Aleksanteri Numminen

KÄYTETTÄVYYDEN MERKITYS KYBERTURVALLISUUDESSA SUOMEN KONTEKSTISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Numminen, Aleksanteri
Käytettävyyden merkitys kyberturvallisuudessa Suomen kontekstissa
Jyväskylä: Jyväskylän yliopisto, 2020, 31 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Kyppö, Jorma

Kyberturvallisuus on alati kasvava ala, johon liittyy paljon haasteita. Se on uusi ala, joka tarvitsee kipeästi uutta tutkimusta. Uuden tutkimuksen avulla voidaan luoda entistäkin turvallisempia järjestelmiä. Näiden uusien järjestelmien tietoturvaa suunniteltaessa ja toteutettaessa pitää kuitenkin ottaa huomioon myös käytettävyysnäkökulma. Jos käytettävyyttä ei huomioida tarpeeksi, niin järjestelmän toteutus voi jopa täysin epäonnistua tai järjestelmää voi olla mahdotonta käyttää tietoturvallisesti.

Käytettävyys on perusta järjestelmän turvalliselle käytölle. Kyberturvallisuudessa on tehty erilaisia ohjenuoria ja säädöksiä siitä, miten kyberturvallisia tietojärjestelmäympäristöjä tulisi toteuttaa. Ottavatko nämä ohjeistukset kantaa järjestelmän käytettävyyteen? Suljetaanko merkittävä osa järjestelmän kokonaisturvallisuudesta ulkopuolelle ohjeistuksissa, kun käytettävyydelle ei anneta sitä merkitystä, mikä sillä pitäisi olla? Mitä Suomen valtionhallinto linjaa tietoturvaohjeistuksissaan käytettävyydestä?

Tässä kandidaatintutkielmassa tarkoituksenani on tutkia, mikä merkitys käytettävyydellä on kyberturvallisuudessa. Aiheesta löytyy jo jonkin verran tieteellistä tutkimusta, mutta on tärkeää laatia niistä yhteenveto. Tutkielmassa otetaan esille käytettävyyden merkitys kyberturvallisuudessa ja tutkitaan myös, mitä Suomen valtionhallinnon linjaukset kyberturvallisuudesta ja tietoturvasta sanovat käytettävyydestä.

Asiasanat: kyberturvallisuus, käytettävyys, tietoturva, merkitys, kokonaisturvallisuus, Suomi

ABSTRACT

Numminen, Aleksanteri
Significance of usability in cybersecurity in Finnish context
Jyväskylä: University of Jyväskylä, 2020, 31 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Kyppö, Jorma

Cybersecurity is a growing field, which includes many challenges. It is a new field that needs more research. With new research, one can create more secure systems. When designing new systems and implementing them usability must be considered as well. If usability is not considered enough, then system development may fail altogether, or it may not be possible to use the system securely.

Usability is part of the foundation of using a system securely. In cybersecurity, there are many different guidelines and regulations about how secure systems should be developed and designed. Do these instructions on systems development include usability? Does the overall security of the system suffer when usability is not considered as it should be? What does the Finnish government say in their security guidelines about usability?

In this thesis it is investigated that what significance does usability have in cybersecurity. There is some research about the subject, but it is important to create a summary of them. In addition to investigating the significance, it is also investigated whether Finnish government considers usability in their security or cybersecurity guidelines when designing or implementing systems.

Keywords: cybersecurity, usability, system security, significance, security, Finland

KUVIOT

SISÄLLYS

1 Johdanto

Suomen Turvallisuuskomitea (2018) määrittää, että kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristöllä viitataan toimintaympäristöön, joka koostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä. Tietoturvalla viitataan tiedon eheyteen (engl. integrity), luottamuksellisuuteen (engl. confidentiality) ja saatavuuteen (engl. availability). Kyberturvallisuus puolestaan tarkoittaa ”digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.” (Turvallisuuskomitea, 2018).

Nykypäivänä kyberturvallisuus on alati kasvava ala, johon liittyy paljon haasteita. Se on uusi ala, ja vaatii kipeästi uutta tutkimusta, jotta voimme luoda entistäkin turvallisempia järjestelmiä. Usein järjestelmien tietoturvasuunnittelua toteutettaessa pitää kuitenkin ottaa huomioon käytettävyysnäkökulma. Jos käytettävyyttä ei huomioida tarpeeksi, niin valmis järjestelmä voi merkittävästi hankaloittaa järjestelmän käyttöä. Järjestelmä on tällöin ainakin tehottomampi kuin järjestelmää tai tietoturvamuutosta ennen vallinnut toimintatapa. On tärkeää koota käytettävyyden merkityksestä järjestelmän turvallisuuteen liittyen yhteenveto.

Aihetta tulisi selkeästi tutkia myös Suomen kontekstissa. Toukokuussa 2020 Valtiovarainministeriön julkaiseman aineiston mukaan yli puolet Suomen kansalaisista kokevat kansalaisille laadittujen verkkopalvelujen käytössä esteitä, joista suurimmat liittyvät palvelujen laatuun ja luottamukseen. Yleisimpiä esteitä ovat esimerkiksi vaikeaselkoiset käyttöohjeet sekä huoli tietoturvan ja tietosuojan suhteen. (Valtiovarainministeriö, 2020c). Näin ollen tulisi tarkastella myös sitä, miten käytettävyyttä on käsitelty Suomen kansallisissa ohjeistuksissa tietoturvaan ja kyberturvallisuuteen liittyen.

Käytettävyydellä tarkoitetaan tämän tutkielman kontekstissa järjestelmän helppokäyttöisyyttä. Käytettävyys voi tarkoittaa toisessa kontekstissa saatavuutta kuten esimerkiksi tietojärjestelmän vikasietoisuutta. Tämän tutkielman puitteissa ei käsitellä näitä asioita, vaan juuri helppokäyttöisyyttä esimerkiksi käyttöliittymän kontekstissa. Käytettävyys määritellään esimerkiksi ISO 9241-11

standardin mukaan sellaiseksi tyytyväisyydeksi, tehokkuudeksi ja vaikuttavuudeksi, jolla käyttäjät saavuttavat määritellyt tavoitteet tietyssä ympäristössä (ISO, 2018).

Tutkielma on tieteellisiin ja virallisiin lähteisiin perustuva kirjallisuuskatsaus, joka pyrkii vastaamaan seuraaviin kysymyksiin:

- Mitä merkitystä käytettävyydellä on erityisesti tietoturvan kanssa?
- Mitä ongelmia voi tulla siitä, että käytettävyyttä ei oteta tarpeeksi esille järjestelmän tietoturvaa suunniteltaessa?
- Mitä Suomen valtionhallinnon ohjeistukset tietoturvaan liittyen mainitsevat käytettävyydestä?

Tutkielman aiheesta, käytettävyyden merkityksestä kyberturvallisuudessa, ei ole juuri aikaisempia tieteellisiä tuotoksia, mutta ainakin kaksi kandidaatintutkielmaa aiheeseen liittyen löytyy Jyväskylän yliopistosta. Lähinnä aihetta on luultavasti Jenny Hornborgin (2020) tämän vuoden kandidaatintutkielma siitä, miten teknostressi ja tietoturva vaikuttavat toisiinsa. Teknostressiä voi aiheutua huonosta käytettävyydestä ja sitä kautta tietoturvakin voi kärsiä. (Hornborg, 2020). Tutkielman kirjoitustyön aikana ilmestyi myös Jonne Lammintauksen (2020) kandidaatintutkielma liittyen käytettävyyden tärkeyteen uudessa mobiililaitteessa ja järjestelmässä. Lammintauksen tutkielma sivuaa hyvin vahvasti tätä tutkielmaa aihepiiriltään, mutta tämä tutkielma pyrkii vastaamaan tietoturvan tärkeyteen eikä kokonaisuudessaan käytettävyyden tärkeyteen järjestelmäsuunnittelussa. (Lammintaus, 2020).

Tutkielmaa varten kirjallisuutta haettiin pääosin Google Scholar ja Finna verkkopalveluista. Pääasiallisina hakusanoina olivat usability cybersecurity, usability and security ja käytettävyys tietoturva. Suomen valtionhallinnon ohjeistuksia haettiin puolestaan Googlen ja Bingin avulla erilaisista valtionhallinnon lähteistä. Valtionhallinnon ohjeistuksia haettiin selvittämällä ensin hakusanoilla valtionhallinto tietoturva ja valtionhallinto kyberturvallisuus, mitkä tahot vastaavat Suomessa tieto- ja kyberturvallisuudesta. Selvityksen jälkeen näiden tahojen julkaisuja käytiin läpi keskittyen ohjeistuksien viimeisimpiin julkaisuversioihin.

