UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

INFORMACIJSKA VARNOST V RAČUNALNIŠKIH CENTRIH SKUPINE HSE

Ljubljana, marec 2019 SAMO FEKONJA

IZJAVA O AVTORSTVU

Podpisani Samo Fekonja, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Informacijska varnost v računalniških centrih skupine HSE, pripravljenega v sodelovanju s svetovalcem prof. dr. Mirom Gradišarjem,

IZJAVLJAM:

1. da sem predloženo delo pripravil samostojno;
2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;
3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;
4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;
5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;
6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;
7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;
8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;
9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu prek Repozitorija Univerze v Ljubljani;
10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi.

V Mariboru, dne _____ Podpis študenta: _____

KAZALO

UVOD 1

1 SPLOŠNO O INFORMACIJSKI VARNOSTI V RAČUNALNIŠKIH CENTRIH 3

1.1 Standardizacija v računalniških centrih 5

1.1.1 SIST ISO/IEC 27001:2013: Sistem za upravljanje informacijske varnosti 5

1.1.2 ISO 22301:2012: Načrt neprekinjenega poslovanja 6

1.1.3 ANSI/TIA 942: Telekomunikacije v računalniških centrih 7

1.1.4 EN 50600: Evropski standardi za računalniške centre 7

1.2 Elementi računalniških centrov 8

1.3 Storitve in modeli računalniških centrov 9

1.3.1 Storitveni modeli računalniških centrov 9

1.3.2 Modeli uporabe računalniških centrov 9

1.4 Organizacija in vloge v računalniških centrih 9

1.5 Zagotavljanje neprekinjenega delovanja računalniškega centra 10

1.5.1 Zanesljivost 11

1.5.2 Razpoložljivost 12

1.5.3 Oskrba z električno energijo 15

1.5.4 Sistemi za tehnično hlajenje 17

1.5.5 Sistemi za nadzor 17

1.5.6 Sistemi za detekcijo in gašenje požara 21

1.6 Fizična in informacijska varnost računalniških centrov 22

2 ANALIZA STANJA INFORMACIJSKE VARNOSTI V RAČUNALNIŠKIH CENTRIH DRUŽB IZ SKUPINE HSE 23

2.1 Računalniški centri v skupini HSE 24

2.1.1 Lokacija računalniških centrov in potresna izpostavljenost 26

2.1.2 Računalniški center DEM 27

2.1.3 Računalniški center TEŠ 31

2.2 Učinkovitost računalniških centrov skupine HSE 35

2.3 Ocena skladnosti računalniških centrov skupine HSE po metodologiji TUV36

2.4 Obvladovanje procesov v računalniških centrih skupine HSE 37

2.5 Skladnost računalniških centrov skupine HSE s standardom ISO/IEC 27001:2013 38

3 VZPOSTAVITEV ENOTNEGA SISTEMA UPRAVLJANJA VAROVANJA INFORMACIJ V RAČUNALNIŠKIH CENTRIH SKUPINE HSE 39

3.1 Izhodišča za delovanje računalniških centrov po prenovi 40

3.2 Prepoznani procesi pri upravljanju računalniških centrov 40
3.3 Kontrole za izvajanje procesov v računalniških centrih skupine HSE 41
3.3.1 Organizacija in človeški viri 43
3.3.2 Upravljanje infrastrukture 48
3.3.3 Izvajanje varovanja 50
3.3.4 Spremljanje in nadzor 51
3.4 Metodologija ocenjevanja tveganj v računalniških centrih skupine HSE 53
3.5 Izjava o primernosti SOA (ang. Statement of Applicability) 55
3.6 Podeljene vloge, naloge in odgovornosti 56
3.7 Izvedba testiranj oskrbne infrastrukture 57
3.8 Ključni indikatorji uspeha 64
3.9 Prenova procesa upravljanja računalniških centrov skupine HSE 64
SKLEP 65
LITERATURA IN VIRI 65

KAZALO SLIK

Slika 1: Računalniški center podjetja DEM, d. o. o. 3
Slika 2: Standardizacija v računalniških centrih 5
Slika 3: EN50600: EU-standardi za računalniške centre EN50600 8
Slika 4: Vloge pri upravljanju računalniških centrov 10
Slika 5: Stopnje odpovedi tehniških sistemov 11
Slika 6: Poraba električne energije v računalniških centrih 16
Slika 7: Sistem za nadzor infrastrukture v RC – diagram napajanja 18
Slika 8: Arhitektura nadzornega sistema 21
Slika 9: Plin Novec 1230 22
Slika 10: Sistem gašenja DC DEM 22
Slika 11: Topologija obstoječega hrbteničnega TK-omrežja HSE 25
Slika 12: Komunikacijska MPLS-arhitektura DC HSE 26
Slika 13: Potresni zemljevid Republike Slovenije 27
Slika 14: Lokacija DC DEM 28
Slika 15: Dinamična UPS in razvod napajanja 29
Slika 16: Tloris računalniškega centra DC DEM 30
Slika 17: Kroženje zraka v DC DEM 30
Slika 18: Tloris računalniškega centra TEŠ 31
Slika 19: Električno napajanje računalniškega centra TEŠ 32
Slika 20: Organiziranost IT v skupini HSE 38
Slika 21: Stanje računalniških centrov HSE pred prenovo in po prenovi 39
Slika 22: Procesi in kontrole ISMS v RC skupine HSE 41
Slika 23: Matrika razpoložljivosti 54

Slika 24: Matrika ocene tveganja 54

KAZALO TABEL

Tabela 1: Kontrole ISO 27001 (dodatek A) 6
Tabela 2: TIER-klasifikacija 15
Tabela 3: Proizvodnja električne energije v skupini HSE 24
Tabela 4: PUE in stroški 35
Tabela 5: Skladnost z metodologijo TIER III 36
Tabela 6: Kontrola organizacije informacijske varnosti 43
Tabela 7: Kontrole varnosti osebja 45
Tabela 8: Tabela, namenjena kontrolam zunanjih partnerjev 46
Tabela 9: Kontrole za upravljanje dobrin 47
Tabela 10: Kontrole upravljanja energije in hlajenja 48
Tabela 11: Kontrole varovanja omrežja 48
Tabela 12: Kontrole informacijskih storitev 49
Tabela 13: Kontrole za upravljanje okolja 50
Tabela 14: Kontrole, namenjene vandalizmu in vlomu 50
Tabela 15: Kontrole za analizo 51
Tabela 16: Kontrole pri izvajanju vzdrževanja 51
Tabela 17: Kontrole za upravljanje incidentov 52
Tabela 18: Kontrole za podporo neprekinjenemu poslovanju 52
Tabela 19: Tabela groženj 55
Tabela 20: Testiranje alarmiranja na napravah 59
Tabela 21: Testiranje in kalibracija senzorjev naprav 60
Tabela 22: Testiranje avtomatskega zagona DEA 61
Tabela 23: Delni obremenilni test – testiranje akumulatorskih baterij 62
Tabela 24: Integralni obremenilni test – odpornost proti izpadom 62

SEZNAM KRATIC

ang. - angleško
HSE – Holding Slovenske elektrarne, d. o. o.
DEM – Dravske elektrarne Maribor, d. o. o.
DC DEM – računalniški center DEM
DC TEŠ – računalniški center TEŠ
VVSP – visoko varni sistemski prostor
SLA – (ang. service level agreement); pogodba o izvajanju storitev
ISO/IEC – organizacija mednarodnih standardov/mednarodni elektrotehniški komite
ANSI/TIA – ameriški nacionalni inštitut za standardizacijo/združenje za telekomunikacije
PDCA – (ang. plan, do, check, act); načrtuj, naredi, preveri, ukrepaj

IT – (ang. information technology); informacijske tehnologije
IaaS – (ang. infrastructure as a service); infrastruktura kot storitev
PaaS – (ang. platform as a service); platforma kot storitev
SaaS – (ang. software as a service); programska oprema kot storitev
MTBF – (ang. mean time between failure); povprečni čas med odpovedmi
TIER – stopnja ureditve napajalnih sistemov
UPS – (ang. uninterruptible power supply); naprava za neprekinjeno napajanje
DEA – dizelski električni agregat
STS – statično preklopno stikalo
IEEE – Institute of Electrical and Electronics Engineers
IKT – informacijsko komunikacijske tehnologije
SMS – (ang. short message service); storitev kratkih sporočil
DCIM – (ang. data center infrastructure management); sistem za nadzor informacijske infrastrukture
LMI – lokalni nadzor za zajem podatkov
CNS – centralni nadzorni sistem
IO – (ang. input/output); vhod/izhod
DWDM – (ang. dense wavelength division multiplexing); zgoščeni način združevanja signalov
NG SDH – (ang. new generation synchronous digital hierarchy); nova generacija sinhrone digitalne hierarhije
TK – telekomunikacijsko omrežje
UDP – (ang. user datagram protocol); uporabniški datagram protokol
PDU – (ang. power distribution unit); električni razdelilnik
NN – nizka napetost
NDA – (ang. non-disclosure agreement); pogodba o nerazkrivanju
SSH – (ang. secure shell); protokol šifriranega prenosa
VPN – (ang. virtual private network); navidezno zasebno omrežje
SOA – (ang. statement of applicability); izjava o primernosti

UVOD

Zahteve po zanesljivih digitalnih informacijah so danes vse večje, pri čemer računalniški centri igrajo vse bolj pomembno vlogo ob zagotavljanju stalne dostopnosti in varnosti vseh vrst podatkov in transakcij. V računalniških centrih so v osnovi nameščeni strežniki, podatkovna skladišča in omrežne naprave. Zanje skrbi oskrbna infrastruktura, kot so: napajalne naprave, brezprekinitveni napajalni sistemi in sistemi tehničnega hlajenja, ponavadi v podvojeni konfiguraciji. Za nadzorovano in učinkovito delovanje zanje skrbijo različni nadzorni in varnostni sistemi, ki so nadgrajeni še s fizičnim varovanjem.

Kompleksnost in neprekinjena rast panoge računalniških centrov, od skrbnikov do vgrajene opreme, zahteva vse večjo razpoložljivost in zanesljivost. Zanesljivost v veliki meri povezujemo s sposobnostjo elementa ali sistema opravljati predvidene funkcije v danem času (Lavuger, 2016). Da bi zadostili zahtevam trga, lastnikov, skrbnikov in uporabnikov omenjene infrastrukture, nastaja množica pobud za vzpostavitev ustrezne zakonodaje, standardizacije in dobrih praks pri načrtovanju, izgradnji in tudi vzdrževanju računalniških centrov. (Levy & Raviv, 2017)

Tako kot je osnovni ukrep za zagotavljanje varnosti in zaščite informacijskih sistemov vzpostavitev nadzora dostopa do podatkov, računalniških naprav in omrežja (Gradišar, Jaklič, Damij & Baloh, 2005), je tudi za zagotavljanje informacijske varnosti v računalniških centrih treba izvesti mnogo ukrepov, ki bistveno presegajo samo informacijsko varnost. Preden upravljalec izbere ukrepe za zagotavljanje varnosti, ki so v veliki meri odvisni od zahtevane stopnje razpoložljivosti, je treba določiti lestvico vpliva izpada kritične infrastrukture na poslovanje podjetja (Moises & Hallstrom, 2017). Glavni elementi vpliva na tveganja v računalniških centrih so: produktivnost, učinkovitost, trajnost in sama izvedba. Vsi omenjeni elementi so med seboj povezani in soodvisni ter jih je treba – z ustreznimi mehanizmi – meriti in zanje pripraviti ustrezne ukrepe ali izboljšave. Pri tem bo treba zagotoviti ustrezno povezanost s standardi in dobrimi praksami iz nabora standardov za kakovost storitev, informacijskega varovanja, neprekinjenega poslovanja, komunikacijskih storitev, energetske učinkovitosti ter vodil tehnološke infrastrukture računalniških centrov. Samo s celovitim organizacijskim pogledom na upravljanje računalniških centrov bo mogoče vzpostaviti ustrezno matriko vlog in odgovornosti na področju kritične infrastrukture ter sestaviti ustrezen klasifikacijski načrt, od katerega bodo odvisni postopki in pravila pri standardizaciji opreme in namestitvene infrastrukture, osnova za projektiranje in enostavnejše določanje veljavnih pravil.

Pri vzpostavitvi učinkovitega sistema varovanja kritične infrastrukture upravljalci in načrtovalci velikokrat prezrejo zelo pomemben element – potrebo po prihodnji porabi električne energije in njen vpliv na obvladovanje tveganj po neprekinjenem napajanju in posledično neprekinjenem poslovanju. V študiji ameriškega nacionalnega laboratorija Berkeley (Shehabi in drugi, 2016) avtorji ugotavljajo bistveno porast porabe električne

energije v računalniških centrih in napovedujejo velik napredek v razvoju energetske učinkovitosti. Z novimi tehnologijami veriženja blokov se potreba po električni energiji znatno zvišuje, za tovrstne in prihodnje potrebe bo treba zagotoviti mehanizme, ki bodo še naprej omogočali neprekinjeno poslovanje. Energetska učinkovitost je tako postala eno od gonil razvoja in investicij v segmentu računalniških centrov, pri čemer neposredno vpliva na varnost pri delovanju kritične infrastrukture. Omenjena problematika je slabo podprta z ustreznimi standardi, ki so v veliko primerih pomanjkljivi ali celo zastareli, zaradi česar se načrtovalci zatekajo k splošno sprejetim standardom o varnosti in zanesljivosti napajalnih sistemov (IEEE, 2007).

Tudi v skupini HSE (Holding Slovenske elektrarne, d. o. o.), ki je največji proizvajalec in prodajalec električne energije v Sloveniji (HSE, 2016), se potreba po celovitem upravljanju varnosti in poenotenju procesov upravljanja v dislociranih računalniških centrih vse bolj izpostavlja. Pomanjkanje formalnih postopkov celovitega upravljanja virov in zagotavljanja ustrezne ravni varnosti, tako podatkov kot opreme, predstavlja določeno tveganje. Pomanjkanje formalnih pravil in kompliciranе matrike standardov, ki se opredeljujejo do samo manjšega dela omenjene problematike, povzroča upravljalcem in lastnikom mnogo preglavic. Pri izgradnji in še posebno kasneje pri vzdrževanju ter upravljanju kritične informacijske infrastrukture, kamor nedvomno spadajo računalniški centri, je treba zagotoviti ustrezna pravila v obliki politik ali navodil, ki bodo živela in se razvijala skozi ves življenjski cikel.

Namen magistrskega dela je pripraviti platformo za učinkovito obvladovanje vseh varnostnih aspektov pri načrtovanju in obvladovanju računalniških centrov v skupini HSE. Pregledali se bodo obstoječi mehanizmi varovanja informacij v računalniških centrih vseh družb skupine, pri čemer se bodo iskali sinergijski učinki in dobre prakse posameznih družb. Poudarek bo na trajnostnem upravljanju in energetski učinkovitosti.

Cilj magistrske naloge je analiza obstoječega sistema varovanja kritične infrastrukture, identifikacija ključnih virov, ki morajo biti pravilno umeščeni v obstoječe poslovne procese, ter zapis osnovnih vodil in politik pri celovitem varovanju računalniških centrov v skupini HSE. Z zapisano rešitvijo bo mogoče poenotiti procese varovanja v vseh družbah skupine in jih enakovredno umestiti v obstoječe poslovne procese. Z uporabo priloge A iz standarda ISO/IEC 27001:2013 bom izdelal natančen spisek ukrepov za ovladovanje vseh tveganj pri upravljanju in delovanju računalniških centrov.

Metode dela bodo temeljile na preučitvi že vzpostavljenih sistemov varovanja informacij v računalniških centrih po svetu, pregledu ustrezne domače in tuje literature in vzpostavitvi matrike standardizacije na področju upravljanja virov v računalniških centrih. V delu analize obstoječih stanj bodo uporabljeni intervjuji zaposlenih na strokovnih področjih, povezanih z varovanjem in vzdrževanjem kritične infrastrukture v skupini HSE, ter dobre prakse v podobnih podjetjih iz energetske panoge. Primerjali se bodo obstoječi postopki iz nabora sistemov vodenja z novonastalo matriko pravil in politik. Na osnovi izvedenih analiz se bo

po metodi sinteze izdelala enotna platforma za celovito upravljanje varovanja informacij in enotno vzdrževanje vseh računalniških centrov v skupini HSE.

1 SPLOŠNO O INFORMACIJSKI VARNOSTI V RAČUNALNIŠKIH CENTRIH

V literaturi in na svetovnem spletu se za poimenovanje računalniških centrov, kot je na sliki 1 prikazan računalniški center podjetja DEM, d. o. o. (Dravske elektrarne Maribor), uporabljajo mnogi različni termini – sistemski prostor, podatkovni center, varna soba, visoko varni sistemski prostor, kolokacijski center, računalniški prostor, računalniški sistemski prostor. Ko govorimo o računalniškem centru, se opredeljujemo do tehničnega objekta, ki centralizira opremo informacijsko-komunikacijskih tehnologij organizacije in v katerem ta hrani, vodi in objavlja svoje podatke ter storitve informacijskih tehnologij. Po Gartnerju pravijo, da je računalniški center tisti prostor v podjetju, ki vsebuje in vzdržuje računalniške sisteme za končne uporabnike, strežnike in podatkovne baze, in to vse na enem mestu. Po njihovo so samostojni računalniški centri redki, pogostejši so distribuirani, v večini primerov celo virtualizirani, modularne zgradbe, namenjeni podpori oblačnim storitvam (Gartner, 2018).

Slika 1: Računalniški center podjetja DEM, d. o. o.



Vir: DEM d.o.o. (2014).

Računalniške centre nekateri opredeljujejo tudi kot vzporedne in distribuirane računalniške sisteme, sestavljene iz zbirke med seboj povezanih in virtualiziranih računalnikov, predstavljene kot ena enota. Delovanje omenjene entitete sloni na pogodbah, ki jih sklepajo ponudniki storitev in končni uporabniki (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009). Računalniški centri gostijo najbolj kritične sisteme v računalniškem omrežju ali informacijskem ekosistemu. So bistvenega pomena za neprekinjeno delovanje sodobnih organizacij. Posledično je ena od glavnih prednostnih nalog sodobnih organizacij vzdrževanje varnosti in zanesljivosti podatkov ter storitev. Bistvene karakteristike računalniških centrov so (Li, 2014):

- dostop na zahtevo – uporabnik definira potrebo po informacijski storitvi, kot so: procesorska moč, potreba po pomnilniku, velikost podatkovnega skladišča, trajanje storitve, pri čemer mu računalniški center in storitve, ki jih ta ponuja, to tudi avtomatsko omogočajo,
- merljivost storitev – nadzorni in upravljalski sistemi omogočajo merjenje uporabe virov (električne energije, diskovni prostor, število procesorjev, čas …), ki jih je mogoče uporabniku tudi zaračunati,
- mrežni dostop – računalniški centri ponujajo uporabniško platformo, ki omogoča uporabnikom izvajanje njihovih nalog,
- deljenje virov – vire računalniških centrov je mogoče, v skladu s podpisanimi pogodbami (ang. SLA – service level agreement), deliti med uporabniki in informacijskimi sistemi,
- virtualizacija – uporabniku ni treba poznati računalniške topologije oz. tega, kateri strežnik podpira njegovo storitev. Računalniški centri lahko na enostaven način migrirajo aplikacije z enega strežnika na drugega, vse z namenom boljše izkoriščenosti virov,
- zanesljivost – vsebine imajo redundantne ali podvojene kopije,
- vzdrževanje – uporabnikom ni treba skrbeti za vzdrževanje, saj to počno za to usposobljeni vzdrževalci računalniških centrov in sistemov.

Preden se vzpostavi učinkovit sistem zaščite računalniškega centra, se je treba, z ustrezno pripravljeno strokovno presojo, jasno opredeliti do vseh tveganj in groženj, ki vplivajo na delovanje omenjenega centra, pri čemer imamo v mislih identifikacijo vseh nevarnosti, ranljivosti in slabosti, ki lahko ogrozijo poslovanje družbe ali organizacije. Vsaka družba bo na osnovi lastnih pravil razvila svoje operativne zahteve po upravičeni zaščiti vseh komponent računalniškega centra in postopkov, ki iz tega sledijo. Seveda je to povezano z dejavnostjo, s katero se ukvarjajo njihovi lastniki; zahteve po varovanju računalniških centrov v vojaški industriji se v mnogočem razlikujejo od onih v finančnih ustanovah, pa vendarle, osnovne funkcije so si precej podobne in o njih bom pisal v magistrskem delu.

V osnovi računalniški centri ponujajo podporo informacijskim storitvam, do katerih dostopajo uporabniki, pri čemer je najpomembneje, da zaščitimo naslednje logične elemente (van Niekerk, 2015):

- protokol dostopa,
- storitev, informacijo ali aplikacijo,
- platformo (virtualno ali tradicionalno),
- omrežje,
- fizične dostope in varnostne elemente.

1.1 Standardizacija v računalniških centrih

V svetovni literaturi ni primera, v katerem bi en v panogi uveljavljen standard pokrival vse zahteve po varnosti v računalniških centrih. Nenazadnje je tudi raznolikost komponent tako velika, da delovanje in varnostne protokole ter procese pokriva kar nekaj mednarodno priznanih standardov. Najcelovitejši je standard ISO/IEC 27001:2013 ali sistem upravljanja varovanja informacij, prikazan na sliki 2, ki nadgrajuje standard kakovosti ISO 9001 in temeljito predstavi organizacijski nivo upravljanja in varovanja v računalniških centrih. Nepogrešljivi standardi pri načrtovanju, vzdrževanju in varovanju računalniških centrov so še: ISO/IEC 22301:2012 ali neprekinjeno poslovanje, ANSI/TIA 942 ali telekomunikacijski standard za računalniške centre, ISO/IEC 27005:2011 ali sistem za upravljanje tveganj in standard za tehnološko infrastrukturo računalniških centrov EN 50600. Pristop do celovitega varovanje je interdisciplinaren in od načrtovalcev in upravljalcev terja nenehno izobraževanje.

Slika 2: Standardizacija v računalniških centrih



Vir: lastno delo.

1.1.1 SIST ISO/IEC 27001:2013: Sistem za upravljanje informacijske varnosti

Glavna skrb omenjenega standarda je varovanje informacijskih virov, posledično pa zagotavlja okolje za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema za upravljanje informacijske varnosti. Kako se bodo izvajali varnostni mehanizmi in kakšni so cilji vzpostavitve tovrstne podpore, je stvar vsake organizacije. Standard pomaga z napotki na organizacijskem nivoju in z dodatkom ISO/IEC 27002 (nekoč priloga standarda A) postavlja pravila obnašanja pri kontrolah informacijske varnosti. Temelji na izvajanju aktivnosti s ciklom PDCA (ang. plan, do, check, act ali načrtuj, naredi, preveri, ukrepaj) ali Demingovem krogu, pri čemer se sistematično opredeljuje do tveganj, celovito obravnava procese, rešuje probleme in predlaga spremembe. Uspešnost sistema je pogojena z aktivnim sodelovanjem tehnologije, organizacije in ljudi.

Najpogosteje se računalniški center obravnava kot informacijski vir, pri čemer se, po ISO/IEC 27001:2013, za obravnavanje tveganj in priložnosti izdela ocena tveganj informacijske varnosti po zapisani metodologiji. Vsa tveganja se obravnavajo v skladu z določenimi in uporabljenimi pravili, hkrati se določijo tudi kontrole, ki so potrebne za izvajanje izbranih možnosti obravnavanja tveganj informacijske varnosti. Standard se jasno opredeljuje do vseh virov, potrebnih za delovanje sistema upravljanja varovanja informacij, tako človeških, pravnih kot tudi tehnoloških (SIST, 2014).

