Outi Aalto

# Windows-toimialueen Domain Admins -oikeuksien kaventaminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

6.4.2017

Metropolia

| | |
|---|---|
| Tekijä<br>Otsikko<br><br>Sivumäärä<br>Aika | Outi Aalto<br>Windows-toimialueen Domain Admins -oikeuksien kaventaminen<br>37 sivua + 1 liite<br>6.4.2017 |
| Tutkinto | Insinööri (AMK) |
| Koulutusohjelma | Tietotekniikka |
| Suuntautumisvaihtoehto | Ohjelmistotekniikka |
| Ohjaajat | Tietoturvapäällikkö Tapio Heinäaro<br>Lehtori Kimmo Saurén |

Tässä energia-alan yritykselle tehdyssä insinöörityöprojektissa vähennettiin Domain Admins -ryhmän jäseniä. Kriittisen infrastruktuurin yrityksessä huoltovarmuus on aina motiivina tietoturvatyössä. Työ perustuu siis vahvasti ISO/IEC 27001 -standardiin, jonka vaatimuksista yksi on mahdollisimman pienet käyttöoikeudet.

Eräs tietoturvan perusasioista on niin sanottu CIA-malli, joka muodostuu kolmesta tekijästä: luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Tämä vaatii tuekseen muiden tietoturvakontrollien lisäksi käyttöoikeuksien hallintaa. Käyttöoikeuksien merkitys tietoturvalle tulee parhaiten esiin haittaohjelmien tavassa toimia kirjautuneen käyttäjän oikeuksilla.

Järjestelmä, jonka puitteissa projekti tehtiin, on Microsoft Windows Active Directory. Domain Admins -ryhmä on yksi sen tärkeimmistä käyttöoikeusryhmistä, mutta se on lukuisissa organisaatioissa aivan liian laajassa käytössä. Sen tarkoitus on antaa oikeuksia Windows-toimialueen ylläpitoon, mutta sitä usein käytetään yleisenä ylläpitoryhmänä.

Projektissa päädyttiin poistamaan kaikki ylläpitäjät Domain Admins -ryhmästä ja luomaan muutama erillistunnus toimialueen ylläpitäjille. Muille ylläpitäjille luotiin uusi käyttöoikeusryhmä, jolla korvattiin ne menetetyt oikeudet, jotka olivat työtehtävien kannalta tarpeellisia.

Projektin alussa tunnistettiin lähinnä käyttöoikeuksien vajauksiin liittyviä ongelmista, mutta todelliset ongelmat olivat ajankäytössä, tiedottamisessa ja tehtävien delegoinnissa. Näiden tunnistamattomien riskien toteutuminen vaikutti myös tunnistettujen riskien toteutumiseen.

Pääosa toteutuksen aikana esiin tulleista ongelmat saatiin korjattua ensimmäisen viikon aikana, eikä vakavia ongelmia jäänyt. Projektin tavoitteet saavutettiin ja käyttöoikeudet ovat nyt hyväksyttävällä tasolla. Kohteena olleiden ylläpitäjien työ ei lopulta kärsinyt niin paljon kuin oli pelätty.

| | |
|---|---|
| Avainsanat | tietoturva, käyttöoikeudet, Active Directory, Domain Admins |

| | |
|---|---|
| Author<br>Title<br><br>Number of Pages<br>Date | Outi Aalto<br>Reducing the Domain Admins privileges in a Windows domain<br><br>37 pages + 1 appendix<br>April 6th 2017 |
| Degree | Bachelor of Engineering |
| Degree Programme | Information Technology |
| Specialisation option | Software Engineering |
| Instructors | Tapio Heinäaro, Chief Information Security Officer<br>Kimmo Saurén, Senior Lecturer |

In this thesis project, done for an energy company, the number of the members of the Domain Admins group was reduced. In a critical infrastructure company, the security of the infrastructure is always an important motivation in the cyber security work. As such this project was heavily based on the ISO/IEC 27001 standard, which includes the principle of the least privilege.

One of the basics of cyber security is the CIA-model, which is comprised of confidentiality, integrity and availability. This needs the support of several security controls, among them user rights management. The importance of proper user rights is highlighted in the way malware functions within the limits of the signed in user.

The system within which the project was implemented is the Microsoft Windows Active Directory. The Domain Admins group is one of the most important of its user rights groups, but it is in far too general use in numerous organisations. The group is meant for granting rights for the management of the Windows domain, but often it is used as a general management group.

In the project all the administrators were removed from the Domain Admins group and a few dedicated user accounts were created for those who manage the domain. The other administrators were placed in a new rights group, which replaced those rights which were necessary for work.

At the beginning of the project, most of the risks recognised concerned the possible lack of rights in the affected user accounts, but the real risks were in time management, information flow and delegation of tasks. The realisation of the unrecognised risks affected the realisation of the recognised risks.

Most of the problems that appeared during the execution were solved within the first week, and no serious problems remained. The goals of the project were achieved, and the user rights are now on an acceptable level. The work of the affected administrators did not suffer as much as was feared.

| | |
|---|---|
| Keywords | cyber security, user privileges, Active Directory, Domain Admins |

## Sisällys

## Lyhenteet

| | |
|---|---|
| GWh | Gigawattitunti. Wattitunti on energian yksikkö, joka vastaa watin tehoa tunnin ajan. Kotitalouksien sähkönkäyttöä mitataan yleensä kilowattitunteina. |
| SCADA | Supervisory Control and Data Acquisition. Tuotannon ohjaamiseen tarkoitettu tietojärjestelmä, joka tuottaa erilaisiin päätöksiin vaadittavaa tietoa tuotannon yksityiskohdista. |
| LDAP | Lightweight Directory Access Protocol |
| DMZ | Demilitarized Zone. Aliverkko, joka eristää toisistaan kaksi verkkoaluetta, joista toista pidetään turvattomampana kuin toista. Sotilaskielen vastaavasta termistä poiketen kyseessä ei ole verkkoalue, jolla ei olisi suojaustoimenpiteitä vaan jossa sijaitsee esimerkiksi välipalvelimia ja muita toimintoja, jotka suojaavat turvallisempaa verkkoa. |
| TCP/IP | Transmission Control Protocol / Internet Protocol. Protokollaryhmä, jota käytetään Internetin ja useimpien lähiverkkojen liikennöinnissä. |
| DNS | Domain Names System. TCP/IP-verkon nimipalvelu, joka kääntää verkkotunnukset IP-osoitteiksi. |
| DHCP | Dynamic Host Configuration Protocol. Protokolla, joka jakaa vaihtuvia IP-osoitteita TCP/IP-verkon laitteille. |
| CIA-malli | Tietoturvan perusmalli. Tulee sanoista Confidentiality, Integrity ja Accessibility. |

ISO/IEC 27001 ISO-järjestelmän tietoturvallisuuden hallinnan standardi.

# 1 Johdanto

Tämän insinöörityöprojektin tarkoitus oli muuttaa erään energia-alan yrityksen Microsoft Windows -ympäristön käyttöoikeuksia. Niiden merkitys tietoturvalle huoltovarmuuskriittisessä yrityksessä on suuri, joten hallintaa muutettiin vastaamaan paremmin ISO/IEC 27001 -standardin vaatimuksia.

Työssä perehdytään käyttöoikeuksiin ja niiden merkitykseen tietoturvan kannalta. Käyttöoikeuksien minimointi on yksi tärkeimmistä tavoista rajoittaa tietoturvauhkien vakavuutta, mutta käytännön syistä se on myös yksi laiminlyödyimmistä. Käyttäjän oikeuksien kasvattaminen on helppo tapa ratkaista erinäisiä tietoteknisiä ongelmia, ja oikeuksia harvoin vähennetään ilman painavaa syytä, koska vähentäminen aiheuttaa aina ongelmia.

Vaikka niin Microsoftin kuin tietoturvankin parhaat käytännöt vaativat käyttäjille, myös ylläpitäjille, mahdollisimman suppeita oikeuksia, monissa organisaatiossa ongelmia on vuosien myötä ratkottu lisäämällä kaikki tai lähes kaikki ylläpitäjät Domain Admins -ryhmän jäseniksi. Näin ylläpitäjillä on varmasti myös hätätilanteissa kaikki ongelmien ratkaisuun vaadittavat oikeudet. Tämä kuitenkin tarkoittaa yleensä, että ylläpitäjillä on arjen työtehtäviinsä nähden aivan liian laajat oikeudet, mikä on merkittävä tietoturvauhka.

Tämän työn viidennessä luvussa käsitellään juuri näitä ongelmia, joihin insinöörityöprojektin puitteissa törmättiin, sekä sitä, mitä niistä on itse projektin ja työn kirjoittamisen yhteydessä opittu. Yritän myös perehtyä syihin, jotka näihin ongelmiin johtivat. Useimmat esiin tulleista ongelmista olisivat todellisuudessa olleet vältettävissä. Luvussa tulevat myös näkyviin tietoturvan kivijalkana pidetyn niin sanotun CIA-kolmion sekä Microsoftin Active Directoryn perusteiden käytännön merkitys.

Microsoftin Active Directory -ympäristö on yksi yritysmaailman käytetyimmistä tavoista tietoteknisen ympäristön keskitettyyn hallintaan, ja sellaisessa ympäristössä tämän työn projektikin tehtiin. Luvussa 4 keskitytään järjestelmän tekniikkaan niiltä osin, kuin se liittyy käyttöoikeuksiin ja projektiin.

Tällaisen ympäristön perusyksikössä, toimialueessa, myös käyttöoikeuksien hallinta on keskitettyä. Yksi eniten oikeuksia omaavista ryhmistä Windows-toimialueella on Domain

Admins -ryhmä, jolla on laajoja oikeuksia paitsi toimialueen jäsenpalvelimiin, myös toimialueen ytimen muodostaviin Domain Controller -palvelimiin. Työssä kuvataan myös itse Active Directoryä.

Aivan ensimmäiseksi kuitenkin avaan huoltovarmuutta, jonka merkitys niin energia-alalla kuin muillakin kriittisen infrastruktuurin aloilla on kasvanut kuluneen vuosikymmenen aikana paljon. Vaikka huoltovarmuuskysymykset ovat varsin merkittäviä nykyaikaisen arjen sujumisen kannalta, käsitteet ja ideat eivät useinkaan ole tuttuja huoltovarmuudesta huolehtivien organisaatioiden ulkopuolella.

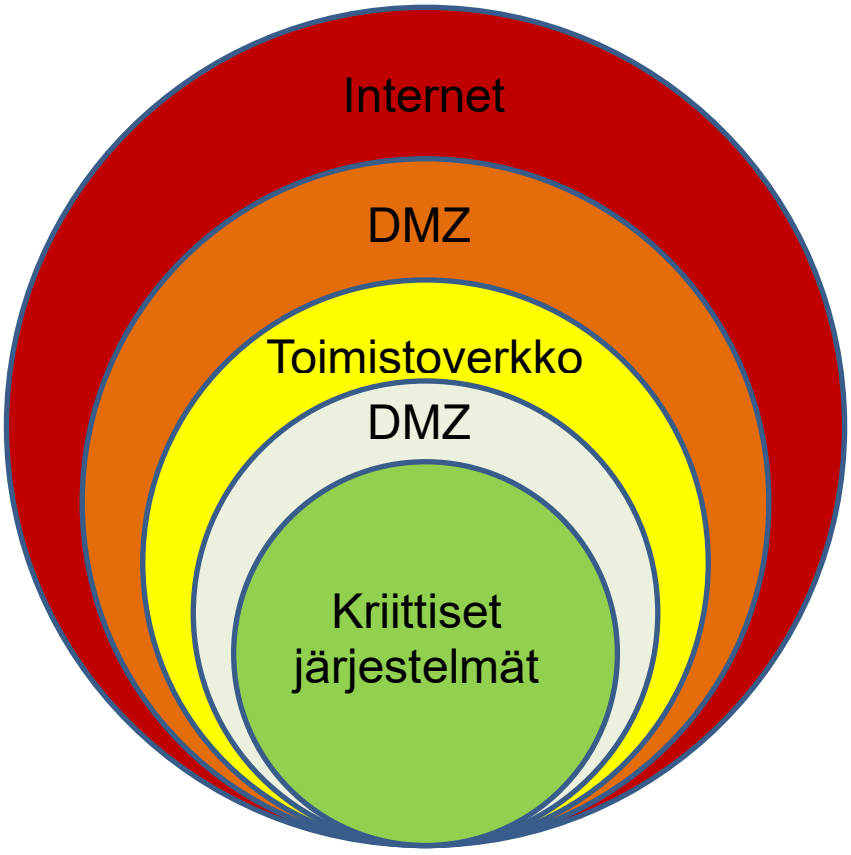
# 2 Huoltovarmuus

## 2.1 Kriittisen infrastruktuurin huoltovarmuus

Kriittisen infrastruktuurin toimijoissa tietoturvalla on erilaisia ulottuvuuksia kuin muissa yrityksissä. Kuitenkin tietoverkot ovat oleellinen osa kriittistenkin järjestelmien suojaamista.