Tutkielma on jaettu neljään erilliseen lukuun. Ensimmäinen niistä on tämä johdantoluku, jossa esitellään ja määritetään aihe ja tutkimuskysymykset. Lisäksi luvussa kerrotaan, miten tutkielma on jaoteltu lukuihin.

Toisessa luvussa pyritään kertomaan käytettävyyden määritelmästä ja merkityksestä. Määritelmä määrittää käytettävyyden käsitteenä. Merkityksen osalta pohditaan, miksi käytettävyys on tärkeää järjestelmien käytössä ja mitä käy, jos käytettävyyttä ei ole otettu huomioon. Luvussa otetaan myös esille erilaisia teorioita käytettävyydestä ja asioita, mitä pitäisi ottaa huomioon järjestelmien käytettävyyttä suunnitellessa.

Kolmannessa luvussa käsitellään käytettävyyden merkitystä tietoturvaan. Luvussa käsitellään muun muassa sitä, millaisia vaikutuksia käytettävyydellä on tietoturvaan ja miten käytettävyyttä tulisi tuoda osaksi kybertoimintaympäristön kokonaisturvallisuutta.

Neljännessä luvussa käsitellään Suomen valtionhallinnon linjauksia käytettävyydestä kyberturvallisuudessa. Luvussa otetaan esille sitä, miten Suomen valtionhallinto painottaa asiaa omissa ohjeistuksissaan. Tutkielmassa ei vertailla Suomea muihin maihin tästä näkökulmasta, vaikka tästä onkin tehty tutkimusta muun muassa KPMG toimesta Valtiovarainministeriön pyynnöstä alkuvuonna 2020. (Valtiovarainministeriö, 2020a).

Tutkielmassa nostetaan esille se, että käytettävyydellä on merkittävä osa järjestelmien tietoturvassa. Käytettävyys on osa kybertoimintaympäristön kokonaisturvallisuutta. Tästä merkittävästä kokonaisturvallisuuden osasta ei kuitenkaan juuri mainita Suomen valtionhallinnon ohjeistuksissa järjestelmien tietoturvaan liittyen. Tutkielmassa ei oteta kantaa siihen, miten mahdolliset epäkohdat voitaisiin ratkaista.

Tutkielmasta on toivottavasti hyötyä jatkotutkimuksia varten. Voi olla, että tutkielma voisi edistää sitä, että valtionhallinnossa kiinnitetään jatkossa enemmän huomiota käytettävyyteen. Tämä olisi toivottavaa eritoten silloin, kun suunnitellaan järjestelmien tietoturvaa ja sen vaatimuksia tai kyberturvallisuutta yleisesti.

2 Käytettävyyden määritelmä ja merkitys

Käytettävyydellä (engl. usability) tarkoitetaan tässä merkityksessä tietotekniikassa käytettyä termiä käytettävyydestä. Käytettävyydestä on oikeastaan kaksi merkittävää määritelmää; ISO:n (International Organization for Standardization) standardi käytettävyydestä ja Jakob Nielsenin määritelmä. Tässä luvussa kerrotaan ensin määritelmät, sitten käytettävyyden merkityksestä tietojärjestelmässä ja siitä, mitä huono käytettävyys on. Lopuksi luvussa käydään läpi sitä, miten käytettävyys otetaan ja miten se tulisi ottaa huomioon järjestelmäsuunnittelussa Nielsenin ja ISO13407 standardin mukaan.

ISO määrittää käytettävyyden siten, missä määrin järjestelmä, tuote tai palvelu voi määritettyjen käyttäjien toimesta saavuttaa tavoitteet tarkoituksenmukaisuuden (engl. effectiveness), tehokkuuden (engl. efficiency) ja tyytyväisyyden (engl. satisfaction) määrätyssä käyttötilanteessa (ISO, 2018). Vuonna 1947 toimintansa aloittanut ISO on kansainvälinen standardisoimisjärjestö, joka tuottaa standardeja 165 jäsenmaansa avulla yhtenäistääkseen standardeja kansainvälisesti (ISO, 2020a). Merkittävimpiä ISO:n laatimia standardeja ovat muun muassa A4-paperikoko, kameroiden valovoimaisuusasteikko ”ISO-arvo” ja lyhytkoodit maailman kielille (ISO, 2020b).

Tieteessä käytettävyyttä on tutkinut varsinkin Jakob Nielsen. Vuonna 1994 julkaisussaan *Usability Engineering* Nielsen loi pohjan sitä seuraaville tieteellisille julkaisuille. *Usability Engineering* on yksi viitatuimmista lähteistä käytettävyyteen liittyen. (lähde) Nielseniä ennen 1980 luvun alussa käytettiin termiä käyttäjäystävällisyys, mutta pian sen jälkeen käytettävyys terminä vakiintui. 90-luvun alussa termi vakiintui entisestään, kun ISO julkaisi standardeja, joissa hyvin nykyistä vastaava käytettävyyden määritelmä esiteltiin. (Bevana, Kirakowskib & Maissela, 1991).

Käytettävyys on merkittävä tekijä nykypäivän järjestelmissä. Käytettävyys mahdollistaa työkalujen käytön ja määrää osittain myös sen, kuinka helposti ihmiset oppivat käyttämään työkaluja. Huonosti suunniteltu käyttöliittymä todistetusti nostaa käyttäjän tekemien virheiden määrää ja saattaa aiheuttaa lisäkustannuksia ylläpitäjälle (Nielsen, 1994).

Järjestelmät voivat olla helposti vain teknisten henkilöiden suunnittelemia. Usein tässä tapauksessa järjestelmät keskittyvät liikaa ominaisuuksiin ja muihin teknisiin näkökulmiin, mutta eivät käyttökokemukseen. Näin koko järjestelmänkehitysprojekti saattaa epäonnistua, koska se ei välttämättä pääse tavoitteisiinsa tuottavuuden ja käyttäjien tyytyväisyyden suhteen. (Ka-Ping Yee, 2004).

Esimerkki huonosta käytettävyydestä on henkilö käyttämässä jotain työkalua, esimerkiksi käyttöjärjestelmää kuitenkaan tajuamatta sitä, että hän käyttää sitä jollain tapaa väärin. Käyttöjärjestelmä voi olla myös riittämätön käytettävyydeltään siten, että se ei ilmoita tarpeestaan tehdä päivityksiä tarpeeksi selkeästi käyttäjälle. Kun tutkimusten mukaan päivitysten asentaminen voi aiheuttaa vaikeuksia järjestelmän käytössä jo normaaleille käyttäjille, niin samaa ei voi vaatia muilta käyttäjäryhmiltä, jotka saattavat sisältää kognitiivisesti rajoittuneempia

tai vähemmän tietotekniikkaan tottuneita käyttäjiä. Näitä voivat olla esimerkiksi vanhukset, kehitysvammaiset tai muuten kognitiivisesti rajoittuneet henkilöt. (August, August & Shin, 2014).

Nielsenin (1994) mukaan käytettävyys on yksi osa järjestelmän käytön peruspilareista. Se ei ole mikään yksittäinen komponentti käyttöliittymässä vaan muodostuu useista komponenteista. Käytettävyys on osa järjestelmän hyödyllisyyttä tai käyttökelpoisuutta (usefulness). Nielsen (1994) määrittelee käytettävyyden viisi ominaisuutta seuraaviin kategorioihin: tehokkuus, virheet, muistettavuus, tyytyväisyys ja opittavuus. Tehokkuudella pyritään siihen, että järjestelmä olisi tehokas käyttää, kun sen käyttäjä on oppinut käyttämään sitä. Virheillä tarkoitetaan sitä, että virheiden tekeminen pitäisi olla hankalaa käyttöliittymässä. Jos niitä kuitenkin tapahtuu, niin niistä pitäisi pystyä käyttäjän oppimaan. Pahoja virheitä järjestelmän käytössä ei kuitenkaan saisi tapahtua. Muistettavuudella pyritään siihen, että tauonkin jälkeen järjestelmää pystyisi käyttämään sellainenkin käyttäjä, kuka ei pääasiallisesti käytä järjestelmää. Tyytyväisyydelle tarkoitetaan järjestelmän käytön miellyttävyyttä käyttäjän suuntaan: käyttäjän tulisi olla omasta mielestään tyytyväinen käyttäessään järjestelmää tai pitää sen käyttämisestä. Opittavuudella tarkoitetaan mahdollisimman helppoa oppimiskäyrää, kun käyttäjä aloittaa käyttämään järjestelmää. Tavoitteena on päästä mahdollisimman nopeasti aloittamaan työskentely järjestelmän parissa. (Nielsen, 1994).

