Konesalin suunnittelu ja toteutus

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

HAMK Riihimäki, Tietotekniikka

kevät, 2019

Jarno Tyni

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietotekniikan koulutusohjelma
Riihimäki

Tekijä Jarno Tyni **Vuosi** 2019

Työn nimi Konesalin suunnittelu ja toteutus

Työn ohjaaja/t Marko Grönfors

TIIVISTELMÄ

Opinnäytetyön tavoitteena on rakentaa nuorelle yritykselle toimiva palvelinjärjestelmä, joka kattaa laitetilasta palvelimiin ja verkkoihin toimivan kokonaisuuden.

Työssä tarkastellaan perustasolla yleisiä laitetilojen elementtejä, jotta lukija voi tehdä perustason päätöksiä alkaessaan suunnittelemaan konesalin rakentamista.

Nykyisellään yritys käyttää ulkoisia palveluntarjoajia ja tulevaisuudessa tarkoitus olisi siirtyä käyttämään omia palveluita ja käyttää ulkoisia vain tavoitettavuuden varmistamiseksi.

Avainsanat Tietoliikennejärjestelmät, tietotekniikka, tietoturva, tietoverkot

Sivut 29 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme In Information Technology
Riihimäki

Author Jarno Tyni **Year** 2019

Subject Data center designing and building

Supervisors Marko Grönfors

ABSTRACT

The aim of this thesis project was to build a data center for the commissioner, young company, which would comprise everything from servers to networks as a working entity.

This work explores all the elements of a data center at a basic level, so that the reader can make basic level decisions based on this information when starting to design a data center.

At present the commissioning company is using external service providers, a future aim is to use the company's own servers and only rely on external services to secure online presence.

Keywords Data networks, information security, information systems, information technology

Pages 29 pages

SISÄLLYS

1 JOHDANTO

Napalmi Tietotekniikka Oy on perustettu vuoden 2015 tammikuussa. Yritys tarjoaa perinteisen tietokonehuollon lisäksi ylläpitoa ja etätukea yritysasiakkaille. Yritys työllistää omistajaosakkaiden lisäksi vuositasolla 1-5 henkilöä. Ensimmäisen neljän tilikauden (2015-2018) liikevaihdot ovat 53 000 €, 142 000 €, 241 000 € ja 246 000 €. Yritys tavoittelee tilikaudelle 2/2019 - 1/2020 maltillista kasvua. Yrityksen toimipiste sijaitsee Hyvinkäällä.

Yritys on tähän asti käyttänyt verkkoliiketoiminnassaan muiden palveluntarjoajien järjestelmiä ja on päättänyt lähteä rakentamaan omia alustoja. Samassa yhteydessä kiinnitetään huomiota yhteyksien skaalautuvuuteen ja suorituskykyyn päivittäisessä liiketoiminnassa.

Palvelinjärjestelmä mahdollistaa erilaisten ”hiekkalaatikko” –ympäristöjen rakentamisen resurssivapaasti ja nopeasti riippumatta kolmansista osapuolista.

Tämän opinnäytetyön tavoitteena on rakentaa toimiva palvelinjärjestelmä tiloineen yrityksen sisäisten ja ulkoisten asiakkaiden käyttöön, ilman luokitusta. Samassa tarkastellaan perusasiat liittyen konesalien rakentamiseen.

2 LAITETILA

Laitetila on huone tai rajattu alue, jota käytetään erillistä suojaa vaativien laitteiden ja järjestelmien käyttöä, ylläpitoa ja säilyttämistä varten. Laitetilassa ei työskennellä lähtökohtaisesti kuin huolto / ylläpito -katkojen aikana ja poikkeustilanteissa. (Pietikäinen, 2013) Tilan on tarkoitus suojata järjestelmiä ympäristön muuttujilta ja turvata palveluiden jatkuminen poikkeusolosuhteissa. Passiivinen suojaus muodostuu rakenteista ja murtosuojauksista sekä hälytysjärjestelmistä ja aktiivinen suojaus muodostuu tietoturvakäytännöistä, riskien arvioinnista ja seurannasta.

Tavanomaisesti laitetilat rakennetaan täyttämään markkinoilla yleisesti käytössä olevat luokitukset ja Suomessa tulee usein kyseeseen VAHTI- (julkisen hallinnon digitaalisen turvallisuuden johtoryhmä) ja Katakri -luokitukset (Kansallinen turvallisuusauditointikriteeristö). Nämä luokitukset tulee täyttää, mikäli haluaa valtion tai viranomaisten asiakkuuksia. Asiakas määrittelee tavoittelemansa suojaustason ja sen mukaisesti rakennetaan järjestelmä.

2.1 Fyysinen rakenne

Sijainti on erittäin tärkeä ominaisuus isoissa konesaleissa. Kustannusten kannalta tärkeimmät ovat yhteyksien saatavuus ja energian hinta. Laadun kannalta tärkeintä on energian saatavuus, henkilöstön saatavuus ja sijainti turvallisessa paikassa. Yhteyksien kannalta tärkeää on, että etäisyydet käyttäjiin ovat lyhyet, jottei viiveet, jotka aiheutuvat jo ihan datan liikkumisesta valon nopeudella aiheuta ongelmia. Esim. 1000 km etäisyys linnuntietä voi olla 1500 km valokuidulla ja aiheuttaa laitteista riippuen n. 20 ms viiveen.

Turvallisuus liittyy olennaisesti sijaintiin. Muun muassa poliittinen ilmapiiri, sotatilat, luonnonolosuhteet (maanjäristykset, tulvat, pyörremyrskyt) ja energian saanti vaikuttavat palveluiden saatavuuteen, luotettavuuteen, yksityisyyteen ja pysyvyyteen.

Konesalin havainnoitavuus vähentää ilkivallan riskiä itsessään jo huomattavasti. Esimerkiksi pieni laitetila voidaan helposti paikantaa jäähdytysilmavirtojen tai varavoimakaluston näkyvyydellä. Jäähdytyksen ja varavoiman koko kannattaa mitoittaa oikein ja piilottaa pois näkyvistä. Konesalin olemassaolon voi joskus päätellä jo ihan rakennuksen kuvasta tai lämpöjäljestä. ”Data Center” –kyltti kannattaa jättää asentamatta.

Äänen ja tärinän eristys tulee huomioida konesalin suunnittelussa. Räkkeihin asennetaan kumijalat ja laitteiden kiinnitys energiaa absorboivin menetelmin. Ilmanvaihdon äänenvaimentimet tulo- ja poistoputkiin estävät tehokkaasti äänen kulkeutumista. Mahdollinen äänenvaimennus salin sisällä työturvallisuuden takia ja räkkien sijoittelu huoneessa ajatellen äänten heijastumista. SSD –levyt vähentävät tärinää ja mekaanista ääntä.

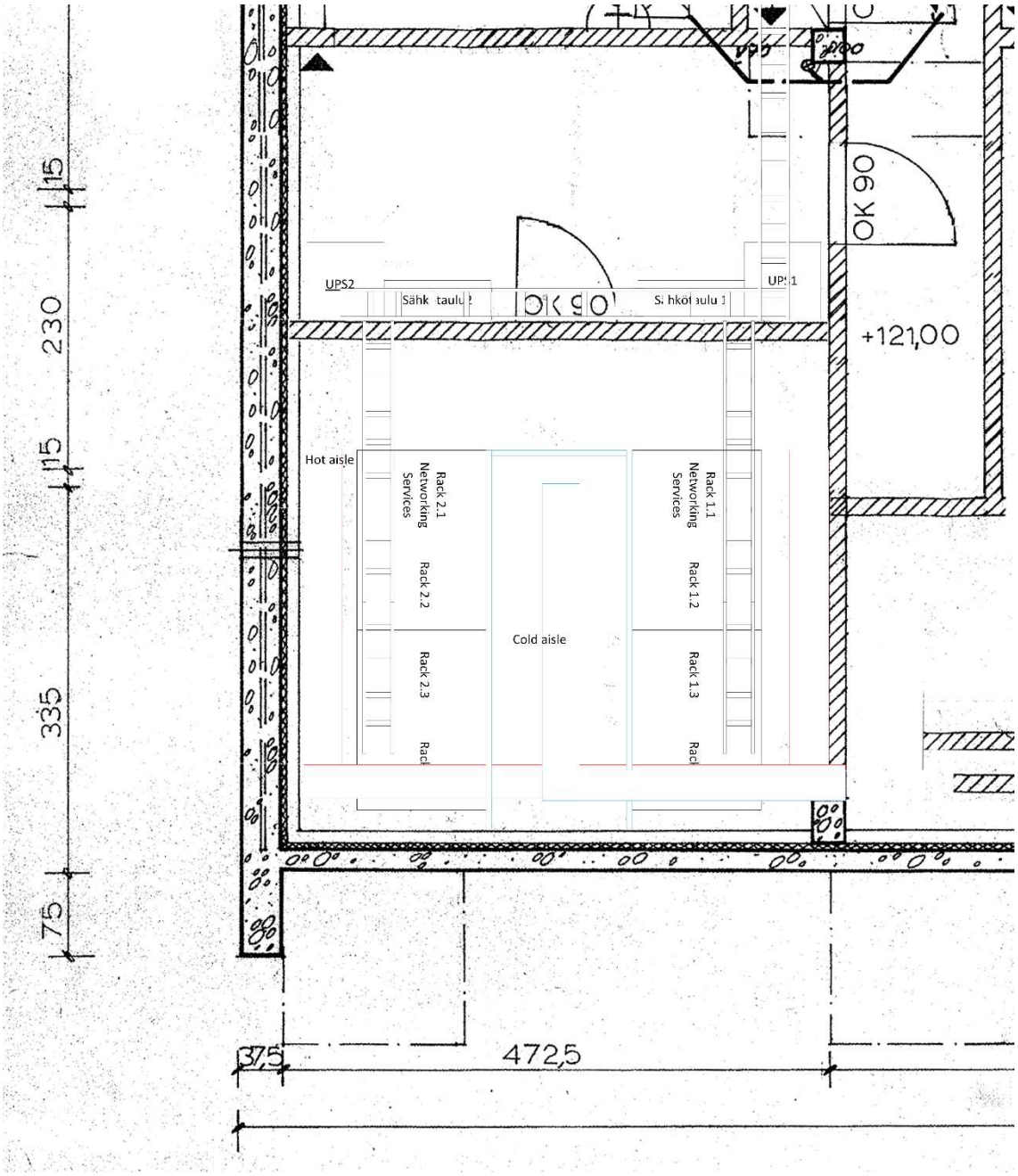
Riskit rakenteessa tulisi poistaa tai minimoida, esim. vesiputket, viemärien puute, tulviminen ja romahtaminen. Mikäli esim. ylempien tilojen viemärit, käyttövesiputket ja lämmitysputket kulkevat tilan läpi tai katon / seinän laatassa niin ne olisi hyvä vähintään gravitaation suuntaisesti koteloida kondensaation ja hitaan vuodon osalta. Parempi vaihtoehto on käyttää kunnon peltikoteloita, joissa kaato on toiseen huoneeseen tai viemäriin. Vuodon varalta voidaan käyttää antureita ja vuotohälyttimiä.

