Teemu Karstila

Datakeskuksen standardinmukaisuus ja riskikartoitus

Opinnäytetyö
Tieto- ja viestintätekniikan koulutus

2018

Kaakkois-Suomen ammattikorkeakoulu

Tekijä/Tekijät	Tutkinto	Aika
Teemu Karstila	Insinööri (AMK)	Joulukuu 2018

Opinnäytetyön nimi	
Datakeskuksen standardinmukaisuus ja riskikartoitus	45 sivua 0 liitesivua

Toimeksiantaja

Kaakkois-Suomen ammattikorkeakoulu Oy

Ohjaaja

Martti Kettunen

Tiivistelmä

Tämän opinnäytetyön tärkein tavoite oli selvittää, miten Kaakkois-Suomen ammattikorkeakoulun Kotkan kampuksen CyberLab-datakeskus täyttää standardin TIA-942-B vaatimukset. ANSI/TIA-942-B on yleisesti käytetty tietoliikenneinfrastruktuurin standardi datakeskuksille. Tutkimuksella pyrittiin selvittämään CyberLab-datakeskuksen standardin määrittelemä luokitus sekä löytämään kehityskohteita datakeskuksen standardiluokittelun parantamiseksi. Toinen tavoite oli suorittaa CyberLab-datakeskukselle fyysisten riskienkartoitus.

Tutkimuksen alkuvaiheissa perehdyttiin CyberLab-datakeskuksen toimintaan, komponentteihin sekä datakeskuksen infrastruktuurin standardin eri luokitustasojen vaatimuksiin. Tutkimuksessa perehdyttiin myös datakeskuksen fyysiseen turvallisuuteen sekä datakeskusta uhkaaviin fyysisiin riskitekijöihin.

Tutkimuksen tuloksena päädyttiin siihen lopputulokseen, että telekommunikaation kategorian tasoluokituksen tasoluokitus on T2, sähköisten järjestelmien kategorian tasoluokituksen tasoluokitus on E1, arkkitehtuurin ja struktuurin kategorian tasoluokituksen tasoluokitus on A2, ja mekaanisten järjestelmien kategorian tasoluokituksen tasoluokitus on M1. Tasoluokittelussa arvosteluasteikko on yhdestä neljään, jossa yksi on alin tasoluokitus ja neljä on korkein tasoluokitus. Tasoluokitusten numeroiden etuliitteenä olevan ison kirjaimen tarkoitus on toimia lyhenteenä kuvastamaan mihin kategoriaan tasoluokituksen arvosana kuuluu. Tasoluokitusten neljä kategoriaa ovat telekommunikaatio, arkkitehtuuri ja struktuuri, sähköiset järjestelmät sekä mekaaniset järjestelmät. Struktuurit kuuluvat osaksi arkkitehtuurin kategoriaa.

Tutkimuksen lopputuloksien perusteella saatiin hyvä kuva CyberLab-datakeskuksen tilanteesta. Saatuja tuloksia ja parannusehdotuksia pystytään käyttämään hyväksi uuden Kotkan kampuksen rakentamisessa. Aikaisempaa vastaavanlaista datakeskuksen standardiluokittelua ei ole Kaakkois-Suomen ammattikorkeakoulun CyberLab-ympäristölle tehty ja tämän standardiluokittelun pohjalta pystytään jatkossa parantamaan CyberLab-datakeskuksen turvallisuutta sekä edistämään datakeskuksen toiminnallisuutta opetusympäristönä.

Asiasanat

riskikartoitus, standardiluokittelu, datakeskus, TIA

South-Eastern Finland University of Applied Sciences

Author (authors)	Degree	Time
Teemu Karstila	Bachelor of Engineering	December 2018

Thesis title

Compliance with data center standards and risk assessment

45 pages
0 pages of appendices

Commissioned by

South-Eastern Finland University of applied sciences

Supervisor

Martti Kettunen

Abstract

The most important objective of this thesis was to find out how the CyberLab data center of the Kotka campus at the South-Eastern Finland University of Applied Sciences meets the requirements of the TIA-942-B standard. ANSI / TIA-942-B is a commonly used telecommunication infrastructure standard for data centers. The aim of the study was to determine the rating of the CyberLab based on the data center standard and to discover points of development to improve the data center standard rating. Another objective was to conduct a physical risk assessment for the CyberLab data center.

The early stages of the study were oriented towards researching the CyberLab data center functions, the components and the requirements of the different classification levels of the data center infrastructure standard. The study also focused on the physical security of the data center and the physical risk factors threatening the data center.

As the result of the study, it was concluded that the rating for telecommunication is T2, the rating for the electrical systems is E1, the rating for the architecture and structure is A1, and the rating of the mechanical systems is M1. The rating scale is from one to four with one being the lowest level rating and four being the highest. The purpose of the capital letter in front of the rating is to depict the rating category to which the rating belongs to. The four rating categories are telecommunications, architecture and structure, electrical systems and mechanical systems. Structures are included in the architecture category.

The results of the study provided a good picture of the situation of the CyberLab data center had been obtained. The results and suggestions for improvements can be utilized in the construction of the new Kotka campus. There is no previous comparable data center standardization classification for the CyberLab environment of the South Eastern Finland University of Applied Sciences, and based on this standard classification, it will be possible to further improve the security of the CyberLab data center and to promote the data center functionality as a learning environment.

Keywords

risk assessment, standard rating, data center, TIA

SISÄLLYS

1 JOHDANTO 6

1.1 Opinnäytetyön tavoitteet 6

1.2 Tutkimusmenetelmän valinta 7

2 DATAKESKUKSET 8

3 FYYSINEN TURVALLISUUS 9

4 RISKIKARTOITUS 10

5 TIA-942-B-STANDARDI 11

5.1 TIA-942-standardin historia 12

5.2 TIA-942-standardin neljä kategoriaa 12

5.3 Datakeskuksen tasoluokittelun perusteet 13

5.3.1 Taso 1: Perustaso 13

5.3.2 Taso 2: Redundanttiset komponentit 14

5.3.3 Taso 3: Samanaikaisesti ylläpidettävä 14

5.3.4 Taso 4: Vikasietoinen 14

6 DATAKESKUKSEN KATEGORIOIDEN TASOLUOKITUKSIEN TULOKSET 15

6.1 Telekommunikaation tasoluokituksen tulokset 15

6.2 Arkkitehtuurin tasoluokituksen tulokset 17

6.3 Sähköisten järjestelmien tasoluokituksen tulokset 22

6.4 Mekaanisten järjestelmien tasoluokitusten tulokset 26

6.5 Tasoluokitusten tuloksien yhteenveto 29

7 TIA:LLE VAIHTOEHTOISET DATAKESKUSSTANDARDIT 30

8 CYBERLAB-DATAKESKUKSEN RISKIKARTOITUS 31

9 JOHTOPÄÄTÖKSET 40

LÄHTEET 42

KUVALUETTELO 45

LYHENNELUETTELO

AHJ	Authority having jurisdiction
ANSI	American National Standards Institute
ASHRAE	American Society of Heating, Refrigerating, and Air Conditioning Engineers
CCTV	Closed-circuit television
CPU	Central processing unit
FPS	Frames per second
IBC	International building code
ICT	Information and Communication Technology
IT	Information Technology
HVAC	Heating, ventilation and air conditioning
LFRS	Lateral Force Resistance Systems
NFPA	National Fire Protection Association
SDC	Seismic Design Category
TIA	Telecommunication Industry Association
UPS	Uninterruptible Power Supply

1 JOHDANTO

Kaakkois-Suomen ammattikorkeakoulun tieto- ja viestintätekniikan koulutuslinjan suuntautuminen on jatkuvasti painottunut enemmän kyberturvallisuuden suuntaan. Palvelimet sisältävät nykyään yritysten lähes kaiken kriittisen tiedon, sekä useat yritykset vaativat toimivan verkkoyhteyden yritystoiminnan pyörittämistä varten. Kyberhyökkäysten ollessa nykypäivää kyberturvallisuuden kehittäminen sekä siihen panostaminen on muuttunut elintärkeäksi kehityskohteeksi niin pienille kuin suurillekin yrityksille.

Opinnäytetyön standardin mukaisen tasoluokittelun ja riskikartoituksen kohteena on Kaakkois-Suomen ammattikorkeakoulun CyberLab-datakeskus. Tasoluokittelun standardiksi valittiin TIA-942-B-standardi. Opinnäytetyö tehdään opinnäytetyön toimeksiantajalle Kaakkois-Suomen ammattikorkeakoululle. CyberLab-datakeskuksen oppimisympäristössä on käytössä virtuaalilaboratorioympäristö, joka tarjoaa opiskelijoille mahdollisuuden harjoitella tietoverkkotekniikan laboratoriotöitä verkkoselaimen kautta miltä tahansa tietokoneelta sekä koska tahansa.

Aikaisempia samankaltaisia opinnäytetöitä on Mikko Lehtisen (Lehtinen 2014) opinnäytetyö Datakeskusten arkkitehtuuri ja suunnittelu, Joonas Rosenbladin (Rosenblad 2015) opinnäytetyö Kyberturvallisuuslaboratorion jäähdytysjärjestelmä, Tero Perälän (Perälä 2014) opinnäytetyö Datakeskuksen poikkeustilanneohje ja Hannu Laitisen (Laitinen 2016) opinnäytetyö Datakeskus. Lehtisen opinnäytetyö käsittelee CyberLab-datakeskuksen suunnittelua ja rakentamista. Joonas Rosenbladin opinnäytetyö käsittelee CyberLab-datakeskuksen jäähdytysjärjestelmän dokumentointia sekä kriittisten valvonta- ja hälytysyhteyksien toteuttamista. Tero Perälän opinnäytetyö käsittelee sähköjärjestelmiä ja niiden toimintaa sekä kuvailee datakeskuksen muita järjestelmiä. Hannu Laitisen opinnäytetyössä kirjoitettiin ohjekirja palvelinsalitekniikoista sekä luotiin rakennussuunnitelma Savonian-ammattikorkeakoulun datakeskusta varten.

1.1 Opinnäytetyön tavoitteet

Tämän opinnäytetyön tavoitteena on suorittaa CyberLab-datakeskuksen tasoluokittelu ANSI/TIA:n TIA-942-B-standardin tasoluokituksien mukaisesti, sekä

suorittaa CyberLab-datakeskuksen riskikartoitus. TIA:n dokumentti valittiin tasoluokittelun standardiksi, koska se on yleisin käytetty datakeskusten standardi. TIA-942.org sivuston mukaan (TIA-942.org) yli 78 % datakeskusten operaattoreista ja omistajista valitsee TIA-942-standardin datakeskuksen suunnittelua ja rakentamista varten. Datakeskuksen riskikartoituksen tarkoituksena on kartoittaa palvelimille potentiaaliset fyysiset uhat sekä selvittää mitä fyysisiä uhkia monitoroidaan jo valmiiksi.

Riskikartoitus perustuu työssä ainoastaan fyysisiin riskeihin, sillä kaikkien potentiaalisten riskien kartoittaminen olisi mahdotonta tämän työn puitteissa. Riskikartoitus on prosessi, jonka avulla tunnistetaan vaaroja, jotka voivat vaikuttaa kielteisesti organisaation kykyyn harjoittaa liiketoimintaa (Rouse 2017a). Riskikartoituksessa selvitetään, mitä olemassa olevia riskejä datakeskuksesta löytyy, miten kyseiset riskit voidaan estää tai miten riskien aiheuttamia laitevahinkoja voidaan lieventää. Riskikartoituksessa etsitään ja tutkitaan myös uusia fyysisiä riskejä, joita ei ole vielä tiedossa ja voivat olla uhkia datakeskuksen turvallisuudelle.

Tässä opinnäytetyössä tutkimusongelmia ovat:

- Mitkä ovat CyberLab-datakeskuksen TIA-942-B-standardin telekommunikaation, arkkitehtuurin ja struktuurin, sähköisten järjestelmien sekä mekaanisten järjestelmien kategorioiden standardin mukaiset tasoluokitukset tällä hetkellä?
- Kuinka datakeskuksen standardin mukaisten tasoluokitusten tuloksia voidaan parantaa?
- Mitä fyysisiä uhkia datakeskuksen riskikartoituksena ilmenee?

1.2 Tutkimusmenetelmän valinta

Tutkimuksessa sen alkuvaiheissa tutkijan on tehtävä päätöksiä menetelmien yhdistämisestä, joiden avulla aloitetaan tutkimuskysymysten ratkaiseminen (Kananen 2015a). Opinnäytetyöhön käytettäväksi tutkimusmenetelmäksi on valittu kehittämistutkimus. Kehittämistutkimus sisältää molempia kvalitatiivista ja kvantitatiivista tutkimusta tai pelkästään kvalitatiivista tutkimusta (Kananen 2017, 18).

