



TL IV luokiteltu monihankeympäristö

Jooseppi Vaarasalo

Opinnäytetyö, AMK

Lokakuu 2021

Tietojenkäsittely ja tietoliikenne

Insinööri (AMK), tieto- ja viestintätekniikka

Vaarasalo, Jooseppi

TL IV luokiteltu monihankeympäristö

Jyväskylä: Jyväskylän ammattikorkeakoulu. Lokakuu 2021, 36 sivua.

Tekniikan ala. Tieto- ja viestintätekniikan koulutusohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Huld Oy tarvitsi turvaluokiteltuja projekteja varten erillisen ympäristön, jossa voidaan käsitellä turvaluokiteltua tietoa. Koska projekteja tulee ja menee ja ne voivat olla myös lyhyitä, ei ollut järkeä luoda ympäristöä, joka kykenisi tuottamaan vain yhden projektin ympäristöä kohden. Huld Oy päätti tehdä monihankeykeneväisen ympäristön, jossa voitaisiin käsitellä enintään turvaluokan IV tietoa.

Projektin tavoitteena oli luoda monihanke kykeneväinen TL IV ympäristö ilman kompromisseja, jotta TL IV projekteja voitaisiin käsitellä tehokkaasti ja nopeasti, ilman ylimääräistä työtä.

Ympäristö rakennettiin turvaluokitellun tilan sisälle, jolloin fyysisen turvallisuuden vaatimukset on rajattu tämän työn ulkopuolelle. Laitteiston hankkimisen jälkeen asennettiin palvelimet ja verkkolaitteet. Ympäristössä oli Windows Server-palvelin, joka toteutti käyttäjähallinnan ja toimikorttikirjautumisen. Valvonnan ja lokituksen toteutti GNU/Linux palvelin.

Ympäristön rakennus saatiin tehtyä onnistuneesti aikataulussa. Ympäristö on auditoitu viranomaisten toimesta täyttävän turvaluokka IV -materiaalin käsittelyn edellyttämät vaatimukset.

Avainsanat (asiasanat)

KATAKRI, Turvaluokiteltu tieto, Turvaluokitukset, tietoturvallisuus, tietoliikenne, Windows, GNU/Linux, ylläpito

Muut tiedot (salassa pidettävät liitteet)

Vaarasalo, Jooseppi

TL IV Environment capable of hosting multiple projects

Jyväskylä: JAMK University of Applied Sciences, September 2020, 36 pages.

Engineering and technology. Degree Programme in Information and Communications Technology. Bachelor's thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

Huld Oy required a separate environment for classified projects that would be able to handle security classified information. Since projects come and go and can also be short, it didn't make sense to create a TL IV environment that could only produce one project per environment. Huld Oy decided to carry out a multi-project environment capable to handle restricted level security classified information.

The aim of the project was to create a multi-project capable TL IV environment without compromise so that TL IV projects could be handled efficiently and quickly, without additional work.

The project was implemented by building the environment in secure facilities and therefore facility security is out of scope of this work. After acquiring the hardware, servers and network equipment were installed. There was a Windows Server in the environment that implemented user management and smart card login. Monitoring and logging was performed by a GNU / Linux server.

The environment was successfully completed on schedule. The environment was audited by the authorities.

Keywords/tags (subjects)

KATAKRI, Classified information, Security Classifications, Cyber Security, network, Windows, GNU/Linux, maintenance

Miscellaneous (Confidential information)

Lyhenne- ja termiluettelo

AD	Active Directory
AD CS	Active Directory Certificate Services
AD DS	Active Directory Domain Services
BIOS	Basic Input and Output System
CA	Certification Authority
CIS	Center for Internet Security
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GPO	Group Policy Object
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
KATAKRI	kansallinen turvallisuusauditointikriteeristö
NCSA	National Communications Security Authority
SNMP	Simple Network Management Protocol
SRP	Software Restriction Policy
SSF	Space Systems Finland
TL IV	Turvallisuusluokka IV
VLAN	Virtual Local Area Network

Sisältö

1	Johdanto	8
1.1	Tietoa toimeksiantajasta	8
2	Ympäristössä käytetyt palvelut	9
2.1	AD DS.....	9
2.2	AD CS	9
2.3	Atlassian Confluence	9
2.4	Atlassian Jira	10
3	Kuvaus tuotantoympäristöstä	10
3.1	Ympäristön laitteet.....	11
3.1.1	Palomuri ja reititin	12
3.1.2	Kytkin	12
3.1.3	Valvontapalvelin	13
3.1.4	Lokipalvelin	13
3.1.5	Dokumentointi- ja Välityspalvelin.....	13
3.1.6	Windows Server	14
3.1.7	Windows 10 Työasemat	14
3.1.8	VPN-palvelin.....	15
3.2	Salassa pidettävien tietojen tallennus	15
3.2.1	Salassa pidettävien tietojen pääsynhallinta	16
4	KATAKRI	16
4.1	KATAKRIn rakenne.....	16
4.2	KATAKRIn käyttö.....	17
5	KATAKRI I-osion vaatimukset sovellettuna ympäristöön.....	18
5.1	I-01 Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – verkon rakenteellinen turvallisuus	18
5.2	I-02 Vähimpien oikeuksien periaate - tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöt ko. turvallisuusluokan sisällä	19
5.3	I-03 Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan – suodatus- ja valvontajärjestelmien hallinnointi	19
5.4	I-04 Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – hallintayhteydet	20
5.5	I-05 Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - langaton tiedonsiirto	21
5.6	I-06 Vähimpien oikeuksien periaate – pääsyoikeuksien hallinnointi.....	21
5.7	I-07 Monitasoinen suojaaminen – tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä	22

5.8	I-08 Vähimmäistoimintojen ja vähimpien oikeuksien periaate – järjestelmäkovenus.	22
5.9	I-09 Monitasoinen suojaaminen – haittaohjelasuojaus	23
5.10	I-10 Monitasoinen suojaaminen – turvallisuuteen liittyvien tapahtumien jäljitettävyys	23
5.11	I-11 Monitasoinen suojaaminen – poikkeamien havainnointikyky ja toipuminen.....	24
5.12	I-12 Tietoturvasuustuotteiden arviointi ja hyväksyntä – salausratkaisut	24
5.13	I-13 Monitasoinen suojaaminen koko elinkaaren ajan – Ohjelmistoilla toteutettavat pääsynhallintatoteutukset	25
5.14	I-14 Monitasoinen suojaaminen – Hajasäteily (tempest)	25
5.15	I-15 Turvasuusluokiteltujen tietojen välitys fyysisesti suojattujen alueiden välillä – Aineiston sähköinen välitys.....	26
5.16	I-16 Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä – Aineiston välitys postilla ja kuriirilla	26
5.17	I-17 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Salassa pidettävien tietojen jäljentäminen – Tulostus ja kopiointi	27
5.18	I-18 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Turvasuustarkoituksia varten tapahtuva salassa pidettävien tietojen kirjaaminen	27
5.19	I-19 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Salassa pidettävää tietoa sisältävien tietoaisteiden hävittäminen	28
5.20	I-20 Salassa pidettävän tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Muutoshallintamenettelyt.....	29
5.21	I-21 Salassa pidettävien tietojen käsittely fyysisesti suojattujen alueiden sisällä – Fyysinen turvasuus	29
5.22	I-22 Salassa pidettävien tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä – Etäkäyttö ja etähallinta	30
5.23	I-23 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Ohjelmisto-haavoittuvuuksien hallinta	31
5.24	I-24 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - varmuuskopiointi....	31
6	Muutostenhallinta ympäristössä.....	32
7	Järjestelmän auditointi ja hyväksyntä	32
7.1	Traficomien arviointiprosessi	32
8	KATAKRIN kehitysideat	Virhe. Kirjanmerkkiä ei ole määritetty.
9	Pohdinta.....	34
	Lähteet	36

Kuviot

Kuvio 1 Yksinkertaistettu verkkotopologia.	11
---	----

Kuvio 2 Arviointiprosessi yksinkertaistettuna.....	33
--	----

1 Johdanto

Yrityksellä Huld Oy oli tarve käsitellä turvallisuusluokkaan IV luokiteltua tietoa, jota aikaisemmin käsiteltiin erilliskoneilla, mutta yrityksellä oli halu löytää käyttäjäystävällisempi ratkaisu ongelmaan. Huld päätti toteuttaa projektin, jossa luodaan monihanke käyttöön soveltuva turvallisuusluokka IV-ympäristö. Tarve oli pystyä käsittelemään useiden eri tiedonmistajien tietoa käyttäen yhtä ympäristöä, josta syystä piti huomioida kaikki vaatimukset sillä tasolla, että kaikki tiedonmistajat voivat hyväksyä ympäristön toteutuksen ilman yhden tiedonmistajan ympäristössä mahdollisia hyväksytyjä poikkeuksia hallintakeinojen toteutuksessa.