Yrityksen huoltovarmuuskriittisten osien suojelemiseksi saattaa olla perusteltua suhtautua tiukemmin myös tavallisen toimistoympäristön tietoturvaan niin sanotun sipulipuolustuksen nimissä. Sipulipuolustuksella tarkoitetaan sitä, että päästäkseen käsiksi kriittisiin järjestelmiin organisaation ulkopuolelta, täytyy kulkea useiden palomuurilla erotettujen verkkokerrosten läpi.

Kuvassa 1 esitetään malli, jossa kriittiset järjestelmät sijoitetaan sipulin ”ytimeen”. Järjestelmiä voidaan myös erottaa vielä toisistaan, niin että ”ytimiä” muodostuu useampia.




Kuva 1. Sipulipuolustuksen perusmalli

Kriittistä infrastruktuuria ylläpitävän yrityksen järjestelmien uumenissa, ”sipulin ytimessä”, olevat kriittisimmät järjestelmät ovat sitä paremmassa turvassa, mitä vaikeampi ”sipulin” edellisistä kerroksista on päästä läpi. Tässä merkityksellistä on paitsi kerrosten välissä olevat verkkolaitteet, esimerkiksi palomuurit, myös kerrosten sisäinen turvallisuus, kuten käyttöoikeudet, joiden merkitykseen perehdytään enemmän luvussa 3.

Tämä luku siis avaa huoltovarmuuden kautta tietoturvatoiminnan motiiveja. Suomen valtiollinen Huoltovarmuuskeskus määrittelee huoltovarmuuden [Mitä on huoltovarmuus? 2017: 1] kyvyksi ”sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa”.

Valtioneuvoston 5.12.2013 antama päätös [Tavoitteet 2017: 2] puolestaan tarkentaa huoltovarmuuskriittisen infrastruktuurin käsittävän

- energian tuotanto, siirto- ja jakeluverkot
- tieto- ja viestintäjärjestelmät, -verkot ja -palvelut
- finanssialan palvelut
- liikenne ja logistiikka
- vesihuolto
- infrastruktuurin rakentaminen ja kunnossapito
- jätehuolto erityistilanteissa.

Näistä energiahuolto on avainasemassa myös suhteessa muuhun kriittiseen infrastruktuuriin, koska monien näiden palveluiden toimittaminen muuttuisi paljon vaikeammaksi, ellei jopa mahdottomaksi, ilman sähköä. Esimerkiksi vesihuolto on monilla paikkakunnilla täysin sähkötoimisten pumppujen varassa, eikä nykyaikaista kauppaa voi pitää auki ilman sähköä. Kriittisiä kohteita turvataan usein varavoimalaitteilla, mutta monet nykyaikaiselle elämälle tärkeät toiminnot, kuten pääkaupunkiseudun raideliikenne, vaativat niin paljon sähköä, ettei rinnakkaista infrastruktuuria ole taloudellisesti mahdollista toteuttaa. Optimaalinen tilanne yhteiskunnan normaalin toiminnan kannalta on siis se, että energiahuolto toimii normaalisti. [Laitinen & Vainio 2009: 3.]

Suomessa huoltovarmuutta hallinnoi ja ohjaa työ- ja elinkeinoministeriön alainen Huoltovarmuuskeskus. Koska iso osa kriittisestä infrastruktuurista on nykyään yritysten käsissä, esimerkiksi energiayhtiöillä ja teleoperaattoreilla, yksi tärkeistä toiminnoista on yhteistyö elinkeinoelämän kanssa. [Huoltovarmuus 2017: 4.]

Perinteisten uhkien, kuten laajavaikutteisten luonnonnettomuuksien ja aseellisten konfliktien, rinnalle ovat tällä vuosisadalla nousseet kybermaailman uhat. Tietojärjestelmät ovat oleellinen osa myös huoltovarmuuskriittisten yritysten toimintaa, ja niihin kohdistuu vakavia uhkia niin rikollisten kuin kansallisvaltioidenkin taholta. [Uhkakuvat 2017: 4.]

Kyberuhkien edessä toinen huoltovarmuuskriittisten yhtiöiden tärkeä yhteistyökumppani on Viestintäviraston Kyberturvallisuuskeskus. Palveluita on tarjolla kaikille suomalaisille toimijoille, mutta erityisesti huoltovarmuuskriittisille toimijoille Kyberturvallisuuskeskus tarjoaa tilannekuvatietoa ja tietojenvaihtokanavan. Kyberturvallisuuskeskuksen tarjoamat palvelut ja osaaminen ovat merkittävä apu suomalaisille organisaatioille. [Huoltovarmuuskriittisille toimijoille 2014: 5.]

## 2.2 Energiantuotannon huoltovarmuus

Hajautettu energiantuotanto on kovassa nosteessa, mutta tällä hetkellä, ja vielä jonkin aikaa tulevaisuuteenkin, pääosa suomalaisten käyttämästä energiasta tuotetaan isoissa voimalaitoksissa. Keskitetyn energiantuotannon aikakaudella energiantuotannon fyysisen turvallisuuden uhat rajoittuvat lähinnä täysimittaiseen sotaan tai massiiviseen terroristi-iskuun. Polttoaineen saatavuutta taas voi uhata energiayhtiön taloudellinen tilanne tai kansainvälisen kaupan häiriöt, joiden pitäisi kyllä olla varsin merkittäviä, jotta polttoaineiden saatavuus vaarantuisi kriittisesti.

Polttoaineen riittävyys poikkeustilanteessa on varmistettu sekä vaatimalla energiayhtiöitä pitämään polttoaineiden varmuusvarantoja että valtion itse pitämillä varastoilla. Esimerkiksi kivihiilen ollessa kyseessä laitosten tulee varastoida vähintään kolmen kuukauden tarvetta vastaava määrä hiiltä. [Erityislainsäädäntö 2017: 10.]

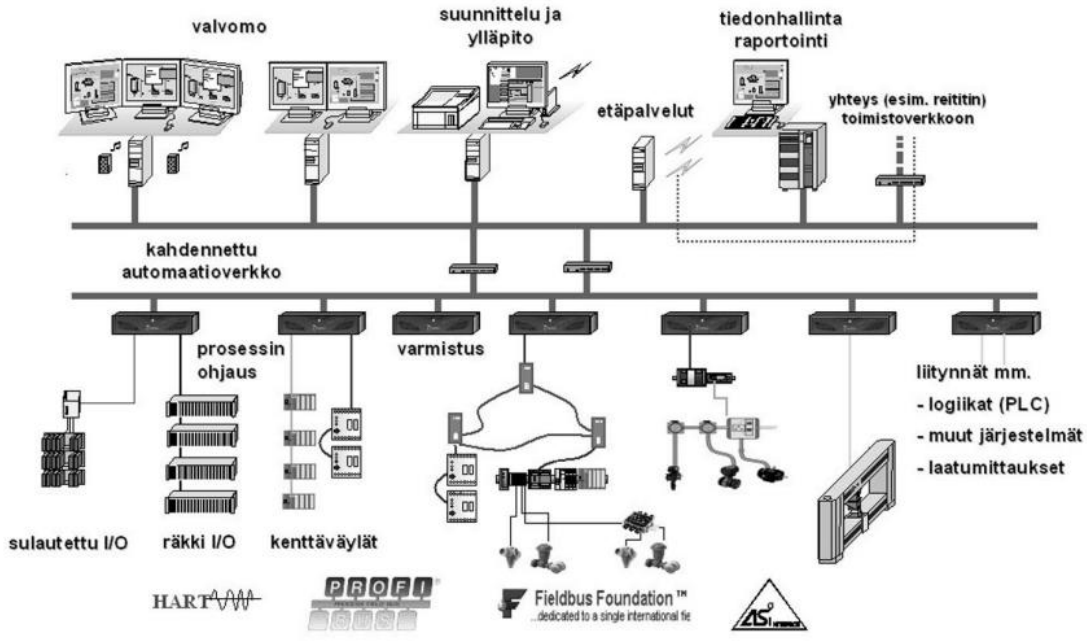
Näin ollen tavallisessa turvallisuustilanteessa energiantuotannon huoltovarmuuden ehkä suurimmaksi uhaksi onkin katsottava kyberuhat. Tähän päätelmään ohjaa myös energiantuotannon koko ajan kasvava riippuvuus tietojärjestelmistä.

Nykyaikaisessa energiantuotannossa itse voimalaitoksia ohjataan tietojärjestelmillä, ja energiantuotannon päätöksiä tehdään erilaisten, esimerkiksi SCADA-tyyppisten, järjestelmien avulla. Tuotantoon liittyy helposti jopa kymmenenkunta erilaisiin tehtäviin tarkoitettua järjestelmää (kuva 2). [Ala-Tala ym. 2010: 6.]

Tietoturvan kannalta merkittävät ohjausjärjestelmät voidaan jakaa kolmeen luokkaan:

- hajautetut automaatiojärjestelmät
- SCADA-käytönvalvontajärjestelmät
- ohjelmoitavat logiikkajärjestelmät [Ala-Tala ym. 2010: 6].

Yleensä näitä kaikkia tarvitaan nykyaikaisessa energiantuotannossa. Vaaditaan paljon informaatiota ja hienosäätöä, kun suuressa laitoksessa tuotetaan energiaa ympäristömääräysten, fysikaalisten prosessien ja taloudellisten vaatimusten ristipaineessa.




Kuva 2. Nykyaikainen automaatiojärjestelmä [Ala-Tala ym. 2010: 6].

Voimalaitokset ovat usein hyvin suojattuja, eikä tiedossa olekaan tuhoisia kyberhyökkäyksiä niitä kohtaan. Laitoksissa on paljon turvajärjestelmiä, joiden tarkoitus on estää niitä toimimasta väärin mistään syystä, joten onnistuneenkaan hyökkäyksen ei pitäisi saada aikaiseksi esimerkiksi ydinonnettomuutta. Yhteiskunnan toiminnan häiritsemiseen ja yrityksen talouden vahingoittamiseen riittäisi se, että voimalaitos saataisiin ajamaan itsensä alas. Liitteessä 1 on esimerkkejä voimalaitoksiin kohdistuneista kyberhyökkäyksistä.

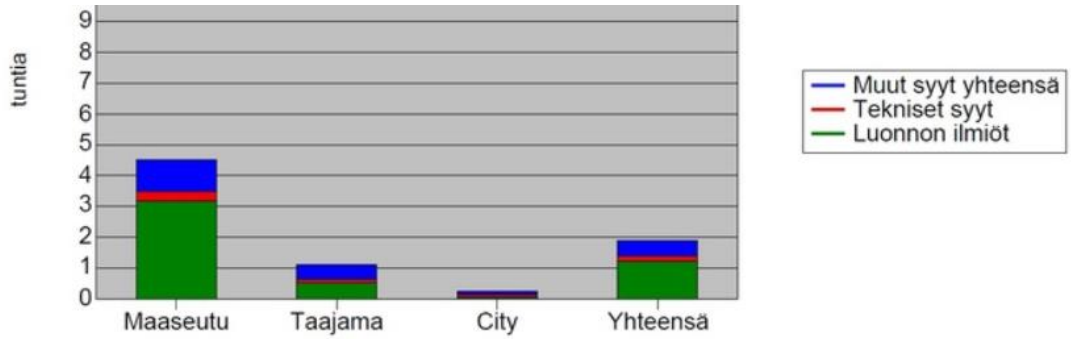
Voimalaitosten ja muun energiantuotannon sijaan energia-alaa kohdanneet kyberhyökkäykset ovatkin kohdistuneet viime vuosina sähkön jakeluun. Vahinkoja ovat kärsineet myös energiahuollon kuluttajapalvelut, kuten kiinteistöautomaatio [Virtanen 2016: 7], mutta ne eivät yleensä ole olleet juuri kyseisiin palveluihin kohdistuneita hyökkäyksiä.

Tulevaisuudessa sähköntuotannon odotetaan olevan nykyistä hajautetumpaa, mikä suojelee sitä fyysisiltä uhilta, mutta ei kyberuhilta. Pientuottajien, kuten kotitalouksien, tietojärjestelmät saattavat olla jopa suuremmassa vaarassa kuin ammattimaisesti suojattujen energiayhtiöiden. [Scott 2016: 18; The Potential Benefits of Distributed Generation and the Rate-Related Issues That May Impede Its Expansion 2007: 19.]