Kehittämistutkimuksessa on kyse monimenetelmäisestä tutkimusotteesta tai tutkimusstrategiasta, missä tarpeiden mukaisesti kvantitatiiviset sekä kvalitatiiviset tutkimusmenetelmät yhdistyvät. Kehittämistutkimuksen tavoitteena on muutoksen aikaansaanti tuotteen, organisaation, menetelmän tai muun vastaavan kehityksen kautta. Kehittämistutkimus alkaa kehittämistyön määrittelemisellä sekä kehittämiskohteiden löytämisellä. Ongelmien määrittelyvaiheeseen on hyvä varata runsaasti aikaa, sillä tämä vaihe vaikuttaa oikeiden ongelmien ja sen syiden löytämiseen ja tätä myöten ongelmien tai niitä aiheuttavien syiden poistamisen onnistumiseen. Tutkimustyön tekeminen on pakollinen osa, jotta ongelma voitaisiin määritellä, löytää ja vaihtoehtoisia ratkaisumalleja voidaan tuottaa. Kehittämistutkimuksiin tehtävän tutkimuksen määrä voi vaihdella ongelman laajuuden sekä ongelmiin perustuvien olemassa olevien tietojen saatavuuden ja laajuuden perusteella (Kananen 2015b.)

2 DATAKESKUKSET

Datakeskusten tehtävänä on keskittää IT-laitteistot luotettavaan ja turvalliseen toimintaympäristöön (Lehtoniemi 2017). Datakeskukset sisältävät suuria määriä kallista elektroniikkaa sekä elintärkeitä tietoja. Datakeskusten fyysinen turvallisuus on yritysten yksi suurimmista huolenaiheista. Datakeskusten laitteiden valintaan, sekä laitehuoneiden suunnitteluun ja rakentamiseen suuret yritykset käyttävät usein paljon aikaa ja rahaa, sillä palvelinten sekä niiden sisältämien tietojen ja toimintojen menetys esimerkiksi tulipalon, vesivahingon tai sähkökatkoksen aikana saattaa vahingoittaa yrityksen liiketoimintaa pitkälläkin aikavälillä. Google on investoinut Haminan datakeskuksen rakentamiseen vuonna 2009 200 miljoonaa euroa sekä ilmoittanut myöhemmin vuonna 2012 150 miljoonan euron lisäinvestoinnista ja marraskuussa 2013 Google ilmoitti investoivansa 450 miljoona euroa Haminan datakeskukseen lisää tuoden investointien kokonaisrahamäärän 800 miljoonaan euroon (Google s.a.).

Datapalvelinten toimivuus on tärkeä osa monien nykyaikaisten yritysten liiketoiminnan jatkuvuuden kannalta nykypäivänä. Suuri osa yritysten mainostuksesta, myynnistä, sekä viestinnästä nykypäivänä tapahtuu sähköisesti tallentuen datakeskusten kovalevyille. Pelkästään hetkellinen yllättävä katkos datakeskuksen toimintaan voi aiheuttaa yritykselle elintärkeiden tietojen menetyk-

sen tai vahingoittaa yrityksen koko liiketoimintaa mittavasti. Ponemon-instituutin vuonan 2013 teettämässä tutkimuksessa todettiin, että yhden minuutin kestävä datakeskuksen alhaalla olo saattaa maksaa yrityksille jopa 7 900 dollaria, joka tekee noin 474 000 dollaria tunnissa (ITWatchDogs 2015.) Datakeskukset ovat verkon kriittisimpiä järjestelmiä ja ovat välttämättömiä verkkoyritysten päivittäisten toimintojen jatkuvuuden kannalta. Näin ollen datakeskusten turvallisuus ja luotettavuus, sekä niiden tiedostojen turvaaminen on verkkopalveluja tarjoavien yritysten ensisijainen tavoite.

3 FYYSINEN TURVALLISUUS

Tämä luku käsittelee datakeskuksien fyysistä turvallisuutta koskevia asioita. Datakeskuksien fyysisen turvallisuuden päämääräisimpänä tehtävänä on pitää henkilöt, joita ei haluta päästää datakeskukseen sisälle ulkona sekä identifioimaan kyseiset henkilöt mahdollisimman nopeasti, mikäli he pääsevät datakeskukseen sisälle (Barker 2012). Datakeskukset voivat kohdata niiden sijainnista riippuen monia erilaisia uhkia. Kaikista yleisimpiä uhkia ovat luonnonvoimat, sekä ihmisten aiheuttamat muuttujat. Kaakkois-Suomen ammattikorkeakoulun CyberLab-datakeskuksen suurimmat luonnonvoimien aiheuttamat riskitekijät ovat Suomen sään aiheuttamat korkeat lämpötilan muutokset, vesisateet sekä lumisateet. Muita pieniä riskitekijöitä fyysiselle turvallisuudelle luonnon puolesta ovat pieneläimet kuten linnut, oravat, rotat ja hiiret.

Tässä vaiheessa on hyvä muistaa, että datakeskusten palvelinten fyysiseen turvallisuuteen lasketaan mukaan palvelinten jäähdytysjärjestelmä. Datakeskusten jäähdytysyksiköt sijaitsevat yleensä datakeskuksen ulkopuolella jonkinlaisessa erillisessä rakennuksessa, ulkoseinän vieressä tai katolla. Pieneläimistä tunnetuimpia sähköverkkojen ja datakeskuksien tuholaisia ovat linnut, oravat, rotat ja hiiret. Lintujen aiheuttamat sähkökatkokset, sekä vahingot aiheutuvat yleensä pesimisestä, sähkölinjoihin tai muuntimiin törmäämisestä. Pienten tuhoeläinten kuten oravien, rottien ja hiirten aiheuttamat vahingot koostuvat useimmiten oikosuluista, jotka ovat aiheutuneet pureskelluista johdoista. Washington postin mukaan (2015) oravat olivat syypäitä 9 prosentista 21 prosenttiin kaikkiin suunnittelemattomiin sähkökatkoksiin vuosina 2013 ja 2014.

Ihmiset ovat kuitenkin kaikista suurin fyysinen uhka datakeskuksille. Ihmisten aiheuttamat vahingot ovat lähes aina tahallisia. Datakeskusten ulkomuodon ja palvelinhuoneen kerroksen tulisi olla huomiota herättämättömiä, jotta datakeskuksen ja palvelinhuoneen sijainnit saataisiin naamioitua piiloon ulkopuolisilta henkilöiltä. Palvelinhuoneeseen ei saa johtaa ikkunoita, sillä ne ovat helppoja murtautumisreittejä ja luovat ulkopuolisille näkyvyyden palvelinhuoneen sisälle. Datakeskuksen rajoitettuihin tiloihin ja varsinkin palvelinhuoneeseen pääsemisen valvomista auttamaan tulisi sisäänkäynnillä olla kaksiosainen sisäänkäyntimetodi, joka päästää ainoastaan yhden henkilön kerrallaan palvelinhuoneeseen sisälle estäen luvattoman sisäänpääsyn ulkopuolisilta henkilöiltä tai työntekijöiltä, joilla ei ole sisäänpääsyoikeuksia (Barker 2012.) Rakennuksen henkilöstö tulisi kouluttaa myös tunnistamaan rakennuksen työntekijät ja reagoimaan tuntemattomiin henkilöihin, mikäli niitä esiintyy työpaikan tiloilla ja varsinkin jos tilat ovat rajoitettuja. Henkilöstö tulisi myös kouluttaa olemaan avaamatta ovia muille ainoastaan sen takia, että he näyttävät kiireisiltä tai työntekijöiltä. Ketään ei tulisi päästää kulkemaan rajoitettuihin tiloihin ilman kulkulupien tarkistusta, jotta henkilöt, joilla ei ole kulkulupaa rajoitettuihin tiloihin eivät pääsisi sosiaalisella manipuloinnilla sisään.

Ovien saranoiden tulisi myös olla varsinkin palvelinhuoneessa huoneen sisäpuolella, jottei ovea pystytä avaamaan nostamalla saranoista tai hajottamalla saranat. Rakennuksen kerroksissa tulee myös olla valvontakameroita tallentamassa rakennuksessa tapahtuvaa toimintaa ja palvelinhuoneen ulkopuoli sekä sisäpuoli tulee olla kameravalvonnan alaisena siten suunniteltuna, että palvelinhuoneen ympäristössä olisi mahdollisimman vähän pimeitä kohtia, joihin kamerat eivät näkisi. Rakennuksen palo-ovissa tulisi myös olla hälyttimet, jotka lähtevät soimaan, mikäli niistä kuljetaan luvattomasti tai jätetään auki (Scalet 2015.)

4 RISKIKARTOITUS

Kyvyttömyys tehdä riskien arviointia ja hallitsemista voi olla erittäin haitallista jatkuvuuden ja tuotannon kannalta sekä tuottaa useita haittavaikutuksia. On suositeltavaa, että datakeskuksen suunnitteluvaiheessa otetaan riskien arviointi huomioon (Ledwell 2015.) Riskikartoituksessa tulee ottaa huomioon datakeskuksen sijainti. Datakeskuksen sijainnin rakennuspaikkaa valittaessa tulee

ottaa huomioon maantieteellisen sijaintiin liittyvät paikalliset riskit, jotta voidaan välttää ilmaston tai maantieteellisen sijainnin mukana tuomia vaaroja tai vähentää niiden vaikutusta datakeskukseen rakentamalla datakeskus kestämään kyseisiä vaaroja.

Riskikartoituksen suorittaminen edellyttää luonnonvoimien, kuten myrskyjen, maanjäristysten tai tulvien aiheuttamien haitallisten tapahtumisten todennäköisyyden ja ihmisten haitallisen toiminnan aiheuttamien tapahtumien huomioon ottamisen. Riskikartoituksessa tulee myös huomioida kuka tai mikä voi vahingoittua vaaratilanteen tapahtuessa (Rouse 2017a.) Riskikartoituksella voidaan tunnistaa haitallisia tapahtumia, jotka voivat vaurioittaa organisaation toimintaa sekä lieventämään niistä aiheutuvia vahinkoja (Rouse 2017b).

Riskikartoitusprosessin suorittaminen alkaa kartoitettavan kohteen riskien tunnistamisella. Kun riskit ja uhat on tunnistettu, tulisi selvittää kyseisten riskien ja uhkien tapahtumisen mahdollisuus sekä päätellä mihin ne saattavat vaikuttaa. Riskien ja niiden vaikutusten tunnistamisen jälkeen tulisi tehdä suunnitelma siitä, kuinka riskitekijöistä päästäisiin eroon tai minimoitua riskistä aiheutuvien vahinkojen määrä. Tulokset tulisi myös dokumentoida ja riskikartoitusta tulisi suorittaa säännöllisesti, koska mahdolliset vaarat riskit ja niistä johtuvat seuraukset voivat muuttua nopeasti (Rouse 2017a)

5 TIA-942-B-STANDARDI

Tämä kappale keskittyy TIA:n (2017) TIA-942-B-standardidokumentinmukaiseen tasoluokitteluun sekä sen sisältämään materiaaliin. ANSI on lyhenne sanoista American National Standards Institute ja TIA on lyhenne sanoista Telecommunications Industry Association. TIA on ANSI:n valtuuttama standardeja kehittävä organisaatio. TIA:n suunnittelukomiteat laativat standardeja sekä teknisiä asiakirjoja, jotka perustuvat ANSI:n olennaisten vaatimusten ohjeistuksiin (TIA.)

5.1 TIA-942-standardin historia

TIA:n datakeskus-standardin luontiin on ottanut osaa yli 60 televiestintäalan organisaatiota. Huhtikuussa 2005 TIA julkaisi TIA-942 datakeskuksien telekommunikaation standardit dokumentin, joka oli ensimmäinen standardi nimenomaisesti vastaamaan datakeskuksien infrastruktuurien standardivaatimuksia. Tässä standardissa oli vielä osana tasoluokittelujen vaatimuksina datakeskuksen palvelimien saatavuusprosentti, mikä on myöhempien standardiluokitusten vaatimuksista poistettu (TIA-942 2006.) Vuoden 2006 standardi dokumentti korvattiin vuonna 2012 TIA STANDARD Telecommunications Infrastructure Standard for Data Centers TIA-942-A-dokumentilla. TIA-942-A-dokumentin korvasi vuonna 2017 julkaistu TIA-942-B-dokumentti, joka on uusin dokumentaatio TIA:lta datakeskuksien standardien luokituksiin.

5.2 TIA-942-standardin neljä kategoriaa

TIA-942-B sisältää tasoluokitukset kokonaisvaltaisen datakeskus tasoluokittelun lisäksi tarkennetun tasoluokittelun sekä kriteerit neljälle eri kategorialle, joista kokonaisvaltainen tasoluokittelu koostuu. Tasoluokittelun neljä kategoriaa ovat telekommunikaatio, arkkitehtuuri ja struktuuri, sähköiset järjestelmät sekä mekaaniset järjestelmät. Kategorioiden sekä kokonaisvaltaisen tasoluokittelun tasot ovat yhdestä neljään, jossa yksi on alin tasoluokitus ja vähiten vaativa sekä neljä on korkein tasoluokitus ja sisältää korkeimmat vaatimukset. Näiden neljän kategorian pohjalta pystytään tarkasti luokitella datakeskuksen eri osa-alueiden toimivuutta ja turvallisuutta sekä paremmin rajoittamaan, mitkä asiat ovat datakeskuksen vahvuuksia ja heikkouksia, sekä kuinka korjata tai parantaa datakeskuksen toimintaa ja turvallisuutta. ANSI/TIA-942-B-kirjan sivuilla 75 - 87 on taulukoituna telekommunikaation, sähköisten järjestelmien, mekaanisten järjestelmien, arkkitehtuurin ja struktuurien kriteereiden vaatimukset eri tasoille.