Työn konkreettiseen osuuteen kuului ympäristön palvelinten ja verkkolaitteiden hankinta, kyseisten laitteiden asennus ja niiden konfigurointi tietoturvalliseksi. Ympäristön turvaluokituksen takia, konfiguraatioita ei voi tarkemmin paljastaa. Opinnäytetyön tavoitteena on luoda yksinkertaistettu ja julkinen versio ympäristön kuvauksesta.

Tämä opinnäytetyö sisältää kuvauksen monihanke käyttöön soveltuvasta turvaluokitellusta ympäristöstä, joka ylittää turvallisuusluokkaan IV (TL IV). Yleisesti TL IV ympäristöjä rakennetaan yhden projektin tarpeisiin nähden, eikä monihankeympäristönä. Haasteena on selkeästi, miten estetään ylläpitäjän pääsyä salassa pidettäviin tietoihin, koska kaikille ylläpitäjille ei ole järkevää tehdä henkilöturvallisuusselvitystä jokaisen tiedonmistajan toimesta, joka on turvaluokitellun tiedon käsittelemisen edellytys. Ympäristössä on myös välttämätöntä estää projektien väliset tietovuodot. Jokaikaisella projektiin osallistujalla tulee olla pääsy vain omiin projekteihin.

1.1 Tietoa toimeksiantajasta

Opinnäytetyön toimeksiantajana toimi Huld Oy, joka on eurooppalainen teknologisen suunnittelun asiantuntijatalo. Huld syntyi suunnittelutoimisto RD Velhon ja ohjelmistotalo SSF (Space Systems Finland) yhdistymisen johdosta. Huldin henkilöstöön kuuluu yli 450 henkilöä. Huldin toimialat ovat digitaaliset palvelut ja ohjelmistot, tuotemuotoilu ja -kehitys, sulautetut ratkaisut ja turvallisuus. Huld keskittyy työnteossaan käyttäjien tarpeisiin, kestäväyyteen sekä turvallisuuteen. (Home, Huld, n.d.)

2 Ympäristössä käytetyt palvelut

2.1 AD DS

Active Directory Domain Services (AD DS) tarjoaa menetelmiä hakemistotietojen tallentamiseen ja näiden tietojen saattamiseksi verkon käyttäjien ja järjestelmänvalvojien saataville. AD DS esimerkiksi tallentaa käyttäjätietotiedot ja sallii muiden valtuutettujen käyttäjien käyttää näitä tietoja samassa verkossa. (Active Directory Domain Services Overview, 2021.)

Active Directory tallentaa tiedot verkossa olevista objekteista ja tekee niistä selkeän järjestelmänvalvojien ja käyttäjien löydettävissä ja käytettäviksi. Objektit ovat yleensä jaettuja resursseja, kuten palvelimia, laitteita, tulostimia sekä verkon käyttäjä- ja tietokonetilejä. Suojaus on integroitu Active Directory -kirjautumistodennuksen ja hakemisto-objektien hallinnan kautta. Yhdellä verkkokirjautumisella järjestelmänvalvojat voivat hallita hakemistotietoja ja organisaatiota verkossa, ja valtuutetut verkon käyttäjät voivat käyttää resursseja missä tahansa verkossa. (Active Directory Domain Services Overview, 2021.)

2.2 AD CS

Active Directory Certificate Services (AD CS) tarjoaa mukautettavia palveluja julkisen avaimen infrastruktuurin (PKI) varmenteiden myöntämiseen ja hallintaan, joita hyödynnetään julkisen avaimen tekniikoita käyttävissä ohjelmistoturvajärjestelmissä. AD CS:n tarjoamia varmenteita voidaan käyttää tietokone-, käyttäjä- tai laitetilien todentamiseen verkossa. Varmenteita voidaan myös käyttää sähköisten asiakirjojen ja viestien salaamiseen ja sähköiseen allekirjoittamiseen. (Active Directory Certificate Services (AD CS) Introduction, 2014.)

2.3 Atlassian Confluence

Confluence on tiimityöskentelyyn luotu työkalu ja sen on kehittänyt Atlassian. Confluencia käytetään perusviestintään, projektinhallintaan ja dokumentointiin. Confluencen tavoitteena on luoda keskitetty työympäristö, joka nopeuttaa ja helpottaa työskentelyä tiimeille. Confluence on tärkeä osa Atlassianin tuoteperhettä ja se integroituu Atlassianin muiden tuotteiden kanssa. Confluence on myös integroitavissa yrityksen muiden sovellusten kanssa. (Confluence basics, n.d.)

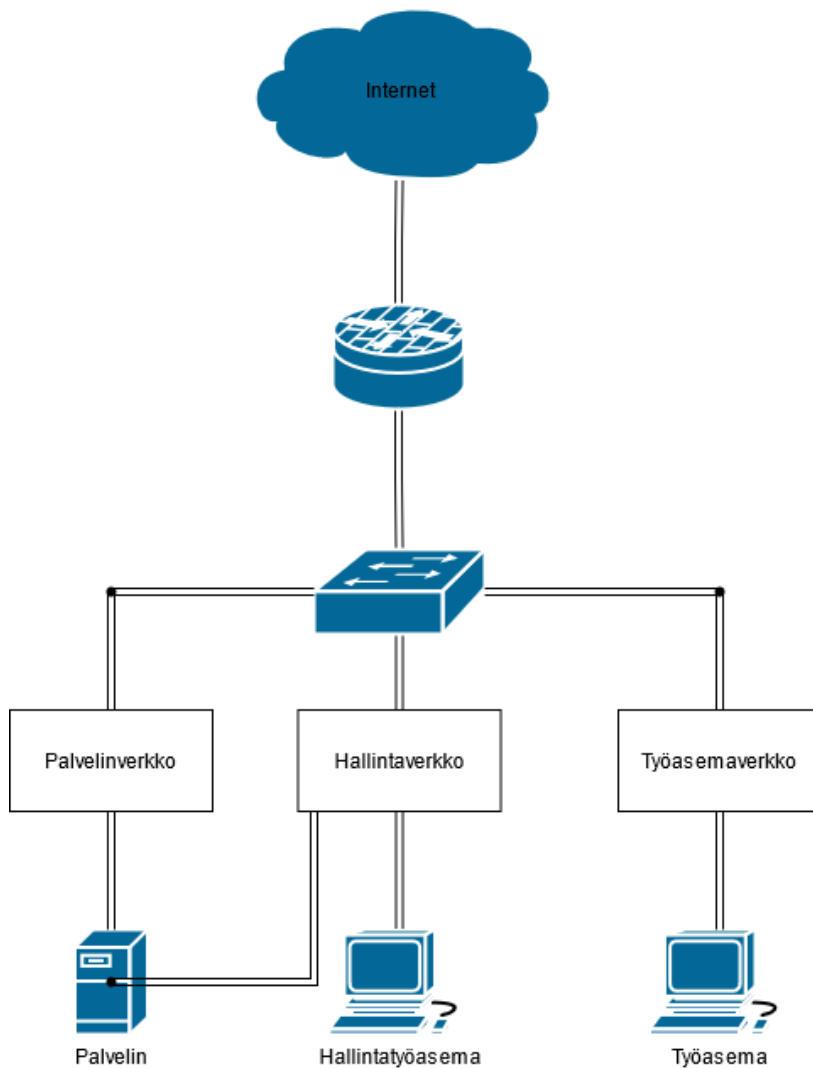
2.4 Atlassian Jira

Jira Software on Atlassianin kehittämä ongelmanseurantatyökalu, joka mahdollistaa virheiden seurannan ja ketterän projektinhallinnan. Jira tarjoaa monta eri tapaa kuvata ja seurata vianetsinnän selvitystä ja etenemistä. Yhdistettynä Confluenceen Jira tarjoaa enemmän vaihtoehtoja työskentelyyn ja mahdollistaa ketterän projektityöskentelyn. Työjonoja voidaan rakentaa Jirassa viitaten samalla sulavasti dokumentointiin Confluencessa. (What is Jira used for?, n.d.)

3 Kuvaus tuotantoympäristöstä

Ympäristö on turvaluokiteltu ja projekteja varten kehitetty erillisympäristö, joka on rakennettu vastaamaan KATAKRI (kansallinen turvallisuusauditointikriteeristö) 2015 turvallisuusluokka IV-tasolle määrittämiä vaatimuksia. Ympäristössä on huomioitu myös ne vaatimukset, joita edellytetään monihankeympäristössä eli ympäristössä voidaan käsitellä useiden eri tiedonantajien tietoa.

Ympäristö koostuu kolmesta eri verkkosegmentistä, jotka on erotettu toisistaan palomuurilla (ks. kuvio 1). Eri Virtuaalisten lähiverkkojen välissä kulkeva liikenne kulkee palomuurin läpi, jossa liikenne suodatetaan palomuurisääntöjen perusteella.



Kuvio 1 Yksinkertaistettu verkkotopologia.

