu. Erillisiin tietoturvatuotteisiin kuten palomuureihin (ja nykyään esimerkiksi sovelluspalomuureihin ja tunkeutumisen havainnointi- ja estojärjestelmiin) on jouduttu tukeutumaan muun muassa sovellusten heikon tietoturvallisuuden takia.

Sovelluskehityksen tietoturvallisuudessa tulee ottaa huomioon kehitettävän sovelluksen tietoturvaominaisuudet, itse sovelluskehitysprosessin tietoturvallisuus sekä tietoturvatietoiset sovelluskehittäjät ja testaajat. Sovelluskehittäjiltä ja kehityskumppaneilta tulee vaatia näyttöä tietoturvaosaamisesta ja tietoturvallisuuden integroinnista sovelluskehitysprosessiin. Tietoturvallisuus tulee ottaa huomioon sovelluksen elinkaaren kaikissa vaiheissa. Kaikki tässä ohjeessa mainitut vaatimukset eivät välttämättä sovi kaikille sovelluksille. Kaikissa sovelluksissa esimerkiksi kirjautuminen ei ole pakollista, mikä vaikuttaa useaan vaatimukseen.

Uusia sovelluksia suunniteltaessa ja käyttöönotettaessa infrastruktuurin tietoturvaratkaisut ja -taso on huomioitava. Uusi sovellus saattaa aiheuttaa uusia, tiukempia vaatimuksia nykyiselle infrastruktuurille.

Haasteita sovelluskehityksen tietoturvallisuudessa

Sovelluskehitys asettaa organisaation toiminnalle sekä hallinnollisia että teknisiä tietoturvahaasteita. Tämän ohjeen tarkoitus on helpottaa sovelluskehityksen ongelmien ratkaisemista esittämällä organisaatiolle käytännöllisiä tehtäviä ja tietoturvavaatimuksia. Seuraavassa listassa on esimerkkejä tietoturvahaasteista, jotka organisaatioiden tulee ratkaista.

- **Sovelluskehityksen prosessissa tietoturvallisuuden huomioon ottaminen kaikissa vaiheissa koetaan usein hidastavana tekijänä. Jälkeenpäin tietoturvallisuuden huomioon ottaminen tulee kuitenkin yleensä kalliimmaksi ja on vaikea toteuttaa.**
- Sovelluskehitykseen ja arkkitehtuuriratkaisuihin osallistuvien henkilöiden tietoturvatietoisuuden kehittäminen.
- Sovelluskehitystä opettavat oppilaitokset eivät useinkaan opeta sitä, miten tietoturvallisuus tulisi ottaa huomioon sovelluskehityksessä. Tällöin varsinkin uusilla ohjelmoijilla saattaa olla puutteita tietoturvallisen ohjelmoinnin osaamisessa.
- Sovellus koostuu useasta eri komponentista, joista vain osa on organisaation itsensä tekemiä. Muiden komponenttien tietoturvallisuuden taso kuitenkin vaikuttaa kokonaisuuden tietoturvallisuuteen.

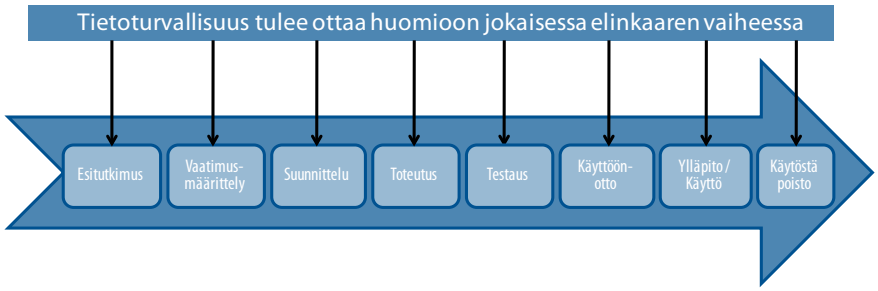
- Tietoturvallisuuteen kiinnitetään yleensä huomiota vasta tietoturva-auditoinnissa sovelluskehityksen loppuvaiheessa.
- Uusien sovellusten toteutuksissa on usein kiire, jolloin sovellusten laatuun ja tietoturvallisuuteen resursointi on heikompaa.
- Tietojärjestelmäympäristöt ovat monimutkaistuneet kaiken aikaa; sovellusten ulkoistaminen, pilvipalvelut, verkottumisen lisääntyminen sekä uusien ohjelmointikielten ja -tekniikoiden käyttöönotto ovat tekijöitä, jotka lisäävät haasteita tietoturvallisuuden toteutukselle.
- Ohjelmoinnissa ja testauksessa ei riittävästi varauduta siihen, että valmista ohjelmaa vastaan pyritään hyökkäämään (defensiivinen ohjelmointi).
- Ohjelmoinnissa ei varauduta riittävän hyvin virhetilanteisiin ja ennalta määrittelemättömiin tilanteisiin sekä niistä turvalliseen palautumiseen.
- Sovellusten riskianalyysit ovat usein puutteellisia tai niitä ei tehdä lainkaan

2.3 Sovelluskehitysmalli

Sovelluskehitysmalli vaihtelee organisaatioittain ja projekteittain. Tässä ohjeessa ei oteta kantaa käytettävään sovelluskehitysmalliin, mutta esitetään erilaisia tapoja, miten ohjeen vaatimukset voidaan sisällyttää organisaation sovelluskehitysprosessiin. Olennaista on, että tietoturvallisuus ja huolellinen suunnittelu tehdään heti projektin alusta lähtien.

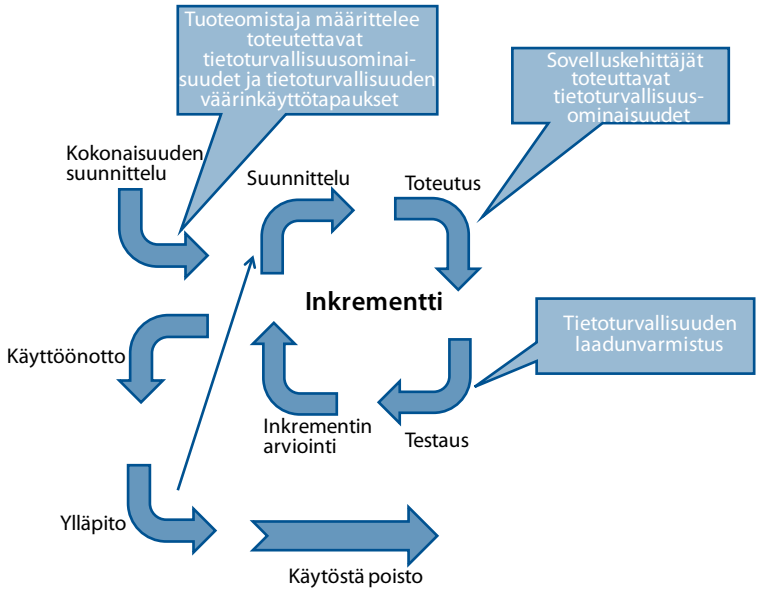
Perinteisen, lineaarisen sovelluskehitysprosessin hyvien käytäntöjen mukaisessa prosessissa (kuva 1) tietoturvallisuus määritellään ja suunnitellaan projektin alkuvaiheissa ja toteutetaan myöhemmissä vaiheissa.

Kuva 1. Tietoturvallisuus sovelluksen elinkaaren eri vaiheissa



Ketterissä menetelmissä sovellusta kehitetään lyhyissä vaiheissa. Jokaiseen vaiheeseen valitaan toteutettavat ominaisuudet, jotka siinä vaiheessa (inkrementissä) toteutetaan. Vaiheita toistetaan, kunnes kaikki halutut ominaisuudet on toteutettu (kuva 2). Sovellus voidaan ottaa käyttöön, vaikka sovellukseen toteutettaisiinkin uusia ominaisuuksia seuraavassa vaiheessa. Tällöin tietoturvallisuus tulee ottaa huomioon sekä projektin alussa sekä jokaisessa toteutusvaiheessa.

Kuva 2. Tietoturvallisuus ketterässä sovelluskehitysmallissa



Tietoturvallisuuden huomioimisesta erityisesti ketterissä menetelmissä voi lukea lisää seuraavista linkeistä:

- Agile Finland: Secure software development and agile methods – notes[1]
- MSDN Magazine: Streamline Security Practices For Agile Development [2]
- Microsoft: Agile Development Using Microsoft Security Development Lifecycle [3]
- Software security in agile product management [4]

Perinteiset lineaariset menetelmät ja ketterät menetelmät saattavat vaikuttaa hyvinkin erilaisilta tavoilta tehdä sovelluskehitystä. Molemmissa menetelmissä tulee kuitenkin ottaa huomioon samat tietoturvatehtävät ja -vaatimukset.

2.4 Sovelluskehityksen tietoturvavastuiden roolit ja työnjako

Sovelluskehitysprojektin tai -hankkeen tietoturvavastuut on määriteltävä projektin käynnistysvaiheessa. Organisaatioista riippuen voidaan käyttää projekti- tai hanketermiä. Vastuiden ja tehtävien selkeällä määrittelyllä varmistetaan tietoturvallisuuden toteutuminen

[1] http://confluence.agilefinland.com/display/af/Secure+software+development+and+agile+methods+-+notes

[2] http://msdn.microsoft.com/en-us/magazine/dd153756.aspx

[3] http://www.microsoft.com/security/sdl/discover/sdlagile.aspx

[4] http://www.fokkusu.fi/agile-security/

projektin kaikissa vaiheissa. Tämä koskee niin koko projektin tietoturvallisuutta kuin sen tuottaman sovelluksenkin tietoturvallisuutta. Projektin avainhenkilöillä on oltava tietoturvallisuuden perustuntemus tehtävään soveltuvilta alueilta.

Erityisen haastavaa on tietoturvallisuuden hallinta monitoimittajaympäristössä. Mikäli projektissa on useita toimijoita, on erityistä huomiota kiinnitettävä tietoturvavastuiden jakoon eri toimijoiden kesken. Usean toimijan ympäristössä korostuu myös tilaajan valvontavastuu.

Seuraavassa on esitelty muutamia suositeltavia rooleja ja rooleille kuuluvia tietoturvavastuita. Tarkka vastuunjako riippuu organisaatiosta ja käytettävästä sovelluskehitysmallista. Olennaista on, että vastuut on jaettu tarkoituksenmukaisesti ja sovelluskehitysmalliin sopivalla tavalla estäen kuitenkin vaarallisten työyhdistelmien syntyminen. Sovelluskehityksen näkökulmasta vaarallisten työyhdistelmien estäminen tarkoittaa käyttäjä-, ohjelmakehitys-, testaus- ja tuotantotehtävien erityttämistä toisistaan. Pienissä organisaatioissa eriyttäminen on vaikeaa ja tällöin pitää miettiä, miten vaarallisista työyhdistelmistä aiheutuvia riskejä voidaan vähentää. Lisäksi ketterissä menetelmissä usein käytetyssä testauslähtöisessä sovelluskehityksessä kehittäjät tekevät merkittävän osan testauksesta. On kuitenkin tärkeää erottaa sovelluskehitystyön tekeminen ja vaatimustenmukaisuuden hyväksyminen.

Erilaisissa organisaatioissa tai projekteissa ei välttämättä ole kaikkia alla mainittuja rooleja ja yhdellä projektiin osallistuvalla henkilöllä voi olla useampia rooleja, mutta silloinkin tulee ottaa huomioon vaarallisiin työyhdistelmiin liittyvät riskit. Erityisesti pienissä organisaatioissa roolijako voi poiketa alla esitetystä.

Kuva 3. Esimerkki sovelluskehityksen roolien tehtävistä hankkeen eri vaiheissa RACI-mallin mukaisesti.

	Johto	Ohjausryhmä	Projektipäällikkö	Projektiryhmä	Omistaja	Tietoturvavastaava	Katselmoija	Tietoturvaryhmä	Auditoija	Pääkäyttäjä	Tietohallintovastaava
Tarvemäärittely	C		R		A	I					C
Esitutkimus		A	R	R		I		C	C		I
Määrittely		A	R	R		C	C	C		I	
Suunnittelu		A	R	R		C	C	C			
Toteutus		A	R	R	I	R	C	C		I	C
Testaus	I	A	R	R		C	C	C	C	C	
Käyttöönotto	I	A	R	R	C	C		C		R	C
Ylläpito/käyttö					A	C		C	C	R	R
Käytöstä poisto	I				A	C		I		R	R

R	Responsible
A	Accountable
C	Consulted
I	Informed

Johto, projektin asettaja

Johdon sitoutuminen tietoturvakulttuurin ja hankkeiden tietoturvallisuuden edistämiseen on ensiarvoisen tärkeää. Johto määrittelee tietoturvallisuuden keskeiset periaatteet esimerkiksi osana toiminta- tai tietohallintostrategiaa sekä päättää merkittävistä hankkeista ja hankinnoista. Sovelluskehitysprojekteissa vastuu yleensä tarkoittaa tehtävien delegoimista ohjausryhmälle.

Projektin asettaja edustaa organisaation johtoa, nimeää projektipäällikön ja toimii useimmiten ohjausryhmässä puheenjohtajana.

Projektin ohjausryhmä

Projektin ohjausryhmässä ovat edustettuina projektin lopputulosta hyödyntävät intressiryhmät. Ohjausryhmä hyväksyy projektisuunnitelmat ja päättää projektin keskeisistä asioista. Ohjausryhmän tulee valvoa, että hankkeen eri osapuolet huomioivat tietoturvallisuuden riittävästi hankkeen eri osatehtävissä.

Tietoturvaryhmä

Tietoturvaryhmän tehtävä on avustaa sovelluskehitysprojekteja tietoturvallisuuden toteuttamisessa. Ryhmää voi hyödyntää esimerkiksi määrittelyssä, suunnittelussa, testauksen suunnittelussa ja tietoturvaloukkausten selvittämisessä. Ryhmässä on oltava riittävä tietoturvaosaaminen ja sovelluskehityksen eri vaiheiden osaaminen, jotta se osaa tukea sovelluskehitystä tarpeen mukaan.

Sovelluksen omistaja

Jokaiselle sovellukselle määritellään omistaja, joka on esimerkiksi sen osaston tai yksikön johtaja, jonka toiminnan tueksi sovellus kehitetään. Omistajan rooliin kuuluu vastata sovelluksen vaatimusmäärittelystä mukaan lukien. tietoturvavaatimukset. Käytännön toteutuksesta voi vastata esimerkiksi tietoturvaryhmä. Omistaja myös hyväksyy kaikki merkittävät järjestelmää koskevat päätökset, kuten käyttöoikeudet ja järjestelmämuutokset sekä vastaa hyväksymistestauksesta ja käyttäjien kouluttamisesta.

Omistaja voi tarvittaessa valtuuttaa toisen henkilön toimimaan puolestaan omistajan roolissa yhden tai useamman vastuunsa osalta. Tällöin varsinainen omistaja on kuitenkin velvollinen valvomaan valtuuttamansa henkilön toimia.

Projektipäällikkö

Projektipäällikkö vastaa vastuulleen ottamansa projektin toteuttamisesta sovelluksen omistajan tavoitteiden mukaan. Projektipäällikkö myös vastaa kehitysprojektin hallinnasta ja sovittujen toimintakäytäntöjen ja standardien noudattamisesta. Tietoturvallisuuden osalta projektipäällikkö vastaa siitä, että rakennettava sovellus noudattaa organisaation tietoturvapolitiikkaa ja -ohjeita. Samalla hän vastaa projektin riskianalyysista sekä

sovelluksen tietoturvasuunnitelmasta. Projektipäällikkö hyväksyttää tietoturvaratkaisut sovelluksen omistajalla ja ohjausryhmällä.

Projektiryhmä

Projektiryhmä toteuttaa projektin käytännön kehitystyön tehtävät sovittuja menetelmiä ja standardeja noudattaen. Tämä tarkoittaa myös tietoturvaratkaisujen toteuttamista politiikan ja ohjeiden mukaisesti. Projektiryhmä raportoi välittömästi projektipäällikölle tietoonsa tulleet tietoturvallisuuteen liittyvät ongelmat tai poikkeamat.

Tietohallintovastaava

Tietohallintovastaava varmistaa, että projektilla on käytettävissään sovelluskehitysympäristö, tarvittavat kehitysvälineet, niiden osaaminen sekä tarvittava tekninen tuki. Tietohallintovastaavan rooliin kuuluu myös varmistaa, että järjestelmä on organisaation tietohallintostrategian ja teknisen arkkitehtuurin sekä tietoarkkitehtuurin mukainen. Tietohallintovastaavan tehtäviä ovat myös laadunvarmistus, projektisalkun hallinta, kehittämistyön koordinointi, menetelmäkonsultointi ja näihin liittyvät tietoturvanäkökohdat.

Tietoturvavastaava

Tietoturvavastaava varmistaa, että kehitettävä sovellus vastaa organisaation tietoturvavaatimuksia ja on hyväksytyn tietoturvapolitiikan sekä arkkitehtuurin mukainen. Tietoturvavastaava tukee tietoturvallisuuden suunnittelua ja toteutusta, tarkastaa tietoturvatehtävien vaihekohtaiset tulokset sekä varmistaa, että organisaatiolla on käytössään riittävä asiantuntemus järjestelmässä käytettävästä tietoturvatekniikasta. Tietoturvavastaava seuraa projektin tietoturvakokonaisuutta ja esittää tarvittavia kehittämistoimia. Tietoturvavastaavan tehtäviin kuuluu myös käytön aikainen tietoturvallisuuden seuranta.

Auditoija

Tietoturvallisuuden auditoija arvioi järjestelmän tietoturvaominaisuuksia ja -kontrolleja sekä tarkastaa, että eri osapuolet ovat täyttäneet roolinsa ja vastuunsa. Normaalisti auditoinnissa verrataan tietoturvaominaisuuksia projektin aikana määriteltyihin tietoturvavaatimuksiin sekä ulkoisiin standardeihin. Tietoturvallisuuden hallintajärjestelmän sertifiointi edellyttää auditointia. Riippumattomuuden varmistamiseksi auditoija on tyypillisesti järjestelmän tilanneen ja toteuttaneen organisaation ulkopuolinen henkilö. Auditoijana voi toimia myös sisäinen tarkastus tai tietoturvaryhmä.

Katselmoija

Katselmointitilaisuudessa katselmoijat vertaavat esitettyjen suunnitelmien tai toteutuksen lopputuloksia määrittelyvaiheessa kuvattuihin tietoturvallisuuden vaatimuksiin.

Sovelluksen pääkäyttäjä ja käyttäjä

Sovelluksen pääkäyttäjän tietoturvatehtäviä ovat huolehtiminen sovelluksen käytettävyydestä ja kehittämisestä, käyttöoikeuksista sekä järjestelmän tietoturvallisuudesta. Pääkäyttäjän vastuulla saattaa olla myös jatkuvuussuunnitteluun liittyviä tehtäviä.

Sovelluksen käyttäjän tietoturvatehtäviä ovat sovelluksen käyttö työtehtävissä annettujen ohjeiden mukaan.

Muita rooleja

Yllä mainittujen roolien lisäksi organisaatiossa on myös muita rooleja, jotka ovat mahdollisesti mukana turvallisen sovelluskehityksen eri vaiheissa. Tällaisia rooleja ovat esimerkiksi

- Sopimuksista ja hankinnoista vastaava
- Tietojen luovuttamisesta vastaava
- Käyttöoikeuksista ja käyttövaltuuksista vastaava
- Käyttötoiminnasta vastaava.

2.5 Projektityön tietoturvallisuus

Hankkeen aikainen projektityö on myös suoritettava tietoturvallisesti. Projektin aikana on huolehdittava muun muassa viestinnän tietoturvallisuudesta, projektidokumentaation turvallisesta käsittelystä ja projektin riskienhallinnasta. Suurissa ja usean toimijan projekteissa projektityön tietoturvallisuuden haasteet korostuvat ja niihin on kiinnitettävä erityistä huomiota. Hankkeen tietoturvallisuudesta on annettu erillinen ohje (VAHTI 9/2008).

VAHTI 9/2008-ohjeessa on annettu valmis esimerkki hankkeen tietoturvaohjeen laatimisesta. Mallipohjan käyttö on suositeltavaa, jotta kaikki olennaiset projektia koskevat tietoturvavaatimukset tulevat huomioitua.

2.6 Tietoturvallisuuden laadun varmistaminen

Tietoturvallisuuden laadun varmistamisen tarkoituksena on saada aikaan luottamus projektin eri osapuolille siitä, että projektille asetetut tietoturvallisuuden vaatimukset ja odotukset täyttyvät.

Jotta toteutettavan sovelluksen tietoturvallisuus saadaan riittävälle tasolle, tulee sovelluksen kriittisyys organisaation ydin- tai liiketoiminnan kannalta arvioida ennen kehitysprosessin aloittamista. Kehitettävän sovelluksen tietoturvavaatimusten analysointiin on käytettävä kahta eri näkökulmaa: sovelluksen käsittelemän tiedon asettamat vaatimukset sekä sovelluksen itsensä kriittisyys organisaation toiminnalle. Sovelluksen käyttötarkoituksesta riippuen esimerkiksi sen saatavuus voi nousta tietosisältöä tärkeämmäksi. Analyysi

on suoritettava ennen varsinaisen kehitysprosessin aloittamista, jotta sovelluksen kehittämisessä käytettävät menetelmät tukevat riittävästi asetettua vaatimustasoa.

Useat valtionhallinnon organisaatiot eivät kehitä sovelluksia itse, vaan toimivat ainoastaan tilaajana. Tilattaessa tässä ohjeessa esitetyt vaatimukset voidaan esittää vaatimuksina toimittajalle.

Valtionhallinnossa tietojen luokittelu on tehtävä valtionhallinnon tietoturvallisuudesta annetun asetuksen mukaisesti. Tarkemmat ohjeet luokittelusta ja sen soveltamisesta on annettu ohjeessa Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010). Järjestelmien luokitukseen löytyy ohjeita Teknisen ICT-ympäristön tietoturvataso -ohjeesta (VAHTI 3/2012). Myös muiden lakien, kuten esimerkiksi henkilötietolain, asettamat vaatimukset on huomioitava sovellusten kehityksessä. Sovelluksen luokittelu perusteluineen on kirjattava sovelluksen tietoturvasuunnitelmaan, tietoturvakuvaukseen tai vastaavaan dokumenttiin.

Edellä mainitun luokittelun perusteella on päätettävä, tarvitaanko projektissa erityistä tietoturva-asiantuntijaa. Joka tapauksessa projektin aikana on tärkeää käyttää tietoturvavastaavan tai -ryhmän asiantuntijatukea merkittävissä tietoturvallisuuteen vaikuttavissa valinnoissa. Lisäksi on päätettävä, millä eri tavoilla sovelluksen tietoturvallisuus katselmoidaan ennen sen tuotantokäyttöä. Katselmoinnit on suunniteltava ja aikataulutettava jo aikaisessa vaiheessa, jotta niiden suorittamiseen voidaan varata riittävästi aikaa ja resursseja. Katselmointien pohjana käytettävät kriteerit on myös sisällytettävä katselmointisuunnitelmaan. Mikäli tietoturva-asiantuntijaa ei nimetä, on vastuu tietoturva-asioista projektipäälliköllä tai tietoturvaryhmällä, jos tällainen on käytettävissä.

Tietoturvallisuuden hallintaan on olemassa lukuisia standardeja. Lakien ja asetusten lisäksi toimintaa voi ohjata esimerkiksi ISO 27000-sarjan standardien pohjalta. Näistä standardeista tärkeimpiä on ISO 27001, joka keskittyy tietoturvallisuuden yleiseen hallintaan organisaatiossa. Lisäksi luonnosvaiheessa on standardi ISO 27034, joka keskittyy sovellusten tietoturvallisuuteen.

2.7 Tietoturvallisuuden dokumentointi osana sovelluskehitystä

Osana sovelluskehitysprosessia tulisi dokumentoida ne toiminnallisuudet ja muut seikat, jotka vaikuttavat sovelluksen tietoturvallisuuteen. Alla on listattu tietoturvallisuuden kannalta tärkeimmät asiat, jotka tulisi dokumentoida joko omana asiakirjanaan tai osana muita asiakirjoja:

- Määrittely sovelluksen tietosisällöstä ja tarkoituksesta
- Tietoturvatason määrittely
- Sovelluksen/järjestelmän tietoturvariskien kartoitus
- Toiminnallinen määrittely
- Tietoturvallisuuden vaatimusmäärittely tietoturva-arkkitehtuurin mukaisesti
- Riippuvuus yhteisistä komponenteista

- Noudatettavat standardit tai muut normit
- Turvakuvaus
- Elinkaaren hallintasuunnitelma
- Mikäli sovelluskehityksessä tehdään valintaa eri tuotteiden välillä, tulee dokumentoida valintakriteerit myös tietoturvanäkökulmasta
- Tietoturvallisuuden testisuunnitelma ja -raportit
- Asennusdokumentaatio
- Käyttöönottosuunnitelma, palvelun asiakkaat
- Ylläpitosuunnitelma ja vastuut
- Jatkuvuus- ja toipumissuunnitelma.

Sovelluskehitysaineiston ja dokumenttien säilytyksessä tulee ottaa huomioon tietoaineiston luokitus ja käsittelysäännöt. Dokumentaatiossa on huomioitava sovelluksen riippuvuudet organisaation kokonaisarkkitehtuurista ja yhteisistä teknisistä komponenteista.

2.8 Yhteistyö toimittajien kanssa

Ulkoistettaessa sovelluskehitys tai sovellusten ylläpito tai ostettaessa valmiita sovelluksia tai niiden osia tulee ottaa huomioon se, miten tietoturvallisuuden toteutumisesta voidaan varmistua. Seuraavissa kappaleissa on käsitelty erilaisia ulkoistamiseen liittyviä erityiskysymyksiä. Hankinnoissa tulee varmistua ainakin siitä, että tässä ohjeessa kuvattuja vaatimuksia on soveltuvin osin käytetty sovelluskehityksessä tai toimittajalla on vähintään yhtä hyvät sisäiset vaatimukset ja prosessit.

Valtionhallinnon ICT-hankintojen tietoturvaohje (VAHTI 3/2011) sisältää tarkat ohjeet tietoturvallisuuden huomioimisesta erilaisissa hankinnoissa, kuten sovelluskehityksen ja ylläpidon hankinnassa.

2.8.1 Monitoimittajuudesta

Useamman toimittajan kanssa toimittaessa sovelluksen toteuttaminen on luonnollisesti monimutkaisempaa. Tyypillisessä tapauksessa käyttöpalvelut ja tietoliikennepalvelut on hankittu eri organisaatiosta kuin sovelluksen kehittäminen. On mahdollista, että eri toimittajat ovat kilpailijoita keskenään. Lisäksi monikansalliset organisaatiot voivat käyttää eri alueiden toteutukseen asiantuntijoita useista eri maista. Tämän ottaminen huomioon jo kilpailutuksessa on erittäin tärkeää.

Sovellustoimitusprojekti tulee pyrkiä organisoimaan siten, että toimitettavasta kokonaisuudesta on vastuussa yksi päävastuullinen toimittaja. Käytännössä kuitenkin saattaa tulla tilanteita, jossa esimerkiksi kilpailuasetelman vuoksi yhtä toimittajaa ei pystytä asettamaan kokonaisvastuulliseksi. Tällöin on varmistuttava tietoturvallisuuden toteutumisesta kaikilla toimittajilla sekä valvottava tietoturvallisuuden tasoa erityisesti vastuualueiden rajoilla.

Monitoimittajuuden ongelma on usein toimittajien erilaisuus; erilaiset työkalut, erilaiset dokumentointistandardit, erilaiset sopimustavat, raportointitavat ja erilaiset työprosessit. Jos tilaajalla on käytössä omat dokumentointi- ja toimintatavat, niin usein on tarkoituksenmukaista edellyttää toimittajia noudattamaan tilaajan määrittelemiä menettelytapoja. Asioiden sopimiseksi yhteistyön toimittajien kanssa pitää alkaa jo sopimusneuvotteluissa.

Sopimusten laatimisessa on otettava huomioon monitoimittajuudesta aiheutuvat erityisvaatimukset kuten

- Vastuut
- Palvelutasosopimukset (service level agreement, SLA)
- Palveluprosessien kuvaukset
- Salassapitositoumukset (non-disclosure agreement, NDA)
- Yhteentoimivuusvaatimukset
- Jaettujen sovellusympäristöjen hallinta (esimerkiksi häiriötikettien käsittely yli organisaatiorajojen).

Noudatettavat tietoturvastandardit, jotka liittyvät sovelluskehityksen eri vaiheisiin tulee listata ja niiden toteuttamista tulee valvoa.

2.8.2 Moniasiakkuudesta

Tietoyhteiskuntakehityksen ja sähköisen asioinnin kehitys johtaa järjestelmiin, joissa on käyttäjiä tai sovelluksen omistajia useista organisaatioista. Kehitettävän sovelluksen omistaja sovitaan aina hankkeen alussa. Omistajavastuu jatkuu koko järjestelmän elinkaaren ajan. Samoin tiedoille määritellään omistaja, joka päättää niiden käytöstä. Eri organisaatioiden erityispiirteiden asettamat vaatimukset on huomioitava myös järjestelmän sisältämien tietojen luokittelussa ja siten myös järjestelmän luokittelussa sekä näistä johdetuissa tietoturvavaatimuksissa.

Kun palveluprosessit ulottuvat yli organisaatiorajojen, järjestelmien muutoshallinta vaikeutuu ja hidastuu. Yhden rajapinnan muuttaminen saattaa koskea usean muun sovelluksen rajapintoja ja sisäisiä rakenteita. Tällaisissa tilanteissa tarvitaan yhteiset päätösmenettelyt esimerkiksi muutoskomiteassa (change advisory board, CAB). Muutoskomitean jäsenet, vastuut ja prosessit on suunniteltava pääpiirteittäin mahdollisimman aikaisessa vaiheessa. Tällä tavalla turvataan palvelujen jatkuvuutta ja käytettävyyttä.

Toimittajat käyttävät samoja järjestelmiä ja alustoja useiden eri asiakkaiden palvelujen ja järjestelmien ajamiseen ja hallitsemiseen. Tästä aiheutuvat riskit, kuten järjestelmien saatavuus, resurssien riittävyys, tietojen vuotaminen organisaation ulkopuolelle ja järjestelmän auditoitavuus pitää ottaa huomioon palveluita hankittaessa.

2.8.3 Pilvipalvelut

Pilvipalvelut jaetaan tyypillisesti kolmeen luokkaan perustuen niiden tuotantomalliin. Eri tuotantomalleja ovat:

- Infrastruktuuri palveluna (Infrastructure as a Service, IaaS)
- Sovellusalusta palveluna (Platform as a service, PaaS)
- Sovellus palveluna (Software as a Service, SaaS)

Esimerkkejä eri tuotantomalleista ovat:

- IaaS: Rackspace Cloud Servers, Amazon EC2
- PaaS: Google App Engine, Microsoft Azureus
- SaaS: Microsoft Office 360, Google Apps for Business

Jokaisella tuotantomallilla on omat erityispiirteensä. Lisätietoja tuotantomalleista ja niiden eroista löytyy esimerkiksi Teknisen ICT-ympäristön tietoturvataso –ohjeen (VAHTI 3/2012) luvusta 4.4.

Sovelluskehityksen näkökulmasta olennaisinta on, käytetäänkö pilvipalvelua sovelluksen kehitys- ja testausympäristönä vai myös lopullisen palvelun tuotantoympäristönä. Ensimmäisessä tapauksessa pilvipalvelut eivät aiheuta merkittäviä lisävaatimuksia varsinaiselle sovellukselle. Jälkimmäisessä tapauksessa on otettava huomioon pilvipalvelun tuotantomalli, jonka mukaan sovellusta ja sen ympäristöä tullaan ylläpitämään.