Tasoluokituksissa jokaisella eri kategorialla on oma etuliite kirjain, joka kuvastaa mihinkä kategoriaan jonkin tietyn tasoluokituksen tulos kuuluu. Telekommunikaation kategoriassa tasoluokituksien eteen merkataan iso T-kirjain kuvastamaan, että tasoluokitus kuuluu telekommunikaation kategoriaan. Arkkitehtuurin ja struktuurin kategoriassa tasoluokitusten eteen merkataan iso A-

kirjain kuvastamaan, että tasoluokitus kuuluu arkkitehtuurin ja struktuurin kategoriaan. Vastaavasti sähköisten järjestelmien kategoriassa tasoluokitusten eteen merkataan iso E-kirjain kuvastamaan, että tasoluokitus kuuluu sähköisten järjestelmien kategoriaan ja mekaanisissa järjestelmissä tasoluokitusten eteen merkataan iso M-kirjain kuvastamaan, että tasoluokitus kuuluu mekaanisten järjestelmien kategoriaan. Esimerkkinä tasoluokittelun lopputuloksesta, jos datakeskuksen kategorioiden tasoluokitusten tulokset ovat T3, E2, A4 ja M3, datakeskuksen kokonaisvaltainen tasoluokitus on 2, koska tasoluokittelun kategorioiden alin tasoluokitus on 2.

5.3 Datakeskuksen tasoluokittelun perusteet

Tässä luvussa on selitettynä datakeskuksen kokonaisvaltaisen tasoluokittelun vaatimukset TIA-942-B-standardi dokumentin sivujen 66 - 67 mukaisesti. Datakeskuksen eri osa-alueiden luokitustasot voivat kuitenkin olla eri arvoisia eri datakeskuksissa. Tällaisissa tapauksissa, joissa datakeskuksen telekommunikaation, sähköisten järjestelmien, arkkitehtuurillisen infrastruktuurin ja mekaanisen infrastruktuurin tasoluokituksen loppuarvosanat ovat erilaiset, on parempi luokitella tulokset alue kohtaisesti, eikä luokitella datakeskukselle kokonaisarvosanaa yhden osa-alueen heikoimman arvosanan mukaan.

Vaikka datakeskuksen yleinen tasoluokitus perustuu sen heikoimpiin komponentteihin, voi olla lieventäviä olosuhteita suhteessa kyseisen laitoksen riski profiilissa, toiminnallisissa vaatimuksissa tai muissa tekijöissä, jotka oikeuttavat alempaan luokitukseen yhdellä tai useammalla osajärjestelmällä (TIA-942-B 2017).

5.3.1 Taso 1: Perustaso

Perustason datakeskuksien jakelupolut, sekä laitteet voivat olla kaikenlaisen aktiviteetin aikana alttiita häiriöille. Perustason datakeskuksilta ei vaadita redundanttisia komponentteja tai järjestelmiä, generaattoreita tai UPS-järjestelmiä ei vaadita. Perustason datakeskuksien laitteilla ja osilla ei tarvitse olla virranjaolle, jäähdytykselle ja tietoliikenteelle muuta kuin yksi jakelureitti olemassa sekä komponenttien, virranjakelureittien, lämmönjakelureittien tai tiedonjakelureittien ei tarvitse olla redundanttisia. Fyysisen turvallisuuden kontrollointimekanismit tällä tasolla ovat usein rajoitetut tai vähäiset. Tämän tason

datakeskuksilta ei vaadita sähkögeneraattoria, mutta mikäli sellainen löytyy, sen ei tarvitse olla redundanttinen ja sen tulisi pystyä vastaamaan UPS:n ja mekaanisten järjestelmien sähkönkulutusta.

5.3.2 Taso 2: Redundanttiset komponentit

Toisen tason datakeskus vaatimuksiin kuuluu, että mekaaniset järjestelmät sekä UPS-järjestelmät ovat kytkettyinä sähkögeneraattoriin, joka on valmiustilassa sähkökatkosten varalta. Sähkögeneraattorin ei tarvitse olla redundanttinen. Toisen tason datakeskukset voivat kuitenkin olla alttiita toimintahäiriöille suunniteltujen tai suunnittelemattomien aktiviteettien aikana. Toisen tason datakeskuksen tulisi pystyä käsittelemään suunniteltuja huoltotoimenpiteitä sekä yksittäiseen komponenttiin ilmestyviä laitevikoja. Toisen tason datakeskuksilta ei vaadita kriittisten tilojen osastointia. Toisen tason datakeskuksissa tulisi olla perus tason fyysisen turvallisuuden kontrollointi. Tällä tasolla datakeskuksella on yleensä käytössä ainoastaan yksittäisiä jakelureittejä sähkölle, jäähdytykselle ja tiedonsiirtoreiteille. Laitteiden ja komponenttien tulisi olla redundanttisia sekä ennaltaehkäisevää huoltoa tulisi suorittaa valmistajan ohjeiden mukaisesti.

5.3.3 Taso 3: Samanaikaisesti ylläpidettävä

Kolmannen tason datakeskuksien tulee pystyä käsittelemään jakelupolkuihin, laitteisiin tai komponentteihin kohdistuvaa suunniteltua laitehuoltoa siten, ettei laitehuolto aiheuta datakeskuksen toimintaan katkoksia. Kolmannen tason datakeskuksissa sähköisten, mekaanisten ja tietoliikenteen kriittisten tilojen lokerointi ei ole pakollista, mutta suositeltavaa ja datakeskuksissa tulisi olla parannettu fyysisen turvallisuuden kontrollointi. Kolmannen tason datakeskusten virranlähteiden, jäähdytysmekanismien ja tietoliikenteiden tulee täyttää vähintään yhden aktiivisen polun (N) ja yhden varalla olevan polun redundanttisuuden (+1).

5.3.4 Taso 4: Vikasietoinen

Neljännen tason datakeskuksen tulee pystyä käsittelemään yhtä tiedonjakelureitin, laitteen tai komponentin viallisuutta koska tahansa siten, ettei vika ja sen korjaaminen aiheuta datakeskuksen toimintaan häiriöitä. Neljännen tason

datakeskuksissa sähköisten, mekaanisten ja tietoliikenteen kriittisten tilojen tulee olla lokeroituina toisistaan erilleen sekä fyysisen turvallisuuden kontrollointi tulee olla vahva. Virranjakelun, jäähdytyksen ja tietoliikenteen minimi redundanttisuus vaatii vähintään kaksi aktiivista polkua (2N /N+N)

6 DATAKESKUKSEN KATEGORIOIDEN TASOLUOKITUKSIEN TULOKSET

Tässä luvussa käsitellään TIA-942-B-dokumentin sivujen 66 - 87 tasoluokitusten vaatimusten vastaavuutta CyberLab-datakeskukseen. Tässä luvussa esitetyissä taulukoissa on kirjattuna kategorioiden arviointikohteet sekä CyberLab-datakeskuksen saama tasoluokitus ja sen kuvaus. Tasoluokitus vastaa arviointikohteen vaatimuksia sekä kuvastaa CyberLab-datakeskuksen tämän hetkistä tilannetta ja annetun tasoluokituksen vaatimusta vastaava kuvaus on dokumentin taulukon mukainen.

Tasoluokittelun arvoasteikko on yhdestä neljään, jossa yksi on alin tasoluokitus ja neljä on korkein tasoluokitus. Mitä korkeammalle tasoluokitukselle halutaan, sitä vaativammat on kriteerit. Telekommunikaatio, arkkitehtuuri ja struktuuri, sähköiset järjestelmät sekä mekaaniset järjestelmät ovat omissa taulukoissansa. Arkkitehtuurin, sähköisten järjestelmien ja mekaanisten järjestelmien taulukot ovat suuria sekä jatkuvat useammalle sivulle. Struktuurin vaatimukset ovat omassa taulukossansa erillään arkkitehtuurin vaatimuksista, jotta struktuurilliset vaatimukset olisivat paremmin huomioitavissa eivätkä sekoittuisi yhteen arkkitehtuurillisten vaatimusten sekaan. Struktuurin tasoluokittelujen vaatimukset kuuluvat arkkitehtuurin kanssa kuitenkin samaan kategoriaan.

6.1 Telekommunikaation tasoluokituksen tulokset

Alla olevassa taulukossa on listattuna TIA-942-B-dokumentin sivun 75 taulukon kaikki telekommunikaation kategorian arvostelukohteet, jotka ovat listattuna taulukon vasempaan reunaan. Taulukossa rating-sarakkeessa on tämän tutkimuksen arvio kustakin arvostelukohteesta. Taulukon oikeanpuolimmaisessa sarakkeessa näkyy CyberLab-datakeskuksen saaman tasoluokituksen dokumentinmukainen selitys arvostelukohteen sen tasoluokituksen vaatimukselle.

Taulukko 1. Telekommunikaation luokittelun tulokset

CATEGORY: Telecommunications	Rating	Description of rating
General	T1-T4	
Cabling, racks, cabinets & pathways compliant with relevant TIA specifications	T4	Yes
Diversely routed access provider entrances and maintenance holes with minimum 20 m separation	T4	Yes
Redundant access provider services - multiple access providers, central offices, access provider right-of-ways	T2	Not required
Redundant entrance room	T4	Yes
Redundant main distribution area	T3	Not required
Redundant intermediate distribution area (if present)	T3	Not required
Redundant backbone cabling and pathways	T4	Yes
Redundant horizontal cabling and pathways	T3	Not required
Routers and switches have redundant power supplies, processors	T4	Yes
Redudant routers and switches with redundant uplinks	T4	Yes
Patch panels, outlets, and cabling to be labeled per ANSI/TIA-606-C	----	-----
Patch cords and jumpers to be labeled on both ends with the name of the connection at both ends of the cable	T1	Not required
Patch panel and patch cable documentation compliant with ANSI/TIA-606-C	-----	-------

Telekommunikaation taulukon arviointikriteereiden tasoluokittelussa korkean tasolukituksen saavuttaminen vaatii, että näihin onko vai eikö ole -kysymyksiin pystytään vastaamaan että, on. Mikäli tasoluokittelun kriteereissä ei pystytty vastaamaan, että on, joudutaan tiputtamaan tasoluokittelun arvio, kunnes tasoluokitus tietylle kriteerille vastaa sillä kriteerillä ei pakollista arvoa. Taulukosta voidaan huomata heti ensimmäisenä, että ANSI/TIA-606-C-dokumenttiin perustuvat kriteerit on jätetty luokittelematta.

Näitä kahta kriteeriä ei voitu käsitellä, sillä se oli vaatinut toisen kalliin standardi-dokumentinostamisen, mikä ei tässä kyseisessä vaiheessa ollut mahdollista. Koska osa-alueille annetaan tasoluokitus arviointikriteereiden pienimmän tasoluokituksen mukaan, joudumme suoran arvioinnin perusteella antamaan telekommunikaatiolle arvosanan T1.

Ainoassa T1-luokituksen saaneessa kriteerissä vaadittiin, että kaapeleiden molemmissa päissä olisi kytkentämerkinnät. Kaapeleihin kytkentöjen merkitse-

minen on pitkä ja aikaa vievä prosessi, mutta tämän kyseisen kriteerin tasoluokitus nousisi T1:stä T4:ään, mikäli tämä prosessi saataisiin suoritettua. Näiden kahden arvon korjauksen jälkeen telekommunikaation kokonaistasoluokitus nousisi T2:een. T2:sta tason nostaminen T3:een vaatisi, että verkonpalvelun tarjoajia olisi kaksi tai enemmän.

6.2 Arkkitehtuurin tasoluokituksen tulokset

Alla olevissa taulukoissa on listattuina TIA-942-B-dokumentin sivujen 76 - 81 taulukoiden kaikki arkkitehtuurin ja struktuurin kategorioiden arvostelukohteet, jotka ovat listattuna taulukon vasempaan reunaan. Taulukossa rating-sarakkeessa on tämän tutkimuksen arvio kustakin arvostelukohteesta. Taulukoiden oikeanpuolimmaisessa sarakkeessa näkyy CyberLab-datakeskuksen saaman tasoluokituksen dokumentinmukainen selitys arvostelukohteen sen tasoluokituksen vaatimukselle.

