REPUBLIKA SLOVENIJA
RAČUNSKO SODIŠČE

REVIZIJSKO POROČILO

Učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji

2021

9 INDUSTRIJA, INOVACIJE IN INFRASTRUKTURA

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 zagotavljanja kibernetske varnosti v Republiki Sloveniji

Številka: 320-2/2019/31
Ljubljana, 3. marca 2021

Povzetek

Računsko sodišče je izvedlo revizijo učinkovitosti **Vlade Republike Slovenije** (v nadaljevanju: vlada), **Urada Vlade Republike Slovenije za varovanje tajnih podatkov** (v nadaljevanju: urad za varovanje tajnih podatkov) in **Ministrstva za javno upravo** (v nadaljevanju: ministrstvo) pri zagotavljanju kibernetske varnosti Republike Slovenije v obdobju od 1. 1. 2016 do 30. 9. 2019. Po mnenju računskega sodišča so bili vlada, urad za varovanje tajnih podatkov in ministrstvo v obdobju, na katero se nanaša revizija, **neučinkoviti.**

Vlada je februarja 2016 sprejela Strategijo kibernetske varnosti – vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti, v aprilu 2018 pa je bil na predlog vlade sprejet Zakon o informacijski varnosti, s katerim je bila v pravni red Republike Slovenije prenesena Direktiva (EU) 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Vlada bi morala nato v roku 1 leta sprejeti strategijo informacijske varnosti, vendar tega ni storila niti do konca obdobja, na katero se nanaša revizija. Seznam bistvenih storitev in metodologijo za določitev izvajalcev bistvenih storitev je vlada določila z več kot 7-mesečno zamudo. Ker ni pravočasno določila izvajalcev bistvenih storitev, je vlada prejela opomin Evropske komisije. Vlada tudi ni določila organov državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti. Kljub temu da je vlada strategijo kibernetske varnosti sprejela že na začetku leta 2016 in s sklepom urad za varovanje tajnih podatkov pooblastila za izvajanje nalog s področja kibernetske varnosti, pa v vsem tem obdobju ni sprejela akcijskega načrta oziroma drugega operativnega dokumenta za izvedbo ukrepov za zagotavljanje kibernetske varnosti. Vlada tudi ni zagotovila virov za izvajanje strategije kibernetske varnosti. V letu 2019 je sicer zagotovila pogoje za ustanovitev obeh v Zakonu o informacijski varnosti predvidenih organov, vendar pa ni opravila analize potreb po kadrovski in tehnološki okrepitvi, kakor tudi ni pravočasno zagotovila zadostnih sredstev za kadrovsko in tehnološko okrepitev na področju kibernetske varnosti. Poleg tega je v letu 2019, in sicer že nekaj mesecev pred v Zakonu o informacijski varnosti predvidenim rokom, ustanovila Upravo Republike Slovenije za informacijsko varnost. Vlada ni uvedla novih programov ozaveščanja na področju kibernetske varnosti in tudi ni uvedla vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja.

Urad za varovanje tajnih podatkov je v skladu s sklepom vlade področje kibernetske varnosti opredelil v okviru svoje organizacije, vendar pa je zaradi kadrovske in finančne podhranjenosti

aktivnosti izvajal le v zelo omejenem obsegu. Aktivno je sodeloval na mednarodnih vajah s področja kibernetske varnosti ter v okviru mednarodnih delovnih teles in združenj s področja kibernetske varnosti, nacionalne vaje s področja kibernetske varnosti pa zaradi pomanjkanja virov ni izvedel. Urad za varovanje tajnih podatkov je po januarju 2019 od nacionalnega centra SI-CERT ter ministrstva začel prejemati informacije o incidentih na področju kibernetske varnosti in o stanju na kibernetskem področju redno seznanjal Svet za nacionalno varnost.

Ministrstvo je z večmesečno zamudo sprejelo Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev, Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave pa je ministrstvo sprejelo s kar 12,5-mesečno zamudo. Ministrstvo ni pripravilo predloga strategije informacijske varnosti, katere sprejem je predvideval Zakon o informacijski varnosti, oziroma ni ocenilo, ali bi bilo treba obstoječo strategijo kibernetske varnosti zaradi novosprejete zakonodaje posodobiti ali spremeniti. Ministrstvo je izvedlo oceno kibernetskih tveganj, ni pa izvedlo analize stanja na področju kibernetske varnosti, na podlagi katere bi ocenilo potrebe in zagotovilo ustrezne vire, v oceni pa tudi ni navedlo konkretnih predlogov posameznih nalog za izboljšanje kibernetske varnosti. Ministrstvo tudi ni poskrbelo za izvajanje programov ozaveščanja na področju kibernetske varnosti, zagotavljalo pa je vire za delovanje nacionalnega centra SI-CERT ter pripravilo interne tečaje za informacijsko varnost. Ministrstvo je pravočasno vzpostavilo odzivni center za kibernetsko varnost organov državne uprave, sodelovalo je na mednarodnih vajah s področja kibernetske varnosti, prav tako je sodelovalo v okviru mednarodnih delovnih teles in združenj s področja kibernetske varnosti. Ministrstvo ni celovito spremljalo zagotavljanja pogojev in izvajanja nalog na področju kibernetske varnosti v skladu z Zakonom o informacijski varnosti, saj izvajalci bistvenih storitev niso bili določeni. Ministrstvo tudi ni prilagajalo ukrepov na področju zagotavljanja kibernetske varnosti, ki bi jih pripravilo na podlagi analize spremljanja zagotavljanja kibernetske varnosti.

