REPUBLIKA SLOVENIJA
RAČUNSKO SODIŠČE

REVIZIJSKO POROČILO

Učinkovitost upravljanja kibernetske varnosti za področje kritične infrastrukture v ELES

2021

7 CENOVNO DOSTOPNA IN ČISTA ENERGIJA

16 MIR, PRAVIČNOST IN MOČ INSTITUCIJE

CILJI TRAJNOSTNEGA RAZVOJA

POSLANSTVO

Računsko sodišče pravočasno in objektivno obvešča javnosti o pomembnih razkritjih poslovanja državnih organov in drugih uporabnikov javnih sredstev ter svetuje, kako naj državni organi in drugi uporabniki javnih sredstev izboljšajo svoje poslovanje.

REPUBLIKA SLOVENIJA
RAČUNSKO SODIŠČE

REVIZIJSKO POROČILO

Učinkovitost upravljanja kibernetske varnosti za področje kritične infrastrukture v ELES

Številka: 321-3/2019/31
Ljubljana, 23. avgusta 2021

Povzetek

Računsko sodišče je izvedlo revizijo učinkovitosti **ELES, d.o.o., sistemskega operaterja prenosnega elektroenergetskega omrežja** (v nadaljevanju: ELES) pri upravljanju kibernetske varnosti za področje kritične infrastrukture v obdobju od 1. 1. 2019 do 31. 7. 2020. Po mnenju računskega sodišča je bil ELES v obdobju, na katero se nanaša revizija, pri upravljanju kibernetske varnosti na področju kritične infrastrukture **učinkovit.**

ELES je že v letu 2009 uvedel obvladovanje tveganj in je v nadaljnjih letih vzpostavil celovit sistem upravljanja tveganj, ki je bil skupaj z vzpostavljenim notranjim kontrolnim sistemom ključni del integriranega sistema upravljanja družbe. Upravljanje tveganj v ELES je temeljilo na procesnem modelu – tveganja v posameznih procesih. ELES je vodil informatiziran katalog tveganj tudi po področjih poslovanja, v letu 2019 pa je uvedel še katalog tveganj na področju kritične infrastrukture in na področju izvajalcev bistvenih storitev. ELES je na podlagi Zakona o kritični infrastrukturi, usmeritev Ministrstva za obrambo, strokovnih usmeritev nosilcev sektorja kritične infrastrukture in lastne metodologije ocenjevanja tveganj pravočasno izvedel identifikacijo virov tveganj za delovanje kritične infrastrukture, analizo in ovrednotenje tveganj za delovanje kritične infrastrukture, določil vire tveganj, spremljal stanje kritične infrastrukture, imel podvojene centre vodenja in izdelal varnostne načrte. ELES je tudi imel dokumentiran sistem upravljanja varovanja informacij, v času revizijskega pregleda pa je zaključeval vpeljavo sistema upravljanja neprekinjenega poslovanja, kot to zahteva Zakon o informacijski varnosti. ELES je na podlagi zahtev nosilcev sektorja pripravil oceno tveganj za delovanje kritične infrastrukture in ukrepe za zaščito kritične infrastrukture. ELES se je odzval na epidemijo novega koronavirusa SARS-CoV-2 z različnimi ukrepi in s tem omogočil neprekinjeno delovanje procesov.

ELES je zaznavanje kibernetskih groženj izvajal učinkovito, in sicer z različnimi dokumentiranimi aktivnostmi, imel je opredeljene vloge in odgovornosti za odkrivanje varnostnih dogodkov ter je izvajal različne aktivnosti odkrivanja. ELES je imel vpeljane postopke posredovanja informacij o odkritih dogodkih, prav tako pa je nenehno izboljševal postopke zaznavanja in ustvarjal različne zbirke znanja, povezane z varnostnimi dogodki. ELES je pri upravljanju odzivanja na kibernetske grožnje uporabljal načrt odzivanja. Zaposleni so bili usposobljeni za odzivanje ter so poročali o dogodkih in posredovali informacije o dogodkih prejemnikom tako znotraj kot tudi izven ELES. Z nekaterimi organizacijami so imeli vpeljano prostovoljno izmenjavo informacij o incidentih. ELES je upravljanje odzivanja izvajal tudi z analiziranjem obvestil ter razumevanjem vpliva incidentov na organizacijo kakor tudi z razvrščanjem incidentov. ELES je imel vpeljane procese za spremljanje, analize in odzivanje na ranljivosti kakor tudi za omejevanje in blažitev incidentov.

ELES ni imel posebne strategije za področje kibernetske varnosti, je pa imel vzpostavljene politike za vse segmente integriranega sistema upravljanja, ki so se prek vodstvenega pregleda redno pregledovale in ustrezno dopolnjevale. ELES ima še možnosti za izboljšave, ki se jih zaveda in jih tudi uvaja.

Računsko sodišče od ELES ni zahtevalo predložitve odzivnega poročila, je pa podalo nekaj priporočil za nadaljnje izboljšanje stanja.

Kazalo

1. Uvod

Revidirali smo učinkovitost ELES, d.o.o., sistemskega operaterja prenosnega elektroenergetskega omrežja pri upravljanju kibernetske varnosti za področje kritične infrastrukture. Revizijo smo izvedli na podlagi Zakona o računskem sodišču[1] in Poslovnika Računskega sodišča Republike Slovenije[2] ter v skladu z mednarodnimi revizijskimi standardi, ki jih določa Napotilo za izvajanje revizij[3]. Sklep o izvedbi revizije[4] je bil izdan 16. 12. 2019, sklep o spremembi sklepa o izvedbi revizije[5] pa je bil izdan 23. 6. 2020.

Naša pristojnost je na podlagi izvedene revizije podati opisno mnenje o učinkovitosti ELES pri upravljanju kibernetske varnosti na področju kritične infrastrukture. Revizijo smo načrtovali in izvedli tako, da smo pridobili zadostna in ustrezna zagotovila za izrek mnenja.

Revizija je obsegala obdobje od 1. 1. 2019 do 31. 7. 2020.

1.1 Opredelitev revizije

Revizija je bila opredeljena kot revizija smotrnosti poslovanja. Obsegala je kibernetsko varnost na področju kritične infrastrukture.

V tem poročilu uporabljamo pojme, povezane s kibernetsko varnostjo kritične infrastrukture v ELES, v naslednjem pomenu:

- **kibernetska varnost:** Strategija kibernetske varnosti – vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti[6] (v nadaljevanju: strategija kibernetske varnosti) opredeljuje kibernetsko varnost kot:
  - skupek aktivnosti in drugih ukrepov, tehničnih in netehničnih, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih ta vsebuje in obravnava, kar vključuje programsko opremo in podatke kot tudi druge elemente kibernetskega prostora, pred vsemi grožnjami, vključno z grožnjami nacionalni varnosti,
  - stopnjo zaščite, ki jo aktivnosti in ukrepi lahko zagotovijo,
  - združena področja profesionalnih naporov, vključno z raziskavami in razvojem na področju implementiranja in izboljševanja ukrepov ter dvigovanja njihove kakovosti;

1 Uradni list RS, št. 11/01 in 109/12.

2 Uradni list RS, št. 91/01.

3 Uradni list RS, št. 43/13.

4 Št. 321-3/2019/2.

5 Št. 321-3/2019/6.

6 Sprejeta na 76. redni seji Vlade Republike Slovenije (v nadaljevanju: vlada) z dne 25. 2. 2016, [URL: https://www.gov.si/assets/vladne-sluzbe/UVTP/DOKUMENTI/Strategija-kibernetske-varnosti.pdf], 20. 8. 2021.

- **upravljavec kritične infrastrukture:** vlada je februarja 2019 ELES določila za upravljavca kritične infrastrukture;
- **kritična infrastruktura**[7] **ELES:** je infrastruktura ELES, ki sta jo pristojni ministrstvi (Ministrstvo za javno upravo (v nadaljevanju: MJU) in Ministrstvo za infrastrukturo (v nadaljevanju: MZI)), nosilca sektorjev kritične infrastrukture, določili februarja in marca 2019 (definicija kritične infrastrukture Republike Slovenije je opredeljena v nadaljevanju);
- **sektorji kritične infrastrukture:** kritično infrastrukturo ELES upravljata MJU in MZI, ki sta na seznamu nosilcev sektorjev kritične infrastrukture in ju je vlada s sklepom določila julija 2018[8].

Zakon o informacijski varnosti[9] (v nadaljevanju: ZInfV), ki ureja področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji, med drugimi opredeljuje naslednje pojme:

- **kibernetska varnost** je sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi;
- **kibernetski prostor** je globalno informacijsko okolje, ustvarjeno s pomočjo elektronskih komunikacijskih omrežij in informacijskih sistemov; kibernetski prostor omogoča nastanek, obdelavo in izmenjavo informacij;
- **kibernetska grožnja** je možnost zlonamernega poskusa poškodovanja ali prekinitve računalniškega omrežja, sistema, storitev in podatkov.

Zakon o kritični infrastrukturi[10] (v nadaljevanju: ZKI), ki ureja ugotavljanje in določanje kritične infrastrukture Republike Slovenije, načela in načrtovanje zaščite kritične infrastrukture, naloge organov in organizacij na področju kritične infrastrukture ter obveščanje, poročanje, zagotavljanje podpore odločanju, varovanje podatkov in nadzor na področju kritične infrastrukture, med drugimi opredeljuje naslednje pojme:

- **kritična infrastruktura Republike Slovenije** obsega tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne posledice za nacionalno varnost, gospodarstvo in druge ključne družbene funkcije ter zdravje, varnost, zaščito in blaginjo ljudi;
- **upravljavci kritične infrastrukture** so gospodarske družbe, zavodi, državni organi in Banka Slovenije, ki imajo v lasti ali upravljajo kritično infrastrukturo;
- **načrtovanje zaščite kritične infrastrukture** obsega ocenjevanje tveganj za delovanje kritične infrastrukture in oblikovanje ukrepov za zaščito kritične infrastrukture;

---

7 Kritična infrastruktura je določena v dokumentu, ki je po Zakonu o tajnih podatkih (v nadaljevanju: ZTP; Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20) označen s stopnjo tajnosti. V tem poročilu ne razkrivamo opisov kritične infrastrukture, ker to ni potrebno za dosego ciljev revizije.

8 Št. 80200-1/2018/10 z dne 5. 7. 2018.

9 Uradni list RS, št. 30/18.

10 Uradni list RS, št. 75/17.

- **nosilci sektorjev kritične infrastrukture** so posamezna ministrstva, ki so odgovorna za delovna področja, kamor spada kritična infrastruktura Republike Slovenije, in Banka Slovenije;
- **ocena tveganj za delovanje kritične infrastrukture** je rezultat celovitega postopka identifikacije, analize in ovrednotenja različnih virov tveganj za delovanje kritične infrastrukture, ki se izvede za zagotovitev podlage za oblikovanje ukrepov za zaščito kritične infrastrukture;
- **sektorji kritične infrastrukture** so posamezne vsebinsko zaokrožene celote delovanja kritične infrastrukture, med katere se štejejo tudi objekti, ki zagotavljajo sistemsko odpornost in redundanco;
- **ukrepi za zaščito kritične infrastrukture** so dejavnosti, katerih namen je zagotoviti varnost kritične infrastrukture, preprečiti motnje v njenem delovanju ali prekinitev njenega delovanja in ublažiti posledice tega, po potrebi vzpostaviti nadomestno ali obhodno delovanje kritične infrastrukture in zagotoviti njeno čimprejšnje ponovno nemoteno delovanje;
- **zaščita kritične infrastrukture** kot del področja kritične infrastrukture je dejavnost, ki se izvaja za zagotovitev neprekinjenosti delovanja kritične infrastrukture.

Marca 2021 smo izdali revizijsko poročilo o učinkovitosti zagotavljanja kibernetske varnosti v Republiki Sloveniji[11], v katerem smo med drugim preverili, kako so vlada, Urad Vlade Republike Slovenije za varovanje tajnih podatkov in MJU pristopili k izvajanju aktivnosti v skladu s strategijo kibernetske varnosti. V tej krovni reviziji smo pregledali zagotavljanje kibernetske varnosti po načelu od zgoraj navzdol, nadaljujemo pa z ločenimi revizijami na posameznih področjih tako pri upravljavcih kritične infrastrukture kakor tudi pri izvajalcih bistvenih storitev.

1.2 Obseg in omejitve revizije

V reviziji smo se osredotočili na zahteve, ki jih ZKI nalaga upravljavcu kritične infrastrukture, in sicer da:

- zagotavlja neprekinjeno delovanje kritične infrastrukture[12];
- pripravi in ažurira dokumente načrtovanja zaščite kritične infrastrukture, ki obsega oceno tveganja za delovanje kritične infrastrukture in ukrepe za zaščito kritične infrastrukture[13];
- izdela oceno tveganj za delovanje kritične infrastrukture na podlagi Navodila za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije[14] (v nadaljevanju: navodilo za ocenjevanje tveganj) in strokovnih usmeritev, ki jih za posamezne sektorje kritične infrastrukture izdelajo nosilci sektorjev kritične infrastrukture[15];
- na podlagi izdelane ocene tveganja za delovanje kritične infrastrukture določi ukrepe za zaščito kritične infrastrukture, ki so lahko stalni ali dodatni; stalni ukrepi se izvajajo v vseh razmerah, ob povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi pa se lahko njihovo

11 Št. 320-2/2019/31 z dne 3. 3. 2021, [URL: https://www.rs-rs.si/fileadmin/user_upload/Datoteke/Revizije/2021/KibernetskaVarnost/KibernetskaVarnost_RSP_RevizijskoP.pdf], 20. 8. 2021.

12 19. člen ZKI.

13 11. in 14. člen ZKI.

14 Uradni list RS, št. 7/19.

15 12. člen ZKI.

izvajanje stopnjuje; dodatni ukrepi se izvajajo ob povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi, če stalni ukrepi, tudi če se njihovo izvajanje stopnjuje, ne zadostujejo[16];

- obvešča nosilca sektorja kritične infrastrukture in Nacionalni center za krizno upravljanje o prekinitvi delovanja kritične infrastrukture, za katero oceni, da lahko ima negativne materialne in druge posledice za delovanje sektorja kritične infrastrukture, in o že izvedenih ukrepih za zaščito kritične infrastrukture[17];
- pripravi letno poročilo upravljavca kritične infrastrukture o zagotavljanju neprekinjenega delovanja kritične infrastrukture za preteklo leto in ga do konca februarja posreduje nosilcu sektorja kritične infrastrukture[18].

V reviziji smo se osredotočili tudi na to, kako ELES upravlja zaznavanje in odzivanje na kibernetske grožnje. Pri tem smo preverili, kako ELES:

- zaznava okoliščine in dogodke, ki bi lahko prevedli do kibernetskih groženj;
- ugotavlja dogodke kibernetske varnosti in preverja učinkovitost zaščitnih ukrepov;
- vzdržuje in preverja postopke zaznavanja izjemnih dogodkov z namenom zagotavljanja ozaveščenosti;
- izvaja in vzdržuje postopke odzivanja;
- usklajuje dejavnosti odzivanja z notranjimi in zunanjimi zainteresiranimi stranmi;
- izvaja analize incidentov;
- izvaja preprečevanje širitve dogodka in zmanjševanje njegovih učinkov;
- izboljšuje in nadgrajuje odzivne aktivnosti.

Revizija ni obsegala presoje sistema upravljanja **neprekinjenega poslovanja** revidiranca in/ali **neprekinjenega delovanja informacijskega sistema** revidiranca. Prav tako v reviziji nismo pregledovali aktivnosti in ukrepov ELES kot izvajalca bistvenih storitev[19] po ZInfV.

1.3 Področje revizije

1.3.1 Kibernetska varnost v Republiki Sloveniji

Področje kibernetske varnosti v Republiki Sloveniji do leta 2016 ni bilo sistemsko urejeno. Sprejeti so bili posamezni strateški dokumenti, ki so urejali tudi nekatere vsebine o kibernetski varnosti. Prvi večji premik na področju normativnega urejanja kibernetske varnosti se je zgodil na začetku

16 13. člen ZKI.

17 Prvi odstavek 23. člena ZKI.

18 24. člen ZKI.

19 Javni ali zasebni subjekt, ki spada v katero od področij, navedenih v 5. členu ZInfV. Posameznega izvajalca bistvenih storitev na podlagi meril iz 7. člena ZInfV določi vlada.

leta 2016, ko je vlada v februarju sprejela Srednjeročni obrambni program Republike Slovenije 2016–2020[20], v katerega je vključila tudi področje kibernetske varnosti, in sicer pod točko o informacijski varnosti in kibernetski obrambi. V skladu s tem programom naj bi do leta 2020 v Slovenski vojski vzpostavili enoto za kibernetsko varnost. Vlada je v februarju 2016 sprejela tudi strategijo kibernetske varnosti, ki predstavlja prvi korak za sistemsko ureditev področja in okrepitev zagotavljanja kibernetske varnosti. S strategijo kibernetske varnosti je Republika Slovenija opredelila ukrepe za vzpostavitev nacionalnega sistema kibernetske varnosti, ki bo zmožen hitrega odzivanja na varnostne grožnje in bo predstavljal učinkovito zaščito informacijsko-komunikacijske infrastrukture in informacijskih sistemov, s tem se bo zagotavljalo neprekinjeno delovanje tako javnega kot zasebnega sektorja ter omogočilo delovanje ključnih funkcij države in družbe v vseh varnostnih razmerah[21]. Konec leta 2017 je Državni zbor Republike Slovenije (v nadaljevanju: državni zbor) sprejel ZKI, v aprilu 2018 pa še ZInfV, s katerim je Republika Slovenija prvič celovito in sistemsko uredila področje informacijske varnosti. Vlada je julija 2018 sprejela Sklep o določitvi kriterijev za ugotavljanje kritične infrastrukture Republike Slovenije in njihovih mejnih vrednosti ter prioritete delovanja sektorjev kritične infrastrukture[22]. Januarja 2019 je Ministrstvo za obrambo (v nadaljevanju: MO) sprejelo navodilo za ocenjevanje tveganj[23]. Vlada je februarja 2019 sprejela seznam kritične infrastrukture in določila upravljavce kritične infrastrukture, med katerimi je tudi ELES. Minister za javno upravo je maja 2019 izdal Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev[24]. Junija 2019 je vlada sprejela Uredbo o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev[25]. Državni zbor je konec septembra 2019 sprejel Resolucijo o strategiji nacionalne varnosti Republike Slovenije[26], ki navaja, da se bodo v mednarodnem varnostnem okolju pojavljale številne grožnje, med katerimi med najpomembnejše spadajo hibridne in informacijsko-kibernetske grožnje, ter da je zagotavljanje suverenosti Republike Slovenije v kibernetskem prostoru izrednega pomena. V oktobru 2019 je vlada potrdila prvo skupino izvajalcev bistvenih storitev, med katerimi je tudi ELES.