Järjestelmän suunnitteluun käytettävyyden osalta on kehitetty ISO:n (1999) puolesta standardi ISO13407, *Vuorovaikutteisten järjestelmien käyttäjäkeskeinen suunnitteluprosessi*. Siinä keskitytään koko suunnitteluprosessin ajan käyttäjäkeskeisyyteen. ISO13407 standardi määrittää seuraavat viisi vaihetta suunnitteluun:

1. Määritä käyttäjäkeskeisen suunnittelun tarpeet
2. Määritä käyttökonteksti
3. Määritä käyttäjän ja organisaation vaatimukset
4. Tuota suunnitteluratkaisuja
5. Arvioi suunnitelmat vaatimusten suhteen

ISO (1999) määrittelee, että ensimmäisessä vaiheessa tulee miettiä, mitä vaatimuksia käytettävyydelle järjestelmän toiminnallisille tavoitteille on. Toisessa vaiheessa selvitetään käyttötilanteet, käyttäjien ominaisuudet, organisaatio ja fyysisen ympäristö käyttökontekstia varten.

Kolmannessa vaiheessa määritetään vaatimukset järjestelmän käytölle: keitä eri käyttäjät ovat ja mitä intressejä heillä on. Samalla asetetaan suunnittelun tavoitteita tärkeysjärjestykseen ja määritetään kriteerit testaukselle.

Neljännessä vaiheessa tuotetaan itse suunnitteluratkaisu käyttäen hyväkseen olemassa olevaa tietoa. Kyseisessä vaiheessa annetaan myös käyttäjien testata prototyyppiä ja antaa palautetta. Palautteen mukaan suunnitelmaa sitten muutetaan, kunnes vaatimukset täyttyvät.

Viimeisessä eli viidennessä vaiheessa varmistetaan, että järjestelmä vastaa käytettävyyden vaatimuksia. Tätä arviointia tulisi suorittaa kaikissa vaiheissa, ei ainoastaan viimeisessä vaiheessa. (ISO, 1999).

ISO:n (2019) mukaan ISO13407 standardi on sittemmin vedetty pois (engl. withdrawn) ja sen on korvannut ISO 9241-210:2019 standardi, *Ihmisen ja järjestelmän vuorovaikutuksen ergonomia – Osa 210: Ihmiskeskeinen suunnittelu vuorovaikutteisille järjestelmille*. ISO 9241-210 rakentuu sen päälle, mitä ISO13407 määritti aikaisemmin. ISO 9241-210 tarjoaa ohjeistusta ihmisen ja järjestelmän vuorovaikutukseen vuorovaikutteisten järjestelmien koko elinkaaren ajan. (ISO, 2019).

3 Käytettävyyden merkitys kyberturvallisuudessa

National Institute of Standards and Technology (2004) esittää, että käytettävyydellä on huomattava merkitys kyberturvallisuudessa. Kasvava tarve tiedon luottamuksellisuudelle (engl. confidentiality), saatavuudelle (engl. availability) ja eheydelle (engl. integrity) on tehnyt tietoturvaominaisuuksista olennaisen osan jokaista järjestelmää. Näistä kolmesta ominaisuudesta käytetään lyhennettä CIA englanninkielisten termiensä mukaisesti. (National Institute of Standards and Technology, 2004). Saatavuuden kategoriaan näistä kolmesta kuuluu käytettävyys.

McCann (2002) määrittää, että tietoturvauhat mahdollistavat riskit voidaan jaotella yleisesti kolmeen eri kategoriaan: prosessiriskit, järjestelmäriskit ja ihmisriskit. Käytettävyys menee näistä ihmisriskien kategoriaan. Näin ollen voidaan olettaa, että järjestelmää mallinnettaessa riskien osalta tulisi ottaa huomioon myös ihmisiin liittyvät riskit ja siten myös erityisesti järjestelmän käytettävyys. Jos käytettävyys kärsii liikaa tietoturvan vuoksi, niin järjestelmän kyberturvallisuus sekä työkalujen että toiminnallisuuden osalta ei ole enää tehokasta. Tämän vuoksi järjestelmien suunnittelussa tulee ottaa huomioon myös sosiaalinen aspekti: kaikkien täytyy osata ja myös haluta käyttää järjestelmää turvallisesti. (McCann, 2002).

Nurse ja kumppanit (2011) esittävät, että järjestelmissä olevia tietoturvaominaisuuksia joutuvat käyttämään niin alan ammattilaiset kuin aloittelijatkin, mukaan lukien ne henkilöt, ketkä eivät ole kovin valveutuneita tietokoneiden käytössä. Tähän edellä mainittuun ryhmään kuuluvat esimerkiksi vanhukset tai kognitiivisilta kyvyiltään rajoittuneet henkilöt. Jos järjestelmä ei pysty tähän, niin se ei ole inklusiivinen ja sen kokonaisturvallisuus kärsii merkittävästi. Järjestelmää ei siis ole turvallista käyttää kaikkien osapuolien osalta. (J. R. C. Nurse, S. Creese, M. Goldsmith & K. Lamberts, 2011). Myös järjestelmän osittainen turvaton käyttö nostaa kaikkien järjestelmää käyttävien riskejä järjestelmän turvallisuuden suhteen (August et al., 2014).

Käytettävyys ei ole asia, mihin voi keskittyä vasta projektin lopussa (Lidwell, Holden & Butler, 2010). Tietoturva ja myös käytettävyys tulisi olla osana suunnitteluprosessia alusta alkaen, jolloin käytettävyyden toteuttaminen pystyy ottamaan sen myös huomioon. Kumpaakin osa-aluetta vaivaa yleisesti se, että niitä pidetään lisäominaisuuksina. Näin ne eivät ole osa järjestelmän normaalia kehitystä. Lopputuloksena käytettävyys kärsii, kun tietoturvaa tuodaan myöhemmin osaksi jo olemassa olevaan järjestelmään. (Ka-Ping Yee, 2004).

Caputon ja kumppaneiden (2016) mukaan perinteinen ajattelutapa on se, että tietoturvallinen järjestelmä tekee sen käyttämisestä hankalampaa, kun taas erityisesti käytettävyyteen paneutunut järjestelmä pyrkii pääsemään näistä esteistä eroon. Tästä on syntynyt käsite ”käytettävä tietoturva”. Käytettävä tietoturva viittaa siihen, että kun tietoturvakontrollit ovat käytettävämpiä, niin käyttäjät todennäköisemmin käyttävät niitä. Tämä johtaa parempaan kokonaisturvallisuuteen. (Caputo, Pfleeger, Sasse, Ammann, Offutt & Deng, 2016). Käytettävä

tietoturva on muodostunut käsitteeksi ja tutkimuksen alaksi. Jotkut väittävät ”käytettävän tietoturvan” olevan itseristiriitainen käsite itsessään, koska tietoturva luo esteitä käytettävyydelle (M. Theofanos, 2020).

Asia ei kuitenkaan ole näin mustavalkoinen, vaan Yee (2004) esittää, että tarkemmin tietoturva pyrkii rajoittamaan pääsyä sellaisiin toimenpiteisiin, jotka ovat lopputulemaltaan haitallisia. Käytettävyys puolestaan parantaa käyttäjän pääsyä toimenpiteisiin, joilla on haluttuja lopputulemia. Näin käytettävyys ja tietoturva yhdessä, eli ”käytettävä tietoturva” ei välttämättä ole ristiriitainen itsessään. Ongelmia syntyy vasta siinä, kun järjestelmä ei pidä sisällään tietoa siitä, mikä on haluttu lopputulema järjestelmän käytössä ja mikä ei. Tähän voidaan vaikuttaa suunnittelemalla oikein käyttöliittymä tukemaan järjestelmän tarkoitettua käyttötarkoitusta. (Ka-Ping Yee, 2004).

Garfinkelin ja Lipfordin (2014) mukaan nykyään on selvää tutkijoiden keskuudessa, että järjestelmät, jotka eivät ole käytettäviä, tulevat kärsimään väistämättä tietoturvaongelmista. Vain kiinnittämällä huomiota tietoturvallisuuden ongelmiin ja käytettävyyteen yhdessä voidaan saada aikaiseksi järjestelmiä, jotka ovat oikeasti turvallisia. (Garfinkel & Lipford, 2014). Hyvä esimerkki tästä on Department of Homeland Securityn (2014) lausunto, että “tietoturva on oltava käytettävää sellaisille henkilöille, joilla ei ole teknistä taustaa, kuin myös ammattilaisille ja järjestelmän pääkäyttäjille. Lisäksi järjestelmien täytyy olla käytettäviä samalla kun ne ovat turvallisia. Jos ei ole käytettävää tietoturvaa, niin ei ole voimassa olevaa tietoturvaakaan.” (Department of Homeland Security, 2014).

