Taneli Gröhn

Ohjelmistorobotiikan tietoturvan kehittäminen viitekehyksien avulla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikka

Insinöörityö

10.5.2022

Tiivistelmä

Tekijä:	Taneli Gröhn
Otsikko:	Ohjelmistorobotiikan tietoturvan kehittäminen viitekehyksien avulla
Sivumäärä:	40 sivua
Aika:	10.5.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Ohjelmistotuotanto
Ohjaajat:	Janne Salonen

Ohjelmistorobotiikka on kansainvälisesti kasvava ala. Jopa yli puolet eurooppalaisista yrityksistä suunnitteli automatisoivansa liiketoiminnallisia prosessejaan vuoteen 2020 mennessä. Robotic Process Automation -ratkaisujen yleistyessä ohjelmistorobotiikan tietoturvan kysymykset nousevat esille yhä useammin. Ohjelmistorobotiikan tietoturvasta ja erityisvaatimuksista löytyvä tutkimus ja kirjallisuus on kuitenkin kohtalaisen vähäistä, eikä ohjelmistorobotiikan tietojärjestelmille löydy räätälöityjä tietoturvaratkaisuja tai viitekehyksiä.
Työssä tutustutaan ohjelmistorobotiikan tietoturvan yleisiin aiheisiin sekä siihen, kuinka tunnettuja tietoturvallisuuden viitekehyksiä on mahdollista soveltaa ohjelmistorobotiikan kontekstissa. Sopiviksi viitekehyksiksi valittiin VAHTI-ohje ja Katakri, joiden pohjalta johdettiin vaatimuksia ohjelmistorobotiikan tietoturvallisuudelle.

Avainsanat: RPA, ohjelmistorobotiikka, tietoturva, viitekehykset

Abstract

Author:	Taneli Gröhn
Title:	Improving information security of RPA applications with common frameworks
Number of Pages:	40 pages
Date:	10 May 2022
Degree:	Bachelor of Engineering
Degree Programme:	Information and communication technology
Professional Major:	Software engineering
Supervisors:	Janne Salonen, Head of School (ICT)

Robotic process automation is an internationally growing trend as over half of European IT companies were planning to automate their business processes before the year 2020. The increasing number of RPA-implementations has raised concerns over the security of robotic process automation. The subject of IT security in RPA has not been researched extensively and there are no subject specific security frameworks for RPA.

This paper focuses on the basics of robotic process automation and what risks it can create, how common IT security frameworks can be applied to RPA and what requirements should be implemented and how from the chosen frameworks. The chosen frameworks where VAHTI-ohje and Katakri created by the Finnish government on which the requirements listed in this paper were derived from.

Keywords: RPA, robotic process automation, information security, frameworks

Sisällys

Lyhenteet

RPA: engl. Robotic Process Automation. Ohjelmistorobotiikka. Kattotermi prosessien ja ohjelmistojen automatisoinnille.

KATAKRI: Kansallinen turvallisuusauditointikriteeristö. Viranomaisten tietoturvallisuuden auditointityökalu.

VAHTI: Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI.

1 Johdanto

Digitalisaation edetessä yhä useampi yritys siirtää liiketoiminnallisia prosesse-jaan perinteisestä paperien pyörittelystä sähköisiin tietojärjestelmiin [1]. Prosessien siirtyminen sähköisiin tietojärjestelmiin ei kuitenkaan välttämättä paranna merkittävästi yritysten toiminnan tehokkuutta, sillä useat työläät prosessit vaativat digitalisoitunakin ihmisten työpanosta. Näiden työläiden prosessien automatisointiin voidaankin käyttää RPA, eli Robotic Process Automation, ratkaisuja. RPA:n avulla yritykset voivat automatisoida liiketoiminnallisia prosesseja ja erityisesti suoraa arvoa tuottamattomia hallinnollisia prosesseja. Yritykset voivatkin saavuttaa merkittäviä hyötyjä oikeaoppisella RPA:n toteutuksella. Prosesseille varattuja henkilöresursseja voidaan vapauttaa mielekkäämpiin tehtäviin, prosessien suoritusajat lyhenevät ja prosessit muuttuvat parhaimmillaan läpinäkyvämmiksi robottien lokitusten ja auditoinnin avulla [1]. Ei olekaan yllätys, että hyvin monet eurooppalaiset yritykset suunnittelevat prosessiensa automatisointeja RPA:n avulla [1].

Ohjelmistorobotiikan yleistyessä ja saavuttaessa suurempaa suosiota, herää väistämättä kysymys, onko ohjelmistorobotiikka riskitöntä? Vastaus tähän kysymykseen on ei. Ihmisten korvaaminen roboteilla liiketoiminnallisissa prosesseissa tuo väistämättä riskejä [2], joihin täytyy varautua. Eettisten kysymysten lisäksi tieto- ja kyberturvallisuus tulee aina ottaa huomioon korvattaessa ihmisiä ohjelmistorobotiikalla. Ohjelmistorobotiikan tieto- ja kyberturvallisuuden riskienhallinta onkin yksi RPA:n tunnistetuista tutkimuskysymyksistä [2].

Tässä työssä esitetään vaatimuksia ja toimenpiteitä, joiden avulla organisaatiot voivat arvioida ohjelmistorobotiikansa tietoturvaa. Tavoitteena on tehdä selvitystyötä ohjelmistorobotiikan kontekstiin sopivista tietoturvan viitekehyksistä, sekä siitä, mitkä näistä viitekehysten vaatimuksista tulisi toteuttaa erityisesti ohjelmistorobotiikan palveluntarjoajan näkökulmasta. Työssä tutustutaan ensin ohjelmistorobotiikan perusteisiin ja yleisimpiin tietoturvariskeihin. Perusteiden jälkeen tutustutaan siihen, mitä tietoturvallisuuden viitekehyksiä on olemassa ja kuinka niitä voisi soveltaa ohjelmistorobotiikan kontekstissa. Lopuksi työssä esitetään esimerkkivaatimuksia valittujen tietoturvallisuuden viitekehysten pohjalta.

2 Ohjelmistorobotiikan perusteet

Työssä käsitellään ohjelmistorobotiikan tietoturvaa, joten työn kannalta on ensiarvoisen tärkeää ymmärtää ohjelmistorobotiikan peruskonseptit, -käsitteet, käyttötapaukset ja yleisimmät teknologiat. Työ ei vaadi lukijaltaan syvällistä perehtymistä ohjelmistorobotiikkaan, mutta perustason tietämyksen avulla työssä käsiteltävät tietoturvan aiheet ovat helpompia hahmottaa ohjelmistorobotiikan kontekstissa.

2.1 Mitä on ohjelmistorobotiikka

Ohjelmistorobotiikalla, eli RPA:lla (engl. Robotic Process Automation), tarkoitetaan aikaisemmin ihmisten suorittamien prosessien automatisointia erinäisillä teknologioilla ja työkaluilla [1]. Ohjelmistorobotiikan työkaluilla operoidaan tietojärjestelmiä ja järjestelmien käyttöliittymiä ihmisten toimintaa imitoiden. Useimmiten ohjelmistorobotiikan avulla pyritään automatisoimaan toistuvia ja yksinkertaisia prosesseja [2], mutta automatisoitavat prosessit voivat olla tilanteesta ja tapauksesta riippuen hyvinkin monimutkaisia.

RPA:n yhteydessä automatisoinneilla tarkoitetaan ihmisen toiminnan korvaamista ulkoisella agentilla ulkoa-sisään (engl. outside-in) -periaatteella. Ulkoa-sisään-periaatetta noudatettaessa kohdejärjestelmään ei tehdä muutoksia automatisointeja toteutettaessa, vaan agentti käyttää järjestelmää ihmisen toimintoja simuloiden. [2.]

Ohjelmistorobotiikan avulla automatisoitavat prosessit täytyvät olla luonteeltaan sääntöperustaisia, standardoituja ja toistettavia [1]. Prosessia on hyvin haastava tai lähes mahdotonta automatisoida, mikäli prosessin suorittamiseen vaadittavat askeleet vaihtuvat usein tai mikäli prosessi vaatii inhimillistä päätöksentekoa. Automatisoinneissa tulisi myös ottaa huomioon prosessien toistuvuus. Harvoin toistuvien prosessien automatisoinneilla saavutetaan harvoin haluttua tulosta automaatioratkaisujen hintaan suhteutettuna [2].

Yksinkertaisena esimerkkinä ohjelmistorobotiikasta voidaan kuvitella seuraava tilanne: Työntekijä vastaanottaa sähköpostiinsa ilmoituksen tuotteen uudesta tilauksesta. Hän syöttää viestin sisältämän asiakkaan tiedot asiakastietojärjestelmään ja poistaa viestin sähköpostistansa. Uusia tilauksia tulee arviolta 30–40 kappaletta päivässä, joten työntekijä joutuu käyttämään suuren osan ajastaan asiakkaiden tietojen kirjaamiseen. Kyseinen prosessi on oivallinen ehdokas automatisoinnille ohjelmistorobotiikan avulla prosessin lineaarisuuden ja toistuvuuden vuoksi [2]. Työntekijä tilaa yritykseltä RPA-palvelun ja selostaa yrityksen edustajalle automatisoitavat prosessit askel askeleelta. Yritys tuottaa työntekijällä prosessille räätälöidyn automatisaation, joka tekee ohjelmallisesti asiakkaan kirjaamiseen vaaditut askeleet. Ohjelmistorobotiikan avulla työntekijän ei enää tarvitse käyttää aikaa asiakkaiden kirjaamiseen, mikäli automaatio toimii odotetusti ja sähköpostiin saapuva asiakasdata on sovitun standardin mukaista.

2.2 Mihin ohjelmistorobotiikkaa tarvitaan

Ohjelmistorobotiikan implementoinnin pääsääntöisinä tavoitteina ovat kulujen karsiminen ja kustannustehokkuus. Automatisoitavat prosessit ovat useimmiten työläitä, toistuvia ja jopa pitkäveteisiä, joten työn siirtämisellä robotin vastuulle voidaan vapauttaa huomattava määrä työntekijöiden resursseja muihin mielekkäämpiin tehtäviin. [1.]

Ohjelmistorobotiikan automatisoituja prosesseja suorittavat sovelluskomponentit, eli robotit tuovat onnistuneessa implementaatiossa muitakin työn laatua parantavia ominaisuuksia.

Devarajan [3] luettelee tutkimuksessaan yleisiä ohjelmistorobotiikan hyötyjä:

- Robotit pyörivät tarvittaessa vuoden jokaisena päivänä kellon ympäri ilman taukoja tai lomia, mikä itsessään voi tuoda yritykselle merkittävää taloudellista hyötyä.
- Robotit eivät väsy, ja työn laatu säilyy tasaisena suoritusten välillä.
- Ohjelmistorobotiikalla voidaan varmistaa lähdemateriaalin laatu ja parantaa prosessin läpinäkyvyyttä. Oikein määritelty robotti havaitsee poikkeuksetta virheet materiaalissa.

- Robotit suorittavat ainoastaan niille annettuja ohjeita, eivätkä ne poikkea ennalta määritetystä prosessista.

Robotit toimivat manuaalisen työn ja ohjelmistojen lähdekooditason automatisointien välimaastossa. Robotit imitoivat ihmisten toimintaa ohjelmistojen ja sovellusten esitystasolla, jolloin yritysten ei tarvitse investoida suuria määriä rahaa vanhojen tai nykyaikaistenkin ohjelmistojen jatkokehittämiseen ja ylläpitoon [3]. Ohjelmistorobotiikka voikin toimia oikein toteutettuna siltana ihmisten tekemän työn ja laajamittaisten ohjelmistojen automatisointien välillä [2]. Edellä mainituista syistä ohjelmistorobotiikkaan sijoittamalla on mahdollista saavuttaa merkittävää tuottoa hyvinkin nopeasti [1].