1.3.2 Kritična infrastruktura

Merila in mejne vrednosti za določitev upravljavcev kritične infrastrukture je vlada določila v juliju 2018. Vlada je kritično infrastrukturo razdelila na 8 sektorjev: energetika, promet, prehrana, preskrba s pitno vodo, zdravstvo, finance, varovanje okolja ter informacijsko-komunikacijska omrežja in sistemi[27]. ZKI določa, da vlada določi kritično strukturo in njene upravljavce[28]. ZKI tudi določa, katero dokumentacijo načrtovanja zaščite kritične infrastrukture[29] izdelajo in hranijo upravljavci kritične

20 [URL: http://mo.arhiv-spletisc.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/predpisi/obramba/SOPR2016_2020.pdf], 20. 8. 2021.

21 Povzeto po strategiji kibernetske varnosti.

22 Št. 80200-2/2018/4 z dne 26. 7. 2018.

23 Tako kot opomba 14.

24 Uradni list RS, št. 32/19.

25 Uradni list RS, št. 39/19.

26 Uradni list RS, št. 59/19.

27 Prvi odstavek 4. člena ZKI.

28 Drugi odstavek 9. člena ZKI.

29 11. člen ZKI.

infrastrukture in kako izvedejo oceno tveganj za delovanje kritične infrastrukture[30]. ZKI tudi določa, kakšne ukrepe za zaščito kritične infrastrukture mora vpeljati vsak upravljavec[31] ter način in pogostost ažuriranja dokumentov načrtovanja zaščite kritične infrastrukture[32]. ZKI prav tako določa, da morajo upravljavci kritične infrastrukture zagotavljati neprekinjeno delovanje kritične infrastrukture[33]. Upravljavci kritične infrastrukture so skladno z določili ZKI tudi dolžni obveščati nosilca sektorja o prekinitvah delovanja[34], kakor tudi redno letno poročati o zagotavljanju neprekinjenega delovanja kritične infrastrukture[35].

Minister za obrambo je februarja 2019 objavil navodilo za ocenjevanje tveganj, ki določa podlage za izdelavo ocen tveganj za delovanje kritične infrastrukture, postopek izdelave ocen tveganj za delovanje kritične infrastrukture ter obveznost ažuriranja teh ocen[36]. Navodilo za ocenjevanje tveganj določa vsebino in postopek izdelave ocene tveganj za delovanje kritične infrastrukture[37], določa pa tudi, da nosilci sektorjev kritične infrastrukture pripravijo strokovne usmeritve nosilca sektorja, ki naj vsebujejo značilnosti posameznega sektorja, pomen posledic prekinitve delovanja ali uničenja kritične infrastrukture, standarde, metodologije in druge smernice za ocenjevanje tveganj, ključna tveganja za sektor, soodvisnost od drugih sektorjev in vpliv mednarodnega okolja na delovanje sektorja[38]. Vsebina tveganja, ki jo pripravi posamezen upravljavec kritične infrastrukture, pa naj vsebuje:

- opis stanja kritične infrastrukture v razmerah rednega delovanja[39]:
  - poslanstvo in temeljne naloge upravljavca za delovanje sektorja,
  - tehnološke in materialno-tehnične zmogljivosti za izvajanje poslanstva in temeljnih nalog,
  - kadrovske zmogljivosti,
  - finančni viri,
  - druge zmogljivosti;
- seznam identificiranih virov tveganj za delovanje kritične infrastrukture[40];
- opisno analizo in ovrednotenje virov tveganj za delovanje kritične infrastrukture[41]:
  - verjetnost uresničitve vira tveganj,
  - resnost potencialne škode, nastale zaradi uresničitve vira tveganj,

30 12. člen ZKI.

31 13. člen ZKI.

32 14. člen ZKI.

33 19. člen ZKI.

34 23. člen ZKI.

35 24. člen ZKI.

36 1. člen navodila za ocenjevanje tveganj.

37 4. člen navodila za ocenjevanje tveganj.

38 5. člen navodila za ocenjevanje tveganj.

39 6. člen navodila za ocenjevanje tveganj.

40 7. člen navodila za ocenjevanje tveganj.

41 8. člen navodila za ocenjevanje tveganj.

- potencialni vplivi uresničitve vira tveganj na poslovne procese,
- drugi dejavniki,
- določitev in ovrednotenje tistih virov tveganj, ki lahko povzročijo izredni dogodek ali krizo.

Navodilo za ocenjevanje tveganj določa, da upravljavec ažurira oceno tveganja za delovanje kritične infrastrukture ob nastanku novih okoliščin, ki lahko pomembno vplivajo na delovanje kritične infrastrukture, najmanj pa 1-krat letno. Upravljavec mora k izdelani oziroma spremenjeni oceni tveganja za delovanje kritične infrastrukture pridobiti soglasje pristojnega nosilca sektorja.

ELES je upravljavec kritične infrastrukture v Republiki Sloveniji. Seznam kritične infrastrukture v Republiki Sloveniji je določen v dokumentu, ki je po ZTP označen s stopnjo tajnosti. Ker to ni potrebno za dosego ciljev revizije in v želji, da bi bilo revizijsko poročilo v celoti dostopno čim širšemu krogu bralcev, v poročilu podrobneje ne razkrivamo, katero kritično infrastrukturo upravlja ELES.

ELES ni upravljavec evropske kritične infrastrukture[42] zaradi neizpolnjevanja kriterijev, določenih z Uredbo o evropski kritični infrastrukturi[43].

ELES ima določeno število objektov kritične infrastrukture za prenos električne energije, ki jih je določil nosilec sektorja energetike. ELES ima tudi določeno število objektov kritične infrastrukture za informacijsko-komunikacijske sisteme in omrežja, ki jih je določil nosilec sektorja informacijsko-komunikacijskih omrežij in sistemov, kjer se nahaja tudi oprema drugih ponudnikov storitev oziroma so vozlišča za optične povezave. Pri teh objektih se kot kritična infrastruktura upoštevajo le prostori in infrastruktura za delovanje in zaščito prostorov brez upravljanja operativnega nivoja za izvajanje storitev.

1.3.3 Predstavitev revidiranca

ELES je bil ustanovljen maja 1996 kot javno podjetje Elektro-Slovenija, p. o.[44] Na podlagi prvega odstavka 72. člena Energetskega zakona[45] (v nadaljevanju: EZ-1) je vlada 24. 6. 2015 sprejela sklep[46] o imenovanju ELES za sistemskega operaterja[47] prenosnega sistema z električno energijo.

42 Evropska kritična infrastruktura obsega kritično infrastrukturo, ki se nahaja v državah članicah in katere okvara ali uničenje bi imelo resne posledice, ocenjene po medsektorskih merilih v vsaj 2 državah članicah.

43 Uradni list RS, št. 35/11.

44 Javno podjetje ELES, d.o.o. je nastalo s preoblikovanjem družbenega podjetja Elektro-Slovenija, p. o. v družbo z omejeno odgovornostjo na podlagi Uredbe o preoblikovanju Javnega podjetja Elektro-Slovenija, p. o. v Javno podjetje Elektro-Slovenija, d. o. o. (v nadaljevanju: akt o ustanovitvi; Uradni list RS, št. 28/96, 108/00, 44/01, 21/03, 63/05 in 54/07), na podlagi katere je Republika Slovenija ustanovitelj in edini lastnik javnega podjetja ELES, d.o.o.

45 Uradni list RS, št. 60/19 – uradno prečiščeno besedilo, 65/20 in 158/20 – ZURE.

46 Sklep o imenovanju sistemskega operaterja prenosnega sistema z električno energijo (Uradni list RS, št. 46/15).

47 Sistemski operater je pravna ali fizična oseba, ki opravlja dejavnost sistemskega operaterja prenosa električne energije in je odgovorna za obratovanje, vzdrževanje in razvoj na določenem območju, za medsebojne povezave z drugimi sistemi, kadar je ustrezno, in za zagotavljanje dolgoročne zmogljivosti sistema za zadovoljitev razumnih potreb po transportu električne energije (Triintrideseti odstavek 4. člena EZ-1).

Ustanovitelj in edini lastnik ELES je Republika Slovenija, ki izvršuje ustanoviteljske pravice prek vlade.

V skladu z aktom o ustanovitvi ELES upravljajo ustanovitelj, nadzorni svet in direktor, ki zastopa in predstavlja ELES. Delovanje in upravljanje ELES je organizirano na 3 ravneh. Organizacijska struktura poleg vodstva vključuje še 6 vodstvenih področij. Posledično poteka tudi funkcijsko odločanje na 3 ravneh: direktor družbe, direktorji področij/vodje služb v okviru vodstva družbe, vodje služb na področjih.

ELES je imel konec leta 2019 567 zaposlenih. Tabela 1 prikazuje podatke o zaposlenih v zadnjih 3 letih[48].

Tabela 1 Podatki o zaposlenih v letih od 2017 do 2019

Podatki o zaposlenih	2017	2018	2019
Število zaposlenih na dan 31. 12.	566	569	567
Povprečno število zaposlenih v letu	565	564	567
Povprečna starost	46 let	47 let	47 let
Povprečna delovna doba	22 let	22 let	23 let
Zaposleni za nedoločen čas	562	566	562
Zaposleni za določen čas	4	3	5
Zaposleni za polni delovni čas	564	567	565
Zaposleni za krajši delovni čas	2	2	2
Delež zaposlenih invalidov	3,7 %	3,5 %	3,4 %
Delež zaposlenih z najmanj visoko izobrazbo	54,2 %	56,4 %	58,0 %

Vir: letna poročila ELES za leta 2017, 2018 in 2019[49].

Odgovorna oseba za poslovanje ELES v obdobju, na katero se nanaša revizija, in med izvajanjem revizije je mag. Aleksander Mervar, direktor, ki je bil na mesto direktorja ELES imenovan 26. 10. 2013.

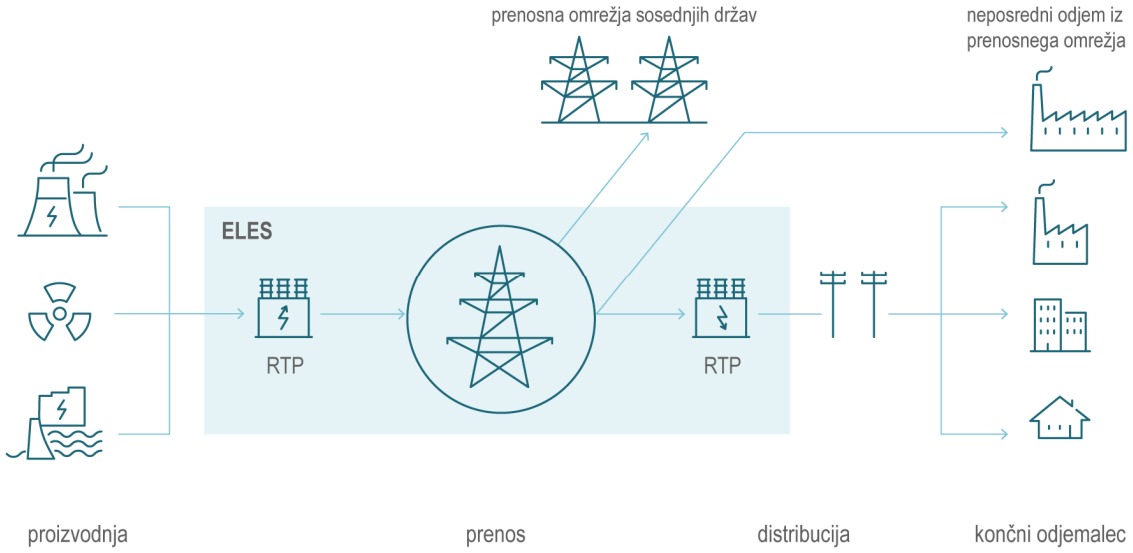
1.3.3.1 Prenos električne energije

ELES je pristojen tako za upravljanje kot za razvoj in vzdrževanje prenosnega omrežja, ki je del elektroenergetskega sistema (v nadaljevanju: EES) (Slika 1). Tega poleg prenosnega omrežja sestavljajo še omrežja neposrednih odjemalcev, distribucijska omrežja ter porabniki in proizvajalci. Tako je prenosno omrežje vezni člen med proizvodnjo in odjemom ter povezava z drugimi EES v Evropi.

48 V času priprave tega poročila letno poročilo ELES za leto 2020 še ni bilo na voljo.

49 [URL: https://www.eles.si/medijsko-sredisce/publikacije], 20. 8. 2021.

Slika 1 Položaj ELES v elektroenergetski verigi v Republiki Sloveniji



Opomba: RTP – razdelilna transformatorska postaja (v nadaljevanju: RTP).
Vir: povzeto po podatkih ELES[50].

ELES je polnopravni član Evropskega združenja sistemskih operaterjev elektroenergetskega omrežja (v nadaljevanju: ENTSO-E[51]).

ELES upravlja daljnovodno omrežje, ki je razpredeno po celotni državi in je imelo konec leta 2019, poleg upravne zgradbe in nekaterih drugih poslovnih lokacij, še 46 RTP (Slika 2) in 2.923 km daljnovodov (v nadaljevanju: DV) (Slika 3).[52] Nekateri objekti so v izključnem lastništvu družbe, drugi so v solastništvu z drugimi elektrogospodarskimi družbami.

50 Elektroenergetski sistem RS, ELES, 2019, strani 12–13, [URL: https://www.eles.si/Portals/0/Images/ELES_2019_Knjizica_Potni_list_Notranjost%20_2020-web.pdf], 20. 8. 2021.

51 Angl.: *European Network of Transmission System Operators*, [URL: https://www.entsoe.eu], 20. 8. 2021.

52 Letno poročilo družbe ELES za leto 2019, [URL: https://letnoporocilo2019.eles.si/wp-content/uploads/2020/11/ELES_LP2019.pdf], 20. 8. 2021.

Slika 2 Razdelilna transformatorska postaja

Vir: ELES, Letno poročilo družbe ELES za leto 2019, stran 33[53].

53 Tako kot opomba 52.

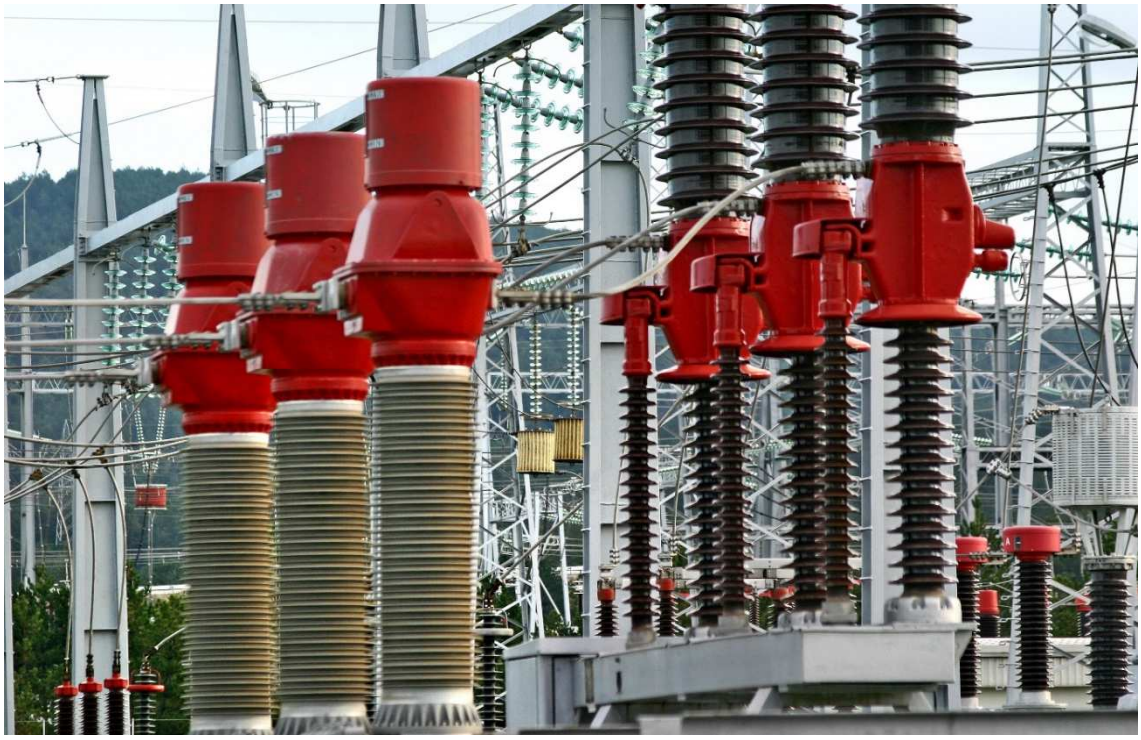
Slika 3 Daljnovoda

Vir: ELES, Letno poročilo družbe ELES za leto 2019, stran 101[54].

Preskrba z električno energijo obsega prenosni in distribucijski sistem ter tudi proizvodne enote – elektrarne (Slika 1). Hrbtenico oskrbe z elektriko predstavlja prenosni sistem, ki ga upravlja ELES in obsega omrežje z napetostjo 400 kV, 220 kV in del omrežja z napetostjo 110 kV s pripadajočimi postajami, v katerih se električni vodi povezujejo med seboj ter z distribucijskim sistemom, končnimi odjemalci, neposrednimi odjemi iz prenosnega omrežja in proizvodnjo. Omrežja različnih napetosti so med seboj povezana prek transformatorjev (Slika 4).

54 Tako kot opomba 52.

Slika 4 Transformator



Vir: ELES, Letno poročilo družbe ELES za leto 2018, stran 76[55].

Poglavitna naloga prenosnega sistema je zagotavljanje napajanja RTP, iz katerih se napaja distribucijsko elektroenergetsko omrežje in posamezni neposredni odjemalci iz prenosnega omrežja. Od tega je odvisna oskrba velikega števila končnih odjemalcev ali posameznih neposrednih odjemalcev iz prenosnega omrežja. Distribucijsko omrežje običajno omogoča preklop napajanja odjemalcev iz ene RTP na sosednjo RTP, v tako imenovano rezervno stanje. Takšen preklop lahko traja nekaj časa, vendar pa ni mogoč za vse končne odjemalce. Pri preklopu se lahko zmanjša kakovost oskrbe odjemalcev (na primer, zmanjša se napetost).

Zaradi zanesljivosti napajanja je prenosni sistem zasnovan na kriteriju n-1[56]. To pomeni, da izpad kateregakoli posameznega elementa sistema še ne povzroči izpada napajanja odjemalcev. Vse napajalne poti prenosnega sistema so najmanj podvojene, razen v nekaj izjemnih primerih, kjer to ni mogoče.