Taulukko 2. Arkkitehtuurin luokittelun tulokset

CATEGORY	Rating	Description
ARCHITECTURAL	A1-A4	
Site Selection		
Proximinity to flood hazard area	A4	Greater than 91m from 100-year flood hazard area
Proximinity to coastal or navigable inland waterways	A4	Greater than 0.8km
Proximinity to major highway traffic arteries and main rail lines	A4	Greater than 0.8km
Proximinity from major airports	A4	Greater than 8km
Parking		
Separate visitor and employee parking ares	A2	not required
Separate from loading docks	A4	Yes (physically separated by fence or wall with separate entries)
Proximinity of visitor parking to data center perimeter building walls	A2	not required
Multi-tenant non-data center occupant within building	A2	Allowed if occupancies are non-hazardous

Fire resistive requirements		
Exterior bearing walls	A2	Code allowable
Interior bearing walls	A2	Code allowable
Exterior nonbearing walls	A2	Code allowable
Structural frame	A2	Code allowable
Interior non-computer partition walls	A2	Code allowable
Shat enclosures	A2	Code allowable
Floors and floor-ceilings	A2	Code allowable
Roofs and roof-ceilings	A2	Code allowable
Meet NFPA 75 or the data center fire protection standard applicable for the location	A4	Yes
Miscelaneous building components		
Vapor barriers for walls, floors, and ceiling of computer room	A4	Yes
Building entrances with security checkpoints	A2	Not required
Access floor panel construction (when provided)	A2	No requirement
Understructure (when access floor is provided)	A2	No requirement
Roofing		
Class	A4	Class A
Type	A3	Non-redundant with non-combustible deck
Roof Slope	A2	Minimum code reguirements
Doors and windows		
Fire rating	A2	Minimum code requirements
Windows on perimeter of the computer room	A2	Allowed with minimum Code required fire rating
Entry lobby		
Physically separate from other ares of data center	A4	Yes
Security counter	A2	Not required
Single person interlock, portal or other hardware designed to prevent piggybacking or pass back	A2	Not required
Fire separation from other areas of data center	A2	Minimum Code Requirements
Administrative offices		
Physically separate from other area of data center	A4	Yes
Fire separation from other areas of data center	A2	Minimum Code Requirements
Security offices		
Physically separate from other areas of data center	A4	Yes
Fire separation from other areas of data center	A2	Minimum Code Requirements
180 degree peepholes or CCTV on security equipmet and monitoring rooms	A4	Yes
Dedicated and hardened security equipment and monitoring rooms	A2	Yes

Operations Center		
Operations Center physically separate from other areas of data center	A4	Yes
Fire separation from other non-computer room areas of data center	A2	Not required
Restrooms and break room areas		
Proximinity to computer room and support areas	A3	If immediately adjacent, provided with leak prevention barrier
Fire separation from computer room and support areas	A2	Minimum Code requirements
UPS and Battery rooms		
Aisle widths for maintenance, repair or equipment removal	A4	Minimum Code requirements (not less than 1.2m clear)
Fire separation from computer room and other areas of data center	A2	Minimum Code requirements
Required exit corridors		
Fire separation from computer room and support areas	A2	Minimum Code requirements
Width	A4	Minimum Code requirements (not less than 1.2m clear)
Shipping and receiving areas		
Physically separate from other areas of data center	A4	Yes
fire separation	A2	Minimum Code requirements
Number of docks	A3	Minimum of one
Generator and fuel storage areas		
Proximinity to computer and support areas	A2	No requirement
Proximinity to publicly accessible areas	A2	No requirement
Security		
System CPU UPS capacity	A1	No requirement
Data Gathering Panels UPS capacity (Field panels)	A1	No requirement
Field Device UPS Capacity	A1	No requirement
Physical Security Staffing	A2	During Scheduled operation (typically 5 days a week during normal business hours)
Security Access Control/Monitoring at:		
Perimeter and restricted areas	A4	Card access or biometric with intrusion detection with door/window open alarm
Main door onto computer room floor	A3	Card access or biometric with intrusion detection with door open alarm
Bullet resistant walls, windows & doors		
Security Counter in Lobby	A2	No requirement
CCTV Monitoring		
Restricted areas and perimeter	A4	Yes
Access Controlled Doors	A4	Yes
CCTV		
CCTV Recording of all activity on all cameras	A4	Yes; digital
Recording rate (FPS)	A4	20 frames/sec (min)
Building construction		
Type of construction (IBC 2015) or equivalent locally adopted building code	A2	No restrictions

Taulukko 3. Struktuurien luokittelun tulokset

CATEGORY	Rating	Description
STRUCTURAL	A1-A4	
Facility design to International Building Code (IBC) Seismic Design Category (SDC) requirements	A4	Per local country standards for the building location (at minimum) or IBC SDC-C requirements or higher for building location (if they exceed local requirements)
Site Specific Response Spectra - Degree of local Seismic Accelerations	A4	With operation status after 5% 100-year event
Importance Factor - Assists to ensure greater than code design	A4	1.5
Telecommunications equipment racks/cabinets anchored to base or supported at top and base or equipped with seismic platforms or other protective measures	A1	No requirement
Deflection limitation on telecommunications equipment within limits acceptable by electrical attachments	A4	Yes
Bracing of electrical conduits runs and cable trays	A4	Per code with importance
Bracing of mechanical system major duct runs	A4	Per code with importance
Floor loading capacity superimposed live loads	---	---
Floor hanging capacity of ancillary loads suspended from below	---	---
Concrete Slab Thickness at ground	---	---
Minimum concrete topping over flutes for equipment anchorage when concrete filled metal deck structure used for elevated floors	---	---
Building LFRS indicate displacement of structure	---	---
Building Energy Dissipation - Passive Dampers/Base Isolation	A2	Minimum code requirements
Construction of Floors above ground level.	---	---

A1-tasoluokituksen saaneita kriteereitä oli neljä kappaletta sekä kuusi kokonaan luokittelematta jätettyä kohtaa. Useissa arkkitehtuurin ja struktuurien tasoluokituksien arviointikriteereissä ja kriteerien tasojen luokitusten vaatimuksissa ongelmana oli kriteerien tai luokitusten vaatimuksien selkeys tai kriteeriin saatavilla olevien tiedonlähteiden vajaus. Tarkemmin tarkasteltuna A1-tasoluokituksen saaneita kohteita olivat turvajärjestelmien prosessoreiden UPS-kapasiteetti, datan keräys paneeleiden UPS-kapasiteetti, kenttälaitteiden UPS-kapasiteetti ja laitekaappien/kabinettien suojaus maanjäristyksiltä.

Luokittelematta jääneet kohteet olivat lattian päällekkäisten kuormien kestävyyden kapasiteetti, lattiaan sen alapuolelta kohdistuvien ripustuskuormien kestävyyden kapasiteetti, rakennuksen betonilaatan paksuus, vähimmäisbetonipäällystys, kun betonilla täytettyjä metallikantorakenteita käytetään korotetuissa lattioissa, rakennuksen rakenteiden rungon sivuttaisvoiman vastusjärjestelmä eli LFRS ja maanpinnan yläpuoleisten kerroksien lattiatasojen rakennustapa.

Tässä kappaleessa käsitellään A1-tasoluokituksen saaneita arviointi kohteita, jotka olivat turvajärjestelmien prosessoreiden UPS-kapasiteetti, datankeräyspaneeleiden UPS-kapasiteetti, kenttälaitteiden UPS-kapasiteetti ja laitekaappien/kabinettien suojaus maanjäristyksiltä. Rakennuksen turvajärjestelmien UPS-kapasiteeteissä vaatimuksena on A2-tasolla, että rakennuksen oma UPS-järjestelmä toimisi turvajärjestelmien varavirtalähteenä tai rakennuksen oman UPS-järjestelmän sijaan turvajärjestelmillä olisi oma neljä tuntia kestävä paikallinen akusto, josta ne saisivat toimiakseen virtaa. A3-tasolla vaadittaisiin rakennuksen omaa UPS-järjestelmää toimimassa varavirtalähteenä tai kahdeksan tuntia kestävää paikallinen akusto ja A4-tasolla turvajärjestelmien prosessoreiden UPS-kapasiteetissä vaaditaan rakennuksen UPS:ää tai kahdeksan tuntia kestävää paikallista akustoa toimimaan varavirtalähteenä ja datan keräys paneeleissa sekä kenttälaitteissa vaaditaan rakennuksen UPS:ää tai 24 tuntia kestävää paikallista patteristoa toimimaan varavirtalähteinä. Koko rakennuksen varavirtalähteenä toimivaa UPS-järjestelmää tai vastaavia patteristoja ei ole, mikä on syy näissä kohdissa A1-tasoluokitukselle. Laitekaappien/kabinettien oleminen suojattuna maanjäristyksiltä on vaatimus luokittelutasoilla A2 - A4, mutta koska laitekaappeja/kabinetteja ei ole suojattu maanjäristyksiltä joudutaan antamaan tässä kohtaa tasoluokitus A1.

Tässä kappaleessa käsittelemme luokittelemattomia arviointikohteita, jotka olivat lattian päällekkäisten kuormien kestävyys, lattiaan sen alapuolelta kohdistuvien ripustuskuormien kestävyys, rakennuksen betonilaatan paksuus maantasolla, betonilla täytettyjen metallikantorakenteiden korotettujen lattioiden betonipäällystyksen minimipaksuus, rakennuksen LFRS ja maanpinnan yläpuoleisten kerroksien lattioiden rakennustapa. Luokittelemattomissa arviointikohdissa lattian päällekkäisten kuormien kestävyyden kapasiteetin tulee olla vähintään luokitustasolla A1 7.2 kPa, luokitustasolla A2 8.4 kPa ja luokitustasoilla A3 sekä A4 12 kPa. Lattiaan sen alapuolelta kohdistuvien ripustuskuormien kestävyyden kapasiteetin tulee olla vähintään tasoilla A1 ja A2 1.2 kPa sekä tasoilla A3 ja A4 2.4 kPa. Rakennuksen betonilaatan ainoana vaatimuksena kaikilla luokittelutasoilla on, että betonilaatan paksuus on 127 millimetriä. Betonilla täytettyjen metallikantorakenteiden korotettujen lattioiden betonipäällystyksen minimipaksuuden tulee olla vähintään 102 millimetriä tasoluokituksilla A1 ja A4.

Rakennuksen rakenteiden rungon sivuttaisvoiman vastusjärjestelmän eli LFRS:n luokittelutason vaatimuksina tasolla A1 on, että runko koostuu teräksestä tai betonista. Luokitustasoilla A2, A3 ja A4 luokituksen vaatimuksena on, että rakennuksen rakenteiden sivuttaisvoimaa vastustava runko on joko betoninen jäykistysseinä tai teräsrakenteinen runko. Maanpinnan yläpuoleisten kerroksien rakennustavassa tulee luokitustasolla A1 olla käytettynä esijännitettyä betonirakennelmaa, A2 luokitustasolla paikoilleen valettua betonirakennelmaa ja tasoilla A3 sekä A4 teräskantista betonilla täytettyä rakennelmaa. Nämä arviointi kriteerit jäivät ilman luokituksia, koska niiden mittaustuloksia ja rakennustietoja ei ollut saatavilla, mutta mitä suurimmalla todennäköisyydellä vastaavat tasoluokituksia A3 ja A4.

Näistä syistä useassa kohdassa arviointi voi olla alempi, kuin mitä se todellisuudessa olisi. Hyvä esimerkki arviointiin kohdistuneista ongelmakohdista olisi kaikki kestävyyteen perustuvat vaatimukset kuten rakennuksen tulen kestävyyden, lattian päällekkäisten kuormien sekä ripustuskuormien kestävyyskapasiteetin tiedot, joita ei ollut tutkimuksen aikana saatavilla. Vaikka tämän arvioinnin perusteella arkkitehtuurille ja struktuurille tulisi pienimmän arvosanan mukaan antaa tasoluokitus A1, saattaa se todellisuudessa olla A2 tai jopa A3, kun otamme huomioon CyberLab-datakeskuksen koon, sijainnin rakennuksessa sekä maailmankartalla.

Sijainnin takia CyberLab-datakeskus on turvassa tulvilta, pyörremyrskyiltä ja maanjäristyksiltä eliminoiden tarpeet erillisesti suojautua näiltä uhilta. Tämän takia CyberLab-datakeskusta ei ole rakennettu olemaan suojattuna kyseisiltä luonnonuhilta. CyberLab-datakeskuksen tarkoitus on suurelta osin toimia opetusympäristönä, eikä silloin sisällä niin kriittisiä laitteistoja, jotka vaatisivat koko kampuksen kattavaa varavirtaverkostoa, toisin kuin suuremmat datakeskus kompleksit tai sairaalat.

6.3 Sähköisten järjestelmien tasoluokituksen tulokset

Alla olevassa taulukossa on listattuna TIA-942-B-dokumentin sivujen 82 - 85 taulukoiden kaikki sähköisten järjestelmien kategorian arvostelukohteet, jotka ovat listattuna taulukon vasempaan reunaan. Taulukossa rating-sarakkeessa

on tämän tutkimuksen arvio kustakin arvostelukohteesta. Taulukon oikeanpuolimmaisessa sarakkeessa näkyy CyberLab-datakeskuksen saaman tasoluokituksen dokumentinmukainen selitys arvostelukohteen sen tasoluokituksen vaatimukselle.

