TALLINNA TEHNIKAÜLIKOOL
INSENERITEADUSKOND
Virumaa kolledž

Andmekeskuse projekteerimine TIER 3 tasemele Astrec Data OÜ näitel

Designing a TIER 3 data center based on the example of Astrec Data OÜ

TELEMAATIKA JA ARUKATE SÜSTEEMIDE ÕPPEKAVA LÕPUTÖÖ

Üliõpilane: Vladimir Moskaljov
Üliõpilaskood: 193085EDTR
Juhendaja: Larissa Joonas, lektor

Kohtla-Järve, 2023

AUTORIDEKLARATSIOON

Olen koostanud lõputöö iseseisvalt.

Lõputöö alusel ei ole varem kutse- või teaduskraadi või inseneridiplomit taotletud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

".... " ..... 20..... .

Autor: .....

/ allkiri /

Töö vastab rakenduskõrgharidusõppe lõputööle/magistritööle esitatud nõuetele "... "
..... 20..... .

Juhendaja: .....

/ allkiri /

Kaitsmisele lubatud ".... " ..... 20..... .

Kaitsmiskomisjoni esimees .....

/ nimi ja allkiri /

LIHTLITSENTS LÕPUTÖÖ ÜLDSUSELE KÄTTESAADAVAKS TEGEMISEKS JA REPRODUTSEERIMISEKS

Mina Vladimir Moskaljov (sünnikuupäev: 26.10.1997)

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose Andmekeskuse projekteerimine TIER 3 tasemele Astrec Data OÜ näitel mille juhendaja on Larissa Joonas,

1.1. reprodutseerimiseks säilitamise ja elektroonilise avaldamise eesmärgil, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta kolmandate isikute intellektuaalomandi ega isikuandmete kaitse seadusest ja teistest õigusaktidest tulenevaid õigusi.

TalTech Inseneriteaduskond Virumaa kolledž

LÕPUTÖÖ ÜLESANNE

Üliõpilane: Vladimir Moskaljov, 193085EDTR

Õppekava, peaeriala: EDTR17/18 - Telemaatika ja arukad süsteemid
Juhendaja(d): lektor, Larissa Joonas, larissa.joonas@taltech.ee

Lõputöö teema:

(eesti keeles) Andmekeskuse projekteerimine TIER 3 tasemele Astrec Data OÜ näitel

(inglise keeles) Designing a TIER 3 data center based on the example of Astrec Data OÜ

Lõputöö põhieesmärgid:

Diplomitöö eesmärgiks on projekteerida TIER 3 andmekeskus, analüüsida ohte ja hinnata andmekeskuse usaldusväärsust Astrec Data OÜ näitel.

Lõputöö etapid ja ajakava:

Nr	Ülesande kirjeldus	Tähtaeg
1.	Uurimus andmekeskuste tööpõhimõtete ja usaldusväärsuse ning tõrkekindluse tagamise kohta.	09.11.22
2.	Turvalisuse põhimõtete rakendamise uurimine Astrec Data OÜ andmekeskuse näitel.	14.03.23
3.	Andmekeskuse ohutusohu analüüs TIER 2 taseme andmekeskuse Astrec Data OÜ näitel.	14.04.23
4.	Andmekeskuse turvalisuse hindamine ja meetmete väljatöötamine selle parandamiseks.	31.04.23
5.	Lõputöö kirjaosa viimistlemine	15.05.23

Töö keel: eesti keel **Lõputöö esitamise tähtaeg:** "…. ”..... 20…. a

Üliõpilane: Vladimir Moskaljov "…. ”..... 20…. a
/allkiri/

Juhendaja: Larissa Joonas "…. ”..... 20…. a
/allkiri/

Programmijuht: Žanna Gratšjova "…. ”..... 20…. a
/allkiri/

SISUKORD

EESSÕNA

Oma töös analüüsis autor Astrec Data OÜ andmekeskuse usaldusväärsust ja tõrkekindlust TIER 2 tasemel ning tegi ettepanekud andmekeskuse moderniseerimiseks TIER 3 taseme saavutamiseks.

Tahaksin eriliselt tänada Larissa Joonast, kes aitas mul valida selle teema lõputööks ja andis materjali uurimiseks. Samuti tahaksin tänada German Karinit, kes viis mind ekskursioonile Astrec Data OÜ andmekeskusesse ja vastas kõikidele minu küsimustele.

Olulised märksõnad: rakenduskõrghariduse lõputöö, andmekeskus, turvalisus, usaldusväärsus, tõrkekindlus, ohuanalüüs.

LÜHENDITE JA TÄHISTE LOETELU

ATS	automaatne ülekandevahetuskontaktor (ingl k *Automatic Transfer Switch*)
HVAC	- kütte-, ventilatsiooni- ja kliimaseadmed (ingl k *Heating, Ventilation, and Air Conditioning*)
IDS	sissetungi tuvastamise süsteem (ingl k *Intrusion Detection System*)
IPS	sissetungi ennetamise süsteem (ingl k *Intrusion Prevention System*)
MAC	võrgus oleva füüsilise seadme unikaalne identifikaator (aadress) (ingl k *Media Access Control*)
MSP	haldusteenuse pakkuja (ingl k *Managed Service Provider*)
PDU	toitejaotusseade (ingl k *Power Distribution Unit*)
PTZ	"pan" tähistab kaamera horisontaalset liikumist, "tilt" vertikaalset kallutamist ja "zoom" pildi suurendamist (ingl k *Pan-Tilt-Zoom*)
QoS	teenuse kvaliteedi juhtimise mehhanism võrgus (ingl k *Quality of Service*)
SLA	teenindustaseme leping (ingl k *Service Level Agreement*)
STS	staatiline ülekandevahetuskontaktor (ingl k *Static Transfer Switch*)
TIA/EIA	TIA ja EIA on kaks eraldi organisatsiooni, mis ühinesid 1988. aastal üheks organisatsiooniks, et töötada välja standardid seadmete ja sidetehnoloogiate jaoks (ingl k *Telecommunications Industry Association / Electronic Industries Alliance*)
TIER	tase
UPS	toitevarustusüsteem (ingl k *Uninterruptible Power Supply*)
VCA	videosisu analüüs on arvutinägemise tehnoloogia (ingl k *Video Content Analysis*)

SISSEJUHATUS

Andmekeskuste teenuseid on oma elus kasutanud ilmselt kõik. Olgu selleks e-kirjade saatmine, internetis ostlemine, videomängude mängimine või lihtsalt sotsiaalmeedia sirvimine, iga bait sellest, mida te Internetis salvestate, hoitakse andmekeskuses. Kuna kaugtöö muutub kiiresti uueks normiks, suureneb vajadus andmekeskuste järele. Keskmistele ja suurtele ettevõtetele muutuvad pilveandmekeskused kiiresti eelistatud andmete salvestamise viisiks. Selle põhjuseks on see, et nad on palju turvalisemad kui traditsioonilistel riistvaraseadmetel olevate andmete hoidmine. Pilveandmekeskused pakuvad laiendatud turvakaitsed, näiteks tulemüüre ja tagavaraseadmeid turvalisuse rikkumise korral. [1]

Andmekeskuse turvalisus on väga oluline, olenemata sellest, kas andmekeskust kasutatakse peamiselt salvestamiseks, hädaolukorra taastamiseks või rakenduste toetamiseks - selle arvutuslikud töökoormused on selle teenindatava äri alus. Lisaks moodustavad ettevõtte konfidentsiaalne teave ja kriitiliselt olulised ärirakendused varanduse, mida häkkerid ja muud ohud võivad rünnata.

Lõputöö eesmärgiks on analüüsida ohutusohud ja hinnata TIER 2 taseme andmekeskuse usaldusväärsust Astrec Data OÜ näitel.

Lõputöö ülesanded:

1. saada ülevaade andmekeskuse tööpõhimõtetest ning usaldusväärsuse ja tõrkekindluse tagamisest andmekeskuses;
2. õppida põhilisi andmekeskuse projekteerimise põhimõtteid Astrec Data OÜ näitel Jõhvis;
3. analüüsida selle andmekeskuse turvalisust ja ohutusohud;
4. koostada Astrec Data OÜ andmekeskuse moderniseerimise plaan.

Lõputöö unikaalsus ja aktuaalsus:

Kaasaegne andmekeskus on väga keeruline ettevõte, millel on palju tehnilisi ja infrastruktuurseid elemente. Autori jaoks oli vaja kasutada suurt hulka nii kolledžis õpitud kui ka iseseisvalt loetud materjale.

Autor sai ainulaadse kogemuse konkreetse andmekeskuse uurimisel, kuna nende projekteerimise üksikasjad tavaliselt turvalisuse kaalutlustel ei avalikustata.

Töö teema on oluline, kuna suurem osa meie arvutustöödest toimub nüüd pilves ning organisatsioonid usaldavad üha enam oma andmete hoidmist ja töötlemist andmekeskustele.

1. ANDMEKESKUSE TÖÖ PÕHIMÕTTED

Tänapäeval on andmed muutunud iga äri jaoks eluliselt oluliseks varaks ning Interneti kasutamine on aastate jooksul suurenenud geomeetrilises progressioonis. [2]

Nutitelefonide ja sotsiaalmeedia kasutamine on viinud andmete kasutamise ja salvestamise kiirele kasvule. Kuidas andmekeskused toimivad ja millised ülesanded neil on, arenevad pidevalt. [2]

1.1. Andmekeskuse mõiste

Andmekeskus on füüsiline asukoht, kus asuvad arvutid ja nendega seotud riistvara. See sisaldab IT-süsteemide jaoks vajalikku arvutusinfrastruktuuri, nagu serverid, andmekandjad ja võrguseadmed. See on digitaalsete andmete hoidla iga ettevõtte jaoks. [3]

Andmekeskused võivad olla erineva suurusega: alates väikestest kappidest kuni eraldi kabinettide või ruumideni. Mõnedel ettevõtetel, kelle andmekeskudes on palju IT-seadmeid, võib olla vaja mitut andmekeskust. Lisaks võivad ettevõtted rentida servereid ja kaasata kolmandaid osapooli andmekeskuse teenuste osutamiseks. [4]

Andmekeskused võivad füüsilise ruumi piiridest välja ulatuda tänu privaatsele või avalikule pilveteenusele, mis võimaldab protsesse kiirendada või salvestusvahendeid suurendada. [4]

Andmeid töötleva keskuse disain põhineb arvutusressursside ja salvestusressursside võrgul, mis tagavad ühiste rakenduste ja andmete tarnimise. Andmekeskuse võtmeosade hulka kuuluvad ruuterid, võrgulülitid, tulemüürid, salvestussüsteemid, serverid ja rakenduste tarnimise kontrollerid. [5]

1.2. Andmekeskuse kasutamine äris

Tavalistel arvutivõrkudel ja IT-süsteemidel ei ole piisavalt arvutusvõimsust selliste andmemahtude töötlemiseks. [6]

Väikestele ja keskmise suurusega ettevõtetele võib füüsiliste serverite hooldamine olla keeruline, seetõttu võivad nad kasutada andmekeskuse teenuseid. Andmekeskuste kasutamise põhjused võivad olla järgmised:

- andmete usaldusväärsuse ja turvalisuse tagamine, sealhulgas tulemüüride ja häkkimiskaitse;
- andmete regulaarne varundamine ja varugeneraatorite olemasolu;

- kokkuhoiu võimalus serverite hooldus- ja tugi kuludelt, kuna kõik ruumi, ühenduse, toite, jahutuse ja turvalisuse haldamisega seotud vajadused lahendatakse andmekeskuses;
- tagatud tõrgeteta rakenduste töö ja andmete kättesaadavus igal ajal. [7]

Andmeanalüütika on iga ettevõtte strateegia võtmekomponent ning arvutusressursid mängivad olulist rolli teabe kogumisel ja töötlemisel. MSP-le või koosmajutamisele pöördumine võib anda väikestele ettevõtetele juurdepääsu suurematele arvutusressurssidele ja "suurandmete" analüüsile turukonkurentsis eelise saamiseks. [7]

Andmekeskuse kasutamine võimaldab vajaduse korral **mastaapsust**, mis on eriti oluline kiiresti kasvavate andmevajadustega väikestele ja keskmise suurusega ettevõtetele. [7]

Andmekeskused tagavad **usaldusväärse juurdepääsu turvalisusele** ja tagatud turvanõuetele, mis on prioriteet iga ettevõtte jaoks. Nad rakendavad kõige kaasaegsemaid turvamehhanisme ja tagavad 100% andmete jälgimist, võimaldades paremini hallata kõiki turvalisuse aspekte. [7]

Andmekeskusega koostöö võimaldab oma andmeid ja riistvarasüsteeme **ööpäevaringselt** kontrollida. [7]

1.3. Andmekeskuse arhitektuuri komponendid

Andmekeskused koosnevad kolmest peamisest tüübist komponentidest:

- serverid;
- salvestussüsteemid;
- võrgu- ja kommunikatsiooniinfrastruktuur. [8]

Komponentide kohta saab üksikasjalikumat teavet Lisa 1.

1.4. Andmekeskuste liigid ja tüübid

On mitu liiki andmekeskuseid:

- statsionaarsed andmekeskused;
- modulaarsed andmekeskused;
- konteinerpõhised andmekeskused. [9]

Andmekeskuste liikidest saab rohkem teavet Lisa 2.

Te võite kokku puutuda erinevat tüüpe andmekeskustega, sõltuvalt nende omandusest, kasutatavatest tehnoloogiatest ja energiatõhususest. Mõned peamist tüüpi andmekeskuste, mida organisatsioonid kasutavad, on järgmised:

- ettevõtte andmekuskused [10];
- kolokatsiooniandmekeskus [11];
- perifeersed andmekuskused [12];
- hüpermastaapsed andmekuskused [13];
- juhtimise teenustega andmekeskused [14];
- pilvepõhised andmekuskused [3].

Andmekeskuste tüüpidest saab lähemalt lugeda Lisa 3.

1.5. Andmekeskuse tasemete klassifikatsioonisüsteem

Andmekeskused on paljude ettevõtete digitaalse infrastruktuuri alus ning paljud neist ei saaks ilma nendeta eksisteerida. Andmekeskuse valimisel on oluline valida õige ja üheks oluliseks kriteeriumiks on The Uptime Institute'i tasemete klassifikatsioonisüsteem. [15]

1.5.1. Andmekeskuste klassifitseerimine

Uptime Institute on välja töötanud andmekeskuste klassifikatsiooni tasemed (TIER), mis on rahvusvaheline jõudluse standard. Need selgitavad, millist infrastruktuuri on vaja andmekeskuse tööks, ja erinevaid tasemeid on olemas sõltuvalt vajalikust süsteemi kättesaadavusest. Need klassifikatsioonid aitavad võrrelda ühe objekti infrastruktuuri jõudlust teisega ja kohandada investeeringuid infrastruktuuri ärieesmärkidega. Uptime Institute on ainus litsentseeritud ettevõte, mis võib väljastada jõudluse nõuetele vastavuse tunnistusi, mistõttu on nad selle hinnangu ainus allikas. [16]

1.5.2. Andmekeskuste tasemeklassifikatsioon

Andmekeskuste tasemeklassifikatsioon jaguneb neljaks tasemeks, millel on igal oma teenindus-, toite-, jahutus- ja tõrkekindluse kriteeriumid. Samuti võidakse arvestada teisi tegureid, nagu ehitusstandardid, turvalisus ja ilmastikutingimused. [16]

1.5.3. Andmekeskuse tasemed

Andmekeskuse tasemed:

- andmekeskused esimesel tasemel (TIER I) on põhitasemeks ning pakuvad IT-infrastruktuuri jaoks eraldatud ruumi koos tagavara elektrigeneraatori, katkematu toiteallika (UPS) ning kütte-, ventilatsiooni- ja konditsioneerimissüsteemidega (HVAC). Siiski pole neil ühegi kriitilise süsteemi osas üleliigset suutlikkust, mistõttu tehnoloogiliste hooldus- või rikkejuhtumite korral tööd tuleb ajutiselt peatada. Esimese taseme andmekeskused sobivad kõige paremini väga väikestele ettevõtetele, kelle jaoks on vajalik majutuse kõige ökonoomsem lahendus. Nad tagavad ainult 99,671% aastasest tööajast ilma tõrgeteta, mis on võrdväärne 28,8 tunniga seisakuaega;

- andmekeskused 2. taseme omavad kõiki 1. taseme keskuste funktsioone, aga ka osalist toitevarustuse (nt UPS-süsteemid) ja jahutuse (nt jahutusseadmed/pumbad) tagamist. Dubleerimine võimaldab neil täita eraldi teenindusfunktsioone ja tagab kõrgema rikkekindluse taseme. Need tagavad 99,741% tööajast aastas ja maksimaalse aastase tööaja 22,7 tundi. Andmekeskused 2. taseme sobivad väikestele ja keskmise suurusega ettevõtetele, kes vajavad ökonoomset ja usaldusväärset valikut oma arvutus- ja salvestusvajaduste, varundamise ja andmete taastamise ning ka mittekriitiliste funktsioonide rahuldamiseks;
- andmekeskused 3. taseme tagavad kõrgema tõrkekindluse taseme kui 1. ja 2. taseme keskused, tänu täiendavatele varundussüsteemidele toite- ja jahutusvõimsuses, mis võimaldab teenindada komponente ilma kliendi IT-operatsioonide peatamata. 3. taseme keskused tagavad 99,982% tööajast aastas, mis vastab 1,6 tundi aastas tööseisakule. Need pakuvad ka laiemaid varundusvõimalusi, sealhulgas N+1 varundust (N: vajalik võimsus andmekeskuse täieliku IT-koormuse toetamiseks. +1: täiendav komponent varundamiseks). Siiski ei ole need täielikult tõrkekindlad, kuna võivad toetuda objektist täielikult sõltumatutele komponentidele. Andmekeskused 3. taseme on tööstusharu standardiks, mis tagab kõrgekvaliteedilise ruumi, toite ja jahutuse, et rahuldada klientide kriitilisi vajadusi arvutuste ja salvestamise osas;
- andmekeskused 4. tasemel tagavad kõrge tõrkekindluse, mis tähendab, et planeerimata tõrked või katkestused ei mõjuta IT-operatsioone. Neil on liigsuse tase 2N või 2N+1, mis tähendab täielikult liigse infrastruktuuri olemasolu, mis võimaldab vältida mõlema süsteemi kompromiteerimist kohaliku sündmusega. Andmekeskused neljandal tasemel tagavad 99,995% tööajast aastas ilma riketeta, mis on võrdne maksimaalse aastase kokkukukkumisajaga 26,3 minutit. Siiski on sellise rajatise ehitamise ja varustamise maksumus märkimisväärselt suurem kui andmekeskuste 2. ja 3. tasemel. Andmekeskused neljandal tasemel rahuldavad ettevõtete vajadusi, kelle jaoks kõrge IT-süsteemi kättesaadavus ja tõrkekindlus on esmatähtsad.