Za zanesljivo napajanje RTP je ključno ohranjanje celovitosti prenosnega sistema, za kar niso potrebni le fizični elementi, ampak tudi izvajanje storitev: vodenje sistema, sistemske storitve, pripravljenost za hitra popravila (ekipe, material, havarijski stebri[57] in podobno). Poleg zagotavljanja

55 [URL: https://letnoporocilo2018.eles.si/wp-content/uploads/2019/10/ELES_LP2018_interaktivno.pdf], 20. 8. 2021.

56 Kriterij n-1 je osnovni kriterij zanesljivosti, ki zagotavlja, da ob izpadu kateregakoli posameznega elementa v EES ne pride do preobremenitev elektroenergetske naprave ali težav z zanesljivostjo obratovanja sistema, [URL: https://www.eles.si/medijsko-sredisce/slovar-izrazov-in-kratic/slovar-izrazov], 20. 8. 2021.

57 Poseben montažni steber, ki omogoča začasno izvedbo daljnovodnih povezav v primeru poškodb.

razpoložljivosti elementov sistema in storitev je pomembna tudi zasnova sistema: kriterij n-1, zazankanost[58], ustrezen koncept zaščit, rezerva regulacijske delovne in jalove moči ter rezervni center vodenja.

Stoodstotnega neprekinjenega napajana z električno energijo ni mogoče zagotoviti pod nobenimi pogoji. Odjemalci, ki nujno potrebujejo neprekinjeno napajanje vsaj za nekatere funkcije (računalniški sistemi, prezračevanje, operacijske sobe in sistemi za ohranjanje življenjskih funkcij v bolnišnicah in podobno), si morajo za nujne funkcije sami zagotoviti rezervne sisteme napajanja (baterije, agregati). Ostali odjemalci praviloma lahko brez večjih posledic prenesejo do nekajurne prekinitve napajanja.

ELES je izvajalec obvezne gospodarske javne službe in mu je podeljena izključna pravica opravljati dejavnost sistemskega operaterja[59], ki vključuje:

- varno, zanesljivo in učinkovito obratovanje in vzdrževanje prenosnega sistema;
- razvoj sistema (upoštevanje potreb, varnosti);
- zagotavljanje dolgoročne zmogljivosti prenosnega sistema;
- upravljanje pretokov električne energije v prenosnem sistemu in zagotavljanje sistemskih storitev;
- izravnavo odstopanj v sistemu;
- posredovanje informacij drugemu operaterju;
- zagotavljanje podatkov uporabnikom sistema in dobaviteljem;
- nediskriminatorno obravnavo uporabnikov in dobaviteljev;
- napoved porabe elektrike ter potrebnih energetskih virov;
- pobiranje plačil med upravljavci prenosnih omrežij;
- nakup elektrike za pokritje izgub v prenosnem sistemu in nakup sistemskih storitev;
- zagotavljanje kakovosti oskrbe v skladu z minimalnimi standardi.

ELES je kot izvajalec obvezne gospodarske javne službe sistemskega operaterja prenosa električne energije izdal Sistemska obratovalna navodila za prenosni sistem električne energije Republike Slovenije[60] (v nadaljevanju: SONPO), ki urejajo obratovanje in način vodenja prenosnih sistemov. Zagotavljati morajo zmožnost skupnega delovanja sistemov ter biti pregledna, objektivna in nediskriminatorna. Urejajo zlasti:

- tehnične in druge pogoje za zanesljivo in varno obratovanje prenosnega sistema;
- vrsto, strukturo, frekvenco in način izmenjave podatkov med elektrooperaterji;
- tehnične zahteve ter pogoje za priključitev uporabnikov sistema in distribucijskega operaterja na prenosni sistem;

58 EES je zasnovan tako, da je v vsakem primeru omogočenih več napajalnih poti.

59 54. člen EZ-1 in 4. člen Uredbe o podelitvi koncesije in načinu izvajanja gospodarske javne službe dejavnost sistemskega operaterja prenosa električne energije – koncesijski akt (Uradni list RS, št. 46/15).

60 Uradni list RS, št. 29/16.

- postopke pri motenem obratovanju prenosnega sistema;
- način zagotavljanja sistemskih storitev;
- tehnične pogoje za medsebojno priključitev in delovanje sistemov različnih sistemskih operaterjev;
- postopke za obratovanje sistemov v kriznih stanjih;
- monitoring kakovosti oskrbe z električno energijo;
- stroške tehničnih ukrepov, ki so potrebni za priključitev novih proizvajalcev elektrike.

ELES je kot sistemski operater zadolžen za varno, zanesljivo ter učinkovito obratovanje in vzdrževanje prenosnega sistema. V ta namen načrtuje in operativno vodi obratovanje EES, upravlja pretoke, zagotavlja sistemske storitve, izvaja izravnavo odstopanj od načrtovanih vrednosti, pokriva izgube, ki nastanejo v prenosnem omrežju, in po potrebi razbremenjuje omrežje.[61]

Sistemski operater v republiškem centru vodenja izvaja vodenje obratovanja, ki zajema izvajanje načrtovanih preklopov in ukrepov ob nastopu motenj s ciljem zagotavljanja kakovostnega in zanesljivega obratovanja[62]. Obratovanje prenosnega sistema je lahko[63]:

- normalno: obratovanje ob izpolnjevanju kriterija n-1[64];
- moteno: stanje pripravljenosti[65] (nezanesljivo stanje, ko ni na razpolago zadostnega obsega sistemskih storitev, da bi bilo po posameznem izpadu elementa sistema možno ponovno vzpostaviti normalno obratovanje), krizno stanje (stanje, ko ni na razpolago minimalnega obsega sistemskih storitev oziroma ni izpolnjen kriterij n-1, tako da lahko posamezni izpad privede do širjenja motnje izven slovenskega EES, kaskadnih izpadov, izgube stabilnosti, delnega ali celotnega razpada sistema), stanje razpadanja (stanje izpada vodov zaradi preobremenitev, proizvodnih enot pa zaradi izpada vodov, prenizke frekvence ali napetosti, s posameznimi delujočimi deli sistema) in stanje vzpostavljanja (stanje povezovanja elementov sistema s ciljem hitre obnove zanesljivega obratovanja).

Sistemski operater je odgovoren in pooblaščen, da z ustreznimi ukrepi prepreči širitev motenj in ob nastopu motenega obratovanja v najkrajšem možnem času vzpostavi normalno obratovalno stanje. V ta namen pripravi načrt ukrepov za primer nastopa motenega obratovanja in si zagotovi ustrezno število proizvodnih enot za namene otočnega obratovanja[66] ter ustrezno število proizvodnih enot s sposobnostjo zagona agregata brez zunanjega vira napajanja.[67]

61 46. člen SONPO.

62 88. člen SONPO.

63 Presoja, ali je stanje sistema normalno ali moteno, je v pristojnosti sistemskega operaterja.

64 91. člen SONPO.

65 94. člen SONPO.

66 Obratovanje dela sistema, ki je po razpadu sistema začasno ločen od preostalega elektroenergetskega sistema. Obsega lahko enega ali več izvorov energije in enega ali več odjemalcev. [URL: https://www.eles.si/medijsko-sredisce/slovar-izrazov-in-kratic/slovar-izrazov], 20. 8. 2021.

67 95. člen SONPO.

1.3.3.2 Informacijsko-komunikacijska tehnologija in storitve

Poleg energetske infrastrukture so pomemben funkcionalni del prenosnega omrežja tudi telekomunikacijska infrastruktura in omrežja, ki so kot podporni sistem primarno namenjeni izvajanju zanesljivih in varnih storitev za potrebe vodenja prenosnega elektroenergetskega omrežja Republike Slovenije in za kakovostno obvladovanje poslovnih procesov v ELES, sekundarno, torej kot viški kapacitet, pa tudi trženju.

ELES ne zagotavlja javnega komunikacijskega omrežja in nima statusa operaterja omrežja po Zakonu o elektronskih komunikacijah[68]. Namenska komunikacijska omrežja v EES se namreč razlikujejo od klasičnih komunikacijskih omrežij, in sicer morajo izpolnjevati posebne zahteve in višje standarde za potrebe obratovanja EES:

- storitve za vodenje morajo biti visoko razpoložljive;
- zveze za zaščito morajo izpolnjevati kratke zakasnilne čase;
- poslovne komunikacije med posameznimi poslovnimi lokacijami družbe potrebujejo velike kapacitete;
- omogočen mora biti daljinski nadzor posameznih procesnih naprav in
- izpolnjena mora biti zahteva po veliki varnosti in zaščiti omrežij.

Zaradi navedenega so vse naprave informacijsko-komunikacijske tehnologije v EES modularne izgradnje s podvojenimi vitalnimi funkcijami in daljinsko nadzorovane. Zveze so zaščitene in pri izpadu primarne poti omogočajo samodejno preusmeritev na drugo razpoložljivo povezavo, internetna omrežja pa imajo dodatne mehanizme za zaščito.

ELES ima 1.600 km fizičnih optičnih povezav, ki so umeščene v strelovodne vrvi DV. Povezave so vzpostavljene z vsemi elektroenergetskimi objekti prenosnega omrežja v Republiki Sloveniji kot tudi z večino imetnikov optične infrastrukture v Republiki Sloveniji, kar omogoča 2 poti dostopa do posameznega energetskega objekta. V primerih, kjer to ni vzpostavljeno, so nameščene brezžične širokopasovne povezave. Na optičnih povezavah je nameščeno več transportnih telekomunikacijskih sistemov, ki so namenjeni različnim uporabnikom, pri čemer povezave potekajo prek sistemov, ki so nameščeni v sistemskih prostorih. ELES ima tudi druge kapacitete, ki mu zagotavljajo neodvisne in redundatne storitve za potrebe obratovanja EES.

Informacijski sistem ELES se deli na 3 področja: področje poslovnega omrežja, področje tehničnega (prenosnega) omrežja in področje oddaljenih enot. Zaradi varnostnih zahtev sta področji poslovnega omrežja in tehničnega omrežja ločeni.

68 Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17.

1.3.3.3 Kibernetska varnost

ELES je identificiral kibernetsko varnost v strateških izzivih, objavljenih v letnem poročilu 2019[69], kakor tudi v razvojnih načrtih za področje sistemov vodenja in nadzora EES[70] in razvojnih usmeritvah informacijskih storitev. ELES namerava v okviru projekta servisnega varnostno-operativnega centra[71] (v nadaljevanju: VOC) vzpostaviti celovit pristop k zagotavljanju kibernetske varnosti v elektroenergetski domeni ter integriranih sistemih informacijske tehnologije (v nadaljevanju: IT) in operativne tehnologije[72].

1.4 Cilj revizije in revizijski pristop

Cilj revizije je bil izrek mnenja o učinkovitosti ELES pri upravljanju kibernetske varnosti za področje kritične infrastrukture v obdobju, na katero se nanaša revizija.

Da bi lahko izrekli mnenje, smo si zastavili glavno revizijsko vprašanje, **ali je ELES učinkovito upravljal kibernetsko varnost na področju kritične infrastrukture.**

Odgovor na glavno revizijsko vprašanje smo pridobili z odgovori na naslednja podvprašanja:

- **ali je ELES učinkovito implementiral zahteve zakonodaje na področju kritične infrastrukture;**
- **ali je ELES učinkovito upravljal zaznavanje kibernetskih groženj;**
- **ali je ELES učinkovito upravljal odzivanje na kibernetske grožnje.**

Odgovore na revizijska vprašanja smo pridobili pri ELES. Uporabili smo različne kvalitativne in kvantitativne metode in tehnike revidiranja, kot so:

- proučevanje pravnih in drugih podlag, ki opredeljujejo kritično infrastrukturo;
- proučevanje pravnih in drugih podlag, ki opredeljujejo pripravo dokumentov načrtovanja zaščite kritične infrastrukture;
- zbiranje, pregled in presoja dokumentacije o upravljanju kritične infrastrukture (zlasti internih dokumentov, ki urejajo oceno tveganj za delovanje kritične infrastrukture in upravljanje ukrepov);
- razgovori s pristojnimi predstavniki revidiranca;
- obiski lokacij, kjer se izvajajo aktivnosti, povezane z upravljanjem kritične infrastrukture;
- pisna vprašanja revidirancu.

---

69 Tako kot opomba 52.

70 Razvojni načrt prenosnega sistema Republike Slovenije 2019–2028, ELES, [URL: https://www.eles.si/Portals/0/Documents/ELES-razvojni-nacrt-2019-2028.pdf], 9. 8. 2021.

71 Angl.: *SOC – Security Operations Center*.

72 Angl.: *Operational Technology*.

2. Upravljanje kritične infrastrukture na ELES

2.1 Implementacija zahtev zakonodaje na področju kritične infrastrukture

2.1.1 Sodila

Za presojo **učinkovitosti ELES pri implementaciji zahtev zakonodaje na področju kritične infrastrukture** smo uporabili določila ZKI s pripadajočimi podzakonskimi akti (navodilo za ocenjevanje tveganj in strokovne usmeritve nosilcev sektorjev kritične infrastrukture).

2.1.2 Opis stanja

ELES je bil v obdobju, na katero se nanaša revizija, upravljavec kritične infrastrukture in je moral v zakonskih rokih implementirati in upravljati zahteve, ki so bile za upravljavce kritične infrastrukture opredeljene v ZKI in pripadajočih aktih.

ELES je imel v obdobju, na katero se nanaša revizija, vzpostavljene politike za vse segmente integriranega sistema upravljanja, ki se s pomočjo mehanizmov vodstvenega pregleda redno pregledujejo in ustrezno dopolnjujejo. Politike integriranega sistema upravljanja sestavljajo:

- politika upravljanja družbe ELES;
- politika trajnostnega razvoja;
- politika kakovosti in odličnosti;
- politika upravljanja tveganj;
- politika upravljanja sredstev;
- politika ravnanja z okoljem;
- politika varovanja informacij;
- politika varnosti in zdravja pri delu;
- kadrovska politika;
- politika komuniciranja in druge poslovne politike.[73]

ELES je uvedel obvladovanje tveganj v letu 2009. V nadaljnjih letih je vzpostavil celovit sistem upravljanja tveganj, ki skupaj z vzpostavljenim notranjim kontrolnim sistemom ostaja ključni del integriranega sistema upravljanja družbe, ki naj bi ELES omogočal obvladovanje tveganj in s tem

[73] [URL: https://www.eles.si/politike-upravljanja], 20. 8. 2021.

varno in donosno izvajanje njegove osnovne dejavnosti.[74] Pri vodstvu ELES je kot organizacijska enota oblikovana služba za sisteme upravljanja, ki med drugim tudi centralno upravlja z obvladovanjem tveganj po posameznih področjih. Obvladovanje tveganj je ELES utemeljil na podlagi standarda SIST[75] ISO 31000:2011[76].

Upravljanje tveganj v ELES temelji na procesnem modelu – tveganja v posameznih procesih. Direktor ELES s pomočjo koordinatorja direktorja za upravljanje s tveganji in koordinatorja direktorja za sisteme upravljanja zagotavlja organizacijski okvir za obvladovanje tveganj in vire za obvladovanje tveganj. ELES tveganja deli na:

- strateška tveganja,
- procesna tveganja,
- tveganja po delovnih tokovih,
- projektna tveganja,
- tveganja kritične infrastrukture,
- tveganja v sistemu varovanja informacij ter
- tveganja varnosti in zdravja pri delu.

Sama struktura tveganj je povezana z zunanjim in notranjim kontekstom delovanja ELES. Kontekst delovanja ELES se nanaša na tisto zunanje in notranje okolje in druge parametre, s katerimi si ELES prizadeva doseči svoje cilje, to pa je lahko vse, kar vpliva na način obravnave tveganj. Odgovorni na ELES najmanj 1-krat letno proučijo zunanji in notranji kontekst delovanja v svojih procesih.

Proces upravljanja tveganj na ELES je sestavljen iz:

- prepoznavanja tveganj,
- analiziranja tveganj,
- ovrednotenja tveganj,
- izbire najbolj ustrezne obravnave tveganj,
- analiziranja in ovrednotenja preostale ravni tveganj,
- izvajanja ukrepov,
- obravnavanja uresničenih tveganj,
- nadzorovanja in pregledovanja obvladovanja tveganj.

Pri oceni tveganj ELES uporablja kvalitativno lestvico za ocenjevanje tveganj z 2 parametroma: obseg škode, ki nastane ob tveganju, in pogostost tveganja. Ocena tveganja je zmnožek ocene obsega škode in pogostosti. Ocena tveganja se lahko giblje med 1 – najmanjše tveganje in 25 – največje tveganje.

74 Tako kot opomba 52.

75 Slovenski inštitut za standardizacijo.

76 Obvladovanje tveganja – Načela in smernice (angl.: *Risk management – Principles and guidelines*), po ISO 31000:2011.

ELES vodi katalog tveganj tudi po področjih poslovanja, in sicer:

- tveganja vodenje družbe,
- tveganja upravljanja s sredstvi in projekti,
- tveganja obratovanja sistema,
- tveganja infrastrukture prenosnega omrežja,
- tveganja podpornih dejavnosti,
- tveganja poslovne informatike in telekomunikacij,
- tveganja varovanja informacij,
- tveganja strateških inovacij in
- okoljska tveganja.

ELES prepoznava in evidentira tveganja tudi na podlagi vzrokov, ki ogrožajo doseganje ciljev in delovanje procesov. ELES vodi informatiziran katalog tveganj, kjer so opredeljena ključna tveganja, ki jih skrbniki dodatno kvantificirajo. Vsako leto ELES izda tudi povzetek iz kataloga tveganj za tekoče leto, kjer so opisno predstavljena pomembna tveganja in spremembe, nastale v zadnjem obdobju.

ELES ima svet za sisteme upravljanja, ki med drugim:

- določa cilje, strategije in druge parametre aktivnosti obvladovanja tveganj;
- odloča o obsegu, globini in metodologijah obravnave tveganj;
- nadzoruje upravičenje virov za obvladovanje tveganj in
- določa način vrednotenja uspešnosti obvladovanja tveganj.

Svet za sisteme upravljanja redno letno sprejme merila tveganja in določi sprejemljivost tveganj, to pomeni mejne vrednosti ocenjenih tveganj, ki so še sprejemljive za svet. Leta 2018 je svet mejo tveganj dvignili z 8 na 10 – ob pogoju, da ocena obsega škode ne dosega ocene 4 ali 5.

ZKI določa, da je ocena tveganj za delovanje kritične infrastrukture rezultat celovitega postopka identifikacije, analize in ovrednotenja različnih virov tveganj za delovanje kritične infrastrukture. Pomembno vodilo za pripravo ocene tveganj ELES so predstavljale strokovne usmeritve MO in ZKI, saj je bila ne nazadnje na tej podlagi prepoznana kritična infrastruktura ELES, dodatno vodilo za pripravo ocene tveganj ELES pa so predstavljale usmeritve nosilcev sektorjev kritične infrastrukture – MJU in MZI.