Aikaisemmin tässä tutkielmassa esitettyyn käyttöjärjestelmän päivittämiseen liittyen voidaan järjestelmän suunnittelun tekniseltä puolelta tehdä oletus, että päivitykset ovat tärkeitä. Tietoturvamäärittely voi vaatia, että järjestelmää päivitetään säännöllisesti. Pohjan tältä tietoturvakontrollilta voi viedä kuitenkin kokonaan se, että päivitys on tehty niin hankalaksi, että kaikki käyttäjät eivät sitä ymmärrä käyttää. Tällöin koko tietoturvamäärittely ja järjestelmän kyberturvallinen käyttö ei ole enää mahdollista. Näin päästään tilanteeseen, jossa käytettävyyteen ei ole panostettu tarpeeksi, minkä takia käyttäjät usein pyrkivät ohittamaan tietoturvakontrolleja. (National Research Council (U.S.). Steering Committee on the Usability, Security and Privacy of Computer Systems, 2010).

Tieteessä on esitetty ohjeistuksia siitä, miten järjestelmät tulisi suunnitella tai toteuttaa niin, että tietoturva ja käytettävyys ovat molemmat otettu huomioon. Esimerkiksi Nurse ja kumppanit (2011) esittävät suuntaviivat käytettävään kyberturvallisuuteen. Lista perustuu heidän tutkimustyöhönsä aikaisempaan tutkimustyöhön nojaten. Suuntaviivat ovat seuraavanlaiset.

- Kyberturvallisuuden käytettävyys tulee ottaa huomioon aikaisessa vaiheessa
- Kaiken tyyppiset käyttäjät tulee ottaa huomioon
- Informatiivista palautetta tulee antaa käyttäjälle
- Avun, neuvojen ja dokumentaation toimittaminen käyttäjälle
- Virheitä tulee ennaltaehkäistä, ne pitäisi pystyä käsittelemään ja niistä pitää pystyä toipumaan
- Järjestelmän tilan tarkastelu pitäisi olla mahdollista

- Tietoturvatoiminnallisuudet tulee olla näkyvillä ja käytettävissä
- Kognitiivinen kuorma tulisi minimoida järjestelmän käytössä
- Käyttäjää tulisi ohjeistaa, mitä tehtäviä tulee tehdä ja milloin
- Positiivista järjestelmäkokemusta ja korkean tason käyttäjätyytyväisyyttä tulisi korostaa
- Esteettiseen ja minimalistiseen muotoiluun tulisi pyrkiä
- Opittavuuteen tulisi panostaa
- Teknisten ja tietoturvaan keskittyneiden termien käyttöä tulisi minimoida
- Tarkan henkisen mallin luomista tulisi edistää
- Tietoturva tulisi tuoda osaksi kaikkiin sovelluksen tasoihin
- Tietoturva tulee suunnitella niin, että se ei vähennä suorituskykyä
- Työkalut eivät ole ratkaisuja
- Erilaiset konseptit tulee erottaa toisistaan
- Tietoturvan hallintakäyttöliittymät saattavat tarvita lisänäkökulmia käytettävyyteen

Tietojärjestelmien ja tietoturvatyökalujen huonoa käytettävyyttä voi myös syyttää ihmisten käyttäytymistä tiettyyn pisteeseen asti (Lorentin & Karvonen, 2008). Käyttäjävirheet ovatkin syynä 24 % tietoturvaloukkauksissa (Ponemon, 2019). Hyvä käytettävyys mahdollistaa käyttäjän käyttää järjestelmää oikealla tavalla. Tähän voi liittyä monia eri tapoja käyttöliittymän ja käytettävyyden puolesta, millä ne voivat viestiä käyttäjälle tietoturvasta. Yeen (2004) mukaan sellaisia tapoja ovat esimerkiksi tietoturvavaroitusten näkyvyys, laatu, toistuvuus, selkeys sekä varoituksen ilmoittama työn määrä, millä varoitus saadaan kuitattua. Jos tietoturva on myös toteutettu niin, että se haittaa työn tekoa, niin käyttäjä voi yrittää etsiä jonkin toisen tavan tehdä asia tai yrittää laittaa tietoturvaominaisuuden pois päältä. Tietoturva voi myös tehdä järjestelmästä liian monimutkaisen, jolloin käyttäjät saattavat pystyä tekemään todella vaarallisia virheitä. (Chaudhary, 2016).

4 Käytettävyyden merkitys kyber- ja tietoturvallisuudessa Suomen kontekstissa

Kyberturvallisuuden johtamisen ylimmän tason Suomessa muodostaa Valtioneuvosto, jonka tehtävänä ovat kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä kyberturvallisuuden voimavaroista ja toimintaedellytyksistä päättäminen (Turvallisuuskomitea, 2013). Lehto ja kumppanit vuoden 2018 julkaisussaan "Kyberturvallisuuden strateginen johtaminen Suomessa" erittelevät kyberturvallisuuden johtamisen Suomen valtionhallinnossa. (Lehto, Limnéll, Kokkomäki, Pöyhönen & Salminen, 2018).

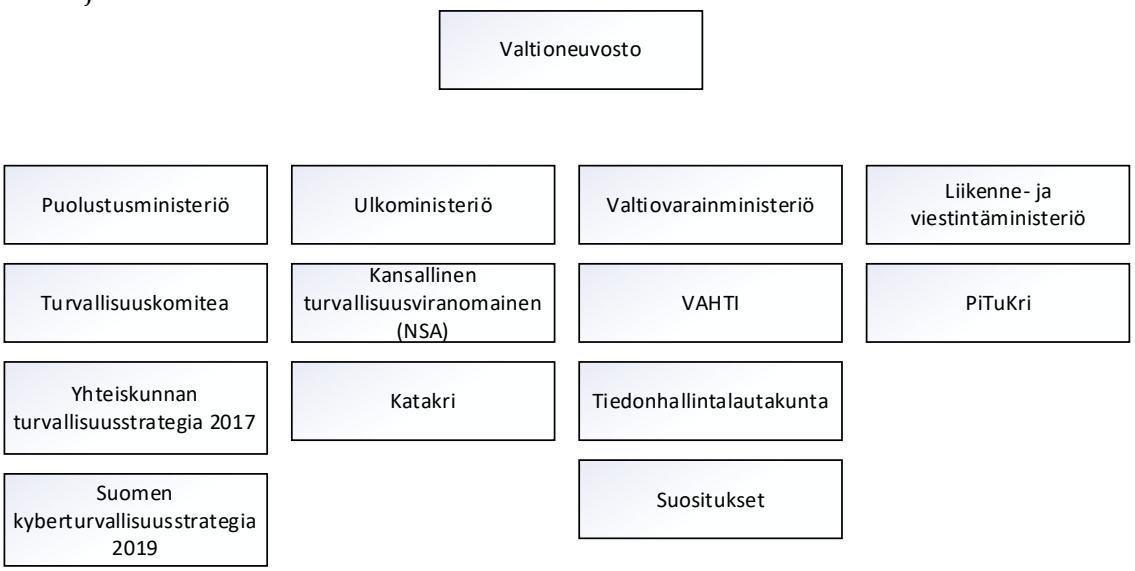
Puolustusministeriön alla toimiva monialainen Turvallisuuskomitea (2013) asettaa kansallisen turvallisuusstrategian ja kyberturvallisuusstrategian valtionhallinnon eri toimijoille. Kyberturvallisuusstrategia asettaa keskeisimmät kansalliset tavoitteet kybertoimintaympäristöjen kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Tätä strategiaa lähtevät toteuttamaan ministeriöt ja hallinnonalat itse omalla alallaan. Ministeriöt ja virastot vastaavat oman toimialansa strategian toimeenpanosta, huoltovarmuusjärjestelyiden ja kyberturvallisuuteen liittyvien tehtävien toteuttamisesta sekä niiden kehittämisestä. (Turvallisuuskomitea, 2013). Turvallisuuskomitean (2019) Kyberturvallisuusstrategian mukaan ministeriöt ja virastot voivat saada tukea ja ohjeistuksia kyberturvallisuutensa toteuttamiseen Liikenne- ja viestintäministeriön Traficomilta. Keskitettyä kyberturvallisuutta koordinoivaa tahoa ei kuitenkaan strategian mukaan Suomessa vielä ole, vaikka siihen on pyritty viime vuosina Suomessa. Kansallisessa kyberturvallisuusstrategiassa esitetään, että kansallista kehittämistä koordinoimaan perustetaan liikenne- ja viestintäministeriöön kyberturvallisuusjohtajan tehtävä. Ensimmäinen kyberturvallisuusjohtaja, Rauli Paananen, toimittaa tätä virkaa 1.4.2020 alkaen. (Turvallisuuskomitea, 2019).