  2N tähendab täielikult identses varusüsteemi olemasolu iga komponendi jaoks, millel on füüsiline isoleeritus ja mis on sõltumatu põhisüsteemist. [17]

Tabeliga, mis annab ülevaate usaldusväärsuse taseme nõuetest igale sertifitseerimisele, saate tutvuda Lisa 4.

1.6. Andmekeskuse insenerisüsteemid

Andmekeskuse aluseks on insenerisüsteemid, mis hõlmavad toite-, jahutus-, võrgu- ja side-, tulekustutus-, füüsilise turvalisuse, ümbritseva keskkonna jälgimise ning tehnilise

teeninduse ja hoolduse süsteeme. Toitesüsteemid tagavad usaldusväärse energia varustamise, jahutussüsteemid hoiavad optimaalset temperatuuri ja niiskust, võrgu- ja side-süsteemid tagavad ühenduse välismaailmaga, tulekustutussüsteemid ennetavad tulekahjusid, füüsiline turvalisus kaitseb konfidentsiaalset teavet, ümbritseva keskkonna jälgimine kontrollib töötingimusi ning tehniline teenindus ja hooldus tagavad süsteemide usaldusväärsuse ja jõudluse. Need süsteemid on keerulised ja nõuavad spetsiaalseid teadmisi nende projekteerimiseks, paigaldamiseks ja hooldamiseks. [18]

1.6.1. Toite süsteemid

Andmekeskused nõuavad usaldusväärseid ja skaalatavaid toitesüsteeme IT-infrastruktuuri toetamiseks. Siin on mõned levinud toitesüsteemid, mida andmekeskustes kasutatakse [19]:

- UPS - see on akuvarutoitesüsteem, mis tagab lühiajalise varutoite pärast elektrienergia katkestust. See võib olla autonoomne või integreeritud muude energiasüsteemidega [19];
- generaator - reservtoiteallikas, mis töötab diislikütusel, looduslikul gaasil või propaanil, mis tagab pikaajalise toite pikaajalise elektrikatkestuse korral [20];
- PDU - toite levitamise blokid, mis jagavad energiat peamisest allikast IT-seadmetele. Need võivad olla põhi- või intelligentseid, jälgides energiatarbimist ja andes andmeid [21];
- andmekeskused kasutavad reserveeritud toitesüsteeme, sealhulgas reserveeritud UPS-i, generaatoreid ja PDU-sid, et tagada kriitilise IT-seadmete katkematu toide.

1.6.2. Jahutussüsteem

Andmekeskuse jahutamine on vajalik elektriseadmete ülekuumenemise vältimiseks, mis võib põhjustada ahelkomponentide kahjustusi, plahvatusi, tulekahjusid ja vigastusi. Ülekuumenemisest tingitud kahjustused on pöördumatud ja ainus viis seadme parandamiseks on mõnede komponentide asendamine. Andmekeskuse jahutamine on ennetav meede, mis tagab teie töötajate ja seadmete ohutuse ning on vajalik organisatsiooni tõhususe tagamiseks. [22]

Siin on mõned saadaolevad süsteemid:

- arvutiruumi õhukäitleja (CRAH);
- arvutiruumi konditsioneer (CRAC);
- aurusti jahutussüsteemid;
- kalibreeritud vektorjahutus;
- külm koridor/Kuum koridor (Cold Aisle/Hot Aisle);
- jahutusvedelikuga otsene kiibijahutus;
- tõusev põrand;

- süvistatav jahutus (Immersion Cooling);
- looduslik jahutus;
- vedeljahutus. [22]

Lisateavet jahutusmeetodite kohta leiate Lisa 5.

Erinevad andmekeskused võivad kasutada erinevaid nende meetodite kombinatsioone, et saavutada parim tasakaal jahutuse tõhususe, energiatarbimise ja hoolduskulude vahel.

1.6.3. Võrgu infrastruktuur ja varukoopiad

Andmekeskuse võrk - andmete ja rakenduste salvestamise ja töötlemise mitmete võrguressursside integreerimine. See sisaldab ühendamist, marsruutimist, koormuse tasakaalustamist ja analüüsi. [23]

Andmekeskuse võrk tagab seadmete ja seadmete vahelise ühenduse, võimaldades neil andmeid võrgu või Interneti kaudu edastada. See peab olema tugev, turvaline, vastama tööstuseeskirjadele ja rahuldama ettevõtte ja kasutajate nõudeid. Andmekeskuse võrgu komponendid hõlmavad võrguseadmeid, kaableid, võrguaadresside skeeme, võrguturvalisust ja Interneti-ühendust. Andmekeskuse võrk on vajalik füüsiliste ja võrguseadmete ja seadmete paigaldamiseks ja ühendamiseks ning toetab kaasaegsete tehnoloogiate, nagu pilvandmetöötlus ja virtualiseerimine, võrguvajadusi. [24]

Kaasaegne andmekeskuse võrgu arhitektuur täidab kõik võrguteenused tarkvaraliselt, mis lihtsustab initsialiseerimisprotsesse ja võimaldab läbilaskevõime ja turvapoliitika planeerimise automatiseerimist. Võrguplatvorm juhib ka rakenduste de-initsialiseerimist, et vältida aegunud reeglite levikut ja tagada turvalisus ning nõuetele vastavus. Tänapäeva andmekeskuste jaoks kõige arenenumad võrgulahendused pakuvad olulisi teenuseid rakendustele ja andmetele, sealhulgas automatiseerimist, pidevat tööd ja mikrosegmendipõhist turvalisust. [24]

Olulised kriteeriumid kaasaegse andmekeskuse võrguplatvormi jaoks:

- võrguteenuste automatiseerimine rakendustele kiiruse ja paindlikkuse saavutamiseks andmekeskustes;
- poliitikate kooskõlastamine reeglite kooskõlastatud täitmiseks andmekeskustes, kusjuures ressursid integreeritakse servast pilve;
- ühtne juhtpaneel keskseks juhtimiseks ühtse kasutajaliidese abil;
- integreeritud turvameetmed, näiteks mikrosegmendid ja IDS / IPS, turvalisuse tagamiseks granuleeritud tasemel;
- nähtavus globaalsel tasemel võrguprobleemide diagnostika lihtsustamiseks. [24]

Võrgustikest, serveritest ja salvestusinfrastruktuurist saate rohkem lugeda Lisa 6.

1.6.4. Tulekustutussüsteem

Tulekahju oht, nagu ka mis tahes muu hädaolukord, on alati olemas, olenemata sellest, kui usaldusväärne on andmekeskuse infrastruktuur. Praegu on mitmeid kindlalt paika pandud suundi tulekahjude likvideerimiseks andmekeskustes:

- pulbri- ja aerosoolisüsteemid;
- gaasi tulekustutussüsteemid;
- veepilv- või udu pihustamisel põhinevad süsteemid;
- hüpoksilise kustutamise meetod. [25]

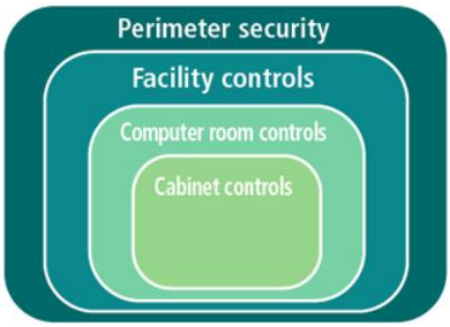
Tulekahjusüsteemide kohta saate rohkem lugeda Lisa 7.

Tulekahjusüsteemi valik sõltub erinevatest teguritest, nagu seadmete hind, hoone ja ruumi omadused. [25]

1.6.5. Turvalisus

Andmekeskuse turvalisus sõltub asukohast, geoloogilisest aktiivsusest, üleujutus- ja hädaolukordade riskist. Riske saab vähendada tõkete või füüsilise konstruktsiooni liigse varuga, kuid parem on vältida andmekeskusele kahjulikku mõju. [26]

Kõige optimaalsem ja strateegilisem viis andmekeskuse kaitsmiseks on selle juhtimine tasemepõhiselt (Joonis 1.1). Tasemed tagavad struktureeritud füüsilise kaitse mustri, mis lihtsustab rikke analüüsi. Välised tasemed on puhtalt füüsilised, samal ajal kui sisemised tasemed aitavad ka takistada igasugust tahtlikku või juhuslikku andmete leket. [26]



Joonis 1.1 Neli tasandit andmekeskuse füüsilisest turvalisusest [26]

Turvalisusmeetmeid saab jagada neljaks tasemeks: perimeetri turvalisus, rajatise juhtimine, arvutiruumi juhtimine ja kapi juhtimine. Mitmetasandilisus takistab volitamata juurdepääsu andmekeskusesse väljastpoolt. Sisemised kihid aitavad samuti vähendada siseohtusid. [26]

Esimene tase on perimeetri turvalisus, kus kasutatakse videovalve süsteeme, turvavalgustust, optilist kaablit ja videokontendi analüüsi (VCA) volitamata sisenemise

avastamiseks. Teine tase on rajatise juhtimine, kus kasutatakse ligipääsu kontrollisüsteeme kaartide või biomeetria lugemiseks, kvaliteetset videovalvet ja VCA-d. Kolmas tase on arvutiruumi juhtimine, kus kasutatakse erinevaid kontrollimeetodeid, sealhulgas VCA-d, biomeetrilisi juurdepääsu kontrollseadmeid ja raadiosageduse määratlust. Neljas tase on kapi juhtimine, kus kasutatakse kappide lukustamismehhanisme, elektroonilisi lukustussüsteeme, nutikaarte, biomeetrilisi andmeid ja PTZ-kaameraid inimese pildi ja tema tegevuste jäädvustamiseks. [26]

1.7. Serveriruumi nõuded ja soovitused

Serveriruum on ruum, kus hoitakse jaotusseadmeid ja telekommunikatsiooniseadmeid. TIA/EIA-569 standardit kasutatakse serveriruumi nõuete ja soovituste väljatöötamiseks. [27]

Lisateavet serveriruumi nõuete ja soovituste kohta leiate Lisa 8.

1.8. Nõuded andmekeskustele Eestis

Andmekeskuse nõuded Eestis võivad erineda organisatsiooni või ettevõtte konkreetsetest vajadustest.

Kõige olulisem on, et andmekeskus vastaks kindla taseme regulatsioonidele ning suudaks pakkuda oma klientidele oma regulatsioone ja kohtuasjaid.

Üldiselt nõuab andmekeskuse loomine ja haldamine Eestis põhjalikku planeerimist ja mitmeid tegureid arvestamist, sealhulgas usaldusväärsust, turvalisust, varundusvõimekust, skaalatavust, vastavust regulatiivsetele nõuetele, asukohta ja kättesaadavust.

2. ANDMEKESKUSE ASTREC DATA OÜ USALDUSVÄÄRSUSE ANALÜÜS

Astrec Data OÜ andmekeskus asutati 2014. aastal Jõhvis. Andmekeskus pakub co-location, serverite ja virtuaalmasinate renditeenuseid.

Autor külastas Astrec Data OÜ andmekeskust novembris 2022, kus talle korraldati ekskursioon ja vastati eelnevalt koostatud küsimustele. Samal päeval sai autor teada, et andmekeskus on ümberkorraldamisel, mis võimaldab autoril tulevikus anda soovitusi andmekeskusele. Autorile ei esitatud tundlikku teavet, mis võiks andmekeskusele kahju tekitada, ja seadmete kohta ei räägitud liiga üksikasjalikult.

Astrec Data OÜ on TIER 2 andmekeskust, mis tähendab võrreldes TIER 1 keskustega suuremat usaldusväärsust. Hädaolukordade ja tehniliste probleemide korral on lubatud aastas kuni 22,7 tundi katkestusi, ja tõrkekindluseaste on 99,741%. Siiski tuleb märkida, et usaldusväärsuse näitajad TIER 3 ja 4 keskustel on kõrgemad kui TIER 2 andmekeskustel.

Astrec Data OÜ usaldusväärsus tagatakse varundamise, reguleerimise, juurdepääsu kontrollimise ja vastutavate isikute kaudu.

2.1. Elektritoite katkematu tagamine

Energiasüsteem on üks kõige kriitiliselt tähtsamaid insenertehnilise infrastruktuuri komponente andmekeskuses. Ohtlike olukordade vältimiseks on andmekeskus varustatud diiselgeneraatorite ja katkematu toiteallikatega.

Astrec Data OÜ andmekeskuses on kaks peamist elektrivarustuse allikat: linnuvõrgu elektrivarustus ja UPS, mis töötab koos diiselgeneraatoriga. Elekter jõuab andmekeskusesse peavõrgust kõrgepingeliinide kaudu. Seejärel vähendatakse pinget transformaatorite abil nõutavale tasemele, mis on vajalik andmekeskuse seadmete tööks.

Seejärel läbib elekter jaotuspaneeli, mis jagab selle mitmeks liiniks ja suunab erinevatesse andmekeskuse osadesse. Jaotuspaneelist saadetakse elekter peamiste paneelide kaudu, mis tagavad erinevate alamsüsteemide, nagu jahutus-, valgustus- ja turvasüsteemide, toite.

Joonis 2.1 Jagamiskapp

Seejärel suunatakse elekter serveritesse, mis tarbivad andmekeskuses suurema osa energiast. Serverite tõhusa töö tagamiseks kasutatakse katkematu toiteallikat (UPS), mis tagab toitekatkestuste korral pideva toite. UPS-i akud laetakse pidevalt ja salvestavad elektrit.

Joonis 2.2 UPS. Vasakul akud, paremal - kontroller

Joonis 2.3 UPS-i kontrolleri ekraan

Kui linna elektrivarustus kaob, siis automaatika tuvastab elektri puudumise ja ühe

minuti jooksul käivitub diiselmootoriga generaator. Diiselmootoriga generaator töötab seni, kuni kütus otsa saab. Andmekeskus võib sõlmida lepingu kütuseettevõttega, kes tarnib diiselkütust, et generaator saaks töötada kauem, kuni linna elektrivarustus taastub.

Kui tekib probleem diiselmootoriga generaatori käivitamisel, siis automaatselt lülitub sisse varutoide - UPS. See toidab koormust akupatareidest, mis võimaldab andmekeskusel töötada autonoomselt umbes 24 minutit. See aeg on tavaliselt piisav, et viga kõrvaldada ja käivitada generaator.

Kui diiselmootoriga generaator on parandatud, siis generaator töötab seni, kuni diiselkütus on lõppenud või kuni linna elektrivarustus taastatakse. Diiselmootoriga generaatril on ühe tonni mahutavusega paak, mis võimaldab töötada kuni 18 tundi ilma kütuse täiendamiseta.

Lisaks, kui UPSid rikuvad või ei suuda tagada nõutavat elektritoite taset, siis toimub jaotuskilbis ümberlülitumine teisele režiimile, mis toidab kogu seadmete komplekti, sealhulgas servereid.

Astrec Data OÜ andmekeskusel on kaks toiteallikat: esimene on linnast tulev elektriliin, teine on UPSid ja diiselmootoriga generaator. See lähenemine on standard ja tagab andmekeskuse usaldusväärsuse ja katkematu töö.

2.2. Usaldusväärsuse tagamine infrastruktuuri ja varukoopiate abil

Infrastruktuur ja varukoopiad on võtmevahendid süsteemide usaldusväärsuse tagamiseks ja olulise teabe säilitamiseks. Infrastruktuur tagab vajalikud ressursid rakenduste tööks ja andmete säilitamiseks, samas kui varukoopiad võimaldavad kiiresti taastada teavet selle kaotamise või kahjustamise korral.

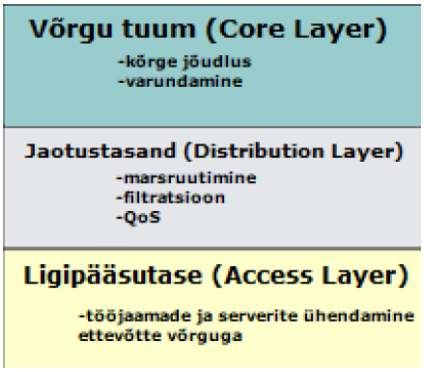
Selles kontekstis on oluline mõista, et süsteemi usaldusväärsus sõltub mitte ainult selle tehnilisest varustatusest, vaid ka teenindava ja hooldava personali pädevusest ja professionaalsusest.