Pri upravljanju računalniških centrov je ključna nadgradnja zgoraj opisanega standarda standard, ki opisuje varnostne tehnike in pravila obnašanja pri kontrolah informacijske varnosti, imenovan ISO/IEC 27002:2013 (SIST, 2013). Zapisana pravila se uporabljajo kot referenca pri izbiri kontrol znotraj procesa varovanja informacij, hkrati pa dajejo družbi smernice za upravljanje informacijske varnosti za naslednja ključna področja:

Tabela 1: Kontrole ISO 27001 (dodatek A)

Številka	Cilj kontrole	Št. kontrol
1	A5. Informacijske varnostne politike	2
2	A6. Organiziranje informacijske varnosti	7
3	A7. Varnost človeških virov	6
4	A8. Upravljanje dobrin	10
5	A9. Nadzor dostopa	14
6	A10. Kriptografija	2
7	A11. Fizična in okoljska varnost	15
8	A12. Varnost operacij	14
9	A13. Varnost komunikacije	7
10	A14. Pridobivanje, razvoj in vzdrževanje sistemov	13
11	A15. Odnosi z dobavitelji	5
12	A16. Upravljanje informacijskih varnostnih incidentov	7
13	A17. Vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja	4
14	A18. Skladnost	8
	Skupaj kontrol:	**114**

Vir: Prirejeno po SIST (2013).

Družba, ki upravlja varnost v skladu s standardom ISO/IEC 27001:2013, se mora opredeliti do vseh kontrol iz dodatka A, zapisanega v tabeli 1. Katero od kontrol je mogoče opustiti, vendar družba za to potrebuje ustrezen razlog in ga ustrezno tudi zapiše.

1.1.2 ISO 22301:2012: Načrt neprekinjenega poslovanja

Neprekinjeno poslovanje je sposobnost družbe, da po incidentu ali varnostnem dogodku nadaljuje poslovne procese na sprejemljivi in vnaprej določeni ravni. Sistem neprekinjenega poslovanja v osnovi vzpostavlja, implementira, upravlja, nadzira, vzdržuje in izboljšuje poslovno kontinuiteto. Deluje tako kot standard ISO/IEC 27001:2013, na osnovi Demingovega kroga, pri katerem so elementi PDCA naslednji (Estall, 2012):

- plan (načrtuj) – vzpostavlja politiko neprekinjenega poslovanja, cilje, kontrole, procese in procedure za izboljšanje, z namenom, da se uskladijo s splošnimi politikami in cilji družbe,
- do (naredi) – izvaja in upravlja politiko neprekinjenega poslovanja, kontrol, procesov in postopkov,
- check (preveri) – spremlja uspešnost izvajanja politik glede na cilje neprekinjenega poslovanja, poroča vodstvu o rezultatih ter določa ukrepe za izboljšavo,
- act (ukrepaj) – spremlja in izboljšuje sistem upravljanja neprekinjenega poslovanja, temelječ na rezultatih vodstvenega pregleda in ponovno ocenjuje vsebino in ustreznost politike in ciljev neprekinjenega poslovanja.

Za uspešnost implementacije tovrstnega sistema v podjetju ni dovolj vključenost osebja IT (informacijska tehnologija), vanjo morejo biti vključeni vsi segmenti poslovanja, zelo pomembna je popolna zavezanost vodstva. Vodstvo je tisto, ki ne zagotavlja samo potrebnih virov, ampak tudi neprekinjeno poslovanje, ki podpira strateške cilje podjetja. Z določanjem in merjenjem ciljev zagotavlja upravljalski okvir za ugotavljanje poslovne vrednosti kontinuiranega poslovanja (Košutič, 2013).

1.1.3 ANSI/TIA 942: Telekomunikacije v računalniških centrih

Standard določa minimalne zahteve za telekomunikacijsko infrastrukturo računalniških centrov in strežniških prostorov ter zagotavlja operativnim vodjem in upravljalcem tveganj okvir za načrtovanje in oblikovanje stabilne infrastrukture. Hkrati določa še smernice za načrtovanje in namestitev računalniškega centra, postavitev oskrbne infrastrukture, kablaže in podporne opreme. Zagotavlja tudi vodila v zvezi z energetsko učinkovitostjo in ponuja smernice za oblikovanje štirih nivojev zanesljivosti računalniškega centra (Geng, 2015).

1.1.4 EN 50600: Evropski standardi za računalniške centre

Serija evropskih standardov, ki določajo zahteve in priporočila za podporo različnim skupinam, se ukvarja z načrtovanjem, nabavo, integracijo, inštalacijo, upravljanjem in vzdrževanjem opreme in infrastrukture v računalniških centrih. Skupine, ki jim je namenjen ta standard, so:

- lastniki, upravljalci opreme, projektni vodje, glavni podizvajalci,
- arhitekti, gradbinci, načrtovalci, projektanti,
- integratorji opreme in inštalacij, ponudniki opreme,
- inštalaterji in vzdrževalci.

Ta evropski standard obravnava napajanje in distribucijo električne energije po merilih razpoložljivosti, fizične varnosti in energetske učinkovitosti. Hkrati ponuja še praktičen koncept za izvajanje fizične varnosti z uporabo splošnih varnostnih načel, pri čemer pravi,

da je treba za odločitev o sprejetju varnostnih ukrepov najprej opraviti oceno tveganja. Standard izrecno obravnava temo organizacijske varnosti in podaja zahteve po organizacijskih ukrepih za spremljanje fizične varnosti (Chille, Mund & Moller, 2018).

V naboru standardov EN 50600 s slike 3 se nahajajo (Cenelec, 2014):

Slika 3: EN50600: EU-standardi za računalniške centre EN50600



Vir: Prirejeno po Cenelec (2014).

1.2 Elementi računalniških centrov

Računalniški centri so kompleksni tehnološki objekti, kjer za neprekinjeno poslovanje ali obratovanje, poleg oskrbne infrastrukture, zanje skrbi še kopica kompleksnih organizacijskih ukrepov in varnostnih mehanizmov. V principu pa osnovne elemente ali gradnike sodobnih računalniških centrov delimo na:

- sisteme za zagotavljanje delovanja
  - stavba (varna celica, dvojni ali dvignjen pod, protipožarna zaščita ...),
  - zagotavljanje delovnih pogojev (električno napajanje, tehnično hlajenje ...),
  - zagotavljanje komunikacij in namestitve (strežniške in komunikacijske omare, ožičenje, napajalne distribucijske enote ali razdelilne enote ...),
- sisteme za zagotavljanje varnosti
  - zaščita pred tveganji iz okolja (protipožarna zaščita, videonadzor, kontrola dostopa, protipotresna zaščita ...),
- sisteme za zagotavljanje nezatajljivosti
  - zagotavljanje revizijskih sledi,
- IKT-sisteme
  - strežniška, komunikacijska in druga oprema, aplikacije,
- poslovne procese in njihove udeležence.

1.3 Storitve in modeli računalniških centrov

Da bi lažje definirali potrebe po nivojih varnosti v računalniških centrih, si moramo pobliže pogledati, katere so tiste osnovne storitve, ki jih računalniški center ponavadi ponuja uporabnikom, in kateri so najpogostejši modeli uporabe računalniških centrov.

1.3.1 Storitveni modeli računalniških centrov

V osnovi poznamo tri storitvene modele računalniških centrov (Strife, 2016):

- IaaS (ang. infrastructure as a service) ali infrastruktura kot storitev – kjer se uporabniku ponujajo informacijski viri računalniških centrov, kot so: virtualizacija, strežniki, diskovni prostor in računalniško omrežje.
- PaaS (ang. platform as a service) ali platforma kot storitev – velja za nadgradnjo storitve IaaS, ki omenjeni storitvi dodaja še operacijski sistem in strežniško opremo. Uporabnik sam poskrbi za podatkovni in aplikacijski del.
- SaaS (ang. software as a service) ali programska oprema kot storitev – model, pri katerem uporabnik dostopa tudi do aplikativnih rešitev prek spleta in zanje plačuje licenčnino, ki je časovno omejena.

Za omenjene storitve se uporabnik odloča glede na zahteve poslovnih modelov, katerim sledi pri svojem poslovanju. Vse več podjetij se odloča za tako imenovane oblačne storitve (tipa Microsoft Office 365, Salesforce, Dropbox, Oracle Cloud Applications itd.), ki v računalniških centrih potekajo kot storitev SaaS.

1.3.2 Modeli uporabe računalniških centrov

Najpogostejša sta dva modela uporabe računalniških centrov (Li, 2014) in oba sta ponavadi opredeljena v pogodbah o ponujanju storitev – bistveno se razlikujeta v aplikativnih performancah. Prvi je tako imenovani dedicirani model, namenjen izvajanju visoko zmogljivih aplikacij, pri čemer delitev virov z drugimi sistemi ne pride v poštev. Pred podpisom pogodbe se za tovrstne sisteme zapiše natančno število strežnikov, procesorjev, procesorske moči, spomina in omrežne pasovne širine, ki bodo namenjeni samo temu sistemu. Drugi je delitveni model, pri katerem se zavoljo optimizacije izkoriščanja virov ti med seboj delijo.

1.4 Organizacija in vloge v računalniških centrih

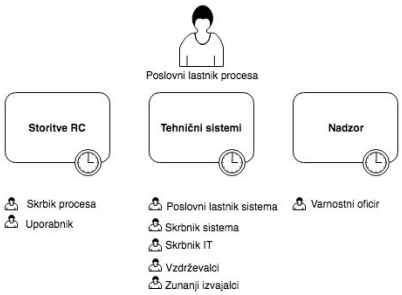
Preden se v družbi uvede proces računalniškega centra, mora organizacija definirati cilje, določiti zunanje in notranje parametre, ki jih je treba upoštevati pri upravljanju tveganj, ter določiti obseg in merila. V pomoč pri vzpostavitvi omenjenega procesa obstajajo pravila, zapisana v standardu ISO 31000:2018: Upravljanje tveganj, v katerem so zapisani določena

načela, okvir in postopek za obvladovanje tveganj. Standard lahko družbam pomaga pri doseganju ciljev, identifikaciji poslovnih priložnosti groženj in učinkovitejši uporabi virov za obvladovanje tveganj. Prav tako zagotavlja smernice za notranje in zunanje presojevalske programe in omogoča platformo, kjer lahko družbe primerjajo svoje prakse upravljanja tveganj z mednarodno priznanimi merili (ISO, 2009).

Eden od pomembnejših segmentov varnosti v računalniških centrih je vzpostavitev ustrezne kadrovske organiziranosti in zasedenosti ključnih vlog z jasno opredeljenimi odgovornostmi. Za lažje upravljanje in vzdrževanje računalniških centrov je treba vzpostaviti takšno organizacijo, ki bo pokrivala vse aspekte delovanja in upravljanja procesov v podporo delovanju omenjenega centra. Nekaj najbolj tipičnih vlog je prikazanih na sliki 4 in si po hierarhiji sledijo:

- poslovni lastnik procesa računalniškega centra, ki zagotavlja vire (direktor podjetja, izvršni direktor …),
- skrbnik procesa računalniškega centra, ki upravlja storitve, ki jih zagotavlja center (tehnični direktor, finančni direktor, direktor za informatiko, direktor trženja …),
- poslovni lastnik sistema računalniškega centra (kot tehničnega objekta) – tehnični direktor, direktor za informatiko, vodja informatike,
- skrbnik sistema računalniškega centra (operativna skrb za delovanje),
- varnostni oficir – nadzor,
- skrbniki IT in drugih sistemov,
- vzdrževalci,
- zunanji izvajalci,
- uporabniki,
- obiskovalci.

Slika 4: Vloge pri upravljanju računalniških centrov



V*ir: lastno delo.*

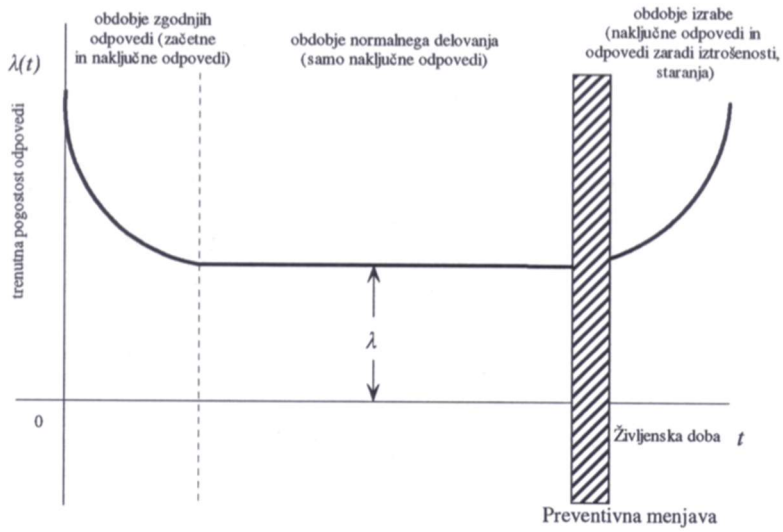
1.5 Zagotavljanje neprekinjenega delovanja računalniškega centra

Zaradi narave poslovanja modernih družb je ključnega pomena, da podporne storitve, med katere nedvomno spadajo storitve kolokacije, delujejo neprekinjeno in zagotavljajo stabilno

infrastrukturo ključnim informacijskim storitvam. Pri tem se je treba zavedati, da nekaterim družbam predstavlja morebiten izpad ključnih IT-storitev, izgubo posla, izpad dohodka in nenazadnje propad.

Tako kot pri večini tehnoloških sistemov ali naprav lahko tudi pri delovanju računalniških centrov poimenujemo tri različna časovna obdobja odpovedi, prikazana na sliki 5, v katerih se zanesljivost delovanja naprav bistveno razlikuje.

Slika 5: Stopnje odpovedi tehniških sistemov



Vir: Aberšek & Flašker (2005).

1. obdobje ali obdobje zgodnjih odpovedi – to je obdobje na začetku življenjske dobe neke naprave ali obdobje zagonov (lahko tudi zaradi površnosti, napake v proizvodnji ali zaradi človeškega dejavnika),

2. obdobje ali obdobje normalnega obratovanja, v katerem je trenutna pogostost odpovedi najmanjša (priča smo lahko le naključnim odpovedim),

3. obdobje ali obdobje izrabe oz. odmiranja, v katerem v večini primerov pride do odpovedi zaradi iztrošenosti, obrabe ali starosti.

1.5.1 Zanesljivost

Zanesljivost računalniškega centra lahko razumemo kot neko lastnost kompleksnega tehnološkega sistema in predstavlja verjetnost, da bo v nekem predvidenem času, v predpisanih pogojih, opravljal funkcije, ki so mu bile namenjene. Je sposobnost, da sistem, ki ga uporabljamo pri določenih pogojih, zadovoljivo deluje, pri čemer opravlja zahtevano funkcijo neki časovni interval (Hudoklin Božič & Rozman, 2004).

Ko govorimo o računalniških centrih, se izraza zanesljivost in razpoložljivost uporabljata izmenično, pri čemer poskušamo opisati pričakovano stopnjo učinkovitosti. Čeprav sta izraza precej povezana, opisujeta izrazito različne pristope. V znanosti se zanesljivost velikokrat povezuje s ponovljivostjo. Če se preizkus ali eksperiment ponavlja z enakim rezultatom, potem smo priča visoki stopnji zanesljivosti. Za merjenje zanesljivosti uporabljamo dva »mehanizma«:

- MTBF (ang. mean time between failure) ali srednji povprečni čas med dvema zaporednima odpovedma, ki predstavlja čas delovanja storitve, deljen s številom napak, kot je razvidno iz enačbe (1)

$$MTBF = \frac{T}{k} = \frac{1}{\lambda} \tag{1}$$

  kjer je:

  - T – skupni čas delovanja storitve,
  - k – število napak (ali odpovedi),
- stopnja odpovedi (ang. failure rate), izražena kot število odpovedi na uro ali število odpovedi v letu. Določitev stopnje odpovedi se izračuna po naslednji formuli (2):

$$\lambda = \frac{k}{T} \tag{2}$$

  kjer je:

  - k – skupno število odpovedi,
  - T – skupni čas delovanja storitve.

1.5.2 Razpoložljivost

»Važen parameter proizvodnih tehniških sistemov je njihova razpoložljivost, tj. delež časa, ko so naprave sposobne obratovati; razpoložljivost je ekonomski parameter, pa tudi merilo tehniške opremljenosti in proizvodne organiziranosti. Odvisna je od zanesljivosti oz. od pričakovane življenjske dobe elementov, iz katerih je proizvodna naprava sestavljena, od načina gradnje teh naprav ter od vrste ukrepov in potrebnih opravil posluževalnega in vzdrževalnega osebja.« (Bratina, 1983)

Razpoložljivost računalniškega centra se izraža v razmerju med pričakovanim nivojem storitev, ki jih ponuja, in delovanjem oskrbne infrastrukture oz. računalniških kapacitet. Najpogosteje se nivoji razpoložljivosti izražajo z metodologijo oz. priporočili Uptime Instituta, imenovanimi klasifikacija ureditve oskrbne infrastrukture TIER (stopnja ureditve napajalnih sistemov), kar je zapisano v tabeli 1. V osnovi pa ločimo naslednje stopnje (Uptime Institute, 2016):

- TIER I – osnovna infrastruktura brez redundance s tipično razpoložljivostjo 99,671 % in povprečnim letnim časom odpovedi 1729 minut.
    - Povzetek zahtev:
        - zagotovljena je zadostna kapaciteta napajanja, hlajenja in prostora za vgrajeno IT-opremo,
        - podporna infrastruktura je brez redundance (t. i. N-zasnova, kjer N v angleškem jeziku pomeni »needed« in predstavlja zadostno kapaciteto),
        - samo ena distribucijska pot (cevovodi, kanali, električni razvod).
    - Delovanje in vzdrževanje:
        - infrastrukturo podatkovnega centra je treba ob rednih vzdrževanjih izklopiti, postavitev oz. širitev kapacitet lahko vpliva na nemoteno delovanje podatkovnega centra.
    - Operativna tveganja:
        - Okvara katerekoli komponente napajanja ali hlajenja oziroma okvara na distribucijski poti bo vplivala na delovanje podatkovnega centra.
        - Podatkovni center oziroma njegovi deli so podvrženi vplivom ob načrtovanih in nenačrtovanih aktivnostih.
        - Človeške napake močno vplivajo na zanesljivost delovanja.
        - Odlašanje oziroma prestavljanje rednega vzdrževanja infrastrukture močno povečuje tveganja za okvare in izpade podatkovnega centra.
- TIER II – redundanca osnovnih komponent (hlajenje, UPS …), vključno z generatorjem električne energije (dizelski agregat, gorivne celice …) in s tipično razpoložljivostjo 99,741 % ter povprečnim letnim časom odpovedi 1361 minut.
    - Povzetek zahtev:
        - redundantna zasnova kapacitet (t. i. zasnova N+R, kjer N predstavlja zadostno kapaciteto, R pa redundanco) električnega napajanja (UPS in električni agregat) in hlajenja,
        - samo ena distribucijska pot.
    - Delovanje in vzdrževanje:
        - infrastrukturo podatkovnega centra je treba ob rednih letnih vzdrževanjih izklopiti,
        - nekatere sklope je mogoče vzdrževati oziroma popravljati brez njihovega izklopa,
        - postavitev dodatnih oziroma širitev obstoječih kapacitet lahko vpliva na nemoteno delovanje podatkovnega centra.
    - Operativna tveganja:
        - okvara katerekoli komponente napajanja ali hlajenja lahko vpliva na delovanje podatkovnega centra,
        - okvara elementov na distribucijskih poteh bo vplivala na delovanje podatkovnega centra,
        - podatkovni center oziroma njegovi deli so podvrženi vplivom ob načrtovanih in nenačrtovanih aktivnostih,

        - človeške napake vplivajo na delovanje,
        - odlašanje oziroma prestavljanje rednega vzdrževanja infrastrukture močno povečuje tveganja za okvare in izpade podatkovnega centra.
- TIER III – redundanca infrastrukture, ki jo je mogoče vzdrževati med obratovanjem (brez izpada). Podvojeni viri za kritične komponente s tipično razpoložljivostjo 99,982 % in povprečnim letnim časom odpovedi 95 minut.
    - Povzetek zahtev:
        - redundantna zasnova kapacitet (UPS – naprava za neprekinjeno napajanje, DEA – dizelski električni agregat, hlajenje) in distribucijskih poti,
        - posamezni deli posamezne distribucijske poti so lahko neaktivni,
        - kot primarni vir napajanja se upošteva električni agregat (skrajšano DEA) in ne mrežno napajanje,
        - DEA ne sme imeti omejitev glede časa delovanja pri polni obremenitvi.
    - Delovanje in vzdrževanje:
        - vsaka in katerakoli komponenta kapacitet in element distribucijskih poti se lahko odstranita z namenom popravila oziroma vzdrževanja, pri tem pa mora delovanje podatkovnega centra ostati nemoteno.
    - Operativna tveganja:
        - ob vzdrževanjih oziroma popravilih bo sistem zaradi redundantne zasnove sicer deloval nemoteno, vendar bo za čas popravila izpostavljen višjemu tveganju,
        - človeške napake lahko vplivajo na delovanje,
        - IT-oprema z enojnim električnim priklopom (brez redundantnih napajalnikov) ali njena nepravilna inštalacija lahko izniči prednosti zasnove TIER III.
- TIER IV – v celoti redundantna infrastruktura s tipično razpoložljivostjo 99,995 % in povprečnim letnim časom odpovedi 26 minut.
    - Povzetek zahtev:
        - redundantna zasnova, fizična ločitev posameznih sklopov (ang. compartmentalization),
        - redundantna kapaciteta,
        - redundantne in neodvisne aktivne distribucijske poti,
        - neprekinjeno hlajenje (zadostna količina shranjene hladilne energije, neprekinjeno napajanje pogonskih sistemov hladu),
        - avtonomni odziv na napake (N po vsakem izpadu),
        - DEA ne sme imeti omejitev glede časa delovanja pri polni obremenitvi.
    - Delovanje in vzdrževanje:
        - okvara katerekoli komponente kapacitet ali elementa distribucijskih poti ne vpliva na delovanje podatkovnega centra.
    - Operativna tveganja:

- izpad posameznega sklopa ali dela kapacitet, elementa distribucijskih poti kot tudi posamezne človeške napake ne vplivajo na nemoteno delovanje podatkovnega centra,
- vzdrževalna dela lahko predstavljajo povišano tveganje za delovanje za čas vzdrževanja,
- vklop stikala EPO (ang. emergency power off), aktivacija sistema gašenja ali zlonamerni človeški posegi lahko vplivajo na delovanje podatkovnega centra.
- IT-oprema z enojnim priklopom (brez redundantnih napajalnikov) ali njena nepravilna inštalacija lahko izniči prednosti zasnove TIER IV.

Tabela 2: TIER-klasifikacija

	TIER I	TIER II	TIER III	TIER IV
Minimalne zmogljivosti oskrbne infrastrukture	N	N+1	N+1	N po vsaki odpovedi
Distribucijske trase – glavni energetski razvod	1	1	1 aktivna 1 pasivna	2 simultano aktivni
Distribucijske trase – napajalni razvod do porabnikov	1	1	2 simultano aktivni	2 simultano aktivni
Vzdrževanje brez izpada	ne	ne	da	da
Toleranca za izpade	ne	ne	ne	da
Ločevanje opreme po conah	ne	ne	ne	da
Kontinuirano hlajenje	ne	ne	ne	da

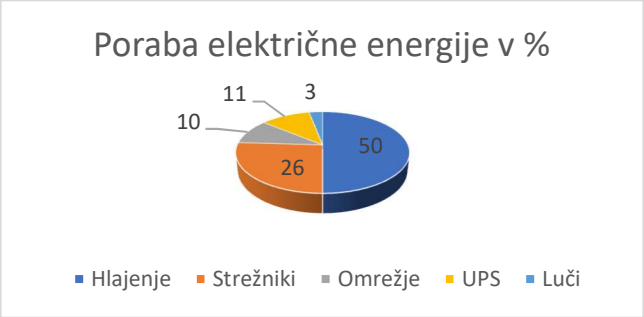
Vir: Uptime Institute (2016)

Z višanjem TIER-nivoja iz tabele 2 cena računalniškega centra raste; ob načrtovanju tako kompleksne infrastrukture je treba temeljito preveriti vse zahteve, še posebno tiste, ki zadevajo varnost. Med razpoložljivostjo 99,671 % pri TIER I in 99,995 % pri TIER IV na pogled ni veliko razlike, vendar merjeno s časovno enoto izpad ključnih informacijskih storitev za 1729 minut ali za 26 na letnem nivoju za družbo lahko pomeni obstoj ali propad.