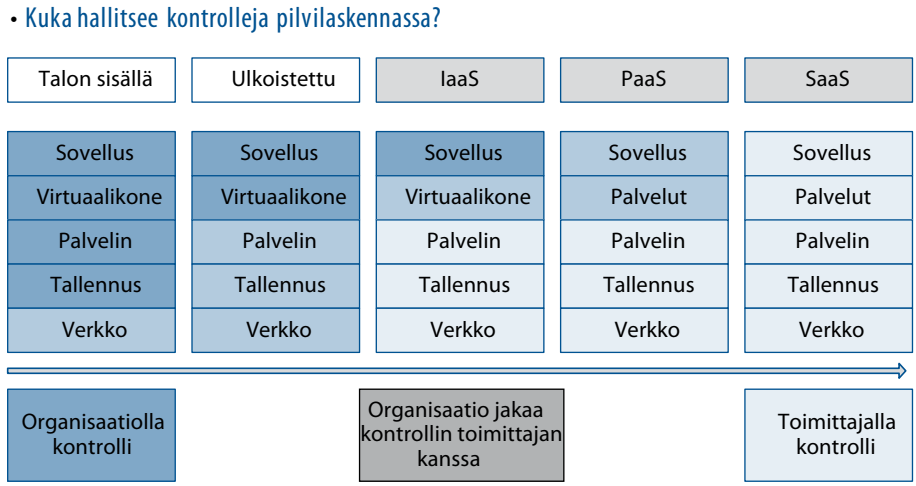
Pilvipalveluita käytettäessä on määriteltävä, mistä tasosta alkaen sovelluksen omistavalla organisaatiolla on kontrolli sovellukseen. Perinteisessä mallissa, jossa sovellus sijaitsee omalla palvelimella, omistajalla on tyypillisesti täysi kontrolli. Ainoastaan verkkoyhteydet toimittaa lähes aina ulkoinen osapuoli. Ulkoistuksessa osa kontrollista menetetään toimittajalle; tyypillisesti palvelin (fyysinen laite) ja tallennus (varmuuskopiot, verkkotallennusratkaisut) ovat pääosin toimittajan hallinnassa. Pilvipalveluissa tilaajalla ei ole enää edes jaettua kontrollia kaikkiin sovelluksen käyttämiin osiin.

Ennen kuin sovelluksen toteuttaminen aloitetaan, tulee arvioida valittuun pilvituotantomalliin liittyvät riskit. Mikäli valittuun tuotantomalliin liittyy sellaisia riskejä, joita ei voida hyväksyä, niin riskejä tulee pyrkiä pienentämään sovellusteknisin ratkaisuin.

Esimerkiksi:

- Jos yhden toimittajan käyttäminen aiheuttaa liian suuren riskin, niin suunnitellun sovelluksen tulee tukea sovelluksen ja sen käyttämän datan helppoa siirrettävyyttä.
- Varmuuskopiointiin suunniteltua palvelua ei voida pitää luotettavana, joten varmuuskopiot salataan
- Varmuuskopiointiin suunniteltua palvelua ei voida pitää luotettavana, joten varmuuskopiot tallennetaan eri palveluntarjoajalle kuin missä varsinaista sovellusta ylläpidetään.

Kuva 4. Kontrollien jakautuminen - alkuperäinen kuva: Governance in the Public Cloud, Dan Blum, "Cloud Computing Security in the Enterprise", Burton Group, Inc., elokuu 2009



Alkuperäinen kuva: Governance in the Public Cloud, Dan Blum, "Cloud Computing Security in the Enterprise", Burton Group, Inc., elokuu 2009

Yhteenvetona voidaan todeta, että pilvipalveluissa tuotettuihin sovelluksiin pätevät samat tietoturvavaatimukset kuin omaan ympäristöön tuotettuihin tai ulkoistuskumppanin ylläpidossa oleviin sovelluksiin. Normaalien vaatimusten lisäksi pilvipalveluun sijoitettavan sovelluksen suunnittelussa tulee muistaa seuraavat erityispiirteet:

- Missä data sijaitsee? Erityisesti tulee varmistaa siirretäänkö henkilötietoja EU-alueen ulkopuolelle.
- Voiko pilvipalvelussa käytettävän sovelluksen tai tallennetun datan maantieteellinen sijainti vaihtua?
- Miten järjestelmään tallennetun datan saa siirrettyä pilvipalvelusta oman organisaation haltuun esimerkiksi toimittajan vaihtotilanteessa?
- Saako pilvipalvelun tietoturvallisuudesta, kuten arkkitehtuurista ja käytetyistä sovelluskehitysmenetelmistä, riittävästi tietoa?
- Voidaanko pilvipalvelun tuottajaa auditoida tai voidaanko sovelluksen tekninen tietoturvallisuus testata?
- Kuka on vastuussa tietojen varmuuskopioinnista?
- Miten varmuuskopioidun datan suojauksesta varmistutaan?
- Miten salausavainten hallinta on toteutettu?
- Miten organisaation omia tietoturvallisuuteen liittyviä palveluita, kuten käyttäjätunnistusta voidaan käyttää palvelussa?
- Tarvitseeko sovelluksen kehityksessä huomioida myös muut jaetun alustan, sovelluksen tai palvelun käyttäjät? Tarvitseeko huomioida palveluntarjoajan ylläpitäjien vahvojen oikeuksien tuoma riski?

Hallinnollisesta näkökulmasta pilvipalveluiden sopimukset voivat erota merkittävästi tavanomaisen ulkoistetun palvelun sopimuksista. Tämä saattaa aiheuttaa haasteita, jotka on muistettava ottaa huomioon sovelluskehitysvaiheessa.

Suositeltavia lisämateriaalin lähteitä:

- Cloud Security Alliance [5]
- Enisa - Cloud Computing Risk Assessment [6]

2.8.4 Sopimukset

Julkishallinnon tietotekniikkahankinnoissa käytetään sopimisen perustana valtion yleisiä tietotekniikkahankintojen sopimusehtoja. Julkisen hallinnon IT-hankintojen yleiset sopimusehdot (JIT 2007) sisältävät useimmat tilanteet kattavat sopimusehdot, erityisehdot, soveltamisohjeet sekä mallisopimukset.[7] Lisäksi sopimuksissa tulee ottaa huomioon hankintakohteen mukaiset erityisehdot.

Sopimuksesta on hyvä laatia luonnosversio jo tarjouspyyntövaiheessa, jotta tarjoajalla on käsitys siitä millaiset sopimusehdot toimitukseen liittyvät. Sopimuksessa tulee ottaa huomioon hankittavan sovelluksen tärkeysluokan ja tietoturvatason vaatimukset, ja asiakkaan on hyvä määritellä tarjouspyyntövaiheessa myös sopimuksessa vaaditut poikkeamat. Tarjoajilta on pyydettävä myös kannanotto sopimusluonnokseen.

Sopimusluonnokseen on sisällytettävä kaikki olennaisesti projektin työmäärään ja kustannuksiin vaikuttavat tietoturvavaatimukset. Erityisen tärkeä on tilaajan auditointioikeuden määrittely ja auditoinneista aiheutuvien kustannusten jakautuminen osapuolten kesken.

Sovellusten tekijänoikeuksista on myös sovittava sopimuksessa. Tarkempi kuvaus tekijänoikeuksiin liittyvistä haasteista on kappaleessa 4.1.

Turvallisuussopimus suositellaan laadittavaksi puitesopimuksen tasoiseksi sopimukseksi. Mikäli hankinta ei kuulu puitesopimuksen piiriin, voidaan turvallisuussopimus laatia hankintasopimuksen tasoiseksi. Turvallisuussopimuksessa määritellään sovelluksen ja toimitusprojektin turvallisuusjärjestelyt, kuten esimerkiksi projektityön turvallisuus, henkilöstöä ja mahdollisia alihankkijoita koskevat vaatimukset ja sopimusosapuolten velvoitteet ja oikeudet. Malli turvallisuussopimukseen löytyy Valtion ICT-hankintojen tietoturvaohjeen (VAHTI 3/2011) liitteestä 2.

Mikäli hankinnassa on erityisiä piirteitä, jotka vaativat tarkempaa turvallisuusasioista sopimista, on sopimuksen laatimiseen otettava avuksi sopimusjuristi.

---

[5] http://cloudsecurityalliance.org

[6] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/

[7] http://www.jhs-suositukset.fi/suomi/jhs166

2.8.5 Turvallisuusluokiteltu materiaali

Järjestelmät,

- joissa käsitellään turvallisuusluokiteltua aineistoa tai
- jotka liittyvät kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseen tai
- joita käytetään kansainvälisiin tarjouskilpailuihin, ja joissa järjestelmiltä edellytetään kansallisen tietoturvaviranomaisen hyväksyntä

tulee hyväksyttää kansallisella tietoturvaviranomaisella (NCSA-FI) tai sen hyväksymällä arviointilaitoksella. Hyväksyntäprosessiin liittyvä tarkastustoiminta on maksullista ja hyväksyntä on voimassa erikseen määritettävän ajan. Auditoinnissa hyödynnetään kansallista turvallisuusauditointikriteeristöä (KATAKRI). Tietoturvallisuuden arviointi perustuu lakiin tietoturvallisuuden arviointilaitoksista (1405/2011).

3 Tietoturvallisen sovelluskehityksen osa-alueet

Tietoturvallisen sovelluskehityksen vaatimukset jakautuvat sekä organisaation toimintaa koskeviin hallinnollisiin vaatimuksiin että sovelluskehitysprosessia koskeviin vaatimuksiin. Sovelluskehitysprosessin aikaisten vaatimusten tavoitteena on parantaa kehitettävän sovelluksen tietoturvallisuutta. Organisaation toimintaa koskevien vaatimusten tavoitteena on taas kehittää toistettavuutta yksittäisten projektien välillä hyvien käytäntöjen mukaisesti.

Tietoturvallisuuden rakentaminen sovelluskehitysprosessiin alkaa tietoturvastrategian määrittelystä. Vaikka strategian laatiminen ei ole tietoturvallisuuden perustasolla pakollista, vaatii hyvän tason saavuttaminen suunnitelmallisuutta. Politiikat ja strategiat ohjaavat sovelluskehitystä koko organisaation tasolla.

Riskienhallinnalla on liittymä kaikkiin sovelluskehityksen vaiheisiin. Sen avulla on johdettavissa eri vaiheissa tarvittavat tietoturvaratkaisut ja -päätökset.

Koulutuksella on suuri merkitys sovelluskehittäjien osaamisen varmistamisessa. Koulutusta on järjestettävä säännöllisesti ja kehittäjille on tarjottava tukea tietoturvalliseen kehitystyöhön.

Sovelluskehitysympäristön on luotava mahdollisuus turvalliseen sovelluskehitykseen. Erityisen tärkeässä asemassa on kehitys-, testi- ja tuotantoympäristöjen eriyttäminen ja sovelluskehitystä tukevien järjestelmien käyttö. Ympäristöissä on huolehdittava myös tietoturvallisuuden perusasioista. Jatkuvuudenhallinnan avulla turvataan myös sovelluskehityksen jatkuvuus erityisoloissa.

Esitetyt vaatimukset on jaettu eri tietoturvatasoille (perus, korotettu ja korkea) muiden VAHTI-ohjeiden mukaisesti. Jokaisen aliluvun lähdemateriaalin vaatimukset on koottu erilliseksi liitteeksi. Lähdemateriaalina on käytetty julkisia ohjeita, joiden sisällöstä tunnistettiin sovelluskehityksen tietoturvallisuuteen liittyviä vaatimuksia.

Näitä ohjeita olivat:

- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010)
- Sisäverkko-ohje (VAHTI 3/2010)
- ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin (VAHTI 2/2009)
- Valtiohallinnon keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004)

- Kansallinen turvallisuusauditointikriteeristö, versio 2 (KATAKRI II)
- Juhlkishallinnon suositukset – ICT-palvelujen kehittäminen: Kehittämiskohteiden tunnistaminen (JHS 171)
- ICT-hankintojen tietoturvaohje (VAHTI 3/2011)
- Lokiohje (VAHTI 3/2009).

3.1 Ympäristön vaatimukset

Sovelluskehityksen tietoturvallisuuden kannalta on tärkeää, että organisaation tavoitteita, toimintaa ja prosesseja kehitetään sisältämään myös tietoturva-asioita. Luvussa 3.3 esitetään menetelmiä, joilla tietoturvallisuus saadaan sisällytettyä organisaation toimintatapoihin, jolloin menetelmät ovat toistettavissa kun siirrytään sovelluskehitysprosessista toiseen.

Oorganisaation toimintaa koskevien vaatimusten osa-alueet ovat:
- Strategia ja resursointi
- Politiikat
- Riskienhallinta
- Osaaminen ja koulutus
- Tekninen sovelluskehitysympäristö
- Jatkuvuuden hallinta.

3.1.1 Strategia ja resursointi

Tietoturvallisuuden toteuttamiseen on varattava riittävästi resursseja. Tämä varmistetaan roolien tunnistamisella ja varaamalla riittävästi aikaa myös tietoturvatehtäviin. Tietoturvastrategiassa suunnitellaan organisaation tietoturvatyötä pidemmällä tähtäimellä.

PERUSTASO

Vastuuhenkilöt ja -roolit (STR-001): Organisaation tulee kartoittaa ja tunnistaa sovelluskehityksen tietoturvallisuuden kannalta merkittävät roolit ja niistä vastuussa olevat henkilöt. Henkilöiden työajasta on varattava riittävästi aikaa myös tietoturvatehtäviin. Tällaisia rooleja ovat esimerkiksi:
- Arkkitehdit ja projektipäälliköt
- Sovelluskehitykseen käytetyn kehitysympäristön omistajat ja ylläpitäjät. Kehitysympäristöön kuuluvat muun muassa versionhallinta, testiympäristöt, jaetut työtilat jne.

- Kehitettävän sovelluksen omistaja
- Testauspäällikkö.

Eri rooleissa toimivien henkilöiden tulee tiedostaa myös oman alueensa tietoturvavastuut ja heidän tulee seurata vastuualueidensa tietoturvaongelmia ja niiden mahdollista toteutumista.

Tunnistetuille henkilöille tulee määritellä varahenkilöt. Lisäksi varahenkilöt tulee kouluttaa tehtäviinsä, jotta he pystyvät tarvittaessa toimimaan varahenkilöinä tehokkaasti.

KOROTETTU TASO

Tietoturvastrategia (STR-002): Organisaation tulee suunnitella strategia, jossa määritellään tietoturvatyön vastuualueet sekä organisaation tietoturvallisuudesta vastuullisten roolit. Tietoturvastrategian tulee olla organisaation ydintoiminnan ja -tavoitteiden mukainen sekä tukea asetettujen tavoitteiden saavuttamista. Strategia ei saa muodostua ydintoiminnasta irralliseksi.

Strategian suunnittelussa on otettava huomioon ainakin seuraavat asiat:

- Tietoturvastrategian tulee olla linjassa ja tukea organisaation liiketoimintasuunnitelman, ydintoimintojen, kasvusuunnitelmien jne. kanssa
- Suunnittelussa tulee olla mukana edustajia kaikista organisaation sidosryhmistä, kuten eri liiketoiminta-alueiden vastaavat, IT-toiminnasta vastaavat, henkilöstöasiat (HR), lakiyksikkö jne. (riippuen toimintaympäristöstä)
- Suunnittelussa otetaan huomioon liiketoimintariskit, jotta tietoturvatyö voidaan kohdistaa liiketoiminnan kannalta tärkeimpiin kohteisiin
- Tulee ottaa huomioon organisaation toimintaan vaikuttavat lait ja asetukset sekä muut sitoumukset.

Dokumentissa käsitellään seuraavia asioita:

- Pitkän ja keskipitkän tähtäimen tietoturvastrategia, tavoitteet ja mittarit tavoitteiden saavuttamiselle
- Strategian hyödyt liiketoiminnalle
- Implementointisuunnitelma, aikataulut, vastuuhenkilöt, tarkastuspisteet (milestone) jne.
- Organisaation ylimmän johdon sitoutumiskirje (commitment letter).

3.1.2 Politiikat

Politiikat ovat ohjeita, joilla ohjataan koko organisaation toimintaa. Tietoturvallisuuden kannalta erityinen merkitys on tietoturvapolitiikalla. Toimintaympäristöstä ja toteutettavasta sovelluksesta riippuen organisaatio saattaa tarvita muitakin tietoturvallisuuteen liittyviä politiikkoja, kuten pääsynhallinta- tai lokipolitiikka.

PERUSTASO

Tietoturvapolitiikka (POL-001): Organisaatiolla tulee olla kirjallinen tietoturvapolitiikka, jossa määritellään tietoturvatyön keskeiset tavoitteet, vastuut ja periaatteet. Politiikan tulee olla organisaation johdon hyväksymä. Politiikkaa voidaan käyttää pohjana tietoturvastrategian määrittelylle. Politiikan päivittäminen ja katselmointi on organisoitu ja vastuutettu.

Turvallisuusselvitykset (POL-002): Organisaatio on kartoittanut ja määritellyt ne roolit, joiden haltijoista tulee tehdä turvallisuusselvitys. Turvallisuusselvitysprosessi on dokumentoitu ja sitä noudatetaan selvityksiä tehtäessä. Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.

Tietojärjestelmien omistajat (POL-003): Kaikille organisaation tietojärjestelmille on määritelty omistaja, joka vastaa kyseisen järjestelmän käytöstä. Tietojärjestelmiin saa asentaa vain järjestelmän omistajan hyväksymiä laitteita tai ohjelmistoja.

KOROTETTU TASO

Tietoturvapolitiikan päivitys (POL-004): Organisaation tietoturvapolitiikkaa ja muita tietoturvallisuuteen liittyviä politiikkoja (kuten lokipolitiikka) katselmoidaan ja tarvittaessa päivitetään vähintään vuosittain. Politiikan katselmoinnille ja päivittämiselle on myös olemassa prosessi ja vastuuhenkilöt.

Lokipolitiikka (POL-005): Organisaatio on määritellyt kirjallisen lokipolitiikan. Politiikka määrittelee vaatimukset kehitettävien sovellusten lokien keräys- ja seurantakäytännöille sekä sille mitkä olosuhteet aiheuttavat hälytyksiä. Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.

Käyttövaltuuspolitiikka (POL-006): Organisaatiolla on kirjallinen käyttövaltuuspolitiikka, joka määrittelee muun muassa seuraavat asiat:

- Kenellä on oikeus myöntää oikeuksia järjestelmiin
- Oikeuksien myöntöperusteet
- Oikeuksien myöntövaatimukset
- Oikeuksien poistoperusteet
- Salasanakäytännöt jne.

Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.

3.1.3 Riskienhallinta

Riskienhallinnalla ja projektiosaamisella on keskeinen merkitys sovelluskehityksessä, käytettiinpä sovellusten kehittämiseen mitä mallia tahansa. Sovelluskehityksen eri vaiheissa on hyvä tarkastella kehitettävän sovelluksen tietoturvauhkia ja riskien ehkäisykeinoja. Riskienhallinnan tarkastelun näkökulmia on kuvattu tarkemmin myöhemmin esitetyissä sovelluskehitysmallin vaiheiden kuvauksissa.

Esimerkkejä riskienhallinnan näkökulmista sovelluskehityksen eri vaiheissa:

- Esitutkimus – liiketoimintariskien analysointi (Business Impact Analysis, BIA)
- Vaatimusmäärittely – sovelluksen riskianalyysi (Worst Case Scenarios) ja
- uhkamallinnus
- Käyttöönotto – organisaation riskikartan päivitys.

PERUSTASO

Organisaation kokonaisriskianalyysi (RSK-001): Organisaation tulee tehdä säännöllisesti riskien analysointia ja hallintaa, ja sen yhteydessä tulee käsitellä myös tietoturvallisuuteen liittyviä riskejä. Riskienhallintaprosessiin tulee kuulua myös tunnistettujen riskien hallintakeinojen määrittely sekä tehtyjen toimenpiteiden onnistumisen seuraaminen.

Riskien tunnistamiseen osallistuvat liiketoiminta-alueiden omistajat sekä muut sidosryhmät. Riskien tunnistamisen tarkoituksena on kerätä lista pahimmista mahdollisista uhkakuvista organisaation liiketoiminta-alueiden toiminnalle ja tietovarannoille. Riskit vaihtelevat toimialueittain, mutta tyypillisiä sovelluksiin liittyviä riskejä ovat:

- Tietovuodot
- Immateriaalioikeuksien rikkomukset (ns. Intellectual Property Rights -rikkomukset)
- Palvelukatkokset
- Varmuuskopioiden riittämätön testaus
- Ulkoistettujen palveluiden epäselvät vastuut
- Taloudelliset tappiot
- Identiteettivarkaudet.

Riskienhallintaprosessin tuotoksesta tunnistetaan ydintoiminnalle merkittävimmät riskit. Riskit priorisoidaan esimerkiksi arvioimalla riskin toteutumisen vaikutus, todennäköisyys ja riskin hallinnan taso. Merkittävimmistä riskeistä kirjoitetaan tarkemmat kuvaukset sekä kaikki mahdolliset riskin lievennys- tai ehkäisykeinot.

Riskit arvioidaan uudelleen säännöllisesti tai organisaation riskiprofiilin muuttuessa merkittävästi. Arvioinnin yhteydessä tarkastetaan myös riskienhallintatoimenpiteiden onnistuminen.

KOROTETTU TASO

Riskienhallintaprosessi (RSK-002): Organisaation riskienhallintaprosessi tulee olla kuvattuna kirjallisesti esimerkiksi organisaation riskienhallintapolitiikassa. Prosessin pitää sisältää vähintään seuraavat asiat:

- Riskien tunnistaminen ja arviointi
- Riskien torjunnan suunnittelu ja tarvittavat toimenpiteet
- Toiminnan suunnittelu riskin realisoituessa
- Riskienhallintakeinojen kuvaus: välttäminen, pienentäminen, siirtäminen, hyväksyminen, varautuminen.

Dokumentaatiota tulee myös ylläpitää ja päivittää säännöllisesti sekä organisaation riskiprofiilin muutosten yhteydessä. Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.

KORKEA TASO

Riskienhallintaprosessin päivittäminen (RSK-003): Organisaation riskienhallintaprosessin tulee ottaa huomioon suuret muutokset organisaation toiminnassa, toimintaympäristössä jne. Tällöin tietoturvariskien arviointi tulee suorittaa uudelleen.

3.1.4 Osaaminen ja koulutus

Sovelluskehittäjien osaaminen on perusvaatimus turvalliselle sovelluskehitykselle. Osaamista voidaan tukea monin tavoin. Kaikkien kehittäjien pitää saada tarvittava tietoturvakoulutus ja kehitystyöhön on oltava oma tietoturvaohjeistus. Lisäksi organisaatiossa on oltava erityisesti tietoturvallisuuteen perehtyneitä henkilöitä, jotka voivat tarvittaessa neuvoa kehittäjiä.

PERUSTASO

Tietoturvakoulutus (OSK-001): Sovelluskehityksestä vastuussa oleville tulee järjestää tietoturvakoulutusta, ns. tietoisuuskoulutusta (awareness training). Koulutuksessa käydään läpi organisaation toteuttamien sovellusten tyypillisiä tietoturvaongelmia. Näin varmistutaan siitä, että kaikki organisaation henkilöt omaavat riittävät taidot rooliinsa kuuluvan tietoturvatyön hoitamiseksi. Tietoturvakoulutus tulee uusia säännöllisesti, vähintään kerran vuodessa. Koulutuksessa on suositeltavaa esitellä toteutettavien sovellusten tyypillisiä tietoturvaongelmia ja sovelluskehityksen menetelmiä niiden estämiseksi. Koulutus voidaan järjestää esimerkiksi 1-2 päivän koulutussessioina tai verkkokoulutuksena. Koulutuksen kattavuus riippuu esimerkiksi siitä, miten paljon tekninen ympäristö on muuttunut edellisen koulutuksen jälkeen sekä miten paljon uusia sovelluskehityksestä vastaavia henkilöitä organisaatioon on tullut. Erityisen tarpeellinen koulutus on uusille sovelluskehittäjille.

Tyypillisiä sovelluskehityksestä vastuussa olevia rooleja ovat:

- Sovelluksen toteutuksesta vastuussa olevat
- Projektipäälliköt
- Sovellusarkkitehdit
- Sovelluksen määrittelijät, suunnittelijat ja toteuttajat
- Sovelluksen testaamisesta vastuussa olevat.

Tietoturvaohjeistus (OSK-002): Organisaation tulee toteuttaa ja ylläpitää listaa dokumenteista, web-osoitteista jne. jotka tarjoavat tietoturvaohjeistusta organisaation käyttämille teknologioille. Resurssit voivat olla sisäistä ohjeistusta tai esimerkiksi OWASP tai MS-ohjeistuksia. Uusien, sovelluskehityksestä vastuussa olevien työntekijöiden tulee tutustua kyseiseen ohjeistukseen perehdytyksen aikana. Listaa ylläpidetään ja päivitetään käytettyjen teknologioiden muuttuessa ja päivittyessä. Lista on organisaatiokohtainen, joten muiden organisaatioiden määrittelemät listat eivät sovellu tähän tarkoitukseen.

Tietoturvaperehdytys (OSK-003): Osana organisaation perehdyttämisprosessia uusille työntekijöille järjestetään tietoturvakoulutus, jossa työntekijälle esitetään organisaation tietoturvasäännöt ja hänet perehdytetään organisaation tietoturvatoimintaan ja -tavoitteisiin. Perehdytyksen tueksi on laadittu kirjallinen ohje, joka sisältää tarkistuslistan läpikäytävistä asioista. Näin varmistutaan siitä, että tärkeiksi koetut tietoturva-asiat saadaan koulutettua uusille henkilöille heti työsuhteen alkaessa. Koulutuksessa tulee muun muassa kertoa taho (kuten tietoturvaryhmä), jolta saa tarvittaessa apua tietoturvaongelmien ratkaisemisessa. Perehdytys voidaan järjestää luokkaopetuksena, verkkokoulutuksena tai muulla soveltuvalla tavalla.

Tietoturvasääntöjen noudattaminen (OSK-004): Organisaation tietoturvasääntöjen noudattamista seurataan ja poikkeamiin puututaan. Sisäisellä tiedottamisella varmistutaan siitä, että työntekijät ymmärtävät sääntöjen rikkomisen seuraukset.

Security Coach (OSK-005): Organisaatiolla tulee olla ainakin yksi sovelluskehityksen tietoturvallisuuteen perehtynyt henkilö (ns. security coach), joka tarjoaa tarvittaessa teknistä tietoturvakonsultaatiota projektitiimeille ja on tarvittaessa vastuussa tietoturvakoulutuksesta. Henkilö voi olla joko organisaation työntekijä tai ulkoinen resurssi, kyseessä ei välttämättä ole kokopäiväinen rooli. Valmentajan olemassaolo tulee tiedottaa organisaation sisällä. Valmentajan osaamisesta varmistutaan riittävällä koulutuksella. Sovelluskehityksen tietoturvavastuut on mainittu henkilön toimenkuvassa ja hänelle annetaan aikaa vastuiden suorittamiseen. Valmentajan roolissa olevien henkilöiden tulee olla aktiivisesti yhteydessä arkkitehtuurin kehittämisestä vastaaviin henkilöihin sekä käytännön sovelluskehitystä tekeviin henkilöihin.

KOROTETTU TASO

Sovelluskehityksen tietoturvakoulutus (OSK-006): Sovelluskehityksestä vastuussa oleville järjestetään räätälöityä koulutusta. Järjestettävän koulutuksen tulee olla roolikohtaista ja ottaa huomioon roolin asettamat tietoturvahaasteet.

Esimerkkisisältöjä:

- Testaajat: tietoturvahaavoittuvuuksien testausmenetelmät, työkalujen esittely
- Toteuttajat: käytettyjen teknologioiden tyypilliset tietoturvaongelmat, turvallinen Java/.NET-ohjelmointi.
- Sovelluksen omistaja: käytetty sovelluskehitysprosessi ja tietoturvallisuuden huomioiminen sen eri vaiheissa.

Koulutuksen ajantasaisuus (OSK-007): Organisaation tietoturvallisuuden koulutussuunnitelma tulee kuvata kirjallisesti. Organisaatio järjestää myös säännöllisiä koulutuksia ajankohtaisista tai tärkeistä tietoturva-asioista. Henkilöstön osallistumista koulutuksiin seurataan. Henkilöstön osaamistaso mitataan koulutuksen päätteeksi. Mittaamisen tarkoituksena ei ole seurata yksilöiden osaamistasoa, vaan kerätä informaatiota organisaation tietoturvaosaamisesta kokonaisuutena. Koulutussuunnitelman päivittäminen ja katselmointi on organisoitu ja vastuutettu.

KORKEA TASO

Toimintaympäristön muutosten vaikutus koulutukseen (OSK-008): Koulutuksen tulee ottaa huomioon myös organisaation toimintaympäristössä tapahtuneet äkilliset muutokset. Organisaatiolla tulee olla valmius järjestää nopealla aikataululla koulutus- tai tiedotustilaisuuksia, mikäli organisaation toimintaympäristössä tapahtuu muutoksia, jotka vaikuttavat merkittävästi organisaation tietoturvallisuuden tilaan. Esimerkkinä tällaisesta tilanteesta on organisaatioon kohdistuva massiivinen tietojenkalasteluhyökkäys.

3.1.5 Tekninen sovelluskehitysympäristö

Sovelluskehitysympäristön tietoturvallisuus vaikuttaa olennaisella tavalla myös kehitettävän sovelluksen tietoturvallisuuteen. Tässä esitettyjen vaatimusten lisäksi on huolehdittava myös ympäristön perustietoturvallisuudesta, kuten päivitysten asentamisesta, pääsynhallinnasta ja virusten torjunnasta.

PERUSTASO

Arkkitehtuuri- ja sovelluskehitysohjeistus (TSK-001): Organisaatiolla tulee olla arkkitehtuuri- ja sovelluskehitysohjeistus, jossa määritellään sovelluskehitystä ohjaavat periaatteet. Tyypillisiä periaatteita ovat:

- Turvalliset oletusarvot (secure default)
- Monikerroksinen suojaaminen (defense in depth)
- Heikoimman alueen suojaaminen (securing the weakest link)
- Virhetilanteiden käsittely tietoturvallisesti (secure failure)
- Matalimmat mahdolliset oikeudet (least privilege)
- Tehtävien eriyttäminen (separation of duties)
- Tietoturvamekanismien salassa pysymiseen ei saa luottaa (security by obscurity).

Teknisten tietoturvaratkaisujen määritys (TSK-002): Organisaation tulee määritellä yhteisesti hyväksytyt tekniset tietoturvaratkaisut. Tietoturvaratkaisut liittyvät muun muassa seuraaviin osa-alueisiin:

- Todentaminen (authentication)
- Valtuuttaminen (authorization)
- Käyttäjän syötteen validointi (input validation)
- Sovelluksen tuotteen turvallinen enkoodaus (output encoding)
- Virheenkäsittely
- Lokien keräys.

Komponenttikirjaston käyttö (TSK-003): Käytetyistä komponenteista tulee muodostaa organisaation paikallinen komponenttikirjasto. Vain komponenttikirjastossa olevia komponentteja tulee käyttää sovelluksissa. Komponenttikirjaston päivitystarvetta tulee seurata aktiivisesti ja eri sovelluksissa käytetyistä versioista tulee pitää kirjaa.

Eriytetyt ympäristöt (TSK-004): Kehitys-, testi-, ja tuotantoympäristöt tulee eriyttää toisistaan. Organisaation tulee määritellä menettely, jota seurataan siirrettäessä sovellusta ympäristöstä toiseen.

Versionhallinta (TSK-005): Organisaation tulee käyttää lähdekoodin säilytykseen soveltuvaa versionhallintajärjestelmää. Järjestelmää tulee käyttää henkilökohtaisin tunnuksin siten, että jokainen muutos lähdekoodiin voidaan jäljittää muutoksen tehneeseen henkilöön ja muutosaikaan.

Kehitysympäristön varmuuskopiointi (TSK-006): Sovelluskehitysympäristön palvelinten ja muiden kehitykseen käytettyjen palveluiden tulee olla säännöllisen varmuuskopioinnin piirissä. Näitä palveluita ovat esimerkiksi versionhallinta, sovelluskehitykseen käytetty wiki, vikatietokanta jne.