Usaldusväärsuse ja kõrge kättesaadavuse tagamiseks kasutab andmekeskus tavaliselt kahte või enam sideoperaatorit. See tagab pideva juurdepääsu internetiliiklusele ja võimaldab kiiret reageerimist igasugustele tõrgetele ja probleemidele. Astrec Data OÜ kasutab kahe operaatori liine, mida kasutavad ka kliendid. Lisaks toimub Astrec Data OÜ andmekeskuses sageli internetiliikluse edastamine ja varundamine, mis võimaldab tagada võrgu stabiilse töö ja minimeerida tõrgete ja kättesaadavuse probleemide riske.

Astrec Data OÜ andmekeskuses kasutatakse kahte võrgulülitit ja kahte ruuterit võrgu

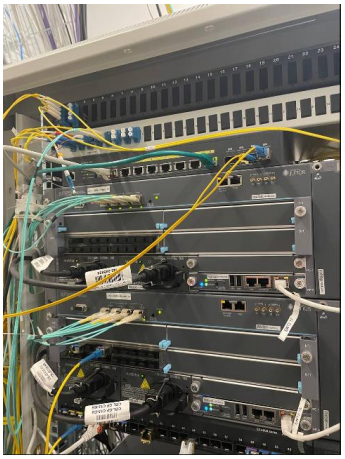
varukoopia ja tõrkekindluse tagamiseks.

Võrgulülitid ja ruuterid on paigutatud hierarhilise võrgumudelina seadmepüstikul(rack mount). Võrgu tuumaks on ruuterid, võrgulülitid kuuluvad levitamise tasemele ja serverid kui juurdepääsu tase.



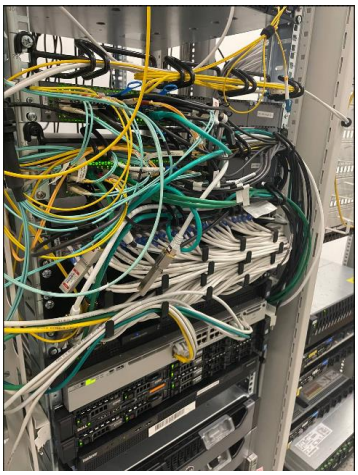
Joonis 2.4 Hierarhiline võrgumudel [28]

Ruuterid on mõeldud andmete edastamiseks erinevate võrkude ja seadmete vahel, võrguliikluse haldamiseks ning võrguressursside turvalisuse ja kaitse tagamiseks. Need võimaldavad ühendada mitu seadet ühes kohalikus võrgus ja ühenduda ka interneti kaudu teenusepakkujaga.



Joonis 2.5 2 suurt ruuterit

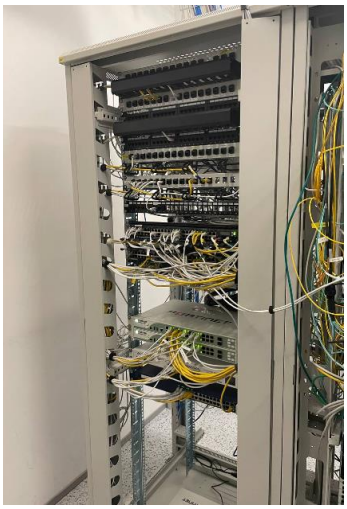
Ruuterid võtavad vastu pakette ja edastavad saadud paketid välise võrgu kaudu saabuvatele võrgulülititele edasiseks jaotamiseks.



Joonis 2.6 Võrgulülitid

Võrgulülitid (switch'id) on mõeldud seadmete ühendamiseks kohalikus võrgus (LAN), tagades nende vahel kiire ja usaldusväärse andmeedastuse, samuti liikluse juhtimise, võrgu jagamise, tõrgete tuvastamise ja kõrgema skaala saavutamise.

Andmekeskuses kasutatakse paneelühendusi, mida kasutatakse paljude kaablite ühendamiseks kindlas järjekorras. Neid kasutatakse sageli arvutivõrkudes ühenduste korraldamiseks arvutite, ruuterite ja muude võrguseadmete vahel. Paneelühendusi kasutatakse ka kaablite haldamise lihtsustamiseks ja võrgu haldamisele struktureerituma ja produktiivsema lähenemisviisi tagamiseks. Paneelühenduste kasutamisel muutub kaabelinfrastruktuur paremini organiseerituks, arusaadavamaks ja kergemini ligipääsetavaks, mis lihtsustab selle hooldamist, seadistamist ja muutmist.



Joonis 2.7 Pistikpaneelid

Astrec Data OÜ andmekeskuses kasutatakse ka blade-servereid ja torn-servereid.

Joonis 2.8 Blade-serverid

Blade-serverid on arvutiserverite vorm, kus eraldi arvutiseadmed (blade'id) paigaldatakse spetsiaalsele platvormile (šassii) ja ühendatakse üheks tervikuks. Tänu nende suurusele on nad kompaktsed ja ei võta palju ruumi.

Igal blade-serveril on 6 toiteplokki. 1 toiteplokk tarbib 2,5 kilovatti. Kui üks toitejoon ebaõnnestub, siis teine tagab topelttoitumise - see tähendab, et süsteemil on varutoitelahendused, mis suudavad tööd jätkata, kui üks allikas ebaõnnestub. See suurendab usaldusväärsust ja vähendab andmete kaotamise riski.

Joonis 2.9 Tornserverid

Tornserver on spetsiaalselt serverina kasutamiseks välja töötatud arvuti, mis on mõeldud kasutamiseks riiulis. Tornserverid on tavaliselt kujundatud torni korpuse kujul, mis seisab vertikaalselt töölaua või põranda peal, erinevalt riiulitele paigaldatud serveritest. Tavaliselt kasutatakse tornservereid väikestes ja keskmise suurusega ettevõtetes, kus pole vaja suurt hulka riiulisse paigaldatud servereid.

Joonis 2.10 Seadmepüstikud

Astrec Data OÜ pakub klientidele eraldi kappe oma andmekeskuses. Klientidel on võimalus otsustada, millist seadet oma kapil hoida.

Allpool on toodud serverite ühendamise skeem seadmepüstikul:

Joonis 2.11 Serverite ühendusskeem seadmepüstikul

Palun pange tähele, et see on vaid näide ja konkreetne serverite ühendamise skeem võib erineda võrgu nõuete ja täiendavate seadmete või komponentide olemasolu tõttu. Samuti sõltub serverite ühendamine projekti spetsiifikast.

Andmekeskuses on saadaval erineva suurusega kapid, kuid standardne kapp on 42 ühikut kõrge, mis võimaldab sellesse paigutada kuni 42 serverit.

Andmekeskuse reserveerimine on kriitilise tähtsusega andmete säilitamise tagamiseks ning toimub tavaliselt dubleerimise, pilvepõhise salvestamise ja muude meetodite abil. Pilvepõhine salvestamine võimaldab varundada andmeid kaugemates kohtades, tagades nende kättesaadavuse ja kaitse kaotuse või kahjustumise eest. Andmekeskus

kasutab ka topeltvarundamist ja peegelvarundamist. Peegelvarundamise korral salvestatakse andmed kahele serverile samal ajal, tagades maksimaalse kaitse kaotuse ja kahjustuste eest.

Andmete edastamist andmekeskuses ei reguleerita, tagatakse vaid garanteeritud internetiühendus. Klient vastutab ise oma andmete eest. Andmekeskuse salvestussüsteem toimib laopõhimõttel, kus kõvakettaid ja tahkisandmeid hoitakse laos. Andmekeskus ei kasuta lindimäluseadmeid, kuid klientidel on nende kasutamise võimalus.

2.3. Jahutussüsteem

Astrec Data OÜ kasutab tõhusat jahutussüsteemi, mis hõlmab külmi ja kuumi koridore.

Hoone katusel, kus asub andmekeskus, on kliimaseadmed - invertersüsteemid, mis jahutavad õhku väljastpoolt ja seejärel õhk siseneb siseruumidesse paigaldatud konditsioneeride siseplokkidesse.

Need siseplokid asuvad serveriruumis ning neist väljub külm õhk altpoolt, mis jahutab kuumi serverikappe. Seejärel kuum õhk eemaldatakse ülemise osa ventilatsiooni abil ja suunatakse hoone katusele paigaldatud välimistesse konditsioneeriblokkidesse.

Joonis 2.12 Siseõhu konditsioneer

Jahutussüsteemi, UPS-id ja üldised elektriliinid paiknevad samas ruumis. Sellel ruumil on juhtpaneel, mis vastutab jahutussüsteemi ja kliimaseadmete (inverterid) juhtimise eest.

Joonis 2.13 Jahutussüsteemi ja kliimaseadmete juhtimise eest vastutav pult

Sellel puldil saate vaadata serveriruumi temperatuuri ja niiskuse protsenti ning teada saada ka telekommunikatsiooni ja jahutussüsteemi asukohta, UPS-i ja üldiste elektriliinide temperatuuri. See pult aitab kontrollida soovitatavat temperatuuri ja niiskust.

Joonis 2.14 Ekraan puldil, mis vastutab jahutussüsteemi ja kliimaseadmete juhtimise eest

Jahutussüsteemi, UPS-i ja üldiste elektriliinide ruumis ning ka telekommunikatsiooniruumis on tavalised split-süsteemid.

Joonis 2.15 Split-süsteem

Astrec Data OÜ selgitas, miks kasutatakse jahutussüsteemi, mis sisaldab külm- ja kuumkoridore. Selle süsteemi eelised on taskukohane hind, lihtne hooldus ja optimaalne energiakulu. Selle süsteemi puudusteks võib pidada vajadust hoida seadmed töökorras ja jälgida külma ja kuuma koridori nõuetekohast toimimist.

Astrec Data OÜ sooviks jahutussüsteemi täiendada kuum- ja külmkoridoride tõketega ning luua võlakorruse, et vältida ülekuumenemist ja külma õhu kadu. Tõkked aitavad piirata kuumade ja külmade õhuvoolude segunemist ruumis ning võlakorrus parandab õhuringlust.

2.4. Tulekustutussüsteem

Astrec Data OÜ kasutab gaasipõhist tulekustutussüsteemi, kuna nad peavad seda parimaks süsteemiks ja pole midagi tõhusamat veel leidnud.

Joonis 2.16 7 gaasiballooni

Astrec Data OÜ kasutab 7 balloonitäit. Neist 5 kasutatakse serveriruumis, 1 balloon elektritoiteseadmetega ruumis ja 1 balloon telekommunikatsiooniruumis.

Kui tulekahju juhtub, käivituvad andurid, mille abil süsteem töötab ja kohe käivitub ka

häire. Kui häire käivitub, avanevad uksed ja personalile antakse 30 sekundit, et lahkuda andmekeskusest ja sulgeda kõik. Lisaks peatatakse tulekahju korral kõik seadmed ja pärast 30 sekundit gaasi toidetakse. Pärast gaasi on vaja ruumi ventileerida ja rõhk langetada.

Gaasi manustamise ajal on personalil parem ruumist lahkuda, kuna see on ohtlik ja võivad tekkida erinevad kahjulikud ühendid, mis võivad inimesele kahjustada. Samuti suletakse uksed hermeetiliselt ja inimene ei saa enam väljuda.

Balloonide kontroll toimub iga 3 kuu tagant. Pärast süsteemi käivitamist on balloonide uuesti täitmine piisavalt kallis.

Gaasisüsteemid on levinud tulekustutussüsteemid, samuti ei kahjusta see süsteem seadmeid ning tungib suurepäraselt ligipääsmatutesse ja seadmete suletud korpustesse.

Kuigi Astrec Data OÜ peab gaasipõhist tulekustutussüsteemi parimaks ja kasutab seda oma andmekeskuses, ei kasutata selles keskuses hüpoksiaga tulekustutusmeetodit suurte rahaliste kulude tõttu, kuid Astrec Data OÜ peab seda parimaks meetodiks. See süsteem vähendab andmekeskuse ruumide hapnikku, mis takistab tulekahju teket. Personal saab töötada pidevas keskkonnas, kus hapniku tase on madal, kui puuduvad olulised füüsilised koormused.

2.5. Turvalisus

Astrec Data OÜ-l on TIER 2 andmekeskuse perimeetri kaitsmiseks piisavalt hea tasemega turvameetmed.

Andmekeskuses jälgitakse pidevalt kasutajate tegevust kaamerate ja lugejatega, sealhulgas kasutajate fotodega kaarte, mis kattuvad andmebaasis olevate fotodega. Andmekeskuses on rakendatud ainult füüsiline juurdepääsu kontroll, kus töötajad ja kliendid kasutavad oma kaarte, samas kui külalised peavad täitma külaliste registreerimisvormi turvalisuse ja juurdepääsu kontrolli tagamiseks.

Andmekeskustes kasutatakse ka kapi lukustamise mehhanisme, elektroonilisi lukustussüsteeme, kus klient saab avada ainult oma kapi.

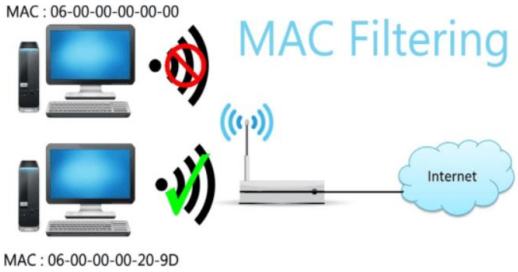
Sissepääsu juures on alati turvafirma, kus 24/7 töötab valve, kes tegeleb andmekeskusesse lubamisega. Andmekeskuse sissepääs on kontrollitud kahe meetri kõrguse piirdeaiaga, tõkkepuuga ja pöördväravatega, mis takistavad autode liikumist.

Personali ja klientide turvalisuse tagamiseks on rakendatud juurdepääsu kontroll, mis võimaldab klientidel juurdepääsu ainult serveriruumile. Isegi kui personali pole kohal, saab külalisklient andmekeskusesse juurdepääsu ainult juurdepääsu kontrolli läbimise järel.

Igal töötajal on kasutajakonto, mis kontrollib juurdepääsu ja logides kuvatakse, milline kasutaja ja millal võrguga ühendati.

Juurdepääsuõiguste piirang tagab, et igal töötajal ja kliendil on oma kasutajakonto ning neil on juurdepääs ainult nendele ressurssidele, millele neil on õigus.

Turvalisuse tagamiseks filtreeritakse andmekeskuses oma sülearvuti ühendamisel klientide MAC-aadresse, et kontrollida, kas need vastavad lubatud aadresside loendile. Kui MAC-aadressi loendist ei leita, siis juurdepääs andmekeskuse ühiskasutatavale võrgule takistatakse, kuid klientidel on võimalik saada juurdepääs ainult külaliste võrgule.



Joonis 2.17 Mac-aadressi filtreerimine [29]

3. OHUANALÜÜS

Andmekeskused on paljude organisatsioonide jaoks oluline osa, kuna need tagavad andmete säilitamise ja kättesaadavuse ning kaitsevad neid ohtude eest. Andmekeskuse ohuanalüüs on vajalik peamiste riskide tuvastamiseks ja praeguse tõrkekidnlustaseme määramiseks. Andmekeskuse ohuanalüüsi läbiviimine aitab organisatsioonidel järgida normatiivseid ja kohalikke nõudeid ning kaitsta oma andmeid. Ohuanalüüs aitab organisatsioonidel võrrelda juhtivaid meetodeid ja standardeid, parandada oma protsesse ning tõsta andmete kaitse taset. [30]

Andmekeskuse ohuanalüüs on vajalik organisatsioonidele, kes peavad järgima äri-, õigus-, lepingulisi ja normatiivseid nõudeid, soovivad saada reaalajas ülevaadet oma infrastruktuurist, tagada IT-rakenduste käivitamine ja taastamine andmekeskuses ning tuvastada probleeme. Ohuanalüüsi puudumine võib suurendada oluliste tõrgete tõenäosust igapäevases töös, ohustada turvalisust, takistada süsteemsete rikete ennetamist ja võitlust väliste ohtude vastu. [30]

3.1. Ohtude tabel

Ohtude tabel andmekeskuse jaoks aitab tuvastada, hinnata ja juhtida potentsiaalseid turvariske, mis võivad tekkida selle töö käigus. Tabel võib hõlmata füüsilisi ohte, andmete turvalisusega seotud ohte ja teenuse rikkumisega seotud ohte. See aitab andmekeskusel määrata, millised ohud võivad sellele kõige suuremat mõju avaldada, ning milliseid meetmeid tuleb ohjeldamiseks võtta. Astrec Data OÜ-l on oma ohtude tabel, kuid turvalisuse kaalutlustel ei saa seda avalikustada oma klientide suhtes. Siiski on andmekeskus jaganud oma kogemusi, rääkides millised ohud võivad esineda ja milliste ohtudega on andmekeskus kokku puutunud. Kurjategijad võivad kasutada erinevaid meetodeid, nagu tarkvara haavatavuste ärakasutamine, sotsiaalne insenerlus, pahatahtlikud kalapüügi rünnakud, DDoS-rünnakud ja pahavara, et saada volitamata juurdepääs ettevõtte süsteemidele ja andmetele või selle klientidele.

Ohtude tabeliga saab tutvuda Lisa 9.

3.2. Ründaja profiil

Ründaja, kes üritab saada juurdepääsu kaitstud võrgule andmekeskuses, võib omada häkkerdamise kogemust ning finants-, ideoloogilisi või poliitilisi motiveeringuid. Ta võib teada, kuidas mööda turvasüsteemist hiilida ja kasutada sotsiaalset inseneri. Siiski võib ründaja profiil olla erinev ning on vaja tagada ruumi ja andmete usaldusväärne kaitse võimalike rünnakute ennetamiseks.