3.1 Ympäristön laitteet

Ympäristö on eristetty muista verkoista palomuurilla, käytössä on laite, joka toimii reitittimenä ja palomuurina. Kytkimenä on konfiguroitava kytkin, jonka turvallisuus vastaa turvaluokka IV vaatimuksia. Verkkolaitteet käyttävät ainoastaan tietoturvallisia protokollia hallintayhteyksiin. Ympäristössä on myös käytössä Windows 10 työasemia, GNU/Linux- ja Windows -palvelimia.

3.1.1 Palomuuuri ja reititin

Käytetty laite toimii reitittimenä sekä palomuurina. Verkko on jaettu eri segmentteihin, käytön ja liitettyjen laitteiden mukaan. Verkossa on erillinen työasemaverkko, palvelinverkko ja hallintaverkko.

Työasemaverkossa on ainoastaan kiinnitettynä työasemat. Reititin toimii myös DHCP (Dynamic Host Configuration Protocol) palvelimena työasemaverkolle. DHCP tarjoaa staattisia osoitteita kyseisen laitteen MAC (Media Access Control) osoitteen perusteella. Palvelinverkossa on ainoastaan kiinnitettynä palvelinten käytön mahdollistavat rajapinnat.

Hallintaverkossa on kaikki ylläpito- ja hallintayhteydet ympäristön osalta. Palvelimilla on erilliset rajapinnat Palvelin- sekä ylläpitoverkkoon. Ylläpitotoimet suoritetaan hallintaverkosta käsin. Etäyhteydet ja muut hallintatavat ovat vain hallintaverkosta mahdollisia.

Palomuurien säännöt ovat laadittu erittäin tiukkaan. Kaikki liikenne, mikä ei ole tarpeellista, estetään. Ainoastaan tunnettuihin ennalta hyväksytyihin verkkoihin ja osoitteisiin liikennöinti on sallittua. Välttämättömällä liikenteellä tarkoitetaan minimiä millä kaikki tarvittavat palvelut toimivat. Julkiseen verkkoon päin rajoitusta hallitaan myös välityspalvelimella, joka toimii valkolistauksena. DNS (Domain Name System) palvelimella toteutetaan myös suodatusta ja ainoastaan ennalta hyväksytyihin toimialueisiin on mahdollista yhdistää.

Palomuurin kaikki lokitiedot kerätään lokipalvelimelle. Palomuuuri on myös valvonnan piirissä, käyttäen SNMP:tä (Simple Network Management Protocol), jolla palomuurista kerätään ajankohtaista tietoa.

3.1.2 Kytkin

Kytkin erottelee verkot VLANeja käyttäen (Virtual Local Area Network), erottelu tapahtuu ethernet porttien perusteella. Kytkin on kovennettu laitevalmistajan ohjeiden mukaisesti. Kytkin myös seuraa liitettyjä laitteita ja hälyttää mahdollisista väärinkäytöksistä ja väärinkytkeytyistä tai tuntemattomista laitteista. Kytkin myös poistaa mahdollisen väärinkäytöksen kohteena olevan fyysisen portin käytöstä. Kytöntä valvotaan aktiivisesti käyttäen SNMP:tä.

3.1.3 Valvontapalvelin

Valvontapalvelimessa toimii lokienkeräyspalvelin ja erillinen valvontakomponentti, jotka valvovat ja taltioivat ympäristön toimintaa. Palvelin myös ilmoittaa mahdollisista ongelmista tai väärinkäytöksistä.

Mahdollisesti hyökkäävän ylläpitäjän varalta, ylläpitäjältä on poistettu pääsy valvontapalvelimen hallintaelimiin täydellisesti. Ylläpitäjällä on mahdollisuus seurata lokeja ja virheilmoituksia keskitetysti palvelimen kautta, mutta muutoksia on mahdoton tehdä ylläpitäjän toimesta. Valvontapalvelimella toimii siis täysin erillinen henkilö ylläpitotoimissa, jolla taas ei ole ylläpito-oikeuksia muihin järjestelmiin kuin valvontapalvelimelle. Ylläpitäjälle on hätätilanteeseen määritetty ylläpitotunnus, mutta kyseisen tunnuksen käyttämisestä jää sekä fyysinen että digitaalinen jälki.

3.1.4 Lokipalvelin

Ympäristöstä kerätään lokia keskitetysti palvelimelle. Kaikista ympäristön palvelimista kerätään lokit keskitetysti talteen. Lokijärjestelmän suojaus on toteutettu siten, että ylläpitäjillä on vain katselu-oikeudet lokijärjestelmään. Lokijärjestelmän ylläpidosta vastaa erillinen henkilö, jolla ei ole ylläpito-oikeuksia muihin järjestelmiin ympäristössä. Lokit ovat salattuja palvelimella, arkistoissa sekä varmuuskopioissa.

3.1.5 Dokumentointi- ja Välityspalvelin

Dokumentointipalvelin tarjoaa Atlassian Jira ja Atlassian Confluencen tuotteiden käyttöliittymät ja hallinnan. Palvelimella on toiminnassa myös ympäristössä käytetty välityspalvelin. Palvelimella on myös sähköpostirele, jotta hälytykset saadaan sähköpostilla perille.

Atlassian Jira tarjoaa tiketöintijärjestelmän sekä käyttäjähallinnan Jiralle ja Confluencelle. Kaikki ylläpitomuutokset tapahtuvat tikettien kautta ja aina turvallisuuspäällikön hyväksynnällä. Muutospyyntöön hyväksynnän jälkeen ylläpitäjä toteuttaa muutokset, dokumentoi ne Confluenceen ja sulkee tiketin Jirasta. Tiketeillä ylläpidetään myös seurantaa ongelmien tai tehtävien etenemisestä.

Atlassian Confluence tarjoaa dokumentointialustan. Ylläpitäjille on tarjolla omat ylläpitäjäsivustonsa, jossa säilytetään ylläpitäjille tarkoitettua dokumentaatiota ja ohjeita ympäristön ylläpitämiseen. Ylläpitäjäsivustolla on myös ylläpitoloki, johon merkitään kaikki ylläpitotoimet. Ylläpitolokiin merkitään palvelin tai palvelu, johon tehtiin muutoksia, milloin muutoksia tehtiin, kuka teki muutoksia, mitä muutoksia tehtiin ja tarvittaessa muutoksen hyväksynnän varmistava tiketti. Tikettiin merkataan tarkemmin ratkaisu tai ongelmanetsinnän tulokset.

Välityspalvelin sallii pääsyn vain sallittuihin osoitteisiin, estäen muut. Välityspalvelimen käyttö on rajoitettu palvelin- ja työasemaverkkoihin. Ylläpitoverkosta ei ole pääsyä välityspalveluun.

3.1.6 Windows Server

Windows palvelimella on ADDS (Active Directory Directory Services), AD CS (Active Directory Certificate Services), virustorjuntaohjelman keskitetty hallinta ja varmuuskopiointiin käytettävän työkalun hallinta. AD DS hallitsee käyttäjätunnuksia, tietokoneiden hallintaa ja käyttäjien kirjautumisen toimikorttien avulla. AD DS hallitsee myös kirjautumisten rajoitusta tietokonekohtaisesti.

AD CS Hallinnoi ympäristön varmenteita ja varmenneketjuja. Ympäristössä on myös kolmannen osapuolen hallinnoimia varmenteita, joita jaetaan AD:n välityksellä. Jokainen palvelin tarvitsee vähintään yhden varmenteen hallintapaneeliaan varten, joka toimii HTTPS (Hypertext Transfer Protocol Secure) käyttäen. Ympäristön jokaisessa palvelimessa on käytössä ympäristön oma varmenne. Palvelimien itse allekirjoitettuja varmenteita ei hyväksytä tuotantoon. Toimikorttien ja VPN (Virtual Private Network) -palvelun varmenteet tulevat kolmannelta osapuolelta. Näiden käyttö on erikseen hyväksytty AD:n jakamissa tietoturvakontrolleissa.

Windows Server hallinnoi myös GPO (Group Policy Object) kautta tapahtuvia hallintatoimenpiteitä ja tietoturvakontrolleja. Mahdolliset keskitetyt skriptit jaetaan AD-palvelimelta.

3.1.7 Windows 10 Työasemat

Työasemat käyttävät Windows 10 käyttöjärjestelmää, joka on kovennettu KATAKRIn vaatimin tavoin. Osa tietoturvaprotokollista pitää luoda käsin, ennen varsinaista asennusta, esimerkiksi liitet-

tävien ja sisäisten laitteiden estäminen BIOSissa (Basic Input Output System). Suurinta osaa työasemia koskevista kovennuksista asetetaan ryhmäpolitiikkaa käyttäen. Ryhmäpolitiikka seuraa linjauksia CIS:in (Center for Internet Security) asettamasta kovennusohjeesta. Kovennusta päivitetään Windows 10 version mukaan.