Yhteydet kehitysympäristöön (TSK-007): Toimittajien yhteydet kehitys-, testi- ja tuotantoympäristöihin tulee olla salattu vahvalla salauksella, mikäli yhteydet kulkevat julkisen verkon yli. Lisäksi kaikkien käytettyjen tunnuksien on oltava henkilökohtaisia.

KOROTETTU TASO

Tehtävien eriyttäminen (TSK-008): Korotetun tason järjestelmissä eri ympäristöjen ylläpito ja ympäristöjen väliset siirrot tulee organisoida siten, että tehtävien eriyttämien on huomioitu (separation of duties).

KORKEA TASO

Komponenttien luokittelu (TSK-009): Kaikki palvelut, sovellukset ja käytetyt komponentit on luokiteltava sen mukaan, minkä suojaustason tietoa ne käsittelevät. Järjestelmän omistaja on vastuussa järjestelmän käsittelemän tiedon luokituksen määrittämisestä. Komponenteilla tarkoitetaan suoraan sovellukseen kuuluvia ohjelmistokirjastoja, krypto-

moduuleja, tietokantoja ja vastaavia. Välillisiä komponentteja, kuten käyttöjärjestelmää tai ohjelmointikielen kirjastoja ei tarvitse luokitella.

Tietoturvallisuusasetus määrittelee seuraavat suojaustasot:

- Suojaustaso I (ST I), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille.
- Suojaustaso II (ST II), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille.
- Suojaustaso III (ST III), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleisille tai yksityisille eduille ja oikeuksille.
- Suojaustaso IV (ST IV), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yleisille tai yksityisille eduille tai, jos kysymys on tietoturvallisuusasetuksen 9 §:n 2 momentissa tarkoitetuista asiakirjoista, jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä.

3.1.6 Jatkuvuuden hallinta

Sovellusten jatkuvuudelle voidaan asettaa eriasteisia tavoitteita riippuen siitä, kuinka kriittinen sovellus on liiketoiminnan kannalta, kuinka pitkiä katkoja sallitaan ja millaisia tietoturvavaatimuksia (eheys, käytettävyys ja luottamuksellisuus) sovelluksen käsittelemille tiedoille on. Edellä mainituista seikoista tulee sovelluskehitykseen vaatimuksia, jotka on hyvä ottaa huomioon jo sovelluksen suunnitteluvaiheessa sekä sovelluksen riskienhallinnassa ja jatkuvuussuunnittelussa. Sovelluskehitysympäristö ei kuitenkaan usein ole valtionhallinnossa kriittinen liike- tai ydintoiminnalle.

PERUSTASO

Toipumisstrategia (JTH-001): Organisaatiolla on kirjallinen toipumisstrategia ja -suunnitelma, jotka määrittelevät toipumismenettelyt tärkeimmille järjestelmille. Dokumentit sisältävät myös tärkeysluokittelun organisaation ICT-järjestelmille. Suunnitelmat ovat johdon hyväksymiä, niiden päivitys ja katselmointi on organisoitu ja vastuutettu.

Jatkuvuuden avainhenkilöt (JTH-002): Jatkuvuuden kannalta avainasemassa olevat henkilöt ja roolit on kartoitettu ja tunnistettu ja varahenkilöt ko. rooleille on määritelty. Varahenkilöt myös koulutetaan tehtäviinsä. Näin varmistutaan siitä, että toimintojen jatkuvuus ei vaarannu, mikäli avainhenkilö ei ole saatavilla tarvittaessa.

KOROTETTU TASO

Toipumissuunnitelmat (JTH-003): Organisaation tärkeimmille järjestelmille on laadittu toipumissuunnitelmat. Suunnitelmien katselmointi ja päivittäminen on organisoitu ja vastuutettu. Järjestelmän omistaja on ollut mukana suunnitelman laatimisessa. Toipumissuunnitelma sisältää:

- ohjeet katastrofista toipumiseen
- ohjeet toiminnan jatkamisesta ja paluusta normaaliin toimintaan,
- listan varajärjestelmistä
- vaatimukset toissijaisille varajärjestelmille
- vastuuhenkilöt ja varahenkilöt
- ohjeet toiminnasta poikkeustilanteessa.

Suunnitelmien päivittäminen ja katselmointi on organisoitu ja vastuutettu.

KORKEA TASO

Jatkuvuus- ja toipumissuunnitelmien testaaminen (JTH-004): Organisaation jatkuvuus- ja toipumissuunnitelmia testataan käytännössä säännöllisesti joko kokonaisuutena tai osissa. Suunnitelmia päivitetään testausten tulosten pohjalta.

Häiriöiden kirjaaminen (JTH-005): Organisaation tulee pitää kirjaa järjestelmien häiriöistä ja niiden syistä. Vikaraportteja käytetään organisaation riskianalyysin tekemisessä sekä yhteistyösopimuksia määriteltäessä. Näin mahdolliset häiriötilanteet saadaan osaksi organisaation toiminnan kehittämistä ja esimerkiksi palvelutasojen määrittelyä alihankkijoiden kanssa.

3.2 Sovelluskehitysmallit

PERUSTASO

Sovelluskehitysprosessi (SKM-001): Organisaatiolla tulee olla kirjallinen sovelluskehitysprosessi, joka kuvaa organisaation käytännöt sovelluskehityksen kaikilla osa-alueilla. Sovelluskehitysprosessi tulee kouluttaa kaikille sovelluskehitystä tekeville työntekijöille, ja organisaation tulee myös varmistua siitä, että prosessia käytetään kaikessa sovelluskehitystyössä. Organisaatio on vastuuttanut prosessin kuvauksen päivittämisen ja kehittämisen. Asiakkailta ja käyttäjiltä saatua palautetta käytetään syötteenä prosessin kehittämisessä. Prosessi ottaa kantaa myös kaikkien kehitysvaiheiden asettamiin tietoturvahaasteisiin (ns. secure SDLC – secure software development life cycle).

Käytettävä Secure SDLC riippuu toteutettavan sovelluksen tietoturvallisuuden tasosta, käytettävästä prosessimallista, teknologioista jne. Se voi ottaa kantaa esimerkiksi seuraaviin asioihin:

- Tietoturvatestaus
- Tyypilliset ongelmat, esimerkiksi SANS/CWE top 25 ohjelmointivirheet ja OWASP Top 10 riskit
- Turvallinen arkkitehtuuri
- Tietoturvavaatimusten määrittely
- Noudatettavat standardit ja vaatimukset
- Noudatettava koodausopas
- Vaadittavat kriteerit eri vaiheista poistumiselle
- Tietoturvallinen ylläpito, asennus, konfigurointi.

Myös tämä dokumentti asettaa vaatimuksia käytettävälle sovelluskehitysprosessille.

Esimerkkejä:

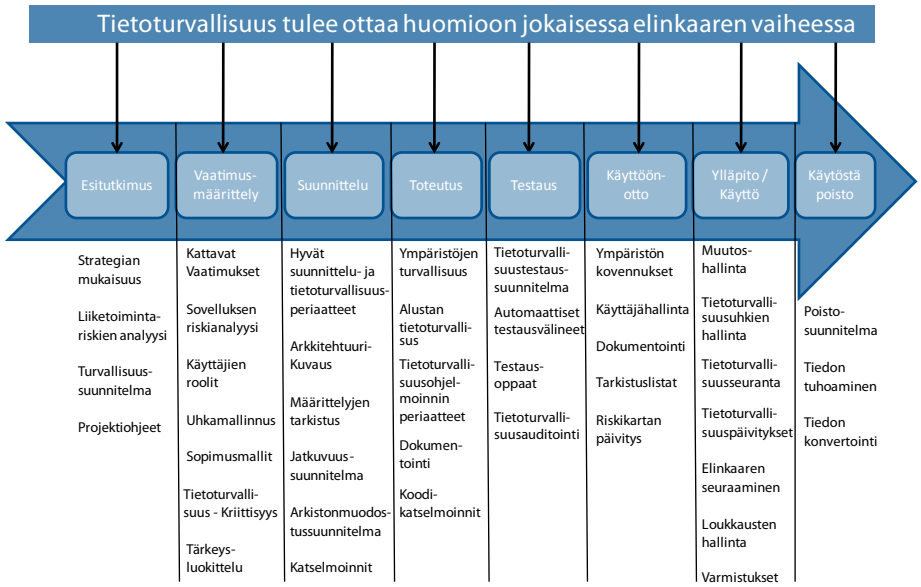
- Homeland Security: Secure Software Development Life Cycle Processes[8]
- SD Elements: Software Security Throughout the Life Cycle: 9 Steps[9]

Turvallisten sovellusten aikaansaamiseksi tietoturvatehtävät tulee integroida organisaation sovelluskehitys- ja systeemityömalleihin luonnolliseksi osaksi muuta kehitystyötä. Suunnittelun lähtökohtana on hyvä olla riskipohjainen lähestymistapa, ja riskianalyysiä joudutaan tekemään sovelluskehityksen eri vaiheissa varsinkin ketterissä menetelmissä. Suunnittelun alkuvaiheessa tulee tiedostaa ja ottaa huomioon sovelluksen kriittisyys ja sille asetetut tietoturvavaatimukset. Sovelluksen tietoturvallisuuden toteutuksesta on hyvä tuottaa dokumentti. Kuvassa 5 on kuvaus eri sovelluskehitysvaiheiden keskeisistä tehtävistä riippumatta siitä, mihin malliin sovelluskehitys perustuu.

[8] https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/sdlc/326-BSI.html

[9] http://www.sdelements.com/secure-sdlc/software-security-throughout-life-cycle-9-steps/

Kuva 5. Sovelluskehityksen työkalupakki



3.2.1 Vesiputousmalli

Vesiputousmallia käyttävissä sovelluskehitysprosesseissa tietoturvallisuus toteutetaan tyypillisesti seuraavasti:

- Jokaiselle vaiheelle määritellään tietoturvallisuuteen liittyvät tehtävät, jotka tulee saattaa valmiiksi työvaiheen aikana (ks. kuva 5).
- Vaiheesta toiseen siirryttäessä määritellään ns. pääsykriteerit (exit criteria). Seuraavaan vaiheeseen ei voida siirtyä, mikäli kriteerit eivät täyty. Tietoturvallisuuden kannalta on tärkeää, että pääsykriteerit sisältävät myös tietoturvallisuuteen liittyviä asioita.
- Projektin ohjausryhmä seuraa myös tietoturvallisuuteen liittyvien tehtävien valmistumista.

Käytännössä vesiputousmallin seuraaminen sovelluskehityksessä on osoittautunut haasteelliseksi. Suurimmat ongelmat johtuvat siitä, että yhden vaiheen loppuun saattaminen siten, että siihen ei tarvitse palata myöhemmin on käytännössä mahdotonta. Vesiputousmalli taas ei ota kantaa siihen, miten projektin aikana tapahtuvat muutokset aiempaan työvaiheeseen tulisi ottaa huomioon. Tyypillisesti vaatimuksia muokataan vielä toteutus- ja käyttöönottovaiheissakin. Lisäksi suurissa kokonaisuuksissa esimerkiksi kehitysvaiheen implementointivaikeuksien ennakointi on mahdotonta. Usein käytännössä paras keino olisi suunnitelman muokkaaminen, mutta se on yleensä käytännössä mahdotonta johtuen aiempiin työvaiheisiin uponneista kuluista ja siitä, että suunnitelma on luokiteltu valmiiksi ja jäädytetty. Mainituilla seikoilla on luonnollisesti vaikutus myös toteutettavan sovelluksen tietoturvallisuudelle.

Vesiputousmallin lisäksi on olemassa myös muita samankaltaisia malleja, kuten esimerkiksi V-malli, joka lähestyy ongelmaa testausnäkökulmasta. V-mallissa testausvaiheet sidotaan suunnitteluvaiheisiin. Esimerkiksi yksittäisen moduulin suunnittelua vastaa yksikkötestaus, jossa testataan toteuttaako moduuli sille määritellyt tehtävät oikein.

3.2.2 Ketterät menetelmät

Ketterä sovelluskehitys perustuu inkrementaaliseen ja iteratiiviseen kehitykseen, jossa vaatimukset ja sovelluksen ominaisuudet elävät projektin aikana ja ne määritellään tiiviissä yhteistyössä eri sidosryhmien kanssa.

Tietoturvallisuuden kannalta on oleellista, että omistaja kykenee määrittelemään tietoturvallisuuteen liittyviä tehtäviä työjonoon. Tähän voi käyttää seuraavia työkaluja:

- **Uhka-analyysi:** Omistajan tulee tehdä korkean tason uhka-analyysi toteutettavasta sovelluksesta. Tarkoituksena on tunnistaa kaikki sovelluksen liiketoimintariskit.
- **Tietoturvakertomukset (security story):** Omistaja määrittelee uhka-analyysin pohjalta yleisen tason tietoturvakertomuksia, jotka määrittelevät sovelluksen korkean tason tavoitteet tietoturvallisuuden osalta.
- **Väärinkäyttötapaukset (abuse case):** Omistaja määrittelee uhka-analyysin pohjalta myös väärinkäyttötapauksia, jotka ovat käyttötapauksia hyökkääjän näkökulmasta.

Toteutusvaiheen aikana tietoturvallisuus sisällytetään toteutettaviin ominaisuuksiin esimerkiksi seuraavilla työkaluilla:

- Tietoturvakriteerien lisääminen työvaiheen ”definition of done” -määrityksiin.
- Tekninen uhka-analyysi työvaiheen aikana toteutettaville ominaisuuksille (uhkien mallintaminen).

3.3 Sovelluskehityksen vaiheet ja tietoturvatasojen vaatimukset

Tietoturvallinen sovelluskehitys vaatii luonnollisesti, että tietoturvallisuus otetaan huomioon ja rakennetaan sovelluksen sisään sen elinkaaren eri vaiheissa. Sovelluskehitysmallista riippumatta kaikkiin projekteihin kuuluu aktiviteetteja seuraavista osa-alueista:

- Esitutkimus
- Vaatimusmäärittely
- Suunnittelu
- Toteutus
- Testaus
- Käyttöönotto

- Ylläpito
- Käytöstä poisto.

Seuraavissa kappaleissa kuvataan sovelluksen elinkaaren eri vaiheiden tietoturvavaatimukset.

3.3.1 Esitutkimus

Esitutkimusvaihe keskittyy sovelluksen analysointiin liiketoiminnan näkökulmasta. Tässä vaiheessa otetaan huomioon laeista ja asetuksista tulevat vaatimukset, sopimukset ja sidosryhmien vaatimukset sekä organisaation periaatteet ja ohjeet. Näistä kaikista liiketoimintaa ohjaavista seikoista johdetaan sovelluksen tietoturvavaatimuksia, kuten esimerkiksi käsiteltävän tiedon vaatima suojaustaso.

PERUSTASO

Tarkoitus ja kriittisyys (ESI-001): Toteutettavan sovelluksen liiketoimintatarkoitus sekä sovelluksen kriittisyys sitä käyttävän organisaation liiketoiminnalle tulee määritellä. Määrittely on dokumentoitava ja sovellus on luokiteltava sen avulla. Lisäksi sovelluksen käsittelemien tietojen luottamuksellisuus tulee määritellä. Käsitelty tieto voi olla luokiteltua esimerkiksi suojaustasojen mukaan. Määritykset toimivat koko projektin ajan sovelluksen tietoturvamekanismien valintaa, suunnittelua ja toteutusta ohjaavina tekijöinä.

Liiketoiminnan vaikutusanalyysi (ESI-002): Toteutettavalle sovellukselle tulee tehdä liiketoiminnan vaikutusanalyysi, jossa selvitetään mitä vaikutusta erilaisten uhkakuvien toteutumisella on organisaation toiminnalle.

3.3.2 Vaatimusmäärittely

Vaatimusmäärittelyn suunnittelussa otetaan huomioon sovelluksen tietoturvataso ja kehitettävän sovelluksen kriittisyys liiketoiminnalle. Vaatimusmäärittelyssä on tärkeä kartoittaa sovellukselle asetetut ympäristöstä tulevat integrointivaatimukset ja ottaa huomioon organisaation kokonais- ja tietoturva-arkkitehtuuri. Uhkamallinnuksella ja riskianalyysilla haetaan rakennettavan sovelluksen potentiaalisia tietoturvallisuuden heikkouksia ja valitaan sovelluksessa käyttöönotettavat suojaukset ja kontrollit.

PERUSTASO

Tietoturvaratkaisuiden dokumentointi (VTM-001): Tietoturvavaatimukset toteuttavat ratkaisut tulee dokumentoida, jolloin dokumentit toimivat suunnittelun pohjana sovelluksen toteuttajille ja ratkaisujen riittävyys voidaan todentaa. Dokumenttien päivitys ja katselmointi pitää organisoida ja vastuuttaa.

Lainsäädännölliset vaatimukset (VTM-002): Sovelluksen pitää huomioida käsiteltyyn tietoon, sovelluksen toimintaympäristöön tai muihin tekijöihin vaikuttavat lainsäädännölliset vaatimukset.

Tietoturva-analyysi (VTM-003): Sovelluksen suunnittelu tulee aloittaa käymällä läpi esitutkimusvaiheessa määritelty sovellusprofiili ja määrittelemällä sen asettamat yleisen tason tietoturvavaatimukset. Analyysin tuotteena saadaan karkean tason kuva sovelluksen tietoturvavaatimuksista tietoturvallisuuden eri näkökulmista (luottamuksellisuus, eheys ja saatavuus). Analyysia käytetään sovelluksen suunnittelun pohjana, jolloin järjestelmän tietoturvaominaisuudet suunnitellaan suojattavan tiedon sekä järjestelmän kriittisyyden mukaan.

Sovelluksen tietoturvataso (VTM-004): Järjestelmän omistajan vastuulla on määritellä, mitä tietoturvatasoa toteutettavan järjestelmän tulee toteuttaa. Järjestelmän omistaja on lisäksi vastuussa järjestelmästä ja sen sisältämästä tietoaineistosta. Lisäksi omistajan tulee määritellä vaatimukset tietoaineiston arkistoinnille yhteistyössä organisaation asiakirjahallinnon kanssa.

Sovelluksen riskianalyysi (VTM-005): Sovelluksen tietoturvavaatimukset tulee ottaa huomioon jo suunnitteluvaiheessa kohdistamalla sovellukseen riskianalyysi. Vaatimukset määräytyvät järjestelmän omistajan tekemän tietoturvatasomäärityksen ja käytetyn autentikaatiomenetelmän valinnan kautta.

Riskianalyysin ytimessä ovat sovelluksen tietoturvallisuuden pahimmat mahdolliset tapaukset (worst case scenario), jotka tulee listata käyttämällä lähtökohtana sovelluksen liiketoimintatarkoitusta, sovelluksen käsittelemää tietoa ja liiketoiminnan riskiprofiilia. Jokainen riski tulee kuvata yhdellä lauseella ja määritellä se hyökkääjän korkean tason tavoitteiksi. Tämän jälkeen jokaiselle riskille tulee määritellä esiehdot joiden pitää päteä jokaiselle hyökkääjän tavoitteen onnistumiselle. Informaatio voidaan esittää ns. uhkapuuna tai rakenteellisena listana.

Esimerkki: Organisaatio kehittää web-sähköpostisovellusta. Eräs tunnistettu pahin mahdollinen tapaus: käyttäjän viestit ovat muiden luettavissa.
Tunnistettu uhka: hyökkääjä voi lukea muiden käyttäjien sähköposteja.
Esiehdot:

1. Datan validointi ei toimi TAI
2. Auktorisointi ei toimi TAI
3. Selaimen välimuistiin jää luottamuksellista informaatiota JA
    a. Käyttäjä käyttää jaettua konetta TAI
    b. Hyökkääjää saa käyttäjän koneen käsiinsä TAI
    c. Selaimen tietoturvapuute altistaa välimuistin hyökkääjälle.

Sovelluksen tietoturvavaatimukset (VTM-006): Kehitettävälle sovellukselle tulee määritellä tietoturvavaatimukset. Sovelluksen tietoturvavaatimukset tulee johtaa seuraavista lähtökohdista:

- Sovelluksen kriittisyys liiketoiminnalle
- Sovelluksen sisältämän ja käsittelemän tiedon asettamat vaatimukset
- Sovelluksen toiminnallisista vaatimuksista johdetut vaatimukset
- Uhka-analyysi.

Analyysin pohjana voi käyttää muun muassa seuraavia näkökulmia:

- tiedon eheys
- tiedon luottamuksellisuus
- tiedon saatavuus
- pääsynhallintavaatimukset
- toiminnon kriittisyys
- tehtävien eriyttäminen (separation of duties)
- vasteajat
- kuormitus.

Liiketoimintaprosessin omistajien ja muiden sidosryhmien edustajien tulee osallistua tietoturvavaatimusten määrittelyyn.

Lait, määräykset ja ohjeistukset (VTM-007): Tietoturvavaatimusten määrittelyn pohjana tulee käyttää myös soveltuvia lakeja, määräyksiä, standardeja ja ohjeistuksia. Tällaisia ohjeistuksia voivat olla muun muassa toimialan best practice -suositukset, liiketoiminta-alaan tai valittuihin teknologioihin soveltuvat standardit, compliance-vaatimukset, ulkoiset tai sisäiset vaatimukset jne. Liiketoiminnan omistajat ja arkkitehdit määrittelevät käytettävät ohjeistukset.

KOROTETTU TASO

Uhkamallinnus (VTM-008): Sovellukselle on tehtävä uhkamallinnus, joka perustuu johonkin valittuun metodiin tai malliin. Esimerkkejä malleista ovat Microsoft STRIDE, DREAD ja väärinkäyttötapausten (abuse case) analyysi. Myös muita malleja voidaan soveltaa, esimerkiksi organisaation omaa mallia.

Väärinkäyttötapausten analyysissä käydään läpi sovelluksen käyttötapaukset ja eritellään, miten hyökkääjä voisi käyttää kyseistä toiminnallisuutta hyväkseen. Näin saatuja väärinkäyttötapauksia tulee käyttää myös testitapausten määrittämiseen.

Esimerkki: käyttötapaus web-sovellukselle: Käyttäjä kirjautuu sovellukseen käyttäen tunnusta ja salasanaa. Vastaavia väärinkäyttötapauksia:

- hyökkääjä murtaa kirjautumisen brute force-hyökkäyksellä
- hyökkääjä salakuuntelee kirjautumistunnukset
- hyökkääjä selvittää tunnukset social engineering-hyökkäyksellä
- hyökkääjä saa salatut tunnukset haltuunsa ja murtaa ne offline-työkaluilla
- hyökkääjä ohittaa kirjautumistoiminnallisuuden
- hyökkääjä näkee luottamuksellista tietoa ilman kirjautumista.

Lisää tietoa saa esimerkiksi OWASP:n sivuilta.[10]

[10] https://www.owasp.org/index.php/Threat_Risk_Modeling

Arkkitehtuurilinjaus (VTM-009): Sovelluksen hankkivalla organisaatiolla tulee olla arkkitehtuurilinjaus, jonka mukaisia hankittavien järjestelmien tulee olla. Arkkitehtuurilinjauksen pitää sisältää myös tietoturvavaatimuksia, kuten:

- Vaaditut salausmenetelmät
- Vaaditut tunnistautumismenetelmät
- Vaaditut lokien keräysmenetelmät.

Tällöin varmistutaan siitä, että kaikki hankittavat järjestelmät täyttävät tietyt tietoturvakriteerit ja sopivat hankkivan organisaation tietoturvainfrastruktuuriin.

Uhkamallinnuksen tarkennus (VTM-010): Rakennettua uhkamallia tulee tarkentaa ottamalla mukaan uhkia jotka liittyvät sovelluksen toteutukseen tai arkkitehtuuriin. Tällaisia asioita ovat muun muassa:

- Käyttäjäroolit
- Tietoturvaoletukset
- Käytetyt teknologiat
- Tietoturvamekanismit.

KORKEA TASO

Komponenttien uhka-arvio (VTM-011): Sovelluksen käyttämille kolmansien osapuolten komponenteille tulee tehdä uhka-arvio. Näitä komponentteja ovat esimerkiksi avoimen lähdekoodin kirjastot, online-palvelut tai COTS-ohjelmistot (commercial off the shelf, valmisohjelmistot). Tulee selvittää, miten haavoittuvuudet tai suunnitteluvirheet komponenteissa vaikuttavat kehitettävän sovelluksen tietoturvallisuuteen.

3.3.3 Suunnittelu

Suunnittelussa toteutetaan määrittelyn vaatimukset organisaation arkkitehtuurien ja standardien mukaisesti. Tässä vaiheessa on suunniteltava myös monia tietoturvaominaisuuksia, kuten tunnistautumismenetelmät ja salausratkaisut. Suunnittelu on tehtävä siten, että sovelluksen hyökkäyspinta-alasta muodostuu mahdollisimman pieni. Tietoturvaratkaisut dokumentoidaan.

PERUSTASO

Yleiset standardit (SNT-001): Arkkitehtuuria suunniteltaessa tulee suosia yleisesti käytössä olevia ja hyväksyttyjä standardeja, mikäli se on mahdollista. Näin varmistetaan se, että suunniteltava sovellus on helppo integroida muihin järjestelmiin. Lisäksi tunnetut ja yleisesti käytetyt ratkaisut ovat yleensä joutuneet tarkemman tietoturva-analyysin koh-

teeksi kuin itse toteutetut tai harvinaisemmat teknologiat. Lisäksi avointen standardien käyttämistä suositaan, koska niiden tietoturvaominaisuudet tunnetaan tyypillisesti suljettuja standardeja paremmin.

Tietoturvapäivitysten suunnittelu (SNT-002): Sovellus tulee suunnitella siten, että korjausten ja tietoturvapäivitysten asentaminen on mahdollisimman helppoa. Käytännössä tämä tarkoittaa ainakin seuraavien asioiden huomioimista:

- Ei kovakoodattuja konfiguraatioarvoja
- Sovellus ei ole riippuvainen tietyistä ohjelmistoversioista, kuten JRE-versiosta. Toteutettavaa sovellusta ei saa suunnitella siten, että se on riippuvainen käytetyn komponentin ominaisuudesta, joka löytyy vain komponentin tietystä versiosta.
- Kirjastoriippuvuudet on toteutettu siten, että päivittäminen onnistuu helposti.

Suositellut ohjelmistot (SNT-003): Organisaation tulee perustaa ja ylläpitää listaa suositelluista ohjelmistokomponenteista, kirjastoista, sovelluskehyksistä jne., joita käytetään organisaation toteuttamissa sovelluksissa. Komponentit luokitellaan toiminnallisuuden mukaan. Komponenttien tietoturvatilannetta ja päivityksiä tulee seurata.

Ulkoiset rajapinnat (SNT-004): Sovelluksen ulkoiset rajapinnat käydään läpi ja verrataan niitä organisaation arkkitehtuuri- ja sovelluskehitysohjeistukseen kirjattuihin periaatteisiin (Katso TSK-001).

Rajapintakohtaisesti selvittäen analysoidaan, toteutuuko periaate sovellustasolla. Tarvittaessa selvitetään, voiko tietoturvamekanismin toteuttaminen kohtuullisella työllä parantaa järjestelmän tietoturvallisuutta.

Tietoturvalliset suunnittelumallit (SNT-005): Sovelluksen arkkitehtuurin suunnittelussa tulee käyttää ns. turvallisia suunnittelumalleja (secure design pattern). Organisaation kehittämät sovellukset tulee luokitella yleisen arkkitehtuurin mukaan. Tavallisia korkean tason arkkitehtuuriluokkia ovat muun muassa:

- client-server
- sulautettu järjestelmä
- työpöytäsovellus
- web-sovellus
- web service
- mobiilisovellus.

Jokaista yleistä arkkitehtuuriluokkaa koskevat suunnittelumallit tulee kerätä ja soveltaa kehitettäviin sovelluksiin. Suunnittelumallien tunnistamisen ja valitsemisen tekevät arkkitehdit ja kokeneet sovelluskehittäjät sovelluksen suunnitteluvaiheessa. Suunnittelumallien pitää sisältää myös tietoturvallisia suunnittelumalleja (secure design patterns) ts. malleja, jotka ratkaisevat tietoturvallisuuteen liittyvän suunnitteluongelman.

Katso esimerkkejä:

- Security Patterns for J2EE Applications, Web Services, Identity Management, and Service Provisioning[11]
- SecurityPatterns.org [12]
- Architecture and Design Considerations for Secure Software [13]
- Secure Design Patterns[14]

Esimerkki: Organisaatio kehittää web-sovellusta verkkokaupankäyntiin. Tunnistettuja ja käytettyjä turvallisia suunnittelumalleja ovat muun muassa:

- Keskitetty lokien keräys
- Keskitetty virheiden- ja poikkeustenkäsittely
- Syötteen validointi
- SSO:n käyttö kirjautumiseen.

Hyökkäyspinta-ala (SNT-006): Sovelluksen hyökkäyspinta tulee tunnistaa. Hyökkäyspinnalla tarkoitetaan kaikkia järjestelmän toiminnallisuuksia, joissa osapuolet eivät voi täysin luottaa toisiinsa ja joita voidaan siten käyttää sovellusta vastaan hyökättäessä. Tällaisia ovat esimerkiksi:

- Avoimet palvelut
- Syöterajapinnat
- Web servicet
- RPC
- Sovelluspalvelimen ja tietokantapalvelimen välinen liikenne
- Järjestelmän palvelimilla toimivat muut sovellukset.

Hyökkäyspinnan määrittely tehdään analysoimalla sovelluksen korkean tason arkkitehtuuria. Arkkitehtuurin jokainen komponentti käydään läpi ja analysoidaan pääsy komponentin rajapintoihin esimerkiksi seuraavilta osin:

- Tunnistautumaton käyttäjä
- Autentikoitunut käyttäjä
- Ylläpitäjä
- Sovelluksen muut roolit.

[11] http://coresecuritypatterns.com/patterns.htm

[12] http://www.securitypatterns.org/patterns.html

[13] https://buildsecurityin.us-cert.gov/swa/downloads/ArchitectureAndDesign_PocketGuide_v2%200_05182012_PostOnline.pdf

[14] www.cert.org/archive/pdf/09tr010.pdf

Tehty kuvaus muodostaa sovelluksen hyökkäyspinnan (attack surface). Sitä käytetään pohjana rajapintojen ja moduulien tietoturvamekanismien suunnittelussa. Hyökkäyspinta pitää päivittää, jos sovellukseen tulee merkittäviä muutoksia.

Arkkitehtuurin tietoturvavaatimukset (SNT-007): Sovelluksen arkkitehtuuri on analysoitava tunnettuja tietoturvavaatimuksia vasten. Vertaa tietoturvavaatimuksia sovelluksen hyökkäyspintaan ja sovelluksen arkkitehtuuriin sekä varmista, että kaikki vaatimukset toteutuvat arkkitehtuuritasolla. Paranna sovelluksen arkkitehtuuria ja suunniteltuja tietoturvamekanismeja mikäli kaikki vaatimukset eivät täyty. Suorita uusi analyysi mikäli arkkitehtuuriin tulee suuria muutoksia.

Tietoturvamekanismien kattavuus (SNT-008): Suunnittelukatselmoinneissa on varmistettava, että yhteisesti hyväksytyt tietoturvaratkaisut (Katso TSK-002) ovat käytössä koko sovelluksessa. Arkkitehtuuria suunniteltaessa käydään läpi kaikki liittymät järjestelmien välillä ja tarkastetaan niiden tietoturvamekanismit. Analyysi tehdään sekä sisäisille että ulkoisille rajapinnoille.

Analyysin tarkoituksena on varmistaa, että suunniteltuja tietoturvamekanismeja käytetään koko sovelluksen laajuisesti. Näin estetään esimerkiksi se, että jokainen sovelluskehittäjä toteuttaa oman lokitoiminnallisuutensa tai virheenkäsittelymekanisminsa. Analyysi toistetaan aina uuden sovellusjulkaisun yhteydessä, jolloin edellisen julkaisun yhteydessä tehdyn analyysin havainnot päivitetään.