## 2.3 Sähkönjakelun huoltovarmuus

Tuotettu sähkö täytyy vielä toimittaa käyttäjille. Luvussa 2.2 esiteltyjen energiantuotannon uhkien lisäksi energiahuollon kokonaisuudessa täytyy siis ottaa huomioon myös energian, yleensä sähkön, jakeluun liittyvät uhat.

Kuten uutisia lukiessakin näkee, Suomen sähköverkkojen suurin uhka ovat sääilmiöt (kuva 3). Vielä vuonna 2014 Suomen sähköverkoista 71 % oli ilmajohtoja, joiden takia erityisesti paikalliset jakeluverkot ovat alttiita säiden aiheuttamille puiden ja verkkotolppien kaatumisille. Isojen myrskyjen yhteydessä Suomessa saattaa olla satoja tuhansia kotitalouksia ilman sähköä. Tätä huoltovarmuuden kipukohtaa aiotaan parantaa lisäämällä sähköverkkojen maakaapelointia. Kalleudesta huolimatta vuoden 2019 lopussa odotetaan jakeluverkkojen maakaapelointiasteen olevan jo 44 %. [Yleistietoa häiriöistä 2016: 12; Sähköverkkojen rakenne 2017: 11.]



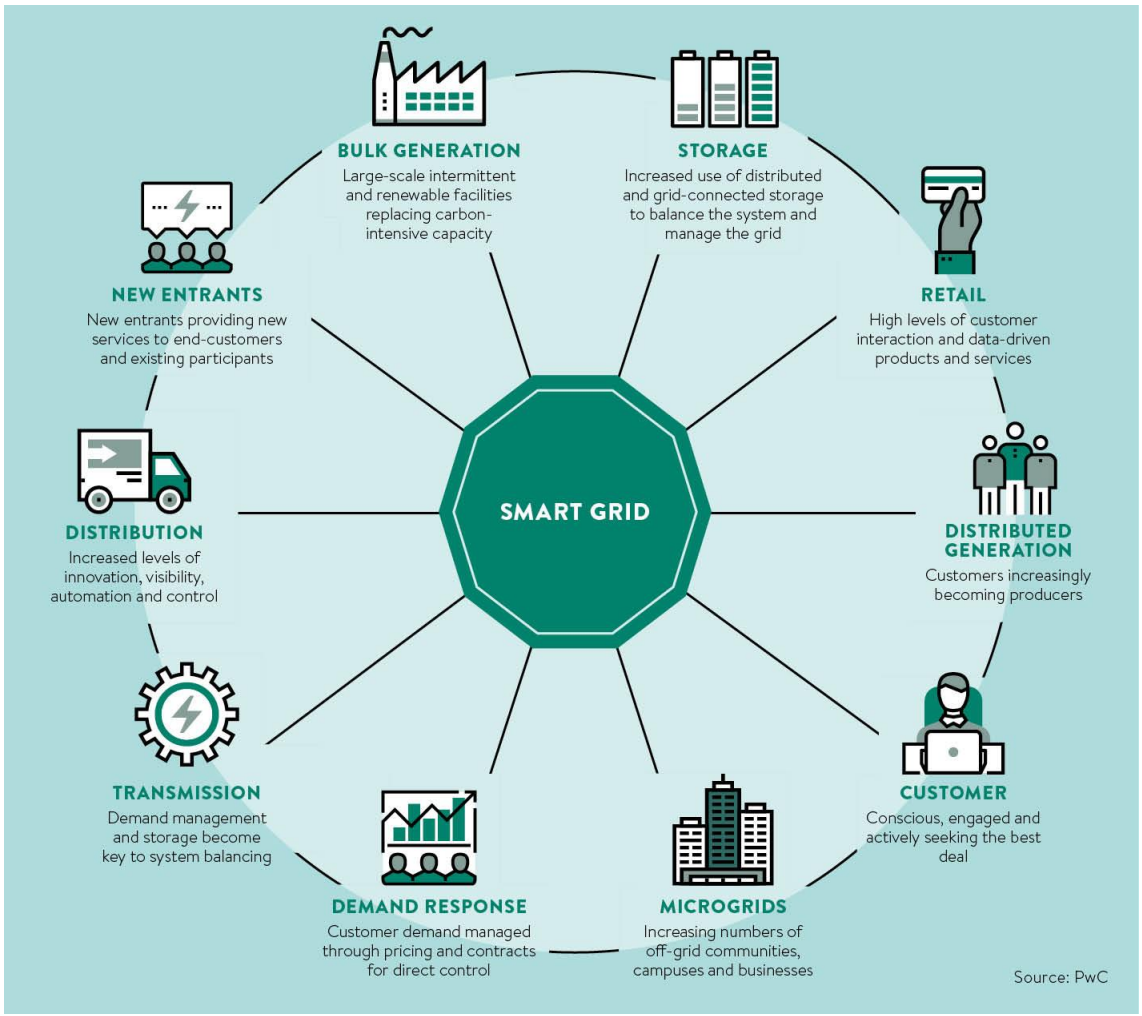

Kuva 3. Sähkönjakelun keskeytysajat tunteina vuodesta 2014 [Yleistietoa häiriöistä 2016: 12].

Suurissa taajamissa maakaapelointiaste on erittäin korkea, ja luonnonilmiöiden aiheuttamia katkoksia ei juuri esiinny. Esimerkiksi Helsingissä on 6 200 km sähköverkkoa, josta 6 000 km (97 %) kulkee maan alla. Tämä johtaa erittäin korkeaan luotettavuuteen. Kun vuonna 2015 suomalainen sähköasiakas kärsi keskimääri 1,4 tuntia sähköttömyyttä ja keskimääräinen kaupunkikäyttäjäkin 17 minuuttia, helsinkiläiseltä sähköt olivat poikki keskimäärin vain neljä minuuttia. [Sähkön luotettavuus Helsingissä maailman huippuluokkaa 2016: 13.] Tässä valossa onkin selvää, että Helsingin kaltaisissa taajamissa luonnonvoimia suurempi uhka sähkönjakelulle ovat tekniset viat muuntamoissa ja vastaavissa solmukohdissa sekä yhä lisääntyvässä määrin sähkönjakelua ohjaaviin järjestelmiin kohdistuvat kyberuhat.

Kyberuhista on saatu pelottava, mutta vaikuttava esimerkki nimettömänä pysyneen tahon hyökkäyksissä Ukrainan sähkönjakelua vastaan vuosina 2015 ja 2016. Joulukuussa 2015 hyökkääjät pääsivät ukrainalaisen Prykarpattyaoblenergo-energiayhtiön järjestelmiin ja katkaisivat sähköt 80 000 asiakkaalta, jolloin jopa 225 000 ihmistä jäi ilman sähköä. Samaan aikaan hyökkääjät kuormittivat Prykarpattyaoblenergon asiakaspalvelua soittamalla turhia puheluja, mikä vaikeutti vianselvitystä. Lähes sama tapahtui uudestaan joulukuussa 2016, kun Ukrainan pääkaupungin Kiovan sähköistä katkaistiin viidennes. [Hackers behind Ukraine power cuts, says US report 2016: 15; Ukraine power cut 'was cyber-attack' 2017: 16.]

Smart Grid eli älykäs sähköverkko on tuonut paljon uusia haasteita sähköverkkojen tietoturvaan. Älykkäät sähkömittarit ovat keventäneet luennan ja asiakashallinnan toteutusta ja mahdollistaneet sähkön käyttäjille lähes reaaliaikaisen näkymän kulutukseensa. Tulevaisuudessa perinteinen, suoraviivainen tuottaja-kuluttajamallinen muuttuu vielä li-

sää (kuva 4), kun mukaan tulee sähkön pientuottajia ja pienvarastoja. Älykäs sähköverkko myös mahdollistaa dynaamisen kulutuksen eli kodin eri toimintojen automaattisen käynnistymisen ja sammumisen esimerkiksi sähkön hinnan tai kulutushuippujen mukaan. [Etäluenta 2017: 17; Scott 2016: 18.]




Kuva 4. Älykkään sähköverkon tulevaisuus [Scott 2016: 18].

Älykäs sähköverkko tuo kuitenkin paljon myös hajautettuja tietojärjestelmiä, jotka sijaitsevat ylläpitäjän näkökulmasta turvattomissa paikoissa, kuten yksityisasunnoissa. Näistä ensimmäinen esimerkki ovat älykkäät sähkömittarit. Jokaisessa suomalaisessa taloudessa on nykyään älykäs, etäluettava ja -hallittava sähkömittari, joka on yhteydessä jonkin luentayhtiön järjestelmiin. Tämä on piste, josta hyökkäys voisi hyvinkin saada alkunsa tulematta lainkaan läpi yleensä vahvasti suojatusta Internet-rajapinnasta.

Tässä luvussa on perehdytty lähinnä niin sanottuun isoon kuvaan. Huoltovarmuus on monissa organisaatioissa aina taustalla, kun tietoturvatyötä tehdään. Seuraavassa luvussa kokoluokka muuttuu paljon pienemmäksi, kun perehdytään käyttöoikeuksien merkitykseen tietoturvalle, unohtamatta sitä, että jokaiselle ”tietoturvasipulin” kerrokselle sen sisältämien järjestelmien käyttöoikeudet ovat merkittävä tietoturvatekijä.

# 3 Käyttöoikeuksien tietoturva

Luvun 2 ”tietoturvasipulin” (katso sivu 3) jokaisen kerroksen tietoturva on tärkeää, ja käyttöoikeudet ovat tärkeä osa tietoturvaa ISO/IEC 27001 -standardinkin mukaan. Koko projektin motivaatio pohjautuu näihin tosiasioihin. Tässä luvussa käyttöoikeuksien tietoturvaan perehdytään kahden tietoturvan tärkeän ohjenuoran, ns. CIA-kolmiomallin ja minimaalisten oikeuksien periaatteen (the least-privilege principle), kautta. Erityisesti minimaalisten oikeuksien periaate tulee näkyviin, kun puhutaan haittaohjelmista. Tästä nähdään esimerkkejä myöhemmin luvussa.

Käyttöoikeudet (Access Controls) kontrolloivat käyttäjän pääsyä erilaisiin tietoteknisiin resursseihin. Oikeuksien hallintaan on järjestelmästä riippuen lukuisia menetelmiä, jotka lähestyvät asiaa erilaisista näkökulmista. Ero voi olla esimerkiksi suhteessa siihen, onko pääsy oletusarvoisesti estetty ja käyttäjille erikseen myönnetään oikeuksia vai onko pääsy oletusarvoisesti sallittu ja pääsy kielletään, jos siihen on erityinen syy. [Harris 2013: 26.]

## 3.1 CIA-kolmio ja sen suhde käyttöoikeuksiin

Minkä tahansa kohteen, digitaalisen tai fyysisen, tietoturvan voidaan katsoa perustuvan kolmeen asiaan, joista muodostuu tietoturvan niin sanottu CIA-kolmiomalli (kuva 5). Nämä asiat ovat saatavuus (Availability), eheys (Integrity) ja luottamuksellisuus (Confidentiality). Jos jokin näistä kolmesta puuttuu, tietoturva ei aja asiaansa. [Harris 2013: 26.]


Kuva 5. Tietoturvan CIA-kolmiomalli [CIA Triad: Confidentiality, Integrity, and Availability 2017: 27].

Käyttöoikeuksien onnistunut kontrollointi vastaa kaikkiin CIA-kolmion alueisiin. Käyttäjän luotettava tunnistaminen (identifiointi ja autentikointi) on oleellinen osa jokaisen alueen varmistamista. [Harris 2013: 26.]

Saatavuus

Mikään tietojärjestelmä ei ole olemassa tyhjiössä, joten jotta järjestelmästä on hyötyä, sen tietoihin täytyy päästä käsiksi. Tämän varmistamiseksi tietoa tarvitsevien käyttäjien, tai ehkä toisen järjestelmän, käyttäjätunnuksella täytyy olla oikeuksia tietoon. Käyttäjätunnuksella voi siis myös olla liian vähän oikeuksia, mikä on ongelma siinä, missä liialliset kin oikeudet. [Harris 2013: 26.]

Samaa pätee muihin tietoteknisiin järjestelmiin. Tulostimen tai muun resurssin muodostamille kustannuksille ei ole oikeutusta, jos yksikään käyttäjä ei pääse käyttämään sitä. Tämä on kuitenkin se osa CIA-kolmiosta, joka helposti uhrataan kahden muun kustannuksella, ja resurssin käytöstä tehdään, jos ei mahdotonta, usein vaikeaa.