Taulukko 4. Sähköisten järjestelmien luokittelun tulokset

CATEGORY	Rating	Description
Electrical	E1-E4	
General		
System allows concurrent maintenance	E2	Not required but preferred for critical parts of infrastructure
Fault Tolerant	E3	Not required
Power System Analysis	E2	Up-to-date short circuit study, coordination study, and arc flash analysis
Computer & Telecommunications Equipment Power Cords	E4	Redudant Cord Feed with 100% capacity on remaining cord or cords
Utility		
Utility Entrance	E3	Minimum 1 active, I standby. Same substation allowed. Self-generation allowed
Main Utility Switchboard		
Service	---	---
Construction	---	---
Surge Suppression	E2	Not required
Uninterruptible Power Supply System		
Redundancy	E2	N+1 equipment level, single path
Topology	E1	Single or parallel modules
Automatic Bypass	E2	Yes, with non-dedicated feeder to automatic bypass
Maintenance Bypass Arrangement	E2	Non dedicated maintenance bypass feeder to UPS output switchboard
Battery String	E1	Single or common string for multiple modules
Battery type	E4	5 or 10-year design life batteries or flywheel
Battery minimum back up time with design load at end of battery life	E4	10 minutes or flywheel capacity
Battery Monitoring System	E3	String level by IPS System
Power Distribution Unit		
Transformer	E2	Standard high efficiency

Automatic Static Transfer Switch		
Dedicated over-current protection device on input of static bypass	E2	Not required
Maintenance Bypass	E2	Not required
Grounding and bonding		
Lightning protection system	E2	Based on risk analyssi as per NFPA 780 and insurance requirements
Lighting fixtures neutral isolated from service entrance derived from lightning transformer for ground fault isolation	E2	Not required
Data center bonding and grounding infrastructure in computer room (as required by ANSI/TIA-607-C)	----	----
Computer Room Emergency Power Off (EPO) System		
Installation	E4	If required by AHJ, type as required with cover guard and warning label
Test Mode	E4	Yes
Alarm	E4	Yes
Disable/enable switch	E4	As allowed by local codes
Central Power Monitoring		
Monitored Points	E2	Utility, UPS, Generator
Notification Method	E4	Control Room Console, Pager, Email, and/or text message to multiple facility personnel
Battery Room		
Separate from UPS Equipment Rooms	E2	Not required
Individual Battery Strings Isolated from Each Other	E2	Not required
Shatterproof Viewing Glass in Battery Room Door or CCTV	E4	Yes
Standby Generating System		
Generator Sizing	E1	If installed, sized for UPS & mechanical systems without redundancy
Generators on Sible Bus	---	---
Load Bank		
Installation	E1	No requirement
Equipment Tested	E4	Generator, UPS
Auto Shutdown	E2	Not required
Testing		
Factory Acceptance Testing	E3	UPS and generator Systems
Site circuit breaker testing	E4	As per local code with minimum of contact resistance test of all critical circuit breakers at primary distribution of the electrical system
Commissioning	E3	Component level and System level
Equipment Maintenance		
Operation and Maintenance Staff	E2	Onsite Day Shift only. On-call at other times
Preventative Maintenance	E4	Comprehensive preventative maintenance program
Facility Training Programs	E1	No requirement

Sähköisten järjestelmien luokittelussa arvioinnin kohdat, joista ei tullut E1-luokittelua korkeampaa tasoluokitusta oli viisi kappaletta, sekä neljä kohtaa, joille ei voitu antaa tasoluokitusta. E1-luokituksen saaneita olivat UPS:n topologia, akusto, generaattori, keinokuormaajan asennus ja henkilökunnan koulutusohjelma. UPS:n topologiassa luokitustason E2 vaatimuksena oli UPS:n moduulien oleminen rinnakkaisia moduuleita yksittäisten sijaan ja tasoilla E3 - E4 joko hajautettu redundanttinen moduuli järjestelmä tai lohkotettu redundanttinen järjestelmä.

Akkujen jono eli akkupankki saadaan aikaan kytkemällä useita akkuja tai akkukennoja sarjaan vaadittavan käyttökelpoisen jännitteen aikaansaamiseksi. Akusto voi koostua yhdestä tai useammasta rinnakkaisesta akkupankista. (Amtex s.a.). Akkujonojen tulisi toimia tasoluokituksella E2 yksittäisenjonon tai yleisenjonon lisäksi modulaarisena UPS:nä tai irrallisilla moduuleilla tulisi olla oma irralliselle moduulille omistautunut akusto. Tasoluokituksilla E3 - E4 jokaisella moduulilla tulisi olla oma sille moduulille omistautunut akkupankki. Generaattoria ei ole CyberLab-datakeskuksen toimintaan liitettynä ollenkaan, jolloin generaattorin koon kohdassa sille tulee arvosana E1, mutta mikäli CyberLab-datakeskuksen UPS:ää ja mekaanisia järjestelmiä vastaamaan hankittaisiin oikean kokoinen generaattori sen luokitustaso nousisi tasolle E2, ja kehittämällä generaattoreiden redundanttisuutta voitaisiin nostaa luokittelun arvosana tasolle E3, kun redundanttisuus on N+1 ja tasolle E4, kun redundanttisuus on 2N.

Keinokuormatestaus on CyberLab-datakeskuksessa tehty siirrettävillä laitteilla kerran UPS-laitteille, mutta ei generaattoreille, sillä CyberLab-datakeskuksen varavirtalaitteistoon ei kuulu tällä hetkellä generaattoreita. Tästä syystä keinokuormauksen kohdalla testattujen laitteistojen kohdalla on voitu antaa luokitustaso E4, mutta mikäli CyberLab-datakeskukselle hankitaan generaattori varavirtalähteeksi, sille tulee suorittaa keinokuormaustestaukset, muuten luokitustaso joudutaan laskemaan E1:een. Asennetun keinokuormatestauksen luokittelutasoksi on jouduttu asettamaan E1, vaikka CyberLab-datakeskuksen UPS-laitteet on kuorma testattu. Tämä johtuu siitä, että CyberLab-datakeskuksen käytössä ei ole keinokuormauslaitteita uusien tutkimusten tekemistä varten. Mikäli CyberLab-datakeskuksen käyttöön hankittaisiin siirrettävät tai asen-

nettaisiin pysyvät kuormauksen testauslaitteet, voitaisiin tasoluokittelun arvosanaa tässä kohdassa nostaa E3:een siirrettävien kuormantestauslaitteiden kohdalla ja E4:ään pysyvästi asennettujen kuormaustestauslaitteiden kohdalla.

Henkilökunnan datakeskuksen laitteiden käyttökoulutusohjelman poissaolo ei ole varteenotettava vaatimus tässä kyseisessä datakeskusympäristössä, jolloin tämän tasoluokittelukohdan voisi periaatteessa jättää huomioimatta, mutta mikäli tasoa halutaan nostaa E1:stä tasolle E2 tulee olla olemassa koulutusohjelma, joka sisältää rajoitetun koulutuksen laitevalmistajilta. E3 tasoluokitus vaatii koulutusohjelmaa, jonka perusteelta laitteiden normaali operointi onnistuisi. Tasolla E4 koulutusohjelman pohjalta laitteiden manuaalisen operoinnin tulisi myös onnistua hätätilanteissa.

Tasoluokittelemattomat kohteet olivat sähkökeskuksen palvelun tyyppisyys sekä rakenteellisuus, datakeskuksen maadoitusinfrastruktuuri ANSI/TIA-607-C:n mukaisesti ja generaattoreiden toimivuus yhdellä väylällä. Sähkökeskuksen palveluiden tyyppisyyden ja rakenteellisuuden tasojenluokitusten vaatimuksista ei käynyt tarpeeksi selväksi, mitä niissä tarkalleen haluttiin tai haettiin takaa, joka on syy siihen, miksi luokittelu puuttuu. Datakeskuksen maadoitusinfrastruktuurin ainut vaatimus jokaisella arvoasteikolla oli, että maadoitusinfrastruktuuri on ANSI/TIA-607-C-dokumentin mukainen, mutta kyseistä dokumenttia ei ole tällä hetkellä tähän opinnäytetyöhön saatavilla, joten maadoituksen tarkistaminen olemaan kyseisten vaatimusten mukainen ei ollut mahdollista. Generaattoreiden toimivuuden ainut vaatimus on, että ne ovat yhdellä sähkönjakeluyksiköllä toiminnassa, mutta koska generaattoreita ei ole ollenkaan niin taso on luokittelematon.

6.4 Mekaanisten järjestelmien tasoluokitusten tulokset

Alla olevassa taulukossa on listattuna TIA-942-B-dokumentin sivujen 86 - 87 taulukoiden kaikki mekaanisten järjestelmien kategorian arvostelukohteet, jotka ovat listattuna taulukon vasempaan reunaan. Taulukossa rating-sarakkeessa on tämän tutkimuksen arvio kustakin arvostelukohteesta. Taulukon oikeanpuolimmaisessa sarakkeessa näkyy CyberLab-datakeskuksen saaman

tasoluokituksen dokumentinmukainen selitys arvostelukohteen sen tasoluokituksen vaatimukselle.

Taulukko 5. Mekaanisten järjestelmien luokittelun tulokset

CATEGORY	Rating	Description
Mechanical	M1-M4	
General		
Redundancy for mechanical equipment. These redundancy requirements extend to all support areas that are critical to the uninterrupted operation of the computer/server room.	M2	N+1 redundancy for mechanical equipment. Loss of electrical supply path or water supply (where applicable) could lead to loss of cooling
Routing of water or drain piping not associated with the data center equipment in data center spaces	M2	Permitted but not recommended
Positive pressure in computer room and associated spaces relative to outdoors and non-data cener spaces	M4	Yes
Floor drains in computer room for condensate drain water, humidifier flush water, and sprinkler discharge water	M4	Yes
Mechanical systems on standby generator	M1	Not required
Humidity Control for Computer Room	M1	Not required
Water-Cooled System		
Indoor Terminal Air Conditioning Units	M1	No redundant air conditioning units
Electrical Service to Mechanical Equipment	M2	Single path of electrical power to AC equipment
Heat Rejection		
Piping Systems	M4	Piping systems provide fault tolerance
Chilled Water & Air Cooled Systems		
Electrical Service to Mechanical Equipment	M2	Single path of electrical power to AC equipment
HVAC Control System		
HVAC Control System	M2	Control system failure will not interrupt cooling to critical areas but might prevent further control of temperature/humidity (steady state)
Power Source to HVAC Control System	M3	Dual path of electrical power in N+1 configuration designed to be concurrently maintainable
Plumbing (for water-cooled heat rejection)		
Make-up Water	M4	Dual sources of water, or one source + on-site storage with a minimum equal to duration of generator fuel supply
Points of Connection to Condenser Water System	M2	Single point of connection
Fuel Oil System		
Onsite generator fuel storage	---	---
Bulk Storage Tanks	---	---
Storage Tank Pumps and Piping	---	---

Fire Suppression		
Fire detection system	M4	yes
Fire sprinkler system	M4	pre-action (When required)
Gaseous suppression system computer rooms and entrance rooms containing active ICT equipment	M4	When used, clean agents should be allowed by local code. Alternative systems (e.g., hypoxic mist) are allowed
Early Warning Smoke Detection System for computer rooms and entrance rooms containing active ICT equipment	M4	yes
Water Leak Detection System for computer rooms and entrance rooms containing active ICT equipment	M4	yes

Mekaanisissa järjestelmissä M1-luokitteluarvosanan saaneita arviointikohteita oli kolme kappaletta ja tasoluokituksenkokonaan saamatta olleita kohtia oli kolme. Nämä kolme M1-tasoluokituksen saanutta arvosanaa olivat mekaanisten systeemien generaattorissa kiinni oleminen, konetilan ilmankosteuden säätelyjärjestelmä ja ilmastointilaitteiden määrä.

M1-luokittelutasolla mekaanisten järjestelmien ei tarvitse olla kiinni valmiustilassa generaattorissa, minkä takia tässä kohtaa on voitu antaa tasoluokitus M1, mutta mikäli M1 tasollakin olisi vaadittu generaattorin kiinniolemista tämäkin arviointikriteeri olisi mennyt luokittelemattomaksi. Jos CyberLab-datakeskukselle hankitaan generaattori ja se liitetään mekaanisiin järjestelmiin toimimaan valmiustilassa, voidaan tasolukitus nostaa tasolle M4. Ilmankosteuden säätelyjärjestelmän puuttumisen takia sille on annettu tasoluokitus M1, sillä sen olemassaolo ei ollut pakollista tällä tasoluokitustasolla. Muilla tasoluokittelun tasoilla vaaditaan, että mikäli ilmankosteuden säätelyjärjestelmä olisi tilaan soveltuva, sellainen olisi siellä käytössä. Rakennuksen ilmankiertojärjestelmän lisäksi datakeskuksessa tulisi myös olla yksi redundanttinen ilmastointilaite jokaisessa kriittisessä tilassa M2 tasoluokituksen saavuttamista varten, sekä sen jälkeen yksi ilmastointilaite viidestä kahdeksaan yksikköä kohden, mikä tarkoittaisi CyberLab-datakeskuksen kohdalla, että yhdellä redundanttisella ilmastointilaitteella saavutettaisiin tasoluokitus M4.

Kolme tasoluokittelematonta kohtaa olivat generaattorin polttoaineen säilytys, polttoaineen säilytystankit, polttoaineen pumput ja putkistot. Syy miksi nämä kohteet eivät saaneet tasoluokitusta johtuu siitä, ettei CyberLab-datakeskuksen käytössä ole generaattoria ollenkaan, jolloin generaattorin polttoaineen

säilyttämiseen liittyvät asiat ja polttoaineen putkistojen ja pumppujen rakentaminen CyberLab-datakeskuksen ympäristöön olisi muutenkin ollut turhaa. Vaikka täällä olisi generaattorille polttoainesäilytykset, pumput ja putket, ei niillä olisi minkäänlaista virkaa, kun generaattori itse puuttuu kokonaan.

6.5 Tasoluokitusten tuloksien yhteenveto

Yhteenvetona telekommunikaation tasoluokituksen suora arvosana olisi T1, koska palvelinten verkkokaapelien päissä ei ole etikettejä merkitsemässä mihin ne yhdistyvät. Mutta koska tämä ja TIA-606-C:n kaapelien dokumentointivaatimukset eivät vaikuta CyberLab-datakeskuksen palvelinten toimivuuteen, päädytään antamaan telekommunikaatiolle loppuarvosana T2. Mikäli CyberLab-datakeskuksen käyttöön saadaan joskus toimimaan redundanttinen verkkoyhteys, voidaan siinä tilanteessa nostaa telekommunikaation tasoluokituksen tulos vastaamaan tasoa T3.