2.1.3 Ugotovitve glede skladnosti

ELES je na podlagi ZKI, usmeritev MO, strokovnih usmeritev nosilcev sektorja kritične infrastrukture in lastne metodologije ocenjevanja tveganj izvedel dejavnosti, ki so opisane v nadaljevanju.

2.1.3.a Identifikacija virov tveganj za delovanje kritične infrastrukture

V okviru ocene tveganja za delovanje kritične infrastrukture je januarja 2020 ELES pravočasno pripravil dokument načrtovanja zaščite kritične infrastrukture ter v njem navedel seznam identificiranih tveganj za posamezno kritično infrastrukturo, vključno s tistimi vrstami tveganj, ki

vplivajo na kritično infrastrukturo. Iz kataloga vseh tveganj so bila navedena tudi posamezna identificirana tveganja za področje upravljanja kritične infrastrukture.

Ocenjujemo, da je ELES realiziral zahtevi iz 7. člena navodila za ocenjevanje tveganj.

2.1.3.b Analiza in ovrednotenje tveganj za delovanje kritične infrastrukture

ELES je izvedel analizo in ovrednotenje tveganj in jih dokumentiral v navedenih dokumentih ocene tveganj za delovanje kritične infrastrukture, izdelal opisno analizo in ovrednotenje virov tveganja za delovanje kritične infrastrukture, kjer je med drugim opredelil verjetnost uresničitve vira tveganj, resnost potencialne škode, nastale zaradi uresničitve vira tveganj, ter potencialne vplive uresničitve vira tveganj na poslovne procese.

Ocenjujemo, da je ELES realiziral zahteve iz prvega odstavka 8. člena navodila za ocenjevanje tveganj.

2.1.3.c Določitev virov tveganj, ki lahko povzročijo izredni dogodek

ELES je v navedenih dokumentih ocene tveganj za delovanje kritične infrastrukture pripravil tudi tabele, kjer je opredelil vire tveganj, ki lahko povzročijo izredni dogodek pri delovanju kritične infrastrukture. Identificiranih je bilo skupaj 70 virov tveganja (43 virov tveganj na prenosu električne energije in 27 virov tveganj na področju sistemskih prostorov).

Ocenjujemo, da je ELES realiziral zahteve iz drugega odstavka 8. člena navodila za ocenjevanje tveganj.

2.1.3.d Spremljanje stanja kritične infrastrukture

ELES za prenos električne energije izvaja osnovno merilo za obratovanje, ki temelji na kriteriju n-1. Samo načrtovanje in operativno vodenje prenosnega sistema je podrobno opisano v organizacijskem predpisu s pripadajočimi internimi dokumenti. V primeru izpada posameznih povezav ima ELES vpeljan sistem otočnega obratovanja. V primeru izpada posameznega centra vodenja njegovo delovanje prevzame drug center vodenja. Za nemoteno komunikacijo med območnimi centri vodenja (v nadaljevanju: OCV) in posameznimi objekti kritične infrastrukture ima ELES podvojene telekomunikacijske povezave.

ELES že več let rešuje težavo zazankanosti ob možnem izpadu povezave DV Divača–Ajdovščina in ob potencialnih težavah s preskrbo severne Primorske z električno energijo. Predvidena je bila vzpostavitev alternativne povezave s posodobitvijo DV, ki ga je Republika Italija zgradila že pred drugo svetovno vojno[77], a se lokalna skupnost že vrsto let ne strinja z načrtovano posodobitvijo. Možnost vzpostavitve omejene alternativne povezave z delom severne Primorske je tudi v nadgradnji havarijske povezave DV Logatec–Idrija, ki je v pripravi.

[77] Tako imenovani Kraški daljnovod.

Ukrep ELES

ELES je skupaj z Elektro Ljubljana oktobra 2020 uskladil navodila za havarijsko povezavo DV Idrija–Logatec.

ELES je za oceno stanja kritične infrastrukture uporabil tudi storitev Geodetske uprave Republike Slovenije in MO glede ocene odpornosti stavb pred potresi za 3 objekte.

Vsi objekti kritične infrastrukture imajo sisteme za neprekinjeno delovanje v primeru izpada električne energije. Ob izpadu na večini lokacij za napajanje naprav z električno energijo poskrbi brezprekinitveni sistem napajanja[78], ki po 15 s vključi dizelske agregate, ki so vključeni v tako imenovano terciarno rezervo. VOC ima med drugim tudi nadzor nad sistemi brezprekinitvenih napajanj v sistemskih prostorih, ki so na lokacijah RTP.

Poleg nadzora nad sistemi brezprekinitvenih napajanj se v VOC izvaja nadzor pristopnih kontrol (več v točki 2.2.3.g) za vse lokacije ter tudi nadzor nad temperaturo in gibanjem v sistemskih prostorih. V vseh prostorih so javljalniki požara, njihov signal pa se prenaša tako v VOC kakor tudi v varnostno-nadzorni center (v nadaljevanju: VNC) pri varnostni organizaciji, s katero ima ELES pogodbo o fizičnem varovanju, v skladu s katero je zagotovljena intervencija 24/7/365[79]. V 2 objektih je nameščen avtomatski sistem gašenja požara s plinom inergen[80], tak sistem gašenja pa se načrtuje tudi pri novih objektih.

Ocenjujemo, da ELES spremlja stanje kritične infrastrukture.

2.1.3.e Podvojenost centrov vodenja

ELES je imel podvojene centre vodenja tako za osnovne dejavnosti kot tudi za kontrolo delovanja sistemskih prostorov. Vsak od 3 OCV lahko prevzame nadzor nad drugimi OCV oziroma nad vodenjem celotnega prenosa električne energije.

ELES je v decembru 2011 pričel z gradnjo novega sodobnega rezervnega centra vodenja in jo zaključil septembra 2017.

Priporočilo

ELES priporočamo, naj občasno izvaja upravljanje prenosa električne energije iz rezervnega centra vodenja.

ELES je leta 2019 vzpostavil lasten VOC, podvojenost tega centra pa je zagotavljal pri zunanjem izvajalcu. ELES je večino delovanja informacijskih sistemov in podpornih storitev nadziral iz lastnega nadzornega centra delovanja IT (v nadaljevanju: storitveni center IKT). Le za nadzor delovanja nad baterijami in sistemi brezprekinitvenega napajanja za sistemske prostore informacijsko-komunikacijske

78 Angl.: *Uninterruptible Power Supply*.

79 24 ur na dan, 7 dni na teden in vse dni v letu.

80 Inergen je plinska mešanica, ki jo sestavljajo dušik, argon in ogljikov dioksid in preprečuje gorenje. Gre za pline, ki so sicer prisotni tudi v naravi, zato mešanica nima nobenega škodljivega vpliva na okolje.

tehnologije (v nadaljevanju: IKT) je bila v času izvajanja revizije še vedno pristojna ena izmed služb IT. ELES načrtuje, da bo tudi ta nadzor centraliziral v storitveni center IKT.

Ukrep ELES

ELES je v sklopu ocenjevanja tveganj ugotovil, da sistem nadzora nad napajalnimi sistemi teče na fizičnem strežniku, ki ni bil podvojen. Po analizi stanja in ocenjevanju možnih rešitev se je odločili, da sistem preseli na virtualno strežniško okolje, ki je postavljeno na 2 lokacijah. Nadzorni sistem za napajalne sisteme je bil skupaj z zbirko podatkov preseljen na virtualno okolje konec aprila 2021. Testirano je bilo delovanje sistema, stari fizični strežnik pa umaknjen iz produkcije. Z novo postavitvijo sistema je ELES dosegel, da v primeru izpada ene izmed lokacij, kjer se izvaja ta storitev, storitev nadzora nad napajalnimi sistemi še vedno deluje ter ne bo potrebe po ročnem upravljanju napajalnih sistemov.

ELES nadzorov storitvenih servisov brezprekinitvenega napajanja kakor tudi lokalnih nadzornih central na posameznih objektih ni imel podvojenih. Po pojasnilih ELES lahko sistem nadzora deluje tudi brez podvojitev, saj je mogoče v primeru izpada posameznih komponent nadzornih central sistem upravljati ročno.

Ocenjujemo, da je ELES realiziral zahtevo po podvojenosti centrov vodenja iz posredovanih smernic nosilca kritične infrastrukture[81].

2.1.3.f Izdelava varnostnih načrtov

ELES je imel konec januarja 2020 za vse objekte, ki so bili določeni kot kritična infrastruktura, izdelane varnostne načrte. ELES mora pri varovanju sredstev upoštevati tudi vrsto drugih zakonov in predpisov[82]. ELES je imel zato izdelan tudi obrambni načrt na podlagi Zakona o obrambi[83] in Uredbe o obrambnem načrtovanju[84].

Ocenjujemo, da je ELES realiziral zahtevo po izdelavi varnostnih načrtov iz posredovanih smernic nosilca kritične infrastrukture.

81 4. točka smernic MZI.

82 Zakon o zasebnem varovanju (v nadaljevanju: ZZasV-1; Uradni list RS, št. 17/11), Uredba o obveznem organiziranju varovanja (Uradni list RS, št. 80/12), Zakon o varstvu pred naravnimi in drugimi nesrečami (Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 97/10 in 21/18 – ZNOrg), Uredba o vsebini in izdelavi načrtov zaščite in reševanja (Uradni list RS, št. 24/12, 78/16 in 26/19), Uredba o organizaciji in delovanju sistema opazovanja, obveščanja in alarmiranja (Uradni list RS, št. 105/07), Navodilo o pripravi ocen ogroženosti (Uradni list RS, št. 39/95), Pravilnik o obveščanju in poročanju v sistemu varstva pred naravnimi in drugimi nesrečami (Uradni list RS, št. 26/08, 28/12 in 42/12), Uredba o organiziranju, opremljanju in usposabljanju sil za zaščito, reševanje in pomoč (Uradni list RS, št. 92/07, 54/09, 23/11 in 27/16).

83 Uradni list RS, št. 103/04 – uradno prečiščeno besedilo in 95/15.

84 Uradni list RS, št. 51/13.

2.1.3.g Dokumentiran sistem upravljanja varovanja informacij in sistem upravljanja neprekinjenega poslovanja

ELES ima vzpostavljen sistem upravljanja za različne sisteme, med drugim tudi za sistem upravljanja varovanja informacij (v nadaljevanju: SUVI). ELES v povezavi s področjem revizije ima oziroma je v preteklosti pridobil različne certifikate: BS OHSAS 18001:2007, ISO 14001:2015, ISO 9001:2015 in ISO/IEC 27001:2013[85].

Certifikat ISO/IEC 27001:2005 so na ELES pridobili 19. 7. 2012 in ga nato nadgradili v ISO/IEC 27001:2013. Zadnjo recertifikacijo ISO/IEC 27001:2013 so izvedli 28. 5. 2018. Sama certifikacija pomeni, da ima ELES implementiran SUVI.

ELES je imel načrte neprekinjenega poslovanja za posamezna področja delovanja. V krovni varnostni politiki, ki je bila sprejeta v februarju 2020[86], opredeljuje, da sta ključnega pomena sistemska umestitev neprekinjenega poslovanja in zagotavljanje storitev. V letu 2019 je ELES zaradi zahtev ZInfV pristopil k pripravi dokumentov sistema upravljanja neprekinjenega poslovanja (v nadaljevanju: SUNP). Ob koncu obdobja, na katero se nanaša revizija, so bili novi načrti neprekinjenega poslovanja in načrti okrevanja ter drugi zahtevani dokumenti v fazi zaključevanja. V sklopu izdelave načrtov skladno s Pravilnikom o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev je bila v izdelavi tudi analiza vpliva na poslovanje.

Obstoječi dokumenti neprekinjenega poslovanja so bili pripravljeni na podlagi dobrih praks za upravljanje IT (ITIL[87]).

Ocenjujemo, da ima ELES vpeljan in dokumentiran SUVI. ELES do konca obdobja, na katero se nanaša revizija še ni vzpostavil SUNP.

Ukrep ELES

ELES je v januarju 2021 sprejel vrsto dokumentov za upravljanje neprekinjenega poslovanja[88]. ELES je zaradi vpeljave SUNP posodobil tudi interne dokumente neprekinjenega delovanja in okrevanja IT ter upravljanja informacijskih varnostnih incidentov, kar je potrdil tudi inšpekcijski nadzor Uprave Republike Slovenije za informacijsko varnost v januarju in aprilu 2021. Ugotovitev inšpektorja je bila, da izvajalec bistvenih storitev (ELES) izpolnjuje svoje obveznosti iz ZInfV in predpisov, izdanih na njegovi podlagi.

2.1.3.h Oceni tveganj in ukrepi za zaščito kritične infrastrukture

ELES je že v preteklosti ocenjeval tveganja (več v točki 2.1.3.i), sprejel je vrsto dokumentov, ki so opredeljevali ukrepe in postopke upravljanja prenosa električne energije in upravljanja sistemskih prostorov. ELES je oceni tveganj za delovanje kritične infrastrukture in pripadajoče ukrepe za zaščito

85 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve.

86 ELES, Krovna varnostna politika, 1. izdaja, z dne 1. 2. 2020.

87 Angl.: *Information Technology Infrastructure Library*.

88 Gre za 10 dokumentov, ki imajo naravo organizacijskega predpisa, opisa procesa, načrta ali navodila in se nanašajo na upravljanje neprekinjenega poslovanja bistvenih storitev ELES ali njegovih služb ter na načrte okrevanja pomembnih sistemov vodenja.

kritične infrastrukture pripravil v skladu z navodili nosilcev sektorjev kritične infrastrukture, saj je v ocenah navedel:

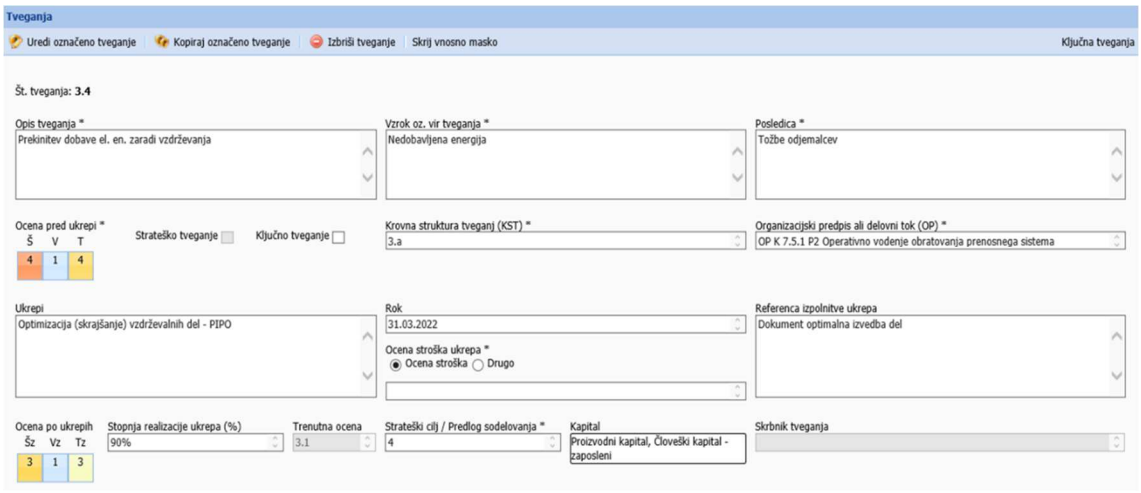
- opis stanja kritične infrastrukture v razmerah rednega delovanja, kjer je opredelil:
  - poslanstvo in temeljne naloge upravljavca kritične infrastrukture za delovanje sektorja kritične infrastrukture,
  - tehnološke in materialno-tehnične zmogljivosti za izvajanje poslanstva in temeljnih nalog kritične infrastrukture,
  - kadrovske zmogljivosti za izvajanje poslanstva in temeljnih nalog kritične infrastrukture,
  - finančne vire za izvajanje poslanstva in temeljnih nalog kritične infrastrukture,
  - druge zmogljivosti za izvajanje poslanstva in temeljnih nalog kritične infrastrukture;
- seznam identificiranih virov tveganj za delovanje kritične infrastrukture, kjer je:
  - identificiral različne vire tveganj na podlagi možnih groženj in vplivov na delovanje kritične infrastrukture,
  - vpisal vire tveganj v seznam identificiranih virov tveganj za delovanje kritične infrastrukture;
- opisno analizo in ovrednotenje virov tveganj za delovanje kritične infrastrukture, kjer je:
  - izdelal opisno analizo identificiranih virov tveganj,
  - ovrednotil in določil tiste vire tveganj, ki lahko povzročijo izredni dogodek pri delovanju kritične infrastrukture ali krizo.

Ocenjujemo, da je ELES v obeh ocenah vključil tveganja in ukrepe za zaščito kritične infrastrukture, kot sta to zahtevala nosilca sektorjev.

2.1.3.i Ocena tveganj za delovanje kritične infrastrukture

ELES je letu 2009 začel sistematično upravljati tveganja. Tveganja je sprva vodil s pomočjo preglednic, leta 2014 pa je pridobil informacijsko rešitev SilverBulletRisk (v nadaljevanju: SBR), ki jo je moral najprej prilagoditi za svoje procese. V aprilu 2016 je ELES začel informacijsko rešitev SBR uporabljati tudi pri vseh ocenjevanjih tveganj. Slika 5 prikazuje primer tveganja, zabeleženega v informacijski rešitvi SBR.

Slika 5 Prikaz tveganja v informacijski rešitvi SBR



Vir: podatki ELES.

Pooblastila za dostop in upravljanje informacijske rešitve SBR imajo skrbniki tveganj, sponzorji tveganj in člani tima za tveganja, ki ga sestavljajo člani vseh področij. Informacijska rešitev SBR temelji na scenarijih tveganj[89], ki jih ELES upravlja, dopolnjuje in zaključi po vsakem četrtletju.

Člani tima za tveganja v svojih sredinah skupaj s skrbniki tveganj redno upravljajo tveganja. Najmanj 2-krat letno pregledajo in posodobijo tveganja. V marcu izvedejo redno letno posodobitev celotnega kataloga tveganj, v septembru pa izvedejo meritev napredka pri obvladovanju tveganj. V skupini procesnih tveganj v okviru scenarija tveganj za obdobje april–junij 2020 je bilo tako na primer navedenih 476 tveganj, od tega je bilo 10 % tveganj, ki so imela identificirane ukrepe v implementaciji. Skrbnik in sponzor tveganja 2-krat letno ocenita stopnjo realizacije načrtovanih ukrepov in vneseta posodobljene podatke v informacijsko rešitev SBR.