Eheys

Tiedon eheys tarkoittaa sitä, että se pysyy koko ajan samana, ellei sitä tietoisesti ja perustellusta syystä muuteta. Esimerkiksi energia-alan toimijalle on tärkeää, että asiakkaan mittaustieto, tai tieto sähköverkon tilasta, on autenttista. [Harris 2013: 26.]

Muutokset tietoon saattavat tapahtua myös vahingossa, vaikkapa ylläpitotoimien yhteydessä, kun ylläpitäjä joutuu operoimaan järjestelmän käyttöliittymässä. Olisikin erityisen tärkeää, ettei tietoa pysty muuttamaan ilman määrättyjä käyttöoikeuksia tai ainakin, että tiedon muuttuminen pystytään havaitsemaan ja väärä tieto hylkäämään. Tiedon muuttumisen havaitsemiseen onkin kehitetty paljon tapoja. Parasta kuitenkin olisi, että tieto pystyttäisiin pitämään muuttumattomana.

Luottamuksellisuus

Usein, kun ajatellaan tietoturvaa, ajatellaan luottamuksellisuutta. Tiedon salaus, tietovuodot ja viestinnän salaisuus ovat uutisten ja jopa elokuvien vakiomateriaalia. Tietoyhteiskunnassa jokaisesta kansalaisesta on monissa järjestelmissä tietoa, ja luottamuksellisuus konkretisoituu jokaisen kohdalla, kun ajattelee esimerkiksi omia terveystietojaan.

Luottamuksellisuuden merkitys on erityisen suuri tietojärjestelmissä, jotka käsittelevät henkilötietoja. Henkilötietojen luottamuksellisuus on noussut tietoyhteiskunnassa niin suureen arvoon, että sille on muodostunut oma termi, tietosuoja. Euroopan Unionin viranomaiset ovat omilla toimillaan korostaneen tietosuojan tärkeyttä uudella tietosuoja-asetuksella, joka tuli voimaan 24.5.2016 [EU:n tietosuojauudistus 2017: 28].

Kaikessa tiedon luottamuksellisuudessa korostuu siis se, kenellä on oikeus nähdä tietoa suhteessa siihen, kenellä on pääsy tietoon. Huolimattomalla käyttöoikeuksien hallinnalla saattaa hyvinkin käydä niin, että ylläpitäjillä on pääsy tietoon, jota heidän ei kuuluisi nähdä. Yleensä esimerkiksi palvelimen ylläpitäjällä ei ole tarvetta nähdä palvelimella olevan tietokannan tai muiden järjestelmien sisältöä.

On tilanteita, joissa saatavuus tai eheys ovat tärkeämpiä kuin luottamuksellisuus. Esimerkiksi tiedon salauksen algoritmeissa pidetään parempana, että algoritmi on julkinen kuin että se olisi salainen (Kerchoffin periaate). Kun algoritmi itsessään on julkinen, kuka tahansa voi tutkia sitä ja löytää sen heikkoudet, jotka voidaan sitten korjata, kun taas

salaisen algoritmin heikkouksista käyttäjillä ei ole mahdollisuutta saada tietoa. [Harris 2013: 26.]

## 3.2 Liialliset käyttöoikeudet ja haittaohjelmat

Yksi merkittävimmistä ongelmista liiallisten käyttöoikeuksien kanssa tulee esiin silloin, kun törmätään haittaohjelmaan. Parhaimmillaan tarpeeksi pienet käyttöoikeudet estävät haittaohjelman asentumisen, jolloin koko ongelmalliselta tilanteelta on vältytty. [Guerrero 2010: 29.]

Koska on erittäin harvinaista, että haittaohjelma pystyisi kasvattamaan oikeuksiaan, ne yleensä joutuvat operoimaan saastuneeseen koneeseen parhaillaan kirjautuneen käyttäjän oikeuksilla. Tällöin liialliset käyttöoikeudet voivat aiheuttaa ikäviäkin ongelmia, joilta olisi muuten vältytty.

### Koneen haltuunotto

Jos käyttäjillä on oikeuksia käyttöjärjestelmän kriittisiin osiin, kuten rekisteriin tai järjestelmätiedostoihin, haittaohjelma voi saada koko koneen haltuunsa.

### Leviäminen

Peruskäyttäjillä ei yleensä ole oikeutta ottaa etäyhteyttä muihin koneisiin tai tallentaa tietoa niihin; jos käyttäjällä kuitenkin on nämä oikeudet tai kirjautuneena on ylläpitäjä, haittaohjelman voi olla luvattoman helppoa levitä toisiin verkossa oleviin tietokoneisiin, jopa palvelimiin.

### Kiristyshaittaohjelmat

Viime vuosina yleistyneet kiristyshaittaohjelmat toimivat salaamalla tiedostoja ja vaatimalla rahaa niiden avaamiseen vaadittavasta salausavaimesta. Tällainen ohjelma voi kuitenkin salata vain ne tiedostot, joihin käyttäjällä on oikeus. Koska ohjelmat osaavat salata myös verkkoresursseissa, esimerkiksi pilvipalveluissa, sijaitsevia tiedostoja, liian laajat käyttöoikeudet voivat johtaa katastrofiin.

Vuonna 2010 arvioitiin, että 90 % Windows-käyttöjärjestelmiin kohdistuvista tietoturvauhista voitaisiin torjua tai niiden haittoja vähentää, jos käyttäjillä olisi rajatumman oikeudet. [Guerrero 2010: 29.]

## 3.3 Minimaalisten oikeuksien periaate

Kaiken edellä kuvatun takia tietoturvan kultaiseksi säännöksi on muodostunut minimaalisten oikeuksien periaate, englanniksi the least-privilege principle. Sen mukaan jokaisella käyttäjällä tulisi olla pienimmät mahdolliset oikeudet, joilla kyseisen käyttäjän työtehtävät on mahdollista suorittaa. [Harris 2013: 26; ISO/IEC 27001 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät 2010: 8.]

Alan standardien mukaan käyttöoikeuksia tulisi käydä säännöllisesti läpi, että minimaalisten oikeuksien periaate toteutuisi. Tällä ehkäistään esimerkiksi se, että usein työtehtävien muuttuessa tunnuksille jää turhia oikeuksia ja ajan myötä niitä voi kertyä paljonkin. [ISO/IEC 27001 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät 2010: 8.]

Tässä tullaan siihen, mihin tällä insinöörityöprojektilla pyrittiin. Kun tietoturvan kivijalkana on, että jokaisella käyttäjällä on mahdollisimman vähän oikeuksia, on seuraavassa kappaleessa kuvatun ja työn ytimessä olevan Domain Admins -ryhmän jäsenyys oletuksena varattava mahdollisimman harvoille. Koska useimmissa yrityksissä ei näin ole päädyttiin tähän projektiin. Ennen projektin käsittelyä perehdytään kuitenkin Microsoftin Windows Active Directory -teknologiaan, jonka puitteissa projektin kohteena olevia oikeuksia hallitaan.

# 4 Microsoft Windows Active Directory -järjestelmä

Luvussa 3 mainittu ISO/IEC 27001 -standardi vaatii käyttöoikeuksien keskitettyä hallintaa. Näitä keskitetyn hallinnan järjestelmiä on monia; tässä työssä käsitellään Microsoft Windows Active Directory -järjestelmää.

Microsoft Windows Active Directory on yrityksissä yleisesti käytetty hakemistopalvelu, jonka avulla voidaan pitää kirjaa ja hallinnoida keskitetysti lähiverkon käyttäjiä, tietokoneita ja muita resursseja. Active Directoryn perusteiden ymmärtäminen on oleellista, jotta voisi ymmärtää, mitä ja miksi tämän työn käsittelemässä projektissa on tehtiin.

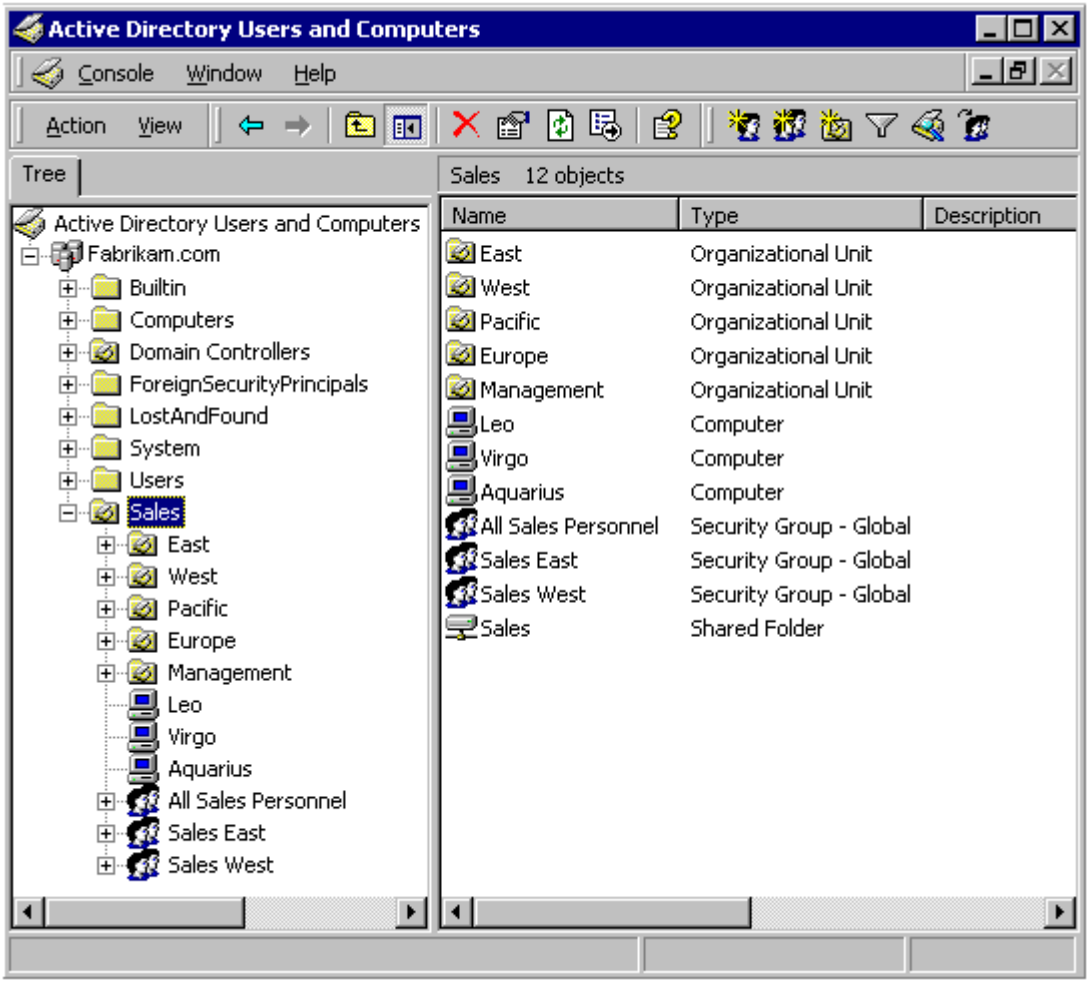
## 4.1 Active Directory -tietokanta

Active Directory tuli Windows-ympäristöihin Windows 2000 Server -palvelinkäyttöjärjestelmän julkaisemisen myötä. Sen yleisimmin käytetty osa, josta tässäkin puhutaan, on Active Directory Domain Services. Kyseessä on eräänlainen tietokanta, joka sisältää erityyppisiä objekteja, lähinnä tietokoneita (sekä työasemia että palvelimia), käyttäjiä ja oikeusryhmiä, järjestettynä ”kansioihin”, joiden virallinen nimi on organizational unit (kuva 6). [Active Directory Tutorial 2007: 20; What is Active Directory Domain Services and how does it work? 2012: 21; Tutorial Overview: ADSI with Visual Basic 2017: 22.]

Toimialueen (domain) lisäksi Active Directoryssä on muitakin rakenteita, kuten puita (tree) ja niiden muodostamia metsiä (forest), mutta niihin ei tarvitse perehtyä tässä yhteydessä. Kyseessä ovat toimialuetta laajemmat rakenteet; toimialue on osa puuta ja puu puolestaan osa metsää, eivätkä ne sinällään vaikuta toimialueen sisäiseen toimintaan, kuten käyttöoikeuksiin. [Active Directory Tutorial 2007: 20; What is Active Directory Domain Services and how does it work? 2012: 21; Tutorial Overview: ADSI with Visual Basic 2017: 22.]