Moni taho julkaisee joko kansallisia tai omaa hallinnonalaa koskevia ohjeistuksia. Tämän tutkielman suppean laajuuden vuoksi tässä keskitytään vain yleisempiin kansallisiin ohjeistuksiin. Lehdon ym. (2018) julkaisun mukaan merkittävimpiä kansalliseen tietoturvaan liittyviä ohjeistuksia laativia tahoja ovat ainakin Valtiovarainministeriön alaisuudessa toimiva VAHTI eli julkisen hallinnon digitaalisen turvallisuuden johtoryhmä ja Tiedonhallintalautakunta sekä Puolustusministeriön alaisuudessa toimiva monialainen Turvallisuuskomitea. Suomessa tietoliikenneturvallisuusviranomaisena toimii puolestaan Liikenne- ja viestintäviraston Traficomin alainen Kyberturvallisuuskeskus. (Lehto et al., 2018) Myös Ulkoministeriöstä löytyy Kansallinen turvallisuusviranomainen, joka on vastuussa kansallisesta auditointikriteeristöstä, Katakrista. (Kansallinen turvallisuusviranomainen, 2015).

Huonon käytettävyyden esimerkkejä on ollut valtionhallinnossa. Esimerkkinä tästä on Valtorin toimittaman toiminnanohjausjärjestelmä TOP:in huono käytettävyys (Salomäki & Pitkänen, 2019). Tapauksesta ei voida suoraan päätellä tietoturvariskien kasvaneen TOP:in käytettävyyden vuoksi.

Suomessa on myös havaittu sairaanhoitopiirien potilastietojärjestelmien ja muiden terveydenhuollon järjestelmien kärsivän vakavista käytettävyysongelmista. (Martikainen, 2015). Suomessa on myös esitetty Jokelan ja Polven (2010) toimesta, että ”käytettävyyttä ei ainakaan tyypillisesti vaadita julkisissa tietojärjestelmien tarjouspyynnöissä”. Jokela ja Polvi tuovat esiin myös sen, että käytettävyysongelmat ovat merkittävä ongelma nimenomaan terveydenhuollossa. (Jokela & Polvi, 2010). Myös uusista potilastietojärjestelmistä, kuten Apotti-hankkeesta, on jonkin verran julkisia tilastoja saatavilla käyttökokemuksesta ja käyttäjätyytyväisyydestä (Yle, 2020). Helsingin Sanomien (2020) mukaan eräässä tapauksessa Apotti on ollut jopa potilaskuoleman syy käytettävyytensä takia. Lisäksi jotkut järjestelmää käyttäneet henkilöt ovat suoraan sanoneet pitäytyvänsä järjestelmän käytöstä ja pyrkineet tekemään työnsä jollain muulla tavalla. (Helsingin Sanomat, 2020). Valtorin tai Apotin yksittäisiä tapauksia ei voi yleistää, mutta julkisten järjestelmäprojektien käytettävyyden merkitystä tulisi mahdollisesti tutkia lisää, koska todistetusti huono käytettävyys voi johtaa tietoturvariskeihin. (J. R. C. Nurse et al., 2011).

Valtionhallinnon tuottamia kansallisia ohjeita on monia. Tässä käydään läpi ne ohjekokonaisuuksittain keskittyen käytettävyyden merkitykseen ohjeissa. Kuvio 1, Kyberturvallisuuden ohjeistukset ministeriöittäin Suomessa, havainnollistaa ohjeet ministeriöittäin.



KUVIO 1 Kyberturvallisuuden ohjeistukset ministeriöittäin Suomessa

4.1 VAHTI-ohjeistukset

Valtiovarainministeriö on perustanut Julkisen hallinnon digitaalisen turvallisuuden strategisen johtoryhmä eli VAHTIn ohjaamaan, kehittämään ja koordinoimaan tietoturvallisuutta valtionhallinnossa (Valtiovarainministeriö, 2020b). Nykyään ryhmä toimii 2020 alusta lähtien uudessa Digi- ja väestötietovirastossa (Digi- ja väestötietovirasto, 2020a). VAHTIn päätavoitteet ovat turvata julkisen

hallinnon toiminnan ja ICT-palvelut, mahdollistaa uuden teknologian turvallinen käyttöönotto, säilyttää kansalaisten ja sidosryhmien luottamus julkiseen hallintoon ja kehittää yhteistyötä kansainvälisesti ja kansallisesti elinkeinoelämän kanssa (Digi- ja väestötietovirasto, 2020b).

Valtiovarainministeriön (2020b) mukaan VAHTI on mukana merkittävissä valtionhallinnon tietoturvalinjauksissa ja -toimenpiteissä ohjaamalla niitä. Sillä on ministeriön mukaan keskeinen rooli myös kyberturvallisuusstrategian toimeenpano-ohjelman toteutuksessa. Aikaisemmin VAHTI oli Valtionhallinnon tietoturvallisuuden johtoryhmä vuosina 1992–2013, Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä vuosina 2014–2016 ja sittemmin Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä vuodesta 2017 (Digi- ja väestötietovirasto, 2020c).

VAHTI on laatinut monia ohjeistuksia valtionhallinnon eri toimijoille monista eri lähtökohdista tavoitteidensa mukaisesti (Valtiovarainministeriö, 2020). Tässä tarkastellaan ohjeistuksien viittauksia käytettävyyteen. Tarkastelusta on jätetty pois sellaiset ohjeistukset, jotka eivät suoraan liity järjestelmän tai päätelaitteiden tai muuten työssä käytettyjen sovellusten käytettävyyteen. Esimerkiksi VAHTI:n tuottama sosiaalisen median käyttöohje tuskin antaa linjauksia valtionhallinnossa tietoturvaan tai muuten kansallisten palveluiden käytettävyyteen. VAHTI on julkaissut seuraavista ohjeista myös mahdollisesti eri versioita. Vain viimeisimmät versiot on otettu huomioon tämän tutkielman tarkastelussa.

- Sähköisen asioinnin tietoturvallisuus -ohje
- Tietoturvapoikkeamatilanteiden hallinta
- Sovelluskehityksen tietoturvaohje
- Päätelaitteiden tietoturvaohje
- Henkilöstön tietoturvaohje
- Toimitilojen tietoturvaohje
- Sovelluskehityksen tietoturvaohje
- Teknisen ympäristön tietoturvataso-ohje
- Valtion ICT-hankintojen tietoturvaohje
- Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma

VAHTI (2017) on laatinut Sähköisen asioinnin tietoturvallisuus -ohjeen kuvaamaan sitä, kuinka turvallisuuden eri osa-alueita tulee ottaa huomioon sähköisiä asiointipalveluita suunniteltaessa ja niitä toteutettaessa. Ohjeessa otetaan esille tietoturvallisuutta käsitteleviä lakeja ja viitekehyksiä. Ohjeessa tarjotaan käytännön esimerkkejä viitearkkitehtuurin ja esimerkkitapausten kautta. Ohjeeseen on koottu sähköisiä asiointipalveluita tarjoaville tahoille velvoittavat vaatimukset sekä muut suositukset ja hyvät käytänteet. (Rousku, 2017).

VAHTIn (2017) Sähköisen asioinnin tietoturvallisuus -ohjeessa esitetään yleisenä tietoturvatavoitteena saatavuus. Sen vaatimuksena on palvelun omistajana tunnistaa kaikki saatavuuteen vaikuttaa osatekijät ja huolehtia niistä. Esimerkkinä tästä mainitaan asiointipalveluiden yhdenmukaisuus, mikä on osa käytettävyyttä. Sovelluskerros -osiossa mainitaan asiakkaan luottamuksen vahvistamisesta. Tähän kategoriaan kuuluu käytettävyyteen liittyviä asioita, kuten

palvelun käyttökokemuksen yksinkertaisuus ja loogisuus, palvelun nimeämiseen liittyvät seikat, varmenne, luotettavuus ja virhetilanteiden looginen käsittely. Palvelun käyttäjät voivat ohjeen mukaan omilla toimillaan vaikuttaa itseään koskevien tietojen suojaamiseen asiointipalvelussa tai palveluketjussa. Palvelun tarjoajan tulee tarjota ohjeet ja tuki turvalliseen käyttöön, esimerkiksi suojaamalla päätelaitteensa haittaohjelmilta. Itse järjestelmän käytettävyyttä kohdalla ei mainita, eikä se ole yksi tietoturvaperiaatteista. Sen sijaan ohje sisältää maininnan saatavuudesta ja listaa muutamia käytettävyyteen liittyviä kriteerejä. (Rousku, 2017).

VAHTI julkaisi 2013 Sovelluskehityksen tietoturvaohjeen. Ohjeessa mainitaan käytettävyys kolme kertaa: sovelluksen pääkäyttäjän tietoturvatehtävä on huolehtia sovelluksen käytettävyydestä, muutoshallinnan yhteydessä koskien muutosprosessia ja jatkuvuuden hallinnan osalta, kun ohjeessa otetaan esille tietoturvavaatimukset sovelluksen käsittelemille tiedoille. Jälkimmäisessä nostettiin esille CIA kategoriat eli eheys, käytettävyys ja luottamuksellisuus. (VAHTI, 2013b).