2.3 Ohjelmistorobotiikan teknologiat

Tällä hetkellä markkinoilta löytyy laaja kirjo prosessien automatisointiin käytettäviä sovelluksia, joista jokainen sopii parhaiten omanlaiseensa käyttötarkoitukseen tai tavoitteeseen [2]. Ohjelmistorobotiikan sovelluksia tarjoaa muun muassa UiPath, Blue Prism ja Automation Anywhere [1].

Prosessiautomaatio-ohjelmistoja tarjoavien yritysten tuotteet poikkeavat teknisellä tasolla toisistaan, mutta näiden ohjelmistojen yleinen käyttötarkoitus on sama, eli prosessien automatisointi. Yleistetysti, ohjelmistorobotiikan työkalut tarjoavat intuitiivisia käyttöliittymiä, joiden avulla kehittäjät voivat koota erinäisistä konfiguroitavista moduuleista ja loogisista operaatioista sekvenssin, eli automaation, ohjelmistorobotin suoritettavaksi [2].

3 Ohjelmistorobotiikan tietoturvariskit

Yritykset adoptoivat ohjelmistorobotiikan toimintoja ja palveluita IT-ekosysteemeihinsä kiihtyvää tahtia ja vuonna 2018 arvioitiin, että jopa 54% eurooppalaisista yrityksistä suunnitteli automatisoivansa vähintään kymmenen prosessia vuoteen 2020 mennessä [2]. On kuitenkin syytä kysyä, kuinka suuri osa näistä yrityksistä huomioi ohjelmistorobotiikan tietoturvan erityisvaatimukset ja vaikutukset organisaation tietoturvan kokonaistasolle. Prosessien oikeaoppinen automatisointi voi parhaimmillaan parantaa organisaation tietoturvaa [3], mutta RPA-toteutukset voivat olla hyökkääjille houkuttelevia kohteita robottien käsittelemän tiedon ja pääsyoikeuksien vuoksi.

3.1 Automatisoitavien prosessien luokittelu

Automatisoitavien prosessien tyyppi ja luonne tulisi ottaa huomioon ohjelmistorobotiikkaa implementoitaessa. Automatisaation kandidaattiprosesseja on olemassa laaja kirjo, ja niistä jokaisella on omanlaisensa vaikutus organisaation kokonaisturvallisuudelle. Luokitellaan prosesseja esimerkin vuoksi kolmeen ohjeelliseen luokkaan prosessin arvioidun riskitason mukaan, eli

- matalan riskin prosesseihin
- kohtalaisen riskin prosesseihin
- huomattavan riskin prosesseihin.

Ohjeellinen luokittelu on toteutettu McGrawin *Risk Analysis in Software Design* [4] artikkelissa esiteltyjen riskianalyysi-metodien perusteella. Prosessin aikana tarvittavat resurssit, käytettävät materiaalit, käyttöoikeudet ja suoritusympäristöt vaikuttavat suoraan automaation arvioituun riskitasoon. Prosesseja arvioitaessa on myös syytä huomioida riskin realisoitumisen todennäköisyys, uhkatekijät ja mahdolliset vahingot riskin realisoituessa. [4.]

Matalan riskin prosesseiksi voidaan luokitella yksinkertaiset prosessit, joissa

- ei lueta, käsitellä tai tallenneta arkaluontoista tietoa

- ei käytetä käyttäjätunnuksia ulkoisissa tai sisäisissä järjestelmissä
- toimitaan rajoitetussa ympäristössä rajoitetuilla oikeuksilla
- toimitaan paikallisesti työasemalla käyttäjän välittömässä valvonnassa.

Matalan riskin prosessiksi voidaan laskea esimerkiksi uuden Excel-tiedoston alustaminen haluttuun muotoon, julkisen tiedon käsittely laskentataulukossa tai hotellien hintatietojen louhiminen julkiselta verkkosivulta. Matalan riskin prosesseilla on hyvin vähäiset mahdollisuudet aiheuttaa haittaa organisaation toiminnalle tai turvallisuudelle prosessin rajoitetun toimintaympäristön, käsiteltävän materiaalin luokituksen tai käyttöoikeuksien vuoksi.

Kohtalaisen riskin prosessit ovat prosesseja, joissa

- luetaan, käsitellään tai tallennetaan arkaluontoista tietoa, muttei henkilötietoja
- kirjaudutaan käyttäjätunnuksilla ulkoisiin tai sisäisiin järjestelmiin
- toimitaan ympäristössä itsenäisesti prosessia varten määritellyillä käyttöoikeuksilla
- käytetään työaseman ulkopuolisia resursseja, sovelluksia tai palveluita, kuten jaettuja verkkolevyjä tai sisäverkon sovelluksia.

Kohtalaisen riskin prosesseiksi voidaan laskea esimerkiksi huonevarausten siirtäminen sähköpostista hallintajärjestelmään, liiketoiminnallisesti tärkeiden tiedostojen lajittelu työasemalta verkkolevyn kansioihin tai sähköisten laskujen hakeminen verkkopalvelusta. Näillä prosesseilla on selkeä mahdollisuus aiheuttaa liiketoiminnallista vahinkoa organisaatioille riskin realisoituessa, mutta mahdollinen vahinko on rajattu prosessin käytössä oleviin resursseihin. Yritysten automaatiolle otolliset liiketoiminnalliset prosessit kuuluvat pitkälti kohtalaisen riskin luokkaan, jo pelkästään Fungin [5] esittämien prosessien automatisoinnin järkevyyttä mittaavien kriteerien perusteella. Yksi Fungin esittämistä kriteereistä on, että prosessin aikana tulisi käyttää montaa eri sovellusta tai järjestelmää.

Huomattavan riskin prosesseiksi voidaan laskea prosessit, joissa

- luetaan, käsitellään tai tallennetaan hyvinkin arkaluontoisia tietoja, kuten GDPR:n alaisia henkilötietoja, potilastietoja tai liiketoiminnallisesti kriittisiä tietoja
- kirjaudutaan ulkoisiin tai sisäisiin järjestelmiin laajoja käyttöoikeuksia omaavilla käyttäjätunnuksilla
- toimitaan ympäristössä toisen luonnollisen henkilön tunnuksilla tai admin-tunnuksilla
- käytetään työaseman ulkopuolisia tietoturvaluokiteltuja resursseja, sovelluksia tai palveluita.

Huomattavan riskin prosesseiksi voidaan laskea esimerkiksi kuukausittaisten palkkatietojen koostaminen ja arkistoiminen, poissaolopyynnön tekeminen työntekijän tunnuksilla HR-järjestelmään tai organisaation strategiasuunnitelmien hakeminen hallintajärjestelmästä. Huomattavan riskin prosesseilla on mahdollisuus aiheuttaa vakavaa vahinkoa organisaation toiminnalle tai maineelle riskin realisoituessa. Tämän riskitason prosessien automatisoinneissa tulee olla erittäin huolellinen ja toteuttaa riskejä minimoivia varotoimenpiteitä, sillä automaation käytössä olevat resurssit ovat arkaluontoisia sekä mahdollisesti lailla suojattuja (GDPR).

Prosessien automatisointeja suunnitellessa kannattaa siis ottaa huomioon automatisoitavan prosessin käyttämät resurssit sekä näiden resurssien tietoturvaluokitukset. Prosessin automatisointia suunnitellessa pitäisi pyrkiä kartoittamaan tarvittavien resurssien arkaluontoisuus sekä tarvittavien käyttöoikeuksien laajuus, jotta ohjelmistorobotiikan implementoinnin riskit pystytään pitämään siedettävällä tasolla [4].

3.2 Arkaluontoisen tiedon käsittely

Ohjelmistorobotiikkaa ja prosessien automatisointeja suunnitellessa nousee hyvin todennäköisesti kysymyksiä siitä, kuinka prosessien suoritukseen tarvittavaa ja suorituksien aikana kertyvää dataa käsitellään. Devarajan [4] esittelee artikkelissaan ohjelmistorobotiikan mahdollisia käyttötapauksia. Valtaosassa esitellyistä käyttötapauksista käsitellään arkaluontoista dataa, kuten asiakastietoja tai organisaation sisäisiä tietoja. Ohjelmistorobotiikan käyttöä suunnitellessa onkin

ensiarvoisen tärkeää määritellä, kuinka, missä ja miten pitkään arkaluontoisia tietoja käsitellään tai talletetaan.

Arkaluontoisen tiedon parissa työskennellessä suurimmat haasteet ovat tiedon sijainti ja tiedon säilytysaika [6]. Ohjelmistorobotiikan ratkaisuja suunnitellessa tulisikin varmistaa, että prosessin suorittava automatisaatio ei tallenna arkaluontoisia tietoja minnekään muualle kuin määriteltyihin kohteisiin. Esimerkiksi lokitusten kanssa tulee noudattaa erityistä varovaisuutta, arkaluontoista tietoa käsitellessä. Ylimääräisen tiedon huolimaton lokittaminen voi johtaa pahimmillaan esimerkiksi henkilötietojen tallentumiseen prosessia suorittavan sovelluksen tietokantaan. Prosessin aikana lokitettu tieto on lähtökohtaisesti ohjelmistorobotiikan ylläpitäjien ja palvelun omistajien saavutettavissa, minkä vuoksi huolimattomat lokitukset voivat johtaa tietovuotoihin tai tietoturvarikkomuksiin.

Ohjelmistorobotiikkapalveluiden tilaajien ja toteuttajien on oltava tietoisia siitä, mitä tietoa robotit käsittelevät, mistä tietoa haetaan ja minne sitä talletetaan. Oikeaoppisella tiedon elinkaaren hallinnalla voidaan minimoida vahinkoluontoisten tietovuotojen riskiä ja varmistua, että tietoa käsitellään ainoastaan määritellyissä sijainneissa tai järjestelmissä.

Jotta tietoa voidaan käsitellä, se täytyy myös siirtää. Epäturvallisesti toteutettu tiedon siirtovaihe (engl. data in transit) voi vaarantaa arkaluontoisen tiedon luottamuksellisuuden [7], erityisesti, jos ohjelmistorobotiikan palveluita tuotetaan organisaation välittömän infrastruktuurin ja sisäverkon ulkopuolelta. Tiedon käsittelyä ja siirtoja suunnitellessa kannattaa huomioida myös lakitekniset tekijät. Esimerkiksi Euroopan unionin lainsäädäntö kieltää henkilötietojen välittämisen maihin, joiden tietosuojalait eivät ole riittävällä tasolla. [6.] Käsitellyn tiedon säilyttämisaika tulee myös määritellä. Mikäli tietoa käytetään tai talletetaan väliaikaisesti prosessin suorittamista varten, se täytyy poistaa määrittelyjen mukaisesti. [6.]

3.3 Ohjelmistorobotiikkapalveluiden ulkoistamisen riskit

Informaatioteknologian palveluita ulkoistetaan usein yrityksenä leikata organisaation kuluja, mutta IT-palveluiden ulkoistamisella voi saavuttaa myös muitakin etuja, kuten pääsyä palveluntarjoajan erityisosaamiseen, uusia liiketoimintamahdollisuuksia sekä mittakaavaetuja. Palveluiden ulkoistamisella on kuitenkin aina omat riskinsä, jolloin palvelun tilaajan riskienhallinnan merkitys korostuu entisestään. Voidaankin väittää, että riskien arviointi ja riskienhallinta ovat merkittävässä roolissa IT-palvelun onnistuneessa ulkoistuksessa. [8.]