1.5.3 Oskrba z električno energijo

Eden najpomembnejših virov za zagotavljanje delovanja računalniških centrov je oskrba z električno energijo. Električna energija je tista, ki ustvarja pogoje za neprekinjeno delovanje, njeno zanesljivo delovanje nam zagotavlja najvišji nivo varnosti pri izvajanju vseh informacijskih storitev. Po statističnih podatkih, ki jih je objavila skupina Infotech (Dayarathana, Wen & Fan, 2016), je največji porabnik električne energije sistem za hlajenje – v povprečju porabi 50 % celotne energije, namenjene obratovanju računalniških centrov. Kako je s preostalimi sistemi podporne infrastrukture, pa kaže graf na sliki 6:

Slika 6: Poraba električne energije v računalniških centrih



Vir: Priprejeno po Dayarathana, Wen & Fan (2016).

Zahteve po kakovosti električne energije so izjemnega pomena; pri načrtovanju napajalnih sistemov ponuja standard IEEE 446-2000 (IEEE, IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications, 1996) najboljšo oporo. Obravnava priporočeno prakso za rezervno in nujno oskrbo z električno energijo, pri čemer navaja sprejemljive čase izpadov napajanja glede na vrsto opreme. Glede na to, da je standard iz leta 2000, so časi, ki so zapisani, danes v večini primerov nezadostni. Računalniškim centrom, ki se gradijo danes, ne zadostujeta le nujna in rezervna električna energija, temveč je jasna zahteva po visoko zanesljivi oskrbi oziroma po brezprekinitveni oskrbi z električno energijo, ki jo lahko dosežemo le z brezprekinitvenimi napajalnimi sistemi. Ključne zahteve po neprekinjenem napajanju lahko strnemo v naslednje (Lavuger, 2016):

- razpoložljivost in zanesljivost napajalnih virov,
- odpornost proti izpadom,
- zagotavljanje ustreznih napetostnih nivojev glede na zahteve porabnikov,
- zagotavljanje ustrezne kakovosti napajalne napetosti pri porabnikih.

Računalniški centri so velik porabnik električne energije, potrebe po električni energiji so vedno večje – po študiji, ki jo je za ameriško vlado pripravil laboratorij Berkeley (Shehabi A. in drugi, 2016), so v ZDA leta 2014 računalniški centri porabili približno 70.000 GWh. Po predvidevanjih se letna poraba veča za 4 %, kar pomeni, da bodo računalniški centri v ZDA do leta 2020 porabili približno 73.000 GWh – za primerjavo: Dravske elektrarne Maribor proizvedejo 2500 GWh električne energije letno. Zaradi naraščajočih potreb in nenazadnje tudi zaradi podnebnih sprememb ter pretiranega globalnega segrevanja se potrebe po tako imenovanih »zelenih računalniških centrih« precej povečujejo, vendar velja poudariti, da na račun zelenih tehnologij ne sme trpeti nivo varnosti, zanesljivosti in učinkovitosti.

1.5.4 Sistemi za tehnično hlajenje

Hladilni sistemi so bistvenega pomena za obratovanje IT-opreme v varnem in zanesljivem okolju. Poraba električne energije za hlajenje in vlaženje računalniških centrov ponavadi znaša 40 % celotne porabe, zato je zelo pomembno, da se v računalniški center namesti učinkovit hladilni sistem z najnižjo porabo električne energije. Večina računalniških centrov še danes uporablja zračno hlajene sisteme, vendar je že mogoče opaziti implementacijo novejših, energetsko učinkovitejših sistemov, kot so vodno hlajeni sistem z zunanjim hladilnim agregatom s prostim hlajenjem in vodno hlajeni sistem z zunanjim hladilnim agregatom s hladilnimi omarami z dvojnimi registri in ločenim hlajenjem iz okolice (Capozzoli & Primicieri, 2015).

V priporočilih tehniškega komiteja ASHRAE (ASHRAE Technical Committee, 2011) je zapisano, da so mejne dovoljene in priporočene temperature v računalniških centrih naslednje:

- temperatura od 18 ºC do 27 ºC,
- vlaga od 35 % do 60 % RH (oz. od 5,5 º do 15 ºCDP).

1.5.5 Sistemi za nadzor

Moderni računalniški centri so opremljeni s kopico nadzornih sistemov, ki skrbijo za njihovo delovanje in posledično za varnost. Lahko rečemo, da so danes bistveno bolj kompleksni, samostojni in nenazadnje bistveno bolj kritični, kot so bili nekoč. Osnovno fizično varnost pokrivajo sistemi za videonadzor in tehnično varovanje, vendar upravljalce in nenazadnje naročnike zanima še bistveno več, na primer:

- kdo in kdaj je vstopil v center,
- kdo je odprl sistemsko omaro in dostopal do naprav IKT (informacijsko-komunikacijska tehnologija),
- kateri dogodki so ogrožali varnost in delovanje njegovih naprav,
- sprotno spremljanje varnostnih in drugih dogodkov,
- morebitni incidenti in njihovo javljanje prek SMS (storitev kratkih sporočil) ali po elektronski pošti,
- revizijske sledi,
- načrtovanje kapacitet …

Na račun omenjenih potreb se v računalniških centrih uporabljajo inteligentni in avtomatizirani sistemi za nadzor informacijske infrastrukture (ang. data center infrastructure management DCIM), ki učinkovito upravljajo kompleksno okolje (Cole, 2012). Tovrstna orodja nadzirajo, merijo in upravljajo celoten računalniški center, porabo in distribucijo energije, distribucijo hladu in hkrati z vso IT-opremo (strežniki, omrežna oprema, podatkovna skladišča …), kar je prikazano na sliki 7:

Slika 7: Sistem za nadzor infrastrukture v RC – diagram napajanja



Vir: DEM DCIM (2018).

Tovrstni nadzorni sistemi omogočajo učinkovito upravljanje kapacitet, upravljanje zmogljivosti, sredstev in vršijo nadzor nad energijo in učinkovitostjo PUE. Ponavadi so to večnivojski sistemi, v celoti prilagojeni potrebam v računalniških centrih ter namenjeni upravljalcem in uporabnikom centrov. Naprednejši nadzorni sistemi ločujejo informacije glede na potrebe oziroma vloge uporabnikov in zagotavljajo ključne informacije neodvisno od delovanja strežnikov. Temeljijo na delovanju porazdeljene arhitekture:

- LMI – lokalni nadzor za zajem podatkov,
- centralni nadzor delovanja (nekoč CNS),
- centralni sistem spremljanja delovanja.

Analiza podatkov, pridobljenih iz nadzornih sistemov, se izvaja ločeno od operativnih podatkov.

Nadzorni sistem mora biti zgrajen za nadzor in deloma upravljanje vseh elementov nadzorne infrastrukture. To pomeni hierarhično izgradnjo nadzornega sistema z implementacijo različnih pravic za različne uporabnike. V nadzornem sistemu sta predvidena modeliranje vseh točk IO (vhod/izhod) po posamezni napravi in izgradnja ustreznih hierarhičnih oken.

Nadzorni sistem infrastrukture mora zagotavljati naslednje funkcionalnosti oz. funkcionalne celote:

- Procesni vmesnik programske opreme DCIM

  Procesni vmesnik je osnovni vmesnik v programski opremi DCIM. Namenjen je osnovni vizualizaciji in pregledu stanja v računalniškem centru. Prikazuje osnovne podatke o centru, kot so skupna poraba, povprečna temperatura, povprečna energetska učinkovitost, seznam aktivnih alarmov ipd. Procesni vmesnik sestavljata tudi

avtentikacijski modul, ki omogoča upravljanje pravic uporabnikov, in modul za dostop do preostalih modulov. Dostop do upravljanja mora biti za vsak modul omejen glede na uporabniške pravice prijavljenega uporabnika. Uporabniki brez prijave ne smejo imeti možnosti upravljanja kateregakoli dela, sistema ali naprave. Za vsako merjeno vrednost mora biti možnost izpisa zgodovine podatkov.

- Nadzor električnega napajanja

  Modul za nadzor električnega napajanja mora omogočati nadzor in upravljanje vseh vgrajenih sistemov za oskrbo z električno energijo. Prikazi morajo biti zasnovani na splošnih prikazih moči po posameznem hierarhičnem nivoju omrežja, po posameznih merjenih odcepih, po posamezni sistemski omari. Prav tako mora biti prikazan logični in resnični blok diagram z vsemi statusi in meritvami v napajalnem sistemu. Vsaka aktivna oprema mora prikazati notranji blok diagram in vrednosti parametrov, kot na osnovnem zaslonu. V modulu se morajo samostojno beležiti in izpisovati alarmi in alarmna stanja samo v sistemu električnega napajanja.

- Nadzor tehničnega hlajenja

  Modul za nadzor tehničnega hlajenja mora omogočati nadzor in upravljanje vseh vgrajenih sistemov za tehnično hlajenje. Prikazi morajo biti zasnovani na splošnih prikazih temperatur in stanja delovanja sistemov po posameznem hierarhičnem nivoju, po posameznih merjenih vrednostih, hladnih conah, po posamezni sistemski omari ter posameznem kosu opreme. Prav tako mora biti prikazan logični in resnični blok diagram z vsemi statusi in meritvami v sistemu. Vsaka aktivna oprema mora prikazati notranji blok diagram in vrednosti parametrov, kot na osnovnem zaslonu. V modulu se morajo samostojno beležiti in izpisovati alarmi in alarmna stanja samo v sistemu tehničnega hlajenja.

- Nadzor pomožnih sistemov

  Nadzor pomožnih sistemov zajema nadzor nad delovanjem pomožnih sistemov, kot so stabilna gasilna naprava, dodatni senzorji temperature in vlage v prostoru, senzorji za zaznavanje izliva tekočin, senzorji odprtosti vrat in drugi pomožni senzorji v sistemskem prostoru. V modulu se morajo samostojno beležiti in izpisovati alarmi in alarmna stanja samo v pomožnih sistemih.

- Upravljanje sistemskih omar

  Upravljanje sistemskih omar omogoča vpogled v stanja v sistemskih omarah. Vpogled zajema realen vpogled v stanja napajanja, temperatur in odprtosti vrat (če so vgrajeni senzorji) ter nameščene opreme. Modul omogoča uporabnikom, da dodajo v posamezno omaro lastno opremo, določijo skupne podatke, kot so tip, model, leto vgradnje, življenjska doba, poraba na izvodih, št. priključkov ipd. Prav tako se vnese položaj

opreme ter označi, s čim so energetski in komunikacijski priključki povezani. V primeru, da so vgrajene PDU-enote z meritvami na vsakem izvodu – vtičnici, se prikazuje tudi realna poraba vsakega tokokroga – porabnika. Upravljanje je omogočeno za obveščanje o zamenjavah, vodenju evidence, napovedovanju rasti porabe el. energije ipd.

- Upravljanje komunikacijskega omrežja

  Upravljanje komunikacijskega omrežja omogoča upravljanje pasivnega komunikacijskega omrežja. Vsebuje evidenco vseh povezav glede na izvor in ponor v centru, njihovo zasedenost ter priključne točke.

- Upravljanje načrtovanih posegov oskrbne infrastrukture

  Upravljanje načrtovanih posegov vsebuje servisni vmesnik za evidenco izvedenih in načrtovanih servisnih in drugih posegov glede na posamezno opremo, tip opreme in vrsto servisov.

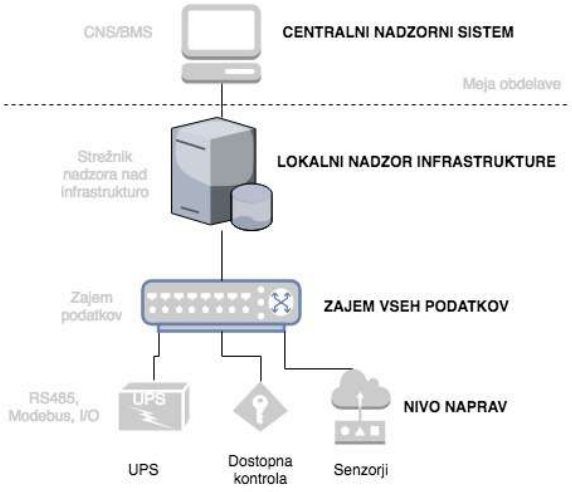
- Upravljanje alarmov in obvestil

  Upravljanje alarmov in obvestil omogoča vpogled in pregled alarmnih stanj, alarmov in drugih dogodkov, njihovo potrjevanje in sporočanje v druge sisteme. Dostop do posameznega modula in/ali okna je mogoč le z ustreznimi pravicami, kar se nastavi na nivoju vsakega uporabnika posebej in/ali skupine uporabnikov.

Nadzorni sistem je zasnovan na porazdeljenem sistemu zajema podatkov, pri čemer podatke iz posameznih tehnoloških sklopov zajemamo na porazdeljenih zajemalnih sistemih – krmilnikih. Z njimi zajemamo digitalne in analogne signale, prek digitalnih in analognih izhodov krmilimo analogne in digitalne aktuatorje ter prek komunikacijskih vodil zbiramo in vodimo delovanje naprav. Posamezni krmilniki so povezani v enotno omrežje prek omrežja ethernet in tako posredujejo podatke in informacije do centralnega nadzornega strežnika, ki jih zbira, obdeluje, pripravlja za prikaz in posreduje drugim sistemom. V sistemu sta predvideni tudi dve sinoptični konzoli, ki olajšata lokalno delo na objektu. Arhitektura sistema je prikazana na sliki 8.

Nadzorni sistem oskrbne infrastrukture je zasnovan v skladu s prikazano arhitekturo, kjer je njegova vloga nadzor in upravljanje tehničnih in tehnoloških sklopov oskrbne infrastrukture, obdelava sporočil iz teh sklopov, njihov sinoptični prikaz ter posredovanje zbranih sumarnih sporočil v višje nivojske nadzorne centre.

Slika 8: Arhitektura nadzornega sistema



Vir: lastno delo.

1.5.6 Sistemi za detekcijo in gašenje požara

Zaradi svoje konfiguracije in nameščenih naprav so računalniški centri v veliki meri podvrženi možnostim izbruha požara. Še posebej so izpostavljeni prostori dizelskega agregata in baterijskih sklopov. Tudi na strežniški opremi v varni celici obstaja možnost požara. Med ukrepe tehnične ali aktivne požarne zaščite v računalniških centrih spadajo vgrajene naprave za odkrivanje požarov (dima, plinov, ognja), vgrajene naprave za gašenje, naprave za odvod dima, varnostna in zasilna razsvetljava, krmiljenje vrat na evakuacijski poti in naprave za oskrbo z elektriko v primeru izrednih situacij. Cilj vseh teh naprav je, da detektirajo morebiten požar in ga v najkrajšem možnem času tudi pogasijo (ob najmanjšem možnem uničenju opreme v računalniškem centru). Elementi požarne zaščite so:

- javljalniki,
- senzorika (temperatura, toplota, svetloba, dim, plini),
- požarna centrala,
- stabilna požarna naprava.

Najpogosteje se za gašenje požarov v računalniških centrih, kot je center podjetja DEM na sliki 10, uporablja plin novec 1230, prikazan na sliki 9. To je sintetično kemično gasilo, ki se shranjuje v tekočem stanju in se ob gašenju sprošča kot plin. Primeren je za gašenje elektronskih naprav, saj ne vsebuje vode. Plin ogenj pogasi z ohlajevanjem, tako da odstrani proste radikale oziroma toploto v trikotniku gorenja (kisik, toplota, gorljiva snov). Pomembno pri tem plinu je tudi, da ob delovanju iz prostora ne posrka kisika, kar bi lahko povzročilo zadušitev vzdrževalnega osebja (Zarja Elektronika, 2018)

.

Slika 9: Plin Novec 1230



Vir: DEM (2018).

Slika 10: Sistem gašenja DC DEM



Vir: DEM (2018).

1.6 Fizična in informacijska varnost računalniških centrov

Računalniški centri elektropodjetij, ki so del kritične oskrbovalne infrastrukture države, so danes še posebej izpostavljeni varnostnim tveganjem. Motivacija in tipi napadalcev se precej razlikujejo, variirajo od vandalizma, kibernetskih napadov pa vse do mednarodnega terorizma. Celovit pristop k varnosti terja upoštevanje številnih vidikov varnosti – na eni strani fizično varovanje informacijskih in infrastrukturnih virov, na drugi strani pa ukrepi logičnega ali kibernetskega varovanja informacijskih storitev in z njimi povezanih informacijskih virov. Ko govorimo o fizični varnosti, imamo v mislih dva tipa napadov: prvi je čisto fizičen napad (vdor nepridipravov na področje računalniških centrov …), pri katerem lahko pričakujemo poškodovanje ali odtujitev opreme, drugi, napad na informacijsko infrastrukturo s fizičnim dostopom (recimo prek USB-vrat), pa lahko povzroči več škode, pri čemer napadalec prek zaseženih vrat sproži napad večjih razsežnosti. Oboje bistveno vpliva na celovito razpoložljivost in finančne izgube. Najbolje se do fizičnega varovanja kritične infrastrukture opredeljuje standard EN 50600, ki nam ponuja nabor ukrepov za fizično varovanje stavbe (zgradbe), v kateri je računalniški center.

Najbolj ranljiv informacijski sistem v računalniškem centru je sistem za nadzor infrastrukture – ponavadi so to SCADA-sistemi, ki so bili v zadnjih letih precejšnja tarča mnogih »uspešnih« vdorov. Najbolj znan je primer kibernetskega napada na ukrajinsko energetsko omrežje iz leta 2015, posledica česar je bil izpad sedmih 110-kV daljnovodov in kar 23 35-kV daljnovodov za obdobje treh ur. 225.000 uporabnikov električnega omrežja je bilo v tem času brez električne energije (E-ISAC, 2016).

Varnost torej ni nekaj, pri čemer se cilj doseže – je proces, ki dnevno odkriva pasti in ranljivosti ter zanje pripravlja ustrezne ukrepe.

Številne družbe še zmeraj ločeno obravnavajo fizično in informacijsko varnost – takšno početje so do nedavnega upravičevali s pomanjkanjem tehnologij integriranih sistemov. Za upravljanje varnosti (tehnično varovanje, videonadzor, zaščita pred vlomi …) so ponavadi uporabljali vsaj tri različne sisteme. Za varnost pred kibernetskimi napadi so uporabljali svoj sistem, prav tako sistem za varovanje omrežnih protokolov. Danes se tovrstna problematika rešuje z vzpostavitvijo enotnega nadzornega organa (sistema) za podporo varnostnim politikam, postopkom in njihovi implementaciji (CISCO, 2011). Direktor ameriških enot za boj proti kibernetskemu kriminalu Scott Borg pravi: »Dokler družbe ločeno obravnavajo fizično in informacijsko varnost, je malo upanja, da bi zavarovali katerokoli od teh dveh področij. Konvergenca obeh se je že zgodila na tehnični ravni – veliko pred tem pa tudi že na organizacijski.« (Martens, 2018)

Za načrtovanje varnosti je danes potreben holističen pristop: ena upravljalska ekipa, organizacija ali skupina je zadolžena za celovit načrt politik in pravil, pri čemer zadovoljujejo zahteve vseh zainteresiranih strani in ostajajo dovolj prilagodljivi za nemoteno izvajanje poslovne dejavnosti.

2 ANALIZA STANJA INFORMACIJSKE VARNOSTI V RAČUNALNIŠKIH CENTRIH DRUŽB IZ SKUPINE HSE

Skupina HSE je največji proizvajalec in trgovec z električno energijo na veleprodajnem trgu v Republiki Sloveniji. V eno blagovno znamko, skupino HSE, so združene naslednje družbe (HSE, 2018):

- Dravske elektrarne Maribor, d. o. o.,
- Termoelektrarna Šoštanj, d. o. o.,
- Soške elektrarne Nova Gorica, d. o. o.,
- Premogovnik Velenje, d. d.,
- HSE, d. o. o.,
- HSE Invest, d. o. o.

V letu 2017 je skupina HSE proizvedla 7034 GWh električne energije, pri čemer so Dravske elektrarne Maribor proizvedle 2333 GWh, Soške elektrarne Nova Gorica 733 GWh in Termoelektrarna Šoštanj 3968 GWh. Delež obnovljivih virov v skupini znaša 44 %.

Tabela 3: Proizvodnja električne energije v skupini HSE

Družba	Proizvodnja el.energije	Število enot
DEM d.o.o.	2.333 GWh	28 turbin
TEŠ d.o.o.	3.966 GWh	2 bloka + 2 pl.turbini
SENG d.o.o.	733 GWh	38 turbin
TET (v likvidaciji)	2 GWh	2 pl.turbini

Vir: HSE (2018).

Informacijski sistem skupine teče v dveh enakovrednih računalniških centrih: eden je v Mariboru (DC DEM) in drugi v Šoštanju (DC TEŠ). Oba gostita celoten poslovnoinformacijski sistem, temelječ na rešitvi SAP ERP in podprt z dokumentacijskim sistemom. V letu 2017 se je začel projekt vzpostavitve visoko razpoložljivega infrastrukturnega okolja, skladno s strategijo konsolidacije celotnega informacijskega sistema skupine HSE in najvišjih standardov na področju informacijske varnosti (HSE, 2018).

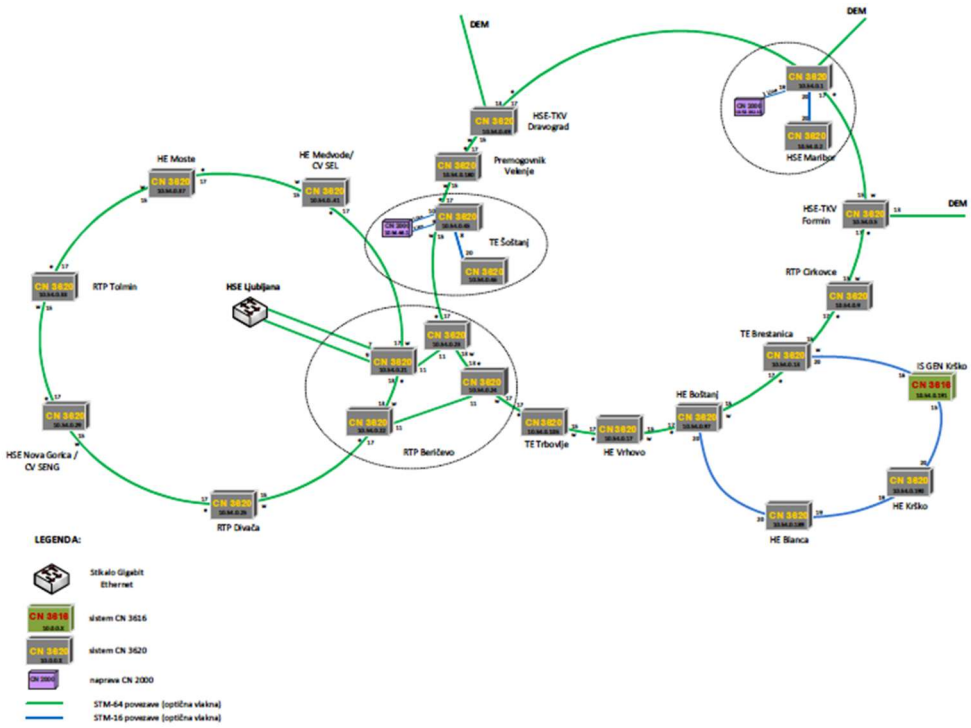
V skupini so identificirana vsa varnostna tveganja, ki nastanejo zaradi neustreznega ali neuspešnega izvajanja varovanja informacij, premoženja, varnosti in zdravja pri delu ter nepredvidljivih eksternih dogodkov, ki imajo lahko izjemen vpliv na poslovanje družb. Med ključnimi varnostnimi tveganji je skupina najbolj izpostavljena pri tveganju naravnih nesreč, katastrof in izrednih dogodkov, pri tveganju varstva in zdravja pri delu in požarne varnosti, pri tveganju informacijske varnosti in tveganju varovanja stvarnega premoženja. Skupina uspešno obvladuje tveganja z vzpostavitvijo in rednim nadgrajevanjem ustreznih preventivnih ukrepov ter sistemov za pravočasno zaznavanje sprememb v okolju poslovanja.