Nimi ja perekonnanimi: Borislav Baitov

Hüüdnimi: "DC-hävitaja"

Sünnikoht: "DC hävitaja" sünnikoha kohta pole teave teada. Ta võib olla mistahes riigi kodanik ja tegutseda mis tahes maailma nurgast, kasutades anonüümsuse ja krüptimise vahendeid, et varjata oma identiteeti ja asukohta. See teeb selle hävitava häkkeri otsimise ja vahistamise ülesande õiguskaitseorganite jaoks keeruliseks

Kirjeldus: Borislav Baitov, rohkem tuntud hüüdnimega "DC hävitaja", on ohtlik osaleja infoturbe valdkonnas. Tal on kõrge kvalifikatsioon infotehnoloogia valdkonnas ja ta suudab tungida kaitstud võrguressurssidesse ja häirida nende toimimist, kasutades erinevaid rünnakumeetodeid, sealhulgas DDoS-rünnakuid ja haavatavuste ärakasutamist. "DC hävitaja" suudab põhjustada märkimisväärset kahju ettevõtetele, kes hoiavad oma andmeid andmekeskuses, mille suurus võib olla mitu tuhat ruutmeetrit.

Motivatsioon: "DC hävitajal" võib olla erinevaid motiveeringuid oma rünnakuteks, sealhulgas rahaline kasu, maine häkkerite kogukonnas või lihtsalt soov näidata oma oskusi. Tema eesmärgid ja motivatsioon jäävad teadmata, mis teeb temast veelgi ohtlikuma ja ettearvamatu.

Ajalugu: On teada mitmeid juhtumeid, kus "DC hävitaja" on rünnanud andmekeskusi. Ta hoiab hoolikalt oma identiteeti varjul ega jäta oma rünnakutest jälgi.

Ettevaatusabinõud: soovitatav on tugevdada andmekeskuse loogilist ja füüsilist turvalisust, paigaldada jälgimis- ja sissetungiavastamissüsteem ning rakendada rangeid juurdepääsu- ja autentimispoliitikaid. Soovitatav on teha koostööd kogenud infoturbe spetsialistidega, et välja töötada tõhusaid meetmeid "DC hävitaja" rünnakute ennetamiseks.

3.3. Tuvastatud puudused

Kuigi autoril on raske rääkida puudustest, kuna ainus DDoS-rünnak, mis andmekeskuses toimus, oli ammu ja pole tulnud rohkem teavet võimalike probleemide kohta, eeldatakse, et pärast seda juhtumit täiustas andmekeskus oma liikluse filtreerimise süsteemi ja hakkas regulaarselt looma varukoopiaid andmetest, et vältida teabe kaotamist rünnaku korral.

Autor pööras tähelepanu laest serveriruumi rippuvatele juhtmetele ja kaablitele ning hakkas mõtlema, kas kliendid või töötajad võivad andmekeskusele kahju tekitada. Talle räägiti aga turvasüsteemidest, sealhulgas videoseirest, mis andis mõista, et see on ebatõenäoline, kuid võimalik.

Astrec Data OÜ võtab kõik vajalikud meetmed klientide turvalisuse ja erinevate ohtude vastu kaitsmiseks. Andmekeskus kasutab kaasaegseid tehnoloogiaid ja meetodeid,

nagu liikluse jälgimine ja analüüs, tarkvara värskendamine, andmete varundamine ja palju muud. Personal saab regulaarselt koolitust rünnakute ennetamise ja avastamise meetodite kohta, et tagada maksimaalne turvalisustase klientidele.

4. ASTREC DATA OÜ MODERNISEERIMISE ETTEPANEKUD

Üleminek TIER 2 andmekeskusest TIER 3 andmekeskusele on oluline samm usaldusväärsuse ja jõudluse parandamiseks. [31]

TIER 3 andmekeskused täiustavad TIER 2 konstruktsiooni, mis nõuab infrastruktuuri täiustamiseks mitmeid töid, sealhulgas toiteinfrastruktuuri, jahutussüsteemide, kommunikatsiooniinfrastruktuuri ja turvasüsteemide parandamist. [31]

TIER 3 andmekeskuses peaksid olema topeltsüsteemid toitevarustuse, kliimaseadmete, võrgulülitite, ruuterite ja andmesalvestussüsteemide jaoks. [31]

4.1. TIER 3 - samal ajal toetatav

TIER 3 andmekeskused täiustavad TIER 2 konstruktsiooni, pakkudes täiendavaid varuallikaid kriitilise võimsuse, jahutusvõimsuse/komponentide ning mitme sõltumatu levitamisteede (peamine juhtmeid), mis suudavad teenindada kriitilisi alasid, kui üks neist on kättesaamatu. See võimaldab iga kriitilist alas teenindava komponendi väljalülitamist tehniliseks hoolduseks või väljastuskasutusest, mõjutamata ettevõtte praegust tegevust. [31]

Allpool on mõned märkused seoses TIER 3 andmekeskusega:

- suurenenud võimsus võrreldes TIER 2 konstruktsiooniga;
- sisseehitatud varustus kõigis valdkondades, sealhulgas kriitilised toitekomponendid, jahutus ja levitamisteed;
- oodatav töökindlus tasemel 99,982% aastas, võimalusega autonoomseks tööks kuni 1,6 tundi;
- sobib keskmisele ja suurele ettevõttele, kus on oluline IT-süsteemi usaldusväärsus, eriti teenindamise ja levitamisteede lülitamise korral. [31]

4.2. Üldnõuded

TIER 3 andmekeskus peab projekteerimisel, paigaldamisel ja hooldamisel vähemalt sisaldama järgmist:

- komponendid võivad olla hoolduseks eemaldatavad või samaaegselt hooldatavad - iga komponent, mis tagab võimsuse kriitilistele IT-aladele, saab hoolduseks eemaldada ilma mõjutamata keskkonda, mida see teenindab;
- topeltrajad levitamiseks - kanalid või teed teabe või materjalide edastamiseks, mis pole süsteemi või seadmete tööks hädavajalikud, ja nende teenindusest eemaldamine ei mõjuta neid teenindavat kriitilist keskkonda;

- kriitilise IT-seadme topeltoitmine - IT-seadmel peab olema topeltoitmine, mis võib töötada samaaegselt või lülituda ümber ühe rikke korral. Kasutada võib ülekandlülitid [STS/ATS].
- toitevarustusüsteem (UPS) - seade, mis tagab katkematu ja stabiilse toiteandmise andmekeskusele ja serveritele, takistades pinge kõikumisi, katkestusi ja tõuse. UPS võimaldab ka teatud tüüpi teenindustöid, mis ei mõjuta andmekeskuse tööd;
- varutoiteallika reserveeritud võimsus [N+1] - võime taluda teatud rikkeid ja tehnilist hooldust, mõjutamata andmekeskuse tööd;
- eraldatud IT-süsteemide ala - et servereid ei tuleks paigaldada kontori nurka;
- eriline jahutusseade, mis suudab töötada väljaspool töötunde. Selline seade ei allu taimerite seadistustele ega kasutajate tegevusest põhjustatud katkestustele, tagades selle katkematu töö;
- vajalik on jahutusagregaadi reserveeritud võimsus [N+1], jahutussoojuse eemaldamise üleliigne võimsus [N+1], pumba reserveeritud jõudlus [N+1], jahutusbloki reserveeritud võimsus [N+1] ja jahutusagregaadi juhtimise reserveeritud võimsus [N+1], et tagada teatud rikete ja tehnilise hoolduse võimalus, mõjutamata andmekeskuse tööd. Kui andmekeskus kasutab ühte ülaltoodud seadet, tagab see kõrge usaldusväärsuse ja vastupidavuse võimalike rikete suhtes töös;
- kui kasutatakse aurustava jahutuse süsteemi, on vaja varuvett, millel peab olema 12-tunnine varustusmahuti kohapeal. Lisaks tuleb varustusveesüsteeme hooldada samal ajal;
- mootor-generaator - elektrikatkestuse korral tagatakse vähemalt 12-tunnine kütusevaru tavapärase töö ajal;
- mootorigeneraator on ette nähtud pidevaks tööks;
- mootor-generaatori varurežiimi võimsus [N+1] ja generaatori kütusesüsteemi varurežiimi mahutavus [N+1] - võimalus teatud rikete korral ja tehniline hooldus mõjutamata andmekeskuse tööd;
- samal ajal hooldatav remonditav mootor-generaator - vastab täielikult nõuetele ja on testitud. [31]

4.3. TIER 3 süsteemi projekteerimise ja paigaldamise eelised

TIER 1 ja TIER 2 infrastruktuuriga kombineerituna pakub TIER 3 andmekeskus mõningaid täiendavaid eeliseid. [31]

Tabel 4.1 TIER 3 süsteemi projekteerimise ja paigaldamise eelised [31]

	TÜÜP	KIRJELDUS
1	Suurenenud usaldusväärsus ja katkematu tööaeg	TIER 3 projekteerimine ja paigaldamine tagavad garanteeritud töökindluse ja kättesaadavuse suurenemise andmekeskusele, samuti katkestuste vähendamise tänu kasutatavatele topoloogiliselt eraldatud teedele ja komponentidele kriitilistes valdkondades. TIER 3 tagab usaldusväärsuse tasemel 99,982% ehk kuni 1,6 tundi katkestusi, samas kui TIER 2 võib tagada ainult 99,741% usaldusväärsuse ehk üle 22 tunni katkestusi.
2	Lihtsam uuendada	Kui süsteemid on TIER 3 õigesti kavandatud, siis nende täiustamine on tulevikus lihtsam kui taseme 2 standardi kasutamisel.
3	Suurenenud energiatõhusus	Rohkem võimalusi energiatõhususe ja andmekeskuse käitamisega seotud kulude juhtimise suurendamiseks.
4	Stabiilsem jõudlus	TIER 3 projekteerimisel kasutatud üleliigsete levimisviiside ja komponentide ning kvaliteetsete alltöövõtjate ja tootjate kaasamise kaudu saab saavutada stabiilsema jõudluse kui TIER 2 projekteerimisel, eriti kui tegemist on hooldusest või riketest tingitud seisakute juhtimisega.
5	Rohkem rahulikkust	Tänu suuremale usaldusväärsusele, turvalisusele ja andmekaitsele saavad kliendid ja organisatsioonid olla rahulikumad.
6	Kliendi usalduse suurendamine	Tagab suurema kindlustunde andmete ruumi rentimisel või välisettevõtetele rentimisel.

4.4. Projekteerimise ja paigaldamise TIER 3 süsteemi tähelepanekud

Analüüs tehakse TIER 2 ja TIER 3 projektide vahel, seega on oluline arvestada ja plaanida mitmeid märkusi. [31]

Tabel 4.2 Projekteerimise ja paigaldamise TIER 3 süsteemi tähelepanekud [31]

	TÜÜP	KIRJELDUS
1	Rohkem keeruline	Süsteemid on oma olemuselt keerukamad kui TIER 2 süsteemi konstruktsioon.
2	Nõudmiste suurenemine ruumile	Täiendava varustuse ja jaotusviiside tõttu, mis on vajalikud varundamise ja hooldatavuse tagamiseks, nõuavad süsteemid täiendavat ruumi hoones. Teatud seadmete jaoks eraldi ruumide kasutamine.
3	Õppe- ja tehnilise hoolduse kulude suurenemine	Täiendava seadme paigaldamise tõttu objektil.
4	Operatsioonikulude suurenemine	Lisavahendid on vajalikud seadmete haldamiseks.

4.5. Astrec Data OÜ moderniseerimine

Autor annab soovitusi selle andmekeskuse jaoks, lähtudes teabe põhjal, mis saadi andmekeskuse külastuse ja andmekeskuse esindajaga konsulteerimise käigus. Kuna autor ei saa avalikult kogu saadud teavet näidata, mainitakse töös ainult neid andmeid, mida saab avalikult avaldada ja mis ei kahjusta andmekeskust.

Autor tutvus kõigi ruumidega ja sai teavet selle kohta, kuidas iga süsteem töötab, kuid sai piiratud teavet seadmete kohta, kuna see oli seotud konfidentsiaalsusega ja autor ei olnud teadlik seadmete seisundist.

Hetkel on andmekeskus piiratud võimalustega ja on jõudnud oma piirini, kuna ruumi ja klientuuri puudumine ei võimalda sellest saada TIER 3 keskust. Hoolimata sellest täidab andmekeskus peaaegu kõik nõuded, et olla juba TIER 3 andmekeskus. Andmekeskusel on vähemalt N+1 seadmeid kriitilistes alamsüsteemides, nagu jahutus, võrk ja osaliselt elektrivarustus, mis tagab juba kõrge kättesaadavuse plaanitud hooldusaja jooksul, kuid puudub varugeneraator elektrisüsteemis, kuid selleks on vaja ruumi, mida pole.

Andmekeskusel on mitu aspekti, mis vajavad moderniseerimist, nagu tulekustutussüsteem, jahutussüsteem ja selle optimeerimine, võrguseadmete asendamine ja serveripargi uuendamine, samuti varugeneraatori soetamine ja UPS-ide asendamine. On ka aspekte, mis ei vaja moderniseerimist, nagu varundussüsteemid ja turvasüsteemid, kuna need süsteemid on juba hästi välja arendatud.

4.5.1. Infrastruktuuri muutmine

Andmekeskuse esindaja teatas ekskursiooni ajal autorile vajadusest asendada võrguseadmed uuematega, mis võib tähendada, et praegused seadmed on vananenud ega suuda tagada vajalikku jõudlust ja andmeedastuse kiirust. Võrguseadmete uuendamine võib aidata parandada andmekeskuse jõudlust ja usaldusväärsust.

Võrgu moderniseerimine ja serveripargi uuendamine on täiendavad meetmed, mis võivad aidata parandada andmekeskuse infrastruktuuri. Võrgu moderniseerimine võib hõlmata võrguseadmete uuendamist, võrgutopoloogia muutmist ja uute kaablite paigaldamist. See võib parandada sidekvaliteeti andmekeskuse sees ja välissidevõrkudega.

Serveripargi uuendamine omakorda võib aidata suurendada andmekeskuse jõudlust ja tagada süsteemi usaldusväärsem töö. Uued serverid võivad omada kiiremat protsessorit, suuremat mälumahtu ja rohkem kettaruumi. See võimaldab suurendada arvutustööde jõudlust, tagada kiirema juurdepääsu andmetele ja suurendada süsteemi usaldusväärsust.

Kokkuvõttes hõlmab andmekeskuse infrastruktuuri parendamine mitmeid meetmeid,

mis võivad aidata suurendada jõudlust, usaldusväärsust ja teenuse kvaliteeti. Võrguseadmete uuendamine, võrgu moderniseerimine ja serveripargi uuendamine on sellise protsessi peamised komponendid.

4.5.2. Elektrienergia süsteemi muutmine

Astrec Data OÜ andmekeskusel on kaks toiteallikat: esimene on linna elektrivõrk ja teine on UPS-id (toitevarustusüsteemid) ja diiselmootoriga generaator. Selline lähenemine on standardne ja tagab andmekeskuse usaldusväärsuse ja katkematu töö. Siiski vajab teine toiteallikas täiustamist, sealhulgas UPS-ide asendamist uuemate mudelitega ja varugeneraatori soetamist.

Vanad UPS-id võivad omada väiksemat võimsust ja kui muuta seadmeid, mis tarbivad rohkem energiat, ei pruugi need tagada piisavat toite taset. Lisaks on vajalik varugeneraatori soetamine TIER 2-st TIER 3 tasemele üleminekuks, kuid hetkel pole andmekeskuses selle paigaldamiseks piisavalt ruumi.

Autor arvab, et kui andmekeskus saab rohkem uusi kliente, tuleks kaaluda ruumi ümberkorraldamist või täiendava ruumi loomist seadmete ümberpaigutamise teel. See võimaldab suurendada usaldusväärsuse taset ja vähendada seisakuaega, mis omakorda meelitab uusi kliente.

4.5.3. Jahutussüsteemi muutmine

Kui autor oli andmekeskuses ja suhtles esindajaga, teavitas too autorit vajadusest moderniseerida jahutussüsteemi. Eelnevalt oli märgitud, et andmekeskus kasutab koridoriorganisatsiooni skeemi - külmade ja kuumade koridoridega. Autor leiab, et selline süsteem on energiatõhus ja aitab suurendada serverite jõudlust ning vähendab nende rikete riski. Lisaks sobib selline süsteem ideaalselt väiksematele serveriruumidele, seega pole muu süsteemi asendamine teravalt vajalik ja see oleks kulukas.

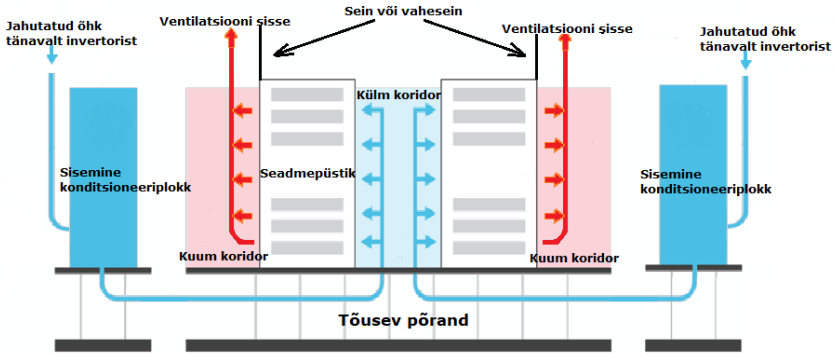
Autor soovitab andmekeskuses jahutussüsteemi moderniseerida. Autor leiab, et on oluline paigaldada tõusev põrand ja eraldatud kuumad ja külmad koridorid. Põrandalus saab kasutada õhu ja serverite ning muu seadme jahtumise jaoks. See võib oluliselt suurendada andmekeskuse turvalisust, varjates kaableid ja juhtmeid klientidele ja külastajatele, et vältida kahjustusi ja volitamata juurdepääsu süsteemidele.