Active Directory varmistaa, että kaikilla lähiverkon käyttäjillä on pääsy niihin resursseihin, joihin heille on myönnetty käyttöoikeus, ja vastaavasti, että resurssien käyttö on rajattu vain sallittuihin käyttäjiin. Autentikointi tapahtuu koko ajan yhdellä käyttäjätunnuksella Active Directoryn tietokantaa vasten, eikä käyttäjillä näin ollen tarvitse olla erillistä tun-

nusta esimerkiksi jokaiselle palvelimelle. [Active Directory Tutorial 2007: 20; What is Active Directory Domain Services and how does it work? 2012: 21; Tutorial Overview: ADSI with Visual Basic 2017: 22.]




Kuva 6. Esimerkki Active Directoryn rakenteesta [Tutorial Overview: ADSI with Visual Basic 2017: 22].

## 4.2 Toimialue

Active Directoryssä täytyy olla vähintään yksi toimialue. Toimialue on hallintoalue, jonka sisäisiä objekteja hallitaan monilla työkaluilla, kuten Security Policy- ja Group Policy -komponenteilla. [Active Directory Tutorial 2007: 20; What is Active Directory Domain Services and how does it work? 2012: 21.]

Toimialueen ytimen muodostaa yksi tai useampi Domain Controller -palvelin, joilla tietokanta ja hallintatyökalut sijaitsevat. Microsoftin suositusten mukaan Domain Controller -palvelimia pitäisi olla vähintään kaksi toimialueen palvelujen takaamiseksi toisen rikkoutuessa. Jokaisella Domain Controller -palvelimella on kopio Active Directory -tietokannassa, joka toimialueen toimiessa normaalisti on identtinen muiden palvelimien tietokantojen kanssa. [What is Active Directory Domain Services and how does it work? 2012: 21.]

Tiedot pysyvät identtisinä niin, että Domain Controllerit replikoivat tietoja keskenään. Kun yhdellä palvelimella jokin Active Directory -objekti muuttuu, palvelin ilmoittaa siitä lähimmille muille Domain Controller -palvelimille, jotka tekevät vastaavat muutokset omiin tietokantoihinsa. [Active Directory Replication 2017: 9.]

Domain Controller syntyy, kun tavallinen palvelin nostetaan Domain Controller -asemaan. Tällöin jokaisella palvelimella tavallisesti sijaitsevat käyttäjäryhmät poistuvat käytöstä ja ”paikallisiakin” käyttäjiä ylläpidetään jatkossa Active Directoryssä. Domain Controllerin Administrator-oikeuksia ei siis saa kuulumalla palvelimen Administrators-ryhmään, vaan tulee kuulua toimialueen Administrators-ryhmään.

Käyttäjän kirjautuessa toimialueen jäsenkoneelle toimialuetunnuksellaan sekä koneen että käyttäjän tili autentikoidaan vasten Active Directory -tietokantaa. Molempien täytyy olla kunnossa, jotta kirjautuminen hyväksytään ja käyttäjät saa itselleen kuuluvat toimialueen palvelut ja resurssit käyttöönsä. [What is Active Directory Domain Services and how does it work? 2012: 21.]

## 4.3 Toimialueen pääkäyttäjät

Windows-toimialueella on useita käyttöoikeusryhmiä, jotka syntyvät automaattisesti, kun toimialue alun perin luodaan. Osalla näistä ryhmistä on erittäin korkeita oikeuksia sekä toimialueen jäsenkoneisiin ja -palveluihin, että toimialueeseen itseensä. [Mathers 2017: 23.]

Nämä ryhmät (englanniksi Protected Groups) erottuvat muista ryhmistä attribuutilla nimeltä AdminSDHolder, joka varmistaa, että siihen liittyvillä käyttöoikeusryhmillä on niiden vaatimat suojaukset ja ettei niitä pysty muuttamaan näiden ryhmien ulkopuolelta.

Esimerkiksi oikeutta vaihtaa ryhmään kuuluvan käyttäjän salasanaa ei voi delegoida käyttäjille, jotka eivät itse ole näiden ryhmien jäseniä. [Price 2014: 24.]

Protected Groups -ryhmien määrä on lisääntynyt Active Directoryn versiosta toiseen (kuva 7): uusimmassa versiossa niitä on 13. Projektin kohteeksi valittiin Domain Admins -ryhmä useista syistä, joista osaa käsitellään luvussa 4.4.

| | | | |
|---|---|---|---|
| **Windows 2000 <SP4** | **Windows 2000 SP4 - Windows Server 2003 RTM** | **Windows Server 2003 SP1+** | **Windows Server 2012, Windows Server 2008 R2, Windows Server 2008** |
| Administrators | Account Operators | Account Operators | Account Operators |
| | Administrator | Administrator | Administrator |
| | Administrators | Administrators | Administrators |
| | Backup Operators | Backup Operators | Backup Operators |
| | Cert Publishers | | |
| Domain Admins | Domain Admins | Domain Admins | Domain Admins |
| | Domain Controllers | Domain Controllers | Domain Controllers |
| Enterprise Admins | Enterprise Admins | Enterprise Admins | Enterprise Admins |
| | Krbtgt | Krbtgt | Krbtgt |
| | Print Operators | Print Operators | Print Operators |
| | | | Read-only Domain Controllers |
| | Replicator | Replicator | Replicator |
| Schema Admins | Schema Admins | Schema Admins | Schema Admins |
| | Server Operators | Server Operators | Server Operators |

Kuva 7. Protected Groups Microsoft Windows-toimialueen eri versioissa [Mathers 2017: 23].

## 4.4 Domain Admins -ryhmä

Domain Admins -ryhmä on ehkä Windows Active Directory -järjestelmän käytetyin ryhmä, mutta myös väärinkäytetyin. Ryhmällä on laajat käyttöoikeudet, ja sen ominaisuudet tunnetaan hyvin, koska se on yksi vanhimmista Protected Groups -ryhmistä. Näin ollen sitä on vuosia käytetty lukemattomissa organisaatioissa eräänlaisena yleis-

avaimena, jonka jäsenyydellä on helppoa ja nopeaa ratkaista ylläpitäjien käyttöoikeusongelmat. Tämä tietenkin rikkoo pienimpien käyttöoikeuksien periaatetta, johon tutustuttiin luvussa 3.

Oletuksena Domain Admins -ryhmä on toimialueen Administrators-ryhmän jäsen (kuva 8), mitä kautta suurin osa ryhmän oikeuksista Domain Controller -palvelimiin tulee. Ryhmän jäsenillä on oikeus hallita toisia Protected Groups -ryhmiä ja muuttaa niiden jäseniä, ja tietenkin Domain Admins -ryhmän voi liittää mihin tahansa oikeusryhmään jäseneksi ja näin tuoda ryhmälle entistä enemmän oikeuksia. [Active Directory Security Groups 2014: 25.]

| Attribute | Value |
|---|---|
| Well-Known SID/RID | S-1-5-<domain>-512 |
| Type | Domain Global |
| Default container | CN=Users, DC=<domain>, DC= |
| Default members | Administrator |
| Default member of | Administrators<br>Denied RODC Password Replication Group |
| Protected by ADMINSDHOLDER? | Yes |
| Safe to move out of default container? | Yes |
| Safe to delegate management of this group to non-Service admins? | No |

Kuva 8. Domain Admins -ryhmän ominaisuuksia [Active Directory Security Groups 2014: 25].

Kun tavallinen niin sanottu stand-alone-palvelin liitetään toimialueeseen jäsenpalvelimeksi, sille syntyy luottosuhde toimialueeseen. Samalla toimialueen Administrator-ryhmä liitetään uuden jäsenpalvelimen paikalliseen Administrators-ryhmään, mitä kautta Domain Admins -ryhmän jäsenillä on sen jälkeen ylläpito-oikeudet tähänkin palvelimeen.

Tässä luvussa on kuvattu teknistä taustaa projektille, jossa toteutettiin ISO/IEC 27001 -sertifikaatin mukainen Domain Admins -oikeuksien katselmointi ja sen seurauksena niiden karsiminen. Luvussa 5 perehdytään itse projektiin.

# 5 Domain Admins -ryhmän jäsenyyksien vähentäminen

Kaikki edellä kirjoitettu on pohjustanut tätä projektikuvausta. Edellisten lukujen myötä on muodostunut kuva niin projektiin liittyvästä tekniikasta kuin myös sen motivaatioista, mukaan luettuna huoltovarmuuskriittisen yrityksen korostunut painotus tietoturvaan.

Tässä luvussa kuvataan itse insinöörityöprojektia: sen esitöitä, toteutusta ja ongelmia. Projektissa suoritettiin ISO/IES 27001 -standardin suosittelema toimialueen käyttöoikeuksien tarkastelu ja päädyttiin arvioimaan uudelleen koko Domain Admins -ryhmän jäsenistö. Tämä on tyypillisesti yrityksissä ongelmallinen ryhmä, ja kohteena oleva toimialue on viisitoista vuotta vanha, joten ylimääräisiä oikeuksia oli ehtinyt kertyä.

Insinöörityö toteutettiin projektimuotoisena, mutta pieneksi arvioidun työmääränsä vuoksi yrityksen virallisen projektihallinnan ulkopuolella. Näin ollen projektilta puuttuivat muodollinen, kirjallinen projektisuunnitelma ja ohjausryhmä, jotka jälkikäteen arvioituna olisivat ryhdistäneet projektin toteutusta.

Projektissa oli yksi pääasiallinen jäsen, mutta aikaa oli varattu runsaasti, joten tämän ei olisi pitänyt olla ongelma. Sekä resurssien käyttö että aikataulutus osoittautui kuitenkin lopulta ongelmalliseksi, mistä puhutaan lisää myöhemmin tässä luvussa.

## 5.1 Riskit

Koska Domain Admins -ryhmän jäsenet ovat jo oletusarvoisesti avainasemassa ja heidän oikeuksiensa kattavuus oli vain laajentunut vuosien myötä, projektin tunnistettiin sisältävän useita riskejä. Yksi ryhmistä, jolle Domain Admins -oikeudet oli myönnetty, oli yrityksen ICT-päivystäjät. Tämä päivystysrinki muodostuu ICT-alan henkilöistä, jotka kukin vuoroviikollaan vastaavat yrityksen tietoteknisen infrastruktuurin toiminnasta virka-ajan ulkopuolella. Huolimaton oikeuksien karsiminen olisi siis saattanut vaarantaa jokapäiväisen ylläpitotyön lisäksi myös virka-ajan ulkopuolella tapahtuvan kriittisen vianselvityksen.

Vuosien mittaan Domain Admins -ryhmälle oli myönnetty erilaisia oikeuksia, joita ei kuitenkaan ollut kirjattu mihinkään, joten ryhmän kaikista oikeuksista ei ollut mitenkään mahdollista muodostaa käsitystä. Tästä lähtötilanteesta pääasiallisiksi riskeiksi katsottiin

- rutiiniylläpidon häiriintyminen
- virka-aikaan ilmenevien vikojen selvittämisen hidastuminen
- virka-ajan ulkopuolella ilmenevien vikojen selvittämisen estyminen
- tietoturvatapahtumien kontrolloimisen vaikeutuminen.

Tilanteen palauttaminen ennalleen olisi sinällään ollut helppoa: oikeudet saataisiin ylläpitäjille takaisin yksinkertaisesti lisäämällä tunnukset takaisin Domain Admins -ryhmään. Tätä kuitenkin pidettiin erittäin ei-toivottavana, koska ylimääräisistä oikeuksista haluttiin nyt kerralla eroon ja koska oikeuksien palauttaminen olisi hidastanut ongelmien selvittämistä. Eräs tekijä oli myös se, että projekti oli ajautunut aikataulullisiin ongelmiin, joita kuvataan myöhemmin, ja niin sanottu roll-back eli tehtyjen muutosten peruminen olisi pahentanut tätä entisestään. Tähän vaihtoehtoon ei missään vaiheessa päädyttykään.

## 5.2 Valmistelevat työt

Projektin aivan ensimmäinen vaihe oli riskien kartoitus, ja kuten luvusta 5.1 käy ilmi, riskejä havaittiin useita. Moninaisten riskien takia projekti aloitettiin huolellisella valmistelulla. Jälkikäteen ajateltuna hieman naiivina pyrkimyksenä oli, että muutoksesta ei aiheutuisi mitään häiriötä eivätkä ylläpitäjät edes huomaisi oikeuksiensa muuttuneen.