IT-palveluiden ulkoistamisprojekteissa yleisiä liiketoiminnallisia riskejä ovat piilokulut, sopimukselliset haasteet, palvelun laadun heikkeneminen ja ulkoistettavan erityisalan kompetenssin katoaminen organisaatiosta [8]. Ohjelmistorobotiikan kontekstissa on kuitenkin yleisempää tilata robotiikkaa uutena palveluna organisaation sisäisen toiminnon ulkoistamisen sijasta. Uuden palvelun kehittämiseen liittyy aina projekteille ominaisia riskejä [4], mutta samalla vältytään olemassa olevan toiminnon ulkoistamiseen liittyviltä riskeiltä. Toinen mahdollinen muutos organisaation robotiikalle on palveluiden toimittajan vaihto tai palveluiden siirtäminen organisaation alaisuuteen. Palveluntarjoajaa vaihdettaessa tulee kuitenkin olla tietoinen haasteista, kuten substanssiosaamisen jääminen aikaisemmalle palveluntarjoajalle ja siirtoon liittyvät kulut [8].

Yksi suurimmiksi koetuista IT-palveluiden ulkoistamiseen liittyvistä riskeistä on kuitenkin tietojärjestelmien tietoturvauhat. Palveluita ulkoistettaessa tietojärjestelmien käyttäjien määrä kasvaa ja yhtä lailla tietomurrot muuttuvat todennäköisemmiksi. Ulkoistava organisaatio menettää samalla palveluun kuuluvien järjestelmien tietoturvan hallinnan, eikä pysty enää vastaamaan siitä, kenellä on pääsy organisaation tietojärjestelmiin. Tietojärjestelmien luottamuksellisuus voidaan myös todeta vaarannetuksi tai jopa menetetyksi silloin, kun organisaatio menettää kykynsä määritellä, kenellä on pääsyoikeudet järjestelmiin ja arkaluontoiseen tietoon. [9.] Tämä pätee erityisesti ulkoistettuihin ohjelmistorobotiikan palveluihin, sillä palvelun ylläpitäjillä on pääsääntöisesti pääsy jokaiseen resurssiin, jonne automaatioita suorittavilla roboteilla on pääsy.

Ohjelmistorobotiikan palveluita ostavan organisaation kannattaakin kiinnittää erityistä huomiota palveluntarjoajan luotettavuuteen ja referensseihin.

4 Viitekehykset ohjelmistorobotiikan tietoturvassa

Yhä useammat yritykset sekä organisaatiot adoptoivat ohjelmistorobotiikkaa jokapäiväisen toimintansa tueksi [1]. RPA-toteutusten yleistyessä ohjelmistorobotiikan yhteiskunnallinen profiili kasvaa, mutta samalla julkishallinnon sekä yksityisen sektorin toimijat ovat alkaneet kiinnittämään huomiota RPA:n riskeihin ja mahdollisiin kyberturvallisuuden uhkiin. Yhdysvaltain Cybersecurity & Infrastructure Security Agency, eli CISA [10], julkaisi vuonna 2021 tiedotteen, jossa luetellaan kyberturvallisuuden uhkia Yhdysvaltalaisille teollisuuden hallintajärjestelmille. Julkaisu korostaa epäturvallisten RPA-toteutusten aiheuttamaa merkittävää kyberturvallisuuden uhkaa yhdysvaltalaiselle tuotannolle ja suositteli yrityksiä varmistamaan automatisaatioidensa riittävän suojauksen.

Kysymyksenä kuuluu, kuinka ohjelmistorobotiikan ja RPA:n palveluita voidaan suojata ja koventaa sekä ulkoisia että sisäisiä uhkia vastaan. Organisaatioiden tietoturvaa voidaan kehittää esimerkiksi noudattamalla asiantuntijoiden kehittämiä tietoturvan viitekehyksiä. Viitekehykset eivät kuitenkaan ole ratkaisu jokaiseen ongelmaan, ja organisaatioilla voi olla tarpeita tai vaatimuksia, jotka ovat ristiriidassa tiukimpien viitekehysten kanssa. Tässä luvussa käsitelläänkin sitä, minkälaisia tieto- ja kyberturvallisuuden viitekehyksiä Suomessa käytetään ja kuinka niitä olisi mahdollista soveltaa ohjelmistorobotiikan ja RPA-palvelutuotannon kontekstissa.

4.1 Tietoturvan viitekehykset

Tietoturvaa toteutettaessa sovelletaan usein erinäisiä kansainvälisesti hyväksyttyjä viitekehyksiä tai standardeja. Viitekehysten ja standardien avulla pyritään kompensoimaan organisaation sisäisen tietotaidon aukkoja, jotka tekevät sisäisten standardien luomisesta mahdotonta. Viitekehysten avulla voidaan parantaa asiakkaiden ja muiden ulkoisten kontaktien luottamusta organisaation toimintaan. [11.]

Markkinoilta löytyy useita kansainvälisesti tunnustettuja tietoturvan viitekehyksiä, kuten ISO 27001, ISO 27005, ITIL, COBIT, NIST RMF, PCI DSS ja

OCTAVE [11]. Osa näistä viitekehyksistä on luotu toimialakohtaisemmiksi, kuten Payment Card Industry Data Security Standard (PCI DSS), kun taas osa on luotu laaja-alaisempaa käyttöä varten. Esimerkiksi Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) on yksityiskohtainen tietoturvallisuusriskien arviointityökalu, jonka avulla voidaan toteuttaa laajoja riskienhallinnan prosesseja [11]. Viitekehysten väliltä löytyy suuriakin eroja käyttötarkoituksesta riippuen. Osa viitekehyksistä voi olla hyvinkin laajoja, tarkkoja ja jopa raskaita, kun taas osa voi olla huomattavasti kevyempiä ja yleiskäyttöisempiä. Yhteistä näille viitekehyksille on kuitenkin se, että niiden sisältämien standardien implementointi kerryttää kustannuksia. Raskaampien ja laaja-alaisempien viitekehysten ottaminen osaksi organisaation toimintaa tulee luonnollisestikin maksamaan enemmän kuin kevyemmän ja suppeamman viitekehyksen omaksuminen [11]. Viitekehyksen valintaan vaikuttaa siis myös tavoitellun tietoturvatason lisäksi taloudellinen puoli.

Kansainvälisesti hyväksyttyjen viitekehysten lisäksi on olemassa myös kansallisia standardeja. Kansalliset standardit on useimmiten kehitetty paikallisen valtionhallinnon ja elinkeinoelämän yhteistyössä paikalliseen ympäristöön sopiviksi. Suomessa tunnettuja tietoturvan viitekehyksiä ovat esimerkiksi valtionhallinnon luomat VAHTI-ohje ja KATAKRI.

VAHTI-ohje on valtiovarainministeriön vuonna 2012 luoma ohjeistus, jonka tavoitteena on ”tehostaa ja yhdenmukaistaa ICT-varautumista ministeriöissä ja hallinnonalojen organisaatioissa”. ICT-varautumisen vaatimukset -ohje sisältää standardeja, toimintatapoja ja käytänteitä julkishallinnon toimijoille sekä julkishallinnon palvelusopimussuhteessa oleville yrityksille. Ohjeella pyritään yhdenmukaistamaan sitä noudattavien organisaatioiden kriittisten ICT-toimintojen varautumista erilaisia kyberuhkia vastaan, sekä edesauttamaan palveluiden jatkuvuutta ja toipumista erilaisissa uhkaskenaarioissa. Valtionhallinnon ja virastojen täytyy noudattaa VAHTI-ohjeessa määriteltyjä vaatimuksia. Myös valtionhallinnon yksityisten palvelutoimittajien tulisi noudattaa VAHTI-ohjeen vaatimuksia. Organisaatioille määritellään VAHTI-ohjeen mukainen varautumisen taso, jota organisaation täytyy noudattaa, toteuttaa ja integroida osaksi valtionhallinnolle tarjoamaansa palvelua. Näitä tasoja ovat

- perustaso
- korotettu taso
- korkea taso.

Ohjeen tasot nimensä mukaisesti määrittelevät, kuinka tiukkoja standardeja palvelun ja organisaation tulee noudattaa. [12.]

Katakri eli Kansallinen turvallisuusauditointikriteeristö on toinen Suomessa laajalti käytetty tietoturvallisuuden standardi. Katakrin tarkoituksena on toimia apuna yritysten turvallisuusjärjestelmien ja tietoturvallisuuden arvioinnissa. Lyhyesti sanottuna Katakrilla pyritään arvioimaan, kuinka hyvin kohdeorganisaatio kykenee suojaamaan viranomaisilta saatua salassa pidettävää tietoa. Katakrin käyttötapaukset eivät rajoitu pelkästään valtionhallinnon tai virastojen suorittamiin turvallisuusselvityksiin, vaan sen sisältöä voidaan hyödyntää organisaatioiden turvallisuuden yleisessä kehittämisessä. Katakrin standardit jaetaan kolmeen eri osa-alueeseen,

- Turvallisuusjohtamista koskevaan osioon (T)
- Fyysistä turvallisuutta koskevaan osioon (F)
- Teknistä tietoturvallisuutta koskevaan osioon (I).

Turvallisuusjohtamisen osiossa käsitellään organisaation tietoturvallisuuden hallintajärjestelmiä ja henkilöstöturvallisuutta, fyysisen turvallisuuden osiossa turvallisuusluokiteltujen tietojen käsittelyä fyysisessä ympäristössä ja teknisen tietoturvan osiossa teknisten järjestelmien ja ympäristöjen turvallisuusvaatimuksia. Katakri on suunniteltu sovellettavaksi, ja yksittäisille vaatimuksille on mahdollistettu tilanteeseen sopivan toteutustavan valinta. Katakria ei tulekaan käyttää suorana pohjana organisaatioiden turvallisuusvaatimuksille, ja vaatimuksissa tulisikin huomioida tapauksen riskit ja erityistarpeet. [13.]

Tässä työssä tutustutaan tarkemmin VAHTI-ohjeeseen ja Katakriin sekä näiden soveltamiseen ohjelmistorobotiikassa. Kansainvälisesti tunnustetut standardit ja viitekehykset täyttävät varmasti tarkoituksensa erinomaisesti, mutta VAHTI-ohjessa ja Katakrissa on huomioitu suomalaisen yhteiskunnan erityispiirteitä ja lainsäädännöllisiä vaatimuksia. Valtionhallinnolle ja virastoille tuotettavilta

palveluilta ja palveluntarjoajilta vaaditaan usein VAHTI-ohjeen tai Katakrin mukaisia auditointeja ja sertifiointeja [12;13], joten niiden käyttäminen tässä työssä edistää ohjelmistorobotiikan palveluita tarjoavien organisaatioiden tietoturvaa valtion, virastojen ja kuntien vaatimusten mukaisesti.

4.2 Viitekehysten soveltamisen haasteet

Maailmalta löytyy huomattava määrä erilaisia tietoturvan standardeja ja viitekehyksiä. Erilaisten kokonaisuuksien lukumäärän vuoksi voi olla vaikeaa valita sopivin viitekehys, joka täyttäisi organisaation tarpeet. Jos tarpeet täyttäviä viitekehyksiä tai standardeja löytyy useita, niin usein joudutaan kysymään, mikä viitekehyksistä täyttää organisaation tarpeet parhaiten kohtuullisilla kustannuksilla. [11.]

Ongelmaksi muodostuu viitekehysten ja standardien lukumäärän lisäksi tutkittu fakta, että ei ole olemassa yksittäistä viitekehystä tai standardia, joka sopisi kaikkiin tilanteisiin ja jokaiselle organisaatiolle [11]. Jokaiseen tilanteeseen sopivan tietoturvallisuuden viitekehyksen kehittäminen on erittäin vaikeaa, ellei jopa mahdotonta. Tämän ja viitekehysten lukumäärän vuoksi käyttötarkoitukseen sopivan viitekehyksen valitseminen voi olla huomattavan haastava prosessi [11]. Osassa viitekehyksistä onkin otettu huomioon erilaisten tilanteiden ja tarpeiden olemassaolo. Esimerkiksi Katakri on tarkoitettu sovellettavaksi käyttötarkoitukseen ja palveluun yhteensopivalla tavalla [13].