Konesaleissa on yleensä lämmönvaihtimien kondensaation takia viemäriputki tai vähintäänkin letku, joka menee viemäriin. Varsinaisen viemärin sijoitus kannattaa olla toisessa huoneessa, jotta vältytään tulvimisriskiltä tilassa. Esim. Runkolinjan tukkeutuminen ja viallinen takaiskuventtiili voisi työntää viemäriaineksen tilaan. Mikäli tilaa ei saada turvattua veden tulolta niin se voidaan varustaa automatisoidulla poistopumpulla ja kaadoilla.

Salia suunnitellessa olisi hyvä varautua poikkeustilanteisiin, kuten tulvaan tai salamaniskuun. Ilman suodatus, kierrätys ja jäähdytys tulisi suunnitella niin että mahdollinen pöly ja pienet epäpuhtaudet suodatetaan.

Rakenteen fyysinen turvallisuus mitoitetaan käyttötarpeen mukaan. Joissain tapauksissa voi olla tarpeen suojata räjähdyksiltä, maanjäristyksiltä, sähkömagneettisilta (EMP - Electro Magnetic Pulse)– ja mikroaaltopulsseilta (HPM – High Power Microwave). Seinät / katot tulisi olla teräsbetonia tai vastaavaa (esim. teräs). Ovien tulisi olla metallisia ja palamattomia. Paksuus ja lukitus tarpeen mukaan. Lattioiden ja sisäpintojen tulisi olla palamatonta materiaalia. Ilmanvaihto ja suodatus tulisi varustaa palopellein ja eriyttää omakseen muusta ilmanvaihtojärjestelmästä. Ovien tulisi tarjota vähintään samanlainen suoja kuin muiden rakenteiden.

Konesali sijaitsee liikekiinteistön maanalaisessa kerroksessa ja sen kaksi seinää ovat maanvastaisia, kuten esitetty kuvassa 1. Rakenne on teräsbetonia lattiasta, kahdesta seinästä, kaksi seinää ovat tiilimuurattuja ja kattona on teräsbetonilaatta. Tilasta on nyt kaksi ilmanvaihtoventtiiliä, joista toinen menee varastoon ja toinen autohalliin. Toistaiseksi ovena on puinen ”mökkiovi”, joka on tarkoitus pellittää ja myöhemmin muuttaa metalliseksi. Varavoiman on tarkoitus tulla vanhaan jätekatokseen rakennuksen sisään muuntamalla ovi verkko-oveksi ja hyödyntää olemassa olevaa savupiippua pakokaasuille. Akusto tulee erilliseen tilaan ja jäähdytyslaitteisto katolle katutasosta näkymättömiin. Pääsy katolle rajataan. Lattia on tarkoitus pinnoittaa 2-komponenttipinnoitteella ja seiniin tulee rappaus kuten nykyäänkin.



Kuva 1. Konesalin pohjapiirustus.

2.2 **Lukitus ja murtosuojaus**

Murtosuojauksen tasoja voi tarkastella seuraavasti.

1. Kuinka kauan sisäänpääsy vie ilman työkaluja?
2. Kuinka kauan sisäänpääsy vie käsityökaluilla?
3. Kuinka kauan sisäänpääsy vie sähkötyökaluilla?
4. Kuinka kauan sisäänpääsy vie räjähteillä ja koneilla?

On tärkeää arvioida montako minuuttia tai tuntia joku voi pitää kovaäänistä pauketta tai työskentelyä ilman että ympäristö kiinnittää huomiota ja mahdollinen tunkeutuja jää kiinni tai luovuttaa.

Ilkivalta on yleensä jotain näkyvillä olevan sotkemista ja potkimista / kivittämistä säpäleiksi. Perus ilkivallalta suojautuminen tapahtuu valaisemalla alueet hyvin yöaikaan, vaikka liiketunnistinvaloilla ja varustamalla kiinteistö kameravalvontakylteillä. Tästä paremmaksi suojaus saadaan pellittämällä ja metalliverkoilla suojaamalla. Palavien materiaalien säilytys esim. seinien läheisyydessä tai vaikka palavan roskakatoksen sijoitus lähellä lisää riskiä ilkivallalle. Sähkönsyöttö kiinteistöön, varavoima, tietoliikennekaapeloinnit ja varmuuskopiot tulee murtosuojata ja varmistaa että lukitukset toimivat.

Ulkopuoliset valvontatilat on suojattava yleiseltä kululta ja kaikki yhteydet verkkoon on oltava salattuina tai muutoin suojattuina. Murtohälyttimet olisi hyvä varustaa vähintään liikkeentunnistimilla ja ovitunnistimilla. Lisäksi olosuhdevalvonta ja esim. palovaroitin olisi hyvä yhdistää niin että hälytys tulisi päivystäjälle.

Sähköyhtiöllä on oltava pääsy putkilukkojen avaimilla sähkötaululle, samoin kuin puhelinverkon ja kaukolämmön toimittajilla vastaaviin laitteisiin. Vain erikseen sovittavilla erikoisjärjestelyillä on mahdollista muuttaa näitä pääsyjä. On suositeltavaa eriyttää ko. pääsyihin oikeuttavat tilat erikseen.

Konesali on vähintään kahden lukitun oven takana. Murtosuojaus tullaan päivittämään murtopellein, sähköisin lukoin ja varmuuslukoin, kun tarve vaatii.

2.3 **Kulunvalvonta**

Kuka on käynyt? Milloin on käynyt? Miksi on käynyt? Tärkeää on voida jälkikäteen varmistaa, ettei tilassa ole käyty ja käyttää tallentavaa kameravalvontaa ja lokia keräävää hälytysjärjestelmää.

Hyviä käytäntöjä kulunvalvontaan:
- Saattaja, henkilöllisyyden ja toimintaluvan varmistus.
- Dokumentointi, seuranta ja valvonta.
- Yhdellä henkilöllä ei pääsyä perille asti.
- Taustojen selvitys

Tilojen valvonnan suunnittelussa tulee huomioida palotarkastukset ja viranomaisten pääsy, sekä lämpöyhtiöiden, vesilaitoksen ja sähkölaitoksen huoltomiesten kulku.

2.4 **Kameravalvonta**

Kaikki tilat koko konesalin toiminta-alueella tulisi varustaa kameroilla. Kamerat mahdollistavat yhdestä sijainnista valvonnan reaaliajassa kokonaisuudelle. Eri vyöhykkeiden valvontakamerajärjestelmät voi eriyttää omikseen ja jakaa tarvittavilta osin vartiointipalvelujen käyttöön.

Kamerat tulisivat olla valottomassa tilassa toimivia ja varustettu infrapunalla pimeässä kuvausta varten. Kaikki osat tilasta tulisi kattaa mukaan lukien kulkuväylät, jäähdytys, ilmastointi ja varavoimajärjestelmien tilat. Kuvanlaatu tulisi testata, säätää ja tarkastella kriittisesti eri valo- ja sääolosuhteissa.

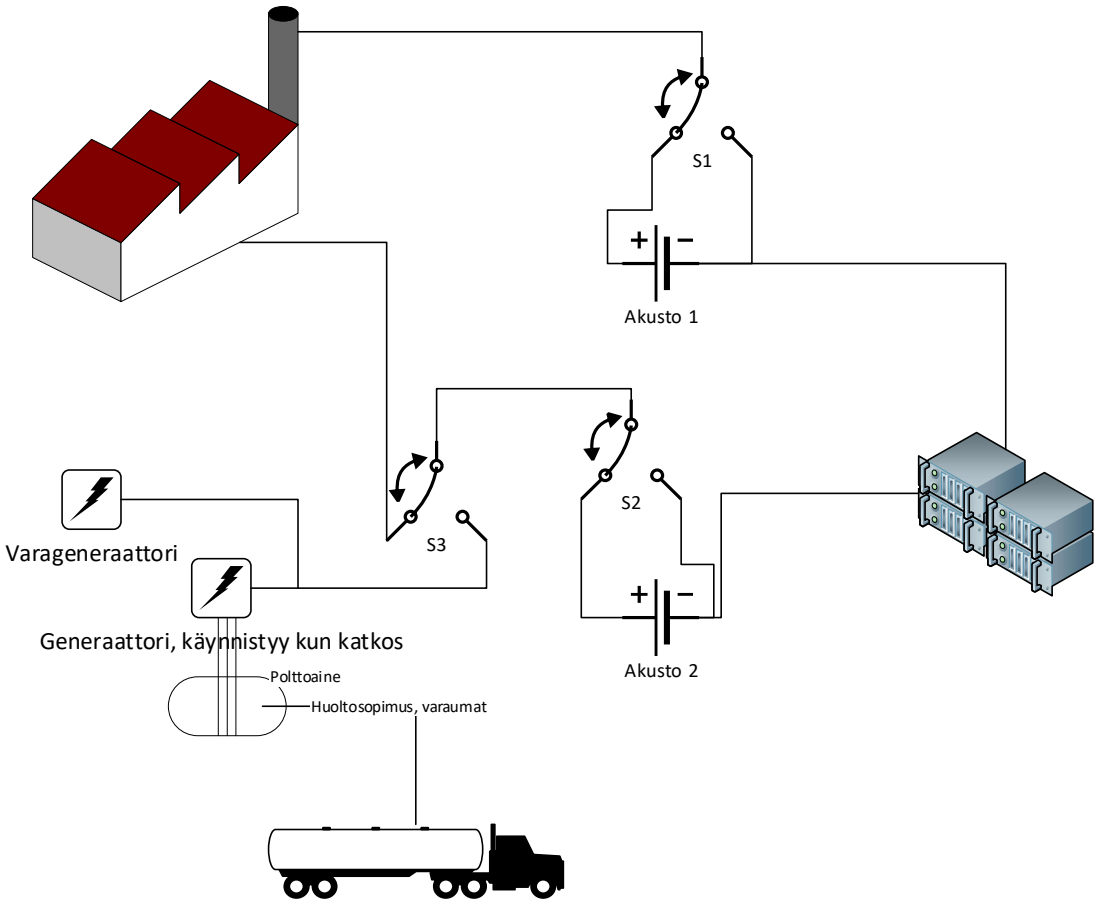
Kameravalvontajärjestelmissä on usein älykkäitä ominaisuuksia, joilla saadaan ilmoitus, kun liikettä tunnistetaan, vaikka sähköpostiin kuvien kera. Konesalien kameravalvonnassa tulee käyttää kokoaikaista tallennusta, jotta voidaan varmistua tarvittaessa jälkeenpäin, ettei kukaan varmasti ole käynyt konesalissa. Kuvaan kannattaa mahduttaa kaikki kulkuväylät saliin ja myös indikaattorit lämpötilalle ja ilmavirralle. Hyvin erottuva villalangan pätkä puhaltimen vieressä on oiva indikaattori ilmavirralle.