Tämä pyrkimys huomioon ottaen tärkein esityö oli sen selvittäminen, mitä oikeuksia ylläpitäjät jatkossa tarvitsisivat. Koska Active Directoryssä ei ole mitään selvää tapaa selvittää sitä, mitä oikeuksia jollekin ryhmälle sen jäsenyyksien kautta muodostuu, tätä jouduttiin lähestymään vähemmän teknisillä ratkaisuilla.

### Oikeustarpeiden kartoitus

Ensimmäisessä vaiheessa käyttäjiltä kyseltiin, minkälaisia oikeuksia heidän työnsä vaatii. Tämä ei ollut kovin onnistunut lähestymistapa, koska osoittautui, että ylläpitäjillä oli varsin hatara käsitys sekä tunnuksensa oikeuksist, että työtehtäviensä vaatimasta oikeustasosta. Monet luulivat aidosti tarvitsevansa Domain Admins -tasoisia tunnuksia esimerkiksi muutaman toimialueen jäsenpalvelimen ylläpitämiseen.

Kartoitusta vaikeutti myös se, että pääosa Domain Admins -ryhmän jäsenistä oli ryhmässä sen takia, että he kuuluivat edellä mainittuun ICT-päivystysryhmään ja heidän tavalliset työtehtävänsä poikkesivat toisistaan huomattavasti. Näissäkin tehtävissä oli kuitenkin saatettu nojautua Domain Admins -oikeuksiin, eikä todellista oikeustarvetta kyseisiin tehtäviin ollut koskaan selvitetty.

Kartoituksen jälkeen asiaa mietittiin uudestaan. Koska ylläpitäjien työt yleisesti ottaen tunnettiin varsin tarkkaan, niitä tarkasteltiin juuri yleisellä tasolla ja arvioitiin tarvittavia oikeuksia. Kaikki Domain Admins -ryhmän jäsenet oli listattu kartoitusta varten, ja nyt listaa käytiin läpi toimialueen omistajan kanssa ja henkilö henkilöltä pohdittiin työtehtäviä ja niiden oikeustarpeita. Tämän läpikäynnin lopputulos oli, että kaikki ylläpitäjät poistetaan Domain Admins -ryhmästä. Näin suuri muutos ei ollut ollut kenelläkään mielessä ennen projektia, joten sitä jouduttiin pohtimaan, mutta tämä todellakin vahvistui parhaaksi toimintatavaksi.

Varsinaiset Domain Admins -oikeudet liittyvät lähinnä itse toimialueen ylläpitoon ja muuttamiseen eikä niinkään palvelinten, edes Domain Controllerien, ylläpitoon. Ei siis ehkä olisi pitänyt tulla yllätyksenä, että todellisuudessa niitä tarvittiin hyvin harvoin.

Päätettiin, että luodaan uusi toimialueen käyttäjäryhmä (jatkossa ”itpro”), jolle annettaisiin kaikki palvelimien ylläpitämiseen tarvittavat oikeudet, ja siihen liitettäisiin kaikki tarpeelliset ylläpitäjät. Toimialueen ylläpitoa varten taas luotiin erilliset tunnukset niille muutamille ylläpitäjille, joilla oli todellinen pätevyys toimialueen rakenteiden muuttamiseen.

Testitunnus

Oli siis osoittautunut varsin vaikeaksi varmistaa kyselemällä käyttäjiltä tai edes asiantuntijalähteiltä, mitä oikeuksia mitkäkin ylläpitotehtävät vaativat. Parhaaksi vaihtoehdoksi katsottiin tehdä uusi ryhmä, itpro, jolla olisi aluksi vain perusoikeudet, ja sijoittaa ryhmään testitunnus. Sitten katsottaisiin, mitkä tehtävät tältä tunnukselta estyisivät, ja ryhmälle lisättäisiin oikeuksia sen mukaan. Tässä vaiheessa projektilla oli jäljellä varsinaista työaikaa enää pari viikkoa (väliin asettuivat vuodenvaihteen pyhät), ja tämän kiireen vaikutuksiin perehdytään luvussa 5.4.

Testitunnuksen käyttö ei teoriassakaan tuottanut täydellistä näkymää tarvittaviin oikeuksiin, koska ylläpitäjien tehtävät olivat hyvin monipuolisia. Oletettiin kuitenkin, että näinkin

päästäisiin hyvään ja sujuvaan lopputulokseen. Lopulta kävi ilmi, että luotto Domain Admins -oikeuksiin oli projektissa aliarvioitu.

## 5.3 Toteutus

Kun näytti siltä, että uudella itpro-ryhmällä oli kaikki tarpeelliset oikeudet, siirryttiin projektin toteutukseen. Aivan ensin luotiin ne uudet tunnukset, joilla oli jatkossa tarkoitus ylläpitää toimialuetta. Tämä oli ensimmäinen toimenpide sen estämiseksi, että jollain projektin aikaisella konfiguraatiovirheellä suljettaisiin ylläpitäjät kokonaan ulos toimialueelta. Tämä olikin lähellä, kuten luvussa 5.4 kerrotaan.

Seuraavaksi kaikki Domain Admins -ryhmän ylläpitäjätunnukset, joille tämän tason oikeudet oli katsottu jatkossa tarpeellisiksi luvun 5.2 listatarkastelussa, siirrettiin uuteen ryhmään ja poistettiin Domain Admins -ryhmästä. Tässä yhteydessä ylläpitäjien oikeudet muuttuivat lähes välittömästi.

Yleinen Active Directory -oikeuksia koskeva käsitys on, että käyttäjätunnuksen oikeuksien muuttuminen vaatii koneelle kirjautumisen. Näin ollen, jos tunnus on kirjautuneena koneella, uudet oikeudet tulevat voimaan vasta uudelleenkirjautumisen yhteydessä. Tämä ei kuitenkaan täysin pidä paikkaansa, vaikka tuo väärinkäsitys tässäkin tapauksessa oli yksi projektin perusoletuksista.

Kirjautuessa tulevien oikeuksien lisäksi Active Directory -tunnuksella on kahdenlaisia oikeuksia. Ensimmäiset, ne oikeudet jotka määritellään jonkin Group Policyn kautta, tulevat voimaan, kun koneen Group Policy -asetukset päivittyvät säännöllisin väliajoin, yleensä noin kahdenkymmenen minuutin välein. Osa oikeuksista taas astuu voimaan välittömästi. Nämä välittömästi voimaan tulevat oikeudet aiheuttivat hämmennystä ja sekaannusta ylläpitäjien parissa, varsinkin kun luvussa 5.5 kuvattavien aikatauluongelmien takia projektin tiedotus oli jäänyt vähäiseksi.

## 5.4 Tekniset ongelmat

Tähän asti oli siis tehty valmistelutöitä ja toivottu ongelmatonta toteutusta, mutta nyt alkoi varsinainen työ. Henkisestä varautumisesta huolimatta tuli ikävänä yllätyksenä, kuinka

paljon ongelmia varsinaisesta muutoksesta aiheutui. Etukäteen huolellisina pidetyt esivalmistelutyöt osoittautuivat alimitoitetuiksi. Myöhemmin tässä luvussa kerrotaan, kuinka projektin ongelmat alkoivat jo ennen muutostyötä.

Tässä luvussa kuvattujen isompien ongelmatilanteiden lisäksi korjattiin lukuisia pienempiä, joita selvityskiireen takia ei kaikkia edes kirjattu. Esiintyi palvelin- tai jopa tietokantakohtaisia oikeuspuutoksia, kun asentamisen aikoihin joidenkin tietokantojen oikeuksiin ei ollut kiinnitetty mitään huomiota, annettu vain kaikki oikeudet Domain Admins -ryhmälle, johon silloin oletettiin kaikkien ylläpitäjien kuuluvan.

Jokaisen ison muutosprojektin tapaan projektin selvityslistalle päätyi myös projektiin liittymättömiä ongelmia. Varsinkin näin kiistellyn muutoksen yhteydessä kaikkien ongelmien, jotka nousivat esiin ajallisesti lähellä tehtyä muutosta, epäiltiin liittyvän muutokseen. Niiden selvittäjille täytyi erikseen perustella, miksi ongelmat eivät olleet aiheutuneet tästä projektista.

Projektin todelliset ongelmat eivät olleet kuitenkaan teknisiä, vaan projektin hallintaan liittyviä. Niitä käsitellään luvuissa 5.5–5.7, kun on ensin perehdytty muutamaan kiinnostavimpaan tekniseen ongelmaan.

Domain Controllerien etäkäyttöoikeudet

Ensimmäinen ongelma tuli esiin jo ennen projektin varsinaista muutostyötä. Testivaiheessa haluttiin varmistua, että itpro-ryhmän jäsenet pystyisivät ylläpitämään toimialueen Domain Controller -palvelimia, vaikka niillä sijaitsevaa toimialuetta ei enää pystyttäisikään ylläpitämään. Tämä oli aikaisemmin ollut itsestäänselvyys, koska Domain Controllereilla ei ollut erillistä, paikallista ylläpitoryhmää kuten toimialueen jäsenpalvelimilla, vaan Domain Admins -ryhmän jäsenet olivat oletusarvoisesti näiden palvelinten ylläpitäjiä toimialueen Administrators-ryhmän jäsenyyden kautta. Nyt nämä roolit haluttiin erottaa toisistaan.

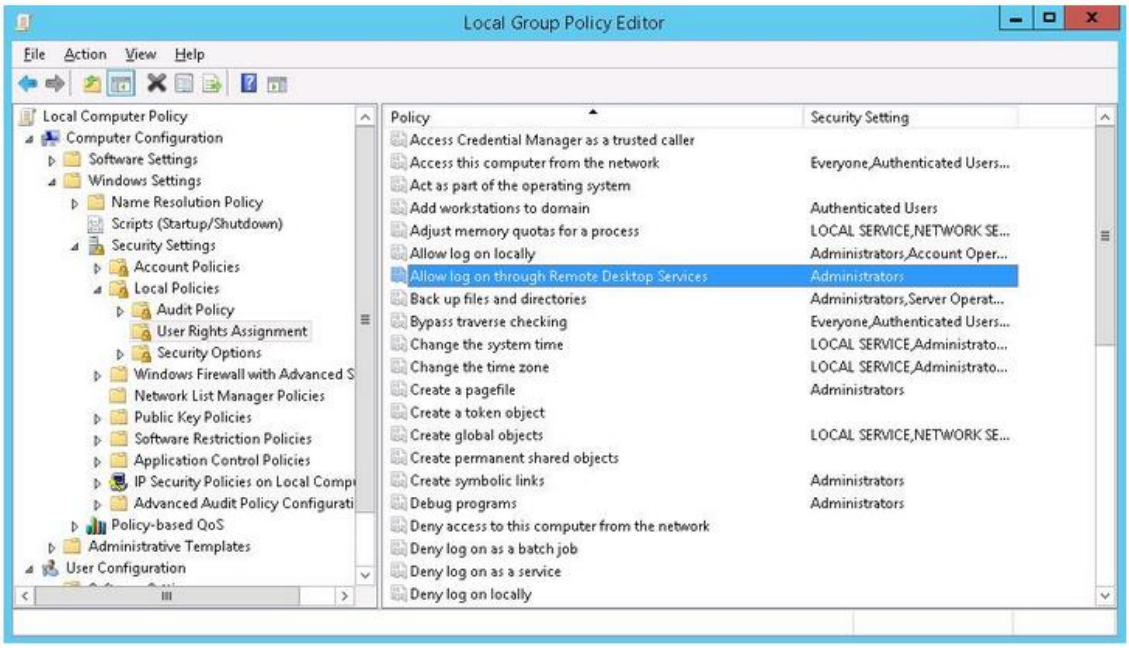
Ensin ryhmä lisättiin Domain Controllerin “näkymättömään” Remote Desktop Users -ryhmään. Tämä ryhmä ei näy missään palvelinhallinnan graafisissa käyttöliittymissä, joten sitä käytetään tekstiliittymien, kuten PowerShellin, kautta (kuva 9). [Allow non-administrators RDP Access to Domain Controller 2015: 30.]


Kuva 9. Domain Controllerin Remote Desktop Users -ryhmän muuttaminen [Allow non-administrators RDP Access to Domain Controller 2015: 30].

Tämän lisäksi ryhmän osalta piti muuttaa Domain Controllerin Group Policyä (kuva 10). Group Policy on Active Directoryn työkalu, jolla voidaan keskitetysti muuttaa sekä palvelimien että työasemien asetuksia. Näiden asetusten muuttaminen paikalliselta koneelta käsin voidaan jopa kokonaan estää. [Group Policy for Beginners 2011: 32.]