SRP (Software Restriction Policy) on käytössä GPO:n kautta, joka mahdollistaa sovellusten ajon rajoittamisen. Sovellusten rajoittamiseen käytetään valkolistausta, kaikki paitsi välttämättömät sovellukset ovat estetty. Sallittuja sovelluksia olivat vain ennalta määritetyt tarvittavat sovellukset. Windowsin omat sovellukset sallittiin, koska huomattiin, että niiden yliampuva esto rikkoo käyttöliittymän. Kaikki Windowsin omat sovellukset, joita voisi yrittää käyttää vahingollisesti estettiin erillisellä säännöllä. Käyttäjien kirjoitusoikeuksia valvotaan kokeilemalla, pystyykö käyttäjä tunnuksillaan kirjoittamaan SRP:ssä määriteltyihin sallittuihin sijainteihin. Jos kirjoittaminen onnistuu, lähtee tapahtumasta ilmoitus lokipalvelimelle, joka sitten hälyttää ylläpitäjiä ja ympäristön valvonnasta vastaavia henkilöitä.

3.1.8 VPN-palvelin

VPN-palvelin on kolmannen osapuolen tarjoama palvelu, johon kuului itse laitteisto, ohjelmistot, VPN-palvelun käyttämät varmenteet ja lisenssit. Käytössä oleva VPN-palvelu on hyväksytty viranomaisen puolesta Turvallisuusluokka III tasolle.

VPN kautta tapahtuva liikenne on aina pakotettu kiertämään ympäristön kautta. VPN kiertäminen ei ole mahdollista ilman ylläpitäjän oikeuksia. VPN lähtee myös automaattisesti päälle koneen käynnistyksen yhteydessä, joten työasemat ovat aina käynnissä ollessaan yhteydessä ympäristön palvelimiin.

3.2 Salassa pidettävien tietojen tallennus

Salassa pidettävät tiedot tallennetaan salattuihin tiedostosäiliöihin. Tiedostosäiliöt on mahdollista tehdä usealla eri sovelluksella, jotka kansallinen turvallisuusviranomainen Traficom NCSA (National Communications Security Authority) on hyväksynyt kyseisen turvallisuusluokan tiedon tallentamiseen.

3.2.1 Salassa pidettävien tietojen pääsynhallinta

Pääsynhallinta salassa pidettäviin tietoihin toteutetaan tiukalla salasanapolitiikalla. Jokainen käyttäjä luo itselleen pääsalasanan, jolla käyttäjä voi todentaa pääsyn hänelle sallittuihin tiedostosäiliöihin. Ylläpitäjällä ei ole mahdollisuutta nollata tiedostosäiliöiden salasanoja ja tätä kautta hyödyntää käyttäjien oikeuksia. Projektin tiedostosäiliön pääsynhallinnasta vastaa erikseen nimetty henkilö ja jokaisella projektilla on oma vastuhenkilö.

Pääsynhallinnan pohjana toimii AD:n tarjoamat käyttäjätunnukset, salaustuote lisää oman salasanansa käyttäjän tietoihin, jota voidaan käyttää salaustoimenpiteisiin. Ylläpitäjällä ei ole oikeuksia, eikä mahdollisuutta nollata käyttäjän asettamaa salaustuotteen salasanaa tai hyväksikäyttää käyttäjien oikeuksia.

4 KATAKRI

KATAKRI on auditointityökalu, joka on suunniteltu viranomaisten käytettäväksi auditointitarkoituksiin. KATAKRilla käyttäen arvioidaan yrityksen kykyä suojata salassa pidettävää tietoa. KATAKRI itsessään ei määritä pakollisia vaatimuksia tietoturvaan. (KATAKRI 2015, 2).

KATAKRI yhdistää minimivaatimukset, jotka perustuvat kansalliseen lainsäädäntöön ja kansainvälisiin tietoturvavelvollisuuksiin. Tärkein kansallinen lainsäädäntö tässä yhteydessä on Valtioneuvoston asetus valtionhallinnon tietoturvasta (681/2010). (KATAKRI 2015, 2).

4.1 KATAKRIn rakenne

KATAKRIn vaatimukset on jaettu kolmeen eri alaosiioon. Turvallisuusjohtamista käsittelevässä (T) osa-alueessa tavoitteena on varmistaa, että organisaatiolla on riittävät turvallisuushallintakyvyt ja -taidot turvallisuusluokiteltujen tietojen suojaamiseen. Organisaation on täytettävä tässä alajaossa kuvatut perustasoa koskevat vaatimukset. Fyysistä turvallisuutta käsittelevässä osassa (F) kuvataan turvallisuusvaatimukset fyysiselle ympäristölle, jossa turvaluokiteltuja tietoja käsitellään. (KATAKRI 2015, 3).

Teknistä tietoturvallisuutta koskeva (I) osa-alue puolestaan kuvaa teknisen tietokoneympäristön turvallisuusvaatimuksia. Vaatimukset on kuvattu siten, että ne mahdollistavat erilaiset toteutukset. Lisätietokentissä tulkinnan tueksi on koottu esimerkkejä toteutuksesta, jossa kuvatut menettelyt voivat saavuttaa hyväksyttävän vähimmäistason useimmissa ympäristöissä. Toteutusesimerkit eivät ole sitovia, ja ne voidaan korvata muilla vastaavan tason suojauksilla. Toteutuksen lähteitä ovat esimerkiksi tiedonhallintokomitean suositukset, VAHTI-ohjeet sekä EU:n turvallisuussääntöjä täydentävät ohjeet. (KATAKRI 2015, 3).

Vaatimukset tai toteutusesimerkit eivät kuvaa riittävää suojaa kaikkiin ympäristöihin tai erityistapauksiin. Esimerkiksi turvaluokiteltuja tietoja käsiteltäessä, joiden on katsottu olevan poikkeuksellisen kiinnostavia ulkopuolisille, on perusteltua täydentää vähimmäissuojaa lisäsuojatoimenpiteillä. (KATAKRI 2015, 3).

4.2 KATAKRIn käyttö

KATAKRia voidaan käyttää tarkastustyökaluna arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yhtiön turvallisuusraportissa ja viranomaisten tietojärjestelmien turvallisuusarvioinneissa. Turvajärjestelyjen riittävyyden arvioinnin on perustuttava järjestelmälliseen riskinarviointiin. Turvallisuusriskien hallinnan on pyrittävä toteuttamaan yhdistelmä turvatoimia, joilla saavutetaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja jäljellä olevan turvallisuusriskin välille. Luokittelemattomien kansallisten turvaluokiteltujen tietojen suojausta voi soveltaa suojausluokan IV vaatimuksin. (KATAKRI 2015, 3).

KATAKRia ei ole tarkoitettu käytettäväksi sellaisenaan julkisten hankintojen turvavaatimuksena. Julkisissa hankinnoissa tarkat turvallisuusvaatimukset olisi määriteltävä erikseen ottaen huomioon hankinnan riskit ja erityistarpeet. Yksittäinen projekti voi sisältää muita kuin KATAKRissa koottuja luottamuksellisten tietojen käsittelyä ja suojausta koskevia vaatimuksia. Niiden vaatimusten täyttymistä, jotka eivät sisälly KATAKRiin, voidaan arvioida esimerkiksi tietoja omistavan viranomaisen tekemillä projektiakohtaisilla arvioinneilla. (KATAKRI 2015, 3).

5 KATAKRI I-osion vaatimukset sovellettuna ympäristöön

KATAKRIn I-osio keskittyy laitteiden tietotekniseen turvallisuuteen ja on pääpisteenä tässä opin-
näytetyössä. Muut KATAKRIn osuudet on sivuutettu. Kriteerit on käyty yksi kerrallaan läpi ja ker-
rottu miten kyseistä kriteeriä on sovellettu ympäristöön. Kriteereihin vastaaminen on toteutettu
myös siten, että monihankeympäristön tarvittavat lisätoimenpiteet toteutuvat.

Opinnäytetyössä käytetään lähteenä KATAKRI 2015, sillä ympäristön rakentaminen aloitettiin, kun
KATAKRI 2020 ei ollut vielä saatavilla. Ympäristön valmistuttua ensimmäisen hyväksyntäauditoin-
nin aikaan arviointilaitoksilla ei myöskään ollut vielä pätevyyttä tehdä KATAKRI 2020 mukaista arvi-
ointia, joten ensimmäisessä arvioinnissa kriteeristönä käytettiin tästä syystä KATAKRI 2015 -ver-
siota. Tämän jälkeen ympäristö arvioitiin myös KATAKRI 2020 -kriteeristön mukaisesti
viranomaisten toimesta. Uudessa versiossa ei ollut niin merkittäviä muutoksia, että se olisi aiheut-
tanut muutoksia ympäristössä toteutettuihin hallintakeinoihin.

5.1 I-01 Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – verkon ra- kenteellinen turvallisuus

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Tietojenkäsittely-ympäristö on erotettu muista ympäristöistä.