Eraldatud kuumad ja külmad koridorid saab realiseerida serverite ja seadmete ridade paigutamisega. Külm koridor tarnib külm õhk serverikappidesse ja kuum koridor eemaldab kuum õhu seadmetest ja viib selle ruumist välja. Koridorid tuleb eraldada seintega või vaheseintega, et vältida kuumade ja külmade õhuvoolude segunemist, mis võib põhjustada ülekuumenemist ja jahutusprobleeme. Kokkuvõttes võib selline

lahendus oluliselt parandada andmekeskuse efektiivsust, usaldusväärsust ja turvalisust.

Kasutades täiustatud jahutussüsteemi, tuleb teha seadmete seadmepüstikute ja seadmete ümberpaigutus. Kliimaseadmed töötavad järgmiselt: alguses jahutavad nad tänavalt tulevat õhku invertorite abil, seejärel juhitakse õhk siseruumidesse konditsioneeriblokkidesse. Siseruumides asuvad konditsioneeriblokid puhuvad külma õhku tõusva põranda all, suunates selle külma koridori, kus jahutatakse seadmeid. Seejärel liigub soojenenud õhk kuuma koridori ja suundub ülemisele ventilatsioonile, seejärel suundub see välise konditsioneeribloki poole, mis asub hoone katusele. Selliselt tagab süsteem efektiivse jahutamise ja õhuringluse andmekeskuses.

Allpool on esitatud parandatud jahutussüsteemi skeem (Joonis 4.3), mida on lihtne mõista. Skeemil pole kujutatud invertereid ega välisseadmete siseühikuid, kuna need asuvad katuse peal.



Joonis 4.3 Täiustatud jahutussüsteem [32]

Samuti on vaja jahutussüsteemi optimeerimist. Serveriruumides jahutussüsteemi optimeerimiseks tuleb analüüsida praegust süsteemi ja hinnata seadmete seisukorda. Kui seadmed on vananenud ja ei suuda tagada efektiivset jahutust, võib olla vajalik nende asendamine. Soovitatav on pöörduda spetsialistide poole, et valida parim seadmete valik, arvestades serveriruumi eripära ja ettevõtte vajadusi. Soovitused jahutussüsteemi optimeerimiseks hõlmavad õhukonditsioneeride ja ventilatsiooniavade õiget paigutamist, süsteemi regulaarset hooldust, termiliselt tundlike materjalide kasutamist ruumi viimistluses, serveriseadmete õiget paigutamist, et tagada õhuvoolu vaba liikumine ja vältida kuumade tsoonide teket. See on äärmiselt oluline optimaalse temperatuuri säilitamiseks ja seadmete ülekuumenemise vältimiseks.

4.5.4. Tulekustutussüsteemi muutmine

Andmekeskus Astrec Data OÜ kasutab gaasil põhinevat tulekustutussüsteemi, kuid autor ei tea, kas andmekeskus soovib seda süsteemi täiustada ning millist gaasi täpselt kasutatakse. Autor on varem öelnud, et gaasil põhinev süsteem on parim valik, kuid

kõige parem variant oleks hüpoksiline tulekustutusmeetod, mis vähendab ruumi hapniku taset. Autor pakub välja kolm võimalust süsteemi täiustamiseks: gaasi asendamine Inergeniga, mis sarnaneb hüpoksilise tulekustutusmeetodiga või hüpoksilise tulekustusmeetodi kasutuselevõtt, mis võib olla inimestele ja seadmetele ohutum, kuid nõuab hapniku taseme kontrolli; või muudatuste tegemata jätmine.

Allpool on selgitused pakutud muudatuste kohta:

Inergen on kolme inertsusega gaaside segu, mis sisaldab atmosfääriõhus olevaid gaase: lämmastik (52%), argoon (40%) ja süsihappegaas (8%). Euroopas on see tuntud kui IG-541. Inergeniga kustutamise mehhanism seisneb hapniku kontsentratsiooni vähendamises kaitstud ruumis sellisele tasemele, et põlemist ei toimu. Samal ajal on hapniku kontsentratsioon piisav inimese hingamiseks. [33]

Tulekustutussüsteemi balloonide arvu määramiseks tuleb arvutada iga ruumi maht eraldi. Sellel juhul tegi autor ligikaudseid arvutusi serveriruumi jaoks.

Serveriruumi ligikaudne maht on 224 m3. Autor lähtus teabest standardsete seadmepüstikute olemasolu ja umbkaudsete mõõtmete kohta, sealhulgas seadmepüstiku pikkus, laius ja kõrgus.

Standardne serveriruumi seadmepüstiku laius on umbes 0,5 meetrit, vasakul ja paremal pool seadmepüstikut on 1,5 meetrit, seega serveriruumi laius on 3,5 meetrit.

Serveriruumi seadmepüstiku pikkus võib varieeruda, tavaliselt umbes 0,6 meetrit. Serveriruumis on 21 seadmepüstikud, seega 12,6 meetrit. Sellele lisandub ruum enne seadmepüstikut (3 meetrit) ja pärast seadmepüstikut (0,4 meetrit). Serveriruumi pikkus on 16 meetrit.

Standardne serveriruumi seadmepüstiku kõrgus on 1,88 meetrit. Serveriruumis on piisavalt kõrgust, et panna seadmepüstik seadmepüstiku peale ja jääb isegi veidi ruumi. Lõplik kõrgus on 4 meetrit.

Kui serveriruumis kasutatakse tulekustutamiseks inergeni ja kasutatakse 5 balloonid, siis sellise jaotuse korral peaks igal balloonil olema umbes 45 kuupmeetrit mahtu. Siiski, konkreetsete soovituste ja teabe saamiseks saadaolevate balloonide variantide kohta on parim lahendus pöörduda inergeni tarnija või turvalisusekspertide poole.

Üleminek hüpoksilisele tulekustutusmeetodile võib olla kallis ja nõuda täiendavaid ehitustöid hoones. Siiski võib see olla inimestele ja seadmetele ohutum. Tuleb märkida, et hüpoksiline tulekustutusmeetod nõuab ruumis hapniku taseme jälgimist ja reguleerimist, mis võib olla keeruline.

Üldiselt peaks tulekustutussüsteemi valik sõltuma andmekeskuse konkreetsetest vajadustest ja võimalustest. Soovitatav on kasutada spetsialiseerunud konsultantide

teenuseid, et otsustada, milline tüüp tulekustutussüsteemist oleks parim valik ja ei oleks liiga kulukas.

4.5.5. Turvalisuse muutused

Autor on tutvunud andmekeskuse turvameetoditega, nagu kasutajate jälgimine kaamerate ja lugejatega, töötajate ja klientide kasutatavad kaardid ning külastajad täidavad turvalisuse ja juurdepääsu kontrolli blankette. Kappidel on lukustussüsteem, et klient saaks avada ainult oma kapi. Turvamees töötab ööpäevaringselt, kes tegeleb andmekeskusesse sisenemisega. On rakendatud juurdepääsu kontroll, mis võimaldab klientidel juurdepääsu ainult serveriruumile. Igal töötajal on konto, mis kontrollib juurdepääsu ja logides kuvatakse, milline kasutaja ja millal on võrguga ühendatud. Juurdepääsuõiguste eraldamine, kus töötajal ja kliendil on oma autentimisandmed ning neile antakse juurdepääs ainult neile ressurssidele, millel on õigused, ning lisaks filtreerimine MAC-aadressi vastavusse viimiseks lubatud aadresside loendiga. Andmekeskuse sisenemist kontrollitakse 2 meetri kõrguse tara, tõkkepuu ja pöördväravatega, mis takistavad autode liikumist. Autor leiab, et turvalisuse tase on piisavalt usaldusväärne üleminekuks TIER 3 tasemele, kuid viitab ka võimalikele täiustustele, nagu biomeetriline autentimine ja mitmefaasiline autentimine.

Biomeetrilise autentimise kasutuselevõtt, nagu silmapõhja skaneerimine või näotuvastus, võib suurendada juurdepääsu kontrolli usaldusväärsust kriitilistes piirkondades. Mitmefaasilise autentimise rakendamine, kus juurdepääsuks on vaja mitte ainult kaarti või biomeetrilisi andmeid, vaid ka täiendavat tegurit, näiteks ühekordset parooli, mis saadetakse mobiilseadmele, võib samuti turvalisust tugevdada. Võtmete kasutamine, mis genereerivad ühekordselt kasutatavaid paroole või teostavad krüptograafilisi toiminguid kasutajate autentimiseks, on veel üks viis isiku tuvastamiseks ja omab kõrgetasemelist kaitset.

Üldiselt tunnistab autor, et praegused turvameetodid andmekeskuses on usaldusväärsed, kuid soovitab kaaluda täiendavate täiustuste rakendamist, et tagada veelgi kõrgem turvalisuse tase.

4.5.6. Tehtud töö analüüs

Autor annab soovitusi infrastruktuuri, elektrienergia süsteemi, jahutussüsteemi, tulekustutussüsteemi ja turvalisuse täiustamiseks. Siiski on autoril piiratud juurdepääs konfidentsiaalsele teabele, mis piirab tema teadmisi seadmetest ja nende praegusest seisukorrast. Kui autor saaks täpsemaid andmeid seadmete seisundi ja mudelite kohta, oleks tal võimalik pakkuda täpsemaid täiustusi ja kaaluda uute seadmete võimalusi.

KOKKUVÕTE

Vladimir Moskaljovi lõputöö "TIER 3 andmekeskuse projekteerimine Astrec Data OÜ näitel" on pühendatud TIER 3 taseme andmekeskuse projekteerimisele, ohuanalüüsile ja andmekeskuse usaldusväärsuse hindamisele Astrec Data OÜ näitel.

Andmekeskused mängivad olulist rolli meie igapäevaelus, tagades sotsiaalsete võrgustike, e-posti, internetiostude ja suuremahulise teabe säilitamise toimimise. Kaasaegsetes andmekeskustes ühendatakse keeruliselt tehnilised ja infrastruktuurielemendid, luues usaldusväärse ja turvalise keskkonna andmete hoidmiseks ja töötlemiseks. Töös käsitletakse andmekeskuse projekteerimise ja moderniseerimise küsimusi TIER 2-st TIER 3-le üleminekul.

Ülesande täitmise käigus omandas autor arusaama andmekeskuse tööpõhimõtetest, usaldusväärsusest ja tõrkekindluse tagamisest, uuris peamisi andmekeskuse projekteerimise põhimõtteid Astrec Data OÜ näitel Jõhvis, analüüsis usaldusväärsust, turvariske ja koostas andmekeskuse moderniseerimiskava.

Autor sai unikaalse kogemuse konkreetse andmekeskuse uurimisel, kuna tavaliselt ei avaldata nende projekteerimise üksikasju turvalisuse kaalutlustel. Teema on aktuaalne, kuna suur osa meie arvutustest toimub nüüd pilves ning organisatsioonid usaldavad üha enam oma andmete säilitamist ja töötlemist andmekeskustele.

Esimeses osas uuris autor põhjalikult andmekeskuste toimimise põhimõtteid. Autor kirjeldas andmekeskuste kontseptsioone ja uuris nende ärirakendusi. Autor analüüsis ka andmekeskuste komponente ning erinevaid tüüpe ja liike. Autor pööras erilist tähelepanu tasemeklassifikatsiooni süsteemile ja andmekeskuste insenerisüsteemidele. Uuriti andmekeskuste klassifitseerimist ja tasemeklassifikatsiooni. Autor kirjeldas TIER-klassifikatsioonisüsteemi päritolu ja andis ülevaate erinevatest andmekeskuste tasemetest. Autor uuris põhjalikult andmekeskuste insenerisüsteeme, sealhulgas toite-, jahutus-, võrguinfrastruktuuri-, varundus-, tulekustutus- ja turvasüsteeme. Autor analüüsis ka serveriruumide nõudeid ja soovitusi ning andmekeskuste nõudeid Eestis.

Teises osas viis autor läbi analüüsi andmekeskuse Astrec Data OÜ kohta. Autor kirjeldas oma kogemust andmekeskuse külastamisel ja jagas saadud teadmisi. Erilist tähelepanu pöörati katkematule elektritoitele. Autor uuris kahe toiteallika kasutamist ning kirjeldas, kuidas usaldusväärsus tagatakse infrastruktuuri ja varukoopia olemasoluga. Samuti uuriti põhjalikult andmekeskuses kasutatavaid jahutus- ja tulekustutussüsteeme. Autor pööras tähelepanu ka turvalisusele ja kirjeldas meetmeid, mis võetakse väärtuslike andmete kaitseks. Kokkuvõttes pakub teine osa tööst üksikasjalikku analüüsi andmekeskuse Astrec Data OÜ usaldusväärsuse kohta.

Kolmandas osas analüüsis autor seotud andmekeskusega seotud ohte, koostades

üksikasjaliku ohtude tabeli, mis aitab hinnata potentsiaalseid riske ning välja töötada vastavad meetmed nende ennetamiseks ja nendele reageerimiseks. Autor kirjeldas ka ründaja profiili, et täpsemalt tuvastada haavatavusi, määratleda ohuallikas ning võtta meetmeid nende kõrvaldamiseks. Kolmandas osas käsitleti ka tuvastatud puudusi andmekeskuses, et määratleda valdkonnad, mis vajavad parendamist ja täiustamist.

Neljandas osas pakkus autor välja meetmed Astrec Data OÜ kaasajastamiseks, sealhulgas soovitused 3. taseme andmekeskusele ja üldised nõuded selle kavandamiseks. Autor kirjeldas ka põhjalikult andmekeskuse kaasajastamist, sealhulgas infrastruktuuri muutusi, elektritoite süsteemi, jahutussüsteemi, tulekustutussüsteemi ja turvameetmeid. Lõpuks viis autor läbi tehtud töö analüüsi.

Piiratud juurdepääsu tõttu konfidentsiaalsele teabele oli autoril piiratud teave mõne seadme elemendi seisundi ja mudelite kohta. Üksikasjalikum teave seadmete kohta võiks võimaldada autoril teha täpsemaid täiustusettepanekuid. Siiski ei takistanud see autori eesmärkide ja ülesannete saavutamist ning TIER 3 andmekeskuse projekteerimist Astrec Data OÜ näitel.

SUMMARY

Vladimir Moskaljov's bachelor’s thesis "Designing a TIER 3 data centre based on the example of Astrec Data OÜ" is dedicated to the design of a TIER 3 data centre, threat analysis and data centre reliability assessment using Astrec Data OÜ as an example.

Data centres play an important role in our daily lives, supporting social networks, e-mail, online shopping and saving vast amounts of data. Modern data centres combine technical and infrastructural elements in a complex way to create a reliable and secure environment for data storage and processing. This paper examines the design and upgrade of a data centre in the transition from TIER 2 to TIER 3.

While performing the task, the author gained an insight into the principles of data centre operation, data centre reliability and resilience, studied the basic principles of data centre design on the example of Astrec Data OÜ in Jõhvi, analysed reliability and security threats and created a plan for data centre modernisation.

The author gained unique experience from studying a specific data centre, as usually details of their design are not published for security reasons. The topic is relevant because most of our computing now takes place in the cloud, and organisations are increasingly entrusting the storage and processing of their data to data centres.

In the first part of the paper, the author explored in detail the principles of data centre operation. The author described the concept of a data centre and considered its application in business. The author also analysed the components that make up data centres, as well as the different types and types of data centres. The author paid special attention to the TIER classification system and data centre engineering systems. He reviewed data centre classifications, as well as data centre TIER classifications. The author described the origin of the TIER classification system and provided an overview of the different TIERs of data centres. The author looked in detail at data centre engineering systems, which include power, cooling, network infrastructure, backups, and fire and security systems. The author also analysed the requirements and recommendations for server rooms and the peculiarities of data centres in Estonia.

In the second part, the author analysed the data centre of Astrec Data OÜ. The author described his experience of visiting the data centre and shared the knowledge he gained. Particular attention was paid to ensuring uninterrupted power supply. The author looked at the use of two power supplies and described how reliability is ensured with infrastructure and backups. The author also looked in detail at the cooling and fire suppression systems that are used in this data centre. The author has also paid attention to the security issue and described the measures taken to protect valuable data. As a result, the second part of the paper provides a detailed analysis of the reliability of the

Astrec Data OÜ data centre.

In the third part, the author analysed threats related to the data centre, creating a detailed threat table to help assess potential risks and develop appropriate measures to prevent and respond to them. The author also described an attacker profile to more accurately identify vulnerabilities, determine the source of the threat and take action to address them. In the third part, the author also looked at the identified weaknesses in the data centre to identify areas for improvement and enhancements.

In the fourth part of the paper, the author proposed upgrade measures for Astrec Data OÜ, including recommendations for a TIER 3 data centre, and general requirements for its design. The author also described in detail the modernisation of the data centre, including changes to the infrastructure, power supply system, cooling system, fire extinguishing system and security. In the end, the author analyzed the work done.

Due to limited access to confidential information, the author had limited information about the status and models of certain pieces of equipment. More detailed information about the equipment could have allowed the author to suggest more precise improvements. Nevertheless, this did not prevent the author from achieving his goals and objectives and from carrying out the design of the TIER 3 data centre on the example of Astrec Data OÜ.