Tunnistautumismenetelmä (SNT-009): Valitulla tunnistautumismenetelmällä on suuri vaikutus kokonaisuuden tietoturvallisuuteen. Sovelluksen omistajan vastuulla on määritellä sovelluksen käsittelemän tiedon luokittelu, joten hänen vastuullaan on myös määritellä se, miten vahvaa tunnistautumista sovelluksessa käytetään. Tämän perusteella valitaan soveltuva käyttäjäntunnistusmenetelmä. Vaihtoehtoja ovat muun muassa:

- Käyttäjätunnus ja salasana
- Tunnuslukulistat
- SMS
- Tietoturvalaite, kuten RSA-tunniste
- Toimikortti
- Pankkitunnistautuminen
- SSO-palvelu
- Federointipalvelu
- KATSO- tai VIRTU-tunnistautuminen.

Salasanavaatimusten konfigurointi (SNT-010): Mikäli sovelluksen omistaja määrittelee riittäväksi tunnistautumismekanismiksi salasanan ja käyttäjätunnuksen, pitää sovellus toteuttaa siten, että ainakin seuraavat salasanan laatuvaatimukset ovat konfiguroitavissa:

- Salasanan pituus
- Erikoismerkkien määrä
- Tunnuksen lukkiutuminen määräajaksi liian monen epäonnistuneen kirjautumisen jälkeen

- Salasanan vanhenemisaika
- Tunnuksen vanhenemisaika.

Mikäli mahdollista, tulisi salasanojen käyttöä itse sovelluksessa välttää ja tallentaa ne esimerkiksi LDAP-tietokantaan, jossa salasanojen laatuvaatimuksia voidaan hallita keskitetysti.

Lisäksi on varmistuttava siitä, että sovelluksen kehittäjille ja ylläpitäjille tulee olla mahdollista määritellä tiukemmat vaatimukset muun muassa salasanan pituuden ja erikoismerkkien suhteen.

On suositeltavaa käyttää salasanalauseita: esimerkiksi vähintään 16 merkkiä ilman kompleksisuusvaatimuksia (erikoismerkit). Salasanalauseiden käytöllä saadaan ehkäistyä yleisimmät salasanoihin kohdistuvat hyökkäykset, kuten brute force -hyökkäys ja ns. sateenkaaritaulukoiden (rainbow tables) käyttö. Kyseiset taulukot sisältävät esilaskettuja tiivistearvoja salasanoista, ja niitä voidaan käyttää salasanatiivisteiden murtamiseen.

Lisäksi on suositeltavaa käyttää samoja salasanavaatimuksia sekä testi- että tuotantoympäristöissä. Muussa tapauksessa siirrettäessä järjestelmää tuotantoon testiympäristössä käytetyt salasanat tulee vaihtaa tuotantoympäristön vaatimukset täyttäviin.

Käyttöoikeustasot (SNT-011): Sovellukset tukevat yleensä useaa eri käyttöoikeustasoa (käyttäjä, ylläpitäjä jne.) Sovelluksen käyttäjille on myönnettävä vain sen tasoiset oikeudet, jotka ovat välttämättömiä heidän roolinsa kannalta (ns. least privilege). Myönnettyjen tunnusten on oltava henkilökohtaisia, ja yleiskäyttöisten tunnusten käyttö on estettävä tai kiellettävä. Sovelluksen tietoturvallisuuteen vaikuttaviin ominaisuuksiin tulee olla pääsy vain sovelluksen pääkäyttäjällä. Samoin sovellus tulee toteuttaa siten, että sen käynnistämät prosessit suoritetaan pienimmällä mahdollisella käyttöoikeustasolla.

Tätä samaa periaatetta tulee käyttää sovelluksen kaikissa komponenteissa, kuten tietokannassa, jossa sovelluskäyttäjältä estetään esimerkiksi tietokantaskeeman muutokset.

Luottamusrajat (SNT-012): Sovellusta suunniteltaessa tulee määritellä ns. luottamusrajat[15] (trust boundaries). Kaikkea rajan toiselta puolelta tulevaa dataa tulee käsitellä ei-luotettuna, ja luottorajan toisella puolella oleviin tarkastuksiin ei tule luottaa. Ei-luotettu data tulee validoida ja kanonisoida ennen käyttöä. Validointi tulee toteuttaa ns. white list -pohjaisesti, toisin sanoen vain erikseen sallittu syöte hyväksytään ja muu hylätään. Myös salausmenetelmiä ja sähköistä allekirjoitusta voidaan käyttää tiedon aitouden ja muuttumattomuuden varmistamiseksi. Samoin ulkoisille komponenteille luovutettava data tulee enkoodata ja kanonisoida ennen lähettämistä. Näin varmistutaan siitä, että luovutettava data on turvallista ulkoisen komponentin käytettäväksi.

Salausratkaisut (SNT-013): Sovelluksessa käytettyjä salausratkaisuja koskevat seuraavat vaatimukset (ks. VAHTI 3/2008 termistön osalta):

- Sovelluksen tulee säilyttää vain sellainen luottamuksellinen data, jota se tarvitsee. Datan säilyttäminen varmuuden vuoksi on kiellettyä.

[15] Luottamusraja on usein sama kuin hyökkäyspinta

- Salausratkaisuiden tulee olla tunnettuja, julkisia ja käyttötarkoitukseen nähden riittävän vahvoiksi todettuja. Tällaisia ovat esimerkiksi AES ja RSA julkisen avaimen kryptografiaan sekä SHA-256 tiivisteiden laskemiseen. Huomaa, että algoritmin ”vahvuus” on elävä suure. [16]
- Salausratkaisuja ei koskaan tule toteuttaa itse, vaan tulee käyttää tunnettuja toteutuksia (esimerkiksi OpenSSL, KeyCzar, jne.)
- Käytettyjen satunnaislukugeneraattoreiden pitää olla vahvoja ja niiden siemenarvojen tulee sisältää riittävästi entropiaa.
- Tallennetuista salasanoista tulee tallentaa vain salt-arvojen kanssa lasketut tiivisteet.
- Salasanojen tallentamiseen on käytettävä adaptiivista tiivistealgoritmia.
- Kaikki tietoliikenne sovelluspalvelimen ja asiakasohjelmiston välillä tulee salata, mikäli se kulkee julkisen verkon yli, jolloin verkkoliikennettä salakuuntelemalla ei ole mahdollista saada haltuunsa luottamuksellista tietoa. Käytetyt salausratkaisut pitää pystyä tarvittaessa vaihtamaan. Mikäli siirrettävä tieto on luonteeltaan julkista, ei sitä tarvitse salata. Tällaista tietoa on esimerkiksi julkiset web-sivustot.
- Turvallisuusluokitellun tiedon salaamiseen käytettyjen ratkaisujen tulee olla tarkastettu ja hyväksytty ko. tasolle kansainvälisen tai kansallisen tietoturvaviranomaisen toimesta tai erillisessä ratkaisulle suoritetussa tarkastuksessa.

Tuki- ja ylläpitoyhteydet (SNT-014): Mikäli sovelluksen tuki- tai ylläpitotoiminnallisuus vaatii toimittajan tai tukea toimittavan tahon pääsyn järjestelmään, on tämä otettava huomioon jo suunnitteluvaiheessa. Erityisesti kriittisiä ovat ulkopuolisten mahdollinen pääsy järjestelmän tietoihin ja mahdollisten etäyhteyksien suojaaminen.

KOROTETTU TASO

Uhkamallinnuksen syventäminen (SNT-015): Vaatimusmäärittelyvaiheessa tehtyä uhkien mallintamista tulee syventää uudella tiedolla esimerkiksi valituista teknisistä ratkaisuista sekä sovelluksen toiminnallisuudesta.

Monitasoarkkitehtuurit (SNT-016): Mikäli sovellus toteuttaa ns. monitasoarkkitehtuuria (n-tier architecture), tulee eri komponenttien, kuten sovelluspalvelin ja tietokanta, välinen tietoliikenne suunnitella ja dokumentoida kattavasti. Sovelluksen tulee mahdollistaa ainakin:

- Eri komponentit voidaan sijoittaa eri verkkosegmentteihin
- Sovelluspalvelimen ja tietokannan välisiin yhteyksiin tulee mahdollisuuksien mukaan käyttää alustojen tukemia nimettyjä tietolähteitä (datasource).
- Komponenttien välisen tietoliikenteen salaaminen, tunnisteiden käyttö sekä molemminpuolinen tunnistaminen (esimerkiksi mutual TLS)
- Hallinta- ja valvontaliikenteen erottaminen muusta liikenteestä.

[16] http://csrc.nist.gov/groups/STM/cavp/index.html

KORKEA TASO

Vahva tunnistautuminen (SNT-017): Korkean tietoturvatason järjestelmän arkkitehtuurin tulee toteuttaa seuraavat vaatimukset:

- Järjestelmään kirjautumiseen on käytettävä vahvaa tunnistautumista, jolloin tunnistautumiseen tarvitaan tietoa kahdesta eri lähteestä (esimerkiksi käyttäjätunnus/salasana sekä RSA-tunniste). [17]
- Sovelluksen on käytettävä monitasoarkkitehtuuria, jossa arkkitehtuurin eri komponentit on sijoitettava eri palvelimille.

3.3.4 Toteutus

Toteutusvaiheessa kirjoitetaan ohjelmakoodi määrittelyjen ja suunnitelman mukaisesti hankkeelle varatussa kehitysympäristössä. Ohjelmointivaiheessa havaitut tietoturvapuutteet palautetaan suunnitteluun. Toteutusvaiheessa on huolehdittava erityisesti virhetilanteiden oikeasta käsittelystä ja lokien kattavuudesta. Oikeaoppisella virheenkäsittelyllä estetään haavoittuvuuksien syntymistä. Lokituksella varmistetaan, että tietoturvaloukkaukset ovat selvitettävissä. Toteutusvaiheessa luodaan myös sovelluksen testiympäristö.

PERUSTASO

Virheiden käsittely (TOT-001): Sovelluksen poikkeus- ja virhetilanteiden käsittely tulee suunnitella ja toteuttaa siten, että virhetilanteet eivät johda sovelluksen tietoturvallisuuden vaarantumiseen. Huomioitavia asioita ovat ainakin:

- Virheiden ja poikkeusten käsittely tulee suunnitella koko sovelluksen kattavasti.
- Virheiden käsittely tulee toteuttaa keskitetysti ja koko sovelluksen kattavasti, jolloin testaus saadaan kattavaksi ja virheiden korjaamien on nopeampaa.
- Niin sanotulla fail-secure -suunnitteluperiaatteella varmistetaan, että virhetilanteessa komponentin tai sovelluksen käyttö ennemmin estetään kuin sallitaan tietoturvaloukkauksen hyväksikäyttö.
- Defensiivinen ohjelmointi
  - Oletetaan, että ohjelmaan on jäänyt virheitä. Jokainen ohjelman osa tekee syötteen tarkastuksen.
  - Tehdään ajonaikainen tarkastus kaikille mahdollisille virhetilanteille ja määritellään poikkeusten käsittely.
- Virheilmoitukset eivät saa sisältää luottamuksellista tietoa, kuten tietokantapalvelimen vastauksia, sovelluspalvelimen versiotietoja jne. Kaikissa virhetilanteissa näytetään yleinen virheilmoitus, joka kuvaa tapahtuneen virheen, mutta ei anna tietoa sovelluksen toteutuksesta. Myöskään ”henkilökohtaista” tietoa, kuten ylläpitäjien nimiä

[17] http://en.wikipedia.org/wiki/Two-factor_authentication

tai yhteystietoja, ei tulisi sisällyttää virheviesteihin social engineering -hyökkäysten estämiseksi.[18]

Lokit virhetilanteista ja tietoturvapoikkeamista (TOT-002): Sovelluksen tulee tuottaa riittävästi lokia virhetilanteista sekä tietoturvapoikkeamista. Riittävien lokien kerääminen sekä onnistuneista että epäonnistuneista tietoturvatapahtumista mahdollistaa hyökkäysten havaitsemisen ja helpottaa selvittämistä jälkikäteen. Lokiviesti pitää kirjoittaa seuraavista tapahtumista:

- Onnistuneet ja epäonnistuneet kirjautumisyritykset
- Onnistuneet ja epäonnistuneet pääsynhallintapäätökset
- Epäonnistuneet syötteenkäsittelypäätökset
- Ylläpitotoimet
- Kriittisen tiedon käsittely, mukaan lukien tiedon lukeminen. Sovelluksen tiedon käsittely, mukaan lukien tietojen katselu, on pystyttävä jäljittämään lokien perusteella.

Lokitapahtumien tiedot (TOT-003): Lokien pitää sisältää riittävästi tietoa operaation tekijän identifioimiseksi, hyökkäyksen tunnistamiseksi ajoissa ja jälkiselvityksen helpottamiseksi. Jokaisen lokikirjoituksen pitää sisältää ainakin seuraavat tiedot:

- Aikaleima luotettavasta lähteestä
- Tapahtuman merkitys tietoturvallisuuden kannalta (esimerkiksi matala, korkea, kriittinen)
- Indikaatio siitä, onko kyseessä tietoturvallisuuteen liittyvä tapahtuma (mikäli tietoturvalokia ei ole eriytetty omaan tiedostoonsa)
- Käyttäjätunnus ja lähdeosoite
- Onnistuiko tapahtuma
- Tapahtuman kuvaus.

Lokeihin ei kuitenkaan saa kirjoittaa luottamuksellista tietoa, kuten salasanoja, henkilötietoja tai luottokorttinumeroita. Lokitietojen tallentamisen yhteydessä tulee myös huomioida mahdollinen henkilörekisterin muodostuminen ja sen lakitekniset seuraukset.

Jokaisen lokirivin tulee noudattaa ennalta määriteltyä rakennetta, jotta lokitiedostojen automaattinen käsittely ja analysointi ovat mahdollisia.

Yhteinen aikalähde (TOT-004): Kaikkien ympäristöön kuuluvien laitteiden tulee synkronisoida kellonsa samasta lähteestä (esimerkiksi NTP-palvelin). Näin varmistetaan se, että tapahtumien järjestys pysyy johdonmukaisena ja eri lähteistä kerättyjen lokien korrelointi onnistuu helposti.

Lokien suojaaminen (TOT-005): Lokien kirjoittaminen: Lokien suojausta ja käsittelyä koskevat seuraavat vaatimukset:

- Lokitiedostojen pääsyoikeudet tulee määritellä siten, että vain tietyillä käyttäjäryhmillä on oikeus lukea ja muokata lokeja.

[18] https://www.owasp.org/index.php/Error_Handling

- Lokitapahtumat tulee kirjoittaa tapahtuma kerrallaan, ts. tapahtumia ei tule puskuroida ennen kirjoittamista mikäli suorituskykysyyt eivät estä suoraa kirjoittamista.

Istunnon suojaaminen (TOT-006): Istunnon kaappaaminen on tyypillinen tietoturvahyökkäys sovelluksia vastaan. Tällöin hyökkääjä saa kirjautuneen käyttäjän istunnon haltuunsa esimerkiksi istuntotunnisteen kaappaamalla. Sovellus tulee toteuttaa siten, että autentikoituneen käyttäjän istuntoa ei voi kaapata luvattomasti. Keinoja istunnon kaappaamisen estämiseksi ovat muun muassa: [19]

- Yhteyden salaus
- Istunnon aikakatkaisu
- Vaikeasti arvattava istuntotunniste
- Istuntotunnisteen suojaaminen (esimerkiksi seuraavat attribuutit: secure, httpOnly, domain, path, expires).
- Istunnon tuhoaminen käyttäjän kirjautuessa ulos
- Sivukohtaiset tunnisteet ns. CSRF-hyökkäyksen estämiseksi. CSRF
- -hyökkäyksessä hyökkääjä ei saa istuntoa kokonaan kaapattua, mutta pystyy pakottamaan käyttäjän tekemään transaktioita.
- Istunnon aloittajan IP-osoitteen tallentaminen ja käyttäminen istunnon seuraamisessa tunnisteen lisäksi.

Käyttäjätunnusten hallinta (TOT-007): Sovelluksen käyttäjätunnusten hallinta on toteutettava siten, että hallinta on mahdollisimman keskitettyä ja ajantasaista. Lisäksi sovelluksen tulee tukea ulkoista yhteistä käyttäjänhallintapalvelua, kuten LDAP-palvelinta.

Koodikatselmoinnit (TOT-008): Koodikatselmoinneissa varmistetaan, että toteutettaessa on:

- Noudatettu organisaation arkkitehtuuri- ja sovelluskehitysohjeistukseen kirjattuja periaatteita (Katso TSK-001)
- Käytetty yhteisesti hyväksyttyjä tietoturvaratkaisuja (Katso TSK-002)
- Huomioitu yleisimmät ohjelmointiin liittyvät tietoturvaongelmat, kuten
  - OWASP Top 10[20]
  - CWE/SANS TOP 25 Most Dangerous Software Errors[21]
  - The CERT Oracle Secure Coding Standard for Java.[22]

---

19 Istunnon kaappauksen estäminen voi olla myös sovelluspalvelimen vastuulla

20 https://www.owasp.org/index.php/Top_10_2010

21 http://www.sans.org/top25-software-errors/

22 https://www.securecoding.cert.org/confluence/display/java/The+CERT+Oracle+Secure+Coding+Standard+for+Java

KOROTETTU TASO

Lokien muokkaaminen (TOT-009): Korotetun tason järjestelmille asetetaan lisäksi seuraavat vaatimukset:

- Lokitietojen katselusta tulee kirjoittaa lokimerkintä
- Sovelluksen tai palvelimen ylläpitäjällä ei saa olla oikeutta muokata lokeja
- Tietoturvaloki tulee voida eriyttää omaan tiedostoonsa.

KORKEA TASO

Lokien parannettu suojaus (TOT-010): Korkean tason sovellusten tietoturvalokeille asetetaan lisäksi seuraavat vaatimukset:

- Lokitiedostoista lasketaan tarkistussumma, jolloin lokeihin jälkikäteen tehdyt muutokset pystytään havaitsemaan. Tarkistussummia säilytetään erillään tietoturvalokeista.
- Lokit tulee tallentaa kertakirjoitteiselle medialle tai ulkoiselle lokipalvelimelle, jolloin lokeja ei voi muokata jälkikäteen
- Lokitiedot voidaan tarvittaessa myös salata siirtovaiheessa ja lokipalvelimella
- Lokitietojen eheys tulee tarkistaa automaattisesti säännöllisesti.

3.3.5 Testaus

Testausvaiheessa keskitytään sovelluksen toiminnallisuuden varmistamiseen määritysten mukaisesti. Tietoturvatestauksella haetaan sovelluksen mahdollisia tietoturva-aukkoja ja testataan sovelluksen selviytymistä virhetilanteista ja väärinkäyttöyrityksistä. Korkealla tasolla voidaan myös vaatia lähdekoodin auditointia ja laajaa, syvällistä tietoturva-auditointia ennen sovelluksen käyttöönottoa. Hyväksymistestauksen vaatimustenmukaisuus tehdään tuotantoa vastaavassa ympäristössä.

PERUSTASO

Tietoturvallisuuden testitapaukset (TST-001): Tietoturvatestitapaukset tulee johtaa useista eri lähteistä, joita ovat ainakin:

- Sovelluksen tietoturvavaatimukset
- Sovelluksen toiminnalliset vaatimukset
- Aiemmat löydökset ja havaitut ongelmat
- Väärinkäyttötapaukset (mikäli näitä on tehty)
- Käytettyjen teknologioiden tyypilliset ongelmat (Kuten Owasp Top 10).

Kehittäjien, tietoturvavastaavien ja QA-vastaavien tulee katselmoida testitapausten tehokkuus, järkevyys ja kattavuus. Testitapausten suunnittelu tulisi tehdä sovelluksen määrittely- ja suunnitteluvaiheessa, sekä uudelleen kun sovellukseen tulee merkittäviä muutoksia.

Testisuunnitelman katselmointi (TST-002): Tietoturvavastaavan tulee katselmoida ja arvioida sovelluksen tietoturvasuunnitelma tai -suunnitelmat. Suunnitelmia tulee päivittää tietoturvavastaavan kommenttien perusteella.

Tietoturvatestien suorittaminen (TST-003): Tietoturvatestit tulee suorittaa osana sovelluksen normaalia testausprosessia. Testauksesta valmistuu testiraportti, joka sisältää tiedon tietoturvatestien suorituksesta.

Testausvaiheen koodikatselmointi (TST-004): Sovelluskehityksen tietoturvavastuullinen (security coach) voi tarvittaessa suorittaa epäformaaleja koodikatselmointeja tietoturvallisuuden kannalta kriittisiin osiin. Katselmointien tulokset kirjataan ylös organisaation prosesseihin parhaiten soveltuvaan paikkaan, jossa katselmointien tuloksia pystytään seuraamaan, esimerkiksi:

- Pöytäkirjaan
- Virheiden hallintatyökalu
- Ohjelmakoodiin.

Havaintojen korjaaminen vastuutetaan ja korjaustoimenpiteiden toteutumista seurataan.

Testidatan luonti (TST-005): Testauksessa käytetty data ei saa sisältää tuotannosta kopioitua salassa pidettävää tietoa. Testidata tulee siten joko generoida testausta varten, tuotantodatasta tulee poistaa salassa pidettävät tiedot tai data on sekoitettava. Sekoitetussa datassa yksittäiset tiedot voivat olla aitoja, mutta niiden yhdistelmät eivät.

Mikäli yllämainitut keinot eivät ole mahdollisia, tulee varmistua siitä, että testiympäristö on suojattu samoilla teknisillä ja hallinnollisilla suojakeinoilla kuin tuotantoympäristö. Tällöin voidaan varmistua siitä, että henkilöt, jotka eivät työssään tarvitse tuotantoympäristössä olevia tietoja, eivät voi niitä myöskään testiympäristössä käsitellä.

KOROTETTU TASO

Automaattiset testaustyökalut (TST-006): Tietoturvatestaamiseen tulee käyttää automaattisia testaustyökaluja. Automaattisten työkalujen käyttö tulee lisäksi olla integroituna sovelluskehitys- ja testausprosessiin. Työkaluja voivat olla esimerkiksi

- Fuzzerit (protokolla, syöte jne.)
- Haavoittuvuusskannerit
- Staattista tai dynaamista koodin analysointia tekevät työkalut
- Jatkuvan integraation (continuous integration) työkalut.

Tietoturva-auditointi (TST-007): Korotetun tason sovelluksen tietoturvallisuus on auditoitava ennen käyttöönottoa. Auditoinnissa on käytettävä sekä automaattisia että manuaalisia menetelmiä. Auditoijan on oltava ulkoinen, riippumaton osapuoli. Auditointi koostuu seuraavista vaiheista:

- Tekninen auditointi, jossa testataan tietoturvakontrollien toimivuus tunkeutumistestauksen keinoin
- Hallinnollinen auditointi, jossa tarkastetaan sovelluksen operointi- ja ylläpitoprosessit jne.
- Arkkitehtuurin auditointi, jossa tarkastetaan sovelluksen arkkitehtuuri tietoturvanäkökulmasta.

Tietoturvamekanismien tarkastus (TST-008): Sovelluksen tietoturvavaatimuksista tulee johtaa lista kooditasolla tarkastettavista asioista. Näitä voivat olla esimerkiksi toiminnallisista vaatimuksista johdettavat tarkastukset, sovelluskohtaiset hyvät käytännöt tai ohjelmointikielikohtaiset käytännöt. Tietoturvallisuuden kannalta kriittiset komponentit tulee käydä läpi käyttäen tarkistuslistaa. Tyypillisiä kriittisiä komponentteja ovat esimerkiksi:

- Autentikaation toteutus
- Pääsynhallinan toteutus
- Istunnon hallinta
- Salauksen toteutus
- Datan parsinta
- Syötteen validointi.

Tarkastus tulee uusia aina kun kyseessä oleviin kohteisiin tehdään merkittäviä muutoksia. Tarkastuksessa voi käyttää ulkoisia tarkistuslistoja (esimerkiksi OWASP ASVS). Katselmoinnista valmistuu pöytäkirja. Tehtyjen havaintojen korjaaminen vastuutetaan ja korjaamista seurataan. Viitemateriaalina katselmoinnissa voi käyttää esimerkiksi SANS/CWE top 25 -ohjelmointivirheiden listaa tai OWASPin koodikatselmointiopasta.

KORKEA TASO

Tietoturvatestien läpäisy (TST-009): Tietoturvatestien läpäisy tulee asettaa vaatimukseksi sovelluksen siirtymiselle vaiheesta toiseen elinkaaressaan. Esimerkiksi tietty kokoelma tietoturvatestitapauksia pitää läpäistä ennen sovellusjulkaisun tekemistä.

Sovelluskehityksen aikainen auditointi (TST-010): Korkean tason sovelluksen tietoturvallisuus on auditoitava myös sovelluskehityksen aikana, esimerkiksi eri tarkastuspisteiden yhteydessä. Näin varmistutaan siitä, että kriittiset tietoturvaongelmat havaitaan ja korjataan jo hyvissä ajoin ennen järjestelmän käyttöönottoa.

Koodikatselmoinnin hyväksytty suorittaminen (TST-011): Koodikatselmoinnin läpäisy tulee asettaa vaatimukseksi sovelluksen siirtymisessä vaiheesta toiseen elinkaaressaan. Siirtyminen seuraavaan elinkaaren vaiheeseen tehdään perustuen riskiarvioon, jolloin vähäiset tietoturvapuutteet sovelluksessa eivät välttämättä estä julkaisun tekemistä.

3.3.6 Käyttöönotto

Käyttöönotossa perustetaan sovelluksen tuotantoympäristö määritysten mukaisesti. Tuotanto- ja ylläpitovastaavat huolehtivat sovellusalustan ja sovelluksen asennuksessa tietoturvakovennuksien käyttöönotosta, tarvittavasta palomuurin konfiguroinnista sekä käyttöoikeuksista. Käyttöönotossa on huolehdittava erityisesti dokumentoinnista ja sovelluksen tuotantovaiheen riskien arvioinnista. Näillä toimilla varmistetaan, että ylläpito- ja poistovaiheissa toimitaan suunnitellusti ja turvallisesti.

PERUSTASO

Toimintaympäristön kuvaus (KTY-001): Toteutettavan sovelluksen odotettu toimintaympäristö kuvataan ja kuvausta ylläpidetään. Dokumentti kuvaa oletukset, joiden täytyy pitää paikkaansa sovelluksen oikean toiminnan varmistamiseksi, esimerkiksi:

- Prosessoriarkkitehtuuri
- OS versiot
- Tarvittavat sovellukset, kirjastot jne.
- Tarvittavat konfiguroinnit (käyttöjärjestelmä ja varusohjelmistot jne.).

Dokumentin katselmointi ja päivittäminen on vastuutettu ja organisoitu. Dokumenttia tulee päivittää säännöllisesti ja aina uusien julkaisuiden yhteydessä.

Sovelluksen tietoturva-asetukset (KTY-002): Sovelluksen asennuksen yhteydessä sovelluksen tietoturvallisuuteen vaikuttavat asetukset huomioidaan ja oletusasetukset vaihdetaan. Lisäksi sovelluksesta kirjoitetaan niin sanottu kovennusdokumentti, jossa kuvataan miten sovelluksen asetukset vaikuttavat tietoturvallisuuteen. Kovennuksessa ja dokumentaatiossa huomioitavia asioita ovat ainakin:

- Oletusarvoiset salasanat ja käyttäjätunnukset
- Hallintaliittymien näkyvyys
- Vianselvitysominaisuuksien poistaminen
- Mahdollinen testidata
- Salauksen aktivointi, organisaation itsensä allekirjoittamien varmenteiden (ns. self signed certificate) poisto ja luotettujen sertifikaattien myöntäjien varmenteiden käyttöönotto.
- Salaussertifikaattien elinkaaren seuranta ja uusien hankinta ennen voimassaolon päättymistä
- Tietoturvallisuuteen vaikuttavat sovellusasetukset ja niiden vaikutukset (ei liian laajoja suoritusoikeuksia sovelluksille).

Sovelluksen säilyttämä tieto (KTY-003): Sovelluksen käyttöönotossa tulee huomioida sovelluksen käsittelemän tiedon asettamat vaatimukset. Sovelluksen omistaja määrittelee käsitellyn tiedon suojaustason. Käyttöönoton vaatimat tietoturvallisuuteen liittyvät toimenpiteet on organisoitu ja vastuutettu.

Organisaation riskikartan päivitys (KTY-004): Sovelluksen aiheuttamat riskit organisaation toiminnalle tulee viimeistään tässä vaiheessa viedä osaksi orgnisaation laajuista riskienhallintaprosessia ja riskikarttaa.

KOROTETTU TASO

Asennusdokumentaatio (KTY-005): Sovelluksen asennuksesta on olemassa kirjallinen dokumentaatio, jossa kuvataan sovelluksen käsittelemän tiedon asettamat tietoturva-asetukset eri tasoilla. Lisäksi dokumentissa tulee kuvata tarvittavat toimenpiteet silloin, kun sovellus siirtyy ympäristöstä toiseen tai pois organisaation hallinnasta. Dokumentin ylläpito ja päivittäminen on organisoitu ja vastuutettu. Dokumentissa pitää kuvata ainakin seuraavat asiat:

- Sovelluksen sisältämä tieto (tietokannat jne.)
- Käytetyt tietoturvaratkaisut eri suojaustasoilla
- Tietokantojen, massamuistien tyhjennysprosessi.

3.3.7 Ylläpito

Tyypillinen sovellus on valtaosan elinkaarestaan ylläpitovaiheessa, jossa seurataan sovelluksen tietoturvallisuuden tasoa ja kapasiteetin riittävyyttä. Tietoturvallisuuden ja jatkuvuuden varmistaminen on siten erittäin merkittävässä roolissa. Sekä sovelluksen että sovellusalustan ajan tasalla olevat tietoturvapäivitykset, varmistukset, poikkeamien ja lokien hallinta sekä suunnitelmallinen muutoshallinta ovat ylläpidon tärkeimpiä tehtäviä.

PERUSTASO

Tietoturvapäivitykset (YLP-001): Kriittiset tietoturvapäivitykset tunnistetaan ja asennetaan. Kaikki sovellukset tarvitsevat suuren määrän ulkoisia komponentteja, kuten käyttöjärjestelmä, sovelluspalvelin, tietokannat, kirjastot jne. Näiden komponenttien tietoturvapäivitysten seuraaminen ja kriittisten päivitysten asentaminen tulee olla organisoitua ja vastuutettua.

Komponenttien elinkaaren seuranta (YLP-002): Sovelluksen käyttämien komponenttien elinkaarta on seurattava. Päivitysprosessi uuteen versioon siirtymiseksi on aloitettava hyvissä ajoin ennen tukiajan päättymistä.

Tietokannan muokkaaminen (YLP-003): Mikäli tuotannossa olevan sovelluksen tietokannassa säilyttämää tietoa joudutaan muokkaamaan ohi sovelluksen normaalin toiminnan, tulee menettely hyväksyttää sovelluksen omistajalla. Lisäksi operaatiosta tulee jäädä merkintä tietokannan lokiin.

Virhetilanteiden dokumentointi (YLP-004): Sovelluksen tyypillisimmät virhetilanteet ja tarvittavat toimenpiteet niiden ratkaisemiseksi tulee olla dokumentoituna. Jos mahdollisia virhetilanteita on paljon, tulee dokumentoitavat virhetilanteet priorisoida sen mukaan, mikä niiden vaikutus on liiketoiminnalle. Jokaisesta virhetilanteesta tulee kuvata:

- Käyttäjälle näytettävä virheviesti
- Kriittisyys ja seuraukset
- Toimintatapa korjaamiseksi
- Mitä tehdä jos korjaaminen ei onnistu?

Dokumentin katselmointi ja päivittäminen on vastuutettu ja organisoitu.