Tietoturvan viitekehysten käyttöönotto ja implementointi osaksi organisaation prosesseja vaatii aina investointeja. Varsinkin pienten ja keskisuurten yritysten on usein vaikea perustella viitekehysten käyttöönottoa, sillä varsinkin laajempien viitekehysten käyttöönotto voi aiheuttaa huomattavan määrän kustannuksia. Kustannusten aiheuttamat ongelmat korostuvat erityisesti, jos yrityksen ylimmän johdon perehtyneisyys tietoturvaan ja tietoturvariskeihin on heikolla tasolla. Suuret yritykset ovatkin viitekehysten aktiivisimpia adoptoijia käyttöönottokustannusten johdosta. [11.]

Useat viitekehykset ja standardit ovat huomattavan monimutkaisia eivätkä sisällä ohjeita standardien tosiasialliseen käyttöönottoon. Viitekehysten dokumentit sisältävät usein pelkästään monimutkaisia prosesseja ja kontrolleja ilman tarkempaa ohjeistusta käyttöönottoprosessista. Viitekehysten käyttöönotto voikin olla organisaatiolle liian vaikeaa abstraktien dokumenttien perusteella, ilman asianmukaisia selkokielisiä ohjeita ja neuvoja. [11.] Siksi nykyään modernit viitekehykset suunnitellaan mahdollisimman selkokieliksi ja mukaan sisällytetään käytännön ohjeita, esimerkkinä Katakri [13]. Tunnetuista viitekehyksistä on myös julkaistu käyttöönotto-ohjeita ja selkeitä toimenpiteitä sisältäviä ohjeita [11].

Viitekehyksiä valittaessa on ensiarvoisen tärkeää ymmärtää viitekehyskandidaattien sisältö, ominaisuudet ja suunniteltu käyttötarkoitus. Toteutettavien standardien valitsijoilla tulisikin olla hyvä ymmärrys siitä, kuinka hyvin arviointiprosessissa mukana olevat viitekehykset vastaavat organisaation tarpeisiin. Viitekehyksiä on mahdollista mukauttaa tarpeiden mukaan, joko mukauttamalla olemassa olevia viitekehyksiä organisaation erikoispiirteisiin sopiviksi tai yhdistelemällä useita viitekehyksiä ja standardeja. Ei ole olemassa yhtä korkean tason dokumenttia, joka vastaisi jokaisen yrityksen tarpeita, joten yrityskohtainen mukautettu tietoturvastandardi voi olla monelle sopivin ratkaisu. [11.]

4.3 VAHTI-viitekehys ohjelmistorobotiikan näkökulmasta

Ohjelmistorobotiikalla automatisoidaan usein organisaatioille kriittisiä prosesseja ja ICT-ympäristön toimintoja. Robotiikan palveluntarjoajalla on siis useimmiten suora velvoite ja vastuu pitää automaatioiden tietoturva ja kokonaisturvallisuus hyväksyttävällä tasolla. Tieto- ja kyberturvallisuus on jatkuvasti tärkeämmässä roolissa asiakastyytyväisyyden kannalta, jolloin tietoturvarikkomuksilla voi olla erittäin vakavia seurauksia niin toimittajalle kuin asiakkaalle. Järjestelmien kokonaisturvallisuuden vastuut ovat kuitenkin valitettavan usein epäselviä asiakas-toimittaja-palvelumallissa. Ohjelmistorobotiikan palveluntarjoajilla tulisikin olla määriteltynä sisäiset standardit ja prosessit, joilla varmistetaan vähintään palveluntarjoajan välittömässä hallinnassa olevien ympäristöjen ja prosessien turvallisuus sekä häiriönsietokyky. VAHTI-ohjeen tarkoituksenmukaisten

varautumistasojen ja vaatimusten toteuttaminen olisikin sopiva lähtökohta ohjelmistorobotiikan riskienhallinnalle.

VAHTI-ohjeessa määritellään kolme toisistaan poikkeavaa vaatimustasoa, jotka ovat perustaso, korotettu taso ja korkea taso. Näiden kolmen tason lisäksi ohjeessa mainitaan myös avoin taso, joka määritellään organisaation varautumisen kehittymisen lähtötasona [12]. Vaatimustasot eroavat toisistaan vaatimusten lukumäärässä ja sisällön vaativuudessa. Korkeammat vaatimustasot vaativat myös alemman tason vaatimusten toteuttamista. Korkeamman tason vaatimusten toteuttaminen vaatii useimmiten huomattavasti enemmän työtä ja resursseja kuin alemman tason vaatimukset.

VAHTI-ohjeessa kuvataan varautumistasoja seuraavanlaisesti:

> Perustaso mahdollistaa turvallisesti organisaation normaalin, voimakkaasti verkostoituneen toiminnan. Perustasolle sijoitetaan palvelut ja järjestelmät, joiden hetkellinen lamautuminen häiriötilanteissa ei keskeytä organisaation ydintoimintoja.
>
> Korotettu taso on tarkoitettu organisaation kriittisille toiminnoille. Vain osa organisaation toiminnasta, palveluista ja järjestelmistä on tarkoituksenmukaista toteuttaa tällä tasolla. Korotetulle tasolle voidaan sijoittaa myös yhteiskunnan elintärkeitä toimintoja tukevia tai kansalaiselle häiriötilanteissa keskeisiä palveluja ja järjestelmiä.
>
> Korkea taso täyttää yhteiskunnan turvallisuusstrategian uhkamallien mukaisiin laajoihin häiriötilanteisiin ja poikkeusoloihin varautumisen tarpeet erityisturvallisuutta vaativissa toiminnoissa. Korkealle tasolle sijoitetaan palveluja ja järjestelmiä, joiden tulee toimia ympärivuorokautisesti ja joiden pienetkin palvelukatkokset aiheuttavat vakavia toiminnallisia häiriöitä tai erittäin huomattavia taloudellisia vaikutuksia. [12.]

Mikäli kappaleessa 3.1 määriteltyjä automatisaatioiden luokituksia verrataan VAHTI-ohjeen mukaisiin varautumistasoihin, niin ohjelmistorobotiikan palvelut tulisivat sijoittumaan pääsääntöisesti perustasolle ja mahdollisesti korotetulle tasolle. Korkean tason palveluita voidaan myös automatisoida, mutta automatisoinnit tehtäisiin todennäköisesti sisäisesti palvelun omistavassa organisaatiossa palvelun kriittisyyden vuoksi. Perustelen väitettä sillä, että korkealle tasolle määriteltyjen kriittisten palvelujen ulkoistaminen ulkoiselle

palveluntarjoajalle on erittäin vaikea perustella varautumisen näkökulmasta. Korkean tason palvelun ulkoistaminen tulisi myös maksamaan huomattavasti palveluntarjoajan varautumistason auditoinnin, sertifioinnin ja vaaditun palvelutason vuoksi.

Korkeampien varautumistasojen vaatimusten täyttäminen ei olekaan useimmiten liiketoiminnallisesti perusteltua käyttöönottokustannusten vuoksi, mutta perustason vaatimusten täyttäminen ja soveltaminen vaatii huomattavasti vähemmän investointeja. Perustason vaatimusten täyttäminen olisikin erinomainen lähtötilanne arkaluontoista tietoa käsittelevissä automatisaatiopalveluissa. Vaikka ohjelmistorobotiikan palveluita tarjoavan organisaation asiakkaat eivät vaatisi VAHTI-sertifiointeja, niin perustason vaatimusten täyttämisellä on mahdollista osoittaa nykyisille ja tuleville asiakkaille organisaation sitoutuminen tietoturvallisuuden periaatteisiin [12]. Mikäli asiakkaat eivät vaadi virallisia sertifiointeja, organisaatiot voivat soveltaa perustason vaatimuksia ja ohjeita liiketoiminnalleen sopivalla tavalla. Valitusta tasosta voidaan jättää toteuttamatta niitä vaatimuksia, jotka eivät ole liiketoiminnalle tarpeellisia, kunhan vaatimuksen toteuttamatta jättämisen riskit ovat tiedostettu. Toteuttamatta jätetyt vaatimukset voidaan toteuttaa myöhemmässä vaiheessa, mikäli liiketoiminnalliset lähtökohdat muuttuvat, esimerkiksi, jos uusi asiakas vaatii perustason tai korotetun tason sertifiointia.

4.4 KATAKRI automaatioratkaisujen auditoinnin työkaluna

Katakri eli kansallinen turvallisuusauditointikriteeristö on dokumentti, joka sisältää kansallisiin säädöksiin ja kansainvälisiin velvoitteisiin perustuvia vaatimuksia, joiden tarkoituksena on varmistaa auditoinnin kohteen riittävät turvallisuusjärjestelyt. Turvallisuusjärjestelyiden auditoinnin tarkoituksena on varmistaa, että kohdeorganisaatiolla on riittävät valmiudet viranomaisten salassa pidettävien tietojen turvaamiseksi. [13.] Katakri ei ole pelkästään viranomaisten käytettävissä yritysturvallisuusselvityksiä varten. Katakrissa mainitaankin käyttötapauksena yrityksien, yhteisöjen sekä viranomaisten turvallisuustyön kehittäminen [13]. Organisaatiot voivat siis hyödyntää vapaasti Katakrin sisältöä ja vaatimuksia turvallisuusjärjestelyidensä kehittämiseen.

Katakri koostuu kolmesta eri osa-alueesta, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen tietoturvallisuus. Katakri kuvaa osa-alueita seuraavanlaisesti:

> Turvallisuusjohtamista koskevassa (T) osa-alueessa pyritään varmistumaan siitä, että organisaatiolla on toimiva tietoturvallisuuden hallintajärjestelmä sekä riittävät henkilöstöturvallisuuden menettelyt turvallisuusluokiteltujen tietojen suojaamiseen.
>
> Fyysistä turvallisuutta koskevassa (F) osa-alueessa kuvataan turvallisuusluokiteltujen tietojen fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset.
>
> Teknistä tietoturvallisuutta koskevassa (I) osa-alueessa kuvataan puolestaan tekniselle tietojenkäsittely-ympäristölle asetetut turvallisuusvaatimukset. [13.]

Katakri ei sisällä yksittäisiin palvelutyyppeihin räätälöityjä vaatimuksia, vaan IT-alalla yleisesti päteviä turvallisuuden konsepteja. Vaatimuksia voidaankin soveltaa myös ohjelmistorobotiikan palveluita tarjoavissa organisaatioissa. Katakri onkin erityisen sopiva ohjelmistorobotiikkapalveluille, sillä auditointikriteeristö on luotu organisaatioiden salassa pidettävän tiedon suojaamisvalmiuden arvioinnin avuksi. Ohjelmistorobotiikan palveluilla tuotetaan usein arkaluontoisten tietojen käsittelyn automatisointeja, joten Katakrin vaatimukset sopivat erinomaisesti ohjelmistorobotiikan turvallisuusjärjestelyjen auditointiin ja kehittämiseen.

Katakri sisältää vaatimuksia ja ohjeita kolmelle eri turvallisuusluokalle. Turvallisuusluokkia ovat IV – käyttö rajoitettu, III – luottamuksellinen ja II – salainen. Vaatimukset kovenevat mentäessä turvallisuusluokituksia ylöspäin, ja samalla kasvavat vaatimusten toteuttamisen kustannukset. Turvallisuusluokka IV:n vaatimukset luovat hyvän perustason ohjelmistorobotiikan palveluille. Tietyt salassa pidettävää tietoa käsittelevät kriittiset prosessit voisi perustellusti asettaa korkeammalle turvallisuusluokalle, mutta korkeamman turvallisuustason ympäristöt ja materiaalit täytyy eristää alemman turvallisuusluokan resursseista, mikä tekee korotetun turvallisuustason virallisesta implementoinnista erittäin työlästä. Mikään ei kuitenkaan estä organisaatioita soveltamasta tarpeen mukaan sopivia III-II turvallisuusluokituksen vaatimuksia.