*2) Tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin
edellyttää vähintään palomuuriratkaisun käyttöä.*

*3) Hallitun fyysisen turva-alueen ulkopuolelle menevä liikenne salataan viranomaisen
ko. suojaustasolle hyväksymällä salausratkaisulla (vrt. I 12 ja I 15). (KATAKRI 2015,
31)*

Toteutimme vaatimukset seuraavasti: Erillisympäristö on erotettu muista ympäristöistä palomuu-
rilla. Salassa pidettävää tietoa voidaan lähettää ainoastaan hyväksyttyihin turvaposteihin. Interne-
tiin liikennöintiä on rajoitettu erittäin vahvasti palomuurilla, sekä välityspalvelinta käyttäen. Aino-
astaan välttämätön liikenne on sallittu ja silloinkin vain salattuja protokollia käyttäen.

5.2 I-02 Vähimpien oikeuksien periaate - tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöt ko. turvallisuusluokan sisällä

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöt on toteutettava vähimpien oikeuksien (least privilege) ja monitasoisen suojaamisen (defence in depth) periaatteiden mukaisesti (KATAKRI 2015, 33).

Toteutimme vaatimukset seuraavasti: Verkot ovat eroteltu VLAN:eja käyttäen, VLANien välillä ei ole yhteyttä, ellei sitä palomuurilta ole erikseen sallittu. Palomuurin ja välityspalvelimen suodatussäännöt perustuvat siihen, että kaikki paitsi välttämätön liikenne estetään. Tarvittavat portit/IP-osoitteet sallitaan ainoastaan ennalta hyväksytyihin portteihin ja osoitteisiin.

Työasemilla ja palvelimilla on myös omat palomuurinsa, jotka toimivat samalla periaatteella. Lisänä näihin palomuuereihin on se, että sovellukset hyväksytään myös erikseen. Työasemien palomuuereja hallinnoidaan keskitetysti ryhmäpolitiikkaa käyttäen. Muiden palomuurien hallinta tapahtuu yksitellen, ainoastaan ylläpitäjällä on pääsy hallitsemaan palomuuereja. Muutokset toteutetaan erikseen turvallisuuspäällikön hyväksynnällä.

5.3 I-03 Tietojenkäsittely-ympäristön turvallisuus koko elinkaaren ajan – suodatus- ja valvontajärjestelmien hallinnointi

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Suodatus- ja valvontajärjestelmien tarkoituksenmukaisesta toiminnasta huolehditaan koko tietojenkäsittely-ympäristön elinkaaren ajan.

2) Liikennettä suodattavien tai valvovien järjestelmien asetusten lisääminen, muuttaminen ja poistaminen on vastuutettu ja organisoitu.

3) Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia.

4) Liikennettä suodattavien tai valvovien järjestelmien asetukset ja haluttu toiminta tarkastetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä. (KATAKRI 2015, 34)

Toteutimme vaatimukset seuraavasti: Suodatus- ja valvontajärjestelmiä seurataan säännöllisesti koko elinkaarensa ajan. Mahdollisia väärinkäyttöjä seurataan automatisoidusti ja aktiivisesti. Sääntöjen muokkaaminen vaatii turvallisuuspäällikön hyväksynnän, jolloin ylläpitäjä toteuttaa muutokset pyydettyäessä. Dokumentaatiota ylläpidetään koko ympäristön elinkaaren ajan juoksevasti. Jokainen muutos ympäristöön dokumentoidaan tarvittavalla tarkkuudella, jotta selviää, kuka on tehnyt muutoksia ja milloin. Asetukset tarkastetaan säännöllisesti dokumentaatiossa määrätyn aikavälin mukaisesti. Asetuksien toiminta varmistetaan testaamalla, ja niitä voidaan muokata, jos kyseisille asetuksille ei ole enää tarvetta. Varmuuskopioiden toiminta testataan säännöllisesti dokumentaatiossa määritellyn aikavälin mukaisesti.

5.4 I-04 Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen – hallintayhteydet

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Hallintayhteydet on rajattu suojaustasoittain, ellei käytössä ole viranomaisen ko. suojaustasoille hyväksymää yhdyskäytäväratkaisua.

2) Hallintaliikenteen sisältäessä salassa pidettävää tietoa ja kulkiessa matalamman suojaustason ympäristön kautta, salassa pidettävät tiedot on salattu viranomaisen hyväksymällä salaustuotteella.

3) Hallintaliikenteen kulkiessa ko. suojaustason sisällä, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella viranomaisen erillishyväksyntään perustuen.

4) Hallintayhteydet on rajattu vähimpien oikeuksien periaatteen mukaisesti. (KATAKRI 2015, 35)

Toteutimme vaatimukset seuraavasti: Hallintayhteydet on eriytetty muusta TLIV ympäristöstä VLANeja käyttäen. Hallintaympäristöön pääsee vain erikseen hyväksytyllä laitteella. Hallintaliikennettä ei kulje matalammilla suojaustasoilla. Hallintayhteydet toimivat vain turvallisilla protokollilla.

Hallintayhteydet on rajattu ainoastaan niitä tarvitseville henkilöille. Loki- ja valvontapalvelimen hallinta on erikseen eriytetty pelkästään turvallisuuspäällikön käytettäväksi, jotta voidaan varmistua lokien autenttisuudesta ja ettei niitä ole muokattu ylläpitäjän toimesta.

5.5 I-05 Suojattavien tietojen siirtäminen fyysisesti suojattujen alueiden ulkopuolella - langaton tiedonsiirto

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Langattomien verkkojen radorajapintaa käsitellään kuin julkista verkkoa (KATAKRI 2015, 37).

Toteutimme vaatimukset seuraavasti: Langattomia verkkoja käytetään ainoastaan VPN-kykeneväisissä laitteissa. Kaikki liikenne kulkee tunnelloituna ja salattuna viranomaisen hyväksymillä salausmetodeilla.

5.6 I-06 Vähimpien oikeuksien periaate – pääsyoikeuksien hallinnointi

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Tietojenkäsittely-ympäristön käyttäjille ja automaattisille prosesseille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä.

2) Salassa pidettävien tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan sekä tietojärjestelmien asianmukaisilla turvallisuusjärjestelyillä ja muilla toimenpiteillä. (KATAKRI 2015, 39)

Toteutimme vaatimukset seuraavasti: Käyttöoikeuksia valvotaan ja muokataan tarpeen mukaan säännöllisesti. Käyttöoikeuksien muokkaamista seurataan ja siitä syntyy merkintä lokipalvelimelle, lisäksi dokumentointiin merkataan käyttöoikeuksien muutoksista merkintä.

Salassa pidettävät tiedot on salausta käyttäen tallennettu tiedostosäiliöihin erikseen ja ne on suojattu tietoturvalisillä salasanoilla. Ylläpitäjällä ei ole pääsyä erillisten hankkeiden tiedostosäiliöiden tietoon käsiksi. Salassa pidettävien materiaalin oikeuksia seurataan säännöllisesti.

5.7 I-07 Monitasoinen suojaaminen – tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät tietojenkäsittely-ympäristön toimijoiden tunnistamiseen. (KATAKRI 2015, 40).

Toteutimme vaatimukset seuraavasti: Ympäristössä on käytössä toimikortilla tapahtuva kirjautuminen ympäristöön. Windows AD kirjautumiseen tarvitaan toimikortti ja käyttäjäkohtainen PIN-koodi. Toimikortteja seurataan ja tarkastetaan säännöllisesti.

Palveluissa, joissa ei ole toimikorttitoiminnallisuutta käytetään turvallisia salasanoja, joiden pituus on määritelty asianmukaiseksi politiikassa ja niiden säilytys on turvallista, ainoastaan asianmukaisilla on mahdollisuus päästä salasanoihin käsiksi.

5.8 I-08 Vähimmäistoimintojen ja vähimpien oikeuksien periaate – järjestelmäkovennus

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Käyttöön on otettu vain käyttövaatimusten ja tietojen käsittelyn kannalta olennaiset toiminnot, laitteet ja palvelut.

2) Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovenettu asennus.

3) Kovenettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi. (KATAKRI 2015, 42)

Toteutimme vaatimukset seuraavasti: Kaikki ylimääräiset ja tarpeettomat laitteet, toiminnot ja palvelut on otettu pois päältä tai estetty muilla tavoin.

Ympäristöön on määritelty erillinen ohje, jolla saavutetaan työaseman tai palvelimen kovennettu asennus. Ohjeessa läpikäydään yksityiskohtaisesti läpi koneelle tarvittavat asetusmuutokset esimerkiksi BIOSissa ja käyttöjärjestelmän puolella. Normaaleilta käyttäjiltä on estetty GPO:n kautta ajamasta mitään ylimääräisiä palveluita, sekä estetty tuntemattomien laitteiden liitäntä.

5.9 I-09 Monitasoinen suojaaminen – haittaohjelmasuojaus

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen (KATAKRI 2015, 44).

Toteutimme vaatimukset seuraavasti: Ympäristössä on käytössä haittaohjelmien estoon tarkoitettu ohjelmisto, jossa on myös keskitetty hallinta. Päivitykset on mahdollistettu asianmukaisilta päivityspalvelimilta. Mahdollisista uhista tulee hälytykset sähköpostiin ylläpitäjille. Palveluiden haavoittuvuusilmoituksia seurataan myös aktiivisesti ylläpitäjän toimesta. Mahdollisia haavoittuvuuksia havaitaan myös erinäisillä työkaluilla, joita ajetaan säännöllisesti.