Sistem upravljanja tveganj v ELES, ki ga je ELES uporabljal večino obdobja, na katero se nanaša revizija, je temeljil na standardu SIST ISO 31000:2011. Ta standard je leta 2018 nadomestil SIST ISO 31000:2018.[90]

ELES je julija 2020, torej ob koncu obdobja, na katero se nanaša revizija, uskladil in nadgradil sistem upravljanja tveganj na posodobljen standard SIST ISO 31000:2018.

Informacijska rešitev SBR je bila v letu 2020 že 2-krat nadgrajena. Dodana sta bila modul za podporo kritični infrastrukturi in bistvene storitve ter modul za vnos podatkov o uresničenih tveganjih s finančno oceno škode in datumom nastanka škode.

89 Scenarij tveganj je izraz, ki ga uporablja aplikacija SBR in predstavlja aktualen katalog tveganj in oceno tveganj v določenem četrtletju.

90 Obvladovanje tveganja – Smernice (angl.: *Risk management – Guidelines*), po standardu SIST ISO 31000:2018.

Zahteve ZKI in ZInfV s pripadajočimi podzakonski akti je ELES želel sistemsko rešiti tako, da bi obvladoval tveganja na enem mestu. Predvsem zaradi dostopnosti in nadzora pooblastil[91] se je ELES odločil za implementacijo dodatnega modula v informacijski rešitvi SBR.

Ocenjujemo, da ELES redno upravlja tveganja, jih ocenjuje ter posodablja.

2.1.3.j Posodabljanje ocene tveganj za delovanje kritične infrastrukture

ELES je oceni tveganj nosilcema sektorja kritične infrastrukture posredoval v januarju 2020. Kot je že navedeno v točki 2.1.2, ima ELES vpeljan sistem ocenjevanja tveganj. Poslovne učinke in verjetnost uresničitve tveganj ELES ocenjuje prek spremljanja uresničenih tveganj in prek spremljanja realizacije ukrepov. ELES redno, to je 1-krat letno, izvede meritev napredka pri obvladovanju tveganj, kjer pregleda na novo prepoznana tveganja, izvede morebitne spremembe že določenih ukrepov ali uvede nove ukrepe, če je to potrebno, ter določi oceno stopnje realizacije ukrepov. Te postopke lahko nosilci tveganj izvajajo sproti ob nastanku, obvezno pa letno na dan 30. 9.

ELES po oddaji ocen tveganj nosilcema sektorjev kritične infrastrukture januarja 2020 ni uvedel večjih sprememb v procesih in sistemih, zato do konca obdobja, na katero se nanaša revizija, še ni bilo treba izvesti izrednega ocenjevanja tveganj ali posredovati posodobljene ocene tveganj nosilcema sektorja kritične infrastrukture.

Ocenjujemo, da ima ELES vpeljan sistem za redno, letno ocenjevanje tveganj, kakor tudi za izredno ocenjevanje tveganj.

2.1.3.k Ukrepi za zaščito kritične infrastrukture

ELES ima za vsa tveganja, ki so navedena v katalogu in presegajo sprejeto sprejemljivo mejo tveganj, navedene ukrepe za zmanjševanje tveganj. Nekateri ukrepi so organizacijski in so vezani na interne dokumente, drugi pa tehnični. Tehnični ukrepi so podrobneje navedeni v točki 2.2.3.

Med organizacijskimi navodili so tudi navodila za vzpostavitev otočnega obratovanja ter navodila za ukrepe za zagotavljanje kriterija n-1. Za nekatere ukrepe je ELES sprožil postopke tudi pri drugih deležnikih. Kot primer navajamo pobudo ELES za dopolnitev Uredbe o izvajanju izvedbene uredbe Komisije (EU) o pravilih in postopkih za upravljanje brezpilotnih zrakoplovov[92], s katero je Javni agenciji za civilno letalstvo Republike Slovenije predlagal geografska področja, kjer bi bili preleti brezpilotnikov prepovedani.

ELES je pristopil k načrtovanju vzdrževanja kritične infrastrukture na način:

- da je nabavil montažne stebre, ki omogočajo hitro sanacijo posameznih stebrov z namenom, da so kritični elementi elektroenergetskega omrežja čim manj časa izpostavljeni možnosti izpada zaradi napake;
- izvajanja rednega usposabljanja operaterjev s postopki, povezanimi z zagotavljanjem delovanja kritične infrastrukture, ter

91 Klasifikacija informacij – interno oziroma poslovna skrivnost.

92 Uradni list RS, št. 195/20 in 31/21.

- vpeljave postopkov izklopa/vklopa DV s sekvenčnimi ukazi, ki izključujejo napako operaterja.

ELES se je odzval na epidemijo covida-19 z različnimi ukrepi. Direktor ELES je 9. 3. 2020 sprejel načrt aktivnosti ob pojavu epidemije. Konec aprila 2020 je ELES sprejel načrt aktivnosti v prehodnem obdobju med prvim in drugim valom nalezljive bolezni covid-19 z ukrepi. V začetku julija 2020 pa je sprejel še načrt aktivnosti za drugi val epidemije z ukrepi.

Med tehnične ukrepe za zaščito kritične infrastrukture ELES uvršča:

- vpeljavo sistema za zaznavanje odstopanj v sistemu SCADA[93];
- vzpostavitev sistema za enkripcijo prometa na komunikacijskih povezavah med postajami in OCV in med OCV;
- podvojene povezave na fizičnem nivoju;
- podvojeno strojno opremo;
- požarne pregrade med posameznimi funkcionalnimi segmenti omrežja;
- nadgradnjo sistema za upravljanje varnostnih informacij in dogodkov[94] (v nadaljevanju: SIEM);
- najem rezervnih povezav za zagotavljanje visoke razpoložljivosti.

Za obvladovanje tveganj, povezanih s kritično infrastrukturo, ELES izvaja obsežen nabor ukrepov, ki se delijo na stalne in dodatne. Stalne ukrepe ELES izvaja v vseh razmerah, ob povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi pa lahko njihovo izvajanje tudi stopnjuje. Dodatne ukrepe ELES izvaja ob povečani ogroženosti kritične infrastrukture, izrednem dogodku ali krizi, če stalni ukrepi, tudi če se njihovo izvajanje stopnjuje, ne zadostujejo.

Ocenjujemo, da ELES z ukrepi ustrezno izvaja zaščito kritične infrastrukture.

2.1.3.l Dokumenti načrtovanja zaščite kritične infrastrukture

ELES je v skladu z navodili nosilcev sektorjev kritične infrastrukture pripravil oceni tveganj za delovanje kritične infrastrukture in ukrepe za zaščito kritične infrastrukture, pripravil je navodila za otočna obratovanja kakor tudi opis procesa in navodila za neprekinjeno delovanje centrov vodenja, saj je eden od pomembnih preventivnih ukrepov nemotenega delovanja centrov vodenja zagotavljanje rezervne lokacije za vsak center vodenja.

Na področju IT ima ELES pripravljeno večje število dokumentov v sklopu SUVI, ki med drugim opisujejo procese zagotavljanja opreme in storitev, upravljanje sprememb ter vključevanje naprav v tehnično omrežje.

Ocenjujemo, da ima ELES ustrezne dokumente in vzpostavljene procese za načrtovanje zaščite kritične infrastrukture.

93 Angl.: *Supervisory Control and Data Acquisition* – skupno ime za sisteme, ki so namenjeni nadzoru in vodenju tehnoloških procesov z računalniki.

94 Angl.: *Security Information and Event Management.*

2.1.3.m Posodabljanje dokumentov načrtovanja zaščite kritične infrastrukture

ELES ima vrsto certificiranih sistemov upravljanja, med njimi tudi ISO 9001:2015, ki je mednarodni standard vodenja kakovosti. V skladu s tem standardom se organizacija zavezuje k posodabljanju procesov in pripadajočih dokumentov. ELES do konca obdobja, na katero se nanaša revizija, še ni posodobil dokumentov načrtovanja zaščite kritične infrastrukture, saj je dokumenta pripravil in posredoval nosilcema sektorjev šele v januarju 2020. ELES ima vpeljano upravljanje s tveganji, v okviru katerega že od leta 2012 redno, vsako četrtletje, izvaja ocenjevanje tveganj, 1-krat letno pa izvede tudi posodobitev celotnega kataloga tveganj (več v točkah 2.1.3.i in 2.1.3.j).

ELES v obdobju, na katero se nanaša revizija, še ni posodobil dokumentov načrtovanja zaščite kritične infrastrukture, ki ju je pripravil januarja 2020.

2.1.3.n Imenovanje kontaktnih oseb za sodelovanje na področju kritične infrastrukture

ELES je nosilcema sektorjev kritične infrastrukture v marca 2019 posredoval podatke o odgovorni in kontakti osebi upravljavca kritične infrastrukture.

Ugotavljamo, da je ELES s tem izpolnil zahtevo iz drugega odstavka 19. člena ZKI.

2.1.4 Sklep

ELES je v obdobju, na katero se nanaša revizija, **učinkovito implementiral zahteve zakonodaje na področju kritične infrastrukture,** saj je pravočasno izvedel vse zahteve, ki jih je opredeljeval ZKI s pripadajočimi podzakonskimi akti.

2.2 Upravljanje zaznavanja kibernetskih groženj

2.2.1 Sodila

Za presojo **učinkovitosti ELES pri upravljanju zaznavanja kibernetskih groženj** smo uporabili Okvir za izboljšanje kibernetske varnosti kritične infrastrukture[95], ki ga je razvil in izdal Nacionalni inštitut za standarde in tehnologijo[96] (v nadaljevanju: okvir NIST). Okvir NIST sestavljajo standardi, smernice in dobre prakse za obvladovanje tveganj kibernetske varnosti kritične infrastrukture in ima 5 področij: identificiranje, ščitenje, zaznavanje, odzivanje in okrevanje[97], njegova raba pa je prostovoljna. Glede na oceno narave tveganj na ELES in v želji po učinkoviti izvedbi revizije smo se odločili, da se osredotočimo le na področje zaznavanja in področje odzivanja. Ocenjujemo namreč, da sta področji identificiranja in ščitenja v pomembnem delu že vključeni v dokumente zaščite kritične infrastrukture, kar je že opisano v točki 2.1. Področja okrevanja, zadnjega od 5 področij, ki jih

95 *Framework for Improving Critical Infrastructure Cybersecurity*, verzija 1.1, [URL: https://www.nist.gov/cyberframework], 20. 8. 2021.

96 *National Institute of Standards and Technology*, [URL: https://www.nist.gov/], 20. 8. 2021.

97 Angl.: *Identify, Protect, Detect, Respond, Recover.*

predvideva okvir NIST, pa v reviziji nismo preverjali, saj ELES še ni doživel kibernetskega napada na kritično infrastrukturo (in posledično aktivnosti okrevanja še ni izvajal). V točki 2.2.3 bomo ocenjevali izpolnjevanje zahtev s **področja zaznavanja** okvira NIST.

2.2.2 Opis stanja

ELES ima pridobljen certifikat kakovosti vodenja ISO 9001:2015, kar se odraža tudi v večjem številu politik, organizacijskih postopkov, opisov procesov in navodil na vseh področjih. Informacijsko podporo v ELES lahko delimo na 3 področja: področje poslovnega omrežja (ki upravlja celotno poslovno informatiko, informacijsko-komunikacijsko infrastrukturo, telekomunikacijske in druge storitve), področje tehničnega omrežja (ki upravlja sisteme za prenos električne energije) in področje oddaljenih enot kritične infrastrukture[98].

Varovanje informacij temelji na krovni varnostni politiki in drugih pripadajočih dokumentih, in sicer: varstvo poslovne skrivnosti, kontrola vstopa in videonadzor, politika izvajanja neprekinjenega delovanja in okrevanja ključnih IT storitev, varovanje in zaščita podatkov poslovnega informacijskega sistema, varovanje informacij v tehničnem omrežju, nadzor in vzdrževanje v tehničnem omrežju, vključevanje naprav v tehnično omrežje, navodilo o vzdrževanju elektroenergetskih prenosih naprav in požarni red ELES.

Poslovna informatika je vpeljala IT procese[99] v skladu z ITIL, ki jih je podprla z opisi procesov, organizacijskimi predpisi in navodili.

Do konca obdobja, na katero se nanaša revizija, ELES še ni imel uspešnega kibernetskega napada oziroma zaposleni še niso zaznali realizacije kibernetskih groženj. ELES meni, da so kibernetski napadi prek centrov vodenja z namenom kompromitacije in podreditve drugih sistemov (na primer poslovnih sistemov) sicer možni, vendar praviloma najtežje izvedljivi in najmanj verjetni. Po oceni ELES so centri vodenja najbolj zaželene tarče kibernetskih napadov, zato so najbolje varovani in se jim tudi posveča največja skrb. Kibernetski napad na center vodenja, kjer bi bilo izhodišče napada v samem centru, pa bi zahteval fizično prisotnost napadalca ali njegovo podaljšano roko v družbi.

2.2.3 Ugotovitve glede zaznavanja kibernetskih groženj

Ugotovitve glede zaznavanja kibernetskih groženj so v nadaljevanju razdeljene po podkategorijah okvira NIST.

2.2.3.a Stanje konfiguracij omrežij

ELES ima narejen krovni omrežni diagram z več različnimi mrežnimi diagrami za področji poslovnega in tehničnega omrežja, ki pa nimajo podatkov o verziji in datumih zadnjih sprememb.

98 Angl.: *Remote Terminal Unit.*

99 ELES je začel vzpostavljati IT procese v letu 2011, najprej brez ustrezne informacijske podpore, potem pa s prilagajanjem procesov in informacijsko podporo procesom v sistemu IBM Maximo.

Priporočilo

ELES priporočamo, naj vpelje označevanje verzij in datumov zadnjih sprememb tudi v dokumente omrežnih diagramov.

ELES sistematično izdeluje tudi evidence pretoka podatkov med posameznimi segmenti omrežja. Sistemi tehničnega omrežja so ločeni od sistemov poslovne informatike. V primeru, da sistem tehničnega omrežja komunicira z zunanjimi sistemi (na primer ENTSO-E, BORZEN, operater trga z elektriko, d.o.o., Agencija za energijo, distributerji električne energije[100]), se komunikacija iz povezave Ethernet[101] pretvori v drugo in nato nazaj v povezavo Ethernet.

ELES je imel ob koncu obdobja, na katero se nanaša revizija, v poslovnem omrežju več tipov komunikacijskih omrežij, tako da v primeru izpada enega lahko drugo prevzame komunikacijo. V skrajnem primeru izpada vseh možnih tipov komunikacijskih omrežij sta še vedno možna zajem informacij in lokalno upravljanje v posameznem energetskem objektu.

Daljinski nadzor elementov in naprav EES je mogoč samo prek namenskega in od ostalih omrežij in sistemov ločenega sistema SCADA. Prek tega omrežja poteka tudi komunikacija s procesnimi napravami, prek katerih se nadzirajo in vodijo EES.

Sistem SCADA za nadzor in upravljanje EES je nameščen na gruči strežnikov, ki sicer ni podvojena, se pa ta gruča strežnikov nahaja na 2 različnih lokacijah. Gruča strežnikov omogoča tudi izpad posameznega strežnika, funkcionalnost tega strežnika pa lahko prevzamejo drugi strežniki. Sam sistem SCADA ni podvojen, a je v primeru celotnega izpada sistema mogoče vse naprave nadzirati in upravljati tudi lokalno.

Ocenjujemo, da ima ELES dokumentirano in vzpostavljeno ter upravljano konfiguracijo omrežij.

2.2.3.b Analiza zaznanih dogodkov

ELES ima vpeljan SIEM, ki je ob koncu obdobja, na katero se nanaša revizija, vključeval več kot 1.100 elementov. V SIEM se stekajo tudi vsi dnevniški zapisi požarnih pregrad in mrežnih elementov. Na področju tehničnega omrežja vsi elementi niso vključeni v SIEM. ELES je ob koncu obdobja, na katero se nanaša revizija, načrtoval, da bo v letu 2021 vzpostavil dodaten segment tehničnega omrežja za analizo anomalij v sistemu SCADA. ELES je pojasnil, da do sedaj ni zaznal vdorov tudi zato, ker je področje tehničnega omrežja zaprto znotraj področja poslovnega omrežja.

SIEM sprotno analizira dogodke, v primeru nastopa dogodka z ocenjeno vrednostjo 7 ali več na 10-stopenjski lestvici pa se prek izbranega orodja sprožijo alarmi, ki imajo obliko SMS sporočil, sporočil elektronske pošte in se prikažejo tudi v aplikaciji za upravljanje produkcije.

100 [URL: https://www.sodo.si/sl/za-odjemalce/seznam-dobaviteljev-elektricne-energije], 20. 8. 2021.

101 Angl.: *Ethernet* – standard za komunikacijo na lokalnih omrežjih, s pomočjo katerega lahko vse priključene naprave komunicirajo med sabo.

ELES uporablja tudi napredne rešitve za odkrivanje groženj[102], s pomočjo katerih odkriva bolj napredne dogodke, ki bi se potencialno lahko prebili preko požarnih pregrad.

V VNC, kjer je zagotovljena intervencija 24/7/365, pa se posredujejo dogodki iz vlomnih, požarnih in pristopnih kontrol.

V SIEM se združujejo tudi informacije oziroma dogodki iz kontrole dostopov.

Ocenjujemo, da ELES učinkovito analizira zaznane dogodke.

2.2.3.c Sinteza zaznanih dogodkov iz različnih virov

Kot že omenjeno v točki 2.2.3.b, se informacije o zaznanih dogodkih združujejo v SIEM. Aplikacijska podpora storitvenega centra z vgrajenimi funkcionalnostmi poslovnega poročanja omogoča tudi spremljanje in nadzor izvajanja procesa upravljanja problemov. Spremljanje in nadzor nad izvajanjem procesa upravljanja problemov poteka v dnevnih, tedenskih, mesečnih in letnih intervalih.

ELES je ob koncu obdobja, na katero se nanaša revizija, načrtoval združevanje in korelacijo določenih dogodkov, kot so na primer zbirka podatkov o vstopih v objekte ELES, podatki o odsotnosti oziroma dopustih zaposlenih, domenske prijave v realnem času, način oziroma lokacija prijave uporabnika (lokalno, prek brezžičnega omrežja, oddaljeno). S tem želi zmanjšati tveganja posojanja ali zlorabe uporabniških računov.

ELES je ob koncu obdobja, na katero se nanaša revizija, načrtoval tudi vzpostavitev rezervnega VOC, ki naj bi bil v novi poslovni stavbi v Beričevem. V VOC je načrtovana tudi implementacija sistema za združevanje in korelacijo vseh podatkov, povezanih z varnostjo.