2.1 Računalniški centri v skupini HSE

Računalniška centra v skupini sta zasnovana tako, da najbolje zagotavljata prožnost informacijskih virov in v celoti tvorita visoko zmogljivo logično celoto, ki že v svoji naravi zagotavlja razširljivost. Komunikacijski sloj jima zagotavlja obstoječe telekomunikacijsko omrežje skupine HSE, prikazano na sliki 11, ki je bilo zgrajeno leta 2005 z uporabo tehnologij DWDM (zgoščeni način združevanja signalov) in NG SDH (nova generacija omrežij sinhrone digitalne hierarhije), namenjeno lastnim potrebam internih uporabnikov v skupini HSE: poslovnoinformacijski sistem, povezovanje različnih članic skupine in njihovih poslovnih in procesnih sistemov, povezovanje podatkovnih centrov itd. V trenutnem obratovalnem stanju omrežje zagotavlja visoko razpoložljive storitve, saj je bil upoštevan princip gradnje TK-omrežja v zankah, ki jih omogočajo zgrajeni optični odseki na posameznih relacijah. Uporabljeni mehanizmi zaščite na obhodne poti, ki jih je omogočila tehnologija NG SDH tako za tip storitev TDM kakor tip storitev ethernet L2, zagotavljajo hitre preusmeritve prometnih tokov v primeru okvar, s čimer zagotavljamo neprekinjene storitve za vse uporabnike znotraj skupine HSE. Omrežni elementi obstoječega telekomunikacijskega omrežja (TK-omrežja) skupine HSE so NG SDH-naprave tipa CN

3620 in CN 3616 ter DWDM OADM moduli tipa CN 2100, oboje proizvajalca CIENA. Princip delovanja omrežja sloni na vzpostavljenih obročih – zahodni in vzhodni, kjer so med posameznimi vozlišči vzpostavljene DWDM-povezave, zgrajene z moduli DWDM OADM. Vsaka smer je opremljena z modulom s 4 vhodnimi vmesniki, kjer se priključujejo aktivni NG SDH-vmesniki vozlišča CN 3620.

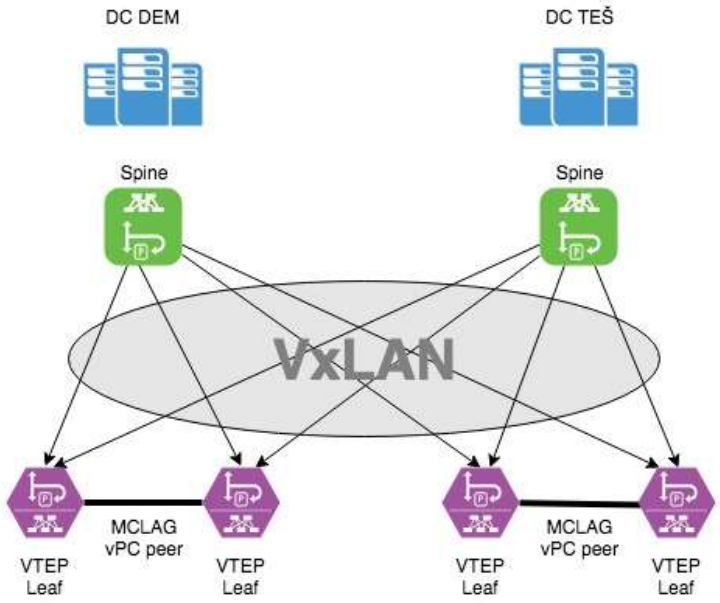
Slika 11: Topologija obstoječega hrbteničnega TK-omrežja HSE



Vir: HSE (2018).

Potrebe zaradi vse večje avtomatizacije in pojava novih informacijskih storitev, konvergence in centralizacije aplikacij v skladu z modernimi trendi razvoja informacijskega sistema skupine HSE ter potrebe po ohranjanju in povečanju razpoložljivosti informacijske infrastrukture, storitev in posledično principov neprekinjenega poslovanja, so narekovale uvedbo podatkovnih centrov, ki se nahajata na lokaciji TEŠ in DEM. Sledi prenova celotnega TK-omrežja, kjer bo komunikacijski koncept slonel na stikalni arhitekturi hrbteničnih in dostopnih stikal s slike 12 (ang. spine in leaf), kjer listno plast sestavljajo dostopna stikala, ki se povezujejo z napravami, kot so strežniki, medtem ko so hrbtenična stikala odgovorna za povezavo vseh listnih stikal (vsako listno stikalo se poveže z vsakim hrbteničnim stikalom). Pot je naključno izbrana tako, da je prometna obremenitev enakomerno porazdeljena med nadrejenimi stikali. Tehnologija virtualizacije omrežja VxLAN ponuja več prednosti. Je industrijski standardni protokol in razširja segmente Layer 2 čez infrastrukturo Layer 3. Enkapsulira pakete ethernet v UDP (uporabniški datagram protokol) glavo in jih transportira do oddaljenih končnih točk VxLAN, pri čemer uporablja normalen usmerjevalni mehanizem IP (Cisco, 2016).

Slika 12: Komunikacijska MPLS-arhitektura DC HSE



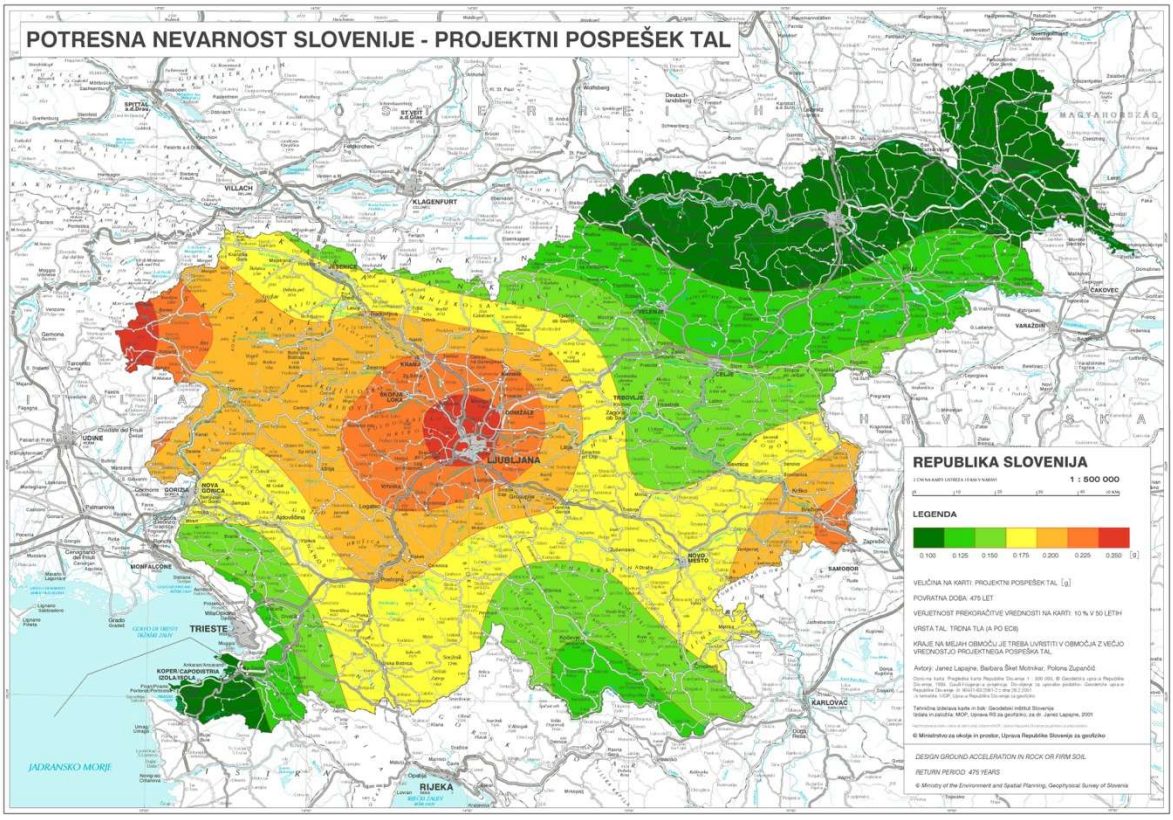
Vir: Prirejeno po Cisco (2016).

2.1.1 Lokacija računalniških centrov in potresna izpostavljenost

Oba računalniška centra skupine HSE se nahajata v Republiki Sloveniji, DC DEM na lokaciji Obrežna 170 v Mariboru, ob hidroelektrarni Mariborski otok, medtem ko se računalniški center DC TEŠ nahaja ob upravni stavbi TEŠ na lokaciji Cesta Lole Ribarja 18 v Šoštanju. Oba računalniška centra sta bila postavljena leta 2010, DC TEŠ v novo poslovno stavbo termoelektrarne, medtem ko je DC DEM nameščen v obnovljeni stavbi ob elektrarni HE Mariborski otok.

Računalniška centra se nahajata na področjih, kjer veljata srednja in nizka stopnja potresne intenzitete – ocena potresnega pospeška tal za območje DC TEŠ znaša 0,125 g oz. 1,23m/s^2, za DC DEM pa 0,1 g oz. 0,98 m/s^2 (povzet po Potresni nevarnosti Slovenije s slike 13). Vrednost pospeška tal na področju DC TEŠ, po standardu Uptime Instituta, predstavlja visoko stopnjo tveganja za potresno ogroženost. Iz trenutno dostopnih podatkov ni mogoče verodostojno oceniti protipotresne varnosti zgradbe in posledično podatkovnega centra.

Slika 13: Potresni zemljevid Republike Slovenije



Vir: PNS (2018).

Na območju, kjer se nahaja računalniški center DC TEŠ, ni zabeleženih primerov poplav, vendar obstaja manjše poplavno tveganje kletnih prostorov, kjer se nahaja podporna infrastruktura za električno napajanje.

2.1.2 Računalniški center DEM

Stavba, v kateri je nameščen računalniški center DC DEM s spremljajočimi prostori, je locirana na obrežju reke Drave, na sedimentni podlagi, kot je prikazano na sliki 14. Nanos sestavljajo aluvialni zasipi reke Drave.

Najbližje vodno telo, ki predstavlja potencialno grožnjo objektu, je reka Drava – približno 40 metrov severno od stavbe. Vendar je stopnja ogroženosti razmeroma nizka, saj se pri jezu v neposredni bližini regulira pretok oz. nivo reke Drave. Potresna intenzivnost območja, kjer je locirana stavba, je razmeroma nizka. Najbližje točke, ki kažejo na geotektonsko aktivnost, so locirane južno v okolici Slovenske Bistrice, z magnitudo 2,7–3,2, kar je nizka stopnja.

Slika 14: Lokacija DC DEM



Vir: DEM (2018).

Celotna spodnja etaža objekta, kjer se nahaja DC DEM, je izvedena tako, da vsebuje tri uporabne prostore, in sicer »varno kletko« (v izvedbi »soba v sobi«, proizvajalca Lampertz, model LSR 18.6 E), konzolni prostor in UPS-prostor (prikazano na sliki 8). Takoj po vstopu v objekt je manjši predprostor, iz katerega se pride v konzolni prostor skozi 60-minutna protivlomna vrata (120 x 220 cm). Iz konzolnega prostora je izveden vhod v »varno kletko« (kletka Lampertz) skozi ustrezna vrata (Lampertz) dimenzij 113 x 230 cm in v UPS-prostor skozi vrata dimenzij 120 x 220 cm. V DC DEM je izveden dvojni pod, na katerega se od vhoda pride po montažni klančini (možnost odstranitve), zaradi lažjega transporta opreme. Kletka Lampertz je notranjih dimenzij 7064 mm x 9484 mm in je dovolj velika za namestitev 18 strežniških omar. Pri tej postavitvi omar je izveden hladni koridor – na sprednji strani omar je koridor pokrit in zaprt z vrati. Dovod hladnega zraka se vrši pod dvojnim podom, kjer je tudi razvod napajanja za opremo, nameščeno v računalniškem centru. Oba klimata (vsak kapacitete hlajenja cca. 70 kW) sta nameščena v varni kletki. To predstavlja določeno prednost, saj se na tak način izognemo požarnim loputam. Hladen zrak prehaja skozi dvojni pod na sprednji strani strežniških omar. Vsi razvodi komunikacij in energetskih povezav znotraj visoko varnega sistemskega prostora potekajo v dvojnem podu po dveh ločenih trasah v mrežastih kanalih. Konzolni prostor je dovolj velik za tri delovna mesta. Prostor je klimatiziran z enim split klimatom kapacitete 2,5 kW z možnostjo ogrevanja prostora (hladilno-grelna naprava) z izvedenim zunanjim kondenzatorjem na zahodni strani fasade. V UPS-prostoru sta nameščeni dve RPS-napravi, prikazani na sliki 15, dveh UPS kapacitete 100 kVA (oz. cca 90 kW) in enega STS – statično preklopno stikalo. Prostor se hladi z dvema profesionalnima klimama hladilne moči cca. 13 kW.

Slika 15: Dinamična UPS in razvod napajanja



Vir: DEM (2018).

Osnovna varnost pred zunanjimi vplivi, kot so požar, voda, eksplozija, je izvedena z varno celico Lampertz Efficiency Room – LSR 18.6E s certifikatom ECB-S, površine 70 m² za 20 strežniških omar. Nameščena je znotraj objekta in popolnoma zaprta. Za komunikacijo z računalniškim omrežjem DEM in širše je DC DEM povezan z:

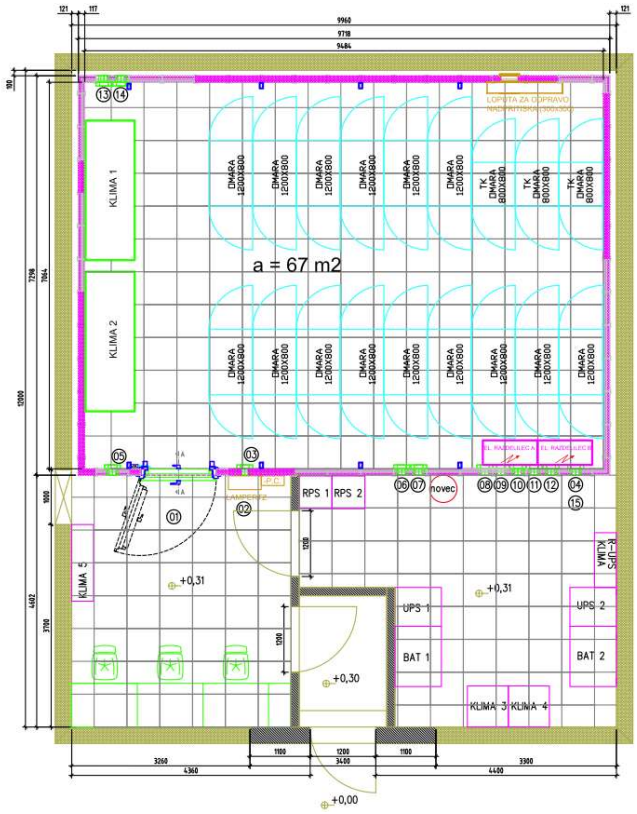
- 2 x 96 optičnih vlaken SM na trasi center vodenja DEM–DC DEM,
- 1 x 96 optičnih vlaken SM na trasi HE Mariborski otok–VVSP (visoko varni sistemski prostor).

Pri načrtovanju in izgradnji računalniškega centra DEM (tloris prikazan na sliki 16) je bil upoštevan standard ANSI/TIA-942. Po standardu je bilo določenih 8 gradnikov, ki zagotavljajo razpoložljivost in zanesljivost po TIER III in TIER IV:

- lokacija postavitve,
- način izgradnje,
- električno napajanje,
- hlajenje,
- varovanje in kontrola dostopov,
- telekomunikacije,
- požarna zaščita,
- podatkovna infrastruktura.

Sistem neprekinjenega napajanja je izveden z dinamičnima sistemoma UPS, diesel agregatom DEA, napajanjem iz lastne rabe HE Mariborski otok in iz 20-kV elektrodistribucijskega omrežja.

Slika 16: Tloris računalniškega centra DC DEM

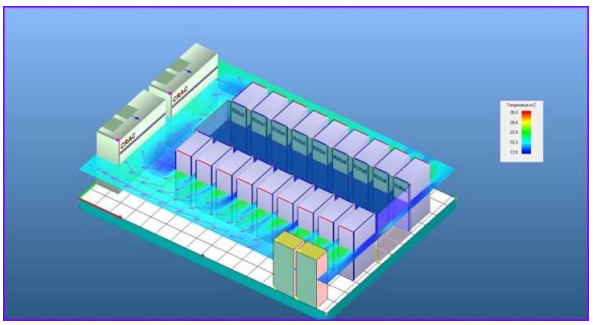


Vir: DEM (2018).

Sistem razvoda električne energije upošteva priporočila Uptime Instituta za takšne sisteme razreda 4 (TIER 4). Temelji na redundanci 1+1, kjer je vsaka IT-naprava napajana iz dveh neodvisnih virov električne energije. Omogočena sta celovit remont in servis kateregakoli elementa brez izpada delovanja celotnega sistema oskrbe.

Za hlajenje varne kletke sta nameščena 2 klimata, od katerih je vsak sposoben pohladiti predvideno nameščeno opremo. Za namen večjega izkoristka je med dvema vrstama omar nameščen hladilni koridor, v katerega se vpihuje hladen zrak (prikazano na sliki 17).

Slika 17: Kroženje zraka v DC DEM



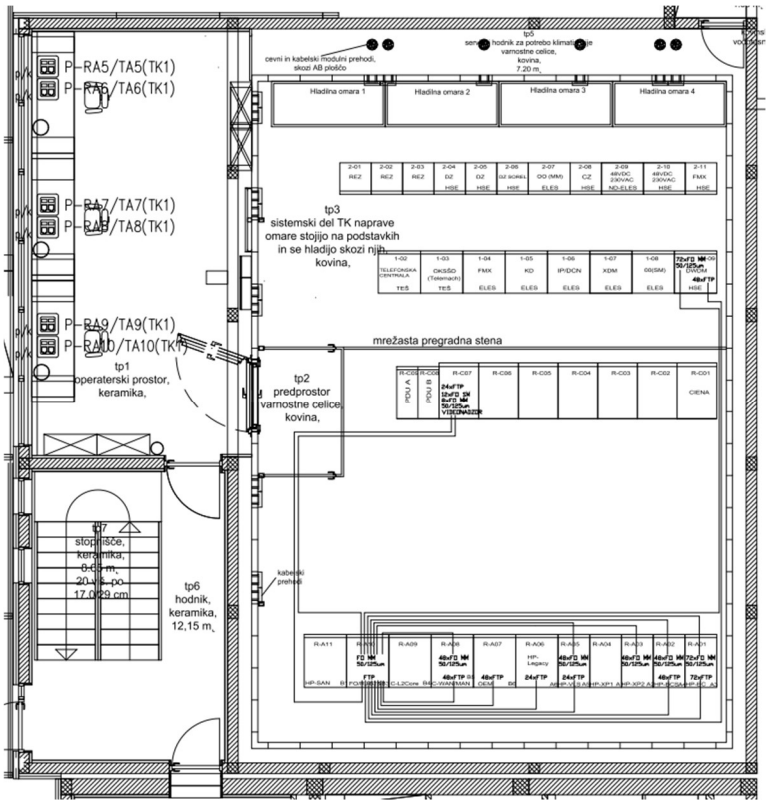
Vir: DEM (2018).

Za fizično in tehnično varovanje skrbi zunanji partner, s katerim družba sodeluje že vrsto let. Celotna senzorika in videonadzor potekata po več komunikacijskih povezavah, povezana sta z učinkovitim sistemom varovanja pri varnostnem podjetju. Za fizično varovanje skrbijo za to usposobljeni varnostniki.

2.1.3 Računalniški center TEŠ

Računalniški center TEŠ (DC TEŠ) s slike 18 je umeščen v pritličje stavbe, v prostor, znotraj katerega je zgrajena »varna celica« po standardu EN-1047/2. Zaradi načina hlajenja vgrajene opreme je celotna konstrukcija računalniškega centra postavljena na dvojni pod, ki je primarno namenjen dovodu hladnega zraka iz hladilnih naprav, nameščenih ob levem zidu varne celice, sekundarno pa služi tudi za razvod kabelskih povezav jakega in šibkega toka ter telekomunikacij. Prostor računalniškega centra je s kovinsko mrežno pregrado razdeljen na tri dele. Prvi del predstavlja vstopno »vežo«, iz katere je s kartičnim sistemom pristopne kontrole mogoče vstopiti v levi ali desni del varne celice. Vstop v prostor računalniškega centra je mogoč le skozi ognjevarna vrata varne celice iz operaterskega predprostora.

Slika 18: Tloris računalniškega centra TEŠ

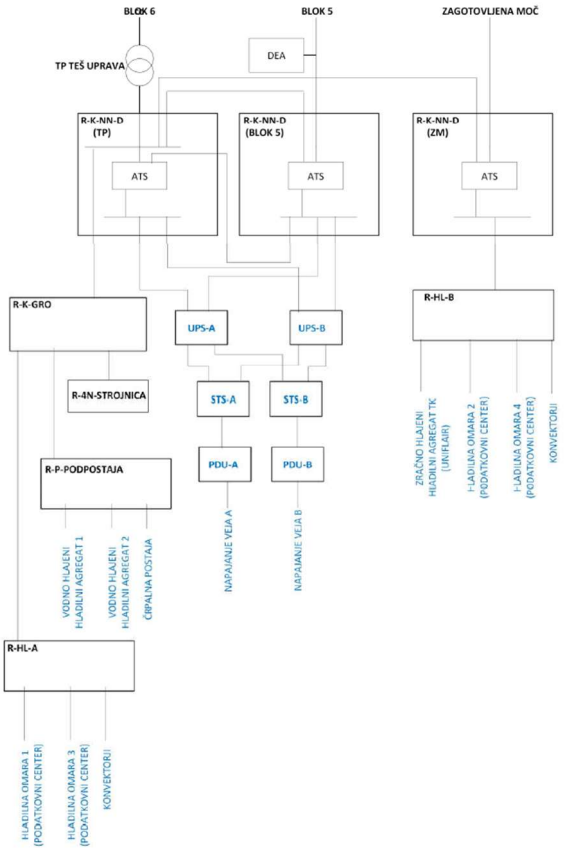


Vir: TEŠ (2018).

Vrata so varovana s sistemom kontrole pristopa na osnovi brezkontaktnih kartic. Vsi prostori so varovani tudi s sistemom videonadzornih kamer. Vstop v ograjeni del računalniškega centra je nadalje mogoč skozi vrata v kovinski ograji, ki so varovana. Predelne stene okoli

varne celice so izdelane iz armiranobetonske konstrukcije. V prostoru je vgrajen dvojni pod svetle višine 80 cm in skupne višine 85 cm. V prostoru ni oken, saj se ta nahaja v varni celici. Okna so nameščena le v predprostoru. V prostoru so razporejene 4 klasične hladilne omare (CRAC) proizvajalca UNIFLAIR in tipa LEONARDO TDCV, ki so nameščene ob levem zidu prostora, gledano od vhodnih vrat. V obeh delih varne celice je postavljenih več komunikacijskih omar, ki se hladijo z vpihom hladnega zraka iz dvojnega poda. Hladilne omare zajemajo segreti zrak pod stropom podatkovnega centra, vpihujejo pa ga skozi odprtine v prostoru dvojnega poda. Taka umestitev hladilnih naprav v primeru servisa zahteva vstop serviserjev v prostor podatkovnega centra, kar predstavlja manjši varnostni pomislek. Električno napajanje bremen v podatkovnem centru je izvedeno po sistemu 2(N+1) (A+B napajanje). Prostor računalniškega centra je požarno varovan s stabilno požarno centralo in sistemom aktivnega gašenja. Detekcija požara poteka v dveh fazah prek vgrajenih klasičnih senzorjev dima/toplote in aspiracijskega sistema, ki preverja vsebnost delcev dima v zraku. Sistem gašenja je izveden na osnovi kemičnega gasilnega sredstva (plina) FM200. Gasilno sredstvo se nahaja v jeklenki, postavljeni v tehnološki hodnik ob prostoru podatkovnega centra, levo od vhoda. Dostop do tega prostora je mogoč le skozi operaterski prostor.

Slika 19: Električno napajanje računalniškega centra TEŠ



Vir: TEŠ (2018).