Katakri on luotu sovellettavaksi, eikä se sovellu sellaisenaan jokaisen organisaation tarpeisiin. Katakrin vaatimusten kuvaukset on suunniteltu mahdollistamaan monia erilaisia toteutustapoja [13], joten Katakri sopii hyvin laajalle kirjolle organisaatioita ja palveluita, ohjelmistorobotiikka mukaan lukien. Katakrin tulkitseminen on tiukempaa yritysturvallisuusselvitysten osana, mutta täyttämällä vaatimuksia vapaaehtoisesti, organisaatiot voivat osoittaa ylläpitävänsä, edistävänsä ja arvostavansa turvallisuusjärjestelyitään.

4.5 Yhteenveto viitekehyksistä

Onkin selvää, että tietoturvallisuuden viitekehyksiä löytyy maailmasta liian monta tässä työssä hyödynnettäväksi ja käsiteltäväksi, joten käytän kahta viitekehystä ohjelmistorobotiikan tietoturvallisuuden rautalankamallin hahmottelemiseksi, VAHTI-ohjetta ja Katakria. Molemmat näistä viitekehyksistä on Suomen valtionhallinnon kehittämiä, ja niiden vaatimuksia sovelletaan laajasti niin julkisissa kuin yksityisissä kilpailutuksissa. Näitä ohjeita yhdistelemällä ohjelmistorobotiikan kontekstiin sopivalla tavalla ja sopivia vaatimuksia valitsemalla onkin mielestäni mahdollista luoda selkeä rautalankamalli, jonka avulla voidaan varmistua ohjelmistorobotiikkapalveluiden tietoturvan perustavanlaatuisten vaatimuksien täyttymisestä.

5 Ohjelmistorobotiikan järjestelmien tietoturvan vaatimukset

Edeltävissä luvuissa käsiteltiin ohjelmistorobotiikan perusteita, ohjelmistorobotiikan tietoturvariskejä ja tietoturvallisuuden viitekehyksiä. Seuraavana kysymyksenä on, kuinka ohjelmistorobotiikan tietoturvaa voidaan kehittää tätä tietoa hyväksikäyttäen ja millä VAHTI-ohjeen ja Katakrin viitekehysten vaatimuksilla on mahdollista varmistua ohjelmistorobotiikkapalveluiden tietoturvallisuuden perustasovaatimusten täyttymisestä.

Tässä luvussa käsitellään sitä, mitä VAHTI-ohjeen ja Katakrin vaatimuksia ohjelmistorobotiikan palveluntarjoajien tulisi täyttää varmistaakseen teknisten ympäristöjensä tietoturvallisuuden. Kappaleiden alle lajitellut vaatimukset ovat valittu ensisijaisesti moniasiakasympäristössä toimivien ohjelmistorobotiikan yritysten tarpeet ja erityispiirteet huomioiden. Sovellan VAHTI-ohjeesta perustason vaatimuksia ja Katakrista IV-turvallisuustason vaatimuksia. Korkeamman turvallisuustason vaatimuksia voidaan ottaa ohjeelliseen viitekehykseen mukaan, mikäli vaatimuksen toteuttaminen ei kasvata viitekehyksen toteuttamisen vaatimaa kokonaisvaltaista työmäärää merkittävästi.

Vaatimusten valinta pohjautuu työn kirjoittajan henkilökohtaiseen kokemukseen ja substanssiosaamiseen ohjelmistorobotiikasta, tietoturvasta, viitekehyksistä ja informaatioteknologian alasta. Työssä esitettävää ohjeellista viitekehystä ei tule käyttää organisaatioiden ohjelmistorobotiikan tietoturvan ensisijaisena kontrollina. Tuotannon järjestelmien tietoturvaa ei tule toteuttaa pelkästään tämän dokumentin perusteella.

Vaatimukset esitetään seuraavalla tavalla:

Vaatimuksen tunniste	Vaatimuksen sanallinen kuvaus

Vaatimuksen lähteet, VAHTI-ohje [12] tai Katakri [13].

Vaatimuksen vapaasanaiset perustelut ja vaatimuksen tarkoitus. Mihin vaatimus perustuu ja miksi se on tärkeä erityisesti ohjelmistorobotiikan näkökulmasta?

5.1 Automaatiot ja käyttöoikeudet

Job-01	Automaatioista ylläpidetään ajantasaisia prosessikuvauksia, joista ilmenee automaation vaiheittainen työnkulku, käsiteltävät tiedot/aineistot sekä tarvittavat resurssit.

VAHTI, 2.1-2

Automaatioista ylläpidetään ajantasaisia prosessikuvauksia, jotta automaation tarvitsemat tai käyttämät tiedot, resurssit ja käyttöoikeudet ovat tunnistettuina koko automaation elinkaaren ajan. Oikeaoppisella prosessidokumentaatiolla mahdollistetaan resurssien ja arkaluontoisten tietojen käytön seuranta, käyttöoikeuksien ajantasaisuuden auditointi sekä lopulta oikeuksien peruuttaminen. Hyvä prosessidokumentaatio helpottaa virhetilanteiden nopeaa käsittelyä ja poikkeamien hallintaa.

Job-02	Automaatiolla on käytettävissä ainoastaan prosessin suorittamiseen vaaditut tiedot, valtuudet ja resurssit, kuten salasanat ja tunnukset.

Katakri, I-06

Prosessien automatisointeja suunnitellessa tulee ottaa huomioon vähimpien oikeuksien periaate. Vähimpien oikeuksien periaatteella tarkoitetaan ohjelmistorobotiikan yhteydessä sitä, että automaatioille annetaan ainoastaan prosessin suorittamiseen vaaditut tiedot ja oikeudet. Vähimpien oikeuksien periaatetta noudattamalla pyritään varmistumaan siitä, ettei käyttäjille tai ohjelmille anneta epähuomiossa oikeuksia arkaluontoiseen tietoon, joihin ei tulisi olla oikeuksia. Prosessien automaatioille annetaan usein käyttöön tunnuksia, salasanoja ja tiedostoja, minkä johdosta automaatioiden kehittäjien tulee rajata automaation käyttöoikeudet mahdollisimman suppeiksi. Automaatioille osoitetuille tunnuksille tulisi antaa ainoastaan prosessin vaatimat käyttöoikeudet eikä automaatioissa tulisi käyttää laajoja käyttöoikeuksia omaavia tunnuksia.

Job-03	Automaatioille määritellään robotti- tai prosessikohtaiset käyttäjätunnukset, joita robotit käyttävät kohdejärjestelmään kirjautumiseen. Luonnollisten henkilöiden tai muiden sovellusten käytössä olevien käyttäjätunnusten käytölle tulee olla perusteltua, mikäli robottikohtaisten käyttäjätunnusten käyttö on prosessin luonteen vuoksi mahdotonta.

Katakri, I-07

Robotti- tai prosessikohtaisia käyttäjätunnuksia käyttämällä voidaan rajata tunnuksen käyttöoikeudet vähimpien oikeuksien periaatteen mukaisesti ja mahdollistaa robotin tai automaation suorittamien toimintojen lokittamisen ja auditoinnin kohdejärjestelmissä. Robottikohtaisten käyttäjätunnusten käyttö myös helpottaa ohjelmistorobotiikkapalveluille luotujen käyttäjätunnusten seurantaa ja ylläpitoa. Luonnollisten henkilöiden tai muiden sovellusten käytössä olevia käyttäjätunnuksia tulee käyttää automaatioissa ainoastaan erittäin painavista syistä, esimerkiksi silloin, kun käyttäjätunnusten luominen muille kuin luonnollisille henkilöille on mahdotonta. Muiden kuin robottikohtaisten tunnusten käyttäminen on kuitenkin riskialtista, ja sitä tulisi käyttää ainoastaan viimeisenä vaihtoehtona.

Job-04	Automaation käytettävissä olevat käyttöoikeudet ja tunnukset ovat määritelty ja dokumentoitu. Käyttöoikeuksien voimassaolo ja ajantasaisuus varmistetaan säännöllisin väliajoin.

VAHTI, 2.1-2; Katakri, I-06

Automaatioiden käytettävissä olevat käyttöoikeudet ja tunnukset tulee määritellä ja dokumentoida alusta alkaen. Käyttöoikeuksien määrittelyllä ja dokumentoinnilla varmistutaan siitä, että automaatioilla on käytettävissä aina asiaan kuuluvat käyttöoikeudet ja että järjestelmiin ei jää ylimääräisiä tai tarpeettomia käyttöoikeuksia. Automaatioiden käyttöoikeudet tulisi katselmoida säännöllisin väliajoin tarpeettomien käyttöoikeuksien ja tunnuksien havaitsemiseksi.

Job-05	Automaatioiden sisältöä, parametreja tai työnkulkua ei voi muokata ilman asianmukaisia oikeuksia. Kaikki muutokset dokumentoidaan ja viedään käytössä olevaan versionhallintaratkaisuun, josta on mahdollista seurata automaation muutoshistoriaa.

Katakri, I-06, I-07, I-10

Automaatioiden ylläpidossa ja kehityksessä tulee olla käytössä asianmukainen versionhallintaratkaisu automaatioiden muutosten jäljitettävyyden mahdollistamiseksi. Ainoastaan ennalta määritetyillä käyttäjillä ja kehittäjillä on pääsy automaatioiden versionhallintaan ja oikeudet tehdä muutoksia prosesseihin. Rajoittamalla pääsyä automaatioiden muutos- ja versionhallintaan estetään luvattomat muutokset prosesseihin. Muutosten dokumentoinnilla ja versionhallinnan avulla mahdollistetaan muutosten auditointi ja muutoshistorian seuranta automaation koko elinkaaren ajalta.

5.2 Ohjelmistorobotiikan sovellukset

App-01	Pääsy ohjelmistorobotiikan sovellusten hallintajärjestelmiin on rajoitettu määritellyille henkilöille tai tunnuksille, ja järjestelmään pääsee ainoastaan tunnistautumalla riittävän luotettavasti.

Katakri, I-07, I-06

Ohjelmistorobotiikan sovellusten ja hallintajärjestelmien pääsynvalvonnalla ja käyttövaltuushallinnalla varmistetaan, että ainoastaan auktorisoidut henkilöt pääsevät käsiksi ohjelmistorobotiikan sovellusten rajoitettuihin osiin, kuten verkkokäyttöliittymiin, työpöytäsovelluksiin tai komentorivikontrolleihin. Ohjelmistorobotiikan hallintajärjestelmillä tarkoitetaan järjestelmäkokonaisuuden komponentteja, joiden avulla voidaan esimerkiksi käynnistää tai pysäyttää automaatioiden ajoja, määritellä ajojen ajastuksia tai muokata automaatioiden parametreja. Hallintajärjestelmien käyttäjien tunnistaminen tuleekin olla riittävällä tasolla, jotta asiattomat henkilöt eivät pääse käsiksi järjestelmän kriittisiin kontrolleihin.

Tunnistautumisen riittäväksi tasoksi voidaan määritellä esimerkiksi salasanalla tunnistautuminen tai kahden tekijän (2FA) käyttäjätunnistuksella.

App-02	Ohjelmistorobotiikan sovellukset lokittavat riittävällä tasolla automaatioiden, hallintajärjestelmien sekä turvallisuuteen liittyvien kokonaisuuksien tapahtumat. Lokituksiin kuuluvat esimerkiksi automaatioiden ajon aikaiset merkittävät tapahtumat, automaatioiden ajojen käynnistykset, ajoajat, pysäytykset ja virheet. Turvallisuuteen liittyviä lokituksia ovat esimerkiksi hallintajärjestelmän kirjautumistiedot.