5.10 I-10 Monitasoinen suojaaminen – turvallisuuteen liittyvien tapahtumien jäljitettävyyden

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitsemiseksi tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen (KATAKRI 2015, 46).

Toteutimme vaatimukset seuraavasti: Ympäristössä on käytössä loki- ja valvontapalvelin, jotka aktiivisesti monitoroivat työasemien ja palvelimien toimintaa. Jäljitettävyyden on mahdollistettu sillä,

että lokia kerätään kaikilta laitteilta ja niitä säilytetään turvallisesti mahdollisimman pitkään. Lokipalvelin helpottaa suuren lokimäärän järjestelemistä ja helpottaa tiettyjen tapahtumien hakemista. Automatisoidut hälytykset, jotka perustuvat osittain lokitapahtumiin vähentävät manuaalista työtä. Tietojen autenttisuudesta varmistutaan tiukalla politiikalla, pääsyoikeuksia lokipalvelimelle on vain valituilla henkilöillä. Ylläpitäjältä on estetty kaikki oikeudet lokipalvelimelle, paitsi katseluoikeudet, jotta ylläpitäjä voi seurata ympäristön toimintaa lokien näkökulmasta. Tällä menettelytavalla varmistutaan siitä, ettei ylläpitäjä pääse muokkaamaan lokimerkintöjä.

5.11 I-11 Monitasoinen suojaaminen – poikkeamien havainnointikyky ja toipumien

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Tietojenkäsittely-ympäristössä toteutetaan luotettavat menetelmät, joilla pyritään havaitsemaan hyökkäys tietojenkäsittely-ympäristöä vastaan, rajoittamaan hyökkäyksen vaikutukset mahdollisimman pieneen osaan tietoja tai tietojenkäsittely-ympäristön resursseja ja estämään muut vahingot, sekä palauttamaan tietojenkäsittely-ympäristön suojattu tilanne (KATAKRI 2015, 48).

Toteutimme vaatimukset seuraavasti: Käytössä oleva viruksentorjunta ohjelmisto, ilmoittaa mahdollisista hyökkäyksistä. Lokipalvelimeen on rakennettu hälytysmekanismeja, jotka reagoivat tiettyjen tapahtumien yhteydessä.

Mahdollisen hyökkäyksen leviämistä on rajoitettu palomuuerein, jotka toimivat myös aliverkkojen välillä, sekä työasemilla. Mahdollisia hyökkäyksiä myös hidastetaan, kun käyttäjille on asetettu oikeudet least-privilege mallin mukaisesti. Laitteiden omat palomuurit hidastavat myös lateraalista leviämistä.

5.12 I-12 Tietoturvaluustuotteiden arviointi ja hyväksyntä – salausratkaisut

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Viranomaisen on hyväksynyt käytetyt salausratkaisut (ja -tuotteet) ko. suojaustasolle ko. käyttöympäristössä salassa pidettävien tietojen luvattoman paljastumisen ja muuntelun estämiseksi (KATAKRI 2015, 49).

Toteutimme vaatimukset seuraavasti: Käytössä olevat salaus- ja tiedostosäiliöjärjestelmät ovat hyväksytyjä TRAFICOMin puolesta. Salaus- ja tiedostosäiliöjärjestelmien käyttöpolitiikka on myös hyväksytty viranomaisen puolesta.

5.13 I-13 Monitasoinen suojaaminen koko elinkaaren ajan – Ohjelmistoilla toteutettavat pääsynhallintatoteutukset

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Tietojenkäsittely-ympäristön turvallisuus, myös niiden tekniset ja muut kuin tekniset turvatoimet, testataan hyväksymisprosessin aikana sen varmistamiseksi, että asianmukainen turvaamistaso saavutetaan, ja sen tarkistamiseksi, että ne on moitteettomasti toteutettu, integroitu ja konfiguroitu.

2) Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn estämiseksi ja havaitsemiseksi tietojenkäsittely-ympäristössä järjestetään luotettavat menettelyt ohjelmistoilla toteutettavien pääsynhallintatoteutusten turvallisuudesta varmistumiseksi. (KATAKRI 2015, 50)

Toteutimme vaatimukset seuraavasti: Ympäristö on auditoitu Traficomien, sekä kolmannen osapuolen toimesta. Salassa pidettävät tiedot ovat salattuina ja ovat luettavissa ainoastaan asianmukaisilla henkilöillä, eli niillä, jotka on turvaselvitetty kyseiselle projektille. Tiedostosäiliöiden pääsy oikeuksien hallintavastuu kuuluu projektipäällikölle.

Mahdollisia väärinkäyttöjä seurataan aktiivisesti. Lokipalvelimelle tallennetaan mahdolliset edeltävät askeleet väärinkäytölle. Ylläpitäjällä ei ole oikeuksia lokipalvelimelle.

5.14 I-14 Monitasoinen suojaaminen – Hajasäteily (tempest)

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Turvatoimia toteutetaan salassa pidettäviin tietoihin liittyvässä tietojenkäsittely-ympäristössä viranomaisen ko. suojaustasolle hyväksymillä menetelmillä niin, että tahattomat sähkömagneettiset vuodot eivät vaaranna tietoja (TEMPEST-turvatoimet). Nämä turvatoimet on suhteutettava tiedon hyväksikäytön riskiin ja suojaustasoon. (KATAKRI 2015, 52)

Toteutimme vaatimukset seuraavasti: TL IV -ympäristöissä ei ole vaatimuksia TEMPEST-turvatoimille.

5.15 I-15 Turvallisuusluokiteltujen tietojen välitys fyysisesti suojattujen alueiden välillä – Aineiston sähköinen välitys

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Kun salassa pidettävää aineistoa siirretään hyväksytyjen fyysisesti suojattujen alueiden ulkopuolella, aineisto/liikenne salataan viranomaisen ko. suojaustasolle hyväksymillä menetelmällä.

2) Kun salassa pidettävää aineistoa siirretään hyväksytyjen fyysisesti suojattujen alueiden sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää riskinhallintaprosessin tulosten perusteella viranomaisen erillishyväksyntään perustuen. (KATAKRI 2015, 53)

Toteutimme vaatimukset seuraavasti: Fyysisesti siirrettävää salassa pidettävää aineistoa on sallittu siirrettävän ainoastaan viranomaisen hyväksymillä salatuilla USB-massamuisteilla. Salaamatonta liikennettä ei ympäristössä ole, jokaiseen hallintaliittymään on asetettu vähintään HTTPS -tasoinen salausta. Muu suojatun alueen ulkopuolelle kulkeva liikenne on salattu viranomaisen hyväksymillä menetelmällä.

5.16 I-16 Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä – Aineiston välitys postilla ja kuriirilla

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Tietojen siirtämisessä yksiköiden ja tilojen välillä fyysisesti suojattujen alueiden ulkopuolella on noudatettava seuraavaa:

1) Yleisenä sääntönä on, että salassa pidettävät tiedot siirretään tietoverkon yli sähköisesti viranomaisen hyväksymillä salaustuotteilla suojattuna.

2) Jos edellä mainittua menettelyä ei käytetä, salassa pidettävät tiedot kuljetetaan joko

a) viranomaisen hyväksymillä salaustuotteilla suojatuilla sähköisillä välineillä (kuten USB-muistitikut, CD-levyt, kiintolevyt); tai

b) kaikissa muissa tapauksissa, viranomaisen antamia ohjeita noudattaen. (KATAKRI 2015, 54)

Toteutimme vaatimukset seuraavasti: Tietoa siirretään julkisen verkon yli vain viranomaisen hyväksymällä salaustoteutuksella. Mahdollisissa muissa tapauksissa käytetään salattuja muistitikkuja, joiden turvallisuus vastaa KATAKRIn asettamia vaatimuksia.

5.17 I-17 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Salassa pidettävien tietojen jäljentäminen – Tulostus ja kopiointi

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Jäljennöksiin ja käännöksiin sovelletaan alkuperäistä asiakirjaa koskevia turvatoimia. (KATAKRI 2015, 56)

Toteutimme vaatimukset seuraavasti: Jäljennöksiin ja käännöksiin sovelletaan alkuperäistä asiakirjaa koskevia turvatoimia. Tuotoksia ei voi tallentaa muualle kuin salattuihin tiedostosäiliöihin. Välimuistissa säilyvät kopiot tyhjennetään jokaisella sammutuksella järjestelmästä. Käyttäjällä ei ole oikeuksia kaivaa välimuistista kopioita. Käyttäjien koulutuksella minimoidaan mahdollisuus, että käyttäjä itse kopioisi tuotoksia.