Tällaisessa projektissa on erityisen tärkeää hahmottaa ero kahden helposti sekaisin menevän Group Policy -objektin, Domain Controller Policyn ja Domain Policyn, välillä. Objektien nimet ovat hyvin samanlaiset, mutta niillä on aivan erilaiset käyttötarkoitukset. [Group Policy for Beginners 2011: 32.]

Domain Controller Policy määrittelee Domain Controller -palvelimien asetuksia. Domain Policy taas koskee jokaista toimialueen jäsenkonetta, sekä työasemia että palvelimia. Tämän objektin muuttamisella olisi siis paljon laajempia vaikutuksia kuin pelkän Domain Controller Policyn muuttamisella. [Group Policy for Beginners 2011: 32.]




Kuva 10. Domain Controller Policyn muuttaminen [Allow non-administrators RDP Access to Domain Controller 2015: 30].

Domain Controller Policyn muuttamisen jälkeen törmättiin vakavaan ongelmaan. Muutosten jälkeen ainoastaan itpro-ryhmän jäsenet, tässä vaiheessa siis vain yksi testitunnus, pääsivät etäyhteydellä Domain Controller -palvelimille. Vikatilanteessa kukaan ei pääsisi ylläpitämään näitä kriittisiä palvelimia, ja koko toimialue saattaisi lamaantua ja estää pääsyn pääosaan lähiverkon resursseista. CIA-kolmion Availability, saatavuus, oli siis pahasti uhattuna.

Tutkimustyön tuloksena saatiin selville, että ”Allow log on through Remote Desktop Services” -asetus sallii oletuksena toimialueen Administrators-ryhmälle, johon myös Domain Admins -ryhmä kuuluu, etäpääsyn Domain Controllereille. Tämä oletusarvo kuitenkin kumoutuu, jos asetusta mitenkään muutetaan, ja muutoksen jälkeen vain erikseen sallituilla käyttäjillä ja ryhmillä on etäkäyttöoikeus. Ongelma siis poistui sallimalla Administrators-ryhmä manuaalisesti. [Adminstrator cannot log on to server via remote desktop after changing default domain policy 2013: 31.]

Jäsenpalvelinten etäkäyttö- ja ylläpito-oikeudet

Toimialueen jäsenpalvelimille oli helppoa sallia etäkäyttö Group Policyn kautta. Kuitenkin, kun ylläpitäjiltä otettiin Domain Admins -oikeudet pois, huomattiin, ettei kukaan pääsekään jäsenpalvelimille. Osoittautui, ettei itpro-ryhmällä enää ollutkaan samoja oikeuksia kuin testivaiheessa.

Syylliseksi esitettiin muun muassa Domain Controllerien replikoinnin häiriötä, mutta se vaikuttaa epätodennäköiseltä, kun mitään muita ongelmia ei esiintynyt. Tosiasia kuitenkin oli, että itpro-ryhmä ei enää ollut jäsenenä osassa niistä käyttöoikeusryhmistä, joihin se testivaiheessa oli liitetty.

Niin kiinnostava kuin ongelma olikin, syy ei koskaan selvinnyt. Group Policyn pikainen muokkaaminen palautti oikeudet, ja siihen jouduttiin tyytymään.

Nimenselvitys- ja IP-osoitepalvelut DNS ja DHCP

Toimialueen DNS- ja DHCP-palvelut sijaitsevat yleensä Domain Controller -palvelimella. Molemmat liittyvät TCP/IP-verkkojen hallintaan ja ylläpitoon.

DNS, Domain Name System, pitää yllä taulukkoa koneiden nimistä ja IP-osoitteista [DHCP and DNS 2017: 33.] Kun käyttäjä tarvitsee resursseja koneelta nimeltä Tiedostopalvelin, DNS-palvelu kertoo käyttäjän koneelle kyseessä olevan kone, jonka IP-osoite on 1.2.3.42. Tämä toimii myös erittäin suurissa tietoverkoissa, esimerkiksi Internetiä käytettäessä opiskelijan kone tarvitsee DNS:ltä tiedon, että www.metropolia.fi-sivuston IP-osoite on 195.148.144.10.

DHCP, Dynamic Host Configuration Protocol, suorittaa useita tehtäviä, joista yleisin on IP-osoitteiden jakaminen lähiverkossa oleville koneille. Verkkoon liittyessään kone saa uniikin osoitteen, niin että kaikki sille tuleva liikennöinti löytää perille. [DHCP and DNS 2017: 33.]

DNS:n ja DHCP:n ylläpito vaatii erilliset oikeudet. Active Directoryssä syntyy toimialuetta luotaessa automaattisesti erinäisiä käyttöoikeusryhmiä. Niistä DHCP Administrators- ja

DNS Admins -ryhmiä ei ollut projektin yrityksessä käytetty aiemmin, koska Domain Admins -ryhmä on näiden ryhmien jäsen, joten ryhmän jäsenyyden mukana tuli nämäkin oikeudet. Liittämällä itpro-ryhmä näihin ryhmiin saatiin ylläpitäjille tarpeelliset oikeudet.

Active Directoryn ylläpito

Vaikka Domain Admins -oikeudet eivät sinällään liity Active Directoryn sisäiseen toimintaan vaan toimialueen ylläpitoon, on Domain Admins -ryhmällä myös tällaisia oikeuksia, ja usein niitä on myös annettu lisää, kun ryhmää on käytetty yleisenä ylläpitäjäryhmänä. Tässäkin projektissa todettiin, että Domain Admins -oikeuksien poiston jälkeen monien toimenpiteiden suorittaminen Active Directoryssä estyi.

Organizational Unit -kansioiden luominen estyi. Kaikki objektit Active Directoryssä on järjestetty Organizational Unit -kansioihin, joita ei yllättäen pystytty enää luomaan. Ongelmaa ei vielä tätä kirjoitettaessa ole selvitetty, koska tämä on varsin harvinainen toimenpide vakiintuneessa toimialueessa eikä ongelmaa ole priorisoitu korkealle.

Ylläpitäjien käyttäjätunnusten salasanojen vaihtaminen estyi. Kuten luvussa 4 mainittiin, Domain Admins -ryhmän kaltaisten Protected Groups -ryhmien jäseniä suojelee attribuutti nimeltä AdminSDHolder, joka muun muassa estää tavallisia tilejä vaihtamasta tällaisten tilien salasanoja. Projektissa oletettiin, että tämä objekti poistuisi, kun tilit poistetaan Domain Admins -ryhmästä, mutta näin ei käynytkään. Huomattiin myös, että monien sellaisten ylläpitotunnusten, jotka eivät koskaan olleet olleetkaan Domain Admins -ryhmässä, salasanoja ei myöskään voitu vaihtaa. Todettiin, että tunnuksia oli tapana luoda kopioimalla jonkun vastaavaa työtä tekevän tunnus uuden tunnuksen pohjaksi, ja näin myös AdminSDHolder-attribuutti oli kopioitunut moniin tunnuksiin. Lopulta laadittiin skripti, joka kartoitti kaikki AdminSDHolder-attribuutilliset tunnukset, jotka eivät olleet parhaillaan jäsenenä jossain Protected Groups -ryhmässä ja poisti objektin.

Jäsenten lisääminen Active Directoryn käyttöoikeus- ja organisaatioryhmiin vaikeutui. Kuten aikaisemmin on mainittu, monissa organisaatioissa Domain Admins -ryhmää on käytetty eräänlaisena yleisenä ylläpitoryhmänä. Näin ollen myös monien Active Directory -ryhmien hallintaoikeudet olivat jääneet säätämättä kuntoon, koska Domain Admins -oikeuksilla niitä pystyi ylläpitämään. Oikeuksien poiston jälkeen on löytynyt useita ryh-

miä, joita oikeastaan kukaan ei ole pystynyt ylläpitämään ennen hallintaoikeuksien säätämistä, koska vain muutamalla jäljellä olevalla Domain Admins -ryhmän jäsenellä oli enää oikeudet ylläpitää niitä.

Group Policy -objektien hallinta estyi hetkellisesti. Group Policy on yksi Windows-toimialueen tärkeimmistä keskitetyn hallinnan työkaluista. Kuitenkin näiden hallintaoikeuksien kanssa oli hyvin samanlainen tilanne kuin edellä mainittujen käyttöoikeus- ja organisaatioryhmien: oikeuksia ei ollut säädetty harkiten, vaan Domain Admins -oikeuksia käytettiin eräänlaisena yleisavaimena. Hiukan ennen projektia oli kuitenkin tullut tarpeelliseksi antaa oikeuksia myös sellaisille ylläpitäjille, jotka eivät kuuluneet Domain Admins -ryhmään, ja näin ollen oli olemassa valmis käyttöoikeusryhmä, jonka kautta Group Policy -oikeudet saatiin niille ylläpitäjille, joilta poistettiin Domain Admins -oikeudet.

## 5.5 Aikatauluongelmat

Projektin suurin ongelma, joka oli perussyynä useimmille muille ongelmille, oli aikataulutus. Aikaa oli alun perin useita kuukausia, ja lopulta projekti vei alusta loppuun lähes vuoden. Työmäärä ei kuitenkaan ollut lainkaan samassa mittakaavassa, eikä projekti suurimman osan tuosta ajasta edistynyt ollenkaan, vaan muut työtehtävät priorisoitiin ohi.

Pääosa siitä ajasta, joka projektiin todellisuudessa käytettiin, meni alussa mainittuun käyttöoikeuskartoitukseen. Sen jälkeen projekti oli pitkään pöytälaatikossa, kunnes aika alkoi loppua. Testitunnusvaiheeseen käytettiin lopulta noin kaksi viikkoa ja itse muutoksen tekemiseen noin tunti. Ongelmia korjattiin aktiivisesti kymmenisen arkipäivää, minkä jälkeen kiireettömämpiä ja myöhemmin esiin tulleita ongelmia on korjattu muiden töiden lomassa.

Lopun kiire oli iso tekijä useimmissa teknisissä ongelmissa. Se myös vaikutti luvuissa 5.6 ja 5.7 mainittuihin tiedotus- ja delegointiongelmiin, joista huono delegointi puolestaan vaikutti omalta osaltaan teknisiin ongelmiin ja niiden selvittämiseen.

## 5.6 Tiedotusongelmat

Heikko tiedotus projektissa oli paitsi ongelma itsessään, se myös pahensi muita ongelmia. Tiedotuksen vähäisyys johtui osin tiedotuksen merkityksen väheksymisestä, osin projektin lopun kiireestä, mutta oli myös vastareaktio projektin kohteena olevien ylläpitäjien äänekkääseen muutosvastarintaan. Projektista ja sen etenemisestä olisi kaikesta huolimatta pitänyt tiedottaa paremmin paitsi kyseisille ylläpitäjille, myös ICT-organisaatiolle yleensä.

Paremmalla tiedottamisella olisi ehkä ollut mahdollista saada parempia vastauksia alun oikeustarvekartoitukseen, jolloin joiltain muutosta seuranneilta oikeuspuutosongelmilta olisi vältytty. Tiedotuksella olisi myös varmasti saatu vähennettyä muutosvaiheen vastareaktiota ja siten nopeutettu vianselvitystä.

Yleinen tiedottaminen olisi vähentänyt huhuja ja selkeyttänyt organisaatiolle projektin vaikutuksia. Näin olisi vältytty monilta niistä tilanteista, joissa projektiin liittymättömiä ongelmia selvittäneet ylläpitäjät eivät olleet varmoja, oliko projektin oikeusmuutos syynä heidänkin ongelmiinsa. Tämä olisi nopeuttanut ongelmien selvittämistä ja pitänyt ne pois kasvattamasta projektin ongelmalistaa.

## 5.7 Delegointiongelmat

Projektin kohteena ollut Active Directory on yksi projektiyrityksen keskeisistä järjestelmistä. Sen muutokseen ja muutoksen tuomiin ongelmiin olisi siis löytynyt teknistä osaamista, jota tässä projektissa ei kuitenkaan hyödynnetty likimainkaan tarpeeksi.

Pääasiallinen syy resurssien käyttämättömyyteen oli kireä aikataulu. Koska kyseisillä asiantuntijoillakin oli paljon töitä ja tiukka aikataulu, ei heiltä löytynyt aikaa ongelmien ratkomiseen aikataulullisesti nurkkaan ajetun projektin puitteissa.

Kiire myös korotti kynnystä kysyä yksinkertaisiakin neuvoja, koska koettiin, ettei ollut aikaa odottaa vastauksia. Moninkertainen aika käytettiin sitten ongelmien ratkaisuun vähemmän osaavien asiantuntijoiden toimesta.