Tietoturvapoikkeamatilanteiden hallinnan julkaisussa mainitaan käytettävyys eheyden ja luottamuksellisuuden ohessa, kun kyse on järjestelmän käytettävyystason vaarantumisesta (Valtiovarainministeriö, 2017). Samaa mainitaan muun muassa Tietoturvallisuuden arviointiohjeessa, Teknisen ICT-ympäristön tietoturvataso-ohjeessa sekä Henkilöstön tietoturvaohjeessa, missä käytettävyydellä tarkoitetaan asiakirjojen saatavuutta (VAHTI, 2012; VAHTI, 2013a; VAHTI, 2014).

VAHTIn (2015) Salauskäytäntöjen ohjeessa mainitaan, että käytettävyystarpeet tulee ottaa huomioon. Tarpeettoman korkeaa suojaustasoa ei tule määrittää, koska se heikentäisi järjestelmän käytettävyyttä. Vaatimusmäärittelyä salausratkaisuja varten tehtäessä tuleekin ottaa ohjeen mukaan erityisesti huomioon toiminnallisten vaatimusten käytettävyystarpeiden täyttyminen. (VAHTI, 2015).

VAHTI-ohjeissa otettiin lähinnä huomioon asiakirjojen saatavuutta tai saatavuustasoja koskevat asiat, kun ohjeissa mainittiin käytettävyys. Tämä ei koskenut itse käyttäjän kokemaa käyttökokemusta.

4.2 Kyberturvallisuusstrategia ja sen toimeenpano

Suomen kyberturvallisuusstrategiassa (2019) asetetaan ”keskeisimmät kansalliset tavoitteet kybertoimintaympäristöjen kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi”. Vuoden 2019 strategia nojaa vanhaan, 2013 julkaistuun, alkuperäiseen kyberturvallisuusstrategiaan. Strategiassa mainitaan myös, että Yhteiskunnan turvallisuusstrategia vuodelta 2017 ja siinä kuvatut yleiset varautumisen ja turvallisuuden yhteensovittamisen sekä toimivaltaisen viranomaisen periaatteet kytkeytyvät kansallisen kyberturvallisuusstrategian toteuttamiseen. Yhteiskunnan turvallisuusstrategia on pohja kyberturvallisuusstrategialle. (Turvallisuuskomitea, 2019).

Suomen kyberturvallisuusstrategiassa mainitaan johdannossa, että ”ihmisen tekemät virheet... voivat vaarantaa yhteiskunnan elintärkeitä toimintoja”. On siis perusteltua sanoa, että ihmisten tekemiä virheitä järjestelmien käytössä tulee ottaa huomioon strategian näkökulmasta. (Turvallisuuskomitea, 2019).

Turvallisuuskomitea (2019) mainitsee kyberturvallisuusstrategiassa myös, että ”Digitaalisen toimintaympäristön keskinäisriippuvuudet edellyttävät kyberturvallisuuden huomioivaa kokonaisarkkitehtuuria”. Kokonaisarkkitehtuurilla viitataan järjestelmän arkkitehtuuriin. Julkaisussa mainitaan myös, että jokaisella tulisi olla riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä. Sekä kokonaisarkkitehtuuriin että riittäviin valmiuksiin toimia digitaalisessa toimintaympäristössä kuuluu olennaisesti käytettävyys ja käyttökokemus. Strategian loppupäässä todetaan, että ”on tärkeää jatkaa aktiivista osallistumista standardointityöhön ja valmistaa tuotteita, joihin turvallisuus on sisäänrakennettua.” (Turvallisuuskomitea, 2013). Tähän ottaa kantaa esimerkiksi VAHTIn laatima sovelluskehityksen tietoturvaohje. (VAHTI, 2013c).

Näitä edellä mainittuja kohtia tarkemmin ei käytettävyyttä käsitellä itse strategiassa, vaan vastuu strategian toteuttamisesta on toimijoilla itsellään. Strategiassa lukeekin, että ”Vastuuviranomaisille asetetaan selkeät tavoitteet kyberturvallisuuden kehittämiseksi” (Turvallisuuskomitea, 2013).

Kyberturvallisuusstrategian toimeenpano-ohjelmassa 2017–2020 määritetään, että julkisten palveluiden digitalisoinnissa kyberturvallisuus on tarkoitus rakentaa palveluihin sisään rakentamalla helppokäyttöisiä ja turvallisia palveluita (Turvallisuuskomitea, 2018). Tämän enempää toimeenpano-ohjelmassa ei paneuduta käytettävyyteen tietoturvassa.

4.3 Katakri ja PiTuKri

Katakri (2015) eli Kansallinen turvallisuusauditointikriteeristö on viranomaisten auditointityökalu. Kriteeristössä määritetään, että sitä voidaan käyttää, kun arvioidaan kohdeorganisaation kykyä suojata tietopääomaansa, tarkemmin salassa pidettävää tietoa. Katakri ei itse aseta tarkkoja vaatimuksia tietoturvallisuudelle, vaan siinä listatut vaatimukset perustuvat olemassa olevaan kansalliseen lainsäädäntöön ja kansainvälisiin velvoitteisiin tietoturvan suhteen. (Kansallinen turvallisuusviranomainen, 2015).

Ensimmäinen Katakri (2015) valmistui vuonna 2009 osana hallituksen sisäisen turvallisuuden ohjelmaa. Katakria valmisteltiin puolustusministeriön johdolla aluksi, mutta sitten sen päivittäminen ja hallinnointi jatkossa siirrettään sisäministeriölle. Sisäministeriö toimitti ensimmäisen päivitysversion 2011. 2014 Katakrin toiminnassa mukana olleet ministeriöt päättivät siirtää päävastuun Katakrista ulkoministeriön alaisuudessa toimivalle Kansalliselle turvallisuusviranomaiselle (NSA). Suomen kansallinen turvallisuusviranomainen ohjaa kansallista toimintaa sekä vastaa esimerkiksi kansainvälisten tietoturvallisuussopimusten valmistelusta. (Ulkoministeriö, 2020).

Katakrissa (2015) ei mainita mitään käytettävyydestä järjestelmän käytön merkityksessä. Järjestelmän käytettävyys ei ole tarkastelun alla turvallisuusauditoinnin kriteeristössä. Sen sijaan järjestelmän dokumentaation käytettävyydestä ja Katakrin itsensä käytettävyyden parantamisesta löytyy maininnat kriteeristöstä. (Kansallinen turvallisuusviranomainen, 2015).

Liikenne- ja viestintäviraston Traficomin (2020) julkaisema PiTuKri on Pilvipalveluiden turvallisuuden arviointikriteeristö, joka toimittaa samaa roolia kuin Katakri, mutta koskee vain pilvipalveluita. Pitukri laadittiin, kun kansallisessa viranomaisten käytössä pilvipalvelut alkoivat yleistymään. (Liikenne- ja viestintävirasto, 2020) Eurostatin (2020) mukaan Suomi onkin yksi pilvipalveluiden käyttäjien kärkimaista. Vuonna 2019 yli 74 % suomalaisista yrityksistä käytti pilvipalveluita (Tilastokeskus, 2019), kun taas Euroopan maiden välinen keskiarvo oli vuonna 2018 26 % pelkästään isojen yritysten pilvikäytössä (Eurostat, 2020).

Liikenne- ja viestintäviraston (2020) PiTuKri ei ota kantaa käytettävyyteen. Ainoa maininta julkaisussa, mikä liittyy käytettävyyteen, PiTuKrissa on kriteerissä MH-02 Järjestelmäkehitys. Siinä mainitaan, että ohjelmointirajapintojen on kestettävä yleiset hyökkäysmenetelmät ilman, että käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu. Tämä on viittaus jo aikaisemmin tässä tutkielmassa esitettyyn CIA-määritelmään, joka sisältää saatavuuden osalta myös käytettävyyden määritelmän. Järjestelmäkehitys-osio viittaa kuitenkin vain ohjelmointirajapintoihin, mutta ei siihen, että sovelluksetkin tulisi kestää CIA:n vaarantumista. (Liikenne- ja viestintävirasto, 2020).

4.4 Valtiovarainministeriön suositukset

Valtiovarainministeriö (2020) on perustanut tiedonhallintalautakunnan 2020 tammikuussa. Tiedonhallintalautakunta on eri alojen väliseen asiantuntijayhteistyöhön perustuva viranomainen, jonka tehtävät liittyvät tiedonhallintalakiin. Tiedonhallintalautakunta laatii muun muassa suosituksia, järjestää työpajoja ja erilaisia koulutustilaisuuksia tiedonhallintalain toimeenpanon helpottamiseksi ja tukemiseksi. Toisena tehtävänä lautakunnalla on valvoa valtion kuntien ja kuntayhtymien sekä valtion laitosten ja virastojen tiedonhallintalain noudattamista. (Valtiovarainministeriö, 2020d).