Tallennin tulee säilyttää turvallisessa ja palosuojatussa paikassa. Tallenteisiin pääsy tulee rajata ja pääsyä valvoa, vähintään yhtä hyvin kuin mitä tahansa salassa pidettävää materiaalia. Pelkästään näppäimistön käytön tarkastelulla tallenteesta voidaan saada selville salasanat järjestelmiin.

2.5 **Sähkönsyöttö**

Ennen konesalin rakentamista olisi hyvä varmistua tarvittavan tehon saamisesta sijaintiin. Isomman kokoluokan salit sijaitsevat lähellä verkkoa ja omaavat omat muuntamot. Pienemmän konesalin rakentamisessa tulee varmistua sähköpääkeskuksen syöttöjohtojen tarpeeksi isosta mitoituksesta ja maadoituselektrodin riittävyydestä ja olemassaolosta.

Sähkönsyöttö konesalissa tulisi olla kahdennettu, jotta mahdolliset huoltokatkot esim. UPS-laitteille ovat mahdollisia. Esimerkiksi kuvassa 2 molemmat sähkönsyötöt on varustettu akkuvarmennuksella ja ohituskytkimillä. Katkoksen sattuessa voidaan generaattorilla ladata akut ja jatkaa toimintaa. Tarvittaessa akut voidaan ohittaa huoltoja varten.



Kuva 2. Sähköjärjestelmä.

Yksinkertaisimmillaan toinen sähkönsyöttö voi mennä ylijännitesuojauksella verkosta ja toinen akuston kautta. Konesalien kanssa tulisi varmistua riittävän maadoituselektrodin olemassaolosta. Kaikki räkit, kiskot, kytkentärimat ja putket tulisi maadoittaa. Sähköverkon viat voivat olla katkoksia, nollavikoja, taajuuden tai amplitudin muutoksia.

IT-laitteistolle tulisi vetää oma 5-johtiminen nousukaapeli pääkeskukselta. Muut laitteistot kuten jäähdytys, vaativat omat nousukaapelit, sekä tulisi eriyttää omiin ryhmäjohtoihin. (Pietikäinen, 2013) Kriittiset järjestelmät tulisi suojata kaikilta tulojännitteen ongelmilta.

Rakennettava konesali sijaitsee vanhassa liikerakennuksessa ja nousut on mitoitettu sähkölämmitystä ja teollisuuskäyttöä ajatellen. Uusittavaa tulee pääsulakkeiden mitoituksen lisäksi kaapelointi sähkökeskukselta saliin.

2.5.1 Varavoima

Palvelun tarpeen ollessa laajamittaisen sähkökatkoksen aikana tulee järjestelmät varustaa varavoimalla akuston lisäksi. Sähkökatkoksen aikana aggregaatti käynnistää itsensä ja alkaa ladata akustoja hyödyntäen automaattista verkonvaihtokytkintä. Verkonvaihtokytkin täytyy olla varmistetussa virrassa

toiminnan takaamiseksi. Tällöin on erityisen tärkeää erottautua runkoverkosta, jottei aggregaatti aiheuta vaaraa sähköntoimittajan asentajille. Mitoituksessa on hyvä huomioida arkkitehtuurin verkkolaitteet ja palvelimien lisäksi jäähdytys. Palautuminen normaaliin tuotantotilaan olisi hyvä tapahtua automaattisesti. Varavoima tulee testata säännöllisesti ja sen toimivuus kylmissä olosuhteissa tulee varmistaa. Sähkönsyötön laatu täytyy olla kohtuullinen, jotta UPS toimii ongelmitta. Polttoaine vanhenee (hapettuu, haihtuu ja kontaminoituu), jonka takia olisi hyvä ajoittain käyttää aggregaattia, jotta varmistutaan polttoaineen laadusta.

Aggregaatti sijoitetaan yleensä ulkotiloihin. Pakokaasut tulee johtaa pois tiloista, joissa ne voivat aiheuttaa haittaa tai paloriskin. Diesel-aggregaatti tarvitsee paljon ilmaa jäähdytykseen ja toimintaan ja muodostaa usein ainakin käynnistyksessä paljon mustaa savua, joten huomaamaton se ei ole. Aggregaatit konesalikäytössä ovat usein dieseleitä. Myös bensiini ja kaasugeneraattoreita käytetään, riippuen kohteen sijainnista maailmalla. Erityisesti pienet generaattorit ovat usein bensiinikäyttöisiä.

Varavoiman on tarkoitus tulla vanhan betonisen jätekatoksen sisään ja käyttää olemassa olevaa savupiippua pakokaasujen poisjohtamiseen. Tilan ovi korvataan metallisella läpinäkymättömällä verkko-ovella, jotta varmistutaan tarvittavasta ilmansaannista generaattorille. Lisäksi tehdään erillinen tuloilmaputki generaattoria varten. Varavoimajärjestelmä varustetaan hätäsammutuskytkimellä ja paloilmaisimella, joka lauetessaan sammuttaa moottorin. Alkuun varavoima mitoitetaan siirrettävyyden ja ei kiinteään asennukseen ja vain bisneskriittisiin sovellutuksiin.

2.5.2 Akusto

UPS (Uninterruptible Power Supply) säilöö virtaa yleensä 12V akkuihin käytettäväksi tarpeen mukaan. Uusinta tekniikka on käyttää Litium Ioni-akkuja. Akusto tulee mitoittaa joko hallittua alas-ajoa varten, varavoiman käynnistykseen menevän ajan mukaan tai sähkökatkon keston mukaan.

Yleisin UPS työasemalle on Standby –tyyppinen ja pienelle yritykselle Line Interactive. Yli 10kVA järjestelmissä kaksoismuunnos on suosituin. (Rasmussen, 2019)

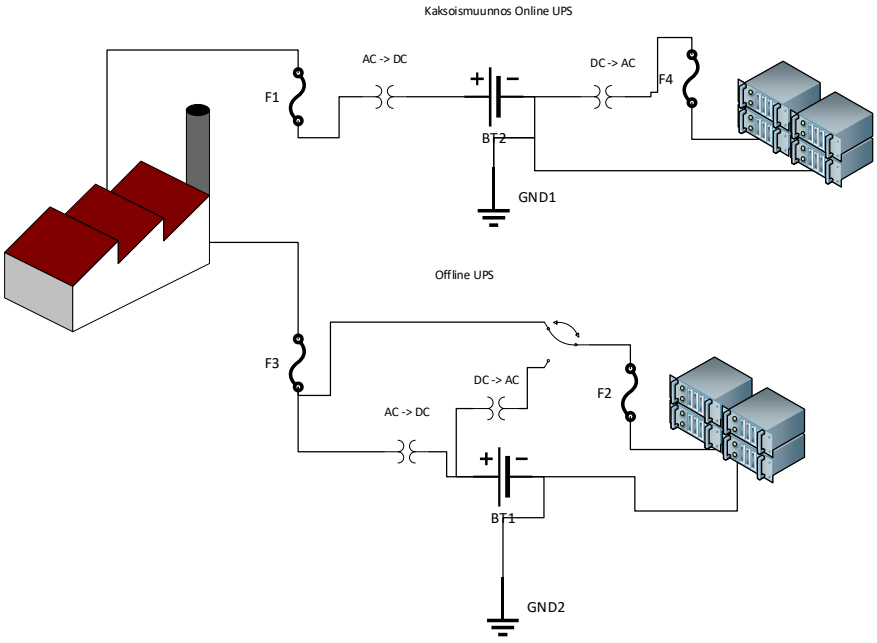
Standby (Off-line) UPS kytkee akuston laitteistoon vasta verkon virran hävitessä siirtokytkimellä ja lataa virran palautuessa akut jälleen täyteen ja palauttaa yhteyden siirtokytkimellä verkkoon, kuten kuvassa 3. Laturi on koko ajan kytkettynä verkkoon.

Line Interactive (Linja-interaktiivinen) UPS on invertterin kautta kytketty aina akustoon ja järjestelmään. Verkkovirran katketessa järjestelmä alkaa automaattisesti syöttämään invertterin kautta virtaa järjestelmään. Se hyödyntää invertterissä OLTC-kytkintä (on load tap changer).

On-line kaksoismuunnos (Double Conversion On-Line) UPS muuttaa verkkovirran tasavirraksi akkuja varten ja invertterilla taas vaihtovirraksi palvelimia varten, kuten kuvassa 3. Laite sisältää ohituskytkimen akustojen huoltoa varten.

Akustolla on mahdollista tehdä hetkellistä huippukulutuksen tasausta. Usein siirtomaksuista osa määräytyy käytetyn huipputehon mukaan. Kun huipputeho on tiedossa etukäteen, voidaan akusto mitoittaa niin että sitä puretaan tässä yhteydessä (Peak Shaving). Akustoon voidaan myös varata aurinkoenergiaa tai tuulienergiaa myöhempää käyttöä varten.

UPS –laitteistojen hankinnassa olisi hyvä kiinnittää myös huomiota mahdolliseen loistehon määrään. Loistehoa voi torjua erillisellä laitteistolla ja se on eriteltynä sähkölaskussa Carunan Tehosiirto -tuotteissa. On-line UPS syö enemmän energiaa jännitteiden jatkuvan muunnoksen takia. Akustot tulisi muistaa huoltaa ja testata, sekä kaikki akuston ohitukset huoltojen yhteydessä tulisi kirjata.



Kuva 3. UPS –esimerkit

Google käyttää väitetysti omissa palvelimissaan sisäänrakennettua 12V akkua ja kaikki jännitteet alle 12V muutetaan emolevyllä. Tällä saavutetaan heidän mukaansa korkeampi hyötysuhde, jopa 99.9%. Keskitetyn ison UPS:n hyötysuhde on yleensä 92-95% (CNET, 2009)

2.5.3 Sulakkeet ja sähkönseuranta

Konesalissa tarvitaan omat sähkötaulut molemmille syötöille. Syötöt on reititetty rakennukseen eri keskuksilta ja eriytettyinä fyysisesti jopa akustojen

osalta. Lisäksi eri vaiheet on hyvä jakaa tasakuormille, jotta vältytään mahdollisten huoltotöiden aikana kuormittamasta yhtä vaihetta liikaa.