KASUTATUD KIRJANDUSE LOETELU

1. J. Y. Ong. What Are Data Centers and Why Are They Important? 18.11.2020 [*Online*] https://www.makeuseof.com/what-are-data-centers-and-why-are-they-important/ (14.05.2023).
2. D. Bureau. Data centers still an important aspect for IT industry. 28.01.2020 [*Online*] https://www.dqindia.com/data-centers-still-important-aspect-industry/ (14.05.2023).
3. AWS. Что такое центр обработки данных? [*Online*] https://aws.amazon.com/ru/what-is/data-center/ (14.05.2023).
4. VMware. What is a data center? [*Online*] https://www.vmware.com/topics/glossary/content/data-center.html (14.05.2023).
5. Cisco. What Is a Data Center? [*Online*] https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html (14.05.2023).
6. Usystems. Why do businesses need data centers? [*Online*] https://www.usystems.com/news/why-do-businesses-need-data-centers/ (14.05.2023).
7. Verticomm. 4 Reasons Your Business Should Be Using A Data Center. 21.02.2022 [*Online*] https://www.verticomm.com/post/4-reasons-your-business-should-be-using-a-data-center (14.05.2023).
8. CheckPoint. What is a Data Center? [*Online*] https://www.checkpoint.com/cyber-hub/cyber-security/what-is-data-center/ (14.05.2023).
9. А. Шалагинов. Какие бывают дата-центры. 14.11.2019 [*Online*] https://shalaginov.com/2019/11/14/6604/ (14.05.2023).
10. Nlyte. What Is an Enterprise Data Center. [*Online*] https://www.nlyte.com/faqs/what-is-an-enterprise-data-center/ (14.05.2023).
11. Nlyte. What Is a Colocation Data Center? [*Online*] https://www.nlyte.com/faqs/what-is-a-colocation-data-center/ (14.05.2023).
12. M. Zhang. What is an Edge Data Center? (With Examples). 12.07.2022 [*Online*] https://dgtlinfra.com/what-is-an-edge-data-center/#:~:text=Edge%20data%20centers%20are%20smaller,reducing%20latency%20and%20optimizing%20bandwidth (14.05.2023).
13. VERTIV. What Is a Hyperscale Data Center? [*Online*] https://www.vertiv.com/en-emea/about/news-and-insights/articles/educational-articles/what-is-a-hyperscale-data-center/ (14.05.2023).

14. K. Yasar. Data center. 04.2022 [*Online*] https://www.techtarget.com/searchdatacenter/definition/data-center (14.05.2023).
15. How to pick a data centre with the Tier Classification System. [*Online*] https://sota.co.uk/data-centre-tier-classification-system/ (14.05.2023).
16. UptimeInstitute. Tier Classification System. [*Online*] https://uptimeinstitute.com/tiers (14.05.2023).
17. M. Zhang. Data Center Tiers: What's the Difference Between 1, 2, 3, and 4? 24.06.2022 [*Online*] https://dgtlinfra.com/data-center-tiers-difference-1-2-3-4/#:~:text=The%20Uptime%20Institute%20ranks%20data,anticipated%20downtime%20or%20best%20performance (14.05.2023).
18. С. Филин. Инженерные системы ЦОД. 2016 [*Online*] http://cons-systems.ru/engineering_systems_of_data_center#:~:text=%D0%94%D0%B0%D1%82%D0%B0%2D%D1%86%D0%B5%D0%BD%D1%82%D1%80%20(%D0%BE%D1%82%20%D0%B0%D0%BD%D0%B3%D0%BB.,%D0%B0%D0%B1%D0%BE%D0%BD%D0%B5%D0%BD%D1%82%D0%BE%D0%B2%20%D0%BA%20%D0%BA%D0%B0%D0%BD%D0%B0%D0%BB%D0%B0%D0%BC%20%D1%81%D0%B5%D1%82%D0%B8%20%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82 (14.05.2023).
19. L. Jose. Uninterruptible Power Supply(UPS) in Data Centers. 06.02.2021 [*Online*] https://dc.mynetworkinsights.com/uninterruptible-power-supply-in-data-centers/ (14.05.2023).
20. GenServe. Why are generators important for data center redundancy? [*Online*] https://www.genserveinc.com/2022/09/07/why-are-generators-important-for-data-center-redundancy/ (14.05.2023).
21. A. S. Gillis. Power distribution unit (PDU) 04.2022 [*Online*] https://www.techtarget.com/searchdatacenter/definition/power-distribution-unit-PDU (14.05.2023).
22. J. Mahan. Data Center Cooling 101: From Start to Finish. 20.01.2023 [*Online*] https://cc-techgroup.com/data-center-cooling/ (14.05.2023).
23. VMware. What is data center networking? [*Online*] https://www.vmware.com/topics/glossary/content/data-center-networking.html (14.05.2023).
24. SunnyValley. What is Data Center Networking? [*Online*] https://www.sunnyvalley.io/docs/network-basics/what-is-data-center-networking (14.05.2023).
25. Системы пожаротушения в ЦОД (центрах обработки данных). 17.12.2020 [*Online*] https://pozhavt.ru/stati/pozharotushenie-cod (14.05.2023).

26. C. Shailaja. Physical security of a data center. 31.03.2020. [*Online*] https://www.isa.org/intech-home/2020/march-april/departments/physical-security-of-a-data-center (14.05.2023).
27. Д. Мацкевич. Требования и рекомендации к серверному помещению. 24.01.2009 [*Online*] http://dcnt.ru/?p=559 (14.05.2023).
28. Иерархическая модель сети. 04.02.2018 [*Online*] http://routeworld.ru/set-i-internet/theory/182-ierarhicheskaya-model-seti.html (14.05.2023).
29. M. Hawthorne. What Is Mac Address Filtering? 30.09.2020 [*Online*] https://www.technipages.com/what-is-mac-address-filtering/ (14.05.2023).
30. Data Centre Risk Assessment. [*Online*] https://egs.eccouncil.org/what-is-data-centre-risk-assessment/ (14.05.2023).
31. B. Morris. DATA CENTER TIERS | Uptime – 1, 2, 3 & 4 Explained. 22.02.2023 [*Online*] https://constructandcommission.com/data-center-uptime-tiers-explained/ (14.05.2023).
32. A. Selectel. Системы охлаждения в дата-центрах Selectel. [*Online*] https://selectel.ru/blog/cooling-data-centre-selectel/#name2 (14.05.2023).
33. Инерген - газовое пожаротушение. [*Online*] https://konsel.kz/fire-safety/gazovoe-pozharotushenie/gazovye-ognetushashchie-veshchestva/product/view/28/84 (14.05.2023).
34. S. Sharma. What is a data center? Definition, architecture and management best practices. 25.07.2022 [*Online*] https://venturebeat.com/data-infrastructure/what-is-a-data-center-definition-architecture-and-management-best-practices/#h-data-center-architecture-key-design-components (14.05.2023).
35. CnewsMarket. Преимущества и недостатки Colocation. Подробный обзор. 02.12.2019 [*Online*] https://market.cnews.ru/news/top/2019-10-21_preimushchestva_i_nedostatki (14.05.2023).
36. T. Dawn-Hiscox. What is a hyperscale data center? 13.09.2022 [*Online*] https://www.datacenterdynamics.com/en/analysis/what-is-a-hyperscale-data-center/#:~:text=The%20clue%20is%20in%20the,management%20services%20to%20third%20parties (14.05.2023).
37. Sunbird. What is Data Center Management? [*Online*] https://www.sunbirddcim.com/what-data-center-management (14.05.2023).

LISA 1. ANDMEKESKUSE ARHITEKTUURI KOMPONENDID

Olenemata sellest, kas tegemist on väikese või suure andmekeskusega, ei saa see kunagi lõpule jõuda ilma kindlate põhikomponentideta, mis määravad selle funktsionaalsuse alates IT-operatsioonidest kuni andmete ja rakenduste salvestamiseni. Andmekeskused koosnevad kolmest põhikomponendi tüübist [34]:

- Serverid

  Need on andmekeskuse mootorid. Serveritel võib olla füüsilisi, virtualiseeritud, konteinerites hajutatud või hajutatud kaugemate sõlmede vahel piirarvutuste mudelis kasutatavad töötlemisvõimsus ja mälu, mis on vajalikud rakenduste käivitamiseks. Serverid on arvutiseadmed, mis sisaldavad kõrge jõudlusega protsessoreid, operatiivmälu ja mõnikord graafikaprotsessoreid tohutute andmemahtude töötlemiseks ja rakenduste käivitamiseks. Mitu serveriplokki ühendatakse ühte andmekeskuse riiulisse. Sõltuvalt kasutusviisist võib eraldi server või riiul olla eraldatud ülesandeks, rakenduseks või konkreetsele kliendile. Üldiselt sisaldavad kaasaegsed andmetsentrid tuhandeid erinevaid ülesandeid/rakendusi töötavaid servereid. [34]
- Salvestussüsteemid

  Andmekeskused salvestavad suures koguses konfidentsiaalset teavet nii oma eesmärkide kui ka klientide vajaduste jaoks. Salvestussüsteemid võivad sisaldada kõvakettaid (HDD), tahkesideseadmeid (SSD) või vananenud robotiseeritud lindisalvesteid. Need plokid sisaldavad olulisi äriteavet ja rakendusi mitme varukoopiaga, tagades lõppkasutajatele lihtsa juurdepääsu ja taastumise küberkuritegevuse või hädaolukorra korral. [34]
- Võrgu- ja kommunikatsiooniinfrastruktuur

  See element ühendab andmekeskuse serverid, salvestussüsteemid ja nendega seotud teenused lõppkasutajate asukohtadega. Andmekeskuse võrguseadmete hulka kuuluvad kaablid, võrgulülitid, ruuterid ja tulemüürid, mis ühendavad servereid omavahel ja välismaailmaga. Nõuetekohaselt seadistatud ja struktureeritud võrgud võivad hallata suuri liiklusmahte ilma jõudluse kahjustamata. [34]

LISA 2. ANDMEKESKUSTE LIIGID

Rakenduse meetodi järgi jagunevad andmekeskused järgmisteks:

- statsionaarsed;
- modulaarsed;
- konteinerpõhised (mobiilsed). [9]

Statsionaarsed andmekeskused on paigaldatud spetsiaalselt ettevalmistatud hoonetesse ja ruumidesse, kus on juba paigaldatud kogu vajalik inseneri infrastruktuur: elektrienergia, jahutus- ja kliimaseadmed, füüsilise turvalisuse süsteemid (sealhulgas videovalve) ja muud atribuudid. [9]

Statsionaarsete andmekeskuste eeliste hulka kuuluvad turvalisus ja usaldusväärsus, puuduste hulka kuuluvad kõrged kapitali- ja käituskulud ning pikad rakendusajad. [9]

Modulaarsed andmekeskused on iseseisvad moodulid, mis saab paigutada mis tahes sobivatesse ruumidesse. Andmekeskuse moodul sisaldab kõiki IT-infrastruktuuri elemente: serverid, salvestusseadmed, võrgulülitid ja juhtimissüsteemid; samuti inseneri infrastruktuuri elemendid: mikrokliima, tulekustutus- ja videokontrollsüsteemid. [9]

Modulaarsed andmekeskused võivad olla ka välimust (väljaspool), et neid saaks paigaldada väljaspool ruume. [9]

Joonis 2.1 Modulaarse sisekujundusega andmekeskuse näide [9]

Konteinerpõhised andmekeskused paigaldatakse standardsetesse konteineritesse (40 või 20 jalga), mis on ligikaudu samasugused nagu kaubaveduks kasutatavad konteinerid. See on tehtud andmekeskuste kiiremaks rakendamiseks ja ehituskulude vähendamiseks. [9]

Konteinerpõhiseid andmekeskuseid saab kasutada statsionaarsete või modulaarsete andmekeskuste mahutavuse kiireks laiendamiseks ning ressursside reserveerimise eesmärgil. Selliseid konteinereid on mugav transportida maanteetranspordiga või muude kaubavedude vormidega (meretransport, raudtee) standardsete laadimis- ja

lossimisvahendite abil. [9]

Joonis 2.2 Konteineripõhine andmesidekeskus [9]

Selliseid konteinereid, millel on IT-infrastruktuur, saab paigutada väljaspool ruume, laias temperatuuri ja niiskuse vahemikus, nii arktilises kui ka subtroopilises ning niiskes merelises kliimas. [9]

LISA 3. ANDMEKESKUSTE TÜÜBID

Ettevõtte andmekeskus (Enterprise Data Centers)

Ettevõtte andmekeskus on rajatis, mida organisatsioon kasutab oma andmetöötlus- ja salvestusvajaduste toetamiseks. Seal paikneb füüsiline arvutuslik riistvara, nagu serverid, võrgusüsteemid ja salvestusseadmed, samuti tugiinfrastruktuur, nagu toite-, jahutus- ja keskkonnaseire süsteemid. [10]

Organisatsioonid võivad luua ettevõtte andmekeskuse nii kohapeal kui ka kaugjuhtimisega. Kohaliku andmekeskuse loomine annab teile otsejuurdepääsu oma serveritele ja suurema kontrolli tervikuna. Kuid ilma õige füüsilise infrastruktuurita ei saa te oma andmekeskust tõhusalt ja turvaliselt hallata. [10]

Ettevõtte andmekeskuse eelised:

- täielik kontroll;
- suurenenud nähtavus;
- vastavuse tagamine;
- tarkvara ühilduvus. [10]

Ettevõtte andmekeskuse puudused:

- äärmiselt kallis;
- potentsiaalselt vananenud;
- ootamatud rikked. [10]

Ettevõtte andmekeskused sobivad ideaalselt ettevõtetele, kes tegutsevad range reguleeritud tööstusharudes ja kellel on intensiivsed andmetöötlusvajadused. Kuid arvestades nende objektide ehitamiseks vajalikku kapitali, peab organisatsioon olema kindel, et sellised investeeringud on pikaajaliselt elujõulised. [10]

Kolokatsiooniandmekeskus (Colocation Data Centers)

See on andmekeskus, kus ettevõte saab rentida serverite ja muu arvutitehnika jaoks kohta. On kahte tüüpi:

- hulgimüük - kui rentnik rendib täielikult valmistatud andmetsakeskuse ruumi;
- jaemüük - kui ruum antakse rendile väikestes osades andmetsakeskuses. Colocation'i teenusepakkuja tagab hoone, jahutuse, toiteallika, läbilaskevõime ja füüsilise turvalisuse ning klient pakub servereid ja salvestusruumi. [11]

Colocation'i eelised:

- IT-eelarve kokkuhoid;
- sobiv seadistus seadmetele;
- lihtne IT-infrastruktuuri skaalautuvus;

- tõrkekindlus;
- turvalisus;
- 24/7 tugi;
- IT-spetsialistide ressursside kokkuhoid;
- paindlikkus. [35]

Colocation'i puudused:

- andmetsakeskuse juurdepääsu eripärad;
- juhtimata riskid;
- varustuse moraalne vananemine;
- suhteliselt kõrgem hind. [35]

Colocation'i teenus on väärt alternatiiv oma serverite ruumide või andmekeskuse sisaldamisele. Mõne ettevõtte jaoks on see lihtsalt asendamatu ressurss kõrge efektiivsuse, pideva ja usaldusväärse töö tagamiseks. [35]

Perifeersed andmekeskused (Edge data centers)

Perifeersed andmekeskused on hajutatud objektid, millel on toitmis- ja jahutusinfrastruktuur, mis tagavad arvutusressursside ja salvestusruumi kättesaadavuse lähedal asuvas kohas, kus andmed genereeritakse ja/või kasutatakse. Seega hoiustavad, töötlevad ja analüüsivad servapiiril asuvad andmekeskused andmeid lõppkasutaja asukoha ümbruses, mitte suunavad liiklust lähimasse suurde turule regioonilises või pilvepõhises andmekeskuses töötlemiseks. [12]

Hüpermastaabilised andmekeskused (Hyperscale data centers)

Need on suured ettevõtete jaoks kriitilise tähtsusega objektid, mille eesmärk on tõhusalt toetada usaldusväärseid, skaalautuvaid rakendusi ja sageli seotud suurte andmete hulka tootvate ettevõtetega, nagu Google, Amazon, Facebook, IBM ja Microsoft. [13]

Hüpermastaabilised andmekeskused on märkimisväärselt suuremad kui ettevõtete andmekeskused ja tänu skaalaeeliste ja kohandatud kujunduse kasutamisele ületavad neid oluliselt. [13]

Iga andmesidekeskus, mis sisaldab vähemalt 5000 serverit, omab pinda vähemalt 10 000 ruutjalga (930 ruutmeetrit) ning pakub vähemalt 40 MW võimsust, loetakse hüpermastaabseks (kõik, mis on väiksem, loetakse korporatiivseks andmesidekeskuseks), kuid need kipuvad olema märksa suuremad. [36]

Juhtimise teenustega andmekeskused (Managed services data centers)

Need andmekeskused, mida haldavad kolmandad osapooled, tagavad kõik andmete salvestamise ja arvutusteenuste aspektid. Ettevõtted rentivad infrastruktuuri ja teenuseid, mitte ei osta neid. [14]

Siia kuulub arvutite ja serverite tööde haldamine, suurte andmemahtude haldamine, teenused ja rakendused ning andmete kaitse ja turvalisus. Kuigi mõnda neist ülesannetest tuleb juhtida otse, saab paljusid neist automatiseerida, vähendades sellega kohapealsete töötajate arvu, kõrvaldades ebavajalikud käsitsi tehtavad tööd ja vähendades sellega seotud ärikulusid. [37]

Andmekeskuste juhtidele on vaja tööriistu, mis tagavad tõrkekindluse, parandavad tööaega ja vähendavad riske kogu andmekeskuse infrastruktuuris, sealhulgas võrgus, elektrienergia varustuses, IT-seadmetes, rakendustarkvaras ja rakendusteenustes. [37]

Pilvepõhised andmekeskused (Cloud-based data centers)