Ocenjujemo, da ELES zbira in združuje zaznane dogodke iz različnih virov, a jih bo v celoti združil šele z nadgradnjo SIEM in vzpostavitvijo rezervnega VOC.

2.2.3.d Učinek zaznanih dogodkov

ELES zaznane dogodke ustrezno obravnava in tudi ukrepa glede na njihovo vsebino. V primeru reševanja poplavne ogroženosti na eni izmed lokacij, kjer sta bili v začetku tega tisočletja 2 poplavi območja kritične infrastrukture, je bil v letu 2011 najprej vzpostavljen poplavni zid ter nato v letu 2019 še klančine, ki sedaj varujejo objekte pred potencialnimi poplavami. Drugi primer je s področja vpeljave videonadzora, kjer so bile na eni lokaciji kritične infrastrukture postavljene videokamere preblizu 400-kV stikališča, kar je zaradi bližine vira visoke napetosti vplivalo na posnetke. Ko je ELES dogodke zaznal in analiziral, je videokamere prestavil in tako odpravil motnje. ELES je v reviziji navedel in predstavil še vrsto drugih primerov dogodkov in ukrepov, ki jih je izvedel.

Ocenjujemo, da ELES učinkovito implementira ukrepe, ki so bili posledica zaznanih dogodkov.

[102] Angl.: *Advanced Threat Protection.*

2.2.3.e Opozorila na zaznane dogodke

Elementi in orodja, ki omogočajo zaznavo in identifikacijo dogodkov, so konfigurirani tako, da področje poslovnega omrežja ščiti tudi EES (področje tehničnega omrežja). Zaznani dogodki se v orodju, ki se uporablja za analizo, lahko prekvalificirajo v incidente. ELES je od implementacije SIEM do konca obdobja, na katero se nanaša revizija, zabeležil približno 180.000 dogodkov, ki jih je orodje za analizo prekvalificiralo v 19.000 alarmov, razdeljenih v 3 skupine (kritične, pomembne in nizke). Ti alarmi se posredujejo po različnih kanalih, prejemniki pa so odvisni od stopnje kritičnosti in posameznega področja, kjer je bil dogodek zaznan.

ELES incidente na področju poslovnega omrežja rešuje na 3 nivojih: prvi nivo je storitveni center, kjer zaznajo dogodek, drugi nivo so strokovnjaki znotraj ELES, tretji nivo pa sestavljajo zunanji pogodbeni izvajalci. Celoten življenjski cikel obravnave incidentov ELES obvladuje v informacijski podpori storitvenega centra. Opis procesa je naveden v internem dokumentu upravljanja incidentov[103].

ELES ima tudi na področju tehničnega omrežja (prenosa električne energije) 3 nivoje obravnave incidentov. Prvi nivo je v centru vodenja, kjer zaznajo dogodek, drugi nivo so dežurni zaposleni strokovnjaki, tretji nivo pa sestavljajo strokovnjaki zunanjega pogodbenega izvajalca.

Ocenjujemo, da ELES učinkovito obravnava opozorila na zaznane dogodke.

2.2.3.f Spremljava omrežja

ELES ne izvaja nobenih storitev na odprtih omrežjih[104], kar bi sicer lahko predstavljalo tveganje za izvajanje bistvenih storitev, če bi napadalci izvedli napad porazdeljene ohromitve storitve[105]. Vse storitve in povezave z drugimi deležniki se izvajajo po zasebnih povezavah[106]. ELES ima sisteme za nadzor segmentirane v posamezna virtualna omrežja.

ELES spremlja omrežja z namenskimi orodji, ki posredujejo dogodke v SIEM, medtem ko se alarmi prek orodja za analize posredujejo skrbnikom in v vednost drugim zaposlenim – odvisno od kritičnosti in vsebine alarma.

Ocenjujemo, da ELES učinkovito spremlja omrežja.

2.2.3.g Spremljava fizičnega okolja

V okviru povezanega delovanja integriranega tehničnega sistema, ki vključuje videonadzorni sistem, protivlomni sistem, protipožarni sistem in kontrole pristopa, se zaznavajo varnostni dogodki. V primeru izrednega varnostnega dogodka se pregledajo posnetki s spremljanjem protivlomnih signalov. 2-krat dnevno VOC pripravi poročila in jih posreduje službi za korporativno varnost.

103 ELES; Opis procesa – Upravljanje incidentov, OP K 7.5.4 P2, 6. izdaja z dne 30. 9. 2019.

104 Ne nudi nobenih storitev prek svetovnega spleta.

105 Angl.: *DDoS – Distirbuted Denial-of-Service*.

106 Angl.: *VPN – Virtual Private Network.*

Nadzor nad fizičnimi dostopi se izvaja v okviru dogodkov pristopnih kontrol (poročila o dogodkih pristopne kontrole).

Vsak vpogled v posnetke snemalnika, presnemavanje, brisanje in obdelava posnetkov sistema je dovoljena izključno pooblaščenim osebam z utemeljenim razlogom za dostop in odobritvijo odgovorne osebe. Pregled dogodkov pristopnih kontrol lahko izvaja le pooblaščena oseba z utemeljenim razlogom za dostop.

Za vse objekte kritične infrastrukture ima ELES načrte varovanja. Vsi objekti kritične infrastrukture razen enega so bili ob koncu obdobja, na katero se nanaša revizija, tudi pod videonadzorom iz VNC in VOC. Projekt videonadzora je ELES začel v letu 2015 in ga zaključil v marcu 2020.

Pojasnilo ELES

Objekt, ki še ni pod videonadzorom, ima ELES v solastništvu z lokalnim podjetjem za distribucijo električne energije. Projekt rekonstrukcije se izvaja od februarja 2020, tehnični prevzem pa je načrtovan avgusta 2021. Med rekonstrukcijskimi deli je tudi vzpostavitev sistema tehničnega varovanja.

ELES ima več kot 3.000 čitalcev za kontrolo dostopov, ki so centralno nadzorovani iz VOC. Prav tako ima ELES veliko število javljalcev požara, ki so prav tako povezani na lokalne alarmne centrale in prek njih na centralno mesto v VOC in VNC. Večina objektov ima tudi protivlomne senzorje v zaščitnih ograjah objektov. Nekateri objekti imajo tudi 12- ali 24-urno varnostno službo.

Sistemski prostori so zaščiteni pred nepooblaščenim dostopom. Zunanjim izvajalcem je omogočen le napovedan in odobren dostop s strani skrbnika objekta v spremstvu zaposlenih skrbnikov IT. Ob koncu obdobja, na katero se nanaša revizija je bil v izdelavi projekt e-dovolilnica, ki bo omogočal centralni nadzor nad dostopi.

Ukrep ELES

ELES je v obdobju od decembra 2019 do maja 2021 izvedel projekt e-dovolilnica, s katerim je vzpostavljen celovit nadzor nad vstopi zunanjih deležnikov družbe v objekte družbe. Najava obiska je možna na spletni strani ELES[107].

V sistemskih prostorih in pred vrati sistemskih prostorov ni videonadzora.

> ***Priporočilo***
>
> *ELES priporočamo, naj prouči možnost vzpostavitve videonadzora vsaj v sistemskih prostorih in pred njimi, kjer imajo nameščene naprave drugi ponudniki storitev, če ne tudi v vseh ostalih sistemskih prostorih.*

Za vstope v sistemske prostore je zahtevana predhodna podaja storitvenega zahtevka prek informacijskega sistema, kjer je treba navesti lokacijo, potek vstopa od do, izvajalce, podrobnosti in namen vstopa. Zahtevek odobri vodja službe za telekomunikacije, nato pa se avtomatsko obvestijo

[107] [URL: https://www.eles.si/najava-obiska], 20. 8. 2021.

vsi, ki morajo biti seznanjeni z vstopom v prostor. Na nekaterih lokacijah sistemskih prostorov se namen vstopa dodatno beleži v papirne dnevnike.

Vsi sistemski prostori razen enega imajo okna, saj se ti prostori nahajajo v starejših stavbah. Na nekaterih oknih so kovinske rešetke, v samih prostorih pa senzorji gibanja. Na steklih so nanešene snovi, ki preprečujejo razpršitev delcev stekla.

> ***Priporočilo***
>
> *ELES priporočamo, naj prouči možnost namestitve kovinskih rešetk na vsa okna vseh sistemskih prostorov.*

Servisnih prostorov za sistemske prostore, kjer bi se lahko nahajale klimatske naprave, neprekinjeno napajanje in sistemi gašenja, ELES nima ločenih od sistemskih prostorov, so le del tega sistemskega prostora.

Na vseh lokacijah, kjer so sistemski prostori, so tudi rezervni dizelski agregati, ki so redno testirani.

Večina opreme tehničnega sistema varovanja je še v garancijski dobi, zato se servisiranje izvaja v tem okviru. Za vzdrževanje programske opreme VOC ima ELES sklenjeno pogodbo z zunanjim izvajalcem.

Ocenjujemo, da ELES učinkovito spremlja fizično okolje.

2.2.3.h Spremljava aktivnosti zaposlenih

ELES s pomočjo določenih orodij v okviru SIEM spremlja nekatere aktivnosti zaposlenih v informacijskih sistemih. Dostopi do dokumentov se beležijo v dokumentnem sistemu. ELES načrtuje tudi vpeljavo sistema za upravljanje privilegiranih dostopov[108], kar bo omogočalo tudi določitev časovnih oken uporabe in podporo delovnemu toku.

Zaposleni lahko prek navideznega zasebnega omrežja dostopajo v informacijski sistem ELES, a je čas trajanja seje omejen. Veljavnost pravic za oddaljen dostop prek navideznega zasebnega omrežja je za zunanje izvajalce omejena, po izteku roka pa morajo ponovno podati vlogo, ki jo skrbnik posameznega elementa informacijskega sistema preveri in odobri.

Ocenjujemo, da ELES ustrezno spremlja aktivnosti zaposlenih.

2.2.3.i Zlonamerna programska koda

ELES za odkrivanje zlonamerne programske kode uporablja 3 različna orodja na področju poslovnega omrežja, področju tehničnega omrežja ter na oddaljenih enotah kritične infrastrukture. ELES ima implementiran sistem za odkrivanje zlonamerne pošte ter orodja za preprečevanje teh vektorjev napada tudi na požarnih pregradah.

---

108 Angl.: *PAM – Privileged Access Management.*

V primeru, da zaposleni na ELES prejme elektronsko sporočilo s sumljivo priponko ali priponko, ki je ni mogoče preveriti, se sporočilo zadrži in prestavi v karanteno ter obvesti prejemnika. Po izjavi prejemnika, da pričakuje določeno pošto od pošiljatelja, se pošta iz karantene prestavi v poštni nabiralnik prejemnika.

Ocenjujemo, da ELES ustrezno upravlja z zlonamerno programsko kodo.

2.2.3.j Nepooblaščena prenosna koda

ELES na področju poslovnega omrežja uporablja orodje za preprečevanje nepooblaščene prenosne kode.[109] Na področju tehničnega omrežja so operacijski sistem ter sistemska in programska oprema licencirani in varnostno preverjeni s strani nosilca licenčne opreme. Prenosna koda je dovoljena v zelo omejenem obsegu, na omejenem številu strežnikov in se uporablja izključno v primerih, ko licenčna programska oprema ne omogoča zahtevane funkcionalnosti. Ob vsaki posodobitvi pregledajo nameščene aplikacije in jih odstranijo, če niso potrebne.

Ocenjujemo, da ELES ustrezno upravlja z nepooblaščeno prenosno kodo.

2.2.3.k Zunanji ponudniki storitev

ELES nima vpeljanega zunanjega izvajanja storitev[110] pri primarnih procesih. Za potrebe izvajanja fizičnega varovanja v skladu z ZZasV-1 ima ELES sklenjene pogodbe s 3 zunanjimi izvajalci. Obvezna priloga vsake pogodbe je izjava o varovanju poslovne skrivnosti, ki je obvezna tudi pri zahtevkih, na primer za oddaljen dostop. Iz izjave, ki jo podpiše zastopnik zunanje družbe, izhajajo vse osebe, ki so bile seznanjene s podatki, in njihovi kontaktni podatki.

Ocenjujemo, da ELES s stališča kibernetske varnosti ustrezno upravlja ponudnike zunanjih storitev.

2.2.3.l Nepooblaščeno osebje, povezave, naprave in oprema

ELES na področju poslovnega omrežja dnevno izvaja kontrolo ustvarjenih uporabniških računov. Vse zahteve po novih uporabniških računih ali po spremembah uporabniških računov se posredujejo prek informacijske rešitve. Uporabniki lahko dostopajo do informacijskih virov le na podlagi pravic, ki so dodeljene skupinam uporabnikov, ki jim pripadajo te pravice v aktivnem imeniku[111]. V primeru, da se dodelitev pravice izvede ročno, avtomatizirana kontrola, ki se periodično izvede, to zazna in samodejno odstrani tako kreiran uporabniški račun.

Na področju tehničnega omrežja (prenos električne energije) se vloge za dostop do uporabniških računov oddajo prek obrazcev, pravice pa so opredeljene prek skupin v aktivnem imeniku.

---

109 Angl.: *Mobile Code* – programska koda, ki se po omrežju prenaša iz oddaljenega računalniškega sistema in se izvaja na lokalnem računalniku običajno brez uporabnikovega posredovanja.

110 Angl.: *Outsourcing*.

111 Angl.: *AD – Active Directory*.

Fizični dostopi do objektov in prostorov se spremljajo prek videonadzornega sistema in sistema kontrole pristopa. Z možnostjo pregleda tekočih in preteklih posnetkov se lahko identificira varnostni dogodek nepooblaščenega dostopa in ukrepa.

Vsi strežniki in delovne postaje na področju tehničnega omrežja (prenosa električne energije) imajo preprečen dostop do USB-vmesnika, storitvi FTP[112] in Telnet pa sta onemogočeni. Vključitev ne testiranih in ne odobrenih naprav v omrežje je onemogočena. Prav tako ni možno nameščati ne odobrene programske opreme. ELES ima proces, ki izvede nameščanje dodatne programske opreme s strani pooblaščene osebe od zahteve, preko odobritve do same namestitve.

Ocenjujemo, da ELES ustrezno izvaja kontrolo nepooblaščenega osebja, povezav, naprav in opreme.

2.2.3.m Pregled ranljivosti

ELES občasno izvaja obdobna vdorna testiranja[113] na področjih poslovnega in tehničnega omrežja, dobljene rezultate analizira in na podlagi analize in priporočil izvajalcev testiranj izvede popravne ukrepe z namenom odprave zaznanih ranljivosti. Zadnja vdorna testa je ELES izvedel v letih 2017 in 2018. Nadzor je v določenih primerih pokazal podhranjenost nekaterih strežnikov, ki so bili na podlagi analize ugotovitev nadgrajeni. V okviru vdornih testov so bili izvedeni tudi preizkusi z zlonamerno programsko kodo.

ELES je imel ob koncu obdobja, na katero se nanaša revizija, v postopku nabave orodje za preverjanje ranljivosti[114]. ELES je pojasnil, da v zadnjih 2 letih nadgrajuje informacijske sisteme, kakor tudi načrtuje dodatne posodobitve z novejšimi napravami in stikali ter vzpostavlja novo domače omrežje za podporo distribucije, zaradi česar v tem času ni izvedel vdornih testov. Ko bodo izvedene načrtovane naloge, naj bi bili izvedeni tudi vdorni testi.

> ***Priporočilo***
>
> *ELES priporočamo, naj redno – vsaj letno načrtuje in izvaja vdorna testiranja.*

ELES redno izvaja tudi testiranje sistemov neprekinjenega napajanja, dizelskih agregatov, požarnih sistemov, klimatskih naprav in sistemov VOC. Za vzdrževanje videonadzornega sistema in protivlomnega sistema je bilo ob koncu obdobja, na katero se nanaša revizija, v pripravi javno naročilo, saj sta bila oba sistema blizu izteka garancijske dobe.

Ocenjujemo, da ELES delno izvaja preglede ranljivosti.

2.2.3.n Vloge in odgovornosti za odkrivanje

Incidenti, vezani na fizično varovanje in tehnični varnostni sistem, se na ELES obvladujejo v okviru VOC. Vloge in odgovornosti so opredeljene v krovni varnostni politiki. Protokoli delovanja VOC so

112 Angl.: *File Transfer Protocol* – protokol za prenos datotek med omrežnimi vozlišči.

113 Angl.: *Penetration Testing.*

114 Angl.: *Vulnerability Scan.*

opredeljeni v okviru nalog operaterja VOC, ki jih slednji opravlja na podlagi ZZasV-1, priročnika za delo VNC in priročnika za delo VOC ELES.

Za področje informacijskih sistemov ima ELES organizacijski predpis, ki opredeljuje posamezne procese in nivoje podpore. V opisu procesov reševanja zahtevkov, upravljanja incidentov, upravljanja, problemov upravljanja sprememb in reševanja zahtevkov – povpraševanje za novo telekomunikacijsko storitev so navedene tudi matrike odgovornosti posameznih izvajalcev.

Kot je že omenjeno v točki 2.1.3.c, ELES vzpostavlja lasten VOC, v katerega bodo združene posamezne delujoče nadzorne komponente. ELES načrtuje tudi, da se bo analitika varnostnih dogodkov odvijala na enem mestu.

Ocenjujemo, da ima ELES opredeljene vloge in odgovornosti za odkrivanje s ciljem zagotavljanja odgovornosti.

2.2.3.o Skladnost aktivnosti odkrivanja

ELES navaja, da izvaja aktivnosti odkrivanja v skladu z naslednjimi standardi, zakoni, usmeritvami, uredbami in pravilniki:

- ISO/IEC 27001:2013,
- ZKI,
- ZInfV,
- Zakon o poslovni skrivnosti[115],
- EZ-1,
- ZTP,
- Zakon o varstvu osebnih podatkov[116],
- Splošna uredba o varstvu podatkov, GDPR[117],
- Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev in
- Zakon o varstvu pred požarom[118].

Na ELES vzpostavljajo varno komunikacijo za izmenjavo podatkov med deležniki ENTSO-E, ki temelji na varnostnem načrtu ENTSO-E za minimalne izvedljive rešitve (MVS)[119], ta pa temelji na ISO/IEC 27001:2013. Za uporabnika, kot je ELES, se predvideva 264 kontrol. ELES bo skladnost preveril v 2 fazah: v prvi kot samoocenitev, v drugi fazi, ki jo načrtuje v letu 2021, bodo pregled v 2 delih opravili

115 Uradni list RS, št. 22/19.

116 Uradni list RS, št. 94/07 – uradno prečiščeno besedilo.

117 Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (UL L št. 119 z dne 4. 5. 2016, str. 1).