Kulutusperusteisessa sähkönlaskutuksessa asiakkailla on omat palvelinkohtaiset tai räkkikohtaiset mittarit ja maksavat PUE-kertoimella (Power Utilization Effectiveness) korotettua maksua sähköstä. Nykyiset sähköyhtiöiden mittarit ovat etäluettavia ja voit helposti katsoa jälkikäteen netistä tuntikohtaiset kulutukset.

2.6 **Jäähdytys ja ilmanvaihto**

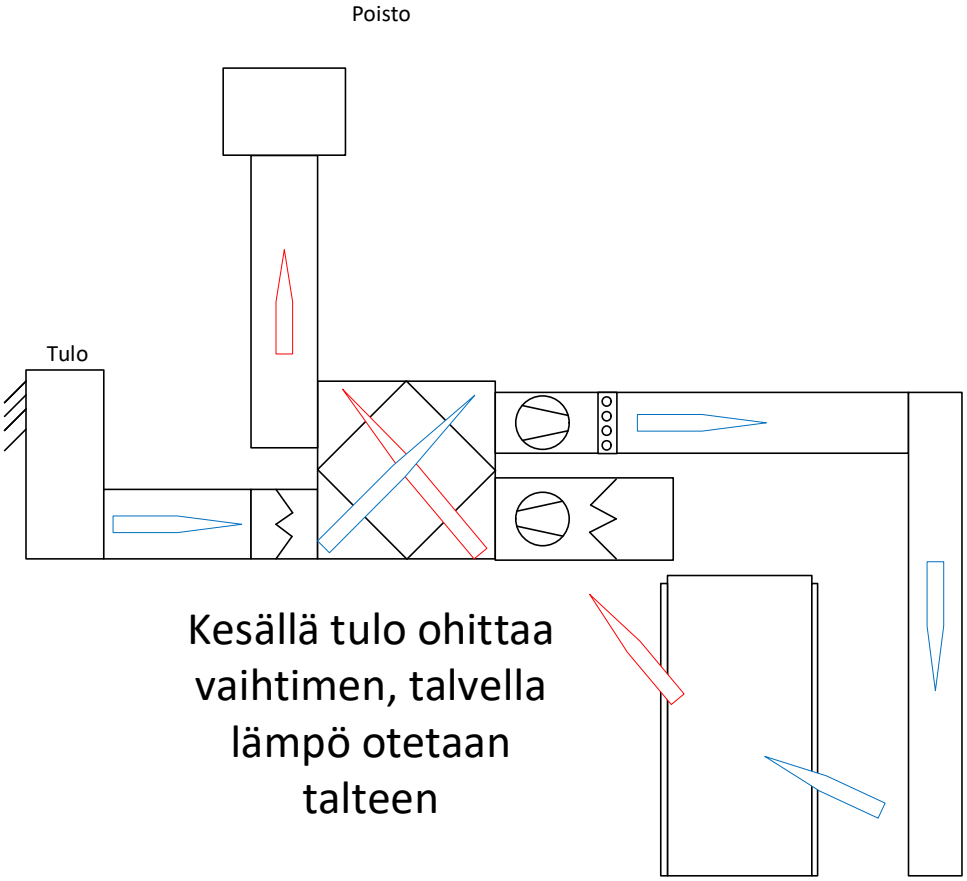
Pienessä laitetilassa riittää yleensä rakenteen ja ilmanvaihdon absorboima lämmönsiirto pois tietoteknisistä laitteista. Konesalien käytössä olevista lämpötiloista ASHRAE 18C-27°C (TIA, 2016) voi havaita, että jo melko pian tulee tarve erilliselle jäähdytyslaitteistolle. Jäähdytysjärjestelmän toiminta tulee varmistaa kahdennuksella ja virransyötön varmistamisella. Lämpötilan hetkellinen nousu lamauttaa konesalin toiminnan hetkessä.

Jäähdytystä voidaan toteuttaa ilmanvaihdolla, lämpöpumpuilla (ilma, maa, ilma-vesi), jäähdytysaltailla ja lämmönvaihtimilla. Perusperiaatteena on, että lämpö siirretään pois joko tuomalla kylmää ilmaa tilalle, siirtämällä lämpö ilmasta toiseen väliaineeseen tai imeyttämällä lämpö rakenteeseen. Konesalissa kaikki tietokoneiden sähkö muuttuu lämmöksi.

Konesalien jäähdytystä toteutetaan yleisten termodynamiikan periaatteiden mukaisesti. Mitä korkeampi on lämpötilaero jäähdytettävän ja lämmitettävän kappaleen / aineen välillä, sitä parempi on lämmön siirtyminen. Konesalissa käytetään kylmä- ja kuumakäytäviä. Ilman sekoittumista näiden välillä estetään yleensä rakenteellisilla ratkaisuilla. Kylmä ilma syötetään laitekaapin etuosasta / alhaalta perforoitujen seinien tai lattian läpi ja poistetaan kuumana laitteiston takapuolelta / katosta.

Korkea lämpötila vaikuttaa komponenttien elinikään. Resistanssi kasvaa suoraan verrannollisesti lämpötilan kasvaessa ja erityisesti kiintolevyjen sisältäessä liikkuvia osia lisätään kitkaa ja kulumista. Myös tuulettimet työskentelevät täydellä teholla ja lisäävät energian kulutusta ja kulumista.

Rakennetussa konesalissa on tarkoitus hyödyntää hukkalämpö rakennuksen ja käyttöveden lämmittämiseen ja ylilämpö ajetaan joko ilma- tai maapiiriin. Tällä hetkellä rakenne imee tuotetun lämmön ja ratkaisu riittää nykyisellä kuormalla. PUE (Power Usage Effectiveness) on 1, kun laitteiston sähkön kulutus on ainoa energiakulu ja rakenne imee lämmön. Talviaikaan -20°C kiinteistön lämmitystarve on 70kW, joten kaikki lämpö voidaan ajaa kiinteistöön. Tällöin hyödyntäen lämmöntalteenottoon vanhaa ristivirtauskennoa, kuten kuvassa 4, saadaan hukkalämmöstä talteen n. 50% lämmittämään kylmää tuloilmaa. Kesäaikaan jäähdytystarve tulee vastaan kovimmilla helteillä, mikäli pyritään <30°C lämpötiloihin salissa.



Kuva 4. Ilmanvaihtolaitteisto.

2.7 Sammutusjärjestelmä ja palosuojaus

Lähtökohtaisesti laitetilat tehdään palamattomiksi. Tulipalo tilassa, jossa ei usein asioida, aiheuttaa isoa vahinkoa. Pelkästään sähköpalon aiheuttama savu voi kiertää laitetilassa kaikkien laitteiden läpi ja kontaminoida järjestelmät.

Savunpoistopuhaltimet yhdistettynä palonilmaisimiin tyhjentävät savun nopeasti salista. Konesaleissa käytetään myös kaasusammutusjärjestelmiä. Esimerkiksi tulipalon sattuessa ilmastointijärjestelmä sammutetaan ja argon kaasu sekoitettuna typpeen vapautetaan ilmaan ja se laskee ilman happipitoisuuden tasolle, jossa tulipalo sammuu. Sammutus on ihmiselle turvallisempi kuin CO2 sammutus.

Valtion Vahti-ohjeistuksen mukaan tiloissa on aina oltava paloilmoituslaitteisto. Palosammutuslaitteisto ja näytteenottoilmaisimet kuuluvat korkeamman suojaustason tiloihin. (Pietikäinen, 2013) Hiilidioksidi käsisammuttimet kuuluvat sähkölaitteita sisältävien tilojen perusvälineistöön, eivätkä saastuta sammutusjauheella kaikkia järjestelmiä.

Laitetilan olisi hyvä kuulua paloluokkaan 1, eli kantava rakenne säilyy palosta huolimatta. Vahtiluokituksissa kerrotaan, että maanalaisten seinien, kattojen

ja lattian tulisi olla teräsbetonia tai vastaavaa materiaalia (Pietikäinen, 2013) ja kestää ylemmän kerroksen sortuma, sekä huonekorkeuden tulisi olla vähintään 2.3m ja alitusten osalta vähintään 2m. Ovien tulisi myös kestää sortuma. Pintojen materiaalien tulisi olla palamattomia. Esimerkiksi keraamisia tai betonisia. Kaikkien läpivientien tulisi olla tiiviitä ja paloturvallisia.

Sähköpalon sattuessa pääkatkaisijalle pääsy on kriittinen. Paikallisemman palon hallintaan olisi hyvä olla pistorasianumerointi ja erilliset sulakkeet, jotta voidaan mahdollisimman pienellä katkoksella sammuttaa vain vialliset järjestelmät. Palvelinsalin ilmanvaihto tulisi olla ylipaineinen eikä siksi palavaan tilaan tule mennä, mikäli se on täynnä savua. Ilmanvaihtojärjestelmän tulisi sammua automaattisesti palon sattuessa ja olla erillään muiden tilojen ilmanvaihdoista.

2.8 **Verkkokaapelointi**

Rakennettavan konesalin maanalaiset valokuidut tulevat talojakamoon operaattorien rimaan, josta ne jatketaan reitittimelle konesaliin. Räkeissä käytetään suojattuja CAT6 –kaapeleita. Konesalin ja toimiston välissä on SM-valokuitu, kytkimissä SFP mini-GBIC kuitumuuntimet. (Small form -factor pluggable transceiver, Gigabit interface converter).

Kaapelikanavat suojataan pellityksillä tai rakennetuilla rakenteilla salin ulkopuolella. Häiriöt minimoidaan reitittämällä verkkokaapelit erikseen sähköverkon komponenteista. Myös huolelliset maadoitukset kaikissa räkeissä ja kaapelitikkaissa pitävät huolen häiriöiden minimoinnista.

2.9 **Dokumentaatio, valvonta ja turvallisuus**

Tietoturvallisen kokonaisuuden hallinta vaatii ajantasaisen ja toimivan dokumentaation. Vain tarpeelliset dokumentit tulee olla fyysisesti käyttöpaikoissa, kuten sähkökaapeissa ja jakamoissa. Laitteet, kytkimet ja pistorasiat tulee merkitä yksilöllisillä tunnuksilla. Seuraavassa listattuna päivittäiselle liiketoiminnalle tarpeelliset dokumentit.