S slike 19 je razvidno, da je električno napajanje upravne stavbe TEŠ, kjer je nameščen računalniški center, izvedeno iz več virov:

- iz NN-bloka TP TEŠ-uprava, ki je postavljen v bližini upravne stavbe. Dovod iz TP do električnega razdelilnika (TP) v kleti objekta je izveden s kablom 2x NY2Y-J 4 x 240 mm^2,
- iz Bloka 5 je izveden dovod do električnega razdelilnika (Blok 5) v kleti objekta s kablom NY2Y-J 4 x 240 mm^2,
- kot tretji vir napajanja je »zagotovljena moč«, za katero je položen kabel NY2Y-J 4 x 70 mm^2 do električnega razdelilnika.

Vsi trije električni razdelilniki se nahajajo v skupnem prostoru v kleti upravnega objekta in imajo vgrajena avtomatska preklopna stikala (ATS), ki v primeru izpada posameznega vira preklopi na drugi razpoložljivi vir (TP TEŠ-uprava, Blok 5, zagotovljena moč). Na tak način je zagotovljena redundanca napajanja že na tem nivoju. Ključno za delovanje preklopov je, da je krmiljenje stikal ATS opravilno. V primeru izpada krmiljenja teh stikal je preklop mogoče izvesti ročno. Dodatno rezervno napajanje razdelilnika (Blok 5) je zagotovljeno z dizelskim električnim agregatom (DEA) proizvajalca MTU (Uljanik, Pulj), moči 529 kW in ročnim zagonom. Agregat je nameščen v posebnem prostoru, namenjenem agregatu, izpuh je speljan na prosto po izpušni cevi, zajem zraka pa poteka prek EM-žaluzij in filtrov. DEA uporablja rezervoar prostornine 2000 litrov, kar pri nazivni porabi pri maksimalni moči 0,26 litra/minuto zadošča za več kot 12 ur avtonomije, kot je zahtevano po klasifikaciji Uptime Instituta. V primeru potreb po daljšem delovanju je mogoče polnjenje rezervoarja ob delovanju DEA.

Sistema brezprekinitvenega napajanja UPS-A in UPS-B sta tipa APC SYMMETRA PX 160 in napajata porabnike, priključene na inteligentna električna razdelilnika PDU-A in PDU-B, ki se nahajata v prostoru računalniškega centra. Sistema UPS sta modularne zasnove, kar pomeni, da:

- omogočata postopno nadgradnjo električne moči brez zaustavitve (ang. hot swap) z vgradnjo dodatnih močnostnih modulov v korakih po 16 kW do moči 160 kW oz. 144 kW na stopnji redundance N+1,
- zamenjavo okvarjenih modulov brez zaustavitve,
- dogradnjo in/ali zamenjavo baterijskih modulov in s tem povečanje avtonomije brez zaustavitve sistema,
- namestitev rezervnih modulov za doseganje stopnje redundance N+r.

Trenutna redundanca posamezne naprave UPS je N+1, kar pomeni, da ima posamezna naprava vgrajenih toliko modulov, da je glede na potrebno moč en modul vedno v redundanci (rezervi). Oba UPS ob trenutni obremenitvi omogočata še precejšnjo rast moči priključene opreme IT in delujeta v sistemu 2(N+1). Nameščena sta v kleti v ločenih prostorih, namenjenih UPS-sistemom – prostor UPS-A in UPS-B, skupaj z baterijami in

STS-stikali. Prostori so med seboj ločeni s požarno varnimi vrati. Prostori so hlajeni s stropnim konvektorskim sistemom. Sistema UPS-A in UPS-B se napajata iz električnih razdelilnikov. Izhoda iz obeh UPS-sistemov sta povezana s STS-stikali proizvajalca MGE, tipa UPSILON STS 250A. V primeru izpada ene od naprav UPS bosta STS-stikali preklopili na drugi vir (drugo napravo UPS) in s tem zagotovili napajanje obeh PDU-razdelilnikov v podatkovnem centru (PDU-A in PDU-B). Seveda pa je za tak način delovanja treba zagotoviti, da posamezna naprava UPS nikoli ni obremenjena z več kot 50 % svoje inštalirane električne moči, saj v primeru izpada ene od obeh naprav celotno breme prevzame druga.

Računalniški center je postavljen v varni sobi proizvajalca Lampertz (varni celici), ki zagotavlja požarno zaščito po standardu EN1047-2, primerno vgrajeni IT-opremi. Varna celica je certificirana po standardu EN1047-2. Certifikat je izdala ECB-S. Standard EN1047-2 definira, da mora v primeru požara zunaj varne sobe ta zdržati 1 uro pri zunanji temperaturi 950 °C, pri čemer se temperatura v varni sobi ne sme povišati za več kot 50 °C (oz. na max. 70 °C), relativna vlažnost pa ne sme preseči 85 %. Klasična ognjevarna gradnja pri izgradnji poslovnih objektov upošteva ognjevarnost, ki v primeru požara v sosednjem prostoru za zgornjo temperaturo upošteva tisto, pri kateri začne papir rumeneti (150 °C). Tipična IT-oprema zdrži maksimalno 70 °C, nekatera diskovna polja in tračne enote pa le 50 °C, kar pomeni, da bi bil v primeru požara zunaj podatkovnega centra, če ta ne bi bil vgrajen v varno celico, izpostavljen nevarnostim odpovedi opreme zaradi pregrevanja in vdora vode ob gašenju. V računalniškem centru je nameščen sistem detekcije požara z optičnimi in termičnimi senzorji ter sistemom aspiracije, ki so priključeni na požarno centralo. Prostor računalniškega centra je požarno varovan s stabilno požarno centralo Zarja NJP 400A in sistemom aktivnega gašenja. Detekcija požara poteka v dveh fazah prek vgrajenih klasičnih senzorjev dima/toplote in aspiracijskega sistema, ki preverja vsebnost delcev dima v zraku. Sistem gašenja je izveden na osnovi kemičnega gasilnega sredstva (plina) FM200. Gasilno sredstvo (225 kg) se nahaja v jeklenki, postavljeni v tehnološki hodnik ob prostoru računalniškega centra, levo od vhoda. Dostop do tega prostora je mogoč le skozi operaterski prostor (tehnološki predprostor).

Za odvod odpadne toplote iz prostorov varne celice ter NN- (nizke napetosti) in UPS-prostorov se uporablja dva hidravlično ločena sistema. Vir primarnega sistema sta dva vodno hlajena hladilca tekočin proizvajalca BlueBox, vir sekundarnega oziroma rezervnega sistema je zračno hlajen hladilec tekočin proizvajalca Uniflair. Sekundarni vir je namenjen samo hlajenju podatkovnega centra in podpornih prostorov, na primarni vir pa so priklopljeni še drugi uporabniki. Preklop med primarnim in sekundarnim sistemom za odvod toplote se izvaja ciklično, predvsem za preverbo delovanja sekundarnega sistema, z namenskim krmilnikom. V primeru odpovedi namenskega krmilnika se zaženeta tako primarni kot sekundarni sistem za odvod odpadne toplote. V prostoru varne celice se nahajajo štiri hladilne omare proizvajalca Uniflair, model TDCV2500. Dve od teh omar sta priklopljeni na primarni hladilni sistem. Za transportni medij na primarnem viru hlajenja se uporablja

vodo. Predvideni režim hladilnega medija je 7/12 °C. Pri tem režimu hladilne tekočine zmore posamezna hladilna omara okoli 74 kW neto senzibilne hladilne moči. Nominalna moč je izračunana pri 24 °C povratnega zraka in 50-% relativni vlažnosti. Kar pomeni, da lahko s primarnim hladilnim sistemom v varni celici zagotovimo pri temperaturnem režimu 7/12 °C okoli 125 kW hladilne moči, saj je pretok transportnega medija omejen s črpalko, kljub temu da lahko s samo hladilno opremo v varni celici dosegamo 148 kW. Z večanjem temperaturne razlike med temperaturo hladilnih reber (odvisna od temperature hladilnega/transportnega medija in pretoka) in temperaturo povratnega zraka večamo zmogljivosti hladilnih enot.

2.2 Učinkovitost računalniških centrov skupine HSE

Učinkovitost računalniških centrov se določa z uveljavljeno metodo PUE (power usage efficiency), ki podaja razmerje med vso porabljeno energijo ali močjo centra (oprema IKT in vsa infrastrukturna podporna oprema) ter močjo oziroma porabo opreme IKT (Belady & Malone, 2007), kot je podano z enačbo (3):

$$PUE = \frac{vsa\ poraba\ ali\ moč\ DC}{IKT\text{-}poraba\ ali\ moč} \tag{3}$$

Učinkovitost računalniškega centra PUE vpliva na celotne stroške delovanja računalniškega centra. V preteklosti stroški za električno energijo niso imeli pomembne vloge, danes ni tako. Z energetsko učinkovitostjo je mogoče bistveno vplivati na stroške. Vpliv učinkovitosti računalniškega centra je prikazan v tabeli 4 – pri čemer je PUE med 1,0 in 2,0 dober, do 2,4 povprečen in do 3,0 slab.

Tabela 4: PUE in stroški

Moč IKT-opreme (kW)	PUE	Skupna moč (kW)	Mesečna količina porabljene energije (kWh)	Mesečni strošek el. energije (EUR)	Preplačilo el. energije*	Strošek izgradnje
100,00	1,00	100,00	74.400	3720,00	0,00	3500,00
100,00	1,15	115,00	85.560	4278,00	558,00	3500,00
100,00	1,30	130,00	96.720	4836,00	1116,00	3500,00
100,00	1,50	150,00	111.600	5580,00	1860,00	3500,00
100,00	2,0	200,00	148.800	7440,00	3720,00	3500,00
100,00	2,50	250,00	186.000	9300,00	5580,00	3500,00

*Pri PUE = 1,00 plačamo ceno električne energije za optimalno učinkovitost, pri PUE = 1,15 plačamo zaradi slabše energetske učinkovitosti 558,00 EUR več itd.

Vir: lastno delo.

V tabeli smo izračunali strošek izgradnje računalniškega centra DC DEM iz leta 2010 z naslednjim stroškovnikom:

- 18 sistemskih omar, kapaciteta 120 kW, skladnost s TIER I–III,
- amortizacija 15 let,
- življenjska doba 20–25 let,
- investicija 650.000,00 EUR,

- cena električne energije 0,05 EUR/kWh.

Izračunani povprečni PUE v skupini HSE na letnem nivoju znašajo:

- DC DEM – 2,00,
- DC TEŠ – 2,50.

2.3 Ocena skladnosti računalniških centrov skupine HSE po metodologiji TUV

Pri pregledu kriterijev za računalniške centre, ki jih je razvilo podjetje TUV (TUV, 2018), smo ocenili varnost in skladnost računalniških centrov skupine HSE, pri čemer smo še posebno natančno pregledali naslednja področja:

- ali so politike in postopki (procedure) v računalniških centrih opredeljeni, dokumentirani in pravilno objavljeni,
- ali so ključni elementi in prostori računalniških centrov ustrezno varovani pred nepooblaščenim dostopom,
- kako se spremljajo dostopi (fizični in oddaljeni) do računalniških centrov in ali se redno preverjajo pravice dostopa,
- kako funkcionirajo kontrole za zaščito strežnikov in druge IT-opreme pred požarom, električnimi napakami in vdorom vode,
- kako se upravlja zmogljivosti računalniškega centra,
- ali se oprema redno vzdržuje in preizkuša,
- ali je zagotovljena rezervna oskrba z električno energijo.

Tabela 5: Skladnost z metodologijo TIER III

Računalniški center	DC DEM	DC TEŠ
Električno napajanje		
Napajalni sistem	TIER III	TIER III
Dizelski agregat	1	1
UPS (brezprekinitveni napajalnik)	2	2
Distribucijska omara	2	2
Vir napajanja	2 (HE Mb. otok + distribucija)	2 (Blok 5, Blok 6)
Hlajenje		
Hladilni agregati RC	2	4
Hladilni agregati UPS	2	
Sistem črpalk	TIER III	TIER III
Vodovod	Ring	Ring
Nadzor opreme		
Centralni nadzorni sistem	Da (DCIM NTR)	Da (CNS TK)
Sistem javljanja napak (SMS, elektronska pošta, alarm dispečerjem)	Da	Opcija
Vzdrževanje		
Možnost celovitega vzdrževanja med obratovanjem	Delno	Delno

Vir: lastno delo.

Ugotovitve glede na izvedeno analizo stanja sistema napajanja računalniškega centra TEŠ in DEM, prikazane v tabeli 5, so:

- sistem redundantnega NN-napajanja iz različnih virov zagotavlja v okvirih nazivne električne moči možnost preklopa med njimi in s tem zagotavlja redundanco napajanja v primeru izpada ali okvare posameznega vira,
- sistem dizelskega električnega agregata v kombinaciji s preklopi in baterijskimi sistemi zagotavlja neprekinjeno delovanje naprav, ki so ključne za zagotavljanje neprekinjenega delovanja računalniških centrov skupine HSE. V prihodnje je treba razmisliti o možnosti priključitve dodatnega (zunanjega) dizelskega agregata – predvsem zaradi morebitnega dolgotrajnega servisa primarnega dizelskega agregata,
- avtomatizirani preklopi med posameznimi viri skrbijo, da se ob izpadu posameznega vira električnega napajanja in težavah ob prevzemu bremena vzpostavi napajanje iz drugih virov,
- izvedba elektroinštalacij, izbrana oprema in nadzor delovanja sistema so tehnično popolnoma ustrezni in izpolnjujejo predpise in tehnične smernice. Za boljše upravljanje je treba razmisliti o poenotenju sistemov za nadzor – uvesti enoten DCIM,
- dokumentacija sistema električnega napajanja je ažurirana in odraža trenutno stanje,
- naprave sistema brezprekinitvenega napajanja so redno vzdrževane, na njih se izvajajo periodični zagoni in testiranja – razmisliti velja o temeljitejšem in bolje dokumentiranem testiranju celotne oskrbne infrastrukture.

Pri analizi trenutnega izvedenega stanja sistema hlajenja infrastrukture računalniških centrov skupine HSE je bilo ugotovljeno naslednje:

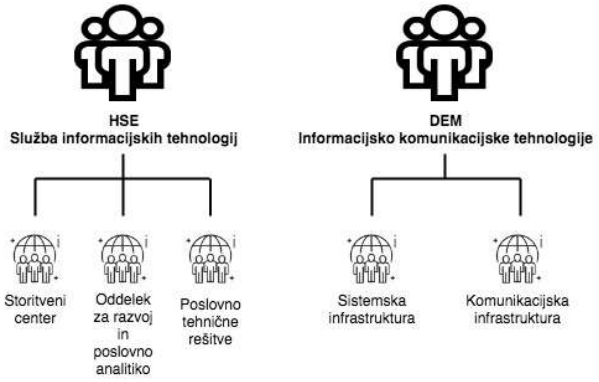
- na lokaciji DC TEŠ je treba s požarnimi pregradami ločiti vse med seboj redundantne sisteme hlajenja (posamezne hladilne agregate, toplotne prenosnike itd.),
- treba je zagotoviti neprekinjeno napajanje hlajenja v času morebitnega izpada električne energije (od izpada omrežnega napajanja do preklopa na alternativni vir oz. do zagona DEA). To se lahko stori s priklopom črpalk za distribucijo hladiva in hladilnih naprav v prostoru DC TEŠ na namenski sistem UPS in zadostno kapaciteto zalogovnikov hladiva. Na tak način bi bila zagotovljena distribucija hladiva iz zalogovnikov do hladilnih enot v prostoru in tudi delovanje hladilnih enot za čas do vzpostavitve rezervnega napajanja,
- v skladu z zahtevami po energetski učinkovitosti je treba v DC TEŠ izvesti sistem hladnega koridorja.

2.4 Obvladovanje procesov v računalniških centrih skupine HSE

Pri obvladovanju procesov v računalniških centrih skupine HSE je bilo treba podpreti ključna izhodišča oziroma vprašanja, kot so: kako obvladati tveganja vsakodnevnega delovanja računalniških centrov, izrednih dogodkov in odzivov na te dogodke. Osnovo ponujata nabor ukrepov iz sistemov vodenja in standardizacije (ISO-standardi: 9001, 27001,

14001, ITIL, Cobit) ter niz organizacijskih predpisov in tehniških navodil. Ključni pri upravljanju oskrbne infrastrukture so strokovnjaki različnih profilov: strojniki, električarji, informatiki in drugo osebje zunanjih partnerjev. Zanje obstajajo objavljena dokumentacija v dokumentacijskem sistemu BC (business connect), sistem za prijavo napak in dogodkov Zenas ter mehanizem upravljanja incidentov. Matrično organizirana skupina s slike 20 zagotavlja IKT-storitve za skupne potrebe družb skupine HSE, pri čemer je družba DEM odgovorna za sistemsko in komunikacijsko infrastrukturo, za preostale IT-storitve pa je pristojen HSE.

Slika 20: Organiziranost IT v skupini HSE



Vir: HSE (2018).

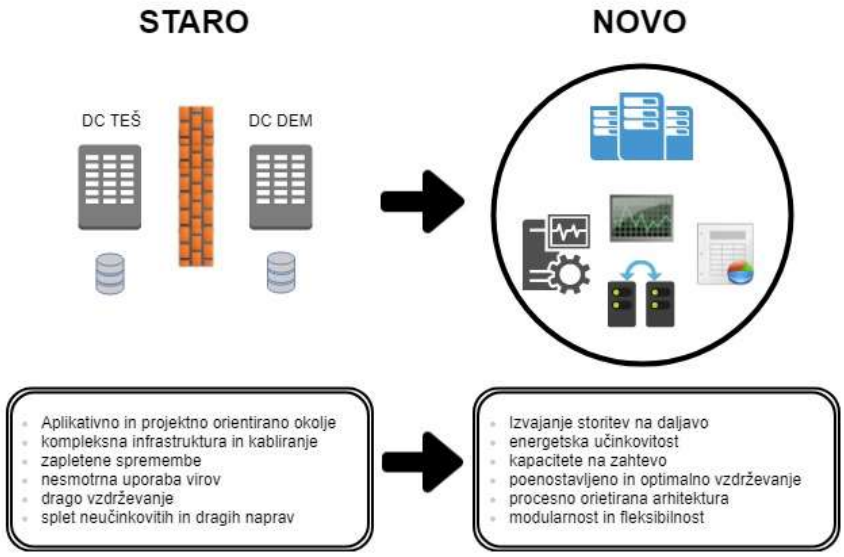
2.5 Skladnost računalniških centrov skupine HSE s standardom ISO/IEC 27001:2013

Oba računalniška centra DC TEŠ in DC DEM sta opredeljena kot informacijski sredstvi v ločenih sistemih upravljanja varovanja informacij po ISO/IEC 27001:2013. Zanju je bila izvedena ocena tveganja in v preteklosti sta bila priči nekaterim dodatnim ukrepom po zagotavljanju informacijske varnosti. V družbah HSE, d. o. o., DEM, d. o. o., in TEŠ, d. o. o., se vsako leto izvajajo notranje in zunanje presoje v skladu s smernicami standarda. Vse tri družbe skupine so pri vsaki presoji skladne s standardom, vendar podrobne presoje računalniških centrov še ni bilo. Vzrok za to v veliki meri tiči v problematiki dojemanja celovitega računalniškega centra z vso oskrbno infrastrukturo in pomanjkanju ustrezne metodologije za odkrivanje varnostnih ukrepov. Glede na to, da omenjene družbe vsako leto prejmejo potrjen oz. recertificiran certifikat skladnosti, lahko trdimo, da so računalniški centri skupine HSE skladni s standardom ISO/IEC 27001:2013.

3 VZPOSTAVITEV ENOTNEGA SISTEMA UPRAVLJANJA VAROVANJA INFORMACIJ V RAČUNALNIŠKIH CENTRIH SKUPINE HSE

Cilj tega poglavja je poenostaviti in racionalizirati procese računalniških centrov skupine HSE z namenom izboljšanja porabe virov, upravljanja in ponujanja storitev. Pri pripravi metodologije bomo upoštevali napotke mednarodno priznanih standardov, še posebno standarda ISO/IEC 27001:2013, ISO 22301 ter priporočila Uptime Instituta in njihove klasifikacije TIER. Pri vzpostavitvi sistema bomo sledili dognanjem in znanju iz 5. poglavja. Analiza stanja informacijske varnosti v računalniških centrih skupine HSE ter dobre prakse uveljavljenih institucij, ki se ukvarjajo z upravljanjem računalniških centrov. Naš cilj bo prehod s starega na nov način upravljanja, kot je prikazano na sliki 21.

Slika 21: Stanje računalniških centrov HSE pred prenovo in po prenovi



Vir: lastno delo.

Eden od načinov zagotavljanja višjega nivoja varnosti v računalniških centrih skupine HSE je implementacija enotnega sistema upravljanja varovanja informacij. V svetu trenutno ne obstaja sistem, ki bi v celoti in ekskluzivno pokrival problematiko računalniških centrov. Sam standard nam ponuja osnovni okvir za vzdrževanje informacijske varnosti, z učinkovitimi ukrepi in mnogimi prilagoditvami smo aplicirali zahteve standarda z izkušnjami po varovanju informacijskih sredstev na sredstvih kritične infrastrukture računalniških centrov. Predstavljen koncept smo implicirali na človeških virih, procesih in tehnologijah. Predstavlja politike in procedure, ki ponujajo učinkovito orodje za upravljanje varovanja informacij.

3.1 Izhodišča za delovanje računalniških centrov po prenovi

Osnovno izhodišče za delovanje računalniških centrov skupine HSE je visoka razpoložljivost oskrbne infrastrukture in varnost delovanja. Ključna izhodišča lahko povzamemo kot:

- visoko razpoložljivo delovanje vse oskrbne infrastrukture,
- varovanje opreme pred zunanjimi in notranjimi grožnjami,
- odpornost proti izpadom posamezne opreme v skladu s poslovnimi cilji,
- nadzorljivost vseh elementov oskrbne infrastrukture,
- možnost spremljanja delovanja in alarmiranja ob izrednih situacijah,
- zagotavljanje celovitega vzdrževanja za ohranjanje ciljne razpoložljivosti.

Hkrati je poslovodstvo, na osnovi predstavljene analize, v pogovorih z vzdrževalci računalniških centrov postavilo naslednje zahteve:

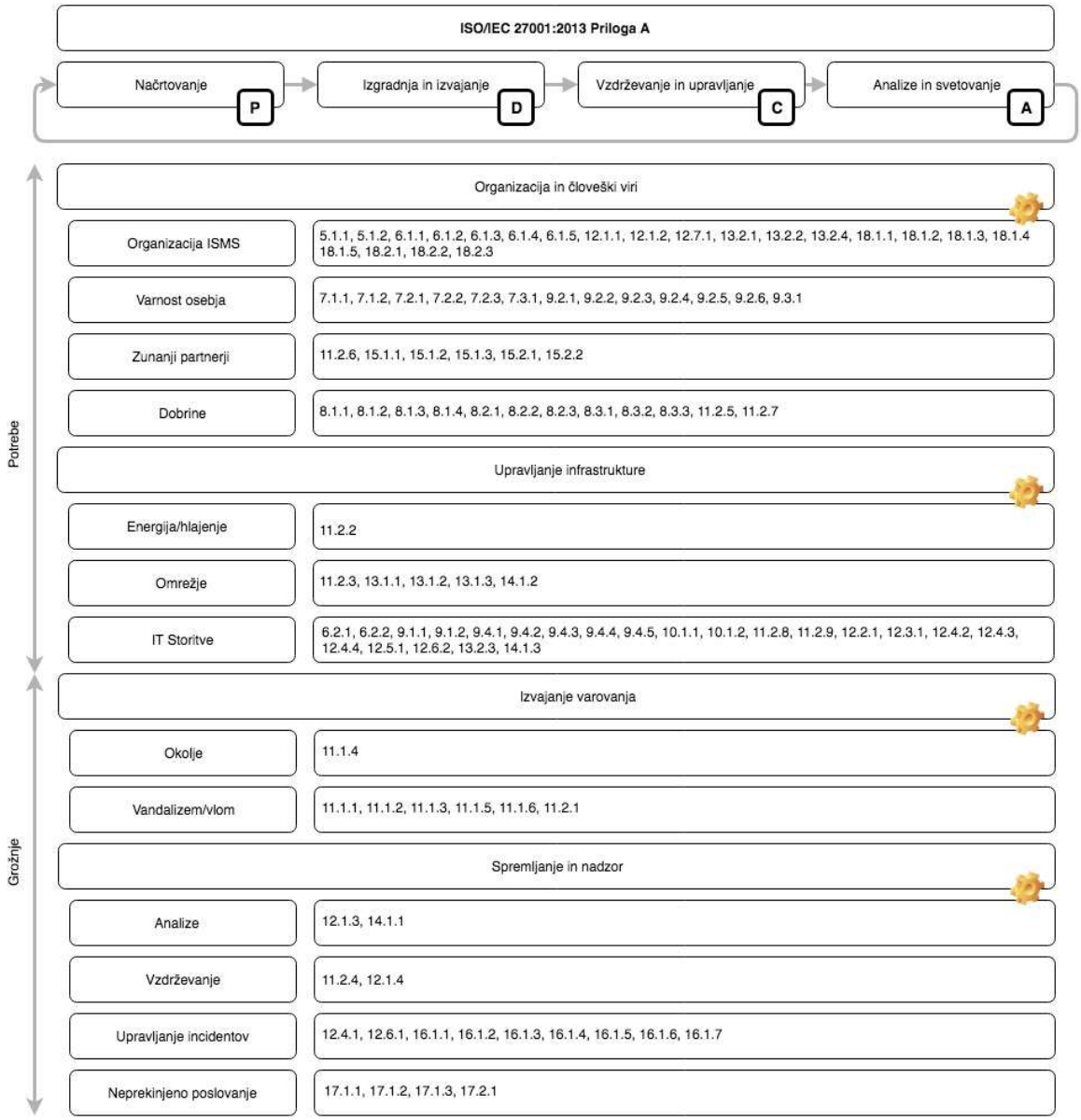
- skladnost s klasifikacijo TIER III po Uptime Institutu v vseh računalniških centrih,
- zahtevana odpornost proti izpadom, ki mora biti zagotovljena za vse enkratne izpade (izpad kateregakoli kosa aktivne opreme),
- zahtevano alarmiranje ob kakršnihkoli izpadih ali preseganju mejnih temperatur,
- sprejemljiv čas odziva vzdrževalcev je največ 2 uri,
- zahtevane kapacitete računalniških centrov v smislu tehničnega hlajenja morajo učinkovito in varno zagotavljati dovolj hladu,
- ciljna energetska učinkovitost vseh centrov, kjer se znižajo stroški za električno energijo za 20 %.