Sovelluksen päivittäminen (YLP-005): Sovelluksen tietoturvapäivitysten ja korjauksien asennus on dokumentoitu. Dokumentin katselmointi ja päivitys on organisoitu ja vastuutettu. Dokumentin pitää kuvata ainakin seuraavat asiat:

- Päivitysten toimittaminen, päivityssykli
- Kriittisten päivitysten toimittaminen
- Päivitysten asennusmenettely
- Varmuuskopiointi
- Varmuuskopioiden palauttaminen.

Päivitysten luokittelu (YLP-006): Organisaatiolla on suunnitellut periaatteet, joiden mukaan päätetään, millaiset tietoturvapoikkeamat luokitellaan kriittisiksi ja on siten korjattava välittömästi. Periaatteissa määritellään myös, miten tietoturvapuutteet luokitellaan riskianalyysin mukaan. Organisaatio on vastuuttanut tietoturvapäivitystarpeen seurannan, korjausten toteutuksen ja asentamisen.

Tietoturvapuutteista raportointi (YLP-007): Organisaatio tarjoaa asiakkaalle ja muille sidosryhmille keinon raportoida vakavista tietoturvapuutteista ja haavoittuvuuksista. Kontaktipiste tiedotetaan sopimuksissa ja esimerkiksi organisaation verkkosivuilla. Organisaatio on vastuuttanut tietoturvaraporttien käsittelyn, jolloin jokaiselle raportille määritellään omistaja joka on vastuussa seuraavista asioista:

- Poikkeamien käsittely
- Ensivastine, vahingon minimointi
- Poikkeaman selvittäminen
- Raportointi johdolle ja sidosryhmille.

Raportoituihin vakaviin puutteisiin reagoidaan ja korjaus toteutetaan ilman tarpeetonta viivyttelyä. Vakavista poikkeamista pidetään kirjaa ja organisaation johtoa tiedotetaan niistä.

Sovelluksen varmuuskopiointi (YLP-008): Ainakin sovelluksen käsittelemät tiedot ja sovelluksen konfiguraatiot on varmuuskopioitava säännöllisesti. Varmistusväli riippuu muun muassa sovelluksen sisältämän tiedon luokittelusta, sovelluksen kriittisyydestä jne. Varmistus pitää tehdä sovelluksesta riippumattomalle järjestelmälle, magneettinauhalle tai varmistuslevyjärjestelmälle. Tällöin sovelluksen vioittuminen ei vaaranna varmistusten saatavuutta. Varmistusten palautusmenettely pitää kuvata järjestelmän toipumissuunnitelmassa. Varmuuskopioista syntyy kirjallinen raportti, joista järjestelmän omistaja tai

muu vastaava taho tarkistaa varmistuksen onnistumisen. Varmistuksia on säilytettävä eri palotilassa, kuin varsinaisia sovelluksen tietoja.

Sovelluksesta tulee kirjoittaa dokumentti, jossa kuvataan mitkä tiedot sovelluksesta tulee vähintään varmistaa. Dokumentissa kuvataan myös varmuuskopiointimenettely. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu.

Lisenssien hallinta (YLP-009): Sovelluksen käyttämien kolmansien osapuolten lisenssit ja vastaavat ovat ajan tasalla. Lisenssien ajantasaisuutta seurataan.

KOROTETTU TASO

Päivitysprosessi (YLP-010): Organisaatiolla on sovelluksen toimintaympäristöön kohdistuva päivitysten hallintaprosessi. Prosessi on dokumentoitu ja dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu. Sisältönä esimerkiksi:

- Tavoiteajat eri vakavuusluokan päivitysten asentamiselle
- Huoltoikkunoiden määrittelyt
- Roolit ja vastuualueet
- Testiympäristön käyttö
- Asennusprosessin kuvaus, miten toimia jos asennus ei onnistu (rollback-prosessi).

Asetusten auditointi (YLP-011): Sovellusympäristön tietoturvallisuuteen vaikuttavat asetukset tarkastetaan säännöllisesti. Havaittujen poikkeamien korjaaminen vastuutetaan sekä korjaamisen onnistumista seurataan. Auditoinnissa tarkastetaan muun muassa seuraavat asiat:

- Käyttöjärjestelmien ja varusohjelmistojen tietoturvapäivitysten tilanne
- Käyttäjätunnukset ja salasanat
- Pääsy luottamukselliseen tietoon tiedostojärjestelmätasolla
- Lokiasetukset käyttöjärjestelmätasolla.

Ohjeena auditoinnissa voidaan käyttää esimerkiksi CIS:n standardeja.

Tietoturvapoikkeamien käsittelyprosessi (YLP-012): Tietoturvapoikkeamien käsittelyprosessi on dokumentoitu. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu. Prosessi voi ottaa kantaa esimerkiksi seuraaviin asioihin:

- Henkilöt ja vastuualueet
- Vahingon minimointi (triage)
- Selvittäminen (forensics)
- Tiedottaminen johdolle ja organisaation sisällä
- Raportointi sidosryhmille.

Tietoturvapoikkeamista tiedottaminen (YLP-013): Joissain tilanteessa voi olla tarpeen tiedottaa tietoturvapoikkeamista julkisesti. Tällöin organisaation tulee kehittää ja dokumentoida tiedottamisprosessi. Dokumentin katselmointi ja päivittäminen tulee organisoida ja vastuuttaa. Tiedottaminen voi olla tarpeellista esimerkiksi:

- Jos kehitettyä sovellusta käytetään organisaation ulkopuolella, tai asiakkaisiin ei ole suoraa kontaktia (esimerkiksi COTS-ratkaisut)
- Jos lait, asetukset tai muut määräykset vaativat tiedottamista (esimerkiksi henkilötiedot).

Dokumentoitu raportoitiprosessi (YLP-014): Korotetun tason sovelluksilla tietoturvapoikkeamien raportointimenettelyn on oltava dokumentoitu. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu. Lisäksi tietoturvapoikkeamaraportille tulee olla ennalta määritelty dokumenttipohja. Pohjan tulee sisältää ainakin seuraavat asiat:

- Raportoivan henkilön yhteystiedot
- Poikkeaman yhteenveto
- Poikkeaman ja raportoinnin aikajana
- Poikkeaman tekniset yksityiskohdat: tikettinumero, tehdyt muutokset, poikkeaman toistamisen askeleet
- Yhteenveto; poikkeaman syy, vaikutus, seuraukset.

Jälkikäteisanalyysi (YLP-015): Sovelluksessa havaitut tietoturvapoikkeamat ja -puutteet analysoidaan jälkikäteen kun korjaus on toteutettu ja toimitettu. Analyysissä pyritään selvittämään puutteen juurisyy ja määrittelemään korjaavat toimenpiteet. Toteutus- ja toimitusprosessia korjataan tarvittaessa samanlaisten ongelmien välttämiseksi tulevaisuudessa.

Muutoshallinta (YLP-016): Sovelluksen päivitys- ja muutosperiaatteet on dokumentoitu. Dokumentin katselmointi ja päivittäminen on vastuutettu. Dokumentissa tulee kuvata ainakin:

- Roolit ja vastuuhenkilöt
- Muutosten luokittelu
- Eri muutosluokkien vaatimat toimenpiteet (esimerkiksi ympäristö, lokitus, versionhallinta)
- Muutosprosessin yksityiskohtainen kuvaus.

Lokien seuranta (YLP-017): Sovelluksen tuottamaa lokia tarkkaillaan aktiivisesti joko automaattisella lokienhallintaohjelmistolla tai manuaalisesti. Lokien aktiivisella tarkkailulla väärinkäytökset tai hyökkäykset on mahdollista havaita jo niiden aikana. Lokien tarkkailun perusteella muodostetaan tietoturvallisuuden kokonaistilannekuvaa. Lisäksi lokien tarkkailun tuloksia käytetään toiminnan kehittämiseen, kuten uusien tietoturvaominaisuuksien suunnitteluun tai olemassa olevien parantamiseen.

Kirjallinen varmuuskopiontipolitiikka (YLP-018): Sovelluksesta on kirjallinen varmuuskopiointipolitiikka ja -prosessi. Dokumenttien kirjoittamisessa on otettu huomioon sovelluksen käsittelemän tiedon asettamat vaatimukset sekä sovelluksen toimintaympä-

ristön erityisvaatimukset. Dokumentaatiossa on huomioitu myös fyysisten varmuuskopioiden säilyttäminen, siirto ja tuhoaminen. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu.

Suojakopiot (YLP-019): Korotetun tason sovelluksesta on otettava edellä mainittujen varmuuskopiointivaatimusten lisäksi suojakopiot. Suojakopiot sisältävät sovelluksen datan lisäksi asennettavat sovellus- ja käyttöjärjestelmämediat, asennusohjeet jne. Suojakopioita säilytetään varmuuskopioista erillään erillisessä palotilassa, jotta niitä voidaan käyttää järjestelmän palauttamiseen jos varmuuskopioita ei jostain syystä voida käyttää.

KORKEA TASO

Verkkopohjainen turvamekanismi (YLP-020): Tuotantoympäristössä tulee olla käytössä mekanismi, jolla voidaan reagoida nopeasti yllättäviin tietoturvatilanteisiin ja estää siten hyökkäys. Tällainen mekanismi voidaan rakentaa esimerkiksi sovelluspalomuurilla.

Palautusten testaaminen (YLP-021): Korkean tason sovelluksen varmuuskopioiden palauttamista tulee testata ja harjoitella säännöllisesti. Testauksessa saadaan usein selville palautusprosessin ongelmia, joita ei ole osattu ennustaa prosessia suunniteltaessa.

Yhteenveto poikkeamista (YLP-022): Kaikista havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto. Yhteenvedosta havaittavia trendejä käytetään pohjana organisaation tietoturvatyön kehittämiselle sekä prosessien, strategian ja toimintatapojen kehittämiselle.

Päivitysten seuraaminen (YLP-023): Sovelluksen tietoturvapäivitysten onnistumista ja päivitysten ajantasaisuutta seurataan. Seurannan tuloksia käytetään pohjana päivitys- ja korjausprosessin kehittämiselle.

Palautusten tilastointi (YLP-024): Korkean tason sovelluksesta tulee tilastoida palautettujen tietojen määrää sekä palautuksen syitä. Tilastoja tulee käyttää toiminnan parantamiseen ja puutteiden korjaamiseen. Lisäksi palautustilastojen antamaa informaatiota voidaan käyttää pohjana sovelluskehitysprosessin parantamiselle.

3.3.8 Käytöstä poisto

Ylläpitovaiheessa on huolehdittu poistettavan palvelun korvaavista menettelyistä ja mahdollisista tietoaineistojen siirroista. Järjestelmän käytöstä poistossa merkittävin haaste on järjestelmän sisältämän tiedon käsittely ja säilytys tietoaineiston luokitusten ja arkistointivaatimusten mukaisesti. Poistuvien järjestelmien osalta huolehditaan kaikkien dokumenttien ajantasaisuudesta.

PERUSTASO

Tiedon arvon määrittely (KTP-001): Sovelluksen sisältämälle tiedolle tulee tehdä arvonmääritys, jonka perusteella päätetään säilytetäänkö sovelluksen tietoa sen käytöstä poiston jälkeen.

Tiedon tuhoaminen (KTP-002): Käytöstä poistettavan sovelluksen tieto, jota ei säilytetä pysyvästi, on tuhottava tietoturvallisesti.

Tiedon konvertointi (KTP-003): Säilytettävä tieto on konvertoitava muotoon, jota pystytään lukemaan myös tulevaisuudessa.

Säilytettävän tiedon luokittelu (KPT-004): Salassa pidettävä tieto tulee luokitella perusteluineen, jotta tietoa osataan käsitellä oikein passiivisessa arkistossa.

4 Erityiskysymyksiä

4.1 Tekijänoikeudet

Sovelluskehitysprojektien lopputuotosten tekijänoikeudet kuuluvat sille organisaatiolle, jonka työntekijä tai virkamies on sovelluksen lähdekoodin kirjoittanut. Hankittaessa sovelluksia tai ohjelmointityötä oman organisaation ulkopuolelta, on huolehdittava tarvittavien oikeuksien siirrosta tilaavalle organisaatiolle.

Ei ole yksiselitteistä sääntöä siitä, kenelle tekijänoikeudet jäävät sovelluksen valmistuttua. Tämän vuoksi on erittäin tärkeää sopia tästä jo sopimusneuvotteluvaiheessa. Valmisohjelmistojen tapauksessa oikeudet ovat useimmiten sovelluksen kehittäjällä ja kehittäjä myy samaa sovellusta myös muille asiakkaille. Räätälöidyt sovellukset ovat harmaalla alueella; alustan oikeudet voivat kuulua kehittäjälle, mutta varsinaiset räätälöinnit ostajalle. Kehitettäessä täysin omaa sovellusta esimerkiksi hankkimalla ohjelmointia konsultointityönä oikeuksien jäämisestä hankkijalle on sovittava.

Mikäli sovellusta kehitetään ainoastaan hankkivan organisaation tarpeisiin, tulee sopimusneuvottelussa lähtökohtana ja tavoitteena olla, että tekijänoikeudet ja lähdekoodi jäävät tilaavalle organisaatiolle toimitusprojektin päättyessä. Tällöin on myös usein syytä käyttää hankkijan omaa versionhallintaa. Näin hankkijalle jää myös täydellinen historiatieto sovelluksen kehittämisestä sen nykyiseen muotoon. Silloin sovelluksen jatkokehitys tai kehityksen siirtäminen toiselle toimittajalle on merkittävästi helpompaa.

Sovelluskehitysprojektissa voidaan sopia myös turvatalletuksen käyttämisestä (escrow). Tässä palvelussa sovelluksen lähdekoodi luovutetaan luotetulle kolmannelle osapuolelle, joka huolehtii sen luovuttamisesta tilaajalle, mikäli toimittaja ajautuu esimerkiksi konkurssiin tai ei voi muusta syystä luovuttaa lähdekoodia tilaajalle.

4.2 Avoimien tietoverkkojen sovellusten tietoturvallisuuden erityispiirteitä

Internetiin avoinna olevien palveluiden tietoturvallisuuden suunnitteluprosessissa ei ole merkittävää eroa. Myös sisäverkon palveluiden tietoturvallisuus tulee suunnitella käsitellyn tiedon ja sovelluksen kriittisyyden asettamien vaatimusten mukaisesti, vaikka niihin ei pysty ottamaan suoraan yhteyttä Internetin kautta.

Internetin yli käytettävän sovelluksen asettamat lisähaasteet tietoturvallisuudelle ovat:

- Käyttäjän tunnistamisen vaatimukset saattavat olla tiukempia, esimerkiksi vahvaa tunnistamista käytetään harvoin sisäverkon sovelluksissa.
- Internetin yli käytettävä sovellus on alttiimpi tietyn tyyppisille hyökkäyksille, kuten palvelunestohyökkäyksille.

On kuitenkin huomattava, että raja sisä- ja ulkoverkon sovellusten välillä on hämärtynyt huomattavasti viime aikoina erilaisten etäkäyttöratkaisuiden ja tietoturvahyökkäysten kehityksen myötä. Sovelluksen pääsyn rajoitteita ei siis voi pitää riittävänä tietoturvamekanismina, vaan tietoturvaominaisuudet on syytä suunnitella siitä lähtökohdasta, että hyökkääjällä on aina rajoittamaton pääsy sovelluksen käyttäjärajapintoihin.

Tarkemmin Internetin käytön suosituksista kerrotaan Valtion tietohallinnon Internet-tietoturvallisuusohjeessa (VAHTI 1/2003).

5 Säädösperusta ja muut ohjeet

Viranomaisten on toteutettava tietoturvallisuus ympäristössä, jossa pääsääntönä on asiakirjan tai sitä vastaavan tietojoukon julkisuus. Viranomaisten asiakirjat ovat julkisia, jollei laissa erikseen toisin säädetä. Ne tiedot, joiden paljastuminen vaarantaisi keskeisten yksityisten tai julkisten etujen toteutumisen, on pidettävä salassa ja niiden suojaamisesta on huolehdittava asianmukaisesti. Päätöksenteossa tarvittavan tiedon tulee myös olla viranomaisen käytettävissä. Eri osapuolten oikeusturvan kannalta on tärkeää, että nämä tiedot ovat samalla oikeita ja asianmukaisia.

Vaikka lopullisen asiakirjan julkisuus on pääsääntö, tulee sovelluskehityksessä ottaa huomioon, että julkisuusaste ja asiakirjan luottamuksellisuuden taso saattavat vaihdella asiakirjan elinkaaren eri vaiheissa.

Keskeinen julkisuutta ja tietojen suojaamista koskeva säädös on **Laki viranomaisten toiminnan julkisuudesta** (JulkL 621/1999) ja siihen liittyvä **Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (**JulkA 1030/1999). Laki asettaa viranomaisille velvoitteen suojata tietojärjestelmänsä. Toinen julkisuuslain perusteella annettu asetus on **Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa** (681/2010). Se on keskeisin viranomaisten tietoturvatyötä ohjaava säädös. Ohjeessa tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010) ohjeistetaan tarkemmin kyseisen asetuksen toteuttamisesta. Asetus tuli voimaan 1.10.2010 ja siinä edellytetyn tietoturvallisuuden perustason siirtymäaika jatkuu 30.9.2013 asti.

Henkilörekistereihin talletettujen tietojen käsittelyä säädellään **Henkilötietolailla (523/1999)**. Sen 32 §:ssä säädetään henkilötietojen suojaamisesta seuraavasti: "Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta".

Tiedon saatavuuden näkökulmasta olennainen säädös on **Laki julkisen hallinnon tietohallinnon ohjauksesta** (634/2011). Lain tarkoitus on parantaa julkisten palveluiden saatavuutta säätämällä julkisen hallinnon tietohallinnon ohjauksesta ja tietojärjestelmien yhteentoimivuuden edistämisestä ja varmistamisesta.

EU-asioissa noudatetaan luokiteltujen tietojen käsittelyn osalta neuvoston päätöstä turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi 31.3.2011 (2011/292/EU). Lisäksi noudatetaan kansallisen turvallisuusviranomaisen (ulkoasianministeriö) ohjetta: Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje 30.11.2010.

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on vaatimusluettelo, jota viranomaiset voivat käyttää auditointien tai sisäisen laadunvarmistuksen pohjana. Kansainvälisiä luokiteltuja tietoaineistoja sisältäville tietojärjestelmille auditointi on pakollinen, kansallisille mahdollinen.

Keskeiset kansalliset tietoturvallisuuden normit, jotka ovat olleet tämän ohjeen perustana ovat seuraavat:

- KATAKRI II – Kansallinen turvallisuusauditointikriteeristö, versio 2
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Henkilötietolaki (523/1999).
- Laki julkisen hallinnon tietohallinnon ohjauksesta (634/2011)
- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010)
- Lokiohje (VAHTI 3/2009)
- Sisäverkko-ohje (VAHTI 3/2010)
- ICT-hankintojen tietoturvaohje (VAHTI 3/2011)
- ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin (VAHTI 2/2009)
- Valtiohallinnon keskeisten tietojärjestelmien turvaaminen (VAHTI 5/2004)
- Teknisen ympäristön tietoturvataso-ohje (VAHTI 3/2012)
- JHS-suositukset, erityisesti JHS 171 ICT-palvelujen kehittäminen: Kehittämiskohteiden tunnistaminen

Valtiokonttori on julkaissut tietoturvallisuuden työkalupakin valtionhallinnon organisaatioiden tietoturvatyön tueksi. Työkalupakin käyttöoikeudet myöntää Valtion IT-palvelukeskus, lisätietoja löytyy Valtiokonttorin www-sivuilta.

Liite 1 – Sovelluskehityksen vaatimustaulukko

Tässä ohjeessa esitetyt vaatimukset ovat saatavilla myös taulukkomuodossa. Vaatimustekstien lisäksi taulukkoon on merkitty myös vaatimuksen pakollisuusaste sekä suositus siitä tuleeko vaatimus sisällyttää tarjouspyyntöön vai ei.

Liite 2 – Lähdemateriaalin vaatimukset

Lähdemateriaalin vaatimukset ovat muissa ohjeissa ja vaatimuskokonaisuuksissa esiintyviä vaatimuksia, jotka liittyvät sovelluskehityksen tietoturvallisuuteen ja jotka on huomioitu tämän ohjeen vaatimusten laadinnassa. Keskeisimmät lähteet on listattu luvussa 5.