Fyysisen rakenteen dokumentit:

- rakennekuvat
- ilmanvaihto ja jäähdytys
- viemäröinti ja vesiputket
- sammutusjärjestelmä
- sähkökaaviot sulakenumerointeineen

Sähköisen rakenteen dokumentit:

- ohjeistukset varavirran kytkentään
- räkkien sulakenumeroinnit
- yhteystiedot huoltoihin ja polttoaineen toimittajalle
- tietoteknisten rakenteiden dokumentit ja ohjeet

- verkkokuvat
- testausdokumentit ja auditoinnin dokumentit
- ohjekirjat akustoihin ja varavoimaan
- laitteiden huoltokirjat
- listaukset kytkennöistä ja laitteista

Ympärivuorokautinen valvonta voidaan järjestää joko etänä, paikalla tai varalla ollen. Palveluiden kriittisyys ja SLA-palvelutasot (Service Level Agreement) määrittävät vasteajat, joissa palveluiden tulee olla takaisin ylhäällä tai korjaavat toimenpiteet ovat alkaneet. SLA vaikuttaa toteutusratkaisuihin ja niissä voi pahimmillaan muodostua korvausvelvollisuudet asiakasta kohtaan, mikäli palvelutasoa ei saavuteta.

Tietotekninen turvallisuus on iso kokonaisuus. Se lähtee tuotannon järjestelmien päivitystasosta, palomuurien perusasetuksista ja sääntöjen tekemisten ohjeistuksista. Tässäkin least privilege –periaate auttaa, kun henkilöille annetaan oikeudet vain niille välttämättömien palveluiden käyttöön. Tietoteknisessä mielessä on hyvä eriyttää eri palveluita tarjoavat verkot niin, ettei mahdollisen tietovuodon tai yhteyden kautta voi aiheuttaa laajamittaista häiriötä. Työntekijöiden koulutus esim. sosiaalisen hakkeroinnin (Social Engineering) ehkäisyssä on tärkeää. Erilaiset kirjaukset ja hälytykset esim. väärän vuorokaudenaikaan kirjautumisesta järjestelmiin olisi hyvä olla käytössä. Henkilön, joka valvoo palveluiden toimintaa ei tule tietää esimerkiksi ovien lukituskoodeja ja henkilön, joka valvoo huoltokäyntejä ei tule tietää palvelinten salasanoja.

Fyysisten ja sähköisten avainten hallinta tulee olla järjestetty luotettavasti. Kriittiset ovet voidaan varustaa järjestelmällä, jossa vaaditaan kahden eri henkilön läsnäoloa oven avaukseen. Tärkeää on, että muilla kuin järjestelmän suunnittelijoilla on vähiten tietoa kokonaisuudesta.

Luokiteltujen konesalien luokitus tarkistetaan auditoimalla ennen käyttöönottoa. Auditointi on sitä, että ulkopuolinen taho arvioi puolueettomasti tilojen soveltuvuuden käyttötarkoitukseen ja testaa turvallisuusrakenteet. Esim. ”Näyttelee asiakasta ja testaa henkilöstön valmiudet ilman ennakkovaroitusta”. Turvallisuutta voidaan testauttaa käyttäen Red Team -valkohattuhakkereita ja isommat organisaatiot testaavat säännöllisesti toimintaansa käytännössä. Tietovuodoista merkittävä osa on työntekijöiden puuhastelemia.
Nykyisissä hajautetun tiedon pilvipalveluissa on mahdollista rakentaa järjestelmät siten, ettei mikään yksittäinen tietokone vaaranna tietoa. Tietokoneen eri osat on virtualisoitu eri sijainteihin, eikä toimivaa kokonaisuutta saa vetämällä yhtä palvelinta verkosta. Lisäksi levyjärjestelmät on kryptattu.

2.10 **Poikkeustiloihin varautuminen ja testaus**

Disaster Recovery DR, eli hätätilanteesta palautuminen, tarkoittaa luonnon

tai ihmisen aiheuttamien katastrofeihin valmistautumista varten tehtäviä prosesseja, proseduureja ja säännöksiä. (Geng, 2014, s. 641)

High Availibility HA, eli korkea käytettävyys on sopimuksiin perustuvien palvelutasojen toteutuksen lähestymistapa, joka varmistaa toiminnallisuuden sovittuina mittausaikoina. HA on osa järjestelmän suunnitteluprosessia ja siihen liittyvien palveluiden käyttöä. (Geng, 2014, s. 641)

Yleisiä uhkia:

- Broadcast storm, laitteiston broadcast alkaa kiertämään tai ominaisuutta hyödyntämällä ruuhkautetaan verkko.
- Nollapäivä hyökkäykset, tuore haavoittuvuus hyödynnetään ennen valmistajan korjausta.
- Vanhat laitteistot, joiden haavoittuvuuksia ei ole paikattu elinkaaren päättymisen takia.

N+1 varautuminen laitteistovaurioihin, eli jokaista laitetta on N kappaletta ja lisäksi +1 kylmänä erillisessä varastossa. +1 laitteet tulee päivittää samoihin versioihin tuotannon kanssa ja testata pistokokein laitteen vaihto säännöllisin väliajoin.

Poikkeustiloja tulisi testata huoltokatkojen yhteydessä, jotta varmistutaan prosessien toimivuudesta tositilanteessa. Käytäntöjä tulee tarkastella ja kehittää. Yleensä yritys on varustautunut tietoturvaosastolla, joka käy ennalta läpi kaikki muutokset ja verifioi aika ajoin konfiguraatiot.

Kaikki katkokset ja poikkeamat palvelussa dokumentoidaan. Poikkeamat läpikäydään ja muutokset tehdään, jotta mahdollinen poikkeaman aiheuttama haitta jatkossa poistetaan tai minimoidaan. (Valtiovarainministeriö, 2016)

3 LAITTEISTO

Konesalin laitteisto sisältää kulunvalvonnan, kameravalvonnan, sähkönsyöttölaitteiston, jäähdytyslaitteiston, verkkolaitteet, palvelimet ja niiden ohjaukseen käytetyt laitteet sekä mahdolliset sammutuslaitteistot. Erityisen tärkeää konesaleissa on käyttää luotettavia laitteita, jotta varmistutaan siitä, että palvelutaso säilyy, ihmisinterventio ja käynnit konesalissa pysyvät minimissä. Suositeltavaa on käyttää laitteita, joissa on takuu ja huoltosopimukset voimassa.

3.1 Serveriräkki

Räkkikaappi palvelinsalissa on 19” leveä kaappi. Yksi rack unit eli U on 1.75” eli 44.45mm. Peruspalvelin on korkeudeltaan 1U ja levypalvelin 2U. Räkkiä

hankkiessa tulee varmistua riittävästä syvyydestä ja korkeudesta. Räkkipalvelimet ovat yleensä varustettu liukukiskoilla huollettavuuden helpottamiseksi ja siksi kevyissä räkkikaapeissa olisi hyvä olla kaatumisen estävä jalka alhaalla, joka vedetään ulos ennen huoltotoimenpiteitä.

Räkkikaapin asennuksessa olisi hyvä huomioida kaapelointi ja ilman virtaus. Räkkikaapit tulee numeroida ja mikäli ovissa on lukitusmahdollisuus niin asentaa lukot. Kaapelit olisi tarkoituksenmukaista niputtaa ilmavirran ja huollettavuuden takia, käyttäen vaikka tarranauhoja ja kaapeliohjureita. Kaikki kaapelit olisi hyvä merkitä molemmista päistä, jotta minimoidaan ihmisten aiheuttamat ongelmat huoltotoimenpiteiden aikana.

Verkkojen kannalta olisi hyvä asentaa jokaiseen räkkiin omat kytkentärimat, jottei laitteiden lisäyksessä tarvitse kiivetä tikkailla kaapelitikapuille lisäämään kaapelia. Sähköjohdot tulisi merkitä seikkaperäisesti ja varmistua reitityksellä ja rasioiden merkinnällä siitä, että virrat tulisivat oikeasti kahdesta eri paikasta. Tyhjät paikat räkkikaapissa tulisi peittää, jotta kylmä- ja kuumakäytävät toimivat optimaalisesti.

Räkkikaappina konesalissa on myyjän mukaan aikanaan Perel Oy:n äänieristämä Knürr-merkkinen räkkikaappi kattopuhaltimella.

3.2 **Palvelimet**

Konesalikäyttöön tarkoitetut palvelimet on varustettu tavanomaisista koneista poiketen räkkiraudoilla ja niitä ei ole suunniteltu hiljaisiksi tai esteettisiksi. Tavanomaisesti kaikki palvelimet konesaleissa sisältävät HOTSWAP (eli ”kuumana” tai virroissa olevana vaihdettavissa olevat) virtalähteet ja kiintolevyt. Laitetilojen turvallisuuden, jäähdytyksen ja energiatehokkuuden takia pyritään pakkaamaan mahdollisimman pieneen tilaan mahdollisimman paljon laskentatehoa ja kapasiteettia. Tästä johtuen palvelimet on yleensä varustettu vähintään kahdella prosessorilla ja lukuisilla muistikammoilla sekä kiintolevyillä.

Virtualisoinnilla tarkoitetaan ohjelmistona pyöritettävää ”tietokonetta” tai käyttöjärjestelmää. On kokonaan virtualisoituja tietokoneita ja osa käyttää samoja järjestelmätiedostoja muiden virtuaalikoneiden kanssa (Container).

Virtualisointi vaatii omat ominaisuutensa prosessoreilta. Tällaisia ovat esimerkiksi virtuaalikoneiden suorat yhteydet muisteihin ja laiteresursseihin. Lisäksi nykyiset palvelinjärjestelmät mahdollistavat esimerkiksi yhden näytönohjaimen jakamisen monelle eri virtuaalikoneelle.

Bisneskriittisissä järjestelmissä käytetään vain takuunalaisia ja laadukkaita palvelimia. Tästä johtuen verkon kauppapaikoilla Euroopassa on saatavilla paljon käytettyjä 2-3 vuoden ikäisiä laitetta.

Konesalin räkkipalvelimet ostettiin käytettyinä Saksasta. Ne ovat Fujitsu-merkkisiä ja varustettu kaksilla prosessoreilla (2*Intel Xeon E5-2680 v2, 10 ydintä ja 20 säiettä per prosessori), kahdennetuilla virtalähteillä, useilla verkkoporteilla, sekä integroidulla laitteiston ohjausjärjestelmällä ja etäohjelmalla. Niissä on järjestelmä, joka mahdollistaa käytön hieman korkeammassa lämpötilassa.