Pilveandmekeskuses saab rentida nii ruumi kui ka infrastruktuuri. Pilvepakkuja hoiab suuri andmekeskusi täieliku turvalisuse ja nõuetele vastavusega. Selle infrastruktuuri saate kasutamiseks kasutada erinevaid teenuseid, mis annavad teile suurema paindlikkuse kasutamise ja maksmise osas. [3]

Pilveandmekeskus vähendab nii seadmete investeerimist kui ka igapäevaseid kulusid mis tahes infrastruktuuri hooldamisel. See tagab suurema paindlikkuse kasutamise võimaluste, ressursside jagamise, kättesaadavuse ja üleliigse varukoopia osas. [3]

LISA 4. USALDUSVÄÄRSUSE TASEME NÕUDED

Tabel 4.1 Usaldusväärsuse taseme nõuded [31]

DETAILID	TIER I [1]	TIER II [2]	TIER III [3]	TIER IV [4]
	Baas maht/võimsus	Veebi varundav/dubleeriv infrastruktuur	Paralleelselt teenindatav	Tõrgetele/vigadele vastupidav
Aktiivsed IT-koormust toetavad komponendid	Normaalne	Normaalne +1	Normaalne +1	Normaalne pärast igasugust riket
Generaatorsüsteem	Põhiline toiteallikas ja kommunaalvõrk	Põhiline toiteallikas ja kommunaalvõrk	Põhiline toiteallikas ja kommunaalvõrk	Põhiline toiteallikas ja kommunaalvõrk
Elektrijuhtmed	1	1	1 Aktiivne 1 Alternatiivne	2 Aktiivset samaaegselt
Jahutussüsteemi juhtmed	1	1	1 Aktiivne 1 Alternatiivne	2 Aktiivset samaaegselt
IT-seadmete toitejuhtmed	1	1	1 Aktiivne 1 Alternatiivne	2 Aktiivset samaaegselt
Paralleelne teenindamisvõimekus	Ei	Ei	Jah	Jah
Tõrkekindlus	Ei	Ei	Ei	Jah
Kompartmenteeritus	Ei	Ei	Ei	Jah
Eraldatud IT-tsoon	Jah	Jah	Jah	Jah
Eraldatud jahutusseadmed	Jah	Jah	Jah	Jah
Piisav IT-võimekus kriitilise komponendi väljalülitamisel	Ei	Jah	Jah	Jah
Varutoite süsteemid (UPS)	Normaalne	Normaalne +1	Normaalne +1	Normaalne pärast igasugust riket
Täiendav veevarustus	Normaalne [12-tunnine varu]	Normaalne [12-tunnine varu]	Normaalne +1 [12-tunnine varu]	Normaalne pärast igasugust riket [12-tunnine varu]
Generaatori mootori reiting	Põhiline	Põhiline	Pidev	Pidev
Generaatori mootor/kütuselement	Normaalne [12-tunnine varu]	Normaalne [12-tunnine varu]	Normaalne +1 [12-tunnine varu]	Normaalne pärast igasugust riket [12-tunnine varu]

LISA 5. JAHUTUSMEETODID

1. Arvutiruumi õhukäitleja (CRAH) - andmekeskuse jahutussüsteemi osa, mis kasutab jahutatud vett ventilaatorite moduleerimiseks ja välisõhu tarnimiseks ruumi sisse. CRAH töötab kõige paremini kohtades, kus on madalamad aastatemperatuurid. [22]

2. Arvutiruumi konditsioneer (CRAC) - CRAH alternatiiv, mis kasutab kompressoreid õhu jahutamiseks jahutusainega täidetud bloki kaudu. CRAC ei ole energiatarbimise seisukohalt kõige tõhusam valik, kuid on taskukohane. [22]

3. Aurusti jahutussüsteemid kasutavad loomulikku aurustumisprotsessi õhust soojuse eemaldamiseks ja on keskkonnasõbralikud ja energiatõhusad jahutusmeetodid. Tõukekarbid on sageli kasutatud aurustumise hõlbustamiseks ja liigse soojuse atmosfääri juhtimiseks. Aurustusjahutus on suurepärane võimalus ettevõtte energiatarbimise vähendamiseks. [22]

4. Kalibreeritud vektorjahutus optimeerib õhuvoolu ja kuumuse juhtimise teed. Jahedat õhku suunatakse läbi kuumade elektroonikakomponentide, et neid jahutada. Süsteemi eesmärk on kasutada võimalikult vähe energiat ja ventilaatoreid ühe võimalikult suure arvu serverite jahutamiseks. [22]

5. Külm koridor/Kuum koridor (Cold Aisle/Hot Aisle) - riiulite paigutamise meetod, kus vahelduvad "kuumad" ja "külmad" koridorid. Kuumad koridorid väljastavad kuuma õhu kliimaseadmete õhuvõtukollektoritesse, seejärel jahutatakse õhku ja väljastatakse külmadesse koridoridesse. Paneelide kasutamine tõkestamaks külma õhu kaotust ja ülekuumenemist. Seda süsteemi nimetatakse mõnikord ka reakseeriva jahutamise meetodiks. [22]

6. Jahutusvedelikuga otsene kiibijahutus - meetod, kus vedel jahutusaine pihustatakse otse protsessori jahutusplaadile ja eraldunud soojus edastatakse jahutatud vee ahelasse. Seda meetodit peetakse üheks kõige tõhusamaks andmekeskuse jahutamisviisiks. [22]

7. Tõusev põrand - süsteem, kus andmekeskuse põrand tõuseb raamile, luues uue ruumi õhuvoolu suurendamiseks või veepõhise jahutussüsteemi paigaldamiseks.

8. Süvistatav jahutus (Immersion Cooling). Sissejuhtumiskülmamine on uus süsteem, kus seadmed sukeldatakse mittesüttivasse ja mittetjuvooluslikku dielektrilisse vedelikku. [22]

9. Looduslik jahutus - süsteem, mis kasutab välist õhku jahutamiseks. See on energiatõhusam kui mittelooduslikud jahutussüsteemid, kuid seda saab rakendada ainult teatud kliimatingimustes. [22]

10. Vedeljahutus- see on süsteem, mis kasutab vedelikku õhu jahutamiseks. See muutub üha populaarsemaks andmekeskustes, kuna võimaldab serverikomponente kiiremini jahutada. Mõnes süsteemis mõjutab vedelik otse serverikomponente, näiteks sukelduskülmumissüsteemis. [22]

LISA 6. VÕRGU-, SERVERI- JA SALVESTUSINFRASTRUKTUUR

Võrgu-, serveri- ja salvestusinfrastruktuur on kolm peamist komponenti, mis moodustavad andmekeskuse võrgu. Nende komponentide ühendamine ja koostöö on vajalik kiiremate ja usaldusväärsemate andmeside teenuste tagamiseks. Andmekeskuse ressursid, nagu võrgulülitid ja marsruuterid, aitavad tagada katkematu ja tõhusa andmeliikluse andmekeskusesse ja sellest välja, olenemata selle asukohast - kas see on kohapeal, avalikus pilves või kaasomaniku asukohas. Need seadmed on kriitilise tähtsusega andmekeskuse infrastruktuuri osad, mille andmeedastuskiirus võib ulatuda kuni 400 Gbit/s pordi kohta. [24]

Andmekeskuse võrgulahendused - st andmekeskuse infrastruktuuri jälgimise terviklahendused - on eluliselt tähtsad andmekeskuse toimingute jaoks, et säilitada kõrge võrgutöö tõhusus ja vastavus teenindustaseme lepingutele (SLA) võrguteenuste osas. Nende võrgulahenduste abil saab füüsilisi ja virtuaalseid servereid ning salvestusseadmeid jälgida, kontrollida, diagnoosida ja veaolukordi lahendada. [24]

Nende komponentide koostöö peab olema kooskõlastatud, et tagada kriitilise tähtsusega äritaristu ja teenuste usaldusväärne kohaletoimetamine. [24]

1. Server

   Andmekeskuse infrastruktuuri mootoriks on server. See toimib erinevate teenuste ja rakenduste hostina ning tagab arvutusvõimsuse arvutustegevuseks. Kuna kogu võrguinfrastruktuur on kavandatud ja konfigureeritud serveri maksimaalse jõudluse tagamiseks, on see andmekeskuse kõige olulisem komponent. [24]

   Serverid on igas andmekeskuses tavapärane osa. Andmekeskuse server on suure mälumahtuvusega kõrge jõudlusega arvuti. Sellel on keskprotsessor, mis on märkimisväärselt kiirem ja võimsam. Üks ülesanne, mitu rakendust või konkreetne klient võivad olla määratud serverile või serverite rühmale. [24]

   Andmete salvestamise süsteemid, nagu kõvakettad, tahkiselaadurid ja automaatsed lindiseadmed, on otsustava tähtsusega iga andmekeskuse võimekuse jaoks käivitada need serverid. Veel üks oluline komponent on võrgu- ja kommunikatsioonivarustus, mis on vajalik võrgu suure läbilaskevõime säilitamiseks serverite vahel. See koosneb marsruutereist, lülititest, võrguliideste kontrolleritest ja kilomeetritest kaablitest, mis võimaldavad andmetel andmekeskuses liikuda. [24]

2. Säilitamine

   Riistvara, tarkvara ja protseduurid, mis toetavad ja kontrollivad andmete säilitamist andmekeskuses, nimetatakse andmekeskuse säilitussüsteemiks. See kehtib kõigi

andmekeskuse IT-varade kohta, mis salvestavad, tõmbavad välja, levitavad, varundavad või säilitavad arvutite andmeid ja rakendusi. Erinevalt "IT-säilitussüsteemist", mis hõlmab nii kohapealset kui ka väliseid salvestusressursse, viitab "andmekeskuse säilitussüsteem" ainult kohapealsele säilitamisele. Võrgusalvestustehnoloogiate näited hõlmavad andmesalvestusvõrke (SAN), võrgusalvesteid (NAS) ja mitme sõltumatu ketta massiivseadmeid (RAID). Muud näited hõlmavad kõvakettaid, lindimäluseadmeid, otsese andmeside seadmeid (DAS), säilituse ja varundamise tarkvarautiilsid ning võrgusalvestustehnoloogiaid, nagu SAN-võrgud. [24]

Andmekeskuse säilitussüsteem hõlmab ka andmete kogumist ja levitamist, juurdepääsu kontrolli, salvestussüsteemi turvalisust, andmete kättesaadavust, salvestusruumi kvootide järgimist, varukoopia kavasid, andmete säilitamise perioode ja muid reegleid ja protseduure, mis reguleerivad andmete säilitamist ja väljavõtmist. Andmekeskuse säilitussüsteem peab vastama riigi- ja kaubandusseadustele, mis reguleerivad andmete säilitamist, teabe konfidentsiaalsust ja andmete turvalisust rahanduse, meditsiini ja muudes rangelt reguleeritud valdkondades. [24]

Säilitussüsteem võib olla kas füüsilise serveri sees või eraldiseisva seadmena, mida tuntakse säilitusmassiivi või ketasmassiivina. Suurte andmemahtude säilitamiseks kasutatakse massiivides mitut ketast. Massiive juhib tsentraliseeritud süsteem ja need on seadistatud efektiivseks IOPS-ide arvuks (sekundis sisend-väljund operatsioonid). [24]

3. Võrk

Serverid, salvestusruum ja võrk on andmekeskuse infrastruktuuri kolm põhikomponenti. Rakendused vajavad servereid arvutusvõimsuse ja andmete hoidmise tagamiseks ning võrku, et ühendada kasutajaid ja teisi rakendusi. Võrk eksisteerib rakenduste ühendamisvajaduste rahuldamiseks ning rakendused teenindavad oma organisatsiooni äri vajadusi. [24]

Andmekeskuse seadmed, nagu kaablid, võrgulülitid, ruuterid ja tulemüürid, ühendavad serverid üksteisega ja välismaailmaga. Õige planeerimise ja korralduse korral saavad need töödelda suuri liiklusmahte ilma efektiivsuse kaotamiseta. Traditsioonilises kolmetasemelises võrgustruktuuris seovad põhilised võrgulülitid andmekeskuse piiri Internetiga ning keskmine üldine tase ühendab baastaseme juurdepääsutase, kus serverid kolmetasemelises võrgustruktuuris asuvad. Tänu arengutele nagu hüper-skaalutatav võrguturvalisus ja tarkvaralised võrgud pakuvad andmekeskuse kohalikud võrgud tänapäeval pilve tasemel mobiilsust ja skaldeeritavust. [24]

LISA 7. TULEKUSTUTUSSÜSTEEMID

1. Pulber- ja aerosoolisüsteemid. Kõige taskukohasem tulekustutussüsteem on seadmed, mis pihustavad tulekustutavat aerosooli või pulbrit. Selle tulemusena tekib kuumadel pindadel kile, mis takistab hapniku tungimist ja seega tulekahju. Peamine puudus on osakeste kõrge läbitungivus. Nii pulbrid kui ka aerosoolid võivad hõlpsasti sattuda serveriseadmetesse, kus nad settivad ja põhjustavad metallielementide korrosiooni ja lühiseid. [25]

Selliste tulekustutusvahenditega seadmete lihtsaid ja tõhusaid puhastamisviise ei ole olemas, seega võib tulekahju andmekeskuses tekitada vähem kahju kui pulbri- või aerosoolisüsteemi tulekustutuse käivitamine. Seadmete kahjustus korrosiooni tõttu võib olla viivitatud. [25]

Ökoloogia ja personali mõju seisukohalt kujutab see tüüp tulekustutussüsteeme teatavat ohtu. Aktiveeritud moodulite asendamine ei tekita raskusi ja see on odav. [25]

2. Gaasipõhised tulekustutussüsteemid. Andmekeskustes on kõige levinumad tulekustutussüsteemid gaasipõhised süsteemid. Selliste lahenduste plussid on ilmsed - gaasi kasutamine ei kahjusta kallist varustust, see tungib suurepäraselt isegi raskesti ligipääsetavatesse kohtadesse ja läbi ventilatsiooniavad - seadmete korpustesse. [25]

Kasutatavad gaasid (erinevad jahutusained jne) on inimestele suhteliselt ohutud, kuid tulekahju korral võivad tekkida erinevad kahjulikud ühendid, seetõttu pole tulekahju ajal ruumis personali viibimine lubatud. Praegu kasutatavad gaasipõhised tulekustutussüsteemides kasutatavad gaasid kuuluvad tavaliselt fluoroheksaani klassi, mis on keskkonnasõbralikud ja ei kahjusta osoonikihti. [25]

Gaasipõhiste tulekustutussüsteemide ümberlaadimine pärast käivitamist on üsna kallis protseduur. [25]

3. Veepritsesüsteemid, mis põhinevad veeudu pihustamisel. See kustutusmeetod pole veel laialt levinud kõrge hinna ja murede tõttu seoses võimaliku veekahjustusega serveritele ja muule paigaldatud tehnikale andmesaalides. [25]

Süttimise lokaliseerimise ja kustutamise meetod töötab süttimiskohtadele peene hajutatud destilleeritud vee (ja seega elektrit juhtimatu) juhtimisega. [25]

Veeudu põhiste tulekustutussüsteemide kasutamisel kulub võrreldava tõhususega sprenklersüsteemidega võrreldes umbes 10% vett. Kuid nende hind on märkimisväärselt kõrgem tänu vajadusele pumbata ja edastada väga suurt survet (sadu või enam korda atmosfäärirõhust). [25]

Süsteemi uuesti täitmine pärast käivitumist ei nõua märkimisväärseid finantsinvesteeringuid. [25]

4. Tulekustutamine hüpoksiaalse meetodiga. See meetod ei võitle juba tekkinud tulekahjuga, vaid ei lase sellel üldse tekkida tänu hapniku kontsentratsiooni vähendamisele andmesaalide õhus. See meetod on kõigist teistest oluliselt tõhusam, kuid ka märgatavalt kallim. [25]

Spetsiaalne seade eraldab lämmastiku atmosfäärõhust ja viib selle andmekeskustesse. Selle tulemusena väheneb hapniku tase kuni 14% -ni, mis takistab tulekahju tekkimist. Inimesed saavad selles ruumis töötada, kui neil ei ole olulist füüsilist koormust. [25]

LISA 8. SERVERIRUUMI NÕUDED JA SOOVITUSED

1. Serveriruumi paigutus

Peamised nõuanded serveriruumi paigutamisel - paigutage see lähedale peamistele kaablikanalitele ja vältige paigutamist hoone elementide lähedusse, nagu liftišahtid, trepikäigud ja ventilatsioonikambrid, et mitte piirata tulevikus ruumi laiendamise võimalust. Samuti soovitatakse paigutada serveriruum võimalusel lähedale peamisele jaotuskeskusele. [27]

2. Serveriruumi laiendamine

Soovitatakse paigutada serveriruum selliselt, et oleks võimalik serveriruumi laiendada naaberruumi ala arvelt. [27]

3. Soovitatavad serveriruumi suurused

Peamised nõuanded serveriruumi suuruse valimisel - valige see vastavalt teenindatava tööala suurusele ja paigaldatava seadmete arvule, arvestage seadmete paigaldus-, juurdepääsu- ja hooldusviisidega ning võimalusega paigaldada täiendavaid seadmeid. Soovitatav on, et serveriruumi kõrgus oleks vähemalt 2,44 meetrit ja minimaalne serveriruumi suurus oleks 14 ruutmeetrit. Samuti soovitatakse eraldada serveriruumi jaoks 0,09 ruutmeetrit pinda iga 10 ruutmeetri teenindatava tööala kohta. [27]

4. Soovitatavad serveriruumi suurused spetsialiseeritud hoonetes

Spetsialiseeritud hoonetes, nagu hotellid, haiglad või laborid, kus telekommunikatsioonipistikute tihedus on madal, soovitatakse valida serveriruumi suurus vastavalt tööpiirkondade arvule. [27]