Arkkitehtuurin ja struktuurin suoranainen tasoluokitusarvosana on A1. Tämä johtuu rakennuksen turvalaitteiden UPS-kapasiteettien puuttumisesta ja palvelinkaappien sekä kabinettien maanjäristyssuojauksien puutteellisuuden takia. Mutta koska nämä kyseiset heikkoudet eivät käytännöllisellä tasolla vaikuta CyberLab-datakeskukseen merkittävällä tavalla, voidaan arkkitehtuurille ja struktuurille antaa tasoluokitus A2. Fyysisen turvallisuuden kannalta olisi kannattavaa, että CyberLab-datakeskuksen kamerat, sensorit sekä hälytyslaitteet olisivat kuitenkin kiinni varavirtalähteissä. Palvelinkaappien kannattaisi myös olla pultattuina lattiaan palvelinkaappien luvattoman siirtämisen tai kaatamisen varalta. Jotta arkkitehtuurille ja struktuurille voitaisiin antaa tasoluokitus A3, tulisi tehdä perinpohjainen selvitys sekä vaadittavat remontit sitä varten, että CyberLab-datakeskus sekä muut rakennuksen rakenteet kuten ulko- ja sisäseinät, ovet ja ikkunat vastaisivat niiden tulen kestävyyden vaatimuksia. Myös tilanteessa, jossa palvelinkeskuksen käyttöön otetaan sähkögeneraattori, tulee sen polttoainesäiliön varustelu rakentaa vastaamaan sijainnin mukaisia vaadittavia tulenkestävyyden suojauksia.

Sähköisten järjestelmien tasoluokitusten arvosana on E1. Jotta sähköisten järjestelmien tasoluokitus saataisiin nostettua tasolle E2, CyberLab-datakeskuk-

sen UPS-laitteiden tulisi olla topologiallisesti rinnakkaisia moduuleita, itsenäisille moduuleille, mikäli niitä on, tulisi olla omat niille omistetut akkupankit tai akkupankkien tulisi olla modulaarisia. CyberLab-datakeskukselle tulisi hankkia sähkögeneraattori vastaamaan CyberLab-datakeskuksen UPS:n ja mekaanisten järjestelmien sähkönkulutusta sekä CyberLab-datakeskuksen henkilökunnalle tulisi suunnitella ajoittainen käyttökoulutusohjelma, mikä pitäisi huolen siitä, että henkilökunta pystyisi käsittelemään CyberLab-datakeskuksen laitteistoja.

Mekaanisten järjestelmien tasoluokitusten arvosana on M1. Mekaanisten järjestelmien tasoluokituksen arvosanaa saadaan kuitenkin nostettua M2:een hankkimalla CyberLab-datakeskuksen käyttöön sähkögeneraattori, sekä kytkemällä se mekaanisiin järjestelmiin valmiustilaan sähkökatkosten varalle. Sähkögeneraattorin toimintaa varten tulee olla ainakin yksi polttoainesäiliö, jonka sisälle mahtuu polttoainetta vastaamaan 24:ää käyttötuntia, mikäli toimivaltainen viranomainen sallii sekä useampi, kuin yksi polttoaine pumppu syöttämään generaattorille polttoainetta. M2:n saavuttamista varten tulee myös asentaa jokaista kriittistä aluetta kohden yksi redundanttinen ilmastointilaite pitämään huolta kriittisten tilojen huoneilman tasapainoisuudesta.

Vielä lopuksi CyberLab-datakeskuksen kategorioiden tasoluokituksien tulokset ovat T2, E1, A2 ja M1. Tällöin koko datakeskusta vastaava yhtenäinen tasoluokitus on 1, koska kategorioiden alin tasoluokitus on 1.

7 TIA:LLE VAIHTOEHTOISET DATAKESKUSSTANDARDIT

Tässä luvussa käsitellään lyhyesti TIA-942-B datakeskuksen telekommunikaation infrastruktuuri -standardi-dokumentille olevia vaihtoehtoisia datakeskuksien standardiluokitteludokumentteja. Vaihtoehtoisiin standardi-dokumentteihin kuuluu Uptime instituutin datakeskuksen infrastruktuurin topologian TIER-standardi dokumentti, jonka jokainen voi ladata ilmaiseksi heidän verkkosivuiltaan. Uptime instituutin lisäksi on olemassa Suomen standardisoimisliitto SFS:n suomalaiseksi kansallisiksi standardeiksi vahvistamat Euroopan datakeskus-standardit, jotka löytyvät nimellä SFS-EN 50600. EN 50600 -sarjan standardit luotiin kompensoimaan datakeskuksien tilojen ja infrastruktuurien standardien vajautta Euroopassa (CIS s.a.).

Uptime instituutti on teetättänyt oman standardisoidun luokittelujärjestelmän, minkä tarkoituksena on jakaa datakeskukset erilaisiin TIER-tasoihin. TIER-luokitusjärjestelmä tarjoaa datakeskusteollisuudelle johdonmukaisen keinon verrata tyypillisesti ainutlaatuisia, räätälöityjä tiloja odotetun infrastruktuurin suorituskyvyn tai käytettävyyden perusteella (Uptime Institute). Uptime Instituutin TIER-luokitukset ovat porrastettu neljään eri osaan. TIER:it (I-IV) ovat progressiivisia; jokainen taso sisältää kaikkien alempien tasojen vaatimukset (Stansberry 2014). Vaikka Uptime instituutin ilmaiseksi ladattavissa oleva dokumentti onkin hieman lyhyt, sen sisällön perusteella pienet, uudet sekä aloittelevat yritykset pystyvät kehittämään oman palvelinhuoneensa tai datakeskuksensa toimivuutta sekä löytämään parannuskohteita omista palvelinhuone- tai datakeskuskomplekseistaan.

SFS:n vahvistamien eurooppalaisten datakeskus standardien käyttö Suomessa datakeskuksen päästandardina Uptime instituutin ja ANSI/TIA:n datakeskusstandardien sijasta olisi suositeltavaa varsinkin suurissa datakeskus- tai palvelinhuonekomplekseissa Suomen tai muiden Euroopan maiden rajojen sisällä, sillä ne vastaavat parhaiten Euroopan unionin vaatimia standardeja sekä lakeja. EN 50600 edustaa eurooppalaista standardia, joka käyttää kokonaisvaltaista lähestymistapaa kattavien eritelmien laatimiseksi datakeskuksen uudelle rakentamiselle ja toiminnalle. 50600 sisältää rakennus-, virtalähde-, ilmastointi- ja ilmanvaihto-, kaapelointi- ja turvajärjestelmien vaatimukset sekä datakeskuksien toimintoja vastaavat kriteerit (Tüv Nord Group s.a.).

8 CYBERLAB-DATAKESKUKSEN RISKIKARTOITUS

Tämä luku keskittyy CyberLab-datakeskuksen fyysisen turvallisuuden riskikartoitukseen. Luvussa tullaan käsittelemään, kuinka turvassa datakeskus on sisäisiltä sekä ulkopuolisilta uhkatekijöiltä omien havaintojen perusteella. Marko Oraksen ylemmän ammattikorkeakoulutason opinnäytetyössä ICTLAB Fyysinen turvallisuus (2017) on käsitelty CyberLab-datakeskuksen fyysistä turvallisuutta TUREAN-tunkeutumisreittianalyysin avulla. TUREAN-analyysillä saadaan luotettavaa tietoa turvallisuusratkaisujen tasosta, todennetaan käytössä olevien ratkaisujen riittävyyttä ja kustannustehokkuutta sekä keskitetään uu-

sien hankkeiden sijoituskohteita (Oras 2017). Oraksen teettämän tunkeutumisreittianalyysin tuloksista käy ilmi, että rikollinen pystyisi murtautumaan VirtualLab-datakeskukseen sisälle tekemään tuhotöitään ja poistumaan paikalta ennen kuin vartiointiliikkeen vartijat ehtisivät paikalle. TUREAN-analyysin tulokset perustuvat analyysin tekijän syöttämien vaihtoehtoisten tunkeutumisreittien tietoihin, joiden pohjalta TUREAN-analyysiohjelmisto laatii eri tapahtumaketjut sisältävän tulosluettelon. TUREAN-analyysin perusteella pystytään tunnistamaan tilojen suojauksien tehokkuuksia (Peltonen 2003).

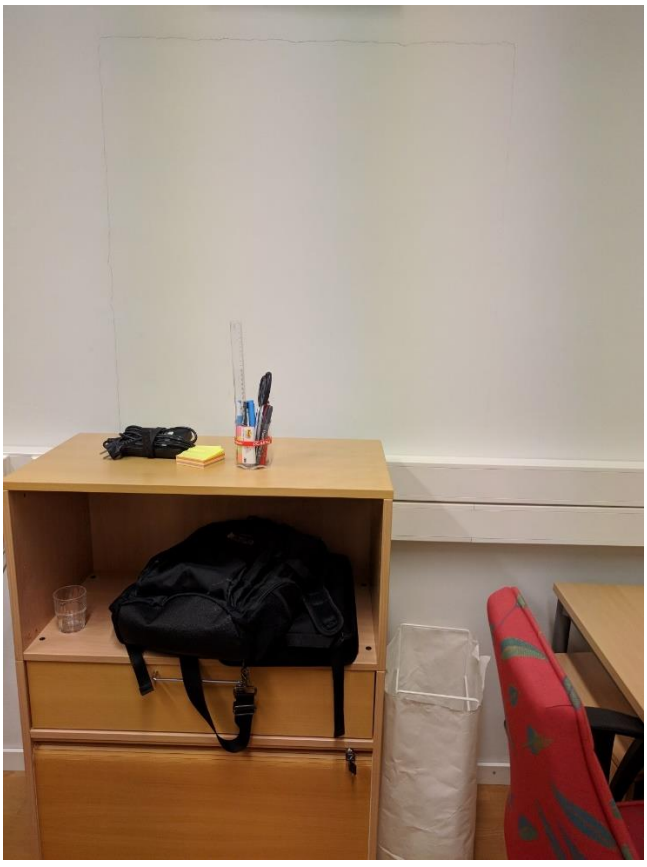
Datakeskuksen naamiointi näkymättömäksi ulkopuolisilta on CyberLab-datakeskuksen ulkopuolelta toteutettu kohtalaisen hyvin. Ainoat huomiota herättävät ulospäin näkyvät merkit datakeskuksen tarkasta sijainnista ovat CyberLab-datakeskuksen sijainnin mainostukset (Kuva 1), jotka voivat herättää datakeskusta etsivän henkilön huomion ja ulkopuolelta huomattavissa oleva jäähdytysyksikkö, joka on huomattavasti erilaisempi kuin kaikki muut jäähdytysyksiköt koulun ympäristössä sekä ainut, jonka ympärille on aseteltu häkki suojaamaan sitä (Kuva 2).

Kuva 1. Datakeskuksen sijainnin naamiointia haittaava mainostus

Kuva 2. Datakeskuksen jäähdytysyksikkö

Merkittäviä turvallisuusheikkouksia datakeskuksessa ja sen ympäristössä ovat käytävällä oleva umpeen muurattu entinen oviaukko (Kuva 3) ja opettajien toimistotilan seinässä oleva umpeen muurattu entinen oviaukko (Kuva 4), jotka molemmat johtavat datakeskuksen tiloihin. Heikkouksia datakeskuksen turvallisuudelle ovat myös datakeskuksen palo-oven asettelu, sekä valvontakameroiden vajaavaisuus. Käytävänpuoleinen entinen oviaukko on huomattava turvallisuusriski, sekä heikkous datakeskuksen turvallisuudelle siitä syystä, että se on datakeskuksen seinärakennelmien heikkokohta, koska ovikohdan laastien rikkominen murtautumiskeinona on huomattavasti helpompaa sekä nopeampaa kuin tiiliseinän ja sen sisäisten metallirakenteiden läpi murtautuminen. Opettajien toimistotilan umpeen muurattu oviaukko on hieman pienempi riskitekijä kuin käytävän puoleinen entinen oviaukko, koska tämän oviaukon luokse pääseminen vaatii huomattavasti enemmän aikaa, se on paljon paremmin piilossa, sekä sen edessä on esteinä pöytä, lipasto ja seinään kiinnitetty kaapelikouru.