3.3 **Levytilat ja allokointitavat**

Konesaleissa käytetään tallennustilana paikallista palvelimessa olevaa kiintolevyä ja levyjärjestelmää, johon fyysinen palvelin on yleensä liitetty joko kuidulla tai kuparikaapelilla. Lisäksi olemassa on pilvipalveluna saatavaa tallennustilaa. Varmuuskopiot otetaan pitkäaikaissäilytykseen nauhoille, joko paikallisella nauhatallentimella tai robotilla verkon ylitse. Varmuuskopiot olisi hyvä sijaita fyysisesti muualla tai ainakin eri osassa salia.

Palvelimissa käytetään suorituskyvyn ja turvallisuuden takia levyjärjestelmiä. Yleinen tapa toteuttaa levyjärjestelmä on RAID:n käyttö. (Redundant Array of Independent Disks). Yksinkertaisin RAID1 (mirroring) säilyttää kahdella eri levyllä samat tiedot ja toisen levyn vikaantuessa vaihdetaan ehjä tilalle ja synkronoidaan datat ilman tiedostojen häviämistä. RAID0 (striping) lisää suorituskykyä jakamalla datat kahdelle eri levylle, mutta toisen rikkoutuessa data vaurioituu. Erilliset varmuuskopiot ovat tärkeitä sen takia, että on olemassa todennäköisyys monen levyn rikkoutumiselle samanaikaisesti, tai RAID-ohjainlaitteiston vioittumiselle.

Rakennettavan palvelinjärjestelmän levyjärjestelmä toteutetaan Ceph:llä ja paikallisella levyllä RAID:ssa. Ceph on hajautettu ”verkkolevy”-ohjelmisto, jolla on mahdollista varmistaa datan saatavuus palvelinympäristössä ja lisätä suorituskykyä. (Ceph, 2019) Esimerkiksi palvelimen rikkoutuessa virtuaalipalvelinten virtuaalisten levyjen tiedot ovat saatavilla muilla palvelimilla ja virtuaalipalvelin käynnistyy hetkessä takaisin toiselle alustalle.

3.4 **Verkkolaitteet**

Palvelinsaleissa käytetään yleensä kytkinlaitteita, joissa on kaksi virtalähdettä ja mahdollisuus käyttää varmennettua yhteyttä (Link Aggregation, verkkolinkkien yhdistäminen, esim. LACP). Verkkolaitteet tulisi erottaa erillisiin kaappeihin toiminnan varmistamiseksi.

Palomuurit palvelinsalin verkossa ovat fyysisiä, virtualisoituja tai ohjelmistoja. Palomuureissakin tulisi pyrkiä ratkaisuihin, joilla yhteydet jatkavat toimintaansa yhden kaapelin irrotessa tai vaurioituessa tai yhteyskatkoksessa. Jotkin fyysiset palomuurit mahdollistavat kahdentamisen kahdelle erilliselle laitteelle. Reititin / reitittimet tulisi määritellä käyttämään useampia yhteyksiä mahdollisten vikatilanteiden takia.

Mediamuuntimet muuttavat valokuidusta tulevat laservalot verkkokaapeleihin sopiviksi sähköpulsseiksi. Mediamuuntimia on erilaisia: integroitu verkkolaitteeseen, erillinen moduuli (esim. mini-GBIC SFP) ja erillinen mediamuunnin (esim. 1510nm SM –> 1000/1000 ethernet).

Palvelinsalissamme käytämme yhteyden osalta operaattorin reitittimestä tulevaa suojattua CAT6-verkkokaapelia, kytkinten välissä valokuituja ja muutoin suojattuja CAT 6-verkkokaapeleita. Palomuurina on toistaiseksi Zyxel –merkkinen laite ja kytkinten osalta käytetään HP:n laitteita.

4 OHJELMISTOT JA PALVELUT

Toimiva konesali sisältää lukuisia erilaisia ohjelmistoja ja palveluita. Nykyisin toimitetaan ohjelmistoa asiakkaille palveluna SaaS (Software as a Service), järjestelmää palveluna IaaS (Infrastructure as a Service) ja alustoja palveluna PaaS (Platform as a service).

4.1 Virtualisointialusta

Virtualisointialusta, eli hypervisor on ohjelmisto, joka pyörii pohjalla olevan käyttöjärjestelmän päällä ja allokoi fyysisiä ja virtuaalisia resursseja virtuaalipalvelimille. Käyttöjärjestelmänä tässä järjestelmässä on Ubuntu, jonka päällä pyörii Proxmox VE -ohjelmisto. Proxmox VE muodostuu KVM-hypervisorista, LXC-containereista, ohjelmistollisesta tallennusjärjestelmästä ja verkkotoiminnoista alustalla. (Proxmox, n.d) Järjestelmä hyödyntää palvelinprosessorien Vt-x tukea virtualisointiin. Intel Vt-x antaa virtuaalikoneen ajaa komentoja suoraan prosessorilla niin että virtuaalikoneelle suoritin näyttäytyy omana suorittimena. Lisäksi Vt-d mahdollistaa fyysisten resurssien ohjauksen suoraan virtuaalikoneelle, esim. erillinen näytönohjain CAD-työskentelyyn vain yhteen virtuaalikoneeseen.

Virtualisointialustan hallintasivulta on helppo allokoida lisää resursseja yksittäiselle virtuaalipalvelimelle, valvoa niiden toimintaa ja kuormaa sekä aikatauluttaa erilaisten palveluiden käytettävyyttä. Myös ylläpitotehtävät ilman katkoksia bisnesaikaan ovat mahdollisia.

4.2 Laiteohjelmistot

Firmwaret, eli laiteohjelmistot, ovat laitteen ohjelmia, joilla hallitaan laitteiden toimintaa ja ominaisuuksia. Uusimmat laiteohjelmistot on hyvä jakaa hallintaverkossa SFTP-palvelimen kautta (SSH File Transfer Protocol) ja samaa palvelinta voidaan hyödyntää myös määritystiedostojen varmuuskopiointiin laiterikon varalta. Laiteohjelmistojen ajantasaisuus on tärkeää, jotta niiden toiminta on laitevalmistajan tarkoittamaa ja tietoturva pysyy yllä.

Järjestelmän palvelimien levyohjainten ja emolevyjen laiteohjelmistot täytyi päivittää. Päivitys tapahtui USB –tikun kautta. Myös palomuurit ja kytkimet päivitettiin ohjelmistojen osalta ennen määritystä.

4.3 **Tarvittavat palvelut**

DNS-nimipalvelimet kertovat verkkonimen / osoitteen oikeaan IP-osoitteeseen tai nimeen / domainiin. Palomuuri olisi hyvä olla liikenteen perussuodatusta varten, jolloin jo ensimmäisessä rajapinnassa voidaan estää haitallinen liikenne. Lisäksi voi olla tarpeen käyttää virustorjuntaa ja sähköpostisuodatusta jo palomuurissa. Palomuurit mahdollistavat erilaiset etäkäytöt asiakkaiden omiin sisäverkkoihin (esim. VPN tai IP-osoitteen salliminen). Roskapostitus tulee estää ja useilla operaattoreilla lähtevien postien määrä per aikaväli on rajoitettu.

Seuraavat palvelut olisi hyvä olla:

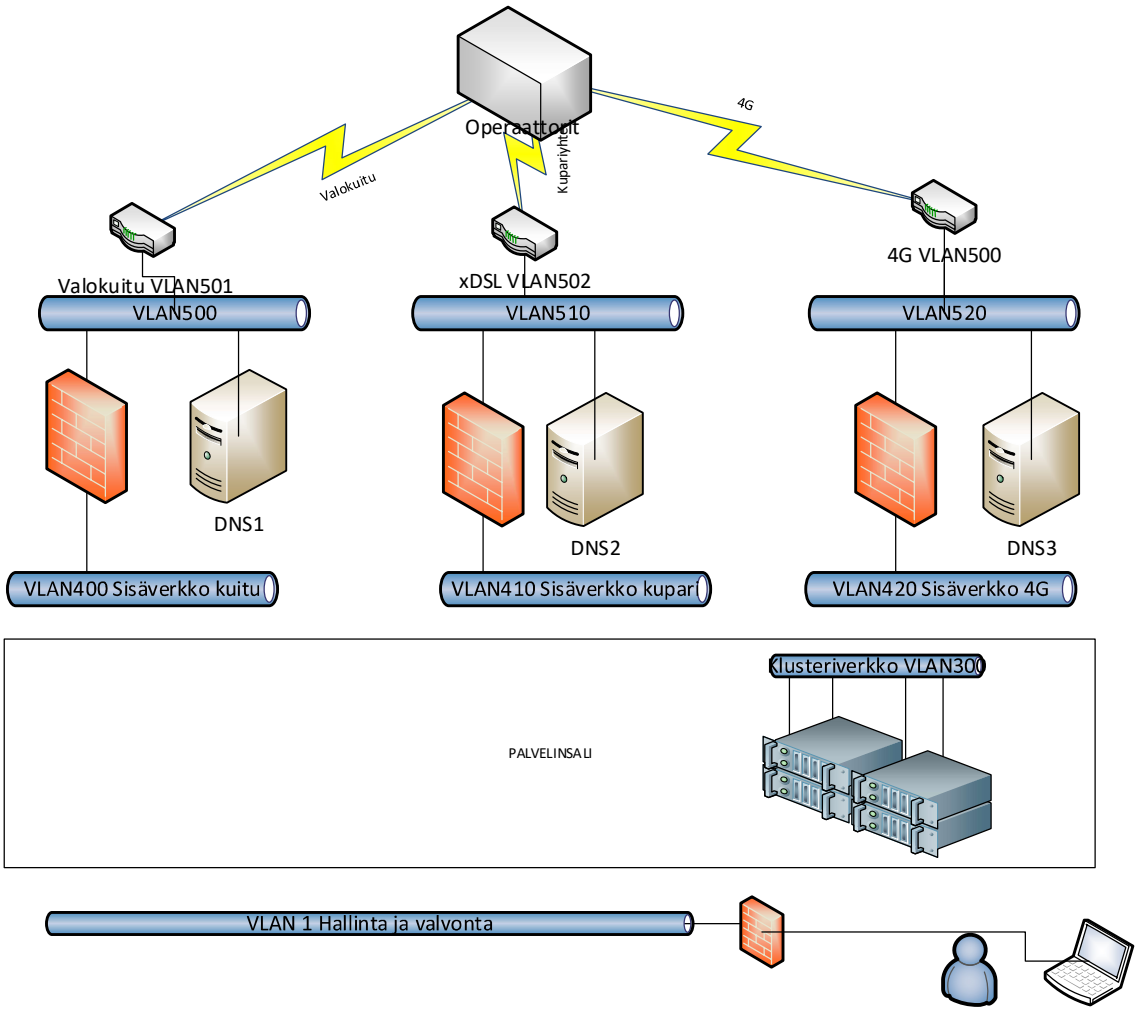
- Reititys
- Apache2, jossa MySQL, PHP-tuki, sekä tietokantojen hallintajärjestelmä phpMyADmin
- SFTP –palvelin, johon käyttöoikeudet rajatusti asiakkaille ja sisäiseen käyttöön.
- Sähköpostijärjestelmä
- Varmuuskopiointijärjestelmä
- Levyjärjestelmä
- Verkon valvonta
- CRM, Asiakassuhteiden hallinta (Customer relations management)
- ERP, Toiminnanohjaus (Enterprise Resource Management)
- Laskutusjärjestelmä

5 **VERKOT**

Verkkojen eriytys virtuaalisesti niin, etteivät laitteet näe toisiaan verkossa, tehdään VLAN:lla (Virtual Lan 802.1q) ja QinQ:lla (VLAN paketti toisen VLAN sisässä 802.1ad). VLAN lisää tagin verkkopaketin kehykseen, jossa kerrotaan verkkolaitteelle paketin kuuluvan tiettyyn virtuaaliseen verkkoon. Kytkinten välissä menee nk. trunk-portit, jotka mahdollistavat VLAN-informaation siirtämisen kytkinten välillä. Kun kehys ohjataan access-porttiin, niin tagi poistetaan. Toinen tapa liikuttaa L2-tasolla tietoa verkosta toiseen on soveltuva VPN-yhteys.