5.18 I-18 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Turvallisuustarkoituksia varten tapahtuva salassa pidettävien tietojen kirjaaminen

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Tietojenkäsittely-ympäristössä toteutetaan hallinnolliset ja tekniset toimenpiteet, jotka koskevat salassa pidettävien tietojen valvomista koko niiden elinkaaren ajan,

jotta autetaan estämään ja havaitsemaan tällaisten tietojen tahallinen tai tahaton vaarantuminen tai katoaminen. (KATAKRI 2015, 57)

Toteutimme vaatimukset seuraavasti: Seuranta salassa pidettäville tiedoille tehdään aktiivisesti ja automatisoidusti. Tietojen vahingollista vuotamista on minimoitu käyttäjäkoulutuksen ja käyttäjän oikeuksien rajaamisella minimiin.

Tietovuotoja estetään myös erinäisiä tekniikoita käyttäen esim. aktiivinen lokien seuranta ja automatisoitu valvonta. Hälytyksillä varmistetaan, että ylläpito on ajan tasalla ympäristöstä, vaikkei fyysisesti olisikaan paikalla. Fyysinen turvallisuus toimii myös hyvänä estäjänä tietojen vahingollista vuotamista vastaan. Tilaan on erittäin vaikea päästä ilman kulkuoikeuksia. Palvelimet ovat lukitussa kaapissa, jonka avain on vain ylläpitäjällä. Vara-avain on turvapussitettu hätätapauksia varten.

Väärinkäytösten havaitseminen tapahtuu lokipalvelimen kautta, jos joku tietty lokimerkintä ilmenee, niin lokipalvelin lähettää hälytyksen ylläpitäjille. Hallintapalvelin lähettää myös hälytyksiä mahdollisista väärinkäytöksistä.

5.19 I-19 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Salassa pidettävää tietoa sisältävien tietoaineistojen hävittäminen

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Ei-sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.

2) Sähköisten aineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.

3) Tietojärjestelmien käytön yhteydessä syntyvät tietoa sisältävät väliaikaistiedostot hävitetään säännöllisesti, jolleivät ne poistu tietojärjestelmästä automaattisesti. (KATAKRI 2015, 58)

Toteutimme vaatimukset seuraavasti: Paperinen materiaali tuhotaan turvallisuustasolle hyväksytyllä paperisilppurilla. Kovalevyjen ja muiden muistivälineiden tuhoamiseen on käytössä kolmannen osapuolen palvelu. Kovalevyt ja muistit tuhotaan totaalisesti kolmannen osapuolen toimesta, ja saamme todistuksen tuhoamisesta. Väliaikaistiedostot poistetaan aina viranomaisen hyväksymällä menetelmällä työaseman sammutuksen yhteydessä automatisoidusti käyttäen ryhmäpolitiikan kautta jaettua skriptiä.

5.20 I-20 Salassa pidettävän tiedon käsittelyyn liittyvän tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Muutoshallintamenettelyt

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Turvallisuuden varmistamista pidetään vaatimuksena koko tietojenkäsittely-ympäristön elinkaaren ajan sen alullepanosta käytöstä poistamiseen.

2) Turvallisuutta koskevat arvioinnit, tarkastukset ja uudelleentarkastelut suoritetaan määräajoin tietojenkäsittely-ympäristön toiminnan ja huollon aikana sekä poikkeuksellisten tilanteiden ilmetessä.

3) Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottamattomana osana muutosten ja asetusten hallintaprosessia. (KATAKRI 2015, 60)

Toteutimme vaatimukset seuraavasti: Turvallisuutta varmistetaan tiukalla päivitysrutiinilla ja haavoittuvuusskannauksilla. Turvallisuutta varmistetaan myös aktiivisesti seuraamalla ympäristön toimintaa. Mahdollisista poikkeamista johtuen, voidaan tehdä uusintatarkastus ympäristölle. Säännölliset uudelleentarkastukset kuuluvat toimintaan. Turvallisuusasiakirjoja päivitetään juoksevasti ympäristön kehittymisen mukana. Muutoksien tietoturvallisuus varmistetaan aina erikseen testamalla.

5.21 I-21 Salassa pidettävien tietojen käsittely fyysisesti suojattujen alueiden sisällä – Fyysinen turvallisuus

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Fyysiset turvatoimet toteutetaan kaikissa tiloissa, rakennuksissa, toimistoissa, huoneissa ja muissa paikoissa, joissa tietoja käsitellään tai säilytetään, tietojenkäsittely-ympäristöjen sijoitusalueet mukaan luettuina.

2) Tietojen käsittely on mahdollista turva-alueilla, hallinnollisella alueella tai viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella.

3) Tietojen säilytys on mahdollista turva-alueilla ja hallinnollisella alueella soveltuvissa lukittavissa toimistokalusteissa, tai tilapäisesti myös viranomaisen hyväksymillä menettelyillä hallinnollisen alueen ulkopuolella. (KATAKRI 2015, 61)

Toteutimme vaatimukset seuraavasti: Fyysiset turvatoimet toteutuvat paikoissa, joissa tietoja käsitellään. Käsittelyn tapahtuessa turvatilojen ulkopuolella, on käytössä viranomaisen hyväksymä menetelmä. Tietoja säilytetään ainoastaan turvatiloissa, jotka on hyväksytty tilaturvallisuutensa puolesta tasolle TL IV. TL IV käsittelyyn käytettävillä tiloilla on toimivaltaisen viranomaisen hyväksyntä TL IV-tasolle.

5.22 I-22 Salassa pidettävien tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä – Etäkäyttö ja etähallinta

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

1) Tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä on mahdollista vain viranomaisen ko. suojaustasolle hyväksymien korvaavien menettelyjen mukaisesti.

2) Henkilöstö on koulutettu ja ohjeistettu turvalliseen etäkäyttöön/-hallintaan.

3) Elleivät hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolelle viedyt suojaustason IV tietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattu viranomaisen ko. suojaustasolle hyväksymällä menetelmällä, tietovälineet säilytetään vastaavantasoisesti suojaten, kuin hallinnollisen turva-alueen lukittavissa toimistokalusteissa säilytettynä, tai tietovälineitä ei jätetä valvomatta.

4) Järjestelmien etäkäyttö/-hallintaratkaisu edellyttää viranomaisen ko. suojaustasolle hyväksymää liikenteen salausta. (KATAKRI 2015, 62)

Toteutimme vaatimukset seuraavasti: Tietojen välitys ja käsittely fyysisen suojatun alueen ulkopuolella tai välillä on ainoastaan mahdollista käyttäen VPN-kykeneväistä työasemaa. VPN toiminnallisuutta ei voi kiertää kyseisissä laitteissa, sillä VPN sovellus on aina päällä, kun työasema on päällä. Henkilöstölle pidetään koulutuksia säännöllisesti, joihin on pakko osallistua. Salassa pidettävien tietojen käsittely ei ole mahdollista ennen koulutusta.

Mahdolliset muut muistivälineet, jotka eivät täytä KATAKRIn vaatimuksia, säilytetään TL III -materiaalin käsittelyyn hyväksytyssä kassakaapissa. Järjestelmien hallintakäytävät käyttävät viranomaisen hyväksymää salausta liikenteessään.

5.23 I-23 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan – Ohjelmistohaavoittuvuuksien hallinta

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Tietojenkäsittely-ympäristön koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi (KATAKRI 2015, 64).

Toteutimme vaatimukset seuraavasti: Palvelimet skannataan säännöllisesti mahdollisia haavoittuvuuksia varten. Ylläpitäjät seuraavat aktiivisesti ja säännöllisesti tietoa ohjelmistojen haavoittuvuuksista. Päivityksiä työasemilla, palvelimille ja verkkolaitteille tehdään säännöllisesti ja tarpeen ilmetessä.

5.24 I-24 Tietojenkäsittely-ympäristön suojaus koko elinkaaren ajan - varmuuskopiointi

KATAKRI esittää vaatimuksena TL IV tasoisessa ympäristössä seuraavat kriteerit:

Salassa pidettävää tietoa sisältävät varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto (KATAKRI 2015, 65).

Toteutimme vaatimukset seuraavasti: TL IV tasoiset tiedot on varmuuskopioitu salattuina viranomaisen hyväksymillä menetelmillä. Tiedot on salattu koko elinkaarensa ajan.

6 Muutostenhallinta ympäristössä

Työasemien Windows –käyttöjärjestelmä päivitykset asennetaan Windows Update –palvelun kautta. Käyttäjät eivät voi muuttaa Windows Updaten asetuksia työasemilla, vaan päivitykset asennetaan pakotetusti. Työasemien päivityksien asentamista seurataan automatisoidusti. Palvelinten päivitykset asennetaan hallitusti manuaalisesti vähintään kuukausittain pois lukien kriittiset päivitykset, jotka asennetaan mahdollisimman pian. Palvelinten päivitys merkitään ylläpitolokiin.

Linux-päivitykset asennetaan luotetuista lähteistä. Päivityslähteet on dokumentoitu ja niiden lisääminen tarvitsee erikseen hyväksyä. Palvelinten päivitys tapahtuu manuaalisesti ylläpitäjien toimesta. Kriittiset tietoturvapäivitykset asennetaan aina mahdollisimman pian. Muiden järjestelmien päivitykset tehdään riskiarvion perusteella.