118 Uradni list RS, št. 3/07 – uradno prečiščeno besedilo, 9/11, 83/12, 61/17 – GZ in 189/20 – ZFRO.

119 Angl.: *Minimum Viable Solution*.

zunanji presojevalci in pripravili poročilo[120]. Prvi del pregleda so zunanji presojevalci opravili v aprilu 2021, drugi del pa je načrtovan za avgust 2021. ELES naj bi z izpolnitvijo zahtev ENTSO-E MVS vzpostavil zasebno komunikacijsko omrežje[121], kamor bo posredoval podatke s področja tehničnega omrežja, telekomunikacij in področja poslovnega omrežja.

ELES je vzpostavil SIEM, znotraj katerega je nameščen modul za varnostno preverjanje. Seznam ranljivosti, ki jih SIEM prepoznava, se dnevno dopolnjuje.

Z zunanjimi varnostnimi pregledi ELES periodično spremlja ustreznost varnostnih sistemov, kot sta na primer preverjanje čitljivosti magnetnih trakov (ob zahtevi za povrnitev podatkov[122], kjer je bilo sočasno potrjeno preverjanje čitljivosti trakov) ter preverjanje delovanja sekundarne lokacije z različnimi testnimi načrti in podobno.

Ukrep ELES

ELES je aprila 2021 prešel na nov sistem varnostnega kopiranja in pregledovanja varnostnih trakov. Poleg človeške komponente pregledovanja je bilo omogočeno tudi strojno preverjanje.

ELES poskuša med tehničnim omrežjem in okolico vzpostaviti zračno vrzel[123], kar je ob koncu obdobja, na katero se nanaša revizija, dosegel s pretvorbo protokolov.

Pogostost testiranja požarne varnosti, klimatskih naprav in naprav za neprekinjeno napajanje je predpisana v internih dokumentih in se izvaja.

Ocenjujemo, da ELES izvaja aktivnosti odkrivanja skladno z mednarodnimi, državnimi in internimi dokumenti.

2.2.3.p Preverjanje procesov odkrivanja

ELES sam ne preizkuša zmogljivosti/sposobnosti odkrivanja varnostnih dogodkov s strani implementiranih rešitev, zato se pri varnostnih rešitvah zanaša na preizkušene rešitve vodilnih proizvajalcev. V sklopu tehnične dokumentacije se praviloma omejuje na vodilne proizvajalce, ki zasedajo v Gartnerjevem diagramu[124] zgornji desni kvadrant. V okviru posameznih vzdrževalnih pogodb ima ELES dogovorjene posodobitve sistema in tudi letne preglede nastavitev implementiranih rešitev.

ELES izvaja posamezne teste odkrivanja ranljivosti, na primer test kakovosti zapisa na magnetne trakove in test preklopa delovanja posameznega segmenta na rezervno lokacijo.

Ocenjujemo, da ELES izvaja preverjanje procesov odkrivanja.

120 [URL: https://www.aicpa.org], 20. 8. 2021.

121 Angl.: *PCN – Private Communication Network*.

122 Angl.: *Restore.*

123 Angl.: *Air Gapping* – varnostni ukrep, katerega cilj je fizična ločitev varovanega omrežja od nevarovanih omrežij.

124 [URL: https://www.gartner.com/en/research/methodologies/magic-quadrants-research], 20. 8. 2021.

2.2.3.q Posredovanje informacij o odkritju dogodka

Kot že opisano v točki 2.2.3.g, v okviru spremljave fizičnega okolja VOC 2-krat dnevno pripravlja poročila, ki jih posreduje službi za korporativno varnost. Pomembnejših varnostnih dogodkov v obdobju od 1. 1. 2019 dalje ni bilo.

Aplikacijska podpora storitvenega centra z vgrajenimi funkcionalnostmi poslovnega poročanja omogoča spremljanje in nadzor izvajanja procesov, in sicer v dnevnih, tedenskih, mesečnih in letnih intervalih. ELES v sklopu tima za informacijsko varnost in sveta za informacijsko varnost obravnava varnostne incidente in po potrebi poroča na kolegiju vodstva. Navedeni delovni telesi sta ustanovljeni za zagotavljanje informacijske varnosti.

ELES v obdobju, na katero se nanaša revizija, o odkritih varnostnih dogodkih ni poročal zunanjim deležnikom (kot na primer Nacionalni odzivni center za kibernetsko varnost (SI-CERT)[125], Agenciji za energijo, ENTSO-E), saj še ni zaznal dogodka, o katerem bi poročal. ELES je od operaterja prenosnega omrežja ene od sosednjih držav prejel obvestilo, da je njihov ponudnik komunikacijskih storitev doživel kibernetski napad na omrežje.

Ukrep ELES

ELES je ob vzpostavitvi SUNP posodobil tudi interne dokumente, povezane z upravljanjem incidentov na področju informacijske varnosti. Pripravil je tudi obrazec za posredovanje informacij o kibernetskem incidentu na SI-CERT.

Priporočilo

ELES priporočamo, naj občasno testira proces poročanja o varnostnih dogodkih.

Ocenjujemo, da ima ELES ustrezen proces posredovanja informacij o odkritih dogodkih.

2.2.3.r Nenehno izboljševanje postopka zaznavanja

ELES v posebnem orodju na področju poslovnega omrežja vodi zbirko znanja IKT o zaznanih dogodkih in aktivnostih razreševanja. Glede na zaznane dogodke sisteme nenehno izboljšuje. Na področju tehničnega omrežja gradi svojo zbirko znanja po principu Wikipedije. Zbirka znanja za področje elementov kritične infrastrukture pa je organizirana v obliki strukturnih datotek na omrežju.

Priporočilo

ELES priporočamo, naj prouči možnost vzpostavitve zbirke znanja o zaznanih dogodkih.

Ocenjujemo, da ELES ustrezno nenehno izboljšuje postopke zaznavanja dogodkov.

125 Angl.: *Slovenian Computer Emergency Response Team,* [URL: https://www.cert.si], 20. 8. 2021.

2.2.4 Sklep

ELES je v obdobju, na katero se nanaša revizija, **učinkovito upravljal zaznavanje kibernetskih groženj**, kar je razvidno iz zgornjih ugotovitev. ELES ima še možnosti za izboljšave, ki se jih zaveda in jih postopno dopolnjuje.

2.3 Upravljanje odzivanja na kibernetske grožnje

2.3.1 Sodila

Za presojo **učinkovitosti ELES pri upravljanju odzivanja na kibernetske grožnje** smo uporabili okvir NIST. V nadaljevanju bomo ocenjevali izpolnjevanje zahtev s **področja odzivanja** okvira NIST.

2.3.2 Opis stanja

ELES je leta 2012 pridobil certifikat ISO/IEC 27001:2005 in ga v kasnejših ponovnih certifikacijah nadgradil na ISO/IEC 27001:2013. Kot je navedeno v točki 2.1.3.g, ima ELES vpeljan SUVI. Zaradi zahtev iz 12. člena ZInfV pa je ELES septembra 2019 pristopil k vpeljavi SUNP po standardu ISO 22301:2019. Vpeljavo je načrtoval do konca leta 2020.

Kot je že navedeno v točki 2.2.2, ima ELES vrsto dokumentov, ki se nanašajo na varovanje informacij in zaščito podatkov. ELES načrtuje, da bo dokumente, ki so bili narejeni ob implementaciji ITIL, in interne dokumente s področja tehničnega omrežja, ki se nanašajo na neprekinjeno delovanje, uskladili z zahtevami standarda ISO 22301:2019.

2.3.3 Ugotovitve glede odzivanja na kibernetske grožnje

2.3.3.a Načrt odzivanja

ELES ima na področju poslovnega omrežja opredeljen načrt odzivanja v okviru politike izvajanja neprekinjenega delovanja in okrevanja IT storitev. Za področje poslovnega omrežja ima ELES navodila za neprekinjeno poslovanje pripravljena po procesih ITIL, kjer se incident zabeleži v informacijsko podporo, kjer je vzpostavljeno obveščanje, prejemniki obvestil pa so odvisni od kategorije in vrste incidenta. ELES ima v načrtu prilagoditev internih dokumentov na skupen načrt neprekinjenega poslovanja. Na področju tehničnega omrežja ima ELES razvite nekatere parcialne rešitve, ki pa jih z vpeljavo SUNP konsolidira.

Za področje fizične zaščite ima ELES za vsak segment varovanja[126] pripravljen načrt odzivanja – tako imenovano shemo ukrepanja.

Ocenjujemo, da ima ELES ustrezen načrt odzivanja na kibernetske grožnje.

[126] Protipožarni, protivlomni, videonadzor ter kontrola dostopa.

2.3.3.b Usposabljanje zaposlenih za odziv

ELES gradi na znanju zaposlenih, ki se usposabljajo v okviru namenskega usposabljanja za določeno vlogo pri implementaciji tehničnega sistema, vendar v ta usposabljanja varnostne vloge in politike niso izrecno vključene. Večina incidentov je razrešenih na drugem nivoju, v redkih primerih se reševanje izvede na tretjem nivoju, to je pri zunanjih izvajalcih – dobaviteljih (več v točki 2.2.3.e).

ELES ima določene vloge v primeru odziva v krovni varnosti politiki in v politiki izvajanja neprekinjenega delovanja in okrevanja IT storitev.

Na področju fizične zaščite so za opravljanje nalog operaterja VOC/varnostnika – interventa zakonsko določeni pogoji in izobraževanja, kar so tudi pogodbeni pogoji, ki jih ELES ob sklenitvi pogodbe z zunanjimi izvajalci fizičnega varovanja tudi zahteva.

ELES veliko vlaga v usposabljanje zaposlenih s ciljem, da usposobi zaposlene, da lahko večino incidentov razrešijo sami. Slika 6 prikazuje del usposabljanj v letu 2019 (izobraževanj, delavnic in konferenc) za zaposlene na področju poslovnega omrežja.

Slika 6 Del izobraževanj za zaposlene na področju poslovnega omrežja v letu 2019

A	B	C	D	E	F
ID tečaja	SM	Začetni datum	končni datum	Tečaji	
TEC000777	992	25.03.2019	29.03.2019	MS Bootcamp Exchange 2016	
TEC000845	992	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	994	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000801	993	17.04.2019	17.04.2019	21. Tehnološka konferenca	
TEC000801	993	17.04.2019	17.04.2019	21. Tehnološka konferenca	
TEC000845	993	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	994	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	994	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	994	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000801	993	17.04.2019	17.04.2019	21. Tehnološka konferenca	
TEC000845	993	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000801	993	17.04.2019	17.04.2019	21. Tehnološka konferenca	
TEC000845	993	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	994	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	994	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000802	993	23.04.2019	23.04.2019	Optična TK dostopkovna omrežja v prostoru	
TEC000837	993	21.05.2019	23.05.2019	14. konferenca CIGRE	
TEC000845	993	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	993	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	994	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000840	992	21.05.2019	23.05.2019	NT konferenca 2019	
TEC000803	993	9.04.2019	10.04.2019	Dnevi inovativnih tehnologij	
TEC000845	992	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000788	991	10.01.2019	11.01.2019	ISO 27000 informacijska varnost	
TEC000845	991	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000803	993	9.04.2019	10.04.2019	Dnevi inovativnih tehnologij	
TEC000803	993	9.04.2019	10.04.2019	Dnevi inovativnih tehnologij	
TEC000845	991	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000830	991	20.03.2019	21.03.2019	Konferenca RISK 2019	
TEC000845	991	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000840	990	21.05.2019	23.05.2019	NT konferenca 2019	
TEC000845	990	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000840	992	21.05.2019	23.05.2019	NT konferenca 2019	
TEC000844	992	6.05.2019	10.05.2019	Windows Server 2016 Bootcamp	
TEC000834	990	14.03.2019	14.03.2019	Digitalne tehnologije in spremembe v energetiki	
TEC000840	990	21.05.2019	23.05.2019	NT konferenca 2019	
TEC000845	990	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000845	990	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000831	992	4.03.2019	8.03.2019	Tečaj MS 20710	
TEC000845	992	28.05.2019	31.05.2019	Usposabljanje ITIL	
TEC000831	992	4.03.2019	8.03.2019	Tečaj MS 20710	
TEC000845	992	28.05.2019	31.05.2019	Usposabljanje ITIL	

Vir: podatki ELES.

Ocenjujemo, da je usposabljanje zaposlenih za odziv v ELES ustrezno.

2.3.3.c Poročanje o dogodkih

Na področju poslovnega omrežja se poročanje o dogodkih izvaja avtomatizirano s pomočjo orodja. Nastavitve orodja omogočajo, da se glede na dogodek aktivirajo različna opravila in izvedejo različne oblike sporočanja (elektronska pošta, SMS-sporočila, prikaz na kontrolni plošči v storitvenem centru).

Na področju tehničnega omrežja operaterji v OCV obveščajo dežurne strokovnjake, ki imajo predpisane odzivne čase. Dogodke operaterji razvrščajo na 6 področij. V ekipi dežurnih so najmanj 4 strokovnjaki, ki imajo tedensko dežurstvo 24 ur na dan. Načrt poročanja je opisan v načrtih neprekinjenega poslovanja.

VOC ima protokol obveščanja ob izrednih dogodkih za protipožarni sistem in za protivlomni sistem.

Ocenjujemo, da ima ELES vzpostavljen ustrezen način poročanja o dogodkih.

2.3.3.d Posredovanje informacij

Shema komunikacij in poročanj je na ELES definirana v načrtih neprekinjenega poslovanja in opisu procesa upravljanja incidentov, kjer je opredeljen tudi načrt ukrepanja. Informacije se pošiljajo prek SMS-sporočil, obvestil elektronske pošte in v prikaz aplikacije za upravljanje produkcije. V načrtih neprekinjenega poslovanja je tudi določen pretok informacij med svetom direktorjev, kriznim štabom in pooblaščenimi osebami za izvajanje načrtov, poleg tega je določena tudi matrika odgovornih, zadolženih, posvetovanih in informiranih (RACI)[127].

VOC in VNC imata protokol ukrepanja, kar je opisano v točki 2.3.3.c.

Ocenjujemo, da ima ELES vpeljan sistem posredovanja informacij.

2.3.3.e Koordinacija zainteresiranih strani

Notranji deležniki so obveščeni skladno s procesom upravljanja z incidenti, pri večjih incidentih dobijo tudi SMS-sporočilo o zaključku incidenta. O stanju varnosti na področju IKT (predvsem o incidentih) informatiki mesečno poročajo službi za korporativno varnost. Zunanjim zainteresiranim stranem v obdobju, na katero se nanaša revizija, niso pošiljali obvestil, saj še ni prišlo do tovrstnega incidenta.

Na področje fizične zaščite služba za korporativno varnost komunicira z najbližjo policijsko postajo skladno z 58. členom ZZasV-1.

V primeru večjih požarov v naravnem okolju ima ELES sklenjen protokol izklapljanja in vklapljanja DV z Upravo Republike Slovenije za zaščito in reševanje.

Med ELES in partnerji doma in v tujini poteka izmenjava informacij in podatkov, ki so potrebni za zagotavljanje neprekinjenega in kakovostnega obratovanja sistema. Poteka prek različnih medijev, v različnih formatih in oblikah. Avtomatsko se izmenjujejo merilni podatki, podatki o stikalnih stanjih, alarmih in podobno. Operativne ekipe ELES sodelujejo z operativnim osebjem relevantnih partnerjev v Sloveniji (distribucijska podjetja, proizvodna podjetja, odjemalci, priključeni na prenosno omrežje, ponudniki sistemske izravnave) in tujini (predvsem tuji sistemski operaterji). Komunikacija poteka prek standardnih kanalov, kot so telefoni, elektronska pošta in druge namenske platforme. Operativno osebje si izmenjuje informacije, ki so pomembne za obratovanje sistema. ENTSO-E ima sistem za ozaveščanje[128] – enotno platformo za obveščanje, določen je protokol, ki predvideva obveščanje o stanju elektroenergetskega sistema, delovanju ključnih aplikacij in podobno. Predvidena je tudi navedba vzrokov za motnje, med katerimi je lahko tudi varnostni incident.

Ocenjujemo, da ELES izvaja koordinacijo v skladu z načrti odzivanja.

127 Angl.: *Responsible, Accountable, Consult, Inform.*

128 Angl.: *EAS – ENTSO-E Awareness System.*

2.3.3.f Prostovoljna izmenjava informacij o incidentih

V sklopu varnostnega foruma ENTSO-E deluje delovna skupina za kibernetsko varnost[129], ki spremlja različne kanale, da pridobi informacije na področju kibernetske varnosti in jih nato posreduje članom. Podobne aktivnosti izvaja tudi Agencija za energijo.

Na področju informatike je ELES določil kontaktni osebi za komunikacijo s SI-CERT. Do konca obdobja, na katero se nanaša revizija, ELES še ni posredoval informacij na SI-CERT.

ELES ima postopke izmenjave informacij opisane v dokumentu o korporativnem komuniciranju.

Ocenjujemo, da ima ELES urejeno prostovoljno izmenjavo informacij o incidentih.

2.3.3.g Analiziranje obvestil

ELES ima področje poslovnega omrežja podprto s storitvenim centrom, kjer informacijska rešitev podpore storitvenega centra omogoča spremljanje in nadzor izvajanja procesa upravljanja dogodkov. Sistemi za obveščanje generirajo sporočila, ki avtomatsko prihajajo v storitveni center. Dežurni v storitvenem centru zabeleži dogodek in ga kategorizira. Dogodek je lahko incident, problem ali zahteva za spremembo. Spremljanje in nadzor nad izvajanjem procesa poteka v dnevnih, tedenskih, mesečnih in letnih intervalih.

Na področju tehničnega omrežja ima ELES posebno informacijsko rešitev za obveščanje o delovanju strežnikov. ELES je imel tudi v tem omrežju informacijsko rešitev za pregledovanje dnevniških zapisov z orodjem za pregledovanje sporočil, a v času od septembra 2019 do februarja 2021 sistem ni deloval, tako da je ELES ob koncu obdobja, na katero se nanaša revizija, ročno analiziral vzroke z vpogledi v zbirko podatkov o dogodkih.

Sistem SCADA za upravljanje in nadzor neprekinjenega napajanja samodejno izvaja analizo stanja.

V okviru delovanja tehničnih varnostnih sistemov operater VOC dogodke zabeleži in poroča odgovornim osebam, tako da pripravi dnevno poročilo VOC. Upravitelj tehničnega sistema izdela mesečno poročilo sistema, v katerem se poleg dogodkov analizirajo tudi razlogi za njihov nastanek in predlagane rešitve. Ukrepi se sprejemajo sproti, poročanje o njih poteka tudi v okviru dnevnega poročila. Poročila se beležijo v obliki, ki omogoča analiziranje pogostosti napak, časov odziva, pogostosti okvar ter odzivnih časov serviserjev.