3.2 Prepoznani procesi pri upravljanju računalniških centrov

Osnovni poslovni procesi pri upravljanju računalniških centrov in vzpostavitev ustrezne varnosti so tisti, ki zagotavljajo varno in zanesljivo ter nemoteno delovanje IKT-opreme, preprečujejo napake in izpade tehnične narave ali zaradi človeškega dejavnika ter zagotavljajo predvidljivost in ponovljivost vseh postopkov. Z vzpostavljenimi pravili pri prepoznanih procesih standardiziramo postopke, opremo, varnostne mehanizme, komunikacijo in ciljne lastnosti ter zahteve za trenutne in bodoče računalniške centre skupine HSE. Na sliki 22 so prikazani procesi pri upravljanju računalniških centrov skupine, opremljeni s kontrolami iz priloge A-standarda ISO/IEC 27001:2013. Gre za tako imenovani model sistema upravljanja varovanja informacij v računalniških centrih skupine HSE. Model izpolnjuje osnovne zahteve po zaupnosti, integriteti in razpoložljivosti. Poudariti je treba, da standard podaja le splošen okvir za vzdrževanje informacijske varnosti v računalniških centrih. Aktivnosti načrtovanja, izvajanja, upravljanja in analiz iz Demingovega ali PDC-kroga se ponavljajo in ves čas izboljšujejo.

Za temeljito obvladovanje varnostnih tveganj v računalniških centrih skupine HSE sem pripravil nabor vseh ukrepov, ki podpirajo prilogo A standarda ISO/IEC 27001:2013, z upoštevanjem štirih glavnih procesov pri delovanju tako kompleksne infrastrukture, kot so računalniški centri. Takšen pristop je inovativen, v svetovni literaturi nisem našel podobnega primera.

Slika 22: Procesi in kontrole ISMS v RC skupine HSE



Vir: lastno delo.

3.3 Kontrole za izvajanje procesov v računalniških centrih skupine HSE

Informacijsko varnost računalniških centrov v skupini HSE smo dosegli z izvajanjem ustreznih kontrol, vključno s politikami, procesi, postopki, organizacijskimi strukturami ter

s sistemsko programsko in strojno opremo. Prepoznavanje in uvedba kontrol so skrbno načrtovani in se v veliki meri osredotočajo na podrobnosti upravljanja in delovanja računalniškega centra. V veliki meri se sistem naslanja na obstoječe varnostne mehanizme v skupini in upošteva že zapisane varnostne mehanizme iz nabora kontrol standarda ISO/IEC 27001:2013. Za uspešno upravljanje sistema informacijske varnosti skrbijo dobro usposobljena organizacijska struktura in s strani vodstva zagotovljeni viri. Sam sistem omogoča celovit in koordiniran pogled na informacijska varnostna tveganja v računalniških centrih skupine HSE, pri čemer lahko izvaja celovit niz navedenih kontrol. Pri prepoznavanju varnostnih zahtev smo v skupini prepoznali tri glavne vire, in sicer:

- izvedba ocene tveganj na informacijskih virih upoštevajoč poslovne strategije in usmeritve vodstva ter ciljev skupine. Prepoznali smo grožnje dobrinam, ovrednotili ranljivosti in verjetnost pojava ter ocenili morebiten vpliv,
- zakonske, pogodbene in pravne vidike, ki jih upoštevajo in izpolnjujejo vsi, ki so na takšen ali drugačen način vpeti v izvajanje storitev v računalniških centrih,
- načela in poslovne zahteve za upravljanje informacij in sredstev, ki ponujajo podporo delovanju računalniških centrov v skupini HSE.

Rezultati izvedbe ocene tveganj, ki temeljijo na izvedenih ukrepih, pomagajo voditi procese in prednostne naloge, izbrane za varno obratovanje kritične infrastrukture.

S predstavljenim modelom se zagotavlja:

- varnost osebja in obiskovalcev,
- varnost storitev in razpoložljivost,
- varnost podatkov,
- revizijske sledi,
- merljive cilje delovanja,
- usmeritve za izvajanje pregledov in vzdrževalnih procesov.

Pri zagotavljanju učinkovite varnosti v računalniških centrih skupine HSE se sledi naslednjim zahtevam:

- določitev varnostnih con in mehanizmi dostopne kontrole,
- določitev pravic dostopa,
- zahteve za tehnično varovanje,
- zagotavljanje revizijskih sledi,
- preprečevanje zlorabe infrastrukture,
- zagotavljanje varnosti in zdravje,
- nadzor.

3.3.1 Organizacija in človeški viri

Pri izvajanju varovanja informacij v računalniških centrih so ljudje ključnega pomena. Vsakdo, ki sodeluje v procesih varovanja podatkov in varnega obratovanja računalniškega centra, se mora zavedati pomembnosti svoje vloge pri preprečevanju ali zmanjševanju groženj. Sposobnost in usposobljenost zaposlenih zagotavljata učinkovito izvajanje nadzornih postopkov in izkoriščanje obstoječe tehnologije. Nekaj primerov iz referenčnih ciljev kontrol in samih kontrol:

- ***Organizacija ISMS***

  V skupini HSE je zavedanje o informacijski varnosti na visokem nivoju – uvedba politik za varovanje informacij in učinkovito upravljanje računalniških centrov sovpada s strateškimi cilji družb v skupini in že sprejetimi in certificiranimi sistemi za upravljanje varovanja informacij. Kontrole s področja organizacije ISMS iz tabele 6 se v veliki meri pokrivajo z že obstoječimi politikami in pravili, nadgrajene so le s specifičnimi zahtevami po višji varnosti in upravljanju nekaterih zunanjih storitev.

Tabela 6: Kontrola organizacije informacijske varnosti

Zap. št.	Št. kontrole	Kontrola
1.	5.1.1	Politike za informacijsko varnost
2.	5.1.2	Pregled politik za informacijsko varnost
3.	6.1.1	Vloge in odgovornosti na področju informacijske varnosti
4.	6.1.2	Razmejitev dolžnosti
5.	6.1.3	Stik s pristojnimi organi
6.	6.1.4	Stik s specifičnimi interesnimi skupinami
7.	6.1.5	Informacijska varnost v upravljanju projektov
8.	12.1.1	Dokumentirani postopki delovanja
9.	12.1.2	Upravljanje sprememb
10.	12.7.1	Kontrole presoje informacijskih sistemov
11.	13.2.1	Politike in postopki prenosa informacij
12.	13.2.2	Dogovori o prenosu informacij
13.	13.2.4	Dogovori o zaupnosti ali nerazkrivanju
14.	18.1.1	Prepoznavanje veljavnih zakonskih in pogodbenih zahtev
15.	18.1.2	Pravice intelektualne lastnine
16.	18.1.3	Zaščita zapisov
17.	18.1.4	Zasebnost in zaščita osebno določljivih podatkov
18.	18.1.5	Uporaba kriptografskih kontrol
19.	18.2.1	Neodvisni pregled informacijske varnosti
20.	18.2.2	Skladnost z varnostnimi politikami in standardi
21.	18.2.3	Pregled tehnične skladnosti

Vir: prirejeno po SIST (2013).

- A.5 Informacijske varnostne politike – politike so tista načela upravljanja, ki jih morajo upoštevati vsi nivoji v družbi. Opisani so koraki, kako naj se politika izvaja, ki nam služijo kot vodila za operativno informacijsko varnost v računalniških centrih. Nekaj varnostnih politik in procedur:

- Računalniški center ima zapisane politike informacijske varnosti, ki jih odobri poslovodstvo. S politiko so seznanjeni vsi zaposleni in zunanji partnerji, ki imajo dostop do omenjene infrastrukture.
- Vsi operativni postopki in predpisi se ustrezno beležijo, shranjujejo in prikazujejo na način, da so vidni vsem zaposlenim.
- Varnostni protokoli in procedure ter politike se obravnavajo na kvartalnih formalnih srečanjih ekipe za varovanje informacij v skupini.

- A.6 Organiziranje informacijske varnosti – računalniški center mora biti del interne organizacije, pristojne za zagotavljanje varnosti in neprekinjenega poslovanja.
  - Področja odgovornosti in dolžnosti je treba ločiti. Določene in dodeljene so vse odgovornosti na področju upravljanja in varovanja informacij v računalniškem centru v skladu z informacijskimi politikami – področja, za katera so posamezniki odgovorni, se navajajo v ustreznih dokumentih (več o vlogah v računalniških centrih skupine HSE v poglavju 6.4).
  - Zaradi povišane stopnje varovanja in zajemanja biometrijskih podatkov (dvostopenjska avtentifikacija) se ustrezni postopki uskladijo z informacijskim pooblaščencem, pri čemer se z omenjenim zajemom obvesti reprezentančni sindikat.
  - Pristojni za informacijsko varnost se redno udeležujejo slovenskih srečanj na temo kibernetske varnosti.
- A.12 Varnost operacij – računalniški centri so kompleksen zbir različnih tehnologij – zanje je treba zapisati jasna navodila, zabeležiti postopke postavitve in zagona ter striktno beležiti vse spremembe in aktivnosti.
  - Vsi postopki sprememb se beležijo, vključno s:
    - postopki namestitve in konfiguracije,
    - izvedbo varnostnega kopiranja (še posebno sistemov za nadzor infrastrukture),
    - zahtevami po obdobnem testiranju in vzdrževanju opreme,
    - kontaktnimi podatki skrbnikov in vzdrževalcev,
    - postopki za ponoven zagon sistemov …
  - Postopki preverjanj operativnih sistemov se skrbno načrtujejo, zanje so izdelani tudi rezervni scenariji.
  - A.13 Varnost komunikacije – v računalniških centrih varujemo dva tipa komunikacij: dohodne komunikacije (v obliki optičnih vodov) in komunikacije znotraj samega računalniškega centra. Oboje zahteva svojo zaščito in ustrezne ukrepe za večjo varnost.
    - Do računalniških centrov skupine HSE po komunikacijskih poteh dostopa več ponudnikov internetnih storitev.
- A.18 Skladnost – delovanje računalniških centrov je v veliki meri podvrženo določeni nacionalni in evropski zakonodaji, raznim pravilom in zaščiti.
  - Vzpostaviti velja sistem, po katerem se redno spremlja zakonodaja – dovolj je, da se spremlja Uradni list Republike Slovenije, kjer se zakonodaja,

povezana z delovanjem računalniških centrov, ustrezno zabeleži in pošlje v obravnavo ustreznim skrbnikom.
    - Preverjati je treba pravice intelektualne lastnine, licenc in dokazov o lastništvu, na sistemih oskrbe infrastrukture in nadzornih sistemov.
    - Zagotoviti je treba sistem hranjenja ključnih informacij (navodil, pravilnikov, merilnih protokolov …).
    - V skladu z ustrezno zakonodajo (ZVOP-1 in GDPR) je treba zapisati ustrezno pravilo oz. politiko, ki ščiti osebno določljive podatke organizacije. Še posebno se je treba opredeliti do biometrijsko zajetih podatkov.
    - Kriptografske metode (določenih dokumentov, prometa DCIM …) se uporabljajo v skladu z zakonodajo.
    - Postopki izvajanja in upravljanja informacijske varnosti v računalniških centrih skupine HSE se izvajajo v skladu s politikami družb skupine HSE in se izvajajo v načrtovanih časovnih presledkih (vsako leto).
    - Za skladnost z varnostnimi politikami in certificiranim sistemom skrbi skrbnik računalniških centrov.
    - Tehnična skladnost vseh komponent in oskrbne infrastrukture se redno preverja in primerja z že znanimi postopki in rezultati.
- ***Varnost osebja***

Tabela 7: Kontrole varnosti osebja

Zap. št.	Št. kontrole	Kontrola
1.	7.1.1	Preverjanje
2.	7.1.2	Določila in pogoji za zaposlitev
3.	7.2.1	Odgovornost vodstva
4.	7.2.2	Ozaveščenost, izobraževanje in usposabljanje glede informacijske varnosti
5.	7.2.3	Disciplinski proces
6.	7.3.1	Prekinitev ali sprememba zaposlitvenih odgovornosti
7.	9.2.1	Registracija in izbris registracije uporabnika
8.	9.2.2	Zagotavljanje dostopa uporabnikom
9.	9.2.3	Upravljanje posebnih pravic dostopa
10.	9.2.4	Upravljanje tajnih informacij uporabnikov za preverjanje verodostojnosti
11.	9.2.5	Pregled uporabniških pravic dostopa
12.	9.2.6	Preklic ali prilagoditev pravic dostopa
13.	9.3.1	Uporaba tajnih informacij za preverjanje verodostojnosti

Vir: prirejeno po SIST (2013).

- A.7 Varnost človeških virov (tabela 7) – ljudje so pri upravljanju in vzdrževanju sistemov in naprav znotraj računalniških centrov ključni za zagotavljanje informacijske varnosti. Zanje je treba izdelati formalne postopke.
    - Pred zaposlitvijo je treba varnostno preveriti kandidata, da bi se preprečila morebitna zaposlitev kriminalca.
    - Vzpostavljena ekipa mora imeti strokovno znanje in sposobnost ravnanja z informacijami v računalniških centrih. Vloge in odgovornosti morajo biti jasno opredeljene.

    - Ekipa računalniškega centra mora razpolagati z verodostojnimi podatki ter redno posodabljati varnostne politike in procedure. Usposabljanje in izobraževanje mora biti del razvoja ozaveščenosti informacijske varnosti.
    - Postopki za podeljevanje in odvzemanje pravic ter informacijskih sredstev novozaposlenih ali odpuščenih morajo biti jasno opredeljeni in zapisani.
- A.9 Nadzor dostopa – kot del kritične infrastrukture je treba poskrbeti, da so dostopi do informacij v sklopu računalniških centrov skupine HSE v celoti pod ustreznim nadzorom in da se z njimi ravna zelo skrbno oziroma v skladu z zapisanimi politikami.
    - Skrbnik računalniških centrov skupine HSE poskrbi za varnostne zahteve aktualnih aplikacij, ki temeljijo na poslovnih zahtevah, in zanje pripravi ustrezne nadzorne mehanizme. Poskrbi za ločevanje vlog, od katerih so odvisni dostopi.
    - Opredeliti se je treba do računalniških omrežij znotraj računalniških centrov (brezžična omrežja so prepovedana).
    - Dostopi se v rednih časovnih presledkih preverjajo in po potrebi nadgrajujejo, zanje se izdela formalni postopek.
    - Zagotovljen je postopek za preklic in prilagoditev pravic dostopa, pri čemer se sodeluje s službo za človeške vire.
- ***Zunanji partnerji (tabela 8)***

Tabela 8: Tabela, namenjena kontrolam zunanjih partnerjev

Zap. št.	Št. kontrole	Kontrola
1.	11.2.6	Varnost opreme in dobrin zunaj prostorov organizacije
2.	15.1.1	Informacijska varnostna politika za odnose z dobavitelji
3.	15.1.2	Obravnava varnosti v dogovorih z dobavitelji
4.	15.1.3	Dobavna veriga informacijske in komunikacijske tehnologije
5.	15.2.1	Spremljanje in pregledovanje storitev dobaviteljev
6.	15.2.2	Upravljanje sprememb storitev dobaviteljev

Vir: prirejeno po SIST (2013).

- A.11 Fizična in okoljska varnost – za opremo, ki se odstrani z lokacije računalniškega centra, je treba zagotoviti varnost.
    - Oddaljeni dostopi do informacijske infrastrukture so za zunanje partnerje onemogočeni.
    - Vsa oprema, ki se vzdržuje pri zunanjih izvajalcih, k njim potuje brez informacij (brisanje diskov …).
    - Oprema, ki se odnese iz prostorov računalniških centrov, nikoli ni brez nadzora.
- A.15 Odnosi z dobavitelji – vsak zaposleni, ki dostopa do sredstev računalniškega centra, mora podpisati pogodbo o nerazkrivanju (ang. NDA, non-disclosure agreement) in biti seznanjen s politiko varovanja informacij.
    - Zunanji partnerji so z varovanjem informacij in strožjim dostopom do informacijskih sredstev v računalniških centrih skupine HSE seznanjeni že v času podpisovanja pogodbe (o sodelovanju, naročilu …).
    - Morebitni incidenti se obravnavajo v skladu s politiko krovne družbe.

- Pri zagotavljanju varnosti mora dobavitelj/izvajalec zagotoviti seznanjenost in upoštevanje politik varovanja v celotni dobavni verigi.
- Skrbniki so zadolženi za skrbno preverjanje postopkov izvedbe in dostopov zunanjih partnerjev in hkrati v sistem za spremljanje dogodkov vpisujejo vse relevantne spremembe.

- ***Dobrine (tabela 9)***

Tabela 9: Kontrole za upravljanje dobrin

Zap. št.	Št. kontrole	Kontrola
1.	8.1.1	Popis dobrin
2.	8.1.2	Lastništvo nad dobrinami
3.	8.1.3	Sprejemljiva uporaba dobrin
4.	8.1.4	Vračilo dobrin
5.	8.2.1	Razvrstitev informacij
6.	8.2.2	Označevanje informacij
7.	8.2.3	Ravnanje z dobrinami
8.	8.3.1	Upravljanje izmenljivih nosilcev podatkov/informacij
9.	8.3.2	Odstranjevanje nosilcev podatkov/informacij
10.	8.3.3	Prenos fizičnih nosilcev podatkov/informacij
11.	11.2.5	Odstranitev dobrin
12.	11.2.7	Varna odstranitev in ponovna uporaba opreme

Vir: prirejeno po SIST (2013).

- A.8 Upravljanje dobrin – z ustrezno politiko se skrbnik zavezuje k zaščiti organizacijskih dobrin in določi ustrezno odgovornost na področju zaščite.
  - Dobrine, povezane z informacijami v računalniških centrih, se prepoznavajo pri izdelavi ocene tveganj. Zanje poskrbijo skrbniki posameznih sistemov in skrbnik računalniškega centra. Popisi morajo biti ažurni, natančni, konsistentni in usklajeni z drugimi predpisi.
  - Lastništvo je znano in natančno opisano v dokumentu Lastniki informacijskih sredstev v RC skupine HSE.
  - Za odstranitev dobrin obstajajo jasna navodila v osnovni varnostni politiki in veljajo enako kot za vsa druga informacijska sredstva v informacijskem sistemu skupine HSE.
- A.11.2.5 Odstranitev dobrin – za vse dobrine, ki so del kritične in oskrbne infrastrukture, je treba izdelati formalne postopke odstranitve. Kritični elementi so nosilci podatkov (strežniški in SAN-diski, elektronski pomnilniki, mediji varnostnega kopiranja …).
  - Odstranitev dobrin in ustrezno ravnanje odobri skrbnik računalniških centrov. Uničenje izvršujejo za to pooblaščena podjetja – za uničenje se izda ustrezno poročilo.
  - Nosilce informacij iz računalniških centrov se zunaj prostorov družb ne sme uporabljati.

3.3.2 Upravljanje infrastrukture

Za delovanje računalniškega centra je oskrbna infrastruktura, pri čemer imamo v mislih napajanje, hlajenje in zagotavljanje komunikacij, ob predpostavki celovite varnosti, ključnega pomena.

- ***Energija/hlajenje (tabela 10)***

Tabela 10: Kontrole upravljanja energije in hlajenja

Zap. št.	Št. kontrole	Kontrola
1.	11.2.2	Podporna oskrba

Vir: prirejeno po SIST (2013).

- A.11 Fizična in okoljska varnost – oprema, ki zagotavlja podporno oskrbo računalniških centrov (napajanje, hlajenje, gašenje …), mora biti skrbno načrtovana in vzdrževana.
    - Pri načrtovanju je treba poskrbeti, da je oprema nameščena tako, da dostop do nje ni mogoč brez ustrezne avtorizacije.
    - Vsa kritična napajalna infrastruktura je izvedena v skladu z omenjeno standardizacijo EN50600-2-2.
    - Oprema se redno preverja in testira (glej poglavje 3.8.2 Primarna infrastruktura in izvajanje testiranj), za kar se vodijo ustrezni dnevniki ali zapisi.
    - Posebna skrb se nameni upravljanju goriva – redno se preverja količina in stanje goriva. Poskrbeti je treba tudi za sistem dobave goriva v času delovanja dizelskega agregata.
    - Z zunanjimi izvajalci se sklenejo ustrezne SLA-pogodbe, upoštevajoč zahteve po informacijski varnosti.
- ***Omrežje (tabela 11)***

Tabela 11: Kontrole varovanja omrežja

Zap. št.	Št. kontrole	Kontrola
1.	11.2.3	Varnost ožičenja
2.	13.1.1	Omrežne kontrole
3.	13.1.2	Varovanje omrežnih storitev
4.	13.1.3	Ločevanje v omrežjih
5.	14.1.2	Varovanje aplikacijskih storitev v javnih omrežjih

Vir: prirejeno po SIST (2013).

- A.11.2.3 Varnost ožičenja – pomembno je zagotoviti ustrezno zaščiteno traso za komunikacijske in energetske povezave – oboje se med seboj ločujejo. Trase morajo biti ustrezno varovane.

- A.13 Varnost komunikacije – zagotoviti je treba visoko stopnjo zaščite vseh komunikacijskih protokolov in povezav. Zanje je treba izdelati ločeno varnostno politiko.
    - Jasno se opredelijo odgovornosti za upravljanje in vzdrževanje omrežnih naprav. Zanje se vodi natančna dokumentacija.
    - Redno se spremljajo datoteke .log na nivoju operacijskih sistemov in aplikacij.
    - Omrežja se med seboj ločujejo glede na funkcionalnost in storitve.
- A.14.1.2 V primeru, da se aplikacijske storitve računalniških centrov skupine HSE prenašajo v javna omrežja, je zanje treba pripraviti ustrezne varnostne mehanizme (SSH ali protokol šifriranega prenosa, kriptiranje, VPN – navidezno zasebno omrežje …).