Kuva 3. Käytävänpuoleinen umpeen muurattu entinen oviaukko



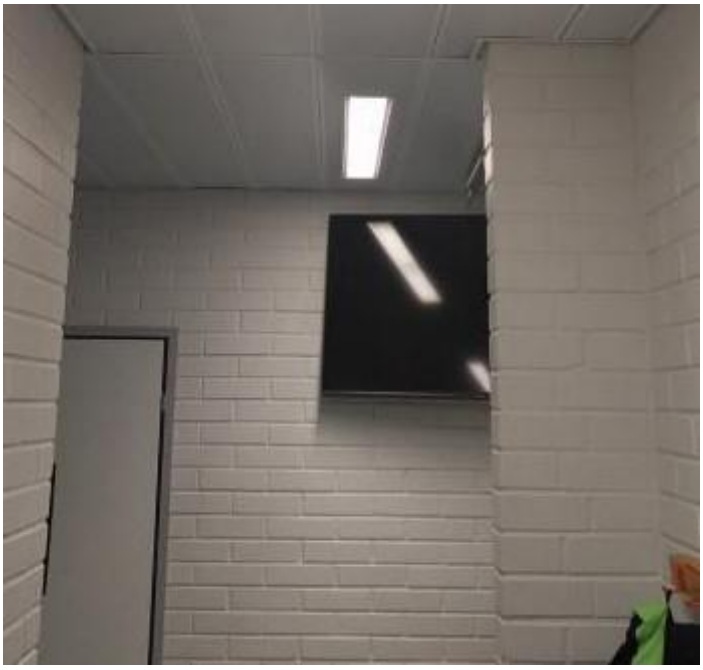
Kuva 4. Opettajien toimistotilan umpeen muurattu entinen oviaukko

Datakeskuksen palo-ovi on aseteltuna väärin suojaamaan datakeskusta, sillä palo-oven saranat ovat datakeskuksen tilan ulkopuolella, jolloin datakeskukseen haluava henkilö pystyisi helposti murtautumaan sisään hajottamalla oven saranat. Palo-ovi ei myöskään ole kiinniollessaan tiivistetysti kiinni oven alareunasta. Palo-ovi on kiinni ollessaan noin senttimetrin verran irti oven kynnyksestä. Tämänkaltainen oven virheasettelu hieman pilaa sen tarkoituksen, mitä varten palo-ovi on alun perin asennettu. Mikäli tilanteessa, jossa datakeskuksen sisäpuolella jokin syttyisi palamaan, sen tulipalon liekit voisivat myös ilmastoinnin kiinni ollessa saada happea palaaksensa palo-oven alareunan kolon kautta, sekä leviämään datakeskuksesta ulos. Sama logiikka pätee myös tilanteessa, jossa datakeskuksen palo-oven ulkopuolella olisi tulipalo. Tilanteessa, jossa datakeskuksessa käytettäisiin sammutuskaasuja tulipalon sammutusjärjestelmänä, sammutuskaasujen tehokkuus saattaisi kärsiä huomattavasti palo-oven aukon tuottaman vuodon takia. Huomattavia paloturvallisuusriskejä datakeskuksen sisältä löytyi palavien materiaalien muodossa. Datakeskuksen sisältä löytyi sinne jätettyinä erinäisiä papereita, pahvilaatikoita, sekä muutama lastulevytuoli.

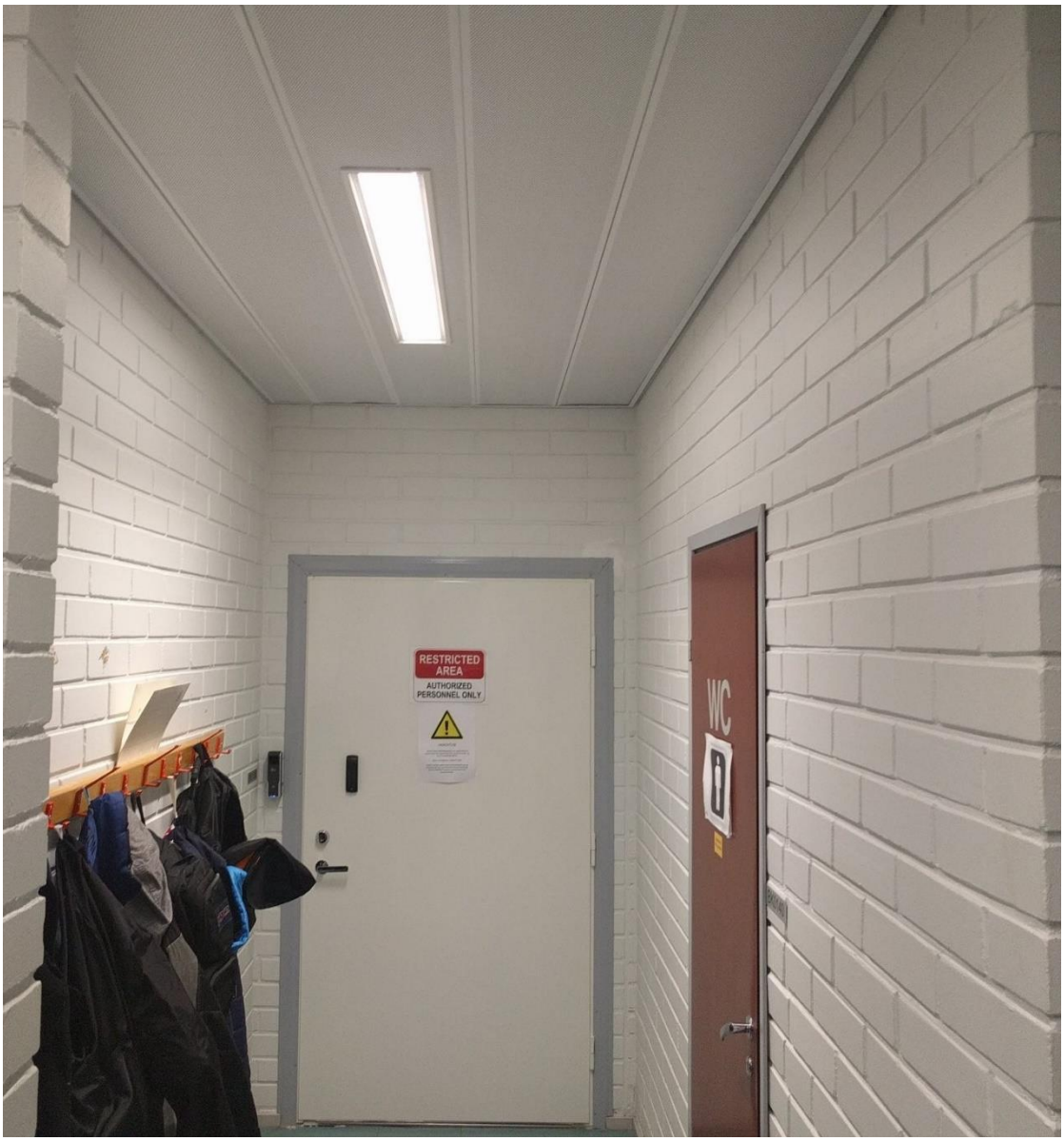
CyberLab-datakeskuksen henkilökunnan sekä opiskelijoiden datakeskustoiminnassa huomattiin myös suuri datakeskukseen liittyvä tietoturvariski. Huomasin useasti tämän tutkimuksen aikana, että datakeskuksen ovikäytännön turvallisuutta laiminlyötiin. Monesti kun jokin opiskelija tai CyberLab-datakeskuksen henkilökuntaan kuuluva työntekijä oli työskentelemässä datakeskuksen tiloissa, datakeskuksen ovi oli jätetty auki. Tällaisessa tilanteessa kaikkein tiukimmat monijakoiset biometriset tunnistimetkin pystytään helposti päivittämään, sillä tunkeilijat pääsevät helposti datakeskukseen sisälle (Clark 2012). Tällainen riskitekijä saataisiin eliminoitua asentamalla kaksiovisen ihmisansan datakeskuksen sisäänkäynnin yhteyteen. Tällaisessa ihmisansassa on kyse pienestä väliovitilasta, mihin mahtuu ainoastaan yksi henkilö kerrallaan sisälle. Väliovitilan tarkoitus on toimia sellaisessa muodossa, että mikäli väliovitilan sisällä havaitaan olevan useampi, kuin yksi henkilö, datakeskuksen ovea ei pystytä avaamaan. Ihmisansan välioven sekä datakeskuksen oven kannattaisi molempien olla automaattisesti sulkeutuvia ja sisältää sensorijärjestelmän, joka estää datakeskuksen oven avaamisen ulkopuolelta, mikäli väliovi on auki

ja välioven avaamisen sisäpuolelta, mikäli datakeskuksen ovi on auki. Datakeskuksen sisäänkäynnin tuottamaa sosiaalisen manipuloinnin riskiä voidaan myös lieventää hieman halvemmalla ja nopeammalla tavalla, eli asentamalla datakeskuksen sisäänkäynnin oveen ovensulkijan ja ovianturin, joka alkaa soimaan, mikäli ovea pidetään liian kauan auki.

Datakeskuksen ympäristön kameravalvonnasta löytyi pieniä puutteita. Vaikka datakeskuksen sisällä onkin kamera, sen sisäänkäynnin toisen puolen valvonnassa on huomattavia puutteita. Datakeskukseen johtavan oven aluetta ei kuvata minkäänlaisella tavalla luoden suuren pimeän kohdan datakeskuksen valvontaan ja riskialueen turvallisuudelle. Datakeskuksen sisäänkäynnin alueen kuvaaminen sisäänkäynnin ulkopuolelta auttaisi tunnistamaan henkilöitä, jotka yrittäisivät päästä datakeskukseen luvattomasti sisään sekä auttaisi valvomaan tilanteita siltä varalta, että joku yrittäisi pakkokeinoin päästä datakeskukseen sisälle. Alla olevissa kuvissa 5 ja 6 näkyy datakeskuksen ovelta käytävälle oleva näkyvyys kuvassa 5 ja datakeskuksen ovelle johtava näkyvyys kuvassa 6. Hyviä kohtia kameralle kuvaamaan datakeskuksen ovea sekä käytävää olisivat kuvassa 5 olevan tv-ruudun yläpuolelle seinään, kuvan 5 oikeassa yläkulmassa näkyvä seinänyläkulma tai kuvassa 6 datakeskuksen ovenseinän oikeayläkulma. Datakeskuksen ja sen ympäristön kameravalvonnasta puuttuu myös huomattava datakeskuksen turvallisuuden suojausta korostava osa, nimittäin aktiivinen kameravalvonta. Tällä hetkellä kukaan ei valvo CyberLab-datakeskuksen valvontakameroiden live-kuvaa. Tämä ongelma on kuitenkin helppo korjata asentamalla henkilökunnan toimistotilan sisäpuolelle kameroiden videokuvan seuraamiseen tarkoitetun näytön, josta henkilökunta pystyisi työajalla valvomaan datakeskuksen fyysistä turvallisuutta tehokkaammin toimistosta käsin. Videovalvonta on olennainen osa datakeskusten fyysistä turvallisuutta, mutta sitä usein laiminlyödään (Wise 2018).



Kuva 5. Datakeskukselta johtava käytävä



Kuva 6. Datakeskukseen johtava käytävä

Jäähdytysyksikön ympärille asetetut fyysisen turvallisuuden suojat ovat niin huonot, että kaikki henkilöt, jotka haluavat päästä jäähdytysyksikköön käsiksi voisivat tehdä niin ilman minkäänlaista vaivaa. Jäähdytysyksikön ympärillä oleva häkki estää ainoastaan ihmisiä vahingossa kävelemästä jäähdytysyksikköä päin tai törmäämästä jäähdytysyksikköön, mutta mikäli henkilö haluaisi päästä verkosta läpi hän pystyisi tekemään niin pihdeillä tai kiipeämällä verkkoa pitkin jäähdytysyksikön häkin sisälle. Häkki asennettiin jäähdytysyksikön ympärille kesällä 2017 tukemaan jäähdytysyksikön fyysistä turvallisuutta, mutta häkki yksinään ei riitä suojaamaan jäähdytysyksikköä hyökkääjiltä.

Jäähdytysyksikön yläpuolella ei ole minkäänlaista kattoa suojaamassa sitä säältä tai hyökkääjiltä. Jäähdytysyksikön metalliosissa, sekä jäähdytysvesiputkien kiinnikkeissä on jo olemassa näkyvää ruostetta, joka on peräisin kelien aiheuttamista vahingoista. Jäähdytysyksikön häkkiin pääsee myös helposti CyberLab-datakeskuksen katon kautta, joka on samalla tasolla jäähdytysyksikön häkin yläreunan kanssa.

Häkin alareuna ja rakennuksen seinän puoleiset reunat ovat muutaman kymmenen sentin verran irti maanpinnasta ja seinänreunasta luoden isokokoiset aukot joista muun muassa oravat ja linnut pääsevät helposti kulkemaan. Häkin ovet ovat lukittuina perinteisillä Abloyn kiekkohaittasylinteririippulukoilla. Lukot ovat kovin pieniä messinkiriippulukkoja, joiden rikkominen on helppoa ja nopeaa vipuvoimalla. Lukkojen tulisi olla järeämmät, sekä suositeltavaa olisi, että lukkojen tyyppi vaihdettaisiin perinteisestä levyhaittasylinteristä Abloy PROTEC2 CLIQ -tyyppiseen lukitusjärjestelmään. Abloy PROTEC2 -tyypin pidetään yhtenä maailman parhaimpana lukkona ja käytännössä mahdottomina tiirikoida, kun taas CLIQ-teknologia mahdollistaa avaimen kulkuoikeuksien muuttamisen etäältä sekä asettamaan avaimelle aikavälit, jolloin avainta pystyy käyttämään eliminoiden avaimen häviämisestä muodostuvan turvallisuusriskin (Abloy s.a.)