Liite 3 – Voimassaolevat VAHTI -julkaisut

LIITE 1. Sovelluskehityksen vaatimustaulukko

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
1. Strategia ja resursointi	STR-001	"Vastuuhenkilöt ja -roolit"	Organisaation tulee kartoittaa ja tunnistaa sovelluskehityksen tietoturvallisuuden kannalta merkittävät roolit ja niistä vastuussa olevat henkilöt. Henkilöiden työajasta on varattava riittävästi aikaa myös tietoturvatehtäviin. Tällaisia rooleja ovat esimerkiksi: • Arkkitehdit ja projektipäälliköt • Sovelluskehitykseen käytetyn kehitysympäristön omistajat ja ylläpitäjät. Kehitysympäristöön kuuluvat muun muassa versionhallinta, testiympäristöt, jaetut työtilat jne. • Kehitettävän sovelluksen omistaja • Testauspäällikkö. Eri rooleissa toimivien henkilöiden tulee tiedostaa myös oman alueensa tietoturvavastuut ja heidän tulee seurata vastuualueidensa tietoturvaongelmia ja niiden mahdollista toteutumista. Tunnistetuille henkilöille tulee määritellä varahenkilöt. Lisäksi varahenkilöt tulee kouluttaa tehtäviinsä, jotta he pystyvät tarvittaessa toimimaan varahenkilöinä tehokkaasti.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	1.3.2.1	Kyllä
	STR-002	Tietoturvastrategia	Organisaation tulee suunnitella strategia, jossa määritellään tietoturvatyön vastuualueet sekä organisaation tietoturvallisuudesta vastuullisten roolit. Tietoturvastrategian tulee olla organisaation ydintoiminnan ja -tavoitteiden mukainen sekä tukea asetettujen tavoitteiden saavuttamista. Strategia ei saa muodostua ydintoiminnasta irralliseksi. Strategian suunnittelussa on otettava huomioon ainakin seuraavat asiat: • Tietoturvastrategian tulee olla linjassa ja tukea organisaation liiketoimintasuunnitelman, ydintoimintojen, kasvusuunnitelmien jne. kanssa • Suunnittelussa tulee olla mukana edustajia kaikista organisaation sidosryhmistä, kuten eri liiketoiminta-alueiden vastaavat, IT-toiminnasta vastaavat, henkilöstöasiat (HR), lakiyksikkö jne. (riippuen toimintaympäristöstä) • Suunnittelussa otetaan huomioon liiketoimintariskit, jotta tietoturvatyö voidaan kohdistaa liiketoiminnan kannalta tärkeimpiin kohteisiin • Tulee ottaa huomioon organisaation toimintaan vaikuttavat lait ja asetukset sekä muut sitoumukset. Dokumentissa käsitellään seuraavia asioita: • Pitkän ja keskipitkän tähtäimen tietoturvastrategia, tavoitteet ja mittarit tavoitteiden saavuttamiselle • Strategian hyödyt liiketoiminnalle • Implementointisuunnitelma, aikataulut, vastuuhenkilöt, tarkastuspisteet (milestone) jne. • Organisaation ylimmän johdon sitoutumiskirje (commitment letter).	Suositus	Pakollinen vaatimus	Pakollinen vaatimus	1.1.1.4	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
2. Politiikat	POL-001	Tietoturvapolitiikka	Organisaatiolla tulee olla kirjallinen tietoturvapolitiikka, jossa määritellään tietoturvatyön keskeiset tavoitteet, vastuut ja periaatteet. Politiikan tulee olla organisaation johdon hyväksymä. Politiikkaa voidaan käyttää pohjana tietoturvastrategian määrittelylle. Politiikan päivittäminen ja katselmointi on organisoitu ja vastuutettu.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	1.1.1.3	Kyllä
	POL-002	Turvallisuusselvitykset	Organisaatio on kartoittanut ja määritellyt ne roolit, joiden haltijoista tulee tehdä turvallisuusselvitys. Turvallisuusselvitysprosessi on dokumentoitu ja sitä noudatetaan selvityksiä tehtäessä. Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	1.3.2.6	Tarvittaessa
	POL-003	Tietojärjestelmien omistajat	Kaikille organisaation tietojärjestelmille on määritelty omistaja, joka vastaa kyseisen järjestelmän käytöstä. Tietojärjestelmiin saa asentaa vain järjestelmän omistajan hyväksymiä laitteita tai ohjelmistoja.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.2.4	Ei
	POL-004	Tietoturvapolitiikan päivitys	Organisaation tietoturvapolitiikkaa ja muita tietoturvallisuuteen liittyviä politiikkoja (kuten lokipolitiikka) katselmoidaan ja tarvittaessa päivitetään vähintään vuosittain. Politiikan katselmoinnille ja päivittämiselle on myös olemassa prosessi ja vastuuhenkilöt.	Suositus	Suositus	Pakollinen vaatimus		Ei
	POL-005	Lokipolitiikka	Organisaatio on määritellyt kirjallisen lokipolitiikan. Politiikka määrittelee vaatimukset kehitettävien sovellusten lokien keräys- ja seurantakäytännöille sekä sille mitkä olosuhteet aiheuttavat hälytyksiä. Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.		Suositus	Vahva suositus		Ei
	POL-006	Käyttövaltuus-politiikka	Organisaatiolla on kirjallinen käyttövaltuuspolitiikka, joka määrittelee muun muassa seuraavat asiat: • Kenellä on oikeus myöntää oikeuksia järjestelmiin • Oikeuksien myöntöperusteet • Oikeuksien myöntövaatimukset • Oikeuksien poistoperusteet • Salasanakäytännöt jne. Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.	Vahva suositus	Pakollinen	Pakollinen	2.7.6	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
3. Riskien-hallinta	RSK-001	Organisaation kokonaisriskianalyysi	Organisaation tulee tehdä säännöllisesti riskien analysointia ja hallintaa, ja sen yhteydessä tulee käsitellä myös tietoturvallisuuteen liittyviä riskejä. Riskienhallintaprosessiin tulee kuulua myös tunnistettujen riskien hallintakeinojen määrittely sekä tehtyjen toimenpiteiden onnistumisen seuraaminen. Riskien tunnistamiseen osallistuvat liiketoiminta-alueiden omistajat sekä muut sidosryhmät. Riskien tunnistamisen tarkoituksena on kerätä lista pahimmista mahdollisista uhkakuvista organisaation liiketoiminta-alueiden toiminnalle ja tietovarannoille. Riskit vaihtelevat toimialueittain, mutta tyypillisiä sovelluksiin liittyviä riskejä ovat: • Tietovuodot • Immateriaalioikeuksien rikkomukset (ns. Intellectual Property Rights -rikkomukset) • Palvelukatkokset • Varmuuskopioiden riittämätön testaus • Ulkoistettujen palveluiden epäselvät vastuut • Taloudelliset tappiot • Identiteettivarkaudet. Riskienhallintaprosessin tuotoksesta tunnistetaan ydintoiminnalle merkittävimmät riskit. Riskit priorisoidaan esimerkiksi arvioimalla riskin toteutumisen vaikutus, todennäköisyys ja riskin hallinnan taso. Merkittävimmistä riskeistä kirjoitetaan tarkemmat kuvaukset sekä kaikki mahdolliset riskin lievennys- tai ehkäisykeinot. Riskit arvioidaan uudelleen säännöllisesti tai organisaation riskiprofiilin muuttuessa merkittävästi. Arvioinnin yhteydessä tarkastetaan myös riskienhallintatoimenpiteiden onnistuminen.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	1.2.3.1	Ei
	RSK-002	Riskienhallinta-prosessi	Organisaation riskienhallintaprosessi tulee olla kuvattuna kirjallisesti esimerkiksi organisaation riskienhallintapolitiikassa. Prosessin pitää sisältää vähintään seuraavat asiat: • Riskien tunnistaminen ja arviointi • Riskien torjunnan suunnittelu ja tarvittavat toimenpiteet • Toiminnan suunnittelu riskin realisoituessa • Riskienhallintakeinojen kuvaus: välttäminen, pienentäminen, siirtäminen, hyväksyminen, varautuminen. Dokumentaatiota tulee myös ylläpitää ja päivittää säännöllisesti sekä organisaation riskiprofiilin muutosten yhteydessä. Dokumentin päivittäminen ja katselmointi on organisoitu ja vastuutettu.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus	1.2.3.3	Ei
	RSK-003	Riskienhallintaprosessin päivittäminen	Organisaation riskienhallintaprosessin tulee ottaa huomioon suuret muutokset organisaation toiminnassa, toimintaympäristössä jne. Tällöin tietoturvariskien arviointi tulee suorittaa uudelleen.	Suositus	Pakollinen vaatimus	Pakollinen vaatimus	1.2.3.6	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
4. Osaaminen ja koulutus	OSK-001	Tietoturvakoulutus	Sovelluskehityksestä vastuussa oleville tulee järjestää tietoturvakoulutusta, ns. tietoisuuskoulutusta (awareness training). Koulutuksessa käydään läpi organisaation toteuttamien sovellusten tyypillisiä tietoturvaongelmia. Näin varmistutaan siitä, että kaikki organisaation henkilöt omaavat riittävät taidot rooliinsa kuuluvan tietoturvatyön hoitamiseksi. Tietoturvakoulutus tulee uusia säännöllisesti, vähintään kerran vuodessa. Koulutuksessa on suositeltavaa esitellä toteutettavien sovellusten tyypillisiä tietoturvaongelmia ja sovelluskehityksen menetelmiä niiden estämiseksi. Koulutus voidaan järjestää esimerkiksi 1-2 päivän koulutussessioina tai verkkokoulutuksena. Koulutuksen kattavuus riippuu esimerkiksi siitä, miten paljon tekninen ympäristö on muuttunut edellisen koulutuksen jälkeen sekä miten paljon uusia sovelluskehityksestä vastaavia henkilöitä organisaatioon on tullut. Erityisen tarpeellinen koulutus on uusille sovelluskehittäjille. Tyypillisiä sovelluskehityksestä vastuussa olevia rooleja ovat: • Sovelluksen toteutuksesta vastuussa olevat • Projektipäälliköt • Sovellusarkkitehdit • Sovelluksen määrittelijät, suunnittelijat ja toteuttajat • Sovelluksen testaamisesta vastuussa olevat.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	1.3.1.2	Kyllä
	OSK-002	Tietoturvaohjeistus	Osana organisaation perehdyttämisprosessia uusille työntekijöille järjestetään tietoturvakoulutus, jossa työntekijälle esitetään organisaation tietoturvasäännöt ja hänet perehdytetään organisaation tietoturvatoimintaan ja -tavoitteisiin. Perehdytyksen tueksi on laadittu kirjallinen ohje, joka sisältää tarkistuslistan läpikäytävistä asioista. Näin varmistutaan siitä, että tärkeiksi koetut tietoturva-asiat saadaan koulutettua uusille henkilöille heti työsuhteen alkaessa. Koulutuksessa tulee muun muassa kertoa taho (kuten tietoturvaryhmä), jolta saa tarvittaessa apua tietoturvaongelmien ratkaisemisessa. Perehdytys voidaan järjestää luokkaopetuksena, verkkokoulutuksena tai muulla soveltuvalla tavalla.	Suositus	Vahva suositus	Pakollinen vaatimus		Ei
	OSK-003	Tietoturvaperehdytys	Osana organisaation perehdyttämisprosessia uusille työntekijöille järjestetään tietoturvakoulutus, jossa työntekijälle esitetään organisaation tietoturvasäännöt sekä hänet perehdytetään organisaation tietoturvatoimintaan ja -tavoitteisiin. Koulutuksen tueksi on laadittu kirjallinen ohje, joka sisältää tarkistuslistan läpikäytävistä asioista. Näin varmistutaan siitä, että tärkeiksi koetut tietoturva-asiat saadaan koulutettua uusille henkilöille heti työsuhteen alkaessa. Koulutuksessa tulee muun muassa kertoa taho (kuten tietoturvaryhmä), jolta saa tarvittaessa apua tietoturvaongelmien ratkaisemisessa. Koulutus voidaan järjestää luokkaopetuksena, verkkokoulutuksena tai muulla soveltuvalla tavalla.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	1.3.1.3	Tarvittaessa
	OSK-004	Tietoturvasääntöjen noudattaminen	Organisaation tietoturvasääntöjen noudattamista seurataan ja poikkeamiin puututaan. Sisäisellä tiedottamisella varmistutaan siitä, että työntekijät ymmärtävät sääntöjen rikkomisen seuraukset.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	1.3.1.5	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	OSK-005	Security Coach	Organisaatiolla tulee olla ainakin yksi sovelluskehityksen tietoturvallisuuteen perehtynyt henkilö (ns. security coach), joka tarjoaa tarvittaessa teknistä tietoturvakonsultaatiota projektitiimeille ja on tarvittaessa vastuussa tietoturvakoulutuksesta. Henkilö voi olla joko organisaation työntekijä tai ulkoinen resurssi, kyseessä ei välttämättä ole kokopäiväinen rooli. Valmentajan olemassaolo tulee tiedottaa organisaation sisällä. Valmentajan osaamisesta varmistutaan riittävällä koulutuksella. Sovelluskehityksen tietoturvavastuut on mainittu henkilön toimenkuvassa ja hänelle annetaan aikaa vastuiden suorittamiseen. Valmentajan roolissa olevien henkilöiden tulee olla aktiivisesti yhteydessä arkkitehtuurin kehittämisestä vastaaviin henkilöihin sekä käytännön sovelluskehitystä tekeviin henkilöihin.		Suositus	Vahva suositus		Ei
	OSK-006	Sovelluskehityksen tietoturvakoulutus	Sovelluskehityksestä vastuussa oleville järjestetään räätälöityä koulutusta. Järjestettävän koulutuksen tulee olla roolikohtaista ja ottaa huomioon roolin asettamat tietoturvahaasteet. Esimerkkisisältöjä: • Testaajat: tietoturvahaavoittuvuuksien testausmenetelmät, työkalujen esittely • Toteuttajat: käytettyjen teknologioiden tyypilliset tietoturvaongelmat, turvallinen Java/.NET-ohjelmointi. • Sovelluksen omistaja: käytetty sovelluskehitysprosessi ja tietoturvallisuuden huomioiminen sen eri vaiheissa.		Vahva suositus	Pakollinen vaatimus		Tarvittaessa
	OSK-007	Koulutuksen ajantasaisuus	Organisaation tietoturvallisuuden koulutussuunnitelma tulee kuvata kirjallisesti. Organisaatio järjestää myös säännöllisiä koulutuksia ajankohtaisista tai tärkeistä tietoturva-asioista. Henkilöstön osallistumista koulutuksiin seurataan. Henkilöstön osaamistaso mitataan koulutuksen päätteeksi. Mittaamisen tarkoituksena ei ole seurata yksilöiden osaamistasoa, vaan kerätä informaatiota organisaation tietoturvaosaamisesta kokonaisuutena. Koulutussuunnitelman päivittäminen ja katselmointi on organisoitu ja vastuutettu.		Pakollinen vaatimus	Pakollinen vaatimus	1.3.1.8	Ei
	OSK-008	Toimintaympäristön muutosten vaikutus koulutukseen	Koulutuksen tulee ottaa huomioon myös organisaation toimintaympäristössä tapahtuneet äkilliset muutokset. Organisaatiolla tulee olla valmius järjestää nopealla aikataululla koulutus- tai tiedotustilaisuuksia, mikäli organisaation toimintaympäristössä tapahtuu muutoksia, jotka vaikuttavat merkittävästi organisaation tietoturvallisuuden tilaan. Esimerkkinä tällaisesta tilanteesta on organisaatioon kohdistuva massiivinen tietojenkalasteluhyökkäys.		Vahva suositus	Pakollinen vaatimus	1.3.1.12	Ei
5. Tekninen sovelluskehitysympäristö	TSK-001	Arkkitehtuuri- ja sovelluskehitysohjeistus	Organisaatiolla tulee olla arkkitehtuuri- ja sovelluskehitysohjeistus, jossa määritellään sovelluskehitystä ohjaavat periaatteet. Tyypillisiä periaatteita ovat: • Turvalliset oletusarvot (secure default) • Monikerroksinen suojaaminen (defense in depth) • Heikoimman alueen suojaaminen (securing the weakest link) • Virhetilanteiden käsittely tietoturvallisesti (secure failure) • Matalimmat mahdolliset oikeudet (least privilege) • Tehtävien eriyttäminen (separation of duties) • Tietoturvamekanismien salassa pysymiseen ei saa luottaa (security by obscurity).	Suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	Viite ohjeeseen	Vaatimuskohde	Kuvaus	Perustaso	Korotettu taso	Korkea taso	Vahti 2/2010	Tarjous-pyyntöön
	TSK-002	Teknisten tietoturva-ratkaisujen määritys	Organisaation tulee määritellä yhteisesti hyväksytyt tekniset tietoturvaratkaisut. Tietoturvaratkaisut liittyvät muun muassa seuraaviin osa-alueisiin: • Todentaminen (authentication) • Valtuuttaminen (authorization) • Käyttäjän syötteen validointi (input validation) • Sovelluksen tuotteen turvallinen enkoodaus (output encoding) • Virheenkäsittely • Lokien keräys.	Suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa
	TSK-003	Komponenttikirjaston käyttö	Käytetyistä komponenteista tulee muodostaa organisaation paikallinen komponenttikirjasto. Vain komponenttikirjastossa olevia komponentteja tulee käyttää sovelluksissa. Komponenttikirjaston päivitystarvetta tulee seurata aktiivisesti ja eri sovelluksissa käytetyistä versioista tulee pitää kirjaa.	Suositus	Vahva suositus	Pakollinen vaatimus		Ei
	TSK-004	Eriytetyt ympäristöt	Kehitys-, testi-, ja tuotantoympäristöt tulee eriyttää toisistaan. Organisaation tulee määritellä menettely, jota seurataan siirrettäessä sovellusta ympäristöstä toiseen.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	TSK-005	Versionhallinta	Organisaation tulee käyttää lähdekoodin säilytykseen soveltuvaa versionhallintajärjestelmää. Järjestelmää tulee käyttää henkilökohtaisin tunnuksin siten, että jokainen muutos lähdekoodiin voidaan jäljittää muutoksen tehneeseen henkilöön ja muutosaikaan.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	TSK-006	Kehitysympäristön varmuuskopiointi	Sovelluskehitysympäristön palvelinten ja muiden kehitykseen käytettyjen palveluiden tulee olla säännöllisen varmuuskopioinnin piirissä. Näitä palveluita ovat esimerkiksi versionhallinta, sovelluskehitykseen käytetty wiki, vikatietokanta jne.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	TSK-007	Yhteydet kehitysympäristöön	Toimittajien yhteydet kehitys-, testi- ja tuotantoympäristöihin tulee olla salattu vahvalla salauksella, mikäli yhteydet kulkevat julkisen verkon yli. Lisäksi kaikkien käytettyjen tunnuksien on oltava henkilökohtaisia.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	TSK-008	Tehtävien eriyttäminen	Korotetun tason järjestelmissä eri ympäristöjen ylläpito ja ympäristöjen väliset siirrot tulee organisoida siten, että tehtävien eriyttämien on huomioitu (separation of duties).		Suositus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	TSK-009	Komponenttien luokittelu	Kaikki palvelut, sovellukset ja käytetyt komponentit on luokiteltava sen mukaan, minkä suojaustason tietoa ne käsittelevät. Järjestelmän omistaja on vastuussa järjestelmän käsittelemän tiedon luokituksen määrittämisestä. Komponenteilla tarkoitetaan suoraan sovellukseen kuuluvia ohjelmistokirjastoja, kryptomoduuleja, tietokantoja ja vastaavia. Välillisiä komponentteja, kuten käyttöjärjestelmää tai ohjelmointikielen kirjastoja ei tarvitse luokitella. Tietoturvallisuusasetus määrittelee seuraavat suojaustasot: - Suojaustaso I (ST I), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille. - Suojaustaso II (ST II), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetuille yleisille eduille. - Suojaustaso III (ST III), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleisille tai yksityisille eduille ja oikeuksille. - Suojaustaso IV (ST IV), jos salassa pidettävän tiedon oikeudeton paljastuminen voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetuille yleisille tai yksityisille eduille tai, jos kysymys on tietoturvallisuusasetuksen 9 §:n 2 momentissa tarkoitetuista asiakirjoista, jos tiedon oikeudeton paljastuminen voi aiheuttaa haittaa yleiselle tai yksityiselle edulle tai heikentää viranomaisen toimintaedellytyksiä."	Suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
6. Jatkuvuuden hallinta	JTH-001	Toipumistrategia	Organisaatiolla on kirjallinen toipumisstrategia ja -suunnitelma, jotka määrittelevät toipumismenettelyt tärkeimmille järjestelmille. Dokumentit sisältävät myös tärkeysluokittelun organisaation ICT-järjestelmille. Suunnitelmat ovat johdon hyväksymiä, niiden päivitys ja katselmointi on organisoitu ja vastuutettu.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.12.3	Tarvittaessa
	JTH-002	Jatkuvuuden avainhenkilöt	Jatkuvuuden kannalta avainasemassa olevat henkilöt ja roolit on kartoitettu ja tunnistettu ja varahenkilöt ko. rooleille on määritelty. Varahenkilöt myös koulutetaan tehtäviinsä. Näin varmistutaan siitä, että toimintojen jatkuvuus ei vaarannu, mikäli avainhenkilö ei ole saatavilla tarvittaessa.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	JTH-003	Toipumissuunnitelmat	Organisaation tärkeimmille järjestelmille on laadittu toipumissuunnitelmat. Suunnitelmien katselmointi ja päivittäminen on organisoitu ja vastuutettu. Järjestelmän omistaja on ollut mukana suunnitelman laatimisessa. Toipumissuunnitelma sisältää: • ohjeet katastrofista toipumiseen • ohjeet toiminnan jatkamisesta ja paluusta normaaliin toimintaan, • listan varajärjestelmistä • vaatimukset toissijaisille varajärjestelmille • vastuuhenkilöt ja varahenkilöt • ohjeet toiminnasta poikkeustilanteessa. Suunnitelmien päivittäminen ja katselmointi on organisoitu ja vastuutettu.		Pakollinen vaatimus	Pakollinen vaatimus	2.12.4	Tarvittaessa
	JTH-004	Jatkuvuus- ja toipumissuunnitelmien testaaminen	Organisaation jatkuvuus- ja toipumissuunnitelmia testataan käytännössä säännöllisesti joko kokonaisuutena tai osissa. Suunnitelmia päivitetään testausten tulosten pohjalta.		Suositus	Pakollinen vaatimus	1.2.5.4	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	JTH-005	Häiriöiden kirjaaminen	Organisaation tulee pitää kirjaa järjestelmien häiriöistä ja niiden syistä. Vikaraportteja käytetään organisaation riskianalyysin tekemisessä sekä yhteistyösopimuksia määriteltäessä. Näin mahdolliset häiriötilanteet saadaan osaksi organisaation toiminnan kehittämistä ja esimerkiksi palvelutasojen määrittelyä alihankkijoiden kanssa.		Suositus	Pakollinen vaatimus	2.12.5	Ei
7. Sovellus-kehitysmalli	SKM-001	Sovelluskehitys-prosessi	Organisaatiolla tulee olla kirjallinen sovelluskehitysprosessi, joka kuvaa organisaation käytännöt sovelluskehityksen kaikilla osa-alueilla. Sovelluskehitysprosessi tulee kouluttaa kaikille sovelluskehitystä tekeville työntekijöille, ja organisaation tulee myös varmistua siitä, että prosessia käytetään kaikessa sovelluskehitystyössä. Organisaatio on vastuuttanut prosessin kuvauksen päivittämisen ja kehittämisen. Asiakkailta ja käyttäjiltä saatua palautetta käytetään syötteenä prosessin kehittämisessä. Prosessi ottaa kantaa myös kaikkien kehitysvaiheiden asettamiin tietoturvahaasteisiin (ns. secure SDLC – secure software development life cycle). Käytettävä Secure SDLC riippuu toteutettavan sovelluksen tietoturvallisuuden tasosta, käytettävästä prosessimallista, teknologioista jne. Se voi ottaa kantaa esimerkiksi seuraaviin asioihin: • Tietoturvatestaus • Tyypilliset ongelmat, esimerkiksi SANS/CWE top 25 ohjelmointivirheet ja OWASP Top 10 riskit • Turvallinen arkkitehtuuri • Tietoturvavaatimusten määrittely • Noudatettavat standardit ja vaatimukset • Noudatettava koodausopas • Vaadittavat kriteerit eri vaiheista poistumiselle • Tietoturvallinen ylläpito, asennus, konfigurointi.					
8. Esitutkimus	ESI-001	Tarkoitus ja kriittisyys	Toteutettavan sovelluksen liiketoimintatarkoitus sekä sovelluksen kriittisyys sitä käyttävän organisaation liiketoiminnalle tulee määritellä. Määrittely on dokumentoitava ja sovellus on luokiteltava sen avulla. Lisäksi sovelluksen käsittelemien tietojen luottamuksellisuus tulee määritellä. Käsitelty tieto voi olla luokiteltua esimerkiksi suojaustasojen mukaan. Määritykset toimivat koko projektin ajan sovelluksen tietoturvamekanismien valintaa, suunnittelua ja toteutusta ohjaavina tekijöinä.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Tarvittaessa
	ESI-002	Liiketoiminnan vaikutusanalyysi	Toteutettavalle sovellukselle tulee tehdä liiketoiminnan vaikutusanalyysi, jossa selvitetään mitä vaikutusta erilaisten uhkakuvien toteutumisella on organisaation toiminnalle.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
9. Vaatimus-määrittely	VTM-001	Tietoturvaratkaisuiden dokumentointi	Tietoturvavaatimukset toteuttavat ratkaisut tulee dokumentoida, jolloin dokumentit toimivat suunnittelun pohjana sovelluksen toteuttajille ja ratkaisujen riittävyys voidaan todentaa. Dokumenttien päivitys ja katselmointi pitää organisoida ja vastuuttaa.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Tarvittaessa
	VTM-002	Lainsäädännölliset vaatimukset	Sovelluksen pitää huomioida käsiteltyyn tietoon, sovelluksen toimintaympäristöön tai muihin tekijöihin vaikuttavat lainsäädännölliset vaatimukset.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	VTM-003	Tietoturva-analyysi	Sovelluksen suunnittelu tulee aloittaa käymällä läpi esitutkimusvaiheessa määritelty sovellusprofiili ja määrittelemällä sen asettamat yleisen tason tietoturvavaatimukset. Analyysin tuotteena saadaan karkean tason kuva sovelluksen tietoturvavaatimuksista tietoturvallisuuden eri näkökulmista (luottamuksellisuus, eheys ja saatavuus). Analyysia käytetään sovelluksen suunnittelun pohjana, jolloin järjestelmän tietoturvaominaisuudet suunnitellaan suojattavan tiedon sekä järjestelmän kriittisyyden mukaan.	Suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	VTM-004	Sovelluksen tietoturvataso	Järjestelmän omistajan vastuulla on määritellä, mitä tietoturvatasoa toteutettavan järjestelmän tulee toteuttaa. Järjestelmän omistaja on lisäksi vastuussa järjestelmästä ja sen sisältämästä tietoaineistosta. Lisäksi omistajan tulee määritellä vaatimukset tietoaineiston arkistoinnille yhteistyössä organisaation asiakirjahallinnon kanssa.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	VTM-005	Sovelluksen riskianalyysi	Sovelluksen tietoturvavaatimukset tulee ottaa huomioon jo suunnitteluvaiheessa kohdistamalla sovellukseen riskianalyysi. Vaatimukset määräytyvät järjestelmän omistajan tekemän tietoturvatasomäärityksen ja käytetyn autentikaatiomenetelmän valinnan kautta. Riskianalyysin ytimessä ovat sovelluksen tietoturvallisuuden pahimmat mahdolliset tapaukset (worst case scenario), jotka tulee listata käyttämällä lähtökohtana sovelluksen liiketoimintatarkoitusta, sovelluksen käsittelemää tietoa ja liiketoiminnan riskiprofiilia. Jokainen riski tulee kuvata yhdellä lauseella ja määritellä se hyökkääjän korkean tason tavoitteiksi. Tämän jälkeen jokaiselle riskille tulee määritellä esiehdot joiden pitää päteä jokaiselle hyökkääjän tavoitteen onnistumiselle. Informaatio voidaan esittää ns. uhkapuuna tai rakenteellisena listana. Esimerkki: Organisaatio kehittää web-sähköpostisovellusta. Eräs tunnistettu pahin mahdollinen tapaus: käyttäjän viestit ovat muiden luettavissa. Tunnistettu uhka: hyökkääjä voi lukea muiden käyttäjien sähköposteja. Esiehdot: 1. Datan validointi ei toimi TAI 2. Auktorisointi ei toimi TAI 3. Selaimen välimuistiin jää luottamuksellista informaatiota JA a. Käyttäjä käyttää jaettua konetta TAI b. Hyökkääjää saa käyttäjän koneen käsiinsä TAI c. Selaimen tietoturvapuute altistaa välimuistin hyökkääjälle.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.13.2	Kyllä