Ocenjujemo, da ima ELES vpeljan sistem za analiziranje obvestil.

2.3.3.h Razumevanje vpliva incidentov

ELES na področju poslovnega omrežja ob zaznavi dogodka v storitvenem centru dopolni osnovne podatke o dogodku z naslednjimi parametri: nujnost, notranja prioriteta, klasifikacija, vrsta storitve, tip storitve, ustreznost opisa težave in konfiguracijski element oziroma storitev. V primeru, da ima

129 Angl.: *WGCS – Working Group Cybersecurity*.

incident najvišjo prioriteto, se po SMS-sporočilu posreduje informacija tudi direktorju področja in vodji storitvenega centra.

Na področju tehničnega omrežja izvaja ELES odzivanje in vpliv v skladu z internimi navodili, ki pa bodo posodobljena z vpeljavo SUNP.

Na področju tehničnega varovanja se prednostno izvajajo intervencije na požarne alarme, tudi če iz videoposnetkov ni zaznan dim. Pri vlomnem alarmu pa se najprej pregledajo posnetki v videosistemu in se potem odloča o ukrepih. Aktivnosti se izvajajo po protokolih, kasnejše aktivnosti pa se izvajajo v korelaciji z ugotovitvami na terenu.

Ocenjujemo, da ELES ustrezno razumeva vpliv incidentov.

2.3.3.i Forenzične preiskave

ELES nima pooblaščenih in izurjenih strokovnjakov za izvajanje forenzičnih[130] analiz, po potrebi lahko k sodelovanju povabi zunanjo pomoč. ELES ima navodila za zbiranje dokazov in zaščito posameznih elementov, prav tako znajo zaposleni zavarovati sisteme in pripraviti izvoze za nadaljnjo analizo.

Ob vzpostavitvi VOC ELES načrtuje izobraževanje o osnovah forenzike za 1 zaposlenega, za kaj več pa bo vključil zunanje strokovnjake.

Čeprav jih sam ne izvaja, ocenjujemo, da ima ELES vzpostavljene postopke za podporo forenzičnih preiskav.

2.3.3.j Razvrščanje incidentov

Ob nastanku dogodka in njegovi zaznavi ter odprtju incidenta v informacijski podpori storitvenega centra se vedno določita nujnost in vpliv, kar je podlaga za izračun prioritete v skladu s sprejeto matriko. Naloga storitvenega centra je, da stalno spremlja stanje vseh incidentov, prijavljenih v informacijski podpori. Informacijska podpora za obveščanje in alarmiranje na podlagi vnaprej definiranega scenarija in prioritete incidenta obvešča deležnike o stanju incidenta.

Na področju tehničnega omrežja se incidenti razvrščajo v informacijsko rešitev, če se incident rešuje več kot 45 min po zaznavi, pa ga je treba še dodatno opisati in po potrebi sporočiti na tretji nivo podpore.

Za tehnično varovanje obstaja protokol izvajanja aktivnosti ob nastanku incidenta in postopek njegovega razvrščanja (več v točki 2.3.3.h).

Ocenjujemo, da ima ELES ustrezno vpeljan proces razvrščanja incidentov.

130 Forenzika je skupno ime za skupek znanj različnih strok, ki prispevajo k razkrivanju kaznivih dejanj.

2.3.3.k Procesi za spremljanje, analizo in odzivanje na ranljivosti

ELES sam ne izvaja preizkušanja zmogljivosti/sposobnosti zaznavanja varnostnih dogodkov implementiranih informacijskih rešitev. Zato se pri varnostnih rešitvah zanaša na preizkušene rešitve vodilnih proizvajalcev. V sklopu tehnične dokumentacije se ELES praviloma omejuje na vodilne proizvajalce, ki zasedajo v Gartnerjevem diagramu zgornji desni kvadrant.

V okviru posameznih vzdrževalnih pogodb ima ELES dogovorjene tudi posodobitve sistema in letne preglede ranljivosti.

ELES ima informacijsko rešitev korektivni in proaktivni ukrepi (v nadaljevanju: KPU), kjer lahko vsak zaposleni poda predloge za izboljšave. Delovni tok, ki je podprt v informacijski rešitvi KPU, omogoča analizo in spremljanje realizacije predlogov.

ELES je pred obdobjem, na katero se nanaša revizija, sodeloval na mednarodnih kibernetskih vajah. Leta 2014 je sodeloval na vaji EU Cyber Europe, ki je bila izvedena s ciljem preverjanja splošne pripravljenosti v primeru kibernetskega napada na informacijske in telekomunikacijske sisteme elektroenergetskih podjetij[131]. Prav tako je ELES sodeloval pri vajah izvajanja vlog napadalcev in braniteljev v okviru evropskega omrežja za kibernetsko varnost ENCS[132] – RTBT[133] 2017 in RTBT 2018.

Ocenjujemo, da ima ELES vpeljane procese spremljanja, analize in odzivanja na ranljivosti.

2.3.3.l Omejevanje incidentov

ELES ima v okviru informacijske podpore in delovnega toka storitvenega centra vzpostavljen proces odzivanja na incidente in prehoda v proces upravljanja problemov. Varnostni incidenti imajo najvišjo prioriteto. Proces obveščanja o incidentih je opisan v točkah 2.3.3.h in 2.3.3.j. Postopek obveščanja se izvaja tudi prek oglasne deske informacijske rešitve in portala ELESNET. V postopku razreševanja problemov se vzpostavljajo dodatni ukrepi za omejevanje incidentov.

Na področju tehničnega omrežja ELES še ni imel varnostnih incidentov, ki bi nastali kot posledica ranljivosti trenutne konfiguracije. Se pa z vzpostavitvijo SUNP vzpostavljajo poenoteni postopki. Na tem področju ELES razmišlja o vzpostavitvi glavnega stikala, ki bi omogočalo prekinitev vseh povezav – električnih, komunikacijskih in drugih[134] in ki bi tehnično omrežje in s tem sistem vodenja prenosa električne energije odrezalo od ostalega sveta v primeru identifikacije varnostnega incidenta/kibernetskega napada v poslovno omrežje.

Ocenjujemo, da ima ELES vzpostavljen proces omejevanja incidentov.

131 [URL: https://www.eles.si/Portals/0/Publikacije/Letna-porocila/Eles_Letno_porocilo_2014_SLO.pdf], 20. 8. 2021.

132 Angl.: *European Network for Cyber Security*, [URL: https://encs.eu/], 20. 8. 2021.

133 Angl.: *Read Team Blue Team*.

134 Angl.: *Master switch*.

2.3.3.m Blažitev incidentov

ELES blaži oziroma zmanjšuje vplive incidentov na več nivojih: dežurstvo na domu, ki zagotavlja odzivnost in reagiranje 24/7, zagotavljanje visokega nivoja znanja in kompetenc zaposlenih z izobraževanjem in seznanjanjem z novostmi, tako da ELES ni močno odvisen od zunanjih partnerjev; vzdrževalne pogodbe za dostop do naprednih znanj in zbirke znanja. V primeru, da dežurne ekipe ne razrešijo incidenta, predajo incident na drugi nivo razreševanja in, če je to potrebno, tudi na tretji nivo, kar pomeni, da vključijo zunanje pogodbene strokovnjake.

Na področju tehničnega varovanja ELES v protipožarne sisteme vgrajuje gašenje s plinom inergen. Prav tako so bili na področjih s povečanim poplavnim tveganjem vzpostavljeni poplavni zidovi in klančine. Na tem področju se ELES uči iz preteklih dogodkov in postopno izboljšuje sisteme.

Ocenjujemo, da ima ELES vzpostavljene postopke za blaženje incidentov.

2.3.3.n Nove ugotovljene ranljivosti

ELES izvaja preglede ranljivosti z izbranim orodjem, varnostno preverjanje celotnega javnega segmenta, na katerem komunikacija poteka prek internetnega protokola, se izvaja periodično. Analiza zaprtih incidentov se izvaja na kolegijih področij. Sestanki, izvedeni v okviru tima za informacijsko varnost in sveta za informacijsko varnost, pa so namenjeni seznanjanju z večjimi projekti in ukrepi.

V razvojni načrt 2021–2030[135] je ELES vključil kategorijo kibernetska varnostna testiranja in s tem predvidel finančna sredstva za izvedbo periodičnih vdornih testov.

V okviru dogodkov, zaznanih s pomočjo tehničnega varovanja, se tveganja obvladujejo dnevno (dnevni sestanki in odprava pomanjkljivosti), obširneje analize se izvedejo tedensko. Mesečno se pregledajo izvedena vzdrževanja posameznih sistemov v okviru poročila upravitelja sistema.

Novougotovljene ranljivosti prek članov tima za tveganja se periodično vnesejo v katalog tveganj (več v točki 2.1.3.i).

Ocenjujemo, da ima ELES vzpostavljene postopke za upravljanje novih ugotovljenih ranljivosti.

2.3.3.o Vključevanje pridobljenih izkušenj

ELES je pri posameznih testiranjih neprekinjenega poslovanja kot tudi pri pregledih ranljivosti nameščenih informacijskih rešitev s strani zunanjih izvajalcev pridobil določene izkušnje, ki jih je nato z ukrepi tudi vpeljal v svoja okolja in nadgradil zaščite.

Kibernetskih incidentov ELES še ni imel, ocenjujemo pa, da se iz napak, ki jih odpravi, tudi uči.

135 ELES, Razvojni načrt prenosnega sistema Republike Slovenije za obdobje 2021–2030, 19. 11. 2020, [URL: https://www.eles.si/Portals/0/Documents/SLO/20210126-RNPS2021-2030.pdf?ver=2021-02-02-152524-633], 20. 8. 2021.

Na področju fizične zaščite se ELES uči iz izkušenj (več v točki 2.2.3.d).

Ocenjujemo, da ELES v svoje načrte vključuje pridobljene izkušnje.

2.3.3.p Posodabljanje strategije

ELES ni imel posebne strategije za področje kibernetske varnosti, imel pa je vzpostavljene politike za vse segmente integriranega sistema upravljanja, ki so se prek vodstvenega pregleda redno pregledovale in ustrezno dopolnjevale. Med te politike sodi tudi upravljanje s tveganji, ki je podrobneje opisano v točkah 2.1.2, 2.1.3.i in 2.1.3.j. ELES je maja 2019 opredelil kibernetsko varnost kot enega izmed strateških izzivov, ki ima vpliv na večino področij[136]. Prav tako je ELES v razvojni načrt za obdobje med letoma 2021 in 2030 dodal kategorijo kibernetska varnostna testiranja[137].

Ukrep ELES

ELES je obravnavo kibernetske varnosti po zaključku obdobja, na katero se nanaša revizija, vključil v 2 strateška dokumenta družbe, in sicer: Trajnostna strategija družbe ELES do leta 2050 (oktober 2020) in Dolgoročni strateški plan družbe ELES za obdobje 2021–2025[138] (februar 2021).

Ocenjujemo, da ima ELES delno vzpostavljene postopke za posodabljanje strategije za odzivanje na kibernetske grožnje.

2.3.4 Sklep

ELES je v obdobju, na katero se nanaša revizija, čeprav v tem obdobju ni doživel kibernetskega napada, **učinkovito upravljal odzivanje na kibernetske grožnje**, kar je razvidno iz zgornjih ugotovitev. ELES ima še možnosti za izboljšave, ki se jih zaveda in jih postopno uvaja.

136 Tako kot opomba 50.

137 Tako kot opomba 135.

138 [URL: https://www.eles.si/Portals/0/Documents/ELES_dolgorocni_strateski_plan_2021_2025.pdf], 20. 8. 2021.

3. Mnenje

Revidirali smo učinkovitost ELES, d.o.o., sistemskega operaterja prenosnega elektroenergetskega omrežja (ELES) pri upravljanju kibernetske varnosti za področje kritične infrastrukture v obdobju od 1. 1. 2019 do 31. 7. 2020.

Mnenje smo oblikovali na podlagi presoje, ali je ELES učinkovito implementiral zahteve zakonodaje na področju kritične infrastrukture, ali je ELES učinkovito upravljal zaznavanje kibernetskih groženj in ali je ELES učinkovito upravljal odzivanje na kibernetske grožnje. Menimo, da je ELES v obdobju, na katero se nanaša revizija, **učinkovito** upravljal kibernetsko varnost na področju kritične infrastrukture.

ELES je že v letu 2009 uvedel obvladovanje tveganj in je v nadaljnjih letih vzpostavil celovit sistem upravljanja tveganj, ki je bil skupaj z vzpostavljenim notranjim kontrolnim sistemom ključni del integriranega sistema upravljanja družbe. Upravljanje tveganj v ELES je temeljilo na procesnem modelu – tveganja v posameznih procesih. ELES je vodil informatiziran katalog tveganj tudi po področjih poslovanja, v letu 2019 pa je uvedel še katalog tveganj na področju kritične infrastrukture in na področju izvajalcev bistvenih storitev. ELES je na podlagi Zakona o kritični infrastrukturi, usmeritev Ministrstva za obrambo, strokovnih usmeritev nosilcev sektorja kritične infrastrukture in lastne metodologije ocenjevanja tveganj pravočasno izvedel identifikacijo virov tveganj za delovanje kritične infrastrukture, analizo in ovrednotenje tveganj za delovanje kritične infrastrukture, določil vire tveganj, spremljal stanje kritične infrastrukture, imel podvojene centre vodenja in izdelal varnostne načrte. ELES je tudi imel dokumentiran sistem upravljanja varovanja informacij, v času revizijskega pregleda pa je zaključeval vpeljavo sistema upravljanja neprekinjenega poslovanja, kot to zahteva Zakon o informacijski varnosti. ELES je na podlagi zahtev nosilcev sektorja pripravil oceno tveganj za delovanje kritične infrastrukture in ukrepe za zaščito kritične infrastrukture. Menimo, da je ELES **učinkovito** implementiral zahteve zakonodaje na področju kritične infrastrukture in jih tudi izvaja.

ELES je zaznavanje kibernetskih groženj izvajal z dokumentiranim stanjem konfiguracij omrežij, analizo zaznanih dogodkov, sintezo zaznanih dogodkov iz različnih virov, implementacijo ukrepov, ki so bili posledica zaznanih dogodkov, ter s spremljavo omrežij, fizičnega okolja in aktivnosti zaposlenih in zunanjih izvajalcev. Preprečeval je aktiviranje zlonamerne programske kode in aktiviranje nepooblaščene prenosne kode. ELES je s stališča kibernetske varnosti ustrezno upravljal ponudnike zunanjih storitev ter preprečeval nepooblaščene dostope oseb, povezav, naprav in opreme. Zaradi nadgradenj informacijskih sistemov v letih 2019 in 2020 ELES ni izvedel vdornih testov, je pa redno preverjal in izvajal testiranje sistemov neprekinjenega napajanja, dizelskih agregatov, požarnih sistemov, klimatskih naprav in sistemov varnostnega operativnega centra. ELES je imel opredeljene vloge in odgovornosti za odkrivanje varnostnih dogodkov ter je izvajal različne aktivnosti odkrivanja. S pomočjo zunanjih vzdrževalcev je izvajal preverjanje procesov zaznavanja. ELES je imel vpeljane postopke posredovanja informacij o odkritih dogodkih, prav tako pa je nenehno izboljševal postopke zaznavanja in ustvarjal različne zbirke znanja, povezane z varnostnimi dogodki. Menimo, da je ELES **učinkovito** upravljal zaznavanje kibernetskih groženj, ima pa še možnosti za izboljšave, ki se jih zaveda in jih tudi aktivno načrtuje in implementira.

ELES je pri upravljanju odzivanja na kibernetske grožnje uporabljal načrt odzivanja. Zaposleni so bili usposobljeni za odzivanje ter so poročali o dogodkih in posredovali informacije o dogodkih

prejemnikom tako znotraj kot tudi izven ELES. Z nekaterimi organizacijami so imeli vpeljano prostovoljno izmenjavo informacij o incidentih. ELES je upravljanje odzivanja izvajal tudi z analiziranjem obvestil ter razumevanjem vpliva incidentov na organizacijo kakor tudi z razvrščanjem incidentov. ELES ni imel pooblaščenih in izurjenih strokovnjakov za izvajanje forenzičnih analiz, po potrebi je lahko k sodelovanju povabil zunanjo pomoč. ELES je imel vpeljane procese za spremljanje, analize in odzivanje na ranljivosti kakor tudi za omejevanje in blažitev incidentov. Prav tako je imel vzpostavljene postopke za upravljanje novih ugotovljenih ranljivosti. ELES je vključeval izkušnje, pridobljene na podlagi napak, vendar pa do konca obdobja, na katero se nanaša revizija, še ni imel izkušenj s kibernetskimi incidenti. ELES ni imel posebne strategije za področje kibernetske varnosti, je pa imel vzpostavljene politike za vse segmente integriranega sistema upravljanja, ki so se prek vodstvenega pregleda redno pregledovale in ustrezno dopolnjevale. Menimo, da je ELES **učinkovito** upravljal odzivanje na kibernetske grožnje, ima pa še možnosti za izboljšave, ki se jih zaveda in jih tudi uvaja.

4. Priporočila

ELES, d.o.o., sistemskemu operaterju prenosnega elektroenergetskega omrežja priporočamo, naj:

- občasno izvaja upravljanje prenosa električne energije iz rezervnega centra vodenja;
- vpelje označevanje verzij in datumov zadnjih sprememb tudi v dokumente omrežnih diagramov;
- prouči možnost vzpostavitve videonadzora vsaj v sistemskih prostorih in pred njimi, kjer imajo nameščene naprave drugi ponudniki storitev, če ne tudi v vseh ostalih sistemskih prostorih;
- prouči možnost namestitve kovinskih rešetk na vsa okna vseh sistemskih prostorov;
- redno – vsaj letno načrtuje in izvaja vdorna testiranja;
- občasno testira proces poročanja o varnostnih dogodkih;
- prouči možnost vzpostavitve zbirke znanja o zaznanih dogodkih.

Pravni pouk

Tega poročila na podlagi tretjega odstavka 1. člena Zakona o računskem sodišču ni dopustno izpodbijati pred sodišči in drugimi državnimi organi.

Tomaž Vesel,
generalni državni revizor

Poslano:

1. ELES, d.o.o., sistemskemu operaterju prenosnega elektroenergetskega omrežja, priporočeno;
2. Državnemu zboru Republike Slovenije, priporočeno;
3. arhivu.

Bdimo nad potmi javnega denarja

Računsko sodišče Republike Slovenije
The Court of Audit of the Republic of Slovenia
Slovenska cesta 50, 1000 Ljubljana, Slovenija
tel.: +386 (0) 1 478 58 00
fax: +386 (0) 1 478 58 91
sloaud@rs-rs.si
www.rs-rs.si