Jäähdytysvesiputkien eristeiden kunto on välttävässä kunnossa. Eristemateriaalista puuttuu joistain kohtia eristettä aivan kuin sitä oltaisiin nypitty siitä irti. Tämä saattaa olla mahdollisesti lintujen aikaansaamaa tuhotyötä. Koska putket ja niiden eristemateriaalit eivät ole keliltä minkäänlaisessa suojassa niiden

pinnalla on nähtävissä sateiden, sekä lumien aiheuttamat vahingot. Eroavaisuus hyväkuntoiseen ja huonokuntoiseen eristemateriaaliin on helposti nähtävissä, kun katsotaan putken alapuolen eristettä, joka näyttää olevan hieman paremmassa kunnossa sekä hieman enemmän suojassa sateilta ja lumelta, kuin eristeen päällimmäinen puoli. Ulkona jäähdytysjärjestelmän putkiston päässä käsien ulottumattomissa on venttiili, jonka avaamalla jäähdytysjärjestelmän putkistojen jäähdytysvedenpaineeseen sekä vaikuttamaan jäähdytysnesteeseen. Vaikka jäähdytysvesiputken venttiili onkin korkealla käsien ulottumattomissa, lukitusmekanismin puuttuminen aiheuttaa riskitekijän, jossa tuhotyötä tekevä henkilö pystyy helposti tuottamaan vahinkoa jäähdytysjärjestelmälle.

Jäähdytysjärjestelmää valvova valvontakamera on piilotettu sijaitsemaan jäähdytysjärjestelmän vieressä sijaitsevan ikkunan toiselle puolelle. Tästä syystä valvontakameraa ei ole mahdollista huomata ulkopuolelta, minkä takia se on hyvin piilotettu, mutta ikkunan sälekaihtimet toimimat osittaisena näköhaittana ja mikäli joku kääntää sälekaihtimia kameran näkyvyys ikkunasta ulos jäähdytysjärjestelmälle pimenee kokonaan. Ongelmana on myös Suomen talviajan pimeys. Pimeällä talvisella kelillä valvontakameran näkyvyys ulos kärsii varsinkin tilanteissa, joissa toimistotilassa on valot päällä, mutta ulkona on pimeää, koska ikkunanlasista takaisinpäin heijastuva valo tulee hieman sokaisemaan kameran kykyä nähdä ulos.

Kuva 7. Jäähdytysyksikön valvontakameran kuva

9 JOHTOPÄÄTÖKSET

Yhteenvedon päätöksenä TIA-942-B-dokumentin kategorioiden arviointikriteereiden mukaiset tasoluokitukset, joita Kaakkois-Suomen ammattikorkeakoulu Oy:n Kotkan kampuksen CyberLab-datakeskus vastaa, ovat T2, E1, A2 ja M1. Yhtenäinen tasoluokitus kokonaisvaltaisesti koko datakeskukselle on datakeskuksen heikoimpien osien mukaisesti perustason tasoluokitus yksi. Kaikista varteenotettavin syy, miksei datakeskukselle voida antaa kokonaisvaltaiseksi arvosanaksi kakkostason redundanttisten komponenttien tasoluokitusta johtuu sähkögeneraattorin puuttumisesta.

Kokonaisvaltaisen tasoluokituksen arvosana saataisiin nostettua seuraavalle tasoluokitus tasolle täydellä varmuudella, mikäli datakeskuksen johtojenpäihin asennettaisiin etiketit, joista selviäisi vastakkaisten kytkentöjen sijainti. Datakeskuksen käyttöön tulisi myös hankkia sähkögeneraattori, joka vastaisi sähköntuotanto tehokkuudeltaan UPS-laitteiden sekä mekaanisten järjestelmien kulutusta sekä kytkeä kiinni mekaanisiin järjestelmiin valmiustilaan sähkökatkosten varalta. Generaattoria varten tulee olla olemassa polttoainesäiliö, joka sisältää tarpeeksi polttoainetta vastaamaan 24:ää tuntia tai toimivaltaisen viranomaisen sallimaa määrää. Polttoainesäiliöllä tulee olla useampi kuin yksi polttoainepumppu syöttämässä redundanttisesti polttoainetta generaattorille. UPS-laitteiden topologia tulisi myös suunnitella toimimaan rinnakkaisina moduuleina. Viimeisin muttei vähäisin parannuksen kohde tasoluokitustason kaksi saavuttamista varten on, että jokaista kriittistä tilaa vastaamaan asennettaisiin redundanttinen ilmastointilaite.

Datakeskuksen ympäristön fyysisestä turvallisuudesta ilmeni useita parannuskohteita ja heikkouksia. Potentiaalisia uhkia, joissa datakeskuksen turvallisuus voisi vaarantua, ilmeni ainoastaan yksi kappale. Kyseisessä tilanteessa datakeskuksessa työskentelevät tai työskennelleet henkilöt ovat jättäneet datakeskus tilan oven auki. Tällöin kuka tahansa pystyisi pienellä sosiaalisella manipuloinnilla pääsemään käsiksi datakeskuksen palvelimiin.

Suurin ongelma opinnäytetyössä datakeskuksen standardiluokittelussa oli tasoluokittelun suorittaminen lyhyen aikavälin sisällä. Tasoluokittelun tuottaminen kunnolla vie paljon aikaa. Tarkka ymmärtäminen jokaisen tason kunkin luokituksen kriteerien eri vaatimuksista on erittäin paljon aikaa kuluttava. Näin varsinkin, jos kyseessä on uusi standardi, jonka kaikki kriteerit eivät ole jo valmiiksi tuttuja. Tasoluokittelussa jouduttiin käsittelemään useasti täysin tuntemattomia asioita, joista ei ollut ollenkaan aikaisempaa ymmärrystä tai kokemusta. Välillä tasoluokittelun vaatimus saattoi koostua ainoastaan yhdestä tai kahdesta sanasta, jotka käsittelivät ennestään tuntemattomia asioita. Tällaisissa tapauksissa jouduttiin käyttämään paljon aikaa uusien asioiden tutkimiseen sekä sitä, mitä näillä muutamasta sanasta muodostuvat vaatimukset oikeasti tarkoittavat. Datakeskuksen tasoluokittelun tekeminen olisi ollut huomattavasti nopeampaa, mikäli dokumentissa olisi ollut paremmin avattuna, mitä tasoluokitusten eri arviointikriteerien kohdissa tarkalleen ottaen vaaditaan.

Tutkimuksessa saavutettiin halutut tavoitteet. TIA:n datakeskusstandardin mukaisen tasoluokituksen tulokset saatiin selvitettyä siinä määrin, että tasoluokitusten tasot pystyttiin määrittämään. Parannuskohteet tasoluokituksen nostamista varten saatiin luokiteltua sekä datakeskuksen fyysisen turvallisuuden riskikartoituksessa onnistuttiin löytämään fyysisen turvallisuuden kehityskohteita sekä paikallistamaan minkälaisia fyysisiä heikkouksia datakeskuksella on.

LÄHTEET

Abloy. s.a. Tuplavarmistettua kulunhallintaa – PROTEC2 CLIQ. WWW-dokumentti. Saatavissa: https://www.abloy.fi/fi/abloy/abloyfi/tuotteet/ratkaisut/abloy-protec2-cliq-lukitus-ja-kulunhallintajarjestelma/ [viitattu 13.12.2018].

Amtex Electronix Pty Ltd. s.a. Battery Charging Terminology. WWW-dokumentti. Saatavissa: http://www.amtex.com.au/application_notes_pdf/Battery_Charging_14-22.pdf [viitattu 12.12.2018].

Barker, D. 2012. A Guide to Physical Security for Data Centers. WWW-dokumentti. Saatavissa: http://www.datacenterjournal.com/a-guide-to-physical-security-for-data-centers/ [viitattu 13.12.2018].

Clark, J. 2012. What is a mantrap and do you need one? WWW-dokumentti. Saatavilla: http://www.datacenterjournal.com/what-is-a-mantrap-and-do-you-need-one/ [viitattu 13.12.2018].

CIS – Certification & Information Security Services. s.a. The European Standard EN 50600. WWW-dokumentti. Saatavissa: http://www.cis-cert.com/Pages/com/System-Zertifizierung/Data-Centers/Certification/European-Standard-EN-50600.aspx [viitattu 13.12.2018].

Google. s.a. Hamina, Finland. WWW-dokumentti. Saatavissa: https://www.google.com/about/datacenters/inside/locations/hamina/ [13.12.2018].

ITWatchDogs. 2015. How does data center uptime impact business revenue? WWW-dokumentti- Saatavissa: http://www.itwatchdogs.com/environmental-monitoring-news/data-center/how-does-data-center-uptime-impact-business-revenue-40076091 [viitattu 13.12.2018].

Kananen, J. 2015a. Online Research for Preparing Your Thesis. Jyväskylä: JAMK University of Applied Sciences. [viitattu 14.9.2018].

Kananen, J. 2015b. Kehittämistutkimuksen kirjoittamisen käytännönopas: Miten kirjoitan kehittämistutkimuksen vaihe vaiheelta. Jyväskylä: JAMK University of Applied Sciences [viitattu 14.9.2018].

Kananen, J. 2017. Kehittämistutkitus interventiotutkimuksen muotona. Jyväskylä: JAMK University of Applied Sciences [viitattu 14.9.2018].

Ledwell, A. 2015. How to reduce risk in data center design and maintenance. WWW-dokumentti. Saatavissa: https://gcn.com/Articles/2015/09/17/Evaluating-data-center-risks.aspx [viitattu 13.12.2018].

Lehtoniemi, P. 2017.Datakeskukset kiinteistösijoitustuotteena Suomessa. Aalto-yliopisto. Kiinteistötalouden koulutusohjelma. Opinnäytetyö. WWW-dokumentti. Saatavissa: https://aaltodoc.aalto.fi/handle/123456789/25123 [viitattu 13.12.2018].

Oras, M. 2017. ICTLAB Fyysinen turvallisuus. PDF-dokumentti. Kaakkois-Suomen ammattikorkeakoulu. Teknologiaosaamisen johtamisen koulutusohjelma. Opinnäytetyö. [viitattu 13.12.2018].

Peltonen, J. 2003. TUREAN tunkeutumisreittianalyysi. WWW-dokumentti. Saatavissa: http://www.yhteisturvallisuus.net/download/TUREAN.pdf [viitattu 13.12.2018].

Rouse, M. s.a. A free IT risk assessment template. WWW-dokumentti. Päivitetty 26.7.2017a. Saatavissa: https://searchdisasterrecovery.techtarget.com/Risk-assessments-in-disaster-recovery-planning-A-free-IT-risk-assessment-template-and-guide [viitattu 19.12.2018].

Rouse, M. s.a. Risk assessment. WWW-dokumentti. Päivitetty 1.6.2017b. Saatavissa: https://searchcompliance.techtarget.com/definition/risk-assessment [viitattu 19.12.2018].

Scalet, S. 2015. 19 ways to build physical security into your data center. WWW-dokumentti. Saatavissa: https://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html [viitattu 13.12.2018].

Shaver, K. 2015. The bushy-tailed, nut-loving menace coming after America's power grid. WWW-dokumentti. Saatavissa: https://www.washingtonpost.com/local/the-bushy-tailed-nut-loving-menace-coming-after-americas-power-grid/2015/12/25/d4b4c2b6-a8db-11e5-9b92-dea7cd4b1a4d_story.html?utm_term=.e4b8a9fa3b17 [viitattu 10.10.2018].

Stansberry, M. 2014. Explaining the Uptime Institute's Tier Classification System. WWW-dokumentti. Saatavissa: https://journal.uptimeinstitute.com/explaining-uptime-institutes-tier-classification-system/ [viitattu 3.10.2018].

Telecommunications Industry Association. s.a. Standards.WWW-dokumentti. Saatavissa: https://www.tiaonline.org/what-we-do/standards/ [viitattu 13.12.2018].

Telecommunications Industry Association. 2006. TIA-942 Data Center Standards Overview. WWW-dokumentti. Saatavissa: http://www.accu-tech.com/hsfs/hub/54495/file-15894024-pdf/docs/102264ae.pdf [viitattu 13.12.2018].

Telecommunications Industry Association. 2017. TIA-942-B Telecommunications Infrastructure Standard for Data Centers. Arlingon, VA U.S.A [viitattu 12.12.2018].

TIA-942.org. s.a. About Data Centers. WWW-dokumentti. saatavissa: http://www.tia-942.org/content/162/289/About_Data_Centers [viitattu 15.12.2018].

Tüv Nord Group. s.a. Data center certification according to DIN EN 50600. WWW-dokumentti. Saatavissa: https://www.tuvit.de/en/services/data-centers-colocation-cloud-infrastructures/din-en-50600/ [viitattu 13.12.2018].

Uptime Institute. s.a. Tier Classification System. WWW-dokumentti. Saatavissa: https://uptimeinstitute.com/tiers [viitattu 3.10.2018].

Wise, M. 2018. Auditor Insights: Security at Data Centers. WWW-dokumentti. Saatavissa: https://kirkpatrickprice.com/blog/auditor-insights-security-data-centers/ [viitattu 12.12.2018].

KUVALUETTELO

Taulukko 1. Telekommunikaation luokittelun tulokset
Taulukko 2. Arkkitehtuurin luokittelun tulokset
Taulukko 3. Struktuurin luokittelun tulokset
Taulukko 4. Sähköisten järjestelmien luokittelun tulokset
Taulukko 5. Mekaanisten järjestelmien luokittelun tulokset
Kuva 1. Datakeskuksen sijainnin naamiointia haittaava mainostus
Kuva 2. Datakeskuksen jäähdytysyksikkö
Kuva 3. Käytävänpuoleinen umpeen muurattu entinen oviaukko
Kuva 4. Opettajien toimistotilan umpeen muurattu entinen oviaukko
Kuva 5. Datakeskukselta johtava käytävä
Kuva 6. Datakeskukseen johtava käytävä
Kuva 7. Jäähdytysyksikön valvontakameran kuva