Tabel 8.1 Soovitatav serveriruumi suurus spetsiaalkasutusega hoonetes. [27]

Tööpiirkondade arv	**Serveriruumi suurused, m^2**
kuni 100	14
101-400	37
401-800	74
801-1200	111

5. Veekahjustuste kaitse

Nõuanded serveriruumi turvalisuse tagamiseks: Vältige serveriruumi paigutamist maa-alusest tasemest allapoole, kui pole veeprotsendi kaitset. Ärge paigutage torustikku ega äravoolusüsteemi serveriruumi, kui need pole ette nähtud serveriruumis asuvate seadmete ja erisüsteemide tööks. Paigaldage äravool, kui on võimalus veekahjustuse tekkeks serveriruumis, näiteks paigutage põrandale äravooluava. Kui serveriruumis kasutatakse pritsimissüsteeme, soovitatakse paigaldada äravoolukanalid torustike alla,

mis juhivad pritsimisvedelikku, et kaitsta seadmeid võimaliku lekke eest. [27]

6. Aknad

Soovitatakse serveriruumi jaoks kasutada aknata ruumi. Kui serveriruumis on aknad, siis tuleb need kinni müürida tellistega. [27]

7. Uks ja ukseava

Serveriruumi ukse valimisel tuleb arvestada järgmiste teguritega. Ukseava peab olema vähemalt 0,91 meetrit lai ja 2 meetrit kõrge. Uks peab olema lukustatav turvalisuse tagamiseks. Kui kavatsetakse viia suuri seadmeid serveriruumi, soovitatakse paigaldada topeltuks, mille minimaalne ava on vähemalt 1,82 meetrit lai ja 2,28 meetrit kõrge. See võimaldab mugavat juurdepääsu seadmetele ja takistab võimalikke kahjustusi nende liigutamise ajal. [27]

8. Ripplagi

Serveriruumis ei soovitata kasutada ripplagesid. [27]

9. Seinte, lae ja põranda viimistlus

Ruum peab olema varustatud kattega, mis raskendab tolmu kogunemist. Lael peaks olema hüdroisolatsioon. [27]

10. Koormus tõusvale põrandale ja põrandaplaadile

On vaja arvutada tõusva põranda ja põrandakatuse dünaamiline ja staatiline koormus, kui on plaanis paigaldada raskeid seadmeid, näiteks akusid või suurt hulka rasket seadmet ühte paigaldusstruktuuri (üle 500 kg). [27]

11. Mikrokliima (temperatuur, niiskus, ventilatsioon)

Mikrokliima kontrolli- ja juhtimissüsteem peab tagama serveriruumis määratud niiskuse ja temperatuuri taseme, mis on arvestatud ööpäevaringselt pideva töö jaoks. Kui tsentraliseeritud mikrokliima süsteem ei suuda tagada määratud taset, tuleb serveriruumis paigaldada autonoomne süsteem. [27]

Tabel 8.2 Soovitatav temperatuur ja niiskus serveriruumis [27]

Soovitatav temperatuur	**Soovitatav suhteline niiskus**
18 °C - 27 °C	40% - 55%

Optimaalsete töötingimuste tagamiseks serveriruumis tuleb arvestada mitme olulise teguriga: temperatuuri ja niiskuse mõõtmine külma õhu sissevoolu piirkonnas või jahutusvee montaažikonstruktsioonis, õhurõhu tagamine suurem kui ümbritsevates

ruumides, ruumi õhuvahetuse vähemalt 1 kord tunnis hooldus personali töö ajal, sissevoolava õhu puhastus- ja filtreerimissüsteemi kasutamine riistvararuumis ning mikrokliima toetussüsteemi ühendamine varutoite süsteemiga, kui selline süsteem hoones olemas on. [27]

12. Kahjulike ainete kaitse

Serveriruumi tuleb kaitsta tolmu ja kahjulike ainete eest, mis võivad mõjutada negatiivselt seadmete tööd ja seadmete materjale. Kahjulike ainete kontsentratsioon serveriruumis ei tohi ületada lubatud piirnorme. [27]

Tabel 8.3 Lubatud piirnorm kahjulike ainete suhtes serveriruumis [27]

Kahjulik aine	**Lubatud piirnorm**
Kloor	0.01 ppm (promille)
Tolm	100 mg/m3/päevas
Süsivesinikud	4 mg/m3/päevas
Vesiniksulfiid	0.05 ppm (promille)
Lämmastikoksiidid	0.1 ppm (promille)
Vääveldioksiid	0.3 ppm (promille)

Vajadusel tuleb kasutada sissevoolava õhu puhastus- ja filtreerimissüsteemi. Õlifiltrite kasutamine riistvararuumides ei ole lubatud. [27]

13. Vibratsioon

Vibratsioon mõjutab negatiivselt aktiivseid seadmeid, kontakte ja ühendusi. Sagedusalas kuni 25 Hz ei tohi vibratsiooni amplituud ületada 0,1 mm. [27]

14. Serveriruumi valgustus

Serveriruumi nõuetekohase töö tagamiseks tuleb järgida järgmisi valgustamissoovitusi: valgustustase peab olema vähemalt 500 luksi ja mõõdetakse 1 meetri kõrgusel põrandapinnast, valgustusseadmed peavad olema paigaldatud laele, lülitid tuleb paigutada 1,5 meetri kõrgusele põrandapinnast ja lähedale uksele. Samuti tuleb tagada eraldi toiteallikas valgustusele ja telekommunikatsiooniseadmetele, toites neid erinevatest elektrikilpidest. On oluline keelata valgustuse sujuva reguleerimise seadmete kasutamine. [27]

15. Elektromagnetilised häired

Serveriruum tuleb paigutada eemal elektromagnetiliste häirete allikatest sellises kauguses, et elektrivälja tugevus serveriruumis ei ületaks 3 V/m kogu sagedusalas. [27]

16. Elektritoide ja elektripistikud

Soovitatav on paigaldada vähemalt 2 kahekordset elektripistikut, mis on toidetud erinevatest toitekaablitest, mis on mõeldud vahelduvvoolule kuni 16 A ja paigutatud kõrgusele mitte alla 0,15 meetri põrandapinnast, vahega 1,8 meetrit seina ääres. Serveriruumi tuleb toita eraldi toitekaabliga, eelistatavalt otse peakaitsmekapist. Kui on paigaldatud varutoite süsteem, tuleb serveriruumi toita sellest. Samuti tuleb paigaldada eraldi elektriline jaotuskapp serveriruumile. Sellega seoses on lubatud paigaldada UPS (toitevarustusseade) kuni 100 kVA serveriruumi, kuid võimsusega üle 100 kVA tuleb neid paigaldada eraldi ruumi. [27]

17. Maandamine

Riistvaruumis peab olema paigaldatud peamine telekommunikatsiooni maandusriba, millele tuleb ühendada maandus- ja ühendusjuhtmed montaažikonstruktsioonidest, telekommunikatsiooniseadmetest ja metallist kaabelkanalitest. [27]

18. Peamiste kaabelkanalite paigaldamine serveriruumi

Serveriruumi tuleb paigaldada peamised kaabelkanalid. [27]

19. Kaablivahendite ja kaablikäikude korraldamine

Telekommunikatsiooniruumis tuleb kasutada kaablivahendeid ja korraldajaid kaablite jaotamiseks. Need tuleb kindlalt kinnitada ja tagada kaablite kaitse minimaalse painderaadiusega. Kaablikanalid tuleb paigaldada kaabelsisendist telekommunikatsioonikappideni ning lae all asuvad kanalid peavad olema avatud edasiste tööde tegemiseks. [27]

20. Serveriruumi kaablivõrgu sisendid

Serveriruumiga töötades tuleb järgida tuleohutuseeskirju. Kaablivõrgu sisendid tuleks paigutada aparaadiruumi lähedale ukse kõrvale ning need tuleb tulekindla materjaliga sulgeda. Laekatte, seinad, vaheseinad ja serveriruumi uks peavad olema mittesüttivad ning tagama tulekindluse vähemalt 36-45 minutit. Tulekahju korral suitsu eemaldamiseks tuleks paigaldada väljatõmbekorstnad, mille pindala on vähemalt 0,2% ruumi pindalast ja mis ei ole kaugemal kui 20 meetrit korstnast. Sprinklerite paigaldamisel soovitatakse katta sprinkleripead kaitsevõrkudega, et vältida juhuslikku aktiveerimist. Toed, riiulid ja valepõrandaplaadid peavad olema mittesüttivast materjalist ning valepõranda ülemine kate võib olla süttivast materjalist. [27]

21. Ligipääsupiirangud

Serveriruum ei tohi olla läbikäidav ruum. Serveriruumi uks peab olema lukustatav. Ligipääsu aparaadiruumile, mida kasutavad mitu klienti, peab korraldama ja kontrollima hoone omanik või tema esindaja. [27]

22. Identifikaator ja märgistus

Kõik aparaadid peavad omama unikaalset identifikaatorit ning neil peab olema märgistus uksele või ukse lähedale. [27]

23. Serveriruumi süsteemide varustamine

Serveriruumis tuleb varustada järgmised süsteemid: turvasignalisatsioon, tulekahjusignalisatsioon, tulekustutus, konditsioneerimine ja ventilatsioon, samuti valgustus ja hädaolukorra valgustus. [27]

LISA 9. OHU TABEL

Tabel 9.1 Ohu tabel

Ohustuse nimi	**Ohustuse kirjeldus**	**Ohustuse allikad**	**Potentsiaalsed kuritegelikud tegevused**	**Ettepanekud objekti kaitsmise parandamiseks**
Seadmete kahjustamise oht	Seadmete ja infrastruktuuri kahjustamine, füüsiline hävitamine volitamata juurdepääsu kaudu objektile, näiteks häkkimise või füüsiliste takistuste ületamise teel	Objekti läheduses viibivad või spetsiaalse murdmiseks mõeldud seadmetega varustatud kurjategijad	Andmete vargus või hävitamine, seadmete või infrastruktuuri kahjustamine või hävitamine, andmekeskuse kriitiliste elementide hävitamine	Objekti turvalisuse tugevdamine, videovalve ja ligipääsukontrollisüstee mi paigaldamine
Andmete kaotamise oht volitamata juurdepääsu tõttu objektile	Andmete kaotamise oht volitamata juurdepääsu tõttu objektile, näiteks häkkimise või füüsiliste takistuste ületamise teel	Objekti läheduses viibivad või spetsiaalse murdmiseks mõeldud seadmetega varustatud kurjategijad	Andmete vargus või hävitamine, pahatahtliku koodi sisestamine, varjatud kaamerate või mikrofonide paigaldamine nuhkimiseks	Objekti turvalisuse tugevdamine, videovalve ja ligipääsukontrollisüstee mi paigaldamine
Konfidentsiaalsuse kaotamise oht privileegide tõstmise kaudu	Volitamata juurdepääs võrgule objektil häkkimise või volitatud kasutajaandmete lekke kaudu	Kurjategijad, kes kasutavad süsteemi haavatavusi, püüavad läbi viia kalatehnikaga rünnakuid, lekitavad kasutajaandmeid	Andmete vargus, muutmine või hävitamine, kahjuliku koodi sissetoomine, nuhkvara paigaldamine	Võrgu turvalisuse tõstmine, sealhulgas krüpteerimine, tarkvarauuenduste tegemine ja juurdepääsu kontrolli tugevdamine
Konfidentsiaalse teabe lekkimise oht	Volitamata sissetung süsteemi andmekeskuses kolmandate kanalite kaudu	Volitamata juurdepääs, töötajate vigu, kahjulikud programmid, kalatehnikad, sisemised rünnakud, tööstuslik luurekogumine	Konfidentsiaalsete andmete vargus, nende muutmine või levitamine, ärilise saladuse leke	Range ligipääsukontrolli reeglite kehtestamine, töötajate koolitus, mitmetasandiline autentimine ja andmete krüpteerimine, jälgimise ja juurdepääsu auditeerimise süsteemi paigaldamine
Volitamata tarkvara sissetungi oht andmekeskuse süsteemi	Volitamata sissetung süsteemi andmekeskuses kolmandate kanalite kaudu	Häkkerid, botnetid, viirused, troojalased, riistvara- ja tarkvaralised tagatised, sotsiaalne inseneritöö	Andmete vargus või hävitamine, nuhkimine, süsteemi töö blokeerimine, väljapressimine	Kaasaegsete kaitse süsteemide paigaldamine, andmete krüpteerimise kasutamine, liikluse filtreerimise seadistamine, regulaarne tarkvara uuendamine. Antiviiruse tarkvara ja sissemurdmise avastamise süsteemi paigaldamine, personali koolitamine küberjulgeoleku alustes

Teenusetõkestus (DDoS) rünnakuoht	Rünnakud andmekeskuse infrastruktuurile, mille eesmärk on ülekoormata võrguressursse ja katkestada juurdepääs teenustele	Botnetid, massiivsed päringud serveritele, sünkroniseeritud rünnakud erinevatest allikatest	Võrguressursside ülekoormus, teenuste tõrked, andmete kaotus, tööseisak	Liikluse filtreerimise süsteemi paigaldamine, turvameetmete sündmuste jälgimine, süsteemi reageerimiskiiruse parandamine, võrgu läbilaskevõime suurendamine, varukoopia andmete loomine.
Oht kasutada teisi kanaleid volitamata teabe hankimiseks	Volitamata juurdepääs konfidentsiaalsele teabele ja andmetele, mis liiguvad andmekeskusesse või sellest välja, läbi volitamata sidekanalite	Kõik tüübid luuretööst, kalatehnikat, sotsiaalset inseneritööd, tarkvara ja süsteemide haavatavuste ärakasutamist, jälgimist, avatud allikate analüüsi, jäätmete ja heitmete analüüsi, kaamerate ja jälgimissüsteemide paigaldamist	Andmete vargus, andmete asendamine, andmete hävitamine, luuretöö, konfidentsiaalsuse rikkumine	Objekti füüsilise ja loogilise turvalisuse tugevdamine, krüptograafiliste meetodite kasutamine andmete kaitseks, turvameetmete sündmuste jälgimise süsteemi paigaldamine..
Sotsiaalse inseneritöö ohud	Risk probleemide tekkimiseks seoses inimeste manipuleerimisega juurdepääsu saamiseks konfidentsiaalsele teabele	Võltsitud e-kirjad, pettus, kalatehnika	Kasutajate volitatud andmete vargus, kahjuliku tarkvara paigaldamine arvutitesse	Regulaarne personali koolitamine sotsiaalse inseneritöö avastamise tehnikate osas, mitmeteguriline autentimissüsteemi paigaldamine, võrguliikluse jälgimise süsteemi kasutamine, regulaarne turvasüsteemi testimine
Elektrienergia katkemise oht ekstreemsete ilmastikutingimuste tõttu	Tormid, orkaanid, tugevad tuuled, äikesetormid, lumetormid, paduvihmad	Seadmete rikke ja juurdepääsu kaotus teabele, samuti andmete kaotus ja seadmete kahjustumine	Elektrienergia kaotus ekstreemsete ilmastikuolude tõttu	Elektrienergia varustuse varundamine, katkematu toite süsteemide kasutamine, varutoiteallikate kasutamine, piksekaitsepaigaldiste kasutamine, vandalismivastaste korpusete kasutamine seadmete jaoks.
Hoone või seadmete kahjustamise oht ekstreemsete ilmastikuolude tõttu	Tormid, orkaanid, tugevad tuuled, äikesetormid, lumetormid, paduvihmad, üleujutused, maavärinad	Kaablite, seadmete, infrastruktuuri ja hoonete kahjustamine, mis viib juurdepääsu katkemiseni teabele ja andmete kaotusele	Hoone või seadmete kahjustamine ekstreemsete ilmastikuolude tõttu	Infrastruktuuri ja seadmete varundamine, hoonete tugevdamine, kaitsekorpuste kasutamine, hädaolukorras avastamis- ja teavitussüsteemide paigaldamine

Seadmete kahjustamise oht ruumi üleujutuse või torude purunemise tagajärjel	Üleujutused, torude purunemine	Andmete kaotus, seadmete ja infrastruktuuri kahjustus	Hoone või ruumi üleujutus nõnade või torude purunemise tõttu	Leke avastamise süsteemide paigaldamine, spetsiaalsete kaitsevahendite kasutamine, kriitiliste infrastruktuurielementide reserveerimine kõrgematel korrustel, regulaarne infrastruktuuri ja seadmete seisundi kontrollimine
Seadmete ja infrastruktuuri kahjustamise oht ilmastikutingimuste ja loodusõnnetuste tagajärjel	Tuul, tolm, lumi, vihm	Seadmete kahjustamine, mis viib juurdepääsu katkemiseni teabele ja andmete kaotusele	Seadmete ja infrastruktuuri saastumine ilmastikutingimuste tõttu	Ventilatsioonisüsteemide filtrite paigaldamine, seadmete ja infrastruktuuri regulaarne puhastamine
Tulekahju tagajärjel tekkiva seadmete ja andmete kahjustamise oht	Tulekahju tekkimise oht, mis võib põhjustada hoone, seadmete ja teabe hävitamist või kahjustamist	Lühis elektriseadmetes, küttesüsteemide rikked, põlevate materjalide olemasolu	Seadmete hävitamine või kahjustamine, andmete kadu või kahjustumine, äritegevuse katkestamine	Tuleohutussüsteemide väljatöötamine ja rakendamine, tulekahjualarmi- ja tulekustutussüsteemi regulaarne kontroll ja hooldus, töötajate koolitamine ja treenimine tulekahju korral tegutsemiseks