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	Viite ohjeeseen	Vaatimuskohde	Kuvaus	Perustaso	Korotettu taso	Korkea taso	Vahti 2/2010	Tarjous-pyyntöön
	VTM-006	Sovelluksen tietoturvavaatimukset	Kehitettävälle sovellukselle tulee määritellä tietoturvavaatimukset. Sovelluksen tietoturvavaatimukset tulee johtaa seuraavista lähtökohdista: • Sovelluksen kriittisyys liiketoiminnalle • Sovelluksen sisältämän ja käsittelemän tiedon asettamat vaatimukset • Sovelluksen toiminnallisista vaatimuksista johdetut vaatimukset • Uhka-analyysi. Analyysin pohjana voi käyttää muun muassa seuraavia näkökulmia: • tiedon eheys • tiedon luottamuksellisuus • tiedon saatavuus • pääsynhallintavaatimukset • toiminnon kriittisyys • tehtävien eriyttäminen (separation of duties) • vasteajat • kuormitus. Liiketoimintaprosessin omistajien ja muiden sidosryhmien edustajien tulee osallistua tietoturvavaatimusten määrittelyyn.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	VTM-007	Lait, määräykset ja ohjeistukset	Tietoturvavaatimusten määrittelyn pohjana tulee käyttää myös soveltuvia lakeja, määräyksiä, standardeja ja ohjeistuksia. Tällaisia ohjeistuksia voivat olla muun muassa toimialan best practice -suositukset, liiketoiminta-alaan tai valittuihin teknologioihin soveltuvat standardit, compliance-vaatimukset, ulkoiset tai sisäiset vaatimukset jne. Liiketoiminnan omistajat ja arkkitehdit määrittelevät käytettävät ohjeistukset.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	VTM-008	Uhkamallinnus	Sovellukselle on tehtävä uhkamallinnus, joka perustuu johonkin valittuun metodiin tai malliin. Esimerkkejä malleista ovat Microsoft STRIDE, DREAD ja väärinkäyttötapausten (abuse case) analyysi. Myös muita malleja voidaan soveltaa, esimerkiksi organisaation omaa mallia. Väärinkäyttötapausten analyysissä käydään läpi sovelluksen käyttötapaukset ja eritellään, miten hyökkääjä voisi käyttää kyseistä toiminnallisuutta hyväkseen. Näin saatuja väärinkäyttötapauksia tulee käyttää myös testitapausten määrittämiseen. Esimerkki: käyttötapaus web-sovellukselle: Käyttäjä kirjautuu sovellukseen käyttäen tunnusta ja salasanaa. Vastaavia väärinkäyttötapauksia: • hyökkääjä murtaa kirjautumisen brute force-hyökkäyksellä • hyökkääjä salakuuntelee kirjautumistunnukset • hyökkääjä selvittää tunnukset social engineering-hyökkäyksellä • hyökkääjä saa salatut tunnukset haltuunsa ja murtaa ne offline-työkaluilla • hyökkääjä ohittaa kirjautumistoiminnallisuuden • hyökkääjä näkee luottamuksellista tietoa ilman kirjautumista. Lisää tietoa saa esimerkiksi OWASP:n sivuilta. https://www.owasp.org/index.php/Threat_Risk_Modeling		Suositus	Vahva suositus		Tarvittaessa
	VTM-009	Arkkitehtuurilinjaus	Sovelluksen hankkivalla organisaatiolla tulee olla arkkitehtuurilinjaus, jonka mukaisia hankittavien järjestelmien tulee olla. Arkkitehtuurilinjauksen pitää sisältää myös tietoturvavaatimuksia, kuten: • Vaaditut salausmenetelmät • Vaaditut tunnistautumismenetelmät • Vaaditut lokien keräysmenetelmät. Tällöin varmistutaan siitä, että kaikki hankittavat järjestelmät täyttävät tietyt tietoturvakriteerit ja sopivat hankkivan organisaation tietoturvainfrastruktuuriin.	Suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa
	VTM-010	Uhkamallinnuksen tarkennus	Rakennettua uhkamallia tulee tarkentaa ottamalla mukaan uhkia jotka liittyvät sovelluksen toteutukseen tai arkkitehtuuriin. Tällaisia asioita ovat muun muassa: • Käyttäjäroolit • Tietoturvaoletukset • Käytetyt teknologiat • Tietoturvamekanismit.		Vahva suositus	Vahva suositus		Ei
	VTM-011	Komponenttien uhka-arvio	Sovelluksen käyttämille kolmansien osapuolten komponenteille tulee tehdä uhka-arvio. Näitä komponentteja ovat esimerkiksi avoimen lähdekoodin kirjastot, online-palvelut tai COTS-ohjelmistot (commercial off the shelf, valmisohjelmistot). Tulee selvittää, miten haavoittuvuudet tai suunnitteluvirheet komponenteissa vaikuttavat kehitettävän sovelluksen tietoturvallisuuteen.		Suositus	Vahva suositus		Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
10. Suunnittelu	SNT-001	Yleiset standardit	Arkkitehtuuria suunniteltaessa tulee suosia yleisesti käytössä olevia ja hyväksyttyjä standardeja, mikäli se on mahdollista. Näin varmistetaan se, että suunniteltava sovellus on helppo integroida muihin järjestelmiin. Lisäksi tunnetut ja yleisesti käytetyt ratkaisut ovat yleensä joutuneet tarkemman tietoturva-analyysin kohteeksi kuin itse toteutetut tai harvinaisemmat teknologiat. Lisäksi avointen standardien käyttämistä suositaan, koska niiden tietoturvaominaisuudet tunnetaan tyypillisesti suljettuja standardeja paremmin.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	SNT-002	Tietoturvapäivitysten suunnittelu	Sovellus tulee suunnitella siten, että korjausten ja tietoturvapäivitysten asentaminen on mahdollisimman helppoa. Käytännössä tämä tarkoittaa ainakin seuraavien asioiden huomioimista: • Ei kovakoodattuja konfiguraatioarvoja • Sovellus ei ole riippuvainen tietyistä ohjelmistoversioista, kuten JRE-versiosta. Toteutettavaa sovellusta ei saa suunnitella siten, että se on riippuvainen käytetyn komponentin ominaisuudesta, joka löytyy vain komponentin tietystä versiosta. • Kirjastoriippuvuudet on toteutettu siten, että päivittäminen onnistuu helposti.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	SNT-003	Suositellut ohjelmistot	Organisaation tulee perustaa ja ylläpitää listaa suositelluista ohjelmistokomponenteista, kirjastoista, sovelluskehyksistä jne., joita käytetään organisaation toteuttamissa sovelluksissa. Komponentit luokitellaan toiminnallisuuden mukaan. Komponenttien tietoturvatilannetta ja päivityksiä tulee seurata.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Tarvittaessa
	SNT-004	Ulkoiset rajapinnat	Sovelluksen ulkoiset rajapinnat käydään läpi ja verrataan niitä organisaation arkkitehtuuri- ja sovelluskehitysohjeistukseen kirjattuihin periaatteisiin (Katso TSK-001). Rajapintakohtaisesti selvittäen analysoidaan, toteutuuko periaate sovellustasolla. Tarvittaessa selvitetään, voiko tietoturvamekanismin toteuttaminen kohtuullisella työllä parantaa järjestelmän tietoturvallisuutta.	Vahva suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	SNT-005	Tietoturvalliset suunnittelumallit	Sovelluksen arkkitehtuurin suunnittelussa tulee käyttää ns. turvallisia suunnittelumalleja (secure design pattern). Organisaation kehittämät sovellukset tulee luokitella yleisen arkkitehtuurin mukaan. Tavallisia korkean tason arkkitehtuuriluokkia ovat muun muassa: • client-server • sulautettu järjestelmä • työpöytäsovellus • web-sovellus • web service • mobiilisovellus. Jokaista yleistä arkkitehtuuriluokkaa koskevat suunnittelumallit tulee kerätä ja soveltaa kehitettäviin sovelluksiin. Suunnittelumallien tunnistamisen ja valitsemisen tekevät arkkitehdit ja kokeneet sovelluskehittäjät sovelluksen suunnitteluvaiheessa. Suunnittelumallien pitää sisältää myös tietoturvallisia suunnittelumalleja (secure design patterns) ts. malleja, jotka ratkaisevat tietoturvallisuuteen liittyvän suunnitteluongelman. Katso esimerkkejä: • Security Patterns for J2EE Applications, Web Services, Identity Management, and Service Provisioning • SecurityPatterns.org • Architecture and Design Considerations for Secure Software • Secure Design Patterns Esimerkki: Organisaatio kehittää web-sovellusta verkkokaupankäyntiin. Tunnistettuja ja käytettyjä turvallisia suunnittelumalleja ovat muun muassa: • Keskitetty lokien keräys • Keskitetty virheiden- ja poikkeustenkäsittely • Syötteen validointi • SSO:n käyttö kirjautumiseen.	Vahva suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	SNT-006	Hyökkäyspinta-ala	Sovelluksen hyökkäyspinta tulee tunnistaa. Hyökkäyspinnalla tarkoitetaan kaikkia järjestelmän toiminnallisuuksia, joissa osapuolet eivät voi täysin luottaa toisiinsa ja joita voidaan siten käyttää sovellusta vastaan hyökättäessä. Tällaisia ovat esimerkiksi: • Avoimet palvelut • Syöterajapinnat • Web servicet • RPC • Sovelluspalvelimen ja tietokantapalvelimen välinen liikenne • Järjestelmän palvelimilla toimivat muut sovellukset. Hyökkäyspinnan määrittely tehdään analysoimalla sovelluksen korkean tason arkkitehtuuria. Arkkitehtuurin jokainen komponentti käydään läpi ja analysoidaan pääsy komponentin rajapintoihin esimerkiksi seuraavilta osin: • Tunnistautumaton käyttäjä • Autentikoitunut käyttäjä • Ylläpitäjä • Sovelluksen muut roolit. Tehty kuvaus muodostaa sovelluksen hyökkäyspinnan (attack surface). Sitä käytetään pohjana rajapintojen ja moduulien tietoturvamekanismien suunnittelussa. Hyökkäyspinta pitää päivittää, jos sovellukseen tulee merkittäviä muutoksia.	Vahva suositus	Vahva suositus	Pakollinen vaatimus		Ei
	SNT-007	Arkkitehtuurin tietoturvavaatimukset	Sovelluksen arkkitehtuuri on analysoitava tunnettuja tietoturvavaatimuksia vasten. Vertaa tietoturvavaatimuksia sovelluksen hyökkäyspintaan ja sovelluksen arkkitehtuuriin sekä varmista, että kaikki vaatimukset toteutuvat arkkitehtuuritasolla. Paranna sovelluksen arkkitehtuuria ja suunniteltuja tietoturvamekanismeja mikäli kaikki vaatimukset eivät täyty. Suorita uusi analyysi mikäli arkkitehtuuriin tulee suuria muutoksia.	Suositus	Vahva suositus	Pakollinen vaatimus		Ei
	SNT-008	Tietoturva-mekanismien kattavuus	Suunnittelukatselmoinneissa on varmistettava, että yhteisesti hyväksytyt tietoturvaratkaisut (Katso TSK-002) ovat käytössä koko sovelluksessa. Arkkitehtuuria suunniteltaessa käydään läpi kaikki liittymät järjestelmien välillä ja tarkastetaan niiden tietoturvamekanismit. Analyysi tehdään sekä sisäisille että ulkoisille rajapinnoille. Analyysin tarkoituksena on varmistaa, että suunniteltuja tietoturvamekanismeja käytetään koko sovelluksen laajuisesti. Näin estetään esimerkiksi se, että jokainen sovelluskehittäjä toteuttaa oman lokitoiminnallisuutensa tai virheenkäsittelymekanisminsa. Analyysi toistetaan aina uuden sovellusjulkaisun yhteydessä, jolloin edellisen julkaisun yhteydessä tehdyn analyysin havainnot päivitetään.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	SNT-009	Tunnistautumis-menetelmä	Valitulla tunnistautumismenetelmällä on suuri vaikutus kokonaisuuden tietoturvallisuuteen. Sovelluksen omistajan vastuulla on määritellä sovelluksen käsittelemän tiedon luokittelu, joten hänen vastuullaan on myös määritellä se, miten vahvaa tunnistautumista sovelluksessa käytetään. Tämän perusteella valitaan soveltuva käyttäjäntunnistusmenetelmä. Vaihtoehtoja ovat muun muassa: • Käyttäjätunnus ja salasana • Tunnuslukulistat • SMS • Tietoturvalaite, kuten RSA-tunniste • Toimikortti • Pankkitunnistautuminen • SSO-palvelu • Federointipalvelu • KATSO- tai VIRTU-tunnistautuminen.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.6.1	Tarvittaessa
	SNT-010	Salasanavaatiumusten konfigurointi	Mikäli sovelluksen omistaja määrittelee riittäväksi tunnistautumismekanismiksi salasanan ja käyttäjätunnuksen, pitää sovellus toteuttaa siten, että ainakin seuraavat salasanan laatuvaatimukset ovat konfiguroitavissa: • Salasanan pituus • Erikoismerkkien määrä • Tunnuksen lukkiutuminen määräajaksi liian monen epäonnistuneen kirjautumisen jälkeen • Salasanan vanhenemisaika • Tunnuksen vanhenemisaika. Mikäli mahdollista, tulisi salasanojen käyttöä itse sovelluksessa välttää ja tallentaa ne esimerkiksi LDAP-tietokantaan, jossa salasanojen laatuvaatimuksia voidaan hallita keskitetysti. Lisäksi on varmistuttava siitä, että sovelluksen kehittäjille ja ylläpitäjille tulee olla mahdollista määritellä tiukemmat vaatimukset muun muassa salasanan pituuden ja erikoismerkkien suhteen. On suositeltavaa käyttää salasanalauseita: esimerkiksi vähintään 16 merkkiä ilman kompleksisuusvaatimuksia (erikoismerkit). Salasanalauseiden käytöllä saadaan ehkäistyä yleisimmät salasanoihin kohdistuvat hyökkäykset, kuten brute force -hyökkäys ja ns. sateenkaaritaulukoiden (rainbow tables) käyttö. Kyseiset taulukot sisältävät esilaskettuja tiivistearvoja salasanoista, ja niitä voidaan käyttää salasanatiivisteiden murtamiseen. Lisäksi on suositeltavaa käyttää samoja salasanavaatimuksia sekä testi- että tuotantoympäristöissä. Muussa tapauksessa siirrettäessä järjestelmää tuotantoon testiympäristössä käytetyt salasanat tulee vaihtaa tuotantoympäristön vaatimukset täyttäviin.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.6.4	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	Viite ohjeeseen	Vaatimuskohde	Kuvaus	Perustaso	Korotettu taso	Korkea taso	Vahti 2/2010	Tarjous-pyyntöön
	SNT-011	Käyttöoikeustasot	Sovellukset tukevat yleensä useaa eri käyttöoikeustasoa (käyttäjä, ylläpitäjä jne.) Sovelluksen käyttäjille on myönnettävä vain sen tasoiset oikeudet, jotka ovat välttämättömiä heidän roolinsa kannalta (ns. least privilege). Myönnettyjen tunnusten on oltava henkilökohtaisia, ja yleiskäyttöisten tunnusten käyttö on estettävä tai kiellettävä. Sovelluksen tietoturvallisuuteen vaikuttaviin ominaisuuksiin tulee olla pääsy vain sovelluksen pääkäyttäjällä. Samoin sovellus tulee toteuttaa siten, että sen käynnistämät prosessit suoritetaan pienimmällä mahdollisella käyttöoikeustasolla. Tätä samaa periaatetta tulee käyttää sovelluksen kaikissa komponenteissa, kuten tietokannassa, jossa sovelluskäyttäjältä estetään esimerkiksi tietokantaskeeman muutokset.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Tarvittaessa
	SNT-012	Luottamusrajat	Sovellusta suunniteltaessa tulee määritellä ns. luottamusrajat (trust boundaries). Kaikkea rajan toiselta puolelta tulevaa dataa tulee käsitellä ei-luotettuna, ja luottorajan toisella puolella oleviin tarkastuksiin ei tule luottaa. Ei-luotettu data tulee validoida ja kanonisoida ennen käyttöä. Validointi tulee toteuttaa ns. white list -pohjaisesti, toisin sanoen vain erikseen sallittu syöte hyväksytään ja muu hylätään. Myös salausmenetelmiä ja sähköistä allekirjoitusta voidaan käyttää tiedon aitouden ja muuttumattomuuden varmistamiseksi. Samoin ulkoisille komponenteille luovutettava data tulee enkoodata ja kanonisoida ennen lähettämistä. Näin varmistutaan siitä, että luovutettava data on turvallista ulkoisen komponentin käytettäväksi.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	SNT-013	Salausratkaisut	Sovelluksessa käytettyjä salausratkaisuja koskevat seuraavat vaatimukset (ks. VAHTI 3/2008 termistön osalta): • Sovelluksen tulee säilyttää vain sellainen luottamuksellinen data, jota se tarvitsee. Datan säilyttäminen varmuuden vuoksi on kiellettyä. • Salausratkaisuiden tulee olla tunnettuja, julkisia ja käyttötarkoitukseen nähden riittävän vahvoiksi todettuja. Tällaisia ovat esimerkiksi AES ja RSA julkisen avaimen kryptografiaan sekä SHA-256 tiivisteiden laskemiseen. Huomaa, että algoritmin ”vahvuus” on elävä suure. • Salausratkaisuja ei koskaan tule toteuttaa itse, vaan tulee käyttää tunnettuja toteutuksia (esimerkiksi OpenSSL, KeyCzar, jne.) • Käytettyjen satunnaislukugeneraattoreiden pitää olla vahvoja ja niiden siemenarvojen tulee sisältää riittävästi entropiaa. • Tallennetuista salasanoista tulee tallentaa vain salt-arvojen kanssa lasketut tiivisteet. • Salasanojen tallentamiseen on käytettävä adaptiivista tiivistealgoritmia. • Kaikki tietoliikenne sovelluspalvelimen ja asiakasohjelmiston välillä tulee salata, mikäli se kulkee julkisen verkon yli, jolloin verkkoliikennettä salakuuntelemalla ei ole mahdollista saada haltuunsa luottamuksellista tietoa. Käytetyt salausratkaisut pitää pystyä tarvittaessa vaihtamaan. Mikäli siirrettävä tieto on luonteeltaan julkista, ei sitä tarvitse salata. Tällaista tietoa on esimerkiksi julkiset web-sivustot. • Turvallisuusluokitellun tiedon salaamiseen käytettyjen ratkaisujen tulee olla tarkastettu ja hyväksytty ko. tasolle kansainvälisen tai kansallisen tietoturvaviranomaisen toimesta tai erillisessä ratkaisulle suoritetussa tarkastuksessa. "	Vahva suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	SNT-014	Tuki- ja ylläpitoyhteydet	Mikäli sovelluksen tuki- tai ylläpitotoiminnallisuus vaatii toimittajan tai tukea toimittavan tahon pääsyn järjestelmään, on tämä otettava huomioon jo suunnitteluvaiheessa. Erityisesti kriittisiä ovat ulkopuolisten mahdollinen pääsy järjestelmän tietoihin ja mahdollisten etäyhteyksien suojaaminen.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus	2.6.3	Tarvittaessa
	SNT-015	Uhkamallinnuksen syventäminen	Vaatimusmäärittelyvaiheessa tehtyä uhkien mallintamista tulee syventää uudella tiedolla esimerkiksi valituista teknisistä ratkaisuista sekä sovelluksen toiminnallisuudesta.	Suositus	Vahva suositus	Pakollinen vaatimus		Ei
	SNT-016	Monitaso-arkkitehtuurit	Mikäli sovellus toteuttaa ns. monitasoarkkitehtuuria (n-tier architecture), tulee eri komponenttien, kuten sovelluspalvelin ja tietokanta, välinen tietoliikenne suunnitella ja dokumentoida kattavasti. Sovelluksen tulee mahdollistaa ainakin: • Eri komponentit voidaan sijoittaa eri verkkosegmentteihin • Sovelluspalvelimen ja tietokannan välisiin yhteyksiin tulee mahdollisuuksien mukaan käyttää alustojen tukemia nimettyjä tietolähteitä (datasource). • Komponenttien välisen tietoliikenteen salaaminen, tunnisteiden käyttö sekä molemminpuolinen tunnistaminen (esimerkiksi mutual TLS) • Hallinta- ja valvontaliikenteen erottaminen muusta liikenteestä.		Suositus	Pakollinen vaatimus		Tarvittaessa
	SNT-017	Vahva tunnistautuminen	Korkean tietoturvatason järjestelmän arkkitehtuurin tulee toteuttaa seuraavat vaatimukset: • Järjestelmään kirjautumiseen on käytettävä vahvaa tunnistautumista, jolloin tunnistautumiseen tarvitaan tietoa kahdesta eri lähteestä (esimerkiksi käyttäjätunnus/salasana sekä RSA-tunniste). • Sovelluksen on käytettävä monitasoarkkitehtuuria, jossa arkkitehtuurin eri komponentit on sijoitettava eri palvelimille.			Suositus		Kyllä
11. Toteutus	TOT-001	Virheiden käsittely	Sovelluksen poikkeus- ja virhetilanteiden käsittely tulee suunnitella ja toteuttaa siten, että virhetilanteet eivät johda sovelluksen tietoturvallisuuden vaarantumiseen. Huomioitavia asioita ovat ainakin: • Virheiden ja poikkeusten käsittely tulee suunnitella koko sovelluksen kattavasti. • Virheiden käsittely tulee toteuttaa keskitetysti ja koko sovelluksen kattavasti, jolloin testaus saadaan kattavaksi ja virheiden korjaamien on nopeampaa. • Niin sanotulla fail-secure -suunnitteluperiaatteella varmistetaan, että virhetilanteessa komponentin tai sovelluksen käyttö ennemmin estetään kuin sallitaan tietoturvaloukkauksen hyväksikäyttö. • Defensiivinen ohjelmointi o Oletetaan, että ohjelmaan on jäänyt virheitä. Jokainen ohjelman osa tekee syötteen tarkastuksen. o Tehdään ajonaikainen tarkastus kaikille mahdollisille virhetilanteille ja määritellään poikkeusten käsittely. • Virheilmoitukset eivät saa sisältää luottamuksellista tietoa, kuten tietokantapalvelimen vastauksia, sovelluspalvelimen versiotietoja jne. Kaikissa virhetilanteissa näytetään yleinen virheilmoitus, joka kuvaa tapahtuneen virheen, mutta ei anna tietoa sovelluksen toteutuksesta. Myöskään ”henkilökohtaista” tietoa, kuten ylläpitäjien nimiä tai yhteystietoja, ei tulisi sisällyttää virheviesteihin social engineering -hyökkäysten estämiseksi.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	TOT-002	Lokit virhetilanteista ja tietoturvapoikkeamista	Sovelluksen tulee tuottaa riittävästi lokia virhetilanteista sekä tietoturvapoikkeamista. Riittävien lokien kerääminen sekä onnistuneista että epäonnistuneista tietoturvatapahtumista mahdollistaa hyökkäysten havaitsemisen ja helpottaa selvittämistä jälkikäteen. Lokiviesti pitää kirjoittaa seuraavista tapahtumista: • Onnistuneet ja epäonnistuneet kirjautumisyritykset • Onnistuneet ja epäonnistuneet pääsynhallintapäätökset • Epäonnistuneet syötteenkäsittelypäätökset • Ylläpitotoimet • Kriittisen tiedon käsittely, mukaan lukien tiedon lukeminen. Sovelluksen tiedon käsittely, mukaan lukien tietojen katselu, on pystyttävä jäljittämään lokien perusteella.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.6.2	Ei
	TOT-003	Lokitapahtumien tiedot	Lokien pitää sisältää riittävästi tietoa operaation tekijän identifioimiseksi, hyökkäyksen tunnistamiseksi ajoissa ja jälkiselvityksen helpottamiseksi. Jokaisen lokikirjoituksen pitää sisältää ainakin seuraavat tiedot: • Aikaleima luotettavasta lähteestä • Tapahtuman merkitys tietoturvallisuuden kannalta (esimerkiksi matala, korkea, kriittinen) • Indikaatio siitä, onko kyseessä tietoturvallisuuteen liittyvä tapahtuma (mikäli tietoturvalokia ei ole eriytetty omaan tiedostoonsa) • Käyttäjätunnus ja lähdeosoite • Onnistuiko tapahtuma • Tapahtuman kuvaus. Lokeihin ei kuitenkaan saa kirjoittaa luottamuksellista tietoa, kuten salasanoja, henkilötietoja tai luottokorttinumeroita. Lokitietojen tallentamisen yhteydessä tulee myös huomioida mahdollinen henkilörekisterin muodostuminen ja sen lakitekniset seuraukset. Jokaisen lokirivin tulee noudattaa ennalta määriteltyä rakennetta, jotta lokitiedostojen automaattinen käsittely ja analysointi ovat mahdollisia.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	TOT-004	Yhteinen aikalähde	Kaikkien ympäristöön kuuluvien laitteiden tulee synkronisoida kellonsa samasta lähteestä (esimerkiksi NTP-palvelin). Näin varmistetaan se, että tapahtumien järjestys pysyy johdonmukaisena ja eri lähteistä kerättyjen lokien korrelointi onnistuu helposti.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	TOT-005	Lokien suojaaminen	Lokien kirjoittaminen: Lokien suojausta ja käsittelyä koskevat seuraavat vaatimukset: • Lokitiedostojen pääsyoikeudet tulee määritellä siten, että vain tietyillä käyttäjäryhmillä on oikeus lukea ja muokata lokeja. • Lokitapahtumat tulee kirjoittaa tapahtuma kerrallaan, ts. tapahtumia ei tule puskuroida ennen kirjoittamista mikäli suorituskykysyyt eivät estä suoraa kirjoittamista.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	Viite ohjeeseen	Vaatimuskohde	Kuvaus	Perustaso	Korotettu taso	Korkea taso	Vahti 2/2010	Tarjous-pyyntöön
	TOT-006	Istunnon suojaaminen	Istunnon kaappaaminen on tyypillinen tietoturvahyökkäys sovelluksia vastaan. Tällöin hyökkääjä saa kirjautuneen käyttäjän istunnon haltuunsa esimerkiksi istuntotunnisteen kaappaamalla. Sovellus tulee toteuttaa siten, että autentikoituneen käyttäjän istuntoa ei voi kaapata luvattomasti. Keinoja istunnon kaappaamisen estämiseksi ovat muun muassa: • Yhteyden salaus • Istunnon aikakatkaisu • Vaikeasti arvattava istuntotunniste • Istuntotunnisteen suojaaminen (esimerkiksi seuraavat attribuutit: secure, httpOnly, domain, path, expires). • Istunnon tuhoaminen käyttäjän kirjautuessa ulos • Sivukohtaiset tunnisteet ns. CSRF-hyökkäyksen estämiseksi. CSRF -hyökkäyksessä hyökkääjä ei saa istuntoa kokonaan kaapattua, mutta pystyy pakottamaan käyttäjän tekemään transaktioita. • Istunnon aloittajan IP-osoitteen tallentaminen ja käyttäminen istunnon seuraamisessa tunnisteen lisäksi.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	TOT-007	Käyttäjätunnusten hallinta	Sovelluksen käyttäjätunnusten hallinta on toteutettava siten, että hallinta on mahdollisimman keskitettyä ja ajantasaista. Lisäksi sovelluksen tulee tukea ulkoista yhteistä käyttäjänhallintapalvelua, kuten LDAP-palvelinta.	Vahva suositus	Vahva suositus	Vahva suositus		Tarvittaessa
	TOT-008	Koodikatselmoinnit	Koodikatselmoinneissa varmistetaan, että toteutettaessa on: • Noudatettu organisaation arkkitehtuuri- ja sovelluskehitysohjeistukseen kirjattuja periaatteita (Katso TSK-001) • Käytetty yhteisesti hyväksyttyjä tietoturvaratkaisuja (Katso TSK-002) • Huomioitu yleisimmät ohjelmointiin liittyvät tietoturvaongelmat, kuten o OWASP Top 10 o CWE/SANS TOP 25 Most Dangerous Software Errors o The CERT Oracle Secure Coding Standard for Java.	Vahva suositus	Vahva suositus	Pakollinen vaatimus		Ei
	TOT-009	Lokien muokkaaminen	Korotetun tason järjestelmille asetetaan lisäksi seuraavat vaatimukset: • Lokitietojen katselusta tulee kirjoittaa lokimerkintä • Sovelluksen tai palvelimen ylläpitäjällä ei saa olla oikeutta muokata lokeja • Tietoturvaloki tulee voida eriyttää omaan tiedostoonsa.		Pakollinen vaatimus	Pakollinen vaatimus	2.6.5	Tarvittaessa
	TOT-010	Lokien parannettu suojaus	Korkean tason sovellusten tietoturvalokeille asetetaan lisäksi seuraavat vaatimukset: • Lokitiedostoista lasketaan tarkistussumma, jolloin lokeihin jälkikäteen tehdyt muutokset pystytään havaitsemaan. Tarkistussummia säilytetään erillään tietoturvalokeista. • Lokit tulee tallentaa kertakirjoitteiselle medialle tai ulkoiselle lokipalvelimelle, jolloin lokeja ei voi muokata jälkikäteen • Lokitiedot voidaan tarvittaessa myös salata siirtovaiheessa ja lokipalvelimella • Lokitietojen eheys tulee tarkistaa automaattisesti säännöllisesti.		Suositus	Suositus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
12. Testaus	TST-001	Tietoturvan testitapaukset	Tietoturvatestitapaukset tulee johtaa useista eri lähteistä, joita ovat ainakin: • Sovelluksen tietoturvavaatimukset • Sovelluksen toiminnalliset vaatimukset • Aiemmat löydökset ja havaitut ongelmat • Väärinkäyttötapaukset (mikäli näitä on tehty) • Käytettyjen teknologioiden tyypilliset ongelmat (Kuten Owasp Top 10). Kehittäjien, tietoturvavastaavien ja QA-vastaavien tulee katselmoida testitapausten tehokkuus, järkevyys ja kattavuus. Testitapausten suunnittelu tulisi tehdä sovelluksen määrittely- ja suunnitteluvaiheessa, sekä uudelleen kun sovellukseen tulee merkittäviä muutoksia.	Suositus	Vahva suositus	Pakollinen vaatimus		Ei
	TST-002	Testisuunnitelman katselmointi	Tietoturvavastaavan tulee katselmoida ja arvioida sovelluksen tietoturvasuunnitelma tai -suunnitelmat. Suunnitelmia tulee päivittää tietoturvavastaavan kommenttien perusteella.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.13.8	Ei
	TST-003	Tietoturvatestien suorittaminen	Tietoturvatestit tulee suorittaa osana sovelluksen normaalia testausprosessia. Testauksesta valmistuu testiraportti, joka sisältää tiedon tietoturvatestien suorituksesta.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	TST-004	Testausvaiheen koodikatselmointi	Sovelluskehityksen tietoturvavastuullinen (security coach) voi tarvittaessa suorittaa epäformaaleja koodikatselmointeja tietoturvallisuuden kannalta kriittisiin osiin. Katselmointien tulokset kirjataan ylös organisaation prosesseihin parhaiten soveltuvaan paikkaan, jossa katselmointien tuloksia pystytään seuraamaan, esimerkiksi: • Pöytäkirjaan • Virheiden hallintatyökalu • Ohjelmakoodiin. Havaintojen korjaaminen vastuutetaan ja korjaustoimenpiteiden toteutumista seurataan.	Suositus	Vahva suositus	Pakollinen vaatimus		Ei
	TST-005	Testidatan luonti	Testauksessa käytetty data ei saa sisältää tuotannosta kopioitua salassa pidettävää tietoa. Testidata tulee siten joko generoida testausta varten, tuotantodatasta tulee poistaa salassa pidettävät tiedot tai data on sekoitettava. Sekoitetussa datassa yksittäiset tiedot voivat olla aitoja, mutta niiden yhdistelmät eivät. Mikäli yllämainitut keinot eivät ole mahdollisia, tulee varmistua siitä, että testiympäristö on suojattu samoilla teknisillä ja hallinnollisilla suojakeinoilla kuin tuotantoympäristö. Tällöin voidaan varmistua siitä, että henkilöt, jotka eivät työssään tarvitse tuotantoympäristössä olevia tietoja, eivät voi niitä myöskään testiympäristössä käsitellä.	Vahva suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa
	TST-006	Automaattiset testaustyökalut	Tietoturvatestaamiseen tulee käyttää automaattisia testaustyökaluja. Automaattisten työkalujen käyttö tulee lisäksi olla integroituna sovelluskehitys- ja testausprosessiin. Työkaluja voivat olla esimerkiksi • Fuzzerit (protokolla, syöte jne.) • Haavoittuvuusskannerit • Staattista tai dynaamista koodin analysointia tekevät työkalut • Jatkuvan integraation (continuous integration) työkalut.		Suositus	Pakollinen vaatimus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	TST-007	Tietoturva-auditointi	Korotetun tason sovelluksen tietoturvallisuus on auditoitava ennen käyttöönottoa. Auditoinnissa on käytettävä sekä automaattisia että manuaalisia menetelmiä. Auditoijan on oltava ulkoinen, riippumaton osapuoli. Auditointi koostuu seuraavista vaiheista: • Tekninen auditointi, jossa testataan tietoturvakontrollien toimivuus tunkeutumistestauksen keinoin • Hallinnollinen auditointi, jossa tarkastetaan sovelluksen operointi- ja ylläpitoprosessit jne. • Arkkitehtuurin auditointi, jossa tarkastetaan sovelluksen arkkitehtuuri tietoturvanäkökulmasta.		Pakollinen vaatimus	Pakollinen vaatimus	2.13.7	Kyllä
	TST-008	Tietoturva-mekanismien tarkastus	Sovelluksen tietoturvavaatimuksista tulee johtaa lista kooditasolla tarkastettavista asioista. Näitä voivat olla esimerkiksi toiminnallisista vaatimuksista johdettavat tarkastukset, sovelluskohtaiset hyvät käytännöt tai ohjelmointikielikohtaiset käytännöt. Tietoturvallisuuden kannalta kriittiset komponentit tulee käydä läpi käyttäen tarkistuslistaa. Tyypillisiä kriittisiä komponentteja ovat esimerkiksi: • Autentikaation toteutus • Pääsynhallinan toteutus • Istunnon hallinta • Salauksen toteutus • Datan parsinta • Syötteen validointi. Tarkastus tulee uusia aina kun kyseessä oleviin kohteisiin tehdään merkittäviä muutoksia. Tarkastuksessa voi käyttää ulkoisia tarkistuslistoja (esimerkiksi OWASP ASVS). Katselmoinnista valmistuu pöytäkirja. Tehtyjen havaintojen korjaaminen vastuutetaan ja korjaamista seurataan. Viitemateriaalina katselmoinnissa voi käyttää esimerkiksi SANS/CWE top 25 -ohjelmointivirheiden listaa tai OWASPin koodikatselmointiopasta."		Suositus	Pakollinen vaatimus		Ei
	TST-009	Tietoturvatestien läpäisy	Tietoturvatestien läpäisy tulee asettaa vaatimukseksi sovelluksen siirtymiselle vaiheesta toiseen elinkaaressaan. Esimerkiksi tietty kokoelma tietoturvatestitapauksia pitää läpäistä ennen sovellusjulkaisun tekemistä.		Suositus	Vahva suositus		Tarvittaessa
	TST-010	Sovelluskehityksen aikainen auditointi	Korkean tason sovelluksen tietoturvallisuus on auditoitava myös sovelluskehityksen aikana, esimerkiksi eri tarkastuspisteiden yhteydessä. Näin varmistutaan siitä, että kriittiset tietoturvaongelmat havaitaan ja korjataan jo hyvissä ajoin ennen järjestelmän käyttöönottoa.		Suositus	Pakollinen vaatimus	2.13.9	Tarvittaessa
	TST-011	Koodikatselmoinnin hyväksytty suorittaminen	Koodikatselmoinnin läpäisy tulee asettaa vaatimukseksi sovelluksen siirtymisessä vaiheesta toiseen elinkaaressaan. Siirtyminen seuraavaan elinkaaren vaiheeseen tehdään perustuen riskiarvioon, jolloin vähäiset tietoturvapuutteet sovelluksessa eivät välttämättä estä julkaisun tekemistä.			Suositus		Tarvittaessa

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
13. Käyttöönotto	KTY-001	Toimintaympäristön kuvaus	Toteutettavan sovelluksen odotettu toimintaympäristö kuvataan ja kuvausta ylläpidetään. Dokumentti kuvaa oletukset, joiden täytyy pitää paikkaansa sovelluksen oikean toiminnan varmistamiseksi, esimerkiksi: • Prosessoriarkkitehtuuri • OS versiot • Tarvittavat sovellukset, kirjastot jne. • Tarvittavat konfiguroinnit (käyttöjärjestelmä ja varusohjelmistot jne.). Dokumentin katselmointi ja päivittäminen on vastuutettu ja organisoitu. Dokumenttia tulee päivittää säännöllisesti ja aina uusien julkaisuiden yhteydessä.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	KTY-002	Sovelluksen tietoturva-asetukset	Sovelluksen asennuksen yhteydessä sovelluksen tietoturvallisuuteen vaikuttavat asetukset huomioidaan ja oletusasetukset vaihdetaan. Lisäksi sovelluksesta kirjoitetaan niin sanottu kovennusdokumentti, jossa kuvataan miten sovelluksen asetukset vaikuttavat tietoturvallisuuteen. Kovennuksessa ja dokumentaatiossa huomioitavia asioita ovat ainakin: • Oletusarvoiset salasanat ja käyttäjätunnukset • Hallintaliittymien näkyvyys • Vianselvitysominaisuuksien poistaminen • Mahdollinen testidata • Salauksen aktivointi, organisaation itsensä allekirjoittamien varmenteiden (ns. self signed certificate) poisto ja luotettujen sertifikaattien myöntäjien varmenteiden käyttöönotto. • Salaussertifikaattien elinkaaren seuranta ja uusien hankinta ennen voimassaolon päättymistä • Tietoturvallisuuteen vaikuttavat sovellusasetukset ja niiden vaikutukset (ei liian laajoja suoritusoikeuksia sovelluksille).	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	KTY-003	Sovelluksen säilyttämä tieto	Sovelluksen käyttöönotossa tulee huomioida sovelluksen käsittelemän tiedon asettamat vaatimukset. Sovelluksen omistaja määrittelee käsitellyn tiedon suojaustason. Käyttöönoton vaatimat tietoturvallisuuteen liittyvät toimenpiteet on organisoitu ja vastuutettu.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.3.1	Ei
	KTY-004	Organisaation riskikartan päivitys	Sovelluksen aiheuttamat riskit organisaation toiminnalle tulee viimeistään tässä vaiheessa viedä osaksi organisaation laajuista riskienhallintaprosessia ja riskikarttaa.		Suositus	Vahva suositus		Ei
	KTY-005	Asennus-dokumentaatio	Sovelluksen asennuksesta on olemassa kirjallinen dokumentaatio, jossa kuvataan sovelluksen käsittelemän tiedon asettamat tietoturva-asetukset eri tasoilla. Lisäksi dokumentissa tulee kuvata tarvittavat toimenpiteet silloin, kun sovellus siirtyy ympäristöstä toiseen tai pois organisaation hallinnasta. Dokumentin ylläpito ja päivittäminen on organisoitu ja vastuutettu. Dokumentissa pitää kuvata ainakin seuraavat asiat: • Sovelluksen sisältämä tieto (tietokannat jne.) • Käytetyt tietoturvaratkaisut eri suojaustasoilla • Tietokantojen, massamuistien tyhjennysprosessi.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus	2.3.3	Kyllä

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
14. Ylläpito	YLP-001	Tietoturvapäivitykset	Kriittiset tietoturvapäivitykset tunnistetaan ja asennetaan. Kaikki sovellukset tarvitsevat suuren määrän ulkoisia komponentteja, kuten käyttöjärjestelmä, sovelluspalvelin, tietokannat, kirjastot jne. Näiden komponenttien tietoturvapäivitysten seuraaminen ja kriittisten päivitysten asentaminen tulee olla organisoitua ja vastuutettua.	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	YLP-002	Komponenttien elinkaaren seuranta	Sovelluksen käyttämien komponenttien elinkaarta on seurattava. Päivitysprosessi uuteen versioon siirtymiseksi on aloitettava hyvissä ajoin ennen tukiajan päättymistä.		Vahva suositus	Pakollinen vaatimus		Ei
	YLP-003	Tietokannan muokkaaminen	Mikäli tuotannossa olevan sovelluksen tietokannassa säilyttämää tietoa joudutaan muokkaamaan ohi sovelluksen normaalin toiminnan, tulee menettely hyväksyttää sovelluksen omistajalla. Lisäksi operaatiosta tulee jäädä merkintä tietokannan lokiin.	Vahva suositus	Vahva suositus	Pakollinen vaatimus		Ei
	YLP-004	Virhetilanteiden dokumentointi	Sovelluksen tyypillisimmät virhetilanteet ja tarvittavat toimenpiteet niiden ratkaisemiseksi tulee olla dokumentoituna. Jos mahdollisia virhetilanteita on paljon, tulee dokumentoitavat virhetilanteet priorisoida sen mukaan, mikä niiden vaikutus on liiketoiminnalle. Jokaisesta virhetilanteesta tulee kuvata: • Käyttäjälle näytettävä virheviesti • Kriittisyys ja seuraukset • Toimintatapa korjaamiseksi • Mitä tehdä jos korjaaminen ei onnistu? Dokumentin katselmointi ja päivittäminen on vastuutettu ja organisoitu.	Suositus	Vahva suositus	Vahva suositus		Ei
	YLP-005	Sovelluksen päivittäminen	Sovelluksen tietoturvapäivitysten ja korjauksien asennus on dokumentoitu. Dokumentin katselmointi ja päivitys on organisoitu ja vastuutettu. Dokumentin pitää kuvata ainakin seuraavat asiat: • Päivitysten toimittaminen, päivityssykli • Kriittisten päivitysten toimittaminen • Päivitysten asennusmenettely • Varmuuskopiointi • Varmuuskopioiden palauttaminen.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.3.1	Kyllä
	YLP-006	Päivitysten luokittelu	Organisaatiolla on suunnitellut periaatteet, joiden mukaan päätetään, millaiset tietoturvapoikkeamat luokitellaan kriittisiksi ja on siten korjattava välittömästi. Periaatteissa määritellään myös, miten tietoturvapuutteet luokitellaan riskianalyysin mukaan. Organisaatio on vastuuttanut tietoturvapäivitystarpeen seurannan, korjausten toteutuksen ja asentamisen.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus	2.3.3	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	Viite ohjeeseen	Vaatimuskohde	Kuvaus	Perustaso	Korotettu taso	Korkea taso	Vahti 2/2010	Tarjous-pyyntöön
	YLP-007	Tietoturvapuutteista raportointi	Organisaatio tarjoaa asiakkaalle ja muille sidosryhmille keinon raportoida vakavista tietoturvapuutteista ja haavoittuvuuksista. Kontaktipiste tiedotetaan sopimuksissa ja esimerkiksi organisaation verkkosivuilla. Organisaatio on vastuuttanut tietoturvaraporttien käsittelyn, jolloin jokaiselle raportille määritellään omistaja joka on vastuussa seuraavista asioista: • Poikkeamien käsittely • Ensivastine, vahingon minimointi • Poikkeaman selvittäminen • Raportointi johdolle ja sidosryhmille. Raportoituihin vakaviin puutteisiin reagoidaan ja korjaus toteutetaan ilman tarpeetonta viivyttelyä. Vakavista poikkeamista pidetään kirjaa ja organisaation johtoa tiedotetaan niistä.	Suositus	Vahva suositus	Pakollinen vaatimus		Tarvittaessa
	YLP-008	Sovelluksen varmuuskopiointi	Ainakin sovelluksen käsittelemät tiedot ja sovelluksen konfiguraatiot on varmuuskopioitava säännöllisesti. Varmistusväli riippuu muun muassa sovelluksen sisältämän tiedon luokittelusta, sovelluksen kriittisyydestä jne. Varmistus pitää tehdä sovelluksesta riippumattomalle järjestelmälle, magneettinauhalle tai varmistuslevyjärjestelmälle. Tällöin sovelluksen vioittuminen ei vaaranna varmistusten saatavuutta. Varmistusten palautusmenettely pitää kuvata järjestelmän toipumissuunnitelmassa. Varmuuskopioista syntyy kirjallinen raportti, joista järjestelmän omistaja tai muu vastaava taho tarkistaa varmistuksen onnistumisen. Varmistuksia on säilytettävä eri palotilassa, kuin varsinaisia sovelluksen tietoja. Sovelluksesta tulee kirjoittaa dokumentti, jossa kuvataan mitkä tiedot sovelluksesta tulee vähintään varmistaa. Dokumentissa kuvataan myös varmuuskopiointimenettely. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu."	Vahva suositus	Pakollinen vaatimus	Pakollinen vaatimus		Kyllä
	YLP-009	Lisenssien hallinta	Sovelluksen käyttämien kolmansien osapuolten lisenssit ja vastaavat ovat ajan tasalla. Lisenssien ajantasaisuutta seurataan.	Suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	YLP-010	Päivitysprosessi	Organisaatiolla on sovelluksen toimintaympäristöön kohdistuva päivitysten hallintaprosessi. Prosessi on dokumentoitu ja dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu. Sisältönä esimerkiksi: • Tavoiteajat eri vakavuusluokan päivitysten asentamiselle • Huoltoikkunoiden määrittelyt • Roolit ja vastuualueet • Testiympäristön käyttö • Asennusprosessin kuvaus, miten toimia jos asennus ei onnistu (rollback-prosessi).	Suositus	Pakollinen vaatimus	Pakollinen vaatimus	2.3.4	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
	YLP-011	Asetusten auditointi	Sovellusympäristön tietoturvallisuuteen vaikuttavat asetukset tarkastetaan säännöllisesti. Havaittujen poikkeamien korjaaminen vastuutetaan sekä korjaamisen onnistumista seurataan. Auditoinnissa tarkastetaan muun muassa seuraavat asiat: • Käyttöjärjestelmien ja varusohjelmistojen tietoturvapäivitysten tilanne • Käyttäjätunnukset ja salasanat • Pääsy luottamukselliseen tietoon tiedostojärjestelmätasolla • Lokiasetukset käyttöjärjestelmätasolla. Ohjeena auditoinnissa voidaan käyttää esimerkiksi CIS:n standardeja.	Suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	YLP-012	Tietoturvapoikkeamien käsittelyprosessi	Tietoturvapoikkeamien käsittelyprosessi on dokumentoitu. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu. Prosessi voi ottaa kantaa esimerkiksi seuraaviin asioihin: • Henkilöt ja vastuualueet • Vahingon minimointi (triage) • Selvittäminen (forensics) • Tiedottaminen johdolle ja organisaation sisällä • Raportointi sidosryhmille.		Suositus	Vahva suositus		Ei
	YLP-013	Tietoturva-poikkeamista tiedottaminen	Joissain tilanteessa voi olla tarpeen tiedottaa tietoturvapoikkeamista julkisesti. Tällöin organisaation tulee kehittää ja dokumentoida tiedottamisprosessi. Dokumentin katselmointi ja päivittäminen tulee organisoida ja vastuuttaa. Tiedottaminen voi olla tarpeellista esimerkiksi: • Jos kehitettyä sovellusta käytetään organisaation ulkopuolella, tai asiakkaisiin ei ole suoraa kontaktia (esimerkiksi COTS-ratkaisut) • Jos lait, asetukset tai muut määräykset vaativat tiedottamista (esimerkiksi henkilötiedot).		Suositus	Vahva suositus		Ei
	YLP-014	Dokumentoitu raportoitiprosessi	Korotetun tason sovelluksilla tietoturvapoikkeamien raportointimenettelyn on oltava dokumentoitu. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu. Lisäksi tietoturvapoikkeamaraportille tulee olla ennalta määritelty dokumenttipohja. Pohjan tulee sisältää ainakin seuraavat asiat: • Raportoivan henkilön yhteystiedot • Poikkeaman yhteenveto • Poikkeaman ja raportoinnin aikajana • Poikkeaman tekniset yksityiskohdat: tikettinumero, tehdyt muutokset, poikkeaman toistamisen askeleet • Yhteenveto; poikkeaman syy, vaikutus, seuraukset.		Suositus	Vahva suositus		Ei
	YLP-015	Jälkikäteisanalyysi	Sovelluksessa havaitut tietoturvapoikkeamat ja -puutteet analysoidaan jälkikäteen kun korjaus on toteutettu ja toimitettu. Analyysissä pyritään selvittämään puutteen juurisyy ja määrittelemään korjaavat toimenpiteet. Toteutus- ja toimitusprosessia korjataan tarvittaessa samanlaisten ongelmien välttämiseksi tulevaisuudessa.		Pakollinen vaatimus	Pakollinen vaatimus	1.1.5.4	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	Viite ohjeeseen	Vaatimuskohde	Kuvaus	Perustaso	Korotettu taso	Korkea taso	Vahti 2/2010	Tarjous-pyyntöön
	YLP-016	Muutoshallinta	Sovelluksen päivitys- ja muutosperiaatteet on dokumentoitu. Dokumentin katselmointi ja päivittäminen on vastuutettu. Dokumentissa tulee kuvata ainakin: • Roolit ja vastuuhenkilöt • Muutosten luokittelu • Eri muutosluokkien vaatimat toimenpiteet (esimerkiksi ympäristö, lokitus, versionhallinta) • Muutosprosessin yksityiskohtainen kuvaus.		Pakollinen vaatimus	Pakollinen vaatimus	2.4.6	Kyllä
	YLP-017	Lokien seuranta	Sovelluksen tuottamaa lokia tarkkaillaan aktiivisesti joko automaattisella lokienhallintaohjelmistolla tai manuaalisesti. Lokien aktiivisella tarkkailulla väärinkäytökset tai hyökkäykset on mahdollista havaita jo niiden aikana. Lokien tarkkailun perusteella muodostetaan tietoturvallisuuden kokonaistilannekuvaa. Lisäksi lokien tarkkailun tuloksia käytetään toiminnan kehittämiseen, kuten uusien tietoturvaominaisuuksien suunnitteluun tai olemassa olevien parantamiseen.		Pakollinen vaatimus	Pakollinen vaatimus	2.11.4	Kyllä
	YLP-018	Kirjallinen varmuuskopiointi-politiikka	Sovelluksesta on kirjallinen varmuuskopiointipolitiikka ja -prosessi. Dokumenttien kirjoittamisessa on otettu huomioon sovelluksen käsittelemän tiedon asettamat vaatimukset sekä sovelluksen toimintaympäristön erityisvaatimukset. Dokumentaatiossa on huomioitu myös fyysisten varmuuskopioiden säilyttäminen, siirto ja tuhoaminen. Dokumentin katselmointi ja päivittäminen on organisoitu ja vastuutettu.		Pakollinen vaatimus	Pakollinen vaatimus	2.10.13	Ei
	YLP-019	Suojakopiot	Korotetun tason sovelluksesta on otettava edellä mainittujen varmuuskopiointivaatimusten lisäksi suojakopiot. Suojakopiot sisältävät sovelluksen datan lisäksi asennettavat sovellus- ja käyttöjärjestelmämediat, asennusohjeet jne. Suojakopioita säilytetään varmuuskopioista erillään erillisessä palotilassa, jotta niitä voidaan käyttää järjestelmän palauttamiseen jos varmuuskopioita ei jostain syystä voida käyttää.		Pakollinen vaatimus	Pakollinen vaatimus	2.10.14	Ei
	YLP-020	Verkkopohjainen turvamekanismi	Tuotantoympäristössä tulee olla käytössä mekanismi, jolla voidaan reagoida nopeasti yllättäviin tietoturvatilanteisiin ja estää siten hyökkäys. Tällainen mekanismi voidaan rakentaa esimerkiksi sovelluspalomuurilla.		Suositus	Vahva suositus		Tarvittaessa
	YLP-021	Palautusten testaaminen	Korkean tason sovelluksen varmuuskopioiden palauttamista tulee testata ja harjoitella säännöllisesti. Testauksessa saadaan usein selville palautusprosessin ongelmia, joita ei ole osattu ennustaa prosessia suunniteltaessa.			Pakollinen vaatimus	2.10.5	Ei
	YLP-022	Yhteenveto poikkeamista	Kaikista havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto. Yhteenvedosta havaittavia trendejä käytetään pohjana organisaation tietoturvatyön kehittämiselle sekä prosessien, strategian ja toimintatapojen kehittämiselle.			Pakollinen vaatimus	1.1.5.5	Ei
	YLP-023	Päivitysten seuraaminen	Sovelluksen tietoturvapäivitysten onnistumista ja päivitysten ajantasaisuutta seurataan. Seurannan tuloksia käytetään pohjana päivitys- ja korjausprosessin kehittämiselle.			Pakollinen vaatimus	2.4.7	Tarvittaessa
	YLP-024	Palautusten tilastointi	Korkean tason sovelluksesta tulee tilastoida palautettujen tietojen määrää sekä palautuksen syitä. Tilastoja tulee käyttää toiminnan parantamiseen ja puutteiden korjaamiseen. Lisäksi palautustilastojen antamaa informaatiota voidaan käyttää pohjana sovelluskehitysprosessin parantamiselle.			Pakollinen vaatimus	2.10.6	Ei