Katakri, I-10

Ohjelmistorobotiikan sovelluksien tapahtumien oikeaoppisella lokittamisella mahdollistetaan tapahtumien jäljitettävyys, mitä tapahtui, milloin ja kenen toimesta. Lokitukset jättävät järjestelmään muistijäljen jokaisesta tärkeästä tapahtumasta, jolloin lokihistoriaa auditoimalla voidaan varmistaa, ettei järjestelmässä tapahdu väärinkäyttöä tai muuten sopimatonta tai epäilyttävää toimintaa.

Lokituksista on myös apua ongelma- ja virhetilanteissa, jolloin lokitiedoista voidaan tarkistaa, mikä osa automaatiota tosiasiallisesti vikaantui. Hyvät lokituskäytänteet mahdollistavat sujuvan ja oikeaoppisen reaktion palvelutuotannon virhetilanteisiin.

App-03	Ohjelmistorobotiikan sovellusten versiot pidetään ajan tasalla, ja sovellusten tietoturvapäivitykset asennetaan mahdollisimman lyhyellä viiveellä. Palveluntarjoajan sisäisten työkalujen ja sovellusten tietoturvaa ylläpidetään aktiivisesti, ja havaitut tietoturvariskit korjataan haavoittuvuuden vakavuuden vaatimalla prioriteetilla.

Katakri, I-16

Ohjelmistorobotiikan sovelluksia, kuten kaikkia sovelluksia yleensäkin, tulee päivittää aika ajoin kriittisten tietoturvariskien ja haavoittuvuuksien korjaamiseksi. Kolmannen osapuolen kehittämien ohjelmistorobotiikan sovelluksien aktiivisesta päivittämisestä tulee pitää huolta koko palvelun elinkaaren ajan. Palveluntarjoajan itsensä kehittämän työkalun tietoturvallisuus tulee olla jatkuvan tarkkailun alaisena, ja mahdolliset havaitut haavoittuvuudet tulee korjata pikimmiten. Haavoittuva ohjelmistorobotiikan sovellus vaarantaa pahimmillaan niin palveluntarjoajan kuin asiakkaiden organisaatioiden järjestelmien tietoturvallisuuden, minkä vuoksi versiopäivitykset ja haavoittuvuuksien korjaukset ovat ensiarvoisen tärkeitä.

App-04	Ohjelmistorobotiikan sovelluksien ja järjestelmien jatkuvan valvonnan tarpeet on määritelty palvelun kriittisyyden kannalta sopivalle tasolle.

VAHTI, 2.5-3

Ohjelmistorobotiikan järjestelmiä ja sovelluksia valvotaan järjestelmillä tuotettavien palveluiden kriittisyyden vaatimalla tasolla. Jatkuvalla valvonnalla tarkoitetaan sovitulla aikajaksolla tehtävää järjestelmien, sovellusten ja automaatioiden seurantaa. Seurantaan voi kuulua esimerkiksi sovellusten yleisen kunnon tarkistukset, sovelluksilla tuotettavien palveluiden ja automaatioiden oikeaoppisen toiminnan valvonta ja lokitietojen seuranta. Järjestelmien ja sovelluksien valvonnalla pyritään varmistamaan palveluiden jatkuvuus ja mahdollistamaan nopea reagointi häiriötilanteisiin.

5.3 Palvelinteknologia, robottikoneet ja -komponentit

Hw-01	Ohjelmistorobotiikan palveluita tuotetaan ainoastaan palveluntuottajan hyväksymillä päätelaitteilla. Muiden laitteiden kytkeminen ohjelmistorobotiikan ympäristöön on kielletty.

Katakri, I-07

Ohjelmistorobotiikan palvelutuotantoon käytetään ainoastaan palveluntarjoajan hallinnoimia ja hyväksymiä päätelaitteita ja palvelimia. Muiden laitteiden käyttäminen tai kytkeminen palvelutuotannon teknisiin ympäristöihin on ehdottomasti kielletty. Hyväksyttyjä päätelaitteita ja palvelimia käyttämällä voidaan varmistua, että päätelaitteet ovat asennettu ja konfiguroitu organisaation tietoturvapolitiikan mukaisesti. Muiden laitteiden, kuten henkilökohtaisten kannettavien, käyttäminen ja kytkeminen ohjelmistorobotiikan teknisiin ympäristöihin sisältää merkittäviä tietoturvariskejä. Useimmiten henkilökohtaisten kannettavien tietoturva ei ole yhtä hyvällä tasolla kuin organisaation IT-yksikön hallinnoimat kannettavat. Henkilökohtaisen kannettavan käyttö palvelutuotannossa voi pahimmillaan altistaa tekniset ympäristöt haittaohjelmille, kiristyshyökkäyksille tai muille pahantahtoisille toimijoille.

Hw-02	Ohjelmistorobotiikan palveluita tuottaville palvelimille tehdään kovennettu asennus. Kovennettuun asennukseseen sisältyy ainoastaan vaatimusten kannalta välttämättömät toiminnot, sovellukset, laitteet, käyttäjätunnukset, käyttöoikeudet ja palvelut. Ylimääräiset sovellukset ja palvelut on joko poistettu tai kytketty pois päältä.

Katakri, I-08

Kovennetulla asennuksella nostetaan arkaluontoista tietoa käsittelevien automaatioiden tietojärjestelmäympäristön tietoturvan perustasoa. Ylimääräisten sovelluksien, ominaisuuksien ja palveluiden käytöstä poistamisella pienennetään palvelun mahdollista hyökkäyspinta-alaa. Hyökkäyspinta-alaa rajoittamalla pyritään minimoimaan ohjelmistovirheiden mahdollistamat potentiaaliset hyökkäykset ja haavoittuvuudet. Ylimääräiset tehdasasennuksen mukana konfiguroidut käyttäjätunnukset tulee poistaa käytöstä, sillä oletusarvoisten käyttäjätunnusten konfiguraatiot ovat harvoin riittävän tietoturvallisia. Palvelimilla tulee olla määriteltynä ainoastaan automaatioiden, eli robottien, aktiivisesti käyttämät tunnukset sekä ylläpitäjien tunnukset.

Hw-03	Ohjelmistorobotiikan palveluita tuottavilla palvelimilla ja asiakaskohtaisilla päätelaitteilla tuotetaan ainoastaan yhden asiakkaan, organisaation tai kriittisen kokonaisuuden palvelut. Useiden asiakkuuksien toimintojen keskittämistä jaetuille palvelimille tulee välttää.

Katakri, I-11

Palvelinten ja päätelaitteiden asiakaskohtaisella resursoinnilla pyritään rajoittamaan tietovuotojen ja -murtojen laajuutta ja vakavuutta. Tietoturvarikkomuksen tapahtuessa tapahtuma rajoittuu eritellyssä ympäristössä ainoastaan yksittäiselle asiakkaalle, organisaatiolle tai liiketoiminnolle. Ympäristöjen eriyttämisellä voidaan estää mahdollisten laajojen, useita asiakkuuksia tai toimintoja kattavien tietoturvarikkomusten tai -murtojen syntyminen ja leviäminen. Ympäristöjen eriyttäminen mahdollistaa myös laajemman ja yksityiskohtaisemman tietoympäristöjen auditoinnin asiakkaille, sillä ympäristö ei sisällä kuin ainoastaan auditoivan asiakkaan arkaluontoisia tietoja.

Asiakaskohtaisissa ympäristöissä ei tehdä tietoliikenneavauksia kuin ainoastaan yksittäisen asiakkaan järjestelmiin ja tietoverkkoihin. Tietoverkkoihin ja -liikenteeseen perustuvat riskit rajoittuvat asiakkaalle resursoidulle palvelimelle, jolloin uhkien leviäminen asiakas 1, palveluntarjoaja, asiakas 2 -välillä on erittäin epätodennäköistä.

5.4 Verkkoteknologia ja tiedonsiirto

Net-01	Ohjelmistorobotiikan automaatioita suorittavat ja valvovat komponentit on erotettu muista ympäristöistä vähintään palomuuriratkaisulla ja tarvittaessa virtuaalilähiverkoilla tai sisäverkon segmentoinnilla.

Katakri, I-01, I-02

Automaatioita suorittavat ja valvovat järjestelmät, palvelimet, sovellukset ja yksittäiset koneet tulee eristää julkisista verkoista ja muista sisäisistä verkkosegmenteistä vähintään palomuuriratkaisulla. Tietojenkäsittely-ympäristöjen palomuureilla ja segmentoinnilla pyritään varmistumaan, että ohjelmistorobotiikan

kriittisiin komponentteihin ei ole mahdollista päästä käsiksi suoraan ulkoverkosta tai luvattomasti toiselta sisäverkon laitteelta. Lisäksi sisäverkkojen segmentoinnilla pyritään vaikeuttamaan potentiaalisen hyökkääjän liikkumista verkon sisällä, rajoittamaan pääsyä tärkeisiin resursseihin sekä helpottamaan verkon sisäisen liikenteen valvontaa [14]. Palomuurien ja virtuaalilähiverkkojen avulla voidaan myös määritellä ohjelmistorobotiikkapalveluiden vaatimat tietoliikenneavaukset tarvittuihin resursseihin turvallisesti ja hallitusti.

Net-02	Ohjelmistorobotiikan palveluntarjoajan hallinnoiman tietojenkäsittely-ympäristön sisäinen ja ulkoinen tietoliikenne on salattu käyttötarkoitukseen sopivalla tavalla. Palveluntarjoajan ja asiakkaiden välinen liikenne salataan, ja tiedonsiirron osapuolet tunnistetaan ennen arkaluontoisten tietojen siirtoa tai käsittelyä.

Katakri, I-01, I-15

Kaikki ohjelmistorobotiikan palvelukokonaisuuteen liittyvä tietojärjestelmien liikenne on salattava käyttötarkoitukseen sopivalla tavalla. Tämä vaatimus korostuu erityisesti niissä käyttötapauksissa, joissa ohjelmistorobotiikan suorittavat komponentit, eli robotit, sijaitsevat asiakasorganisaation välittömän fyysisen ympäristön ja verkon ulkopuolella. Erityisesti robottien ja kohdejärjestelmien välinen internetin kautta kulkeva tietoliikenne on salattava käsiteltävän tiedon luottamuksellisuuden ja eheyden varmistamiseksi. Internetin kautta kulkeva tietoliikenne voidaan salata esimerkiksi VPN-yhdyskäytäväratkaisuilla tai epäsymmetrisellä salauksella (HTTPS).

Net-03	Ainoastaan erikseen hyväksytty (default-deny) liikennöinti sallitaan ohjelmistorobotiikan palveluille varatun verkkosegmentin rajan ylitse. Hyväksymättömät yhteydenavaukset ja liikennöinti estetään ja suodatetaan.

Katakri, I-02

Erikseen hyväksymättömän tietoliikenteen ja yhteyksien avausyritysten suodattamisella kovennetaan järjestelmää yleisiä verkkohyökkäyksiä vastaan. Default-deny periaatteella toteutettu suodatus mahdollistaa ainoastaan ohjelmistorobotiikan toiminnan kannalta välttämättömät yhteydet ulkoisiin järjestelmiin ja organisaation ulkopuolisiin verkkoihin. Suodatuksissa tulisi ottaa huomioon myös eri protokollat, ja ainoastaan ohjelmistorobotiikan palvelujen käyttämät protokollat tulisi sallia.

Net-04	Ohjelmistorobotiikkapalveluiden edellyttämien tietoliikenneavausten määrittely, ylläpito ja konfigurointi ovat vastuutettuna palveluntarjoajan organisaatiossa. Suodatussäännöistä ja tietoliikenneavauksista sekä niiden muutoksista on olemassa riittävä dokumentaatio palvelun koko elinkaaren ajalta.