Kuten kuvasta 5 käy ilmi, tuodaan ulkoverkkojen yhteydet jostain verkon osasta sisään ja eriytetään ne VLAN:lla käyttöpaikkoihin. Palomuurin jälkeen käytetään joko suoraan julkisia osoitteita tai sitten lähiverkon IP-osoitteita.

Samaan julkiseen IP-osoitteeseen voidaan palomuurin porttiohjaus määrityksillä tehdä lukuisia ohjauksia eri sisäverkon IP-osoitteisiin ja jokaisessa sisä- tai ulkoverkon osoitteessa voi olla monta eri nimiohjausta. Esim. Sama palvelin vastaa samasta IP-osoitteesta eri domaineihin kohdistuviin pyyntöihin erilaisilla vastauksilla. Käytettäessä virtuaalisia verkkorakenteita, tulee tarkastella porttien liikennemääriä ja tarvittaessa lisätä kaistaa laitteiden väliin.



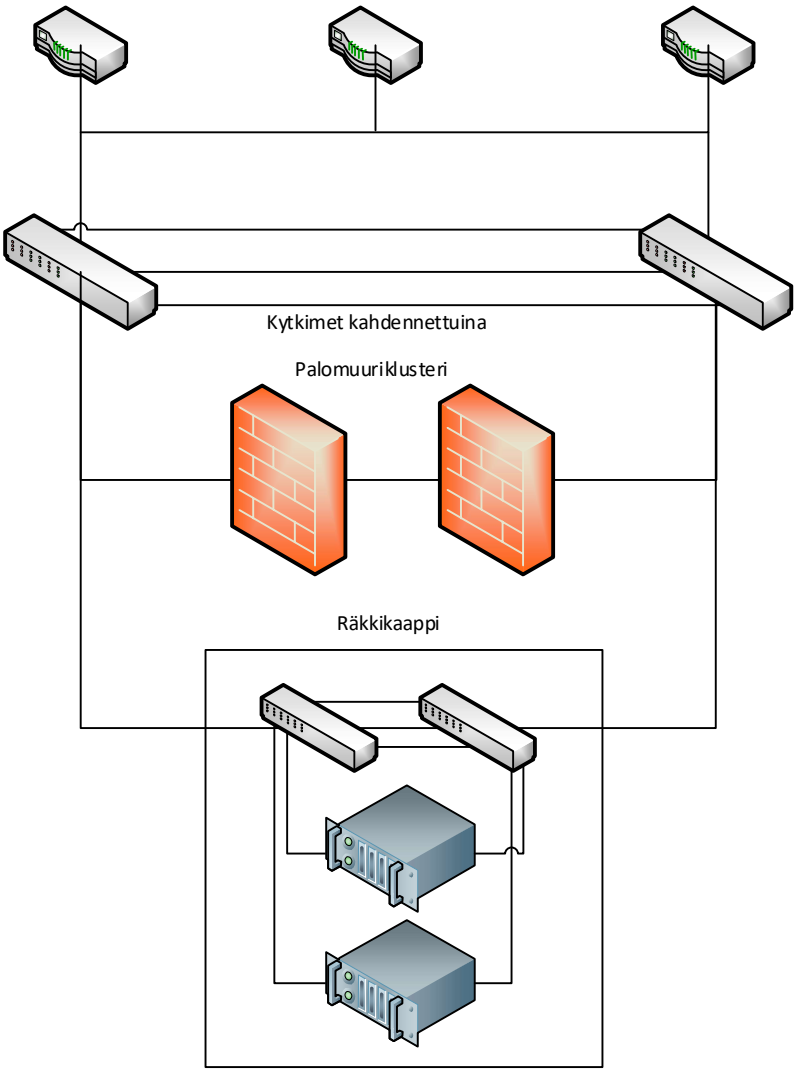
Kuva 5. Looginen topologia

Lisäksi verkkoja voi yhdistää toisten laitteiden lävitse reititystaulujen avulla hyödyntäen reitityssääntöjä. Tällöin kehyksen MAC-tieto häviää eikä kyseessä ole enää normaali puhdas L2 lähiverkko toiminnallisuuden puitteissa.

Fyysinen eriytys tehdään tekemällä kaapelien reititys niin, että ne eivät mene samoja reittejä pitkin ja samoihin portteihin ja voidaan jopa hyödyntää erillisiä verkkolaitteita. Reititystaulussa voidaan määrittää käyttäjällä reittien painoarvoilla (weight) missä tilanteissa käytetään mitäkin reittiä.

Verkon kahdentamisessa otetaan kaikkia verkon tarpeellisia laitteita kaksi kappaletta ja määritellään ne niin että mahdollisessa vikatilanteessa toinen laite ottaa toisen toiminnallisuuden kokonaisuudessaan hoitaakseen, kuten

kuvassa 6 esitetään. Kahdentamista on mahdollista tehdä myös niin että toinen laite on varalla ja aktivoituu vasta tarpeen vaatiessa. Kytkimissä käytetään Spanning Tree –protokolla (STP) tai sen uudempaa versiota Rapid Spanning Tree (RSTP). STP estää looppien synnyn luomalla Root Bridgen. Lisäksi on mahdollista yhdistää useampi verkkokaapeli laitteiden välissä yhdeksi virtuaaliseksi verkkoportiksi linkkien yhdistämisellä (link aggregation), jolloin saadaan lisää suorituskykyä tai suojaudutaan toisen kaapelin katkeamiselta.



Kuva 6. Fyysinen topologia

Verkkojen varmistaminen on mahdollista toteuttaa varayhteyden kautta, jolloin vikatilanteessa yhteys operaattorille siirtyy käyttämään esimerkiksi 4G-reititintä tai toista kuitua.

Kaikki kriittiset yhteydet ja konfiguroinnit tulee testata ja dokumentoida, jotta voidaan varmistua niiden toimivuudesta tositilanteessa ja ettei verkkokaapelin irtoaminen aiheuta ongelmaa tuotannossa. Erityisesti toimipisteiden välisissä linkeissä tulee varmistua yhteyden laadusta tarkistamalla porttivirheiden määrä ja testaamalla viive, sekä miten paketit löytävät perille.

Hyvä käytäntö on käyttää aina uusia verkkokaapeleita kaikissa liiketoiminta-kriittisissä operaatioissa, jottei mahdollisissa asennus / purkuvaiheissa vaurioituneen kaapelin uudelleenkäytön aiheuttamiin ongelmiin mene työtunteja hukkaan. Kaapelit ja valokuidut ovat fyysisiä materiaaleja ja venyvät ja taipuvat sekä kuluvat eristeiden ja muovien kuivumisessa ja puristuksissa ollessaan ja voivat aiheuttaa kaikenlaisia pienempiä häiriöitä lämpötilojen ja asentojen mukaan. Kaapelien hinta on minimaalinen verrattuna vianetsinnän hintaan.

Hallintaverkkoa käytetään järjestelmien ohjaukseen, valvontaan ja konfigurointiin. Palvelinten suorituskyvyn ja fyysisen kunnon tarkastelu ja hallinta mahdollistavat ennakoivat korjaukset pullonkaulojen ja vikaantumisten ehkäisyssä. Hälytykset ja valvonnat kannattaa automatisoida ja valvontaverkossa oman kokemuksen mukaan on hyödyllistä olla linjavalvonnat eri toimipisteiden välille, jossa näkyy ns. kartta siitä, miten kohteiden väliset yhteydet toimivat. Yhdellä vilkaisulla nähdään missä on ongelma ja voidaan ryhtyä vähentämään ongelman aiheuttamaa haittaa.

Hallintaverkoissa suoritetaan yleensä järjestelmän eri laitteiden kunnon valvontaa ICMP- ja SNMP- ja syslog -valvonnoilla. Näin saadaan nopeasti tieto mahdollisista katkoksista ja vikaantumisista, sekä ruuhkatilanteista esimerkiksi DDOS-palvelunestohyökkäyksen tapahtuessa.

Hallintaverkko toteutetaan omana VLAN-verkkona kytkinten ja muiden verkkolaitteiden läpi tai kokonaan erillisenä verkkona. Hallintaverkkoon otetaan yhteys nk. eteistietokoneen kautta, johon on erittäin rajattu pääsy ja valvonta lokien kera.

Olemassa voi olla myös nk. ylläpito-verkko, jonka kautta suoritetaan varmuuskopioinnit ja mm. kytkinten konfigurointien ja firmwaren päivitykset. Hallintaverkossa on usein esim. tekstiviestihälytys siltä varalta, että viestintäyhteydet ovat kokonaan poikki. Tämän laitteen osalta on suositeltavaa käyttää toisen palveluntarjoajan liittymää. Isommissa kokonaisuuksissa voi olla järkevää luoda useampia hallintaverkkoja vikasietoisuuden lisäämiseksi.