Vaatimustaulukko				Vaatimustaso: Suositus, Vahva suositus, Pakollinen vaatimus				
Alue	**Viite ohjeeseen**	**Vaatimuskohde**	**Kuvaus**	**Perustaso**	**Korotettu taso**	**Korkea taso**	**Vahti 2/2010**	**Tarjous-pyyntöön**
15. Käytöstä poisto	KTP-001	Tiedon arvonmäärittely	Sovelluksen sisältämälle tiedolle tulee tehdä arvonmääritys, jonka perusteella päätetään säilytetäänkö sovelluksen tietoa sen käytöstä poiston jälkeen.	Suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	KTP-002	Tiedon tuhoaminen	Käytöstä poistettavan sovelluksen tieto, jota ei säilytetä pysyvästi, on tuhottava tietoturvallisesti.	Pakollinen vaatimus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	KTP-003	Tiedon konvertointi	Säilytettävä tieto on konvertoitava muotoon, jota pystytään lukemaan myös tulevaisuudessa.	Suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei
	KTP-004	Säilytettävän tiedon luokittelu	Salassa pidettävä tieto tulee luokitella perusteluineen, jotta tietoa osataan käsitellä oikein passiivisessa arkistossa.	Suositus	Pakollinen vaatimus	Pakollinen vaatimus		Ei

LIITE 2. Lähdemateriaalin vaatimukset

Strategia ja resursointi

Vaatimus	Taso	Lähde
Organisaatioon on nimitetty tietoturvavastaava, jonka työnkuvassa on mainittu tietoturvavastuut.	Perustaso	VAHTI 2/2010
Tietoturvallisuuden avainroolit on tunnistettu ja niille on nimetty varahenkilö tai -henkilöt.	Perustaso	VAHTI 2/2010
Kaikkien tietoturvavastuita omaavien työnkuvissa vastuu on mainittu.	Korotettu taso	VAHTI 2/2010
4. Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi. Strategian on oltava organisaation ydintavoitteiden mukainen ja tuettava niiden saavuttamista.	Korotettu taso	VAHTI 2/2010

Politiikat

Vaatimus	Taso	Lähde
Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.	Perustaso	VAHTI 2/2010
Organisaatiolla on kirjallinen sovelluskehitysprosessi, joka ottaa kantaa kaikkiin sovelluskehityksen osa-alueisiin. Sovelluskehitysprosessi ja sen kehittäminen on vastuutettu ja organisoitu.	Perustaso	VAHTI 2/2010
Organisaatiossa on määritelty tehtävät tai roolit, joiden hakijasta tehdään turvallisuusselvitys, ja selvityksen hakuprosessi on dokumentoitu.	Perustaso	VAHTI 2/2010
Laitteiden, rekistereiden ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu.	Perustaso	VAHTI 2/2010
Organisaatiossa on kirjallinen lokienkeräys-, hälytys- ja seurantapolitiikka, joka on muodostettu ottaen huomioon toiminnan vaatimukset.	Korotettu taso	VAHTI 3/2009
Tietojärjestelmään saadaan asentaa tai liittää vain järjestelmän omistajan hyväksymiä ohjelmia ja laitteita.	Korotettu taso	VAHTI 2/2010
Organisaatiolla on käyttövaltuuspolitiikka	Korotettu taso	VAHTI 2/2010

Riskienhallinta

Vaatimus	Taso	Lähde
Organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia.	Perustaso	VAHTI 2/2010
Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä.	Perustaso	VAHTI 2/2010
Organisaatiossa tehdään ydintoimintojen tietoturvariskien arviointia vähintään vuosittain.	Korotettu taso	VAHTI 2/2010
Organisaatiolla on riskien arvioinnin menetelmä ja ohjeistus.	Korotettu taso	VAHTI 2/2010
Organisaatiolla on kirjallinen tietoturvasuunnitelma, joka määrittelee mitä teknisiä ja hallinnollisia toimia ja prosesseja organisaatiossa käytetään havaittujen tietoturvariskien hallitsemiseksi.	Korotettu taso	VAHTI 2/2010
Riskienarviointia tehdään myös suurten muutosten yhteydessä.	Korkea taso	VAHTI 2/2010
Organisaatiolla on riskienhallintapolitiikka.	Korkea taso	VAHTI 2/2010
Suurimmista riskeistä pidetään koko organisaation tasolla kirjaa ja riskienhallintatoimenpiteiden toteutumista seurataan.	Korkea taso	VAHTI 2/2010

Osaaminen ja koulutus

Vaatimus	Taso	Lähde
Ylläpitäjät ja käyttäjät saavat riittävän koulutuksen ohjelmiston hallintaan ja käyttöön. Sovellushankintaan ja -kehitykseen osallistujille on järjestetty riittävä tietoturvakoulutus. Riittävä koulutus määräytyy toteutettavan järjestelmän tason mukaan.	Perustaso	VAHTI 5/2004
Organisaatiossa järjestetään säännöllisesti tietoturvakoulutusta henkilöstölle ja muille avainryhmille. Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään.	Perustaso	VAHTI 2/2010
Työhön perehdytyksessä käsitellään myös tietoturva-asioita. Perehdytykseen on laadittu kirjallinen ohje, jossa on tarkistuslista käsitellyille asioille.	Perustaso	VAHTI 2/2010
Sääntöjen noudattamista seurataan ja poikkeamiin puututaan. Sääntöjen rikkomisen seuraukset on tiedotettu henkilöstölle.	Perustaso	VAHTI 2/2010
Organisaatiolla on kirjallinen tietoturvan koulutussuunnitelma. Koulutuksiin osallistumista valvotaan ja osaamistaso mitataan koulutuksen päätteeksi.	Korotettu taso	VAHTI 2/2010
Tietoturvakoulutuksessa otetaan huomioon organisaatiossa ja lähiympäristössä tapahtuneet muutokset ja tietoturvapoikkeamat.	Korkea taso	VAHTI 2/2010

Tekninen sovelluskehitysympäristö

Vaatimus	Taso	Lähde
Palvelut, sovellukset ja komponentit (kuten kirjastot) on kaikki luokiteltava niiden käsittelemien tietojen turvaluokituksen pohjalta.	Perustaso	VAHTI 5/2004

Jatkuvuudenhallinta

Vaatimus	Taso	Lähde
Organisaatiossa on yleinen toipumisstrategia ja suunnitelma tärkeimpien omien järjestelmien häiriöille, jossa on mm. johdon hyväksymä tärkeysjärjestys ICT-palveluille.	Perustaso	VAHTI 2/2010
Organisaatiolla on tärkeimmistä järjestelmistä kirjalliset toipumissuunnitelmat.	Korotettu taso	VAHTI 2/2010
Jatkuvuus- ja valmiussuunnitelmia ohjeineen testataan ja harjoitellaan säännöllisesti käytännön tasolla erityistilanteiden ja poikkeusolojen hallitsemiseksi.	Korkea taso	VAHTI 2/2009, VAHTI 2/2010
Järjestelmien häiriöistä ja niiden syistä pidetään kirjaa. Tietoa käytetään hyväksi riskianalyyseissä ja palvelutasosopimusten teossa.	Korkea taso	VAHTI 2/2010

Esitutkimus

Ei vaatimuksia ohjeen lähteistä.

Vaatimusmäärittely

Vaatimus	Taso	Lähde
Järjestelmän suunnittelu aloitetaan analyysillä siitä, mitä tietoa järjestelmällä käsitellään.	Perustaso	VAHTI 3/2010
Ennen toteuttamista sovellukseen ja sen toimintoihin tehdään riskiarviointi. Riskiarvioinnissa tulee huomioida erilaiset yleiset uhat, kuten haittaohjelmat, eritasoiset ulkopuoliset murtautujat ja sovelluksen käyttäjät.	Perustaso	KATAKRI, VAHTI 3/2010, VAHTI 2/2010, JHS 171
Sovelluksen vaatimusmäärittelyn tulee sisältää tietoturvaa koskevat vaatimukset. Vaatimusmäärittelyn tueksi tulee tehdä sovelluskohtainen riskianalyysi.	Perustaso	VAHTI 5/2004
Vaatimusten mukaiset tietoturvaratkaisut tulee dokumentoida yksityiskohtaisesti. Teknisen määrittelyn pohjalta voidaan todentaa ratkaisujen soveltuvuus ja riittävyys ja toisaalta tekninen määrittely toimii ohjeena sovelluksen toteuttajille	Perustaso	VAHTI 5/2004
Sovelluksen tietosisältöön tai toimintaan liittyvät lakisääteiset vaatimukset tulee huomioida.	Perustaso	KATAKRI II
Järjestelmään kohdistetaan riskianalyysi, jolla pyritään löytämään tietoturvavaatimukset tarjouspyyntöön, vaatimusmäärittelyyn tai uuden version asennuksen projektisuunnitelmaan.	Perustaso	VAHTI 2/2010
Hankkivalla organisaatiolla on tietoturvavaatimuksia sisältävä tietojärjestelmien arkkitehtuurilinjaus, jonka mukaisia hankittavien tai kehitettävien järjestelmien tulee olla.	Korotettu taso	VAHTI 2/2010

Suunnittelu

Vaatimus	Taso	Lähde
Arkkitehtuurin suunnittelussa huomioidaan eri ratkaisujen yhteensopivuus. Yleisesti käytettyjä ja hyväksyttyjä standardeja suositaan ja niiden käyttöä vaaditaan.	Perustaso	VAHTI 5/2004
Sovelluksen käyttämä tunnistautumismenetelmä valitaan sen sisältämän tiedon luokittelun perusteella. Sovelluksen omistaja hyväksyy, kuina luotettavaa identiteettiä ja vahvaa tunnistautumista sovelluksen käyttöön tarvitaan.	Perustaso	VAHTI 5/2004, VAHTI 2/2010
Mikäli sovellukseen kirjaudutaan käyttäjätunnus/salasanaparilla, tulee salasanan laatuvaatimukset olla konfiguroitavia ainakin seuraavilla parametreilla: salasanan pituus, ei-aakkosmerkkien lukumäärä, lukkiutuminen määräajaksi liian monen epäonnistuneen kirjautumisen jälkeen.	Perustaso	VAHTI 3/2010, VAHTI 2/2010, KATAKRI II
Käyttäjille on annettava vain tarvittavat oikeudet sovelluksiin. Samoin sovelluksia tulee aja vain tarvittavilla minimioikeuksilla.	Perustaso	VAHTI 5/2004
Huonolaatuisten salasanojen käyttöä estetään.	Perustaso	VAHTI 2/2010
Käyttö- ja ylläpitotunnusten tulee olla henkilö- ja roolikohtaisia.	Perustaso	KATAKRI II
Sovelluksen käyttäjänhallintamenettelyjen tulee varmistaa, että sovelluksen toimintaan vaikuttavien tietoturva-asetusten muokkaus on estetty peruskäyttäjiltä.	Perustaso	KATAKRI II,
VAHTI 2/2010	Perustaso	VAHTI 5/2004
Kaikki sovelluksen tai sovelluskomponentin ulkopuolelta tullut syöte on tarkastettava ennen käyttöä. Tarkistusvastuuta ei voi jättää esim. asiakasohjelmalle tai toiselle komponentille. Sähköisillä allekirjoituksilla voidaan myös varmistaa tiedon aitous ja muuttumattomuus siirron aikana.	Perustaso	VAHTI 5/2004
Sovellusistunto on toteutettava huolellisesti varmistaen, ettei istuntoa voida kaapata, väärentää eikä luvattomasti nauhoittaa ja toistaa. Joutilas istunto on aikakatkaistava ja aika on oltava määriteltävissä.	Perustaso	VAHTI 5/2004
Käyttäjätiedot on hallittava ajantasaisesti ja mahdollisimman keskitetysti. Hallintaprosessit ja työnkulku on dokumentoitava. Sovelluksiin liittyvät käyttäjätiedot on kyettävä kytkemään yhteiseen käyttäjähallintamenettelyyn.	Perustaso	VAHTI 5/2004
Järjestelmästä valmistuu kattava dokumentaatio, joka sisältää vaatimukset, määrittelyt, tuotevertailut, testisuunnitelmat, testiraportit, asennukset, turvakuvaukset jne.	Perustaso	VAHTI 5/2004
Mikäli järjestelmässä käytetään salausratkaisuja, tulee niiden olla hyväksytty kansallisen tai kansainvälisen tietoturvaviranomaisen toimesta tai niiden turvallisuuden tulee olla muuten varmistettu.	Korotettu taso	KATAKRI II
Tietoliikenne tulee salata käyttäjän laitteesta sovelluspalvelimelle. Sovelluksen tulee käyttää tunnistautumisessa menetelmiä, jossa tunnistautumiseen käytettävät arkaluontoiset tiedot, kuten salasanat eivät kulje verkon yli salaamattomana.	Korotettu taso	VAHTI 5/2004, VAHTI 3/2010, KATAKRI II
Aiemmin esitettyjen salasanavaatimusten lisäksi: • Pituus vähintään 10 merkkiä • Salasana on vaihdettava 90 päivän välein • Järjestelmä muistaa 10 viimeisintä salasanaa ja estää niiden käytön uudelleen • Sisällettävä kolmea seuraavista neljästä merkkiryhmästä: isot kirjaimet, pienet kirjaimet, numerot, erikoismerkit	Korotettu taso	VAHTI 3/2010
Mikäli sovellus rakentuu useammasta eri palvelusta (esim. tietokanta ja sovelluspalvelimet), tulee näiden väliset tietoliikennetarpeet dokumentoida ja mahdollistaa eri palveluiden sijoittaminen eri verkon segmentteihin.	Korotettu taso	VAHTI 3/2010
Sovelluksen tulee mahdollistaa hallinta- ja valvontaliikenteen erottamisen muusta liikenteestä verkkomielessä.	Korotettu taso	VAHTI 3/2010
Järjestelmään kirjautumiseen on käytettävä vahvaa tunnistautumista.	Korkea taso	KATAKRI II
Sovellus tulee kehittää käyttämällä monitasoarkkitehtuuria, jossa eri osat on sijoitettu eri palvelimille.	Korkea taso	VAHTI 3/2010

Toteutus

Vaatimus	Taso	Lähde
Sovelluksessa on varmistettava virhetilanteiden hallinta. Vakavassa tai yllättävässä virhetilanteessa sovelluksen tulee varmistaa, ettei ylimääräisiä tietoturvariskejä synny. Erityisesti tietoturvakomponenttien tulee noudattaa fail safe-mallia eli yllättävän virheen sattuessa komponentin ja sovelluksen käyttö estetään mieluummin kokonaan kuin annetaan mahdollisuus luvattomaan käyttöön.	Perustaso	VAHTI 5/2004
Sovelluksen tulee lokittaa epäonnistuneet kirjautumisyritykset sekä muut valtuuksien puutteeseen kariutuneet toimenpideyritykset siten, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti.	Perustaso	VAHTI 3/2010, VAHTI 2/2010
Sovellus lokittaa kirjausketjun kriittisistä ylläpitotoimista.	Perustaso	KATAKRI II, VAHTI 5/2004
Sovellus lokittaa kriittisen tiedon käsittelyn, sisältäen tiedon lukemisen.	Perustaso	KATAKRI II,
VAHTI 2/2010		
Sovelluksen tiedon käsittely, mukaan lukien tietojen katselu, on pystyttävä jäljittämään.	Perustaso	VAHTI 5/2004
Kaikkien lokiympäristöön kuuluvien laitteiden, kuten lokien lähde- ja keräysjärjestelmien kellojen tulee olla samassa ajassa, jotta tapahtumien tapahtumajärjestys on mahdollista selvittää. Käytännössä tämä tarkoittaa keskitetyn aikapalvelimen (NTP) käyttöä.	Perustaso	VAHTI 3/2009
Myös lokitietojen katselusta eli määriteltyjen käyttöoikeuksien käytöstä on pidettävä omaa lokia. Luonnollisesti myös oikeuksien ylitysyrityksistä tulee pitää kirjaa.	Korotettu taso	VAHTI 3/2009
Sovelluksen tulee mahdollistaa lokitus sellaiseen paikkaan, josta niitä ei päästä jälkikäteen muuttamaan esim. mahdollistamalla lokitus ulkoiselle lokituspalvelimelle.	Korotettu taso	VAHTI 3/2010, VAHTI 2/2010, VAHTI 3/2009, VAHTI 5/2004
Lokitiedostoista lasketaan tarkistussumma. Tarkistussumman laskemisella pyritään siihen, että arkistoituihin lokeihin tehdyt muutokset havaitaan.	Korkea taso	VAHTI 3/2009

Testaus

Vaatimus	Taso	Lähde
Tietoturvavastaava tarkastaa järjestelmän tietoturvasuunnitelman tai -suunnitelmat.	Perustaso	VAHTI 2/2010
Sovellus ja sen tietoturvallisuuden hallinnointi on auditoitava ennen käyttöönottoa. Auditoinnilla tarkoitetaan riippumattoman sisäisen tai ulkoisen toimijan tekemää sovelluksen tietoturvan teknistä ja hallinnollista tarkastusta.	Korotettu taso	VAHTI 5/2004, VAHTI 2/2010
Kehitys- tai räätälöintityön aikana järjestetään katselmointeja tietoturvallisuuden kannalta kriittisiin osiin ja katselmoinneista valmistuu pöytäkirja.	Korkea taso	VAHTI 2/2010

Käyttöönotto

Vaatimus	Taso	Lähde
Kaikissa asennuksissa huomioidaan tietoturvallisuus. Oletusarvoiset asennukset ymmärretään turvattomiksi. Sovelluksesta tehdään dokumentaatio, jossa kuvataan miten järjestelmä saadaan kovennettua.	Perustaso	VAHTI 5/2004, KATAKRI II
Tietojärjestelmän ja työasemien käyttöönottoasennuksessa ja käytöstä poistamisessa otetaan huomioon järjestelmän tietosisällön tietoturvavaatimukset	Perustaso	VAHTI 2/2010
Tietojärjestelmien ja työasemien käyttöönottoon ja käytöstä poistamiseen liittyvät toimenpiteet on vastuutettu ja organisoitu.	Perustaso	VAHTI 2/2010
Tietojärjestelmien ja työasemien ensiasennuksesta ja käytöstä poistosta on kirjallinen ohjeisto, jossa kerrotaan mm. eri turvatasoilla käytettävät tietoturva-asetukset sekä laitteiden käsittelyn ja massamuistien tyhjennyksen menettelyt silloin kun ne siirtyvät ympäristöstä toiseen tai kun ne poistuvat organisaation hallinnasta.	Korotettu taso	VAHTI 2/2010
Ohjeiden päivitys on vastuutettu ja organisoitu.	Korotettu taso	VAHTI 2/2010

Ylläpito

Vaatimus	Taso	Lähde
Ohjelmistojen käsittelemät tiedot ja ohjelmiston käyttöasetukset varmistetaan säännöllisesti.	Perustaso	VAHTI 5/2004
Varmistusten onnistuminen tarkastetaan raporttien pohjalta.	Perustaso	VAHTI 5/2004
Järjestelmästä tulee muodostaa dokumentaatio, jossa kuvataan, miten järjestelmän tiedot voidaan varmuuskopioida.	Perustaso	KATAKRI II
Ohjelmistolisenssit ovat ajan tasalla ja hallinnassa.	Perustaso	VAHTI 5/2004
Laitteiden ja tietojärjestelmien tietoturvapäivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus on vastuutettu ja organisoitu erityisesti tietoturvapäivitysten osalta.	Perustaso	VAHTI 2/2010
Organisaatiolla on periaatteet, jotka kertovat, millaiset päivitykset tai muutokset asennetaan välittömästi ja millaisiin päivityksiin ja muutoksiin käytetään riskitason huomioon ottavaa tarveharkintaa.	Perustaso	VAHTI 2/2010
Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa.	Perustaso	VAHTI 2/2010
Ohjelmistoille on saatavilla riittävät tuki- ja päivityspalvelut.	Perustaso	VAHTI 5/2004
Sovelluskehityksen yhteydessä tulee määritellä tapa, jolla sovelluksen ja sen alustan tietoturvapäivitykset pystytään tekemään.	Perustaso	VAHTI 3/2010
Korjaus- ja tietoturvapäivityksiä varten on oma dokumentoitu prosessinsa	Perustaso	VAHTI 5/2004
Tietoturvapoikkeamien raportointimenettely on kuvattu kirjallisesti ja siihen on määrämuotoinen pohja.	Korotettu taso	VAHTI 2/2009
Organisaation päivitys- ja muutosperiaatteet ovat kirjalliset.	Korotettu taso	VAHTI 2/2010
Tietoturvapoikkeamista tehdään jälkikäteisanalyysi ja käynnistetään tarvittavat korjaavat toimenpiteet tapahtuman uusiutumisen ehkäisemiseksi.	Korotettu taso	VAHTI 2/2010
Lokien seurannan perusteella muodostetaan tilannekuvaa ja havaitaan tietoturvapoikkeamia sekä kehitetään toimintaa.	Korotettu taso	VAHTI 2/2010
Organisaatiossa on kirjallinen varmuuskopiointipolitiikka ja -prosessi, jotka on muodostettu ottaen huomioon toiminnan vaatimukset ja joissa ohjeistetaan myös varmuus- ja suojakopioiden käsittely siirron ja varastoinnin aikana.	Korotettu taso	VAHTI 2/2010
Organisaatiossa otetaan tärkeimmistä järjestelmistä myös suojakopioita, joita säilytetään eri palotilassa kun varsinaisia varmuuskopioita.	Korotettu taso	VAHTI 2/2010

Vaatimus	Taso	Lähde
Havaituista tietoturvapoikkeamista tehdään vuosittain yhteenveto.	Korkea taso	VAHTI 2/2010
Päivitysten ajantasaisuutta ja onnistumista mitataan ja seurataan.	Korkea taso	VAHTI 2/2010
Eri järjestelmien varmuuskopioiden palautusta testataan säännöllisesti.	Korkea taso	VAHTI 2/2010
Varmuuskopioilta palautettavien tietojen määrää ja palautuksen syitä tilastoidaan.	Korkea taso	VAHTI 2/2010
Varmuuskopioilta palautettavien tietojen määrää ja palautuksen syitä tilastoidaan.	Korkea taso	VAHTI 2/2010

Käytöstä poisto

Ei vaatimuksia ohjeen lähteistä.

LIITE 3. Voimassa olevat VAHTI -julkaisut

VAHTI 1/2013	Sovelluskehityksen tietoturvaohje
VAHTI 3/2012	Teknisen ICT-ympäristön tietoturvataso-ohje
VAHTI 2/2012	ICT-varautumisen vaatimukset
VAHTI 1/2012	VAHTIn toimintakertomus vuodelta 2011
VAHTI 3/2011	Valtion ICT-hankintojen tietoturvaohje
VAHTI 2/2011	Johdon tietoturvaopas
VAHTI 4/2010	Sosiaalisen median tietoturvaohje
VAHTI 3/2010	Sisäverkko-ohje
VAHTI 2/2010	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
VAHTI 7/2009	Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä
VAHTI 6/2009	Kohdistetut hyökkäykset
VAHTI 5/2009	Effective Information Security
VAHTI 4/2009	Information Security Instructions for Personnel
VAHTI 3/2009	Lokiohje
VAHTI 2/2009	ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin
VAHTI 9/2008	Hankkeen tietoturvaohje
VAHTI 8/2008	Valtionhallinnon tietoturvasanasto
VAHTI 7/2008	Informationssäkerhetsanvisningar för personalen
VAHTI 6/2008	Tietoturvallisuus on asenne - Selvitys julkishallinnon tietoturvakoulutustarpeista
VAHTI 5/2008	Valtion ympärivuorokautisen tietoturvavalvonnan hanke-esitys
VAHTI 4/2008	Valtionhallinnon tietoturva-arviointipoolin toimintaraportti
VAHTI 3/2008	Valtionhallinnon salauskäytäntöjen tietoturvaohje
VAHTI 2/2008	Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta
VAHTI 3/2007	Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan
VAHTI 2/2007	Älypuhelimien tietoturvallisuus
VAHTI 1/2007	Osallistumisesta vaikuttamiseen – valtionhallinnon haasteet kansainvälisessä tietoturvatyössä
VAHTI 12/2006	Tunnistaminen julkishallinnon verkkopalveluissa
VAHTI 11/2006	Tietoturvakouluttajan opas
VAHTI 10/2006	Henkilöstön tietoturvaohje
VAHTI 9/2006	Käyttövaltuushallinnon periaatteet ja hyvät käytännöt
VAHTI 8/2006	Tietoturvallisuuden arviointi valtionhallinnossa
VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen

VAHTI 5/2006	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006	Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006	Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006	Electronic-mail Handling Instruction for State Government
VAHTI 3/2005	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005	Information Security and Management by Results
VAHTI 5/2004	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004	Datasäkerhet och resultatstyrning
VAHTI 3/2004	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004	Tietoturvallisuus ja tulosohjaus
VAHTI 7/2003	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 3/2003	Tietoturvallisuuden hallintajärjestelmän arviointisuositus
VAHTI 2/2003	Turvallinen etäkäyttö turvattomista verkoista
VAHTI 1/2003	Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 3/2002	Valtionhallinnon etätyön tietoturvaohje
VAHTI 1/2002	Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 4/2001	Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti-ohjeet

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 Valtioneuvosto
Puhelin 0295 160 01
Telefaksi 09 160 33123
www.vm.fi

1/2013
VAHTI
Tammikuu 2013

ISSN 1455-2566 (nid.)
ISBN 978-952-251-417-2 (nid.)
ISSN 1798-0860 (pdf)
ISBN 978-952-251-418-9 (pdf)