Katakri, I-03

Ohjelmistorobotiikkapalveluiden kannalta välttämättömien tietoliikenneavausten, kuten reitittimen tai palomuurin konfiguraatioiden, määrittely ja toteuttaminen on vastuutettu palveluntarjoajan organisaatiossa. Vastuuhenkilön vastuulla on varmistaa, että ainoastaan tarkoituksenmukaiset yhteydet sallitaan ohjelmistorobotiikan järjestelmiin. Palomuureihin ja muihin verkkojen välisiin valvontajärjestelmiin tehdyt tietoliikenneavaukset sekä muut konfiguraatiot tulee dokumentoida asianmukaisesti koko palvelun elinkaaren ajan. Dokumentaation avulla pyritään ehkäisemään tilanteita, joissa palomuuriin tai muuhun verkkovalvontateknologiaan tehdyt muutokset ja konfiguraatiot jäisivät epähuomiossa voimaan tarpeettomina default-deny -periaatteen vastaisesti, laajentaen mahdollista hyökkäyspinta-alaa.

Net-05	Ohjelmistorobotiikkapalveluiden hallintayhteydet sisäverkon ulkoisilta koneilta vaativat VPN-yhdyskäytäväratkaisun ja palvelun komponentteihin ei ole olemassa muita hallintayhteyksiä organisaation sisäverkon ulkopuolelta.

Katakri, I-04

Ohjelmistorobotiikkapalveluun kuuluviin komponentteihin, kuten robottikoneisiin tai palvelimiin, ei ole mahdollista ottaa hallintayhteyksiä organisaation sisäverkon tai ohjelmistorobotiikalle varatun verkkosegmentin ulkopuolelta ilman salattua VPN-yhdyskäytäväratkaisua. Järjestelmien hallintayhteydet ja -oikeudet ovat houkuttelevia kohteita potentiaaliselle hyökkääjälle. Hallinta- ja ylläpito-oikeuksilla on usein mahdollista päästä käsiksi tietoturvaluokiteltuun materiaaliin, joko suoraan tai epäsuoraan. Sisäverkon ulkopuolelta ei tule olla mahdollista ottaa hallintayhteyksiä ohjelmistorobotiikan komponentteihin, mutta myös hallintatyöaseman ja komponentin välinen tietoliikenne tulee salata esimerkiksi VPN-yhdyskäytäväratkaisulla.

6 Palveluntarjoajan organisaation tietoturvan vaatimukset

Organisaation hallinnollisen tietoturvan vaatimuksien tarkoitus on varmistaa, että organisaatiolla on käytössään tarvittavat turvallisuusjohtamisen keinot turvallisuusluokiteltujen tietojen suojaamiseksi [13]. Seuraavat vaatimukset ovat VAHTI-ohjeen ja Katakrin vaatimuksista valittuja, ohjelmistorobotiikan toimintaympäristöön sovellettuja kokonaisuuksia, joiden tarkoituksena on varmistaa hallinnollisen tietoturvan perustason toteutuminen ohjelmistorobotiikan palveluntarjoajan organisaatiossa.

6.1 Tietoturvastrategia

Str-01	Ohjelmistorobotiikkapalveluita tarjoava organisaatio tunnistaa toimintaansa ohjaavat standardit ja lainsäädännön.

VAHTI, 1.1-1

Ohjelmistorobotiikkapalveluita tarjoavien organisaatioiden tulee tietää ja ymmärtää toimialaan liittyvä lainsäädäntö, kuten tietosuojalaki (Finlex 5.12.2018/1050). Toimintaa ohjaavat standardit ja lakipykälät on tunnistettu, ja niitä noudatetaan asiaankuuluvalla tarkkuudella. Toimintaa ohjaavia standardeja voivat olla esimerkiksi organisaation sisäiset toimintamallit tai asiakkaan kanssa sovitut toteutettavat tietoturvan viitekehykset ja sertifioinnit. Palveluntarjoaja ylläpitää tietoisuuttaan palveluun vaikuttavista määräyksistä, varmistuu sisäisesti määräysten noudattamisesta ja viestii asiakkaiden kanssa aktiivisesti mahdollisista vaatimusten tai määräysten muutoksista.

Str-02	Ohjelmistorobotiikkapalveluita tarjoavalla organisaatiolla on olemassa hyväksytyt turvallisuusperiaatteet.

Katakri, T-01

Hyväksytyillä turvallisuusperiaatteilla pyritään sitouttamaan organisaatiota tietoturvallisuuden perusperiaatteisiin ja tietoturvastrategiaan. Turvallisuusperiaatteet kuvaavat organisaation sitoutumista tietoturvallisuuden edistämiseen kaikessa toiminnassaan. Turvallisuusperiaatteet sisältävä dokumentti kuvaa korkealla tasolla, kuinka tietoturvallisuustoimenpiteet liittyvät ja ovat osana organisaation jokapäiväistä toimintaa. Turvallisuusperiaatteiden toteutumista seurataan aktiivisesti.

Str-03	Ohjelmistorobotiikkapalveluita tarjoavalla organisaatiolla on olemassa ohjeistukset arkaluontoisten tietojen käsittelystä sekä arkaluontoista tietoa sisältävien järjestelmien käytöstä.

Katakri, T-04

Ohjelmistorobotiikkapalveluita tarjoava organisaatio ohjeistaa ja opastaa työntekijöitään arkaluontoisten tietojen tietoturvalliseen käsittelyyn. Ohjeissa voidaan määritellä esimerkiksi, mitä tietoja on luvallista käsitellä, vaatiiko tietojen jakaminen erillisen luvan tai mikä tiedosta on salassa pidettävää. Arkaluontoista tietoa sisältävät järjestelmät ovat työntekijöillä tiedossa, ja työntekijöitä on ohjeistettu kyseisten järjestelmien käytöstä vahingonomaisten tietoturvarikkomusten välttämiseksi.

Str-04	Ohjelmistorobotiikkapalveluita tarjoavalla organisaatiolla on olemassa tarvittava asiantuntemus tieto- ja kyberturvallisuuden varmistamiseksi sekä turvallisuusperiaatteiden toteuttamiseksi.

Katakri, T-05

Organisaatiolla on käytettävissään tarvittava asiantuntemus turvallisuusperiaatteiden toteuttamista varten. Asiantuntemus voi olla lähtöisin työntekijöiden osaamisperustasta, koulutustaustasta tai työkokemuksesta. Organisaatio voi

myös hyödyntää organisaation ulkopuolisten asiantuntijoiden apua ja tietämystä osana toimintaansa. Tarvittavalla asiantuntemuksella varmistetaan, että organisaatio pystyy tosiasiallisesti toteuttamaan määriteltyjä turvallisuusperiaatteita ja tietoturvallisuuden määräyksiä sekä seuraamaan toimenpiteiden riittävyyttä ja ajantasaisuutta.

Str-05	Ohjelmistorobotiikkapalveluita tarjoavalla organisaatiolla on olemassa tietoturvarikkomusten ja -poikkeamien raportointikäytännöt.

Katakri, T-07

Tietoturvarikkomusten raportoinnilla pyritään mahdollistamaan tapahtuneen vahingon minimointi, tehokas viestintä organisaation sisällä sekä tapahtuneesta oppiminen. Organisaation sisällä yleisesti tiedossa oleva tietoturvarikkomusten raportointiprosessi ennaltaehkäisee rikkomusten peittelyä ja tuo läpinäkyvyyttä tietoturvan nykytilanteeseen. Proseduureissa määritellään myös, minkälaiset tietoturvarikkomukset vaativat yhteydenottoa viranomaisiin.

6.2 Fyysiset ympäristöt

Fys-01	Fyysisten turvatoimien tavoitteena on varmistaa ohjelmistorobotiikan palveluiden aineellisien osien luottamuksellisuus ja eheys fyysisiä uhkia vastaan.

Katakri, F-01

Fyysisten turvatoimien tavoitteena on estää luvaton pääsy ohjelmistorobotiikan palvelun laitteistoihin ja komponentteihin. Palvelun päätelaitteet, tietokoneet, palvelimet sekä muut komponentit tulee suojata ulkopuolisilta toimijoilta asianmukaisten turvatoimien avulla, kuten kulunvalvonnalla, valvontakameroilla ja vartioinnilla. Fyysisten turvatoimien päätavoite on estää oikeudeton tunkeutuminen, mutta asianmukaisilla kontrolleilla voidaan pienentää sisäisten toimijoiden aiheuttamaa riskiä.

Fys-02	Ohjelmistorobotiikan aineelliset osat on suojattu palvelua ja tietoturvallisuutta uhkaavilta teoilta ja uhkatekijöiltä riskiarvioon nähden riittävällä tasolla.

Katakri, F-03

Ohjelmistorobotiikan aineelliset osat, kuten konesalit, työtilat ja arkistot, on suojattu monitasoista suojausperiaatetta sekä vyöhykkeistämistä soveltavalla, riskiarvion uhkatekijöiden mukaan mitoitetulla tavalla. Monitasoisella suojausperiaatteella ja vyöhykkeistämisellä tarkoitetaan fyysisten turvatoimien tasoittaista suunnittelua, jossa turvatoimet mitoitetaan vyöhykkeen turvallisuustason mukaan sekä jossa ulomman vyöhykkeen murtuminen ei vaaranna sisempiä vyöhykkeitä. Vyöhykkeiden turvatoimiin voi kuulua esimerkiksi tunkeutumisen ilmaisujärjestelmiä, esteitä, kuten aitoja, kameravalvontaa, vartijoita, valaistusta yms. Turvatoimien oikeaoppisilla yhdistelmillä toteutetaan riittävä kyvykkyys tunkeutumisen ja epäilyttävän toiminnan estämiseksi ja havaitsemiseksi.

Fys-03	Kaikille ohjelmistorobotiikan palvelutuotannon käytössä oleville alueille on määritelty asianmukaiset turvallisuusmenettelyt.

Katakri, F-06.5

Ohjelmistorobotiikan palveluita tuottavilla alueilla on määritelty turvallisuusmenettelyt, joihin sisältyy vähintään tiedon käsittelyn ja säilyttämisen periaatteet, valvontatoimenpiteet, alueen pääsyoikeudet sekä vierailijamenettelyt. Turvallisuusmenettelyillä varmistetaan arkaluontoisen tiedon tietoturvallinen käsittely ja säilyttäminen sekä tilakohtaisen toimitilaturvallisuuden perusteet. Turvallisuusmenettelyohjeita ylläpidetään aktiivisesti, ja tietoa määräyksistä sekä menettelytavoista jalkautetaan työntekijöille säännöllisin väliajoin.

Fys-04	Pääsyoikeudet ja kulkutunnisteet ohjelmistorobotiikan palvelutuotannon käytössä oleville alueille myönnetään tarve- ja rooliperustaisesti.

Katakri, F-06.3

Pääsyoikeudet ja kulkutunnisteet ohjelmistorobotiikan palvelutuotannon alueille myönnetään ainoastaan niille henkilöille, jotka todistetusti tarvitsevat pääsyä kyseisille alueille. Automaatioiden ylläpitäjät eivät todennäköisesti tarvitse pääsyä palveluita isännöivään konesaliin, kuten vastavuoroisesti konesalipalveluiden ylläpitäjät eivät tarvitse pääsyä ohjelmistorobotiikkatiimin toimistoihin. Pääsyoikeuksien hallinnalle tulee määritellä hallinnointiprosessit, kuten keneltä oikeudet haetaan, millä työnkuvilla on pääsyoikeudet millekin alueille ja kenellä on voimassa olevia pääsyoikeuksia.

6.3 Henkilöstön turvallisuusjohtaminen

Emp-01	Henkilöstön tehtävät ja vastuut ohjelmistorobotiikan palvelukokonaisuudessa on määritelty, ja jokainen työntekijä on tietoinen omista vastuistaan.