Haavoittuvuustiedotteiden osalta seurataan sekä sovellusvalmistajien tiedotteita että eri CERT-toimijoiden listoja. Ympäristön vastuullinen ylläpitäjä vastaa tiedotteiden seuraamisesta ja päivitystarpeen arvioinnista.

7 Järjestelmän auditointi ja hyväksyntä

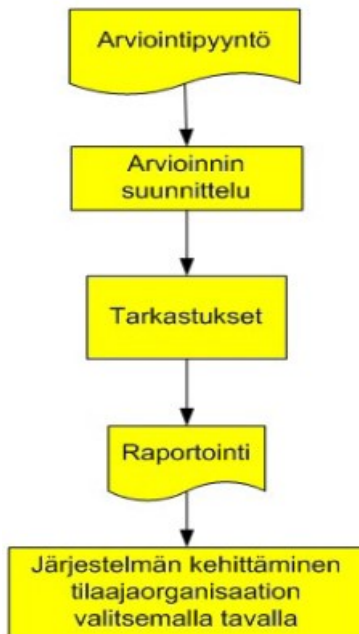
Järjestelmä on auditoitu toteutuksen jälkeen akkreditoidun arviointilaitoksen sekä Traficomien toimesta. Järjestelmän toteutus sekä dokumentaatio arvioitu auditointien yhteydessä.

Kyseessä on turvaluokiteltua tietoa käsittelevä järjestelmä, joten järjestelmän tarkempia kuvauksia ja dokumentaatiota käsitellään myös turvaluokitellun tiedon perustein. Auditoinneissa on kuitenkin varmistettu ulkopuolisten auditoijien toimesta, että ympäristön dokumentaatio täyttää sille asetut vaatimukset.

7.1 Arviointiprosessi

Tietojärjestelmien turvallisuutta koskeva arviointiprosessi alkaa, kun arvioitavan kohteen arviointipyyntö saapuu viranomaiselle. Keskeiset vaiheet arviointiprosessissa ovat seuraavat: arvioinnin suunnittelu, tarkastukset ja raportointi. Yksinkertaistettu arviointiprosessi on esitetty kuviossa 2

(ks. Kuvio 2). Arviointiprosessia voidaan käyttää esimerkiksi kohdeorganisaation sisäisen turvallisuustyön tukemiseen, jättäen jäljellä olevien riskien riskienhallinnan yksinomaan kohdeorganisaation vastuulle. (KATAKRI 2015, 70.)



Kuvio 2 Arviointiprosessi yksinkertaistettuna

8 Kehitysehdotuksia KATAKRIIN

Turvallisuuskriteerien tulisi kuvata vähimmäisvaatimukset, mutta myös tukea kohderyhmien turvallisuus- ja riskienhallintaprosesseja. Vaatimukset tulisi myös kuvata kohtuullisen konkreettisella tasolla. Ristiriitaiset suunnittelutavoitteet yleensä luovat kompromisseja kriteereiden kehitykseen. Mitä tarkemmalla abstraktiotason kuvaus on, sitä enemmän ammattilaisilta vaaditaan taitoja riittävän samanlaisten tulosten saavuttamiseksi. Yleensä matalan tason tekniset yksityiskohdat menettävät merkityksensä ajan myötä. Se voi myös johtaa haasteisiin muiden suunnittelutavoitteiden, kuten skaalautuvuuden ja sääntelyn toteuttamisessa. (Kelo, Eronen & Rousku 2018.)

Kriteeristö tarjoaa vain minimivaatimukset, mutta ei laajenna kriteeristöä tarpeeksi erilaisten ympäristöjen toteutustapoihin. Kriteeristö tarjoaa TL IV tasolle vain minimivaatimukset, mutta ei riskiperustaisesti täydentäviä hallintakeinoja, joilla tässä tapauksessa monihankeympäristössä pienennettiin ylläpitäjiin liittyviä riskejä. Joihinkin vaatimuksiin jouduttiin pyytämään ennakkoon

näkemyksiä, että onko joku tietty toteutustapa riittävä. Kriteeristön pitäisi olla niin selkeä tai tarjota laajempia esimerkkejä, jotta toteutusta voitaisiin tehdä itsenäisesti.

9 Pohdinta

Monihankeympäristön toteutus oli erittäin mielenkiintoista ja haastavaa. Erityisesti ongelmiksi muodostui ylläpitäjän pääsyn estäminen turvaluokiteltuun tietoon. Tämä piti toteuttaa käyttämällä tiedostosäiliöitä. Tiedostosäiliöiden käyttö loi omat haasteensa koulutuksen puolesta, piti varmistua, että tiedostosäiliöitä käytetään oikein. Ylläpitäjillä ei ole myöskään kykyä nollata konttien salasanoja, vaan tämä jää projektipäälliköiden tehtäväksi. Ylläpitäjän totaalinen estäminen valvontapalvelimelle loi myös omat haasteensa.

Selkeästi vaikeimpana asiana koin ympäristön joustamattomuuden, kaikki muutokset pitää olla harkittuja, hyväksyttyjä ja ainoastaan tarpeen. Tämä oli suuri muutos omalta kannaltani, kun ennen muutoksia pääsi tekemään omien mielipiteiden ja havaintojen perusteella. Ympäristön joustamattomuus koitui myös esteeksi muutoksien tapahtuessa. Nopeat tarvittavat muutokset ovat todella haastavia tehdä, kun tarvitsee hankkia hyväksynyt muutoksille ja kiire puskee päälle.

Vaikeaksi osoittautui myös uusien koneiden asentaminen ympäristöön. Tekemäni asennusohje on kyllä helppo ymmärtää, mutta pitkästyttävää tekemistä, tähän mennessä olen kaiken automatisoinut, minkä olen pystynyt, mutta ihan kaikkea ei pysty kuitenkaan automatisoimaan.

Windowsin suuremmat muutokset versiopäivityksien muodossa aiheuttivat myös päänsäryä. Siirryttäessä seuraavaan Windows 10 versioon siirryttäessä tarvitsee käydä uusiutuneet tietoturva-asetukset ja uusien Windows 10 palveluiden pakottaminen pois päältä, jos ne ovat ylimääräisiä. Joskus päivitykset rikkovat jo olemassa olevaa säännöstöä, joka aiheuttaa lisätyötä.

Itse työn tekemisessä aiheutti hankaluuksia KATAKRIN uusiutuminen kesken työn, työ on tehty käyttäen KATAKRI 2015, koska uutta versiota ei silloin ollut saatavilla, kun työn aloitin ja suurimman osan työstöstä tehnyt. KATAKRI 2015 ja 2020 välillä ei ole suurempia sisällöllisiä eroja. KATAKRI 2020 on huomattavasti tehokkaammin koostettu, joitain kriteerejä on sulautettu yhteen.

Kehitettäviä huomioita tekemisestäni on ehdottomasti varmenteet. Ennen tätä osaamiseni varmenteista oli minimaalinen, mutta tätä tehdessä oli pakko opetella syvemmin, miten varmenteita tehdään ja missä muodossa niitä pitää käyttää. Linux -palvelimien varmenteet osoittautuivat haastavimmiksi.

Ympäristö on siirtynyt ylläpitovaiheeseen, päivityksiä ja parannuksia tehdään melkein jatkuvasti. Seuraava askel itselleni on suorittaa testihyökkäys ympäristöön, käyttämättä tunnuksiani ja jättämättä merkkejä. Mahdollisia hyökkäystapoja olen jo kirjoitellut ylös riskiarviointiin. Toinen skenaario tunkeutumisesta olisi käyttää tunnuksiani, mutta yrittää tehdä jotain haitallista niin, ettei tekoja pystytä jäljittämään minuun. Näillä toimenpiteillä saadaan huomattavaa lisäarvoa ympäristön kokonaisturvallisuuteen.

Lähteet

Home Huld. Viitattu 9.11.2021. <https://huld.io/>

Active Directory Domain Services Overview. Viitattu 3.11.2021. <https://docs.microsoft.com/fi-fi/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>

Active Directory Certificate Services (AD CS) Introduction. Viitattu 3.11.2021. <https://social.technet.microsoft.com/wiki/contents/articles/1137.active-directory-certificate-services-ad-cs-introduction.aspx>

Confluence basics. Viitattu 3.11.2021. <https://www.atlassian.com/software/confluence/guides/get-started/confluence-overview>

What is Jira used for? Viitattu 3.11.2021 <https://www.atlassian.com/software/jira/guides/use-cases/what-is-jira-used-for#Jira-for-requirements-&-test-case-management>

KATAKRI 2015. KATAKRI 2015 Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 10.10.2019. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokal_u_viranomaisille.pdf

Kelo, Tomi, Juhani Eronen, and Kimmo Rousku. "Model for efficient development of security audit criteria." Proceedings of the 17th European Conference on Cyber Warfare and Security: ECCWS. 2018.