Tiedonhallintalautakunta on julkaissut suosituksia verkkosivuillaan erilaisiin tiedonhallintaan liittyviin asioihin liittyen Tiedonhallintalain mukaisesti. Tiedonhallintalaki määrittää julkisen hallinnon organisaatioiden toiminnalta edellytettävät tiedon hallinnan tietoturvallisuusvaatimukset (Digi- ja väestötietovirasto, 2020). Suosituksista tulee ottaa huomioon se, että ne eivät ole velvoittavia kuten lainsäädäntö on, eli valtionhallinnon eri toimijoita ei ole velvoitettu noudattamaan tiedonhallintalautakunnan ohjeistuksia. (Valtiovarainministeriö, 2020).

Seuraavat ovat Valtiovarainministeriön (2020) tiedonhallintalautakunnan tähän mennessä julkaisemia suosituksia liittyen tiedonhallintaan tai tietoturvaan.

- Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta
- Suositus tiedonhallinnan muutosvaikutusten arvioinnista
- Suositus tiedonhallintamallista
- Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä
- Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta
- Suositus asiakirjajulkisuuskuvauksen laatimisesta
- Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa

Suositukset ottavat kantaa käytettävyyteen ja tietoturvaan. Esimerkiksi *Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta* (2020) käytettävyydestä viittaamalla tiedonhallintalakiin. Tiedonhallintalain 13.2 § määrittää, että ”Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.” (Laki julkisen hallinnon tiedonhallinnasta 906/2019.2019). Suosituskokoelma ottaa kantaa, että toiminnallista käytettävyyttä tulisi varmistaa jo kehittäessä ja otettaessa käyttöön järjestelmää sekä silloin, kun tietojärjestelmään tehdään toiminnallisuuksiin tai käyttöliittymään käyttäjän toimintaan vaikuttavia muutoksia. (Tiedonhallintalautakunta, 2020c).

Tiedonhallintalauta ottaa esille turvallisuusluokiteltavien asiakirjojen käsittelyyn liittyvässä suosituksessaan tiedon eheyden, luottamuksellisuuden ja käytettävyyden vaarantumisen (Tiedonhallintalautakunta, 2020b) Lisäksi käytettävyys mainitaan johdon vastuiden toteuttamisen suosituksissa siltä osin, että tietojärjestelmät tulisi olla toiminnallisesti käytettäviä niin, että niiden käytettävyystestaukset tai heuristiset arvioinnit on myös tehty (Tiedonhallintalautakunta, 2020a). Näin ollen tiedonhallintalautakunta ottaa kantaa järjestelmän käytettävyyteen Nielsenin tarkoittamassa kontekstissa (Nielsen, 1994).

5 Yhteenveto

Tutkielmassa tutkittiin käytettävyyttä, sen merkitystä kyberturvallisuudessa sekä sitä, miten hyvin käytettävyyttä otetaan huomioon Suomen valtionhallinnon kontekstissa. Tutkielmassa käytettiin tukena tieteellisiä lähteitä käytettävyyden ja kyberturvallisuuden aiheteemojen ympärillä, mutta myös Suomen valtion virallisia ohjeistuksia kyberturvallisuuden toteuttamisesta. Näitä virallisia ohjeistuksia tutkittiin vielä, jotta saatiin selville, mitä Suomen valtionhallinnon tietoturvaohjeistuksissa sanotaan käytettävyydestä.

On tutkittu, että loppukäyttäjän käytettävyystarpeiden jättäminen sivuun järjestelmäkehitystyössä tuottaa huonoja lopputuloksia. On myös tutkittu, kuinka loppukäyttäjä käyttäytyy, jos järjestelmä(t) eivät ole hänen mielestänsä työtä tukevia. Näissä tilanteissa loppukäyttäjä ryhtyy ohittamaan tietoturvakontrolleja tai käyttäytymään muuten poikkeavasti, joko tahattomasti tai tahallisesti. Tämä on epäedullinen tilanne kokonaisturvallisuutta ajatellen.

Esimerkiksi Nurse ja kumppanit (2011) esittävät kuitenkin suuntaviivat sellaiselle järjestelmäkehitykselle, joka ottaa sekä tietoturvan että käytettävyyden huomioon. Vastaavia tutkimuksia oli todella vähän, joten aihetta olisi hyvä tutkia lisää. Yee (2004) esittää myös, että käytettävyys on tärkeää ottaa mukaan järjestelmän kehitysprosessiin kuin myös tietoturva. Näin ne voivat tukea toisiansa ja kehitystyön lopussa ei jouduta tekemään vakavia kompromisseja kummankaan suhteen.

Suomen valtionhallinnon ohjeistukset tietoturvasta tai kyberturvallisuudesta eivät näyttäisi perinteisesti juuri ottavan kantaa käytettävyyteen. Järjestelmiä on kehitetty tekninen näkökulma edellä, mikä on ilmeisesti joissain tapauksissa johtanut myös käytettävyyteen kärsimiseen. Käytettävyydestä ei ole tullut kokonaisturvallisuuden osaa, vaikka tutkimusten mukaan se pitäisi olla yksi kokonaisturvallisuuden komponenteista.

Vasta vuoden 2019 uusi tiedonhallintalaki määrittää selvemmin käytettävyyden yhdeksi järjestelmän vaatimuksista. Tiedonhallintalain myötä perustettiin myös Tiedonhallintalautakunta Valtiovarainministeriöön tänä vuonna. Lautakunnan ohjeistukset ottavat selvemmin kantaa käytettävyyteen ja siihen, että käytettävyysvaatimukset tulisi olla mukana kaikissa tietojärjestelmätoteutuksissa niin kehittämisen ja käyttöönoton kuin myös mahdollisten päivitysten yhteydessä. Toisaalta tiedonhallintalautakunnan ohjeistukset ovat vain suosituksia eli ne eivät velvoita toimijoita toimimaan niiden mukaisesti. Tiedonhallintalain vaatima riittävä taso käytettävyydelle jää siis jatkossakin toimijoiden itsensä määriteltäväksi.

CIA:n kategorioita eli luottamuksellisuutta, eheyttä ja saatavuutta mainittiin liki kaikissa valtionhallinon tietoturvaohjeistuksissa tietoturvaan liittyen ja joissain yhteyksissä saatavuus oli nimetty käytettävyydeksi. Saatavuuden toteuttaminen jalkautettiin esimerkiksi kyberturvallisuusstrategiassa eri alan toimijoille itselleen. Näitä toimijoiden omia toteutuksia ei päästy tämän tutkielman puitteissa tutkimaan, mutta niitäkin olisi hyvä tutkia jatkotutkimuksissa.

Hyvä jatkotutkimuskohde olisi vertailla Suomen kyberturvallisuuden ja tietoturvallisuuden ohjeita muun maailman vastaaviin. Vertailuun ei keretty tämän tutkielman puitteissa paneutumaan, mutta tämänlaisen tutkimuksen tulokset voivat olla hyvinkin mielenkiintoisia. Tätä varten tulisi kuitenkin ensin löytää jokin järkevä viitekehys strategioiden ja ohjeistuksen vertailua varten. Tästä on ollut jo tutkimusta muuten kuin käytettävyyden näkökulmasta esimerkiksi 2020 KPMG tekemän tutkimuksen myötä.

Myös esimerkiksi valtionhallinnon toimijoiden, kuten Valtorin, tuottamien palveluiden huono käyttäjäkokemus olisi hyvä kohde jatkotutkimukselle. Tuottaako huonompi käytettävyys mahdollisesti tietoturvariskejä asiakkailla tai omilla käyttäjillä? Suomessa on ollut jo tapauksia, joissa esimerkiksi potilasturvallisuus on vaarantunut potilastietojärjestelmän huonon käytettävyyden vuoksi. Tämänkaltaisessa tapauksessa on kyse jo todella merkittävästä käytettävyyden puutteesta, kun järjestelmää ei osata käyttää. Mutta aiheuttaako jo pienempikin käytettävyyden puute tietoturvariskejä? Asiaa tulisi tutkia lisää.

Kolmas jatkotutkimusaihe voisi olla pilvipalveluiden vaikutus käyttäjäkokemukseen. Pilvipalvelut ovat usein tehostamassa ja nopeuttamassa digitaalista murrosta. Mutta onko esimerkiksi useampien pilvipalveluiden yhtäaikainen käyttö riski käytettävyyden kannalta? Käyttäjä saattaa joutua esimerkiksi miettimään, mihin hänen kuuluisi tiedostonsa tallentaa sen järjestelmän sijaan, missä hän juuri sillä hetkellä muokkaa tiedostojansa. Näin järjestelmät voivat olla usein päällekkäisiä, eikä niiden käyttöä välttämättä pysty vielä nykyteknologioilla valvomaan.

LÄHTEET

August, T., August, R. & Shin, H. (2014). Designing user incentives for cybersecurity. *Communications of the ACM, 57*(11), 43-46.