VAHTI, 3.1-1

Ohjelmistorobotiikan palvelukokonaisuuden parissa työskentelevien henkilöiden tehtävät ja vastuut tulee määritellä. Vastuut viestitään työntekijöille selkeästi ja jokainen tietää, mitä heiltä odotetaan. Tehtävien ja vastuiden selkeällä jaottelulla varmistetaan, että työt jalkautuvat tekijöilleen sujuvasti ja mahdollisimman nopeasti niin normaalissa toiminnassa kuin poikkeustilanteissa. Vastuiden selkeällä jaottelulla pyritään myös estämään tilanteita, joissa on epäselvää, kenen vastuulle mikäkin työ kuuluu. Vastuita voidaan jaotella esimerkiksi asiakkuuksittain, automaatiokohtaisesti, palvelinkohtaisesti tai muilla selkeillä ja rajatuilla tavoilla.

Emp-02	Ohjelmistorobotiikan palvelukokonaisuuden kannalta kriittiset tehtävät ja roolit on tunnistettu, ja tehtäviin on osoitettu palvelun jatkuvuuden kannalta riittävästi henkilöstöä.

VAHTI, 3.4-1

Tunnistamalla ohjelmistorobotiikan palvelukokonaisuuden kannalta kriittiset tehtävät ja roolit voidaan varmistaa kyseisille tehtäville riittävät henkilöstöresurssit. Kriittisissä tehtävissä ja rooleissa tulee olla jatkuvasti tarpeeksi osaavaa henkilöstöä palvelun jatkuvuuden turvaamiseksi, erityisesti poikkeustilanteissa tai yllättävissä henkilöstövaihdoksissa. Tehtäviin voidaan osoittaa myös varahenkilöitä, mutta tässä tapauksessa varahenkilöiden osaamista ja ammattitaitoa tulee pitää riittävällä tasolla tehtävien menestyksekkääseen suorittamiseen poikkeustilanteessa.

Emp-03	Ohjelmistorobotiikan palvelukokonaisuuden kriittisistä toiminnoista vastuullisilla henkilöillä on riittävä ammattitaito ja osaaminen tehokkaaseen toimintaan poikkeus- ja häiriötilanteissa.

VAHTI, 3.4-2

Ohjelmistorobotiikan palvelukokonaisuuden kriittisistä toiminnoista vastuullisilla henkilöillä tulee olla riittävä ammattitaito ja osaaminen, jotta ongelmatilanteet palvelun kriittisissä osissa saadaan ratkaistua mahdollisimman nopeasti. Henkilöstön ammattitaito on usein ratkaisevassa roolissa siinä, kuinka nopeasti poikkeamiin pystytään reagoimaan, joten vastuuhenkilöillä tulee olla riittävä tietotaito merkittävien palvelukatkosten minimoimiseksi.

Emp-04	Henkilöstölle pidetään organisaation määrittelemiä tietoturvakoulutuksia, ja työntekijöiden tietoturvallisuusosaamista kehitetään koko työsuhteen ajan.

VAHTI, 3.2-1

Ohjelmistorobotiikan parissa työskentelevien henkilöiden tietoturvaosaamista kehitetään koko työsuhteen ajan esimerkiksi koulutusten, kurssien tai työpajojen muodossa. Tietoturvakoulutuksilla varmistetaan, että henkilöstöllä on riittävä tietämys tietoturvan ajankohtaisista aiheista. Henkilöstön kouluttamisella voidaan ehkäistä yleisimpiä tietoturvarikkomuksia sekä korostaa turvallisuus ensin -ajatusmallia.

Emp-05	Henkilöstö tietää tietoturvapoikkeamien raportointimenettelyt ja osaa tarvittaessa saattaa vireille ilmoituksen poikkeamasta. Automaatioiden ylläpidon parissa työskentelevät henkilöt osaavat viestiä poikkeamista oikeaoppisesti prosessien omistajille.

VAHTI, 3.3-1

Työntekijät ovat tietoisia tietoturvapoikkeamien raportointiprosessista sekä poikkeamien raportointiin liittyvistä määräyksistä. Tietoturvapoikkeamien raportoimatta jättämisestä on määritelty seuraamuksia, joista henkilöstön tulee olla tietoisia. Automaatioiden ylläpidon parissa työskentelevät henkilöt osaavat viestiä poikkeamista asiakkaille oikeaoppisella ja etukäteen suunnitellulla, vahinkoja minimoivalla tavalla. Tietoturvapoikkeamista raportointi on tärkeä osa organisaation virheistä oppimisen prosessia, ja tämä tulee olla henkilöstön tiedossa.

Emp-06	Ohjelmistorobotiikan palvelukokonaisuuteen rekrytoitavista henkilöistä on tehty tarvittavat taustaselvitykset, ja henkilöiden tulee olla riittävän luotettavia toimiakseen arkaluontoisen tiedon parissa.

VAHTI, 3.3-2

Henkilöiden taustasta tulee tehdä tarvittavat selvitykset rekrytoitaessa uusia työntekijöitä ohjelmistorobotiikan palvelukokonaisuuden kriittisten tai

arkaluontoisten toimintojen pariin. Taustaselvityksillä varmistetaan tarvittaessa henkilön nuhteettomuus ja soveltuvuus tehtävään, jossa tulee vastaan arkaluontoisia tietoja, kuten esimerkiksi henkilötietoja tai yritysten talouslukuja. Ohjelmistorobotiikan palveluiden asiakkaat voivat vaatia asiakkuudelle töitä tekevistä henkilöistä turvallisuusselvitykset suojelupoliisilta, joten tähän tulee varautua jo rekrytointivaiheessa.

7 Yhteenveto

Automaatioratkaisujen yleistyessä ohjelmistorobotiikan tietoturvakysymyksiin tullaan tulevaisuudessa kiinnittämään entistä tarkempaa huomiota, sillä aihe on jo nostettu esille esimerkiksi CISA:n tietoturvakatsauksessa [10]. Onkin mahdollista, että ohjelmistorobotiikkapalveluita tarjoavien organisaatioiden tieto- ja kyberturvallisuudelle asetetaan asiakkaiden toimesta entistä kovempia ja tarkempia vaatimuksia. Ohjelmistorobotiikan palveluntarjoajien tulisikin viimeistään nyt aloittaa valmistautumaan toimintaympäristön tietoturvavaatimusten muutoksiin.

Ohjelmistorobotiikalla automatisoidaan usein prosesseja, joissa käsitellään arkaluontoisia tietoja. Automaatioilla ja roboteilla voi olla pahimmillaan pääsy erittäin laajoihin tietoaineistoihin, arkistoihin ja tietokantoihin. Ohjelmistorobotiikkapalvelut eivät siis voi olla tietojärjestelmän turvallisuuden näkökulmasta heikoin lenkki. Perusteltuihin kysymyksiin ohjelmistorobotiikan tietoturvasta täytyykin löytää uskottavat ratkaisut ja periaatteet mahdollisten riskien minimoimiseksi, ja tällöin kuvaan astuvat kansallisesti ja kansainvälisesti hyväksytyt tietoturva-viitekehykset.

Maailmalta löytyy huomattava määrä erilaisia tietoturvallisuuden viitekehyksiä, joista jokainen on räätälöity omaa käyttötarkoitustansa varten, mutta oikean viitekehyksen valinta voi olla organisaatiolle erittäin haastavaa [11]. Tässä työssä esiteltiin VAHTI-ohjeen ja Katakrin pohjalta johdettuja ja sovellettuja vaatimuksia, joilla organisaatiot voivat aloittaa ohjelmistorobotiikkapalveluidensa tietoturvan koventamisen ja kehitystyön. Työssä esitetyt vaatimukset tuovat alustavaa näkemystä siihen, mitä kaikkea palvelun tietoturvassa tulisi ottaa huomioon ja mitkä asiat ovat mahdollisesti palveluiden tietoturvan suurimpia kompastuskiviä. Vaatimukset jaoteltiin teknisen tietoturvan ja organisaation hallinnollisen tietoturvan kokonaisuuksiin, ja näiden alla vaatimukset jaoteltiin aihealueittain.

VAHTI-ohjeesta ja Katakrista pystyi johtamaan paljon ohjelmistorobotiikkapalveluille soveltuvia vaatimuksia, mutta tämän työn tarjoamaa ohjeellista viitekehystä ei kuitenkaan voi pitää kaiken kattavana dokumenttina ohjelmistorobotiikan tietoturvan toteutukselle. Todellisen viitekehyksen kehittäminen ja

toteuttaminen vaatisi huomattavasti enemmän valmistelevaa työtä ja asiantuntemusta useilta eri aihealueiden asiantuntijoilta. Työssä esitetyt vaatimukset sopivat kuitenkin ohjelmistorobotiikan tietoturvan kehittämisprosessin ensiaskeliksi.

Tieto- ja kyberturvallisuuden toimintakenttä muuttuu jatkuvasti, ja tietotekniikan alan tulee mukautua toimintaympäristönsä muutoksiin. Viitekehyksien avulla voidaan valaa tieto- ja kyberturvallisuuden perustukset, mutta vuotojen paikkaaminen vaatii jatkuvaa ja aktiivista kybersään tarkkailua.

Lähteet

1 Hofmann, P., Samp, C. & Urbach (2020), N. Robotic process automation. Electron Markets 30, 99–106.

2 van der Aalst, W.M.P., Bichler, M. & Heinzl (2018), A. Robotic Process Automation. Bus Inf Syst Eng 60, 269–272.

3 Devarajan Y. (2018), A Study of Robotic Process Automation Use Cases Today for Tomorrow's Business, International Journal of Computer Techniques -– Volume 5 Issue 6, Nov

4 D. Verdon and G. McGraw (2004), "Risk analysis in software design," in IEEE Security & Privacy, vol. 2, no. 4, pp. 79-84, July-Aug. 2004

5 Fung, H.P. (2014), Criteria, use cases and effects of information technology process automation (ITPA). Adv. Robot. Autom. 3, 1–11

6 M. Henze, M. Großfengels, M. Koprowski and K. Wehrle (2013), "Towards Data Handling Requirements-Aware Cloud Computing," 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, 2013, pp. 266-269, doi: 10.1109/CloudCom.2013.145.

7 X. Yu and Q. Wen (2010), "A View about Cloud Data Security from Data Life Cycle," 2010 International Conference on Computational Intelligence and Software Engineering, 2010, pp. 1-4, doi: 10.1109/CISE.2010.5676895.

8 B. A. Aubert, M. Patry and S. Rivard (1998), "Assessing the risk of IT outsourcing," Proceedings of the Thirty-First Hawaii International Conference on System Sciences, 1998, pp. 685-692 vol.6, doi: 10.1109/HICSS.1998.654830.

9 C. Wright (2004), Top Three Potential Risks With Outsourcing Information Systems, Information Systems Audit and Control Association

10 Cybersecurity & Infrastructure Security Agency (2021), Cyber threats to critical manufacturing sector Industrial Control Systems (ICS), CISA Insights, verkkojulkaisu: https://www.cisa.gov/sites/default/files/publications/CISA%20Insight%20Control%20Systems%2023Dec2021_508%20Updated.pdf

11 W. Al-Ahmad and B, Mohammad (2012), Can a single security framework address information security risks adequately, International Journal of Digital Information and Wireless Communications (IJDIWC) 2(3): 222-230 The

Society of Digital Information and Wireless Communications, 2012 (ISSN: 2225-658X)

12 Valtionhallinnon tietoturvallisuuden johtoryhmä (2012), ICT-varautumisen vaatimukset, Valtiovarainministeriö ISBN 978-952-251-375-5 (PDF)

13 Kansallinen turvallisuusviranomainen (2020), Katakri 2020 – Tietoturvallisuuden auditointityökalu viranomaisille, ISSN 2669-8757, verkko

14 N. Wagner et al. (2016), "Towards automated cyber decision support: A case study on network segmentation for security," 2016 IEEE Symposium Series on Computational Intelligence (SSCI), 2016, pp. 1-10, doi: 10.1109/SSCI.2016.7849908.