- ***IT-storitve (tabela 12)***

Tabela 12: Kontrole informacijskih storitev

Zap. št.	Št. kontrole	Kontrola
1.	6.2.1	Politika na področju mobilnih naprav
2.	6.2.2	Delo na daljavo
3.	9.1.1	Politika nadzora dostopa
4.	9.1.2	Dostop do omrežij in omrežnih storitev
5.	9.4.1	Omejitev dostopa do informacij
6.	9.4.2	Varni postopki prijave
7.	9.4.3	Sistem upravljanja gesel
8.	9.4.4	Uporaba posebnih pomožnih programov
9.	9.4.5	Nadzor dostopa do programske izvorne kode
10.	10.1.1	Politika uporabe kriptografskih kontrol
11.	10.1.2	Upravljanje ključev
12.	11.2.8	Nenadzorovana uporabniška oprema
13.	11.2.9	Politika čiste mize in praznega zaslona
14.	12.2.1	Kontrole proti zlonamerni programski opremi
15.	12.3.1	Varnostno kopiranje informacij
16.	12.4.2	Zaščita zabeleženih informacij
17.	12.4.3	Beleženje aktivnosti administratorjev in operaterjev
18.	12.4.4	Uskladitev ur
19.	12.5.1	Namestitev programske opreme na operativne sisteme
20.	12.6.2	Omejitve pri namestitvi programske opreme
21.	13.2.3	Elektronsko sporočanje
22.	14.1.3	Zaščita transakcij aplikacijskih storitev

Vir: prirejeno po SIST (2013).

- A.6 Organiziranje informacijske varnosti – zaradi velikega tveganja mobilnih aplikacij in naprav ter dela na daljavo je potrebna za tovrstne storitve še posebna previdnost.
    - Mobilne naprave se ne uporabljajo v varnih celicah, mobilni moduli za SMS-javljanja so podvrženi tedenskemu preverjanju.
    - Pri delu na daljavo se omogoča dostop samo iz lokalnega omrežja skupine HSE. Za morebitne posege zunanjih partnerjev se omogoča časovno omejen in enkraten dostop.

    - Pri napravah nadzora in njihovih operacijskih sistemih se izklapljajo daljinski dostopi.
- A.9 Nadzor dostopa – do vseh naprav oskrbne infrastrukture in sistemov za nadzor je treba dostopati po vnaprej znanih in zabeleženih protokolih.
    - Politika dostopa do informacijskih sredstev računalniških centrov HSE je zapisana v krovni politiki varovanja informacij.
    - Tudi vsa pravila krovne varnostne politike veljajo v prostorih računalniških centrov in povezavah do njih.
- A.10 Kriptografija – v večini primerov se izvaja na komunikacijskih poteh do informacijskih virov.

3.3.3 Izvajanje varovanja

Za varnost računalniških centrov in celotne oskrbne infrastrukture je pomembno področje, kjer se, predvsem v fazi izgradnje in načrtovanja, pripravijo in izvedejo ustrezni ukrepi za zaščito pred zunanjimi in okoljskimi grožnjami.

- ***Okolje (tabela 13)***

Tabela 13: Kontrole za upravljanje okolja

Zap. št.	Št. kontrole	Kontrola
1.	11.1.4	Zaščita pred zunanjimi in okoljskimi grožnjami

Vir: prirejeno po SIST (2013).

- A.11.1.4 Zaščita pred zunanjimi in okoljskimi grožnjami – kjer se z ustreznimi fizičnimi in tehničnimi ukrepi prepreči možnost naravnih nesreč, namernih poškodb, eksplozij, požarov …
    - Dela na varovanem območju se izvajajo samo po potrebi in v skrajni sili.
    - Stanje se pregleduje in redno spremlja.
    - Nepooblaščeno fotografiranje in snemanje nista dovoljena.
- ***Vandalizem/vlom (tabela 14)***

Tabela 14: Kontrole, namenjene vandalizmu in vlomu

Zap. št.	Št. kontrole	Kontrola
1.	11.1.1	Varovanje fizičnih meja območja
2.	11.1.2	Kontrole fizičnega vstopa
3.	11.1.3	Varovanje pisarn, sob in naprav
4.	11.1.5	Delo na varovanih območjih
5.	11.1.6	Dostavne in nakladalne površine
6.	11.2.1	Namestitev in zaščita opreme

Vir: prirejeno po SIST (2013).

- A.11 Fizična in okoljska varnost – zelo pomemben segment kontrol pri zagotavljanju popolne varnosti računalniških centrov skupine HSE.
    - Vzpostaviti je treba varnostne cone in jih fizično in logično zaščititi. Dostopi se omogočajo samo pooblaščenim osebam, za vse druge obstajajo strogi pravilniki, ki jih izvajajo vsi, ki imajo dostop do računalniških centrov.
    - Vsi pristopi so kontrolirani, na vhodih v računalniške centre se izvaja dvostopenjska kontrola, za kontrolo dostopa je treba poskrbeti tudi na nivoju strežniških in komunikacijskih omar.
    - Vzpostavljeni so videonadzorni sistemi, ponavadi povezani v celovit sistem tehničnega varovanja družbe.

3.3.4 Spremljanje in nadzor

Pomembno sredstvo za obvladovanje varnostnih mehanizmov in delovanja storitev v računalniških centrih skupine HSE so sistemi za spremljanje in nadzor.

- ***Analize (kontrole iz tabele 15)***

Tabela 15: Kontrole za analizo

Zap. št.	Št. kontrole	Kontrola
1.	12.1.3	Upravljanje zmogljivosti
2.	14.1.1	Analiza in specifikacije informacijskih varnostnih zahtev

Vir: prirejeno po SIST (2013).

- A.12.1.3 Upravljanje zmogljivosti – pomembna dejavnost v računalniških centrih skupine HSE. Za ponujanje storitev RC je treba redno preverjati zmogljivosti in hkrati skrbno načrtovati porabo virov. Vse spremembe in zahteve se vodijo v sistemu za nadzor in upravljanje.
- A.14.1.1 Analiza in specifikacije informacijskih varnostnih zahtev – vse varnostne zahteve se spremljajo enotno in se obdelujejo na rednih tedenskih usklajevanjih skrbnika RC in preostalih skrbnikov oz. vzdrževalcev.

- ***Vzdrževanje (kontrole iz tabele 16)***

Tabela 16: Kontrole pri izvajanju vzdrževanja

Zap. št.	Št. kontrole	Kontrola
1.	11.2.4	Vzdrževanje opreme
2.	12.1.4	Ločevanje razvojnih, testnih in obratovalnih naprav

Vir: prirejeno po SIST (2013).

- A.11.2.4 Vzdrževanje opreme – za popolno razpoložljivost in celovitost opreme računalniških centrov skupine HSE in celotne oskrbne infrastrukture so zapisani napotki za izvajanje vzdrževanja, kjer se še posebno poskrbi, da vsa dela izvaja za to usposobljeno in pooblaščeno osebje. Za vzdrževanje se vodi terminski koledar, redno se izvajajo testiranja, za katera se izdelajo ustrezni merilni protokoli.
- A.12.1.4 Ločevanje razvojnih, testnih in obratovalnih naprav – pred vključitvijo naprav v računalniški center skupine HSE se izvede ločeno testiranje opreme, najprej samostojno, šele v zaključni fazi priključeno v računalniški center.
- ***Upravljanje incidentov (kontrole iz tabele 17)***

Tabela 17: Kontrole za upravljanje incidentov

Zap. št.	Št. kontrole	Kontrola
1.	12.4.1	Beleženje dogodkov
2.	12.6.1	Upravljanje tehničnih ranljivosti
3.	16.1.1	Odgovornosti in postopki
4.	16.1.2	Poročanje o informacijskih varnostnih dogodkih
5.	16.1.3	Poročanje o informacijskih varnostnih slabostih
6.	16.1.4	Ocena informacijskih varnostnih dogodkov in odločitev o njih
7.	16.1.5	Odgovor na informacijske varnostne incidente
8.	16.1.6	Učenje iz informacijskih varnostnih incidentov
9.	16.1.7	Zbiranje dokazov

Vir: prirejeno po SIST (2013).

- A.12 Varnost operacij – s čimer zagotavljamo spremljanje različnih vrst dogodkov.
    - Dnevniki dogodkov se redno pregledujejo, služijo nam kot podlaga za obdelavo varnostnih incidentov in mnogih vzdrževanj. Dnevniki se zbirajo na centralnem mestu (DCIM) razen strežniških dnevnikov, kjer se shranjujejo na korporativnem strežniku Microsoft SCOM.
- A.16 Upravljanje informacijskih varnostnih incidentov – uporabljamo postopke iz korporativnega upravljanja informacijske varnosti, pri čemer za zbiranje dokazov skrbi osebje računalniškega centra skupine HSE oz. sam skrbnik.
- ***Neprekinjeno poslovanje (kontrole iz tabele 18)***

Tabela 18: Kontrole za podporo neprekinjenemu poslovanju

Zap. št.	Št. kontrole	Kontrola
1.	17.1.1	Načrtovanje neprekinjene informacijske varnosti
2.	17.1.2	Izvajanje neprekinjene informacijske varnosti
3.	17.1.3	Preverjanje, pregledovanje in vrednotenje neprekinjene informacijske varnosti
4.	17.2.1	Razpoložljivost naprav za obdelavo informacij

Vir: prirejeno po SIST (2013).

- A.17 Vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja – sama konfiguracija dveh računalniških centrov nam omogoča, da se ob podpori

komunikacijske infrastrukture, strežniških aplikacij virtualnih okolij in repliciranih SAN-polj rešitev neprekinjene informacijske varnosti ponuja sama po sebi.

- Zapisani so okrevalni načrti po zagotavljanju neprekinjenega delovanja računalniških centrov skupine HSE.
- Testiranje delovanja postopkov je opredeljeno v okrevalnih načrtih.
- Redno se preverja razpoložljivost naprav za replikacijo in sisteme za neprekinjeno poslovanje.

3.4 Metodologija ocenjevanja tveganj v računalniških centrih skupine HSE

Za potrebe ocenjevanja tveganj pri upravljanju v računalniških centrih skupine HSE se je izdelala metodologija za izdelavo ocene tveganj. V pomoč pri izračunu ocene tveganja smo izdelali matriko, in sicer iz:

- Ocene zaupnosti in celovitosti, kjer ocenjujemo, kakšno škodo bi imela skupina (družba) v primeru izgube zaupnosti in celovitosti.

  Verjetnost uresničitve grožnje:
  - 1 – zelo nizka: zelo nizka verjetnost oz. pogostost uresničitve grožnje. Tovrstni dogodki se v okolju delovanja družbe (Slovenija) dogajajo enkrat na desetletje ali redkeje. V družbi takšnega dogodka še nismo imeli ali pa je od zadnjega preteklo že več kot 10 let.
  - 2 – nizka: nizka verjetnost oz. pogostost uresničitve grožnje. Tovrstni dogodki se v okolju delovanja družbe (Slovenija) dogajajo na vsakih nekaj let. V družbi smo v preteklih 10 letih imeli največ dva takšna dogodka.
  - 3 – srednja: srednja verjetnost oz. pogostost uresničitve grožnje. Tovrstni dogodki se v okolju delovanja družbe (Slovenija) dogajajo praktično vsako leto. V družbi smo v preteklih 10 letih imeli takšne dogodke.
  - 4 – visoka: visoka verjetnost oz. pogostost uresničitve grožnje. Tovrstni dogodki se v okolju delovanja družbe (Slovenija) stalno dogajajo. V družbi smo v zadnjem letu imeli takšne dogodke.
  - 5 – zelo visoka: zelo visoka verjetnost oz. pogostost uresničitve grožnje. Tovrstni dogodki se v družbi pogosto dogajajo. V zadnjem letu smo imeli vsaj 5 takšnih dogodkov.

  Zaupnost in celovitost:
  - 1 – nepomembna,
  - 2 – zelo malo pomembna (do 10.000,00 EUR[1]),
  - 3 – malo pomembna (od 10.000,00 EUR do 100.000,00 EUR),
  - 4 – pomembna (od 100.000,00 EUR do 1.000.000,00 EUR),

[1] Izguba zaupnosti ali celovitosti povzroči škodo (poslovno, materialno, moralno …) v zapisani višini EUR.

- 5 – zelo pomembna (od 1.000.000,00 EUR do 10.000.000,00 EUR),
- 6 – bistvena (nad 10.000.000,00 EUR).

- Ocene razpoložljivosti, kjer preverjamo, kakšna bi bila škoda, če informacijsko sredstvo, ko ga potrebujemo, ne bi bilo dostopno v nekem časovnem obdobju. Končno oceno ocenitve razpoložljivosti dobimo glede na največjo ugotovljeno oceno:
  - 1 – nepomembna,
  - 2 – zelo malo pomembna (do 10.000,00 EUR),
  - 3 – malo pomembna (od 10.000,00 EUR do 100.000,00 EUR),
  - 4 – pomembna (od 100.000,00 EUR do 1.000.000,00 EUR),
  - 5 – zelo pomembna (od 1.000.000,00 EUR do 10.000.000,00 EUR),
  - 6 – bistvena (nad 10.000.000,00 EUR).

Slika 23: Matrika razpoložljivosti

Čas nerazpoložljivosti	Grožnja poslovnemu preživetju	Zelo velika škoda	Velika škoda	Srednja škoda	Manjša škoda	Brez vpliva
Ena ura	4	3	3	2	1	1
En dan	5	4	3	3	2	1
En teden	6	5	4	3	3	1
En mesec	6	6	4	4	3	1

Vir: lastno delo.

Slika 24: Matrika ocene tveganja

		Verjetnost uresničitve grožnje				
		Zelo nizka	Nizka	Srednja	Visoka	Zelo visoka
		1	2	3	4	5
Nepomembna	1	1	2	3	4	5
Zelo malo pomembna	2	2	3	4	5	6
Malo pomembna	3	3	4	5	6	7
Pomembna	4	4	5	6	7	8
Zelo pomembna	5	5	6	7	8	9
Bistvena	6	6	7	8	9	10

Vir: lastno delo.

Za vsako informacijsko sredstvo, ki ga ocenjuje kvalificiran presojevalec ob pomoči lastnika ali skrbnika sredstva, je treba opisati grožnje, ki lahko vplivajo nanj. Kot pomoč pri pripravi groženj služi seznam groženj, ki so v celoti prilagojene sredstvom v računalniških centrih.

Tabela 19: Tabela groženj

Zap. št.	Grožnja	Zap. št.	Grožnja
1.	Odpoved hlajenja/gretja	19.	Terorizem
2.	Odpoved napajanja	20.	Napaka pri vzdrževanju
3.	Vlom (neavtoriziran dostop)	21.	Nepopolna dokumentacija
4.	Poplava	22.	Katastrofa (eksplozija, potres, nameren požig …)
5.	Požar/dim	23.	Napaka na sistemski ali mrežni programski opremi
6.	Človeška napaka	24.	Napaka na aplikacijski programski opremi
7.	Napaka pri komunikaciji	25.	Napaka na sistemih rezervnega napajanja (dizelski agregat, baterije …)
8.	Dostop s prekrito identiteto s strani pogodbenih izvajalcev	26.	Nepravilno načrtovanje o sredstvih (dizelsko gorivo, ljudje, voda …)
9.	Dostop s prekrito identiteto s strani zaposlenih	27.	Napaka uporabnika
10.	Kraja	28.	Napaka pri vzdrževanju
11.	Namerna škoda s strani zaposlenih	29.	Pomanjkanje osebja
12.	Vnos škodljive kode	30.	Goljufija
13.	Tehnična napaka na orodjih za upravljanje	31.	Nedovoljeno posredovanje informacij
14.	Kršitev notranjih pravil	32.	Nepopolni načrti ob prekinitvah delovnega procesa
15.	Slabo vodenje	33.	Nepopolni postopki za ukrepe v izrednih razmerah
16.	Kršitev zakonodaje	34.	Prekinitev poslovnih aktivnosti
17.	Stavka		
18.	Sabotaža		

Vir: lastno delo.

Pri izdelavi ocene tveganj je rezultate treba ustrezno analizirati in pripraviti v obliki poročila, ki ga podpišejo vsi sodelujoči v procesu izdelave ocene tveganj. Sprejemljiv nivo tveganj (s poslovnega vidika) določi uprava družbe. Za vsa informacijska sredstva, pri katerih je ocena tveganja nad sprejemljivim nivojem tveganja, je treba poiskati vzroke za nastanek tveganja in jih z ukrepi zmanjšati na sprejemljiv nivo.

3.5 Izjava o primernosti SOA (ang. Statement of Applicability)

Opredeljena sredstva iz nabora sredstev v sklopu računalniških centrov, ki lahko predstavljajo informacijska tveganja in so v obsegu varovanja informacij, se skozi intervjuje s skrbniki popišejo. Popis dejanskega stanja se izvede skozi analizo vrzeli, opisani z metodologijo iz predhodnega poglavja. Izhodni dokument je izjava o primernosti oziroma po ang. statement of applicability (v nadaljevanju SOA). V dokumentu so navedene vse kontrolne točke iz priloge A-standarda ISO/IEC 27001:2013 in razlage, kje se ukrepi nahajajo.

3.6 Podeljene vloge, naloge in odgovornosti

Pri izvajanju procesa upravljanja računalniških centrov skupine HSE sodelujejo različni profili poslovnih uporabnikov ali izvajalcev, vsak od njih pa ima prav posebno vlogo, s čimer so povezane odgovornosti in naloge, ki jih dotični opravlja. Nekatere vloge so osebne, druge grupirane.

a) Poslovni lastnik računalniškega centra – zagotavlja vire za delovanje računalniškega centra, sodeluje pri izdelavi strategije razvoja in potrjuje načrt neprekinjenega poslovanja (direktor tehničnega področja, direktor informatike, poslovni direktor).
b) Skrbnik storitve računalniškega centra – skrbi za storitve, ki jih zagotavlja računalniški center, koordinira vsa vzdrževanja, skrbi za pogodbe z zunanjimi izvajalci, načrtuje izobraževanja in sodeluje pri izdelavi analiz. Usklajuje in odobrava zahtevke po novih kapacitetah ter usklajuje aktivnosti pri izvajanju načrta neprekinjenega poslovanja (vodja informatike, vodja SUVI, direktor informatike).
c) Varnostni oficir – pripravlja varnostni načrt, ga usklajuje s strategijo podjetja, sodeluje z zunanjimi izvajalci tehničnega in fizičnega varovanja, je član tima, ki obravnava varnostne incidente. Je član širše ekipe korporativnega varovanja in organizacijsko ne spada v informatiko.
d) Skrbniki:
    - IKT – zadolžen za informacijske in komunikacijske storitve (postavitev računalniške strežniške opreme, priklapljanje komunikacijskih povezav, nameščanje sistemov za upravljanje računalniških centrov …),
    - elektro – zadolžen za skrbno načrtovanje, izvajanje in upravljanje kompleksnega sistema napajanja, vključno z baterijskimi sistemi in dizelskim agregatom; prisoten pri mesečni testnih zagonih in manipulacijah,
    - strojni – zadolžen za skrbno načrtovanje, izvajanje in upravljanje sistema hlajenja, gretja in razvlaževanja vseh prostorov računalniškega centra; seznanjen je z mesečnimi testiranji strojne oskrbne infrastrukture,
    - gradbeni – zadolžen za skrbno načrtovanje, izvajanje in upravljanje stavb, prostorov in okolic računalniških centrov.
e) Vzdrževalci:
    - elektro – zadolžen za vzdrževanje elektrooskrbne infrastrukture. S skrbnikom sodeluje pri načrtovanju aktivnosti manipulacij, beleži stanja opreme in sodeluje pri mesečnih testiranjih. Upravlja in vzdržuje sisteme UPS, STS, dizelski agregat in baterijske sisteme, pri čemer sodeluje tudi z zunanjimi izvajalci. Skrbi za vnašanje sprememb v tehnično dokumentacijo in skrbno beleži potrebo po novih virih,
    - strojni – zadolžen za neprekinjeno delo strojnih inštalacij, kamor spadajo hladilni agregati, sistemi za prezračevanje in razvlaževanje, črpalke in dovodi vode. Skrbi za pravilno mehansko delovanje dizelskega agregata in sistemov za pravilno prezračevanje prostorov, kjer se nahaja,

- gradbeni – zadolžen za vzdrževanje gradbenih elementov računalniških centrov. Preverja podatke gradbene statike in predlaga ukrepe, povezane z upravljanjem stavbe,
- čiščenje – skrbijo za redno čiste prostore v računalniških centrih. Naloge izvajajo po terminskih načrtih, usklajeni so s skrbnikom storitve računalniškega centra. Dostop do prostorov jim zagotavlja eden izmed imenovanih vzdrževalcev.

f) Zunanji izvajalci – usklajujejo izvajanje vzdrževalnih del s skrbnikom in vzdrževalci za posamezna področja. Podvrženi so varnostnemu preverjanju in ves čas dela tudi spremljani s strani vzdrževalcev, zadolženih za posamezne sklope. Dela izvajajo izključno s predhodno potrjeno pogodbo in dokumentacijo. Podpišejo izjavo o zaupnosti.
g) Uporabniki – dostop do računalniških centrov jim je omogočen samo v redkih primerih – usklajeni so s skrbnikom in poslovnim lastnikom.
h) Obiskovalci – podobno kot uporabniki imajo samo redki možnost dostopati do računalniških centrov. Zanje velja poseben sistem dostopa (predhodna odobritev na osnovi izkazanega interesa – s strani poslovnega lastnika), preverjanje pri varnostni službi, identifikacija in spremstvo pooblaščenih oseb.

3.7 Izvedba testiranj oskrbne infrastrukture

Ena od ključnih varnostnih zahtev pri ponujanju storitev računalniških centrov skupine HSE je stalno zagotavljanje delovanja celotne oskrbne infrastrukture. Za preverjanje delovanja smo izdelali nabor testiranj, ki se izvajajo v točno določenih časovnih intervalih. Namen vseh obremenilnih testiranj je preveritev pravilnosti delovanja oskrbne infrastrukture, odpornost proti izpadom in doseganje predvidenih končnih obremenitev. Postopek obremenilnega testiranja je vnaprej določen in predvideva testiranje delovanja oskrbne infrastrukture pod realnim ali simuliranim bremenom. Pri tem spremljamo ključne podatke sprejemljivosti, ki nam povedo, ali računalniški center in v njem nameščena IT-oprema še vedno delujeta v normalnih pogojih. Prav tako spremljamo druge merjene podatke in sistem zaznavanja ter sporočanja stanja delovanja in morebitnih napak. Slednje se izkaže nadvse pomembno v primeru resničnega nastopa izrednih razmer zaradi napak ali odpovedi posameznih sistemov. Natančno, pravilno in hitro javljanje napake nam predstavlja možnost za pravočasno odpravo napak in s tem zmanjšuje verjetnost odpovedi celotnega centra.

V polno funkcionalnih in živečih centrih so obremenilni testi še posebno zahtevni, saj potekajo ob nameščeni in delujoči opremi. Zato je pravilno in natančno izvajanje testnih procedur vitalnega pomena. Pred začetkom testiranj je treba določiti naslednja izhodišča:

- določiti merilne točke v sistemu oskrbne infrastrukture,
- izvesti inicialne merilne procedure za določitev začetnega stanja,
- doreči postopek prekinitve testiranj v primeru izrednih dogodkov.

Glavna naloga oskrbne infrastrukture v računalniških centrih je zagotavljanje delovnih pogojev za delovanje IKT-opreme. Med delovne pogoje spadajo predvsem:

- temperatura in vlaga na zajemu naprav, ki morata biti znotraj specifikacij proizvajalca oziroma skladna z ASHRAE TC 9.9 (ASHRAE Technical Committee 9.9, 2012),
- električna napetost v skladu z ITIC-diagramom oziroma specifikacijami (ITIC, 2017),
- varnost s stališča izlivov tekočin, požara in podobnih dogodkov, ki lahko ogrozijo delovanje IKT-opreme.

Zato je treba pri postopkih testiranja spremljati navedene parametre. Postopki testiranja morajo biti izvedeni tako, da delovanje IKT-naprav ni nikoli ogroženo, in sicer:

- temperatura na zajemu naprav ne sme prekoračiti mejne temperature 25 °C,
- električna napetost mora biti ves čas razpoložljiva, sočasno lahko odpove le en napajalni sistem,
- v računalniškem centru mora biti med testiranjem ves čas prisotno osebje, ki nadzoruje delovanje vseh pomožnih sistemov.