Bevana, N., Kirakowskib, J. & Maissela, J. (1991). What is usability. Citeseer.

Caputo, D. D., Pfleeger, S. L., Sasse, M. A., Ammann, P., Offutt, J. & Deng, L. (2016). Barriers to usable security? three organizational case studies. *IEEE Security & Privacy, 14*(5), 22-32.

Chaudhary, S. (2016). *The use of usable security and security education to fight phishing attacks*. Tampere: Tampere University Press. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-03-0292-4

Department of Homeland Security. (2014). A roadmap for cybersecurity research. Haettu osoitteesta https://www.dhs.gov/publication/cybersecurity-roadmap

Digi- ja väestötietovirasto. (2020a). Digi- ja väestötietovirasto käynnistää uudistetun VAHTI-toiminnan. Haettu osoitteesta https://dvv.fi/-/digi-ja-vaestotietovirasto-kaynnistaa-uudistetun-vahti-toiminnan

Digi- ja väestötietovirasto. (2020b). Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. Haettu osoitteesta https://dvv.fi/vahti

Digi- ja väestötietovirasto. (2020c). VAHTI-ohjeet. Haettu osoitteesta https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

Eurostat. (2020). Cloud computing - statistics on the use by enterprises. Haettu osoitteesta https://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

Garfinkel, S. & Lipford, H. R. (2014). Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust, 5*(2), 1-124.

Helsingin Sanomat. (2020). Valvira vahvistaa: Apotti-järjestelmä oli osallisena potilaan kuolemaan johtaneessa tapahtumaketjussa helsingissä. Haettu osoitteesta https://www.hs.fi/kaupunki/art-2000006391154.html

Hornborg, J. (2020). *Teknostressin ja tietoturvallisuuden vaikutukset toisiinsa.* Jyväskylän yliopisto.

ISO. (1999). Iso 13407:1999. Haettu osoitteesta www.iso.org

ISO. (2018). Iso 9241-11:2018. Haettu osoitteesta https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/35/63500.html

ISO. (2019). Iso 9241-210:2019. Haettu osoitteesta https://www.iso.org/standard/77520.html

ISO. (2020a). ISO - about us. Haettu osoitteesta https://www.iso.org/about-us.html

ISO. (2020b). Popular standards. Haettu osoitteesta https://www.iso.org/popular-standards.html

J. R. C. Nurse, S. Creese, M. Goldsmith & K. Lamberts. (2011). Guidelines for usable cybersecurity: Past and present. *2011 Third International Workshop on Cyberspace Safety and Security (CSS)*, , 21-26. doi:10.1109/CSS.2011.6058566

Jokela, T. & Polvi, J. (2010). Miten vaatia käytettävyyttä terveydenhuollon tietojärjestelmien tarjouspyynnöissä? tapaus oulun omahoitopalvelu. *Finnish Journal of eHealth and eWelfare, 2*(3), 129-135.

Kansallinen turvallisuusviranomainen. (2015). Katakri - tietoturvallisuuden auditointityökalu viranomaisille. Haettu osoitteesta https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Ka-Ping Yee. (2004). Aligning security and usability. *IEEE Security & Privacy, 2*(5), 48-55. doi:10.1109/MSP.2004.64

Laki julkisen hallinnon tiedonhallinnasta 906/2019. (2019). Haettu osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190906

Lammintaus, J. (2020). Käytettävyyden tärkeys uudessa mobiililaitteessa ja järjestelmässä. Haettu osoitteesta https://jyx.jyu.fi/handle/123456789/71086

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen suomessa. Haettu osoitteesta http://urn.fi.ezproxy.jyu.fi/URN:ISBN:978-952-287-532-7

Lidwell, W., Holden, K. & Butler, J. (2010). *Universal principles of design, revised and updated: 125 ways to enhance usability, influence perception, increase appeal, make better design decisions, and teach through design*. Rockport Pub.

Liikenne- ja viestintävirasto. (2020). Pilvipalveluiden turvallisuuden arviointikriteeristö. Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Lorentin, B. & Karvonen, K. (2008). Enhancements to the anti-phishing browser toolbar.

M. Theofanos. (2020). Is usable security an oxymoron? *Computer, 53*(2), 71-74. doi:10.1109/MC.2019.2954075

Martikainen, S. (2015). *Towards better usability : Usability and end-user participation in healthcare information technology systems development*. Kuopio: University of Eastern Finland. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-61-1981-6

McCann, T. (2002). *Information security : Keeping data safe*. Morristown, NJ: Financial Executives Research Foundation, Inc. Haettu osoitteesta

http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=105082&site=ehost-live

National Institute of Standards and Technology. (2004). Standards for security categorization of federal information and information systems. doi:https://doi.org/10.6028/NIST.FIPS.199

National Research Council (U.S.). Steering Committee on the Usability, Security and Privacy of Computer Systems. (2010). *Toward better usability, security, and privacy of information technology : Report of a workshop*. Washington, D.C.: National Academies Press.

Nielsen, J. (1994). *Usability engineering*. Morgan Kaufmann.

Rousku, K. (2017). Sähköisen asioinnin tietoturvallisuus -ohje. Haettu osoitteesta http://urn.fi.ezproxy.jyu.fi/URN:ISBN:978-952-251-868-2

Salomäki, S. & Pitkänen, S. (2019). Toiminnanohjausjärjestelmän käytettävyys asiakastukiympäristössä: Case valtori. Haettu osoitteesta https://jyx.jyu.fi/handle/123456789/66581

Tiedonhallintalautakunta. (2020a). Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-367-288-8

Tiedonhallintalautakunta. (2020b). Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-367-292-5

Tiedonhallintalautakunta. (2020c). Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-367-295-6

Tilastokeskus. (2019). Tietotekniikan käyttö yrityksissä 2019 - pilvipalvelut. Haettu osoitteesta https://www.stat.fi/til/icte/2019/icte_2019_2019-12-03_kat_003_fi.html

Turvallisuuskomitea. (2013). Suomen kyberturvallisuusstrategia – turvallisuuskomitea. [Blogikirjoitus]. Haettu osoitteesta https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/

Turvallisuuskomitea. (2018). Kyberturvallisuusstrategian toimeenpano-ohjelma 2017-2020. Haettu osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

Turvallisuuskomitea. (2019). Suomen kyberturvallisuusstrategia 2019 – turvallisuuskomitea. Haettu osoitteesta https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/

Ulkoministeriö. (2020). Kansallinen turvallisuusviranomainen NSA. Haettu osoitteesta https://um.fi/kansallinen-turvallisuusviranomainen

VAHTI. (2012). Teknisen ICT-ympäristön tietoturvataso-ohje. Haettu osoitteesta https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_3_2012_pdf.pdf

VAHTI. (2013a). Henkilöstön tietoturvaohje. Haettu osoitteesta https://www.suomidigi.fi/sites/default/files/2020-06/Vahti_4_2013_pdf.pdf

VAHTI. (2013b). Sovelluskehityksen tietoturvaohje. Haettu osoitteesta https://www.suomidigi.fi/sites/default/files/2020-06/Vahti_ohje_1_2013_pdf_0.pdf

VAHTI. (2013c). VAHTI 1/2013 sovelluskehityksen tietoturvaohje. Haettu osoitteesta https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-12013-sovelluskehityksen-tietoturvaohje

VAHTI. (2014). Tietoturvallisuuden arviointiohje. Haettu osoitteesta https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2014_pdf_0.pdf

VAHTI. (2015). Ohje salauskäytännöistä. Haettu osoitteesta https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22015-ohje-salauskaytannoista

Valtiovarainministeriö. (2017). Tietoturvapoikkeamatilanteiden hallinta. Haettu osoitteesta http://julkaisut.valtioneuvosto.fi/handle/10024/79258

Valtiovarainministeriö. (2020a). Digitaalisen turvallisuuden kansainvälinen vertailu. Haettu osoitteesta https://vm.fi/documents/10623/307681/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu/7aafe82e-86e7-7450-358c-f1adfeecb3e5/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu.pdf

Valtiovarainministeriö. (2020b). Digitaalisen turvallisuuden ohjaus. Haettu osoitteesta https://vm.fi/vahti-toiminnan-organisointi

Valtiovarainministeriö. (2020c). Digitalisaation mittarit ja tilannekuva toukokuussa 2020. Haettu osoitteesta https://vm.fi/digitalisaation-edistamisen-ohjelma

Valtiovarainministeriö. (2020d). Tiedonhallintalautakunta. Haettu osoitteesta https://vm.fi/tiedonhallintalautakunta

Yle. (2020). Nettisivustolla kysytään tietojärjestelmästä kokemuksia nimettömänä, lääkärit haukkuivat lyttyyn – toimitusjohtaja: Apotin ongelmat ovat tiedossa. Haettu osoitteesta https://yle.fi/uutiset/3-11229349