## 5.8 Projektin tulos

Lukuisista ongelmista huolimatta projekti saatiin lopulta päätökseen sillä lopputuloksella kuin oli tarkoituskin. Domain Admins -ryhmää on pienennetty huomattavasti, eikä merkittäviä oikeuspuutoksia ole tullut vastaan.

# 6 Yhteenveto

Tässä raportissa on esitelty energiayhtiössä toteutettua, ISO/IEC 27001 -sertifikaattia seurailevaa insinöörityöprojektia, jossa vähennettiin toimistoverkon Domain Admins -ryhmän jäsenten määrää. Kuten monissa organisaatioissa, myös projektiyhtiössä Domain Admins -oikeuksia oli käytetty eräänlaisena ylläpitäjien yleisavaimena, vastoin alan parhaita käytäntöjä.

Vaikka liialliset käyttöoikeudet ovat yleinen ongelma yrityksissä, ongelma korostuu huoltovarmuuskriittisessä organisaatiossa. Lisääntyneet kyberuhat niin erilaisten aktivistien ja kyberrikollisten kuin kansallisvaltioidenkin taholta ovat nostaneet huoltovarmuustoimijoiden tietoturvan aiempaa suuremman huomion kohteeksi.

Työssä perehdyttiin tietoturvan merkitykseen huoltovarmuuskriittisille organisaatioille kansainvälisten esimerkkien valossa, sekä siihen, kuinka suuri merkitys kyberuhilla on urbaanissa toimintaympäristössä. Tiiviissä kaupunkiympäristössä energiahuoltoa muualla Suomessa uhkaavien luonnonilmiöiden vaikutus on infrastruktuurin luonteen vuoksi olematon.

Projektin ymmärtämisen kannalta perustiedot Microsoftin Windows Active Directory -ympäristöstä ovat oleellisia, ja sitä onkin esitelty luvussa 4. Tämä ympäristö on erittäin yleisesti käytetty yritysmaailmassa, joten kuvatut ongelmat, niin projektin alkuasetelma kuin sen toteutuksen aikana esiin tulleetkin, ovat hyvin yleisiä.

Koko projektin ydin, käyttöoikeudet, on kaikessa arkisuudessaan merkittävä tekijä minkä tahansa järjestelmän tai organisaation tietoturvassa. Tietoturvan kivijalkana pidetyn CIA-kolmion kaikkiin kolmeen osatekijään, tiedon ja tietoteknisten resurssien saatavuuteen, eheyteen ja luottamuksellisuuteen, voidaan vaikuttaa käyttöoikeuksien asianmukaisella hallinnalla. Esimerkiksi haittaohjelmat pääosin toimivat niillä oikeuksilla, jotka parhaillaan kirjautuneen käyttäjän tunnuksella on, eli tarpeeksi matalat oikeudet voivat torjua haittaohjelmatartunnan alkuunsa ja liian suuret oikeudet taas mahdollistavat suurenkin tuhon tekemisen.

Huolellisista valmisteluista huolimatta projektissa törmättiin lukuisiin ongelmiin, joista vain muutamat olisivat todellisuudessa olleet väistämättömiä. Projektin tärkeimmät opit liittyvät ajanhallintaan, resurssien käyttöön ja tiedottamiseen.

Projektille oli todellisuudessa varattu varsin pitkä aika, mutta ajan täyden hyödyntämisen sijaan toteutus tehtiin viime hetkellä. Parempi ajankäyttö olisi mahdollistanut huolellisemmat esityöt ja kannustanut projektin ulkopuolisten resurssien laajempaan käyttöön. Resurssien laajempi käyttö ja tehtävien delegointi olisi ehkäissyt monia teknisiä ongelmia. Organisaatiossa on laajaa teknistä osaamista, joka osin painottuu nimenomaan niihin järjestelmiin, joita tässä projektissa muutettiin. Tekniset osaajat olisivat pystyneet ennakoimaan ongelmia, ja korjaamaan niitä nopeammin.

Osin projektin alun muutosvastarinnan takia toteutusvaiheen tiedottaminen jätettiin varsin niukaksi. Toteutuksen lähestyessä muutoksen kohderyhmältä olisi kuitenkin saatettu saada arvokasta tietoa odotettavissa olevista ongelmista. Välittömästi muutosta seuranneen vianselvityssuman kiireen tuntua, sekavia vikailmoituksia ja yleistä harmitusta olisi myös voitu huomattavasti lieventää paremmalla etukäteistiedotuksella.

Itse projektissa opittujen asioiden lisäksi myös insinöörintyöraportin kirjoitusprosessi on tuonut lisäoppia. Jotkin projektin osat ovat selkiytyneet, kun ne on täytynyt pukea sanoiksi ulkopuolisen ymmärrettävään muotoon, ja samalla myös projektissa tehdyt virheet ovat kirkastuneet. Jopa itse kirjoitustyö on opettanut projektia vaivannutta ajanhallintaa. Työn kirjoittaminen onkin saanut miettimään, pitäisikö pienistäkin projekteista tehdä vaikka vain omaan käyttöön jonkinlainen raportti tai niin sanottu debriefing kaiken hyödyn irti saamiseksi.

Ennen insinöörityön kirjoittamista pidin sitä oikealle työelämälle vieraana, historiallisena jäämänä muuten niin käytännönläheisessä ammattikorkeakouluopetuksessa. Kirjoitustyön varrella sen merkitys valmistuvalle insinöörille on kuitenkin käynyt selväksi, kun jopa työelämässä jo kohtuullisen ajan viettänyt opiskelija saa siitä näin paljon irti.

## Lähteet


1 Mitä on huoltovarmuus? 2017. Verkkodokumentti. Huoltovarmuuskeskus. <https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/mita-on-huoltovarmuus/> Luettu 11.3.2017.

2 Tavoitteet. 2017. Verkkodokumentti. Huoltovarmuuskeskus. <https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/tavoitteet/> Luettu 11.3.2017.

3 Laitinen, Jaana & Vainio, Suvi. 2009. Pitkä sähkökatko ja yhteiskunnan elintärkeiden toimintojen turvaaminen. Helsinki: Puolustusministeriö.

4 Uhkakuvat. 2017. Verkkodokumentti. Huoltovarmuuskeskus. <https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/uhkakuvat/> Luettu 11.3.2017.

5 Huoltovarmuuskriittisille toimijoille. 2014. Verkkodokumentti. Viestintävirasto. <https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/hvk-toimijoille.html>

6 Ala-Tala, Antti, Havaste, Annika, Heimbürger, Harri, Helenius, Marko, Henttu, Markku, Hänninen, Pasi, Kajava, Jorma, Koponen, Pekka, Kyrölä, Tuija, Riipinen, Terho, Savola, Reijo, Seppälä, Jari, Sundquist, Matti, Taskinen, Veli, Tuovinen, Esa & Tyynelä, Markku. 2010. Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. Helsinki: Suomen Automaatioseura ry.

7 Virtanen, Jori. 2016. Verkkodokumentti. Kylmentyneineitä kerrostaloja paljastui lisää – hakkerit iskevät lämmitykseen. <http://www.tivi.fi/Kaikki_uutiset/kylmentyneineita-kerrostaloja-paljastui-lisaa-hakkerit-iskevat-lammitykseen-6598148> Luettu 4.4.2017.

8 ISO/IEC 27001. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. 2010. Helsinki: Suomen Standardoimisliitto SFS.

9 Active Directory Replication. 2017. Verkkodokumentti. Microsoft. <https://technet.microsoft.com/en-us/library/cc961788.aspx> Luettu 6.4.2017.

10 Erityislainsäädäntö. 2017. Verkkodokumentti. Huoltovarmuuskeskus. <https://www.huoltovarmuuskeskus.fi/toimialat/energiahuolto/erityislainsaadanto/> Luettu 11.3. 2017.

11 Sähköverkkojen rakenne. 2017. Verkkodokumentti. Energiateollisuus ry. <http://energia.fi/perustietoa_energia-alasta/energiaverkot/sahkoverkot> Luettu 12.3.2017.

12 Yleistietoa häiriöistä. 2016. Verkkodokumentti. Energiateollisuus ry. <http://energia.fi/perustietoa_energia-alasta/energiaverkot/sahkokatkot> Luettu 12.3.2017.

13 Sähkön luotettavuus Helsingissä maailman huippuluokkaa. 2016. Verkkodokumentti. Helen Sähköverkko Oy. <https://www.helensahkoverkko.fi/uutiset/2016/sahkon-luotettavuus/> Luettu 12.3.2017.

14 New cyber resilience report: energy sector prime target for cyber-attacks. 2016. Verkkodokumentti. World Energy Council. <https://www.worldenergy.org/news-and-media/press-releases/new-cyber-report-energy-sector-prime-target-for-cyber-attacks/> Luettu 12.3.2017.

15 Hackers behind Ukraine power cuts, says US report. 2016. Verkkodokumentti. BBC. <http://www.bbc.com/news/technology-35667989> Luettu 12.3.2017.

16 Ukraine power cut 'was cyber-attack'. 2017. Verkkodokumentti. BBC. <http://www.bbc.com/news/technology-38573074> Luettu 12.3.2017.

17 Etäluenta. 2017. Verkkodokumentti. Helen Sähköverkko Oy. <https://www.helensahkoverkko.fi/palvelut/etaluenta/> Luettu 13.3.2017.

18 Scott, Mike. 2016. Smart grid is set to get a lot smarter. Verkkodokumentti. <https://www.raconteur.net/sustainability/smart-grid-is-set-to-get-a-lot-smarter> Luettu 13.3.2017.

19 The Potential Benefits of Distributed Generation and the Rate-Related Issues That May Impede Its Expansion. 2007. Verkkodokumentti. United States Department of Energy. <https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/1817_Report_-final.pdf> Luettu 13.3.2017.

20 Active Directory Tutorial. 2007. Verkkodokumentti. Techtarget.com. <http://searchwindowsserver.techtarget.com/tutorial/Active-Directory-Tutorial> Luettu 18.3.2017.

21 What is Active Directory Domain Services and how does it work? 2012. Verkkodokumentti. Serverfault.com. <http://serverfault.com/questions/402580/what-is-active-directory-domain-services-and-how-does-it-work> Luettu 18.3.2017.

22 Tutorial Overview: ADSI with Visual Basic. 2017. Verkkodokumentti. Microsoft.com. <https://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx> Luettu 18.3.2017.

23 Mathers, Bill. 2017. Appendix C: Protected Accounts and Groups in Active Directory. Verkkodokumentti. <https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory> Luettu 23.3.2017 .

24 Price, Ed. 2014. AdminSDHolder, Protected Groups and Security Descriptor Propagator. Verkkodokumentti. <https://social.technet.microsoft.com/wiki/contents/articles/22331.adminsdholder-protected-groups-and-security-descriptor-propagator.aspx> Luettu 23.3.2017.

25 Active Directory Security Groups. 2014. Verkkodokumentti. Microsoft..com. <https://technet.microsoft.com/en-us/library/dn579255(v=ws.11).aspx#BKMK_DomainAdmins> Luettu 23.3.2017.

26 Harris, Shon. 2013. CISSP Exam Guide. Sixth Edition. McGraw-Hill Education.

27 CIA Triad: Confidentiality, Integrity, and Availability. 2017. Verkkodokumentti. Central Oregon Community College. <https://www.cocc.edu/its/infosec/concepts/cia-triad/> Luettu 24.4.2017.

28 EU:n tietosuojauudistus. 2017. Verkkodokumentti. Tietosuojavaltuutetun toimisto. <http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html> Luettu 26.3.2017.

29 Guerrero, Javier. 2010. Permissions and malware. Verkkodokumentti. <http://www.pandasecurity.com/mediacenter/security/permissions-and-malware/> Luettu 31.3.2017.

30 Allow non-administrators RDP Access to Domain Controller. 2015. Verkkodokumentti. Windows OS Hub. <http://woshub.com/allow-non-administrators-rdp-access-to-domain-controller/> Luettu 1.4.2017.

31 Adminstrator cannot log on to server via remote desktop after changing default domain policy. 2013. Verkkodokumentti. StackExchange. <http://serverfault.com/questions/491314/adminstrator-cannot-log-on-to-server-via-remote-desktop-after-changing-default-d> Luettu 1.4.2017.

32 Group Policy for Beginners. 2011. Verkkodokumentti. Microsoft. <https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx> Luettu 6.4.2017.

33 DHCP and DNS. 2017. Verkkodokumentti. Microsoft. <https://technet.microsoft.com/en-us/library/cc958921.aspx> Luettu 6.4.2017.

## Kyberhyökkäyksiä kriittistä infrastruktuuria vastaan

[New cyber resilience report: energy sector prime target for cyber-attacks. 2016: 14]