3.7.1.1 Vrste testiranj v računalniških centrih

Pri obremenilnih testih se srečujemo z različnimi merilnimi protokoli in postopki, ki imajo različne namene. Glavni del so obremenilni testi, pri katerih testiramo delovanje sistemov med obremenitvijo. Preden pa lahko začnemo opravljati obremenilne teste, moramo preveriti delovanje sistemov alarmiranja ter obveščanja in delovanja merilnih sistemov. Sestavni del obremenilnih testov je tudi preverba delovanja signalizacije napak na posameznih ključnih sistemih, kar lahko opravimo med izvajanjem obremenilnih testov ali pa tudi samo s preverjanjem izvedbene dokumentacije.

a) Predhodni testi

Predhodni testi so potrebni za zagotovitev delovanja sporočanja izrednih situacij – alarmiranja. Sem sodijo:

- preverba nastavitev alarmiranja,
- testiranje delovanja alarmiranja za ključne sisteme in podatke.

Predhodni testi se izvedejo pred začetkom kakršnihkoli drugih testov. Pomembni so zato, ker s pomočjo merilnih točk in alarmiranja sprejmemo informacijo o kakršnemkoli izpadu ali tveganju za delovanje IKT-opreme. Predhodni testi se izvajajo za:

- testiranje alarmiranja po napravah, prikazan v tabeli 20 – primer zapisanih parametrov in vsebina tovrstnega testiranja:

Tabela 20: Testiranje alarmiranja na napravah[2]

Parameter	Vsebina
Območje testiranja	Omejeno testiranje – samo na posamezni napravi
Ciljne naprave/sistemi	Krmilnik DEA, UPS-sistemi, STS-sistemi, hladilne omare, hladilni agregati
Spremljajoči pomožni testi	/
Namen testa	Preveriti nastavitev proženja alarmov na napravah
Sočasno potekajoči testi/sistemi	Testiranje prenosa alarmov in prenosa alarmnih sporočil do porabnika
Predvideno trajanje testa	Cca. 30 minut
Testna procedura	• Preverjanje konfiguracije naprav na nastavitvah alarmov • Simulacija preseganja kritičnih vrednosti in proženje alarmov v tem primeru (kjer se to da)
Ključne merilne točke	Spremljanje dnevnika alarmov na napravah
Namenske merilne točke	/
Normalni zaključek testa	Vsi ključni alarmi naprave so nastavljeni.
Izredni zaključek testa	/
Ključno osebje	/
Tveganja	Jih ni.

Vir: lastno delo.

- testiranje prenosa alarmov,
- testiranje posredovanja alarmnih sporočil.

b) Funkcionalni testi

Funkcionalni testi na računalniških centrih skupine HSE zajemajo preverbo delovanja samih sistemov in prenosa podatkov ter sporočil na nadzorni sistem, pa tudi prek sporočilnega sistema do ključnih uporabnikov. Sem sodijo:

- parametriranje in preverba nastavljenih parametrov na vseh sistemih,
- pravilnost merjenih podatkov na lokalnih in oddaljenih senzorjih,
- prenos podatkov med enotami in napravami,
- prenos podatkov na nadzorni sistem,
- vizualizacija podatkov na nadzornem sistemu,
- prenos sporočil z nadzornega sistema na sporočilni sistem.

[2] Navedeni so samo nekateri testi – merilni protokoli obstajajo še za: testiranje prenosov alarmov, testiranje posredovanja alarmnih sporočil, delovanje naprav, zagon DEA, testiranje izpada posamezne naprave, testiranje izliva tekočin, avtomatski preklop STS, obremenilni test DEA, obremenilni test UPS-sistema – vsak UPS ločeno, testiranje izpada hladilnih agregatov – vsak agregat ločeno, testiranje izpada obtočnih črpalk 1 in 2 – vsaka ločeno, test izpada hladilnih omar, statično delovanje – normalna obremenitev, statično delovanje – nazivna obremenitev, dvig – normalna obremenitev, dvig – nazivna obremenitev, pull down – normalno breme, pull down – nazivno breme.

Tabela 21: Testiranje in kalibracija senzorjev naprav

Parameter	Vsebina
Območje testiranja	Omejeno testiranje – samo na posamezni napravi
Ciljne naprave/sistemi	Krmilnik DEA, UPS-sistemi, STS-sistemi, hladilne omare, hladilni agregati
Spremljajoči pomožni testi	/
Namen testa	Preveriti pravilnost in točnost meritev
Sočasno potekajoči testi/sistemi	Kalibracija senzorjev in prenos podatkov na nadzorni sistem
Predvideno trajanje testa	Cca. 30 minut
Testna procedura	• Preverjanje merilnih rezultatov in sočasna kalibracija ob uporabi precizijskih merilcev • Pregled in kontrola merjenih vrednosti na nadzornem sistemu
Ključne merilne točke	• Merjene vrednosti na zaslonu naprave • Merjene vrednosti na precizijskem instrumentu • Merjene vrednosti na nadzornem sistemu
Namenske merilne točke	/
Normalni zaključek testa	Merjene vrednosti na vseh sistemih so v območju predvidenih toleranc.
Izredni zaključek testa	/
Ključno osebje	/
Tveganja	Jih ni.

Vir: lastno delo.

c) Dogodkovni testi

Dogodkovni testi v računalniških centrih skupine HSE zajemajo preverbo delovanja prenosa alarmnih sporočil v primeru izrednih dogodkov – napak na ključnih elementih oskrbne infrastrukture. Sem sodijo:

- izpad elementov napajalnih sistemov; izpad mrežnega napajanja, izpad DEA, napaka ali izpad UPS-sistemov, izpad ali napake na STS-sistemih,
- izpad elementov hladilnih sistemov (agregatov), izpad na hladilnih omarah v vseh prostorih,
- izgube pretoka hladilnega medija ali njegova visoka temperatura v cevovodih,
- signalizacija alarmov na zasilnih termometrih v vseh nadzorovanih prostorih,
- signalizacija alarmov požarnih central iz vseh prostorov,
- parametrizacijo alarmov in izrednih dogodkov na nadzornem sistemu.

Dogodkovni testi se izvajajo skupaj z obremenilnimi testi, saj s posameznimi dogodki sprožimo simulacije izpadov delovanja posamezne opreme. Merila za uspešno zaključitev testa so sprejeto obvestilo o posameznem kritičnem dogodku v vnaprej določenem času po nastopu dogodka.

Tabela 22: Testiranje avtomatskega zagona DEA

Parameter	Vsebina
Območje testiranja	Omejeno testiranje – samo na posamezni napravi
Ciljne naprave/sistemi	Krmilnik DEA, naprave DEA
Spremljajoči pomožni testi	/
Namen testa	Preveriti odzivnost DEA na izpad omrežne napetosti
Sočasno potekajoči testi/sistemi	Testiranje delovanja stikal in prenos podatkov na nadzorni sistem
Predvideno trajanje testa	Cca. 90 minut
Testna procedura	• Simulacija izpada omrežne napetosti • Iniciran avtomatski start DEA • Izvede se avtomatski preklop med mrežo in DEA. • Po povrnitvi omrežnega napajanja se napajanje preklopi nazaj na mrežo, DEA se zaustavi.
Ključne merilne točke	• Merjene vrednosti na zaslonu naprave • Merjene vrednosti na nadzornem sistemu • Signalizacija na zaslonu naprave
Namenske merilne točke	/
Normalni zaključek testa	Merjene vrednosti in odziv sistema so v območju toleranc.
Izredni zaključek testa	/
Ključno osebje	/
Tveganja	Jih ni.

Vir: lastno delo.

d) Obremenilni testi

Obremenilni testi so osrednji del testiranja in nam kažejo odpornost infrastrukture proti izpadom posameznih kosov opreme. Pri obremenilnih testih pravzaprav testiramo, ali lahko celotna oskrbna infrastruktura ob izpadu posamezne naprave še vedno zagotavlja normalne pogoje za delovanje IKT-opreme. S tem pa je povezana tudi sprejemljivost delovanja, ki se kaže kot ustreznost temperature in vlage ter zagotavlja napajanje brez prekinitev. Obremenilni testi se izvajajo integralno, na celotnem sistemu hkrati, na vseh oskrbnih sistemih in vejah. Ločimo delne in celovite obremenilne teste. Večino predvidenih testov lahko izvajamo kot delne obremenilne teste – le del testov se izvaja kot celotne obremenilne teste:

- Delni obremenilni testi – delni obremenilni testi so tisti obremenilni testi, ki se izvajajo le na delu sistemov, ne vplivajo pa na preostale sisteme, ki niso vključeni v postopek testiranja. Med delne teste sodijo naslednja testiranja:
    - testiranja električnih sistemov,
    - testiranja hladilnih sistemov.

Tabela 23: Delni obremenilni test – testiranje akumulatorskih baterij

Parameter	Vsebina
Območje testiranja	Omejeno testiranje – samo na posamezni napravi
Ciljne naprave/sistemi	Baterije posameznega UPS-sistema
Spremljajoči pomožni testi	/
Namen testa	Ugotoviti stanje in delovanje baterijskih modulov
Sočasno potekajoči testi/sistemi	Testiranje delovanja stikal in prenos podatkov na nadzorni sistem
Predvideno trajanje testa	Cca. 240 minut
Testna procedura	Izpad mrežne napetosti: • Merjenje napetosti na baterijah v določenih časovnih intervalih • Breme ločene veje mora delovati nemoteno. Avtonomni test baterij • Odklop baterij iz UPS • Priklop baterij na elektronsko breme • Praznjenje baterij prek bremena • Sprotne meritve napetostnih celic vsakih 30 minut • Ponovni vklop baterij na UPS-sistem
Ključne merilne točke	• Meritve napetosti na posameznih baterijah in skupna napetost na baterijah • Meritev električne porabe po porabnikih in na vseh sistemih • Meritve preostalih veličin v centru
Namenske merilne točke	Signalizacija delovanja baterije na UPS-napravi
Normalni zaključek testa	Padec napetosti na baterijah v mejah dovoljenih vrednosti
Izredni zaključek testa	Prevelik padec napetosti na posameznih baterijah v določenem časovnem obdobju, preklop na drugo vejo napajanja ne deluje.
Ključno osebje	Pooblaščeno osebje za preklope stikal na dovodih in UPS-sistemu
Tveganja	Srednje

Vir: lastno delo.

Tabela 24: Integralni obremenilni test – odpornost proti izpadom

Parameter	Vsebina
Območje testiranja	Celovito testiranje
Ciljne naprave/sistemi	Vsi oskrbni sistemi, vsak sistem posamezno: DEA, STS, ATS, UPS, BAT, hladilni agregati, hladilne omare
Spremljajoči pomožni testi	Delovanje nadzornega sistema in pomožnih meritev temperature, el. vrednosti ipd.
Namen testa	Ugotoviti vpliv izpada posameznega sistema na delovanje celotne oskrbne infrastrukture
Predvideno trajanje testa	Meritve potekajo 30 minut oz. do stabilizacije razmer v prostoru.
Testna procedura	Ob 100-% obremenitvi z ročnim posegom povzročiti izpad posameznega sistema in spremljati odzivnost
Ključne merilne točke	• Meritve temperature v sistemskem prostoru na različnih mestih v 15-minutnih intervalih (ob spremembah pogosteje) • Meritve električne porabe po porabnikih in na vseh sistemih v 15-minutnih intervalih (ob spremembah pogosteje) • Meritve preostalih veličin v centru
Namenske merilne točke	/
Normalni zaključek testa	Vklop obeh vej in vzpostavitev stabilnih pogojev delovanja
Izredni zaključek testa	/
Ključno osebje	/
Tveganja	Srednje

Vir: lastno delo.

- Integralni obremenilni testi – integralni obremenilni testi so tisti obremenilni testi, ki se izvajajo na pretežnem delu ali vseh oskrbnih sistemih hkrati. Posledično vplivajo na delovanje vse nameščene infrastrukture.

Vsa predvidena testiranja se izvajajo le ob vnaprej dogovorjenih terminih in s celotno skupino upravljalcev in vzdrževalcev. Kritična testiranja, ki imajo srednje ali veliko tveganje, se morajo izvajati ob posebnih varnostnih ukrepih z možnostjo preklopa na rezervno lokacijo. Vsi testi s povečanim tveganjem se izvajajo ob prisotnostih vseh skrbnikov ključnih naprav, pri čemer mora biti zagotovljena tudi odzivnost vzdrževalcev strojev in programske opreme. Za testiranja so se definirali naslednji intervali:

a) zagonska testiranja – izvajajo se ob namestitvi in zagonih sistemov. V obsegu zagonskih testiranj se izvajajo vsi navedeni testi, pri čemer se breme simulira z ustreznimi toplotnimi bremeni. Pred prevzemom se predajo ustrezna testna poročila,
b) redna tedenska testiranja – obsegajo predvsem funkcionalna testiranja, in sicer predvsem zagon DEA in avtomatski zagon DEA z avtomatskim preklopom STS-stikala,
c) redna mesečna testiranja – njihov namen je zagotovitev delovanja ključnih naprav in zagotovitev delovanja signalizacije. Mesečno se izvajajo naslednja testiranja:
   - zagon DEA,
   - testiranje izliva tekočine,
   - avtomatski zagon DEA,
   - avtomatski preklop STS,
   - obremenilni test DEA,
   - testiranje posredovanja alarmnih sporočil,
d) redna šestmesečna in letna testiranja – obsegajo testiranja ključne infrastrukture glede na njeno delovanje. Sem sodijo naslednji testi:
   - testiranje alarmiranja na napravah,
   - testiranje prenosa alarmov,
   - testiranje posredovanja alarmnih sporočil,
   - testiranje in kalibracija senzorjev naprav,
   - delovanje naprav,
   - zagon DEA,
   - testiranje izpadov posamezne naprave,
   - testiranje izliva tekočine,
   - avtomatski zagon DEA,
   - avtomatski preklop STS,
   - testiranje akumulatorskih baterij,
   - obremenilni test DEA,
   - test odpornosti proti izpadom,

e) izredna letna testiranja – se od rednih ločijo po tem, da se izvajajo le ob izjemnih dogodkih. Takrat se lahko izvajajo vsa testiranja v navedenem obsegu.

3.8 Ključni indikatorji uspeha

Največkrat uporabljena metrika za porabo energije v računalniških centrih je PUE (ang. power usage effectiveness). Uporabljamo jo zaradi svoje interpretacije preprostosti – nižja vrednost je boljša. PUE v računalniških centrih skupine HSE se na podlagi meritev in izračunov znotraj sistemov za nadzor oskrbne infrastrukture izračunava v vrednosti, ki jo mnogi interpretirajo kot kazalnik, kako »zeleni« so njihovi centri. Za predstavitev uspešnosti poslovanja oz. delovanja računalniških centrov se uporabljajo tudi klasični indikatorji, kot so:

- utilizacija – kaže, kolikšna je izkoriščenost virov oskrbne infrastrukture, ki so na voljo,
- razpoložljivost – kaže stopnjo, do katere naprave oskrbne infrastrukture delujejo in so na voljo, v splošnem pa določa razmerje med pričakovanim nivojem storitev in tistih, ki ga računalniški center dejansko zagotavlja. V računalniških centrih skupine HSE je razpoložljivost najpomembnejša – v veliki meri je od razpoložljivosti odvisna varna in zanesljiva proizvodnja električne energije,
- načrtovana nerazpoložljivost – ob morebitnih večjih nadgradnjah je treba načrtovano nerazpoložljivost skrbno načrtovati. Zahteve po nerazpoložljivosti so najmanjše možne.

Ob izdelavi analize je bilo ugotovljeno, da je izkoriščenost virov slabša od pričakovane. Deloma je kriva tudi slabša energetska učinkovitost enega od centrov, pri čemer bo treba v prihodnje tovrstno nedoslednost urediti. Razpoložljivost je na visoki ravni, ob prenovi omrežja MPLS/IP MAN bo ta še boljša. Nerazpoložljivost se že načrtuje, zanjo je treba zapisati le potrebne organizacijske dokumente. V prihodnje bo, za izboljšanje rasti porabe energije v računalniških centrih skupine HSE, treba izvesti ukrepe na naslednjih področjih:

- energetska optimizacija in izvajanje energetskega menedžmenta na strežniški opremi,
- porazdelitev moči in uporaba mehanizmov za ponovno izkoriščanje odvečnih virov.

3.9 Prenova procesa upravljanja računalniških centrov skupine HSE

Osnova za prenovo procesa upravljanja bo izvedena ocena tveganj na infrastrukturi računalniških centrov skupine HSE, vključno s celotno podporno infrastrukturo. Poenotenje postopkov upravljanja in vzdrževanja bo imelo za posledico večjo učinkovitost in nižje stroške. Zanje bosta v osnovi poskrbela na novo postavljena organizacijska enota in za to delo usposobljen strokovni kader.

SKLEP

V pričujočem delu smo obravnavali informacijsko varnost v računalniških centrih skupine HSE, se opredelili do celotne oskrbne infrastrukture in za učinkovito upravljanje in zagotavljanje varnosti pripravili nabor ukrepov, temelječih na znani standardizaciji. Inovativnost naloge se kaže pri izdelavi celovitega modela upravljanja informacijske varnosti po prilogi A-standarda ISO/IEC 27001:2013. Zanjo smo pripravili celoten nabor 14 domen in 144 ukrepov, ki so namenjeni podpori varovanja informacij v računalniških centrih. Pripravljen model je zasnovan na treh stebrih varnosti: zaupnosti, celovitosti in razpoložljivosti, pri čemer smo v koncept vključili ljudi, različne procese in tehnologijo. Razdeljen je na osnovne procese po Demingovem krogu – organizacija in človeški viri, upravljanje infrastrukture, izvajanje varovanja, spremljanje in nadzor – z zapisanimi podprocesi, ki bistveno poenostavijo uvajanje prepotrebnih varnostnih zahtev pri upravljanju kritične infrastrukture.

Temeljita analiza delovanja računalniških centrov v skupini HSE in že izvedenih varnostnih ukrepov je podala izhodišče za pripravo pravil o zagotavljanju varnega in zanesljivega delovanja IKT-opreme, preprečevanju napak ter zagotavljanju predvidljivosti in ponovljivosti. Ob upoštevanju krovne varnostne politike in specifičnih politik računalniških centrov ter temeljitega testiranja postopkov in delovanja zagotavljamo računalniškim centrom celovito varnost.

LITERATURA IN VIRI

1. Aberšek, B. & Flašker, J. (2005). *Vzdrževanje – sistemi, strategije, procesi in optimiranje.* Maribor: Fakulteta za strojništvo.
2. ASHRAE Technical Committee. (2011). *2011 Thermal Guidelines for Data Processing Environments – Expanded Data Center Classes and Usage Guidance.* Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers.
3. ASHRAE Technical Committee 9.9. (2012). *Data Center Networking Equipment – Issues and Best Practices.* Atlanta: ASHRAE TC.
4. Belady, C. & Malone, C. (2007). *Metrics and an infrastructure model to evaluate data center efficiency*. ASME InterPACK *'07*. IPAC2007-33338. Los Angeles: ASME
5. Bratina, J. (1983). Zanesljivost proizvodnih naprav. *Železarski zbornik, 17*(2), 77–83.
6. Buyya, R., Yeo, C., Venugopal, S., Broberg, J. & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6), 599–616.
7. Capozzoli, A. & Primicieri, G. (2015). Cooling systems in data centers: state of art and emerging technologies. *Energy Procedia*, *83*, 485–493.
8. Cenelec. (2014). *EN50600 Standard – Information technology – data centre facilities and infrastructure.* Brusseles: European Committee for Electrotechnical Standardization.

9. Chille, V., Mund, S. & Moller, A. (2018). Harmonizing physical and IT security levels for critical infrastructures. *Sicherheit 2018, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik* (133–143). Bonn, Nemčija: Gesellschaft für Informatik.
10. Cisco. (2011). *Why Integrate Physical and Logical Security?.* San Jose, ZDA: Cisco.
11. Cisco. (2016). *Cisco Data Center Spine-and-Leaf Architecture: Design Overview.* San Jose, ZDA: Cisco.
12. Cole, D. (2012). *Data Center Infrastructure Management (DCIM).* West Chester, ZDA: Data Center Knowledge.
13. Dayarathana, M., Wen, Y. & Fan, R. (2016). Data Center Energy Consumption Modeling: A Survey. *IEEE Communications Surveys & Tutorials 18*(1), 732–794.
14. E-ISAC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Washington, ZDA: SANS Ics.
15. Estall, H. (2012). *BCMS – Implementation and certification to ISO 22301.* Swindon, UK: BCS – The Chartered Institute for IT.
16. Gartner. (2018). *Gartner*. Pridobljeno 12.decembra 2018 iz https://www.gartner.com/it-glossary/data-center/
17. Geng, H. (2015). *Data Center Handbook.* Palo Alto, ZDA: Wiley.
18. Gradišar, J., Jaklič, J., Damij, T. & Baloh, P. (2005). *Osnove poslovne informatike.* Ljubljana: Ekonomska fakulteta.
19. HSE. (2016). *Letno poročilo skupine HSE.* Ljubljana: HSE.
20. HSE. (2018). *Letno poročilo 2017.* Ljubljana: HSE.
21. Hudoklin Božič, A. & Rozman, V. (2004). *Zanesljivost in razpoložljivost sistemov človek – stroj.* Kranj: Moderna organizacija v okviru FOV.
22. Institute of Electrical and Electronics Engineers. (1996). *IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications.* New York, ZDA: The Institute of Electrical and Electronics Engineers, Inc.
23. Institute of Electrical and Electronics Engineers. (2007). *IEEE Std 493–2007 (Revision of IEEE Std 493–1997) – IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*. New York, ZDA: The Institute of Electrical and Electronics Engineers, Inc.
24. ISO. (2009). *ISO 31000 Risk management – Principles and guidelines.* Geneva: ISO.
25. ITIC (2017). *ITIC 2017–2018 Global Server Hardware, Server OS Reliability Report.* Concord, MA ZDA: Information Technology Intelligence Consulting (ITIC) Corp.
26. Košutič, D. (2013). *Becoming resilient – The definitive Guide to ISO 22301 Implemenation.* Zagreb: EPPS Services Ltd.
27. Lavuger, B. (2016). *Razpoložljivost sistemov zanesljive oskrbe z električno energijo* (magistrsko delo). Maribor: Fakulteta za elektrotehniko in računalništvo.
28. Levy, M. & Raviv, D. (2017). A Novel Framework for Data Center Metrics using a Multidimensional Approach. *Florida, ZDA: Advances in Science, Technology and Engineering Systems Journal, 3* (2), 238 – 251.
29. Li, Y. (2014). *Network-Aware Job Placement in Datacenter Environments* (Master thesis). ALBERTA, Canada: University of Calgary.
30. Martens, R. (2018). *IoT Makes New Security.* Pridobljeno 2. januarja 2019 iz https://www.securityindustry.org/2016/04/01/iot-security-partnerships/.

31. Moises, L. & Hallstrom, J. (2017). A new approach to data center infrastructure monitoring and management (DCIMM). *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC),* 1–6.
32. Shehabi, A., Smith, S., Sartor, D., Brown, R., Herrlin, M., Koomey, J., Masanet, E., Horner, N., Azevedo, I. & Lintner, W. (2016). *United States Data Center Energy Usage Report.* Berkeley, California: Lawrence Berkeley National Laboratory.
33. SIST. (2013). *ISO/IEC 27002 Informacijska tehnologija – Varnostne tehnike – Zahteve,* Ljubljana: Slovenski inštitut za standardizacijo.
34. SIST. (2014). *SIST ISO/IEC 27002.* ISO/IEC 27002 Informacijska tehnologija – Varnostne tehnike, Ljubljana: Slovenski inštitut za standardizacijo.
35. Strife, M. (2016). *An analysis of Cloud-based Shadow IT and a framework for managing its risks and opportunities*. (Master thesis). Enschede, Netherlands: University of Twente.
36. TUV. (2018). *TRC-021_Kriterienkatalog_RechenZ_en.* Pridobljeno 2. januarja 2019 iz https://www.tuv.com/media/corporate/training_consulting/data_center/TRC-021_Kriterienkatalog_RechenZ_en.pdf/
37. Uptime Institute. (2016). *Data Center Site Infrastructure Tier Standard: Topology.* Seattle, ZDA: Uptime Institute.
39. Van Niekerk, B. (2015). *Toward a Secure Data Center Model*. ISACA journal – *3*, 1–10. Illinois, ZDA: Isaca
40. Zarja Elektronika. (2018). *Stabilni gasilni sistemi.* Kamnik: Zarja elektronika, d. o. o.