5.1 **Ulkoverkko**

Julkinen verkko toteutetaan usean eri operaattorin yhteyksillä, jotka voidaan jakaa monelle eri fyysiselle ja virtuaaliselle palomuurille kahdennettujen kytkinten kautta VLAN-verkoissa. Verkkopalveluiden tavoitettavuus vikatilanteessa varmistetaan DNS, eli nimipalveluiden oikealla konfiguraatiolla (eri IP-blokeista ja operaattoreilta). Fyysisesti nimipalvelinten tulee olla vähintään kahden eri Internet-yhteyden takana, eri palvelinlaitteilla ja eri IP-osoitteissa. (Liikenne- ja viestintävirasto, 2019)

Isojen konesalien yhteydessä on usein käytännön syistä johtuen omat ISP-palvelut ja yhteydet. ISP:n tulee olla vähintään kahteen eri TRUNK-yhteyteen

kytkeytyneenä vähintään kahdella eri AS-nimikkeen omaavalla reitittimellä. Sen lisäksi konesaleissa on usein mahdollista ostaa myös muilta operaattoreilta kaistaa. Vaihdantaliikenne maksaa operaattorille ja sen takia operaattorilla on usein oma laite lähimmässä liikenteenvaihtopisteessä.

Kuiturinki on kaksi kuitua, joista esim. toinen on varalla tai jakamassa kuormaa ja tulee fyysisesti eri reittiä, vikatilanteessa käytetään vain toista. Tällä vältetään yhden paikan haavoittuvuus eli SPOF (single point of failure).

Konesaliin tulee tällä hetkellä kuituyhteys (nopeus nyt 50/10), xDSL kupariyhteys (nopeus nyt 24/3) ja 4G yhteys 100M (toteutuva n. 50/10). Kaikki yhteydet tulee olla staattisilla muuttumattomilla IP-osoitteilla, ilman operaattorien palomuuripalveluita, jotta nimipalveluiden ja porttien toimivuus varmistetaan.

5.2 **Sisäverkko**

Erilaisissa tietokonejärjestelmissä on luotettavaan tiedonsiirtoon laitteiden välille tarpeen olla myös ulkoverkkoon näkymätön verkko, sisäverkko. Sisäverkko on konesalissa palvelinten / asiakkaiden välinen verkko, jossa vaihdetaan saman verkon tietoja. Yleinen toteutustapa on yhdistää konesalin levypalvelin VPN –yhteydellä (Virtual Private Network) yrityksen toimipisteeseen. Pienissä yrityksissä lokaaliin palvelimeen yhdistetään toimistojen välisiä yhteyksiä hyödyntäen. Tämä voi kuitenkin ruuhkauttaa päätoimipisteen yhteyden ja lisäksi ylläpito ja laitteiden tavoitettavuus voi olla ongelmallista vikatilanteessa. Kun levypalvelin on konesalissa ja järjestelmät on oikein rakennettu, käyttäjän on vaikea hahmottaa, onko palvelin toimistossa vai muualla. Selkeimpänä hyötynä on yleisesti konesalien paremman yhteydet verkkoon ja esimerkiksi tietoliikennekatkoksessa viiveet korjaukseen ovat paljon pienemmät.

Isommissa järjestelmissä kaikki liikenne ajetaan ja suodatetaan keskitetysti yhden ison palomuurijärjestelmän kautta ja mm. valvonta kaikille laitteille on keskitetty konesalin puolelle.

5.3 **Etäyhteydet**

Yhteydet toimistoilta konesaliin toteutetaan useimmiten VPN –yhteyksillä. Toinen yleinen vaihtoehto on operaattorin MPLS –yhteys (Multiprotocol Label Switching), jossa hyödyntäen eri verkkotekniikoita luodaan yhteydet toimipisteiden välille.

On mahdollista yhdistää toimipisteitä suoraan esim. valokuituyhteyksillä. Tällöin voidaan etäisyyden ollessa sopiva ajaa yhteen SM-kuitupariin kymmeniä gigabittejä dataa sekunnissa käyttäen eri aallonpituuksiin vaikka passiivista WDM:ää. (Wavelength-division multiplexing).

6 YHTEENVETO

Opinnäytetyön tarkoituksena oli saada suunniteltua ja rakennettua konesali yritykselle peruskäyttöön omaan liiketoimintaan ja käydä läpi perustasolla asiat. Konesali on tällä hetkellä esitestausvaiheessa ja ennen viimeisten rakennusvaiheiden läpimenoa tarkastellaan kriittisesti millä tasolla asioita toteutetaan ja mitkä järjestelmäkomponentit toteutetaan milläkin ohjelmistolla tai raudalla. Projekti kokonaisuudessaan on ollut pitkäkestoinen ja edennyt verkkaisesti ja vähän joka askelta varmistellen. Ongelmana on ollut tarvittavan ajan järjestäminen ja erinäiset hankintaerät liittyen projektiin. Verkot ja looginen kokonaisuus on suunniteltu valmiiksi, sekä pohjakuvat ja ilmanvaihdot alustavasti.

Konesalien rakentaminen oikein alusta alkaen omasta kokemuksesta edellyttää jonkinlaisia pohjatietoja vaatimuksista. On mahdotonta tehdä luokitukset täyttävää tilaa esimerkiksi sellaiseen paikkaan, jonka rakenne ei kestä tarvittavia muutostöitä tai mihin on mahdotonta rakentaa sähkö- / varavoima- / jäähdytysinfrastruktuuria. Nuorelle yritykselle on tärkeää päästä kokeilemaan nopeasti mitä mahdollisuuksia liiketoiminnalle oman laitetilan käyttö mahdollistaa.

Suomessa konesalin pyörittämisen huonoja puolia vaikuttaisi olevan sähkön siirtohinta ja isojen energiamäärien perusmaksut. Energia itsessään on parhaimmillaan Euroopan edullisimpien joukossa. Poliittinen ilmapiiri ja hyvät tietoliikenneyhteydet mahdollistavat vapaan ja luotettavan alustan testata erilaisia toteutuksia ja antaa mahdollisuuden tarjota palveluita myös ulkomaille. Ilmasto on sopivan leuto ja muutamia kuukausia lukuun ottamatta jäähdytysenergia voidaan hyödyntää lähes kokonaisuudessaan muihin energiamuotoihin, kuten esim. lämmitykseen. Tässäkin salissa alkuvaiheen testausten lämpö häviää hienosti rakenteisiin.

Rakennettaessa ketterillä menetelmillä testiversiota, vaikuttaisi korostuvan tarve sille, että alustavasti on tiedossa hahmotelma isommasta kokonaisuudesta. Väärät investoinnit aiheuttavat turhaa rahanmenoa ja hankittaessa uutta laitteistoa, vaikkapa väärän merkkisenä, vaikeuttaa niiden myyntiä huomattavasti.

Opinnäytetyötä kirjoittaessa suurin osa tekstistä tuntui syntyvän ihan omien kokemusten pohjalta. Olen ollut töissä yrityksessä, joka rakensi luokitellun konesalin, sekä ollut tekemisissä muutamien konesalien omistajien kanssa.

Mikäli asioissa olisi työmäärällisesti ollut mahdollista paneutua seikkaperäisemmin jokaiseen osa-alueeseen, niin olisi täytynyt käyttää huomattavasti enemmän lähteitä ja opiskella tuhansia sivuja. Pelkästään yhdestä tämän opinnäytetyön osa-alueesta saisi jo itsessään tehtyä monta opinnäytettä.

Kokonaisuuden rakentaminen alusta loppuun vaatii vuosien kehittämisen, mikäli aikoo toteuttaa kaiken yksin. On täysin eri asia rakentaa pelkkä tila tai toimittaa pelkkä rauta tai määrittää tietoliikenneyhteydet tai vuokrata virtuaalipalvelin ja käyttää sitä. Tärkein ylläpidollisesti on tietää olennainen kaikista palveluista ja osata paikantaa ongelmat nopeasti, tehden tietoon perustuvat toimenpiteet. Kaikenlainen testailu ei kuulu tuotantokäytössä oleviin järjestelmiin.

Kustannuksiksi pieneen konesaliin, josta myydään asiakkaille tilaa arvioisin n. 3000€/kk. Tietoliikenneyhteydet 1000€/kk (hyvästä sijainnista), sähkö 800-1000€/kk jäähdytyksen kanssa ja laitteisto 1000€/kk järkevillä rahoitusajoilla. Tällaisella sijoituksella saa jo merkittävästi virtuaalisia palvelimia olemassa olevista saleista tai pilvestä. Arvioni mukaan tällaisen sijoituksen nollapiste olisi n. 30 asiakaspalvelinta, mikäli tarjottaisiin vain tilaa ja yhteyksiä. Lisämahdollisuuksia voisi tuoda operaattorina toimiminen lähialueen kiinteistöihin. Tämä toisi infrastruktuuriin lisäkuluja tarvittavien yhteyksien yms. osalta ainakin 1000€/kk + kuitujen asennus ja kaivuukulut talojen väliin. Tästä pikaisesta laskelmasta voi päätellä, kuinka vaikeaa on nollasta rakentaa ilman valmiita asiakassuhteita uudelle yritykselle infraa niin, että siitä ei maksaisi mitään palkkaa, saati toiminta olisi muuten kannattavaa. Tähän vielä päälle mahdolliset vuokrat tai muut kiinteistön kulut. Kaikenlainen rakentaminen edellyttää aina pitkäaikaista sitoutumista hankkeeseen.

Opinnäytetyöprosessi sujui kokonaisuudessaan hyvin ja projektissa saavutettiin hankkeen testausvaihetta varten toimiva kokonaisuus. Nyt yritys voi alkaa rakentamaan tarvittavia palveluita, jotka voi siirtää toimivaan kokonaisuuteen sellaisenaan.

7 LÄHDELUETTELO

Ceph. (n.d). Ceph Storage. Haettu 31.1.2019 https://ceph.com/ceph-storage/

CNET. (11.12.2009). Google uncloaks once-secret server. Haettu 31.1.2019 https://www.cnet.com/news/google-uncloaks-once-secret-server-10209580/

Geng, H. (2014). Data Center Handbook. John Wiley & Sons, Incorporated.

Liikenne- ja viestintävirasto. (21.12.2018). Verkkotunnusvälittäjän opas. Haettu 31.1.2019 https://www.traficom.fi/sites/default/files/media/file/Verkkotunnusvalittajan-opas.pdf

Pietikäinen, S. (5.6.2013). Vahtiohje.fi. Liite 4. Tietoteknisten laitetilojen turvallisuussuositukset. Haettu 31.1.2019 https://www.vahtiohje.fi/web/guest/666

Proxmox. (n.d). Proxmox homepage, virtualization. Haettu 31.1.2019 https://www.proxmox.com/en/proxmox-ve

Rasmussen, N. (2011). apc.com. Different Types of UPS Systems. Haettu 31.1.2019 https://www.apc.com/salestools/SADE-5TNM3Y/SADE-5TNM3Y_R7_EN.pdf

TIA. (16.4.2016). Telecommunications Pathways and Spaces. ANSI/TIA-569-D.

Valtiovarainministeriö. (7.6.2016). Vahtiohje.fi. Toiminnan jatkuvuuden hallinta. Haettu 31.1.2019 https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229