Računsko sodišče je od vlade in ministrstva zahtevalo **predložitev odzivnih poročil,** v katerih morata izkazati popravljalne ukrepe, in podalo **priporočila** za izboljšanje stanja.

Kazalo

1. Uvod 8

1.1 Opredelitev revizije 8

1.2 Področje revizije 9

1.2.1 Kibernetska varnost v Republiki Sloveniji 9

1.2.2 Kibernetska varnost v svetu 11

1.3 Predstavitev revidirancev 15

1.3.1 Vlada Republike Slovenije 15

1.3.2 Urad Vlade Republike Slovenije za varovanje tajnih podatkov 16

1.3.3 Ministrstvo za javno upravo 18

1.3.4 Drugi deležniki revizije 20

1.4 Revizijski pristop 21

2. Vzpostavitev pogojev za zagotavljanje kibernetske varnosti 22

2.1 Strateški in pravni okvir 22

2.1.1 Strateški okvir 22

2.1.2 Prenos NIS direktive v slovenski pravni red 25

2.1.3 Podzakonski predpisi 27

2.1.4 Operativni dokumenti za izvajanje aktivnosti 27

2.1.5 Opredelitev vlog, nalog in pristojnosti 28

2.2 Organizacijska struktura za zagotavljanje kibernetske varnosti 34

2.2.1 Ustanovitev organov 34

2.2.2 Analiza potreb in zagotavljanje kadrovske in tehnološke okrepitve 38

2.2.3 Preverjanje varnosti in funkcionalnosti informacijske opreme 40

2.3 Pravne podlage za zagotavljanje kibernetske varnosti 41

2.3.1 Strateški in operativni dokumenti 41

2.3.2 Akti na podlagi ZInfV 41

3. Izvajanje nalog za zagotavljanje kibernetske varnosti 44

3.1 Vlada Republike Slovenije 44

3.1.1 Strategija informacijske varnosti 44

3.1.2 Preveritev potreb in zagotavljanje virov 45

3.1.3 Programi ozaveščanja 45

3.1.4 Uvajanje vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja 46

3.1.5 Spodbujanje razvoja in vpeljave novih tehnologij 46
3.1.6 Posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij 46
3.1.7 Zagotavljanje pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih 48
3.2 Urad Vlade Republike Slovenije za varovanje tajnih podatkov 49
3.2.1 Organiziranost urada za varovanje tajnih podatkov in kadri 49
3.2.2 Izvajanje nalog 50
3.2.3 Sodelovanje na mednarodnih vajah 54
3.2.4 Sodelovanje v mednarodnih delovnih telesih in združenjih 55
3.2.5 Nacionalne vaje 56
3.3 Ministrstvo za javno upravo 57
3.3.1 Predlog strategije informacijske varnosti 57
3.3.2 Priprava podzakonskih aktov in drugih aktov poslovanja 58
3.3.3 Analiza stanja na področju kibernetske varnosti in zagotavljanje virov 60
3.3.4 Izvajanje programov ozaveščanja 62
3.3.5 Uvedba vsebine s področja kibernetske varnosti v sistem izobraževanja in usposabljanja 63
3.3.6 Razvoj in vpeljava novih tehnologij 63
3.3.7 Sodelovanje v mednarodnih delovnih telesih in združenjih 64
3.3.8 Ocenjevanje tveganj za delovanje kritične infrastrukture 65
3.3.9 Načrtovanje ukrepov na podlagi ocen tveganj 65
4. Spremljanje izvajanja ukrepov za zagotavljanje kibernetske varnosti 67
4.1 Vlada Republike Slovenije 67
4.1.1 Seznanjanje s stanjem, spremljanje napredka in prilagajanje ukrepov 67
4.2 Urad Vlade Republike Slovenije za varovanje tajnih podatkov 68
4.2.1 Spremljanje delovanja sistema 68
4.2.2 Spremljanje priprave in izvajanja strategije informacijske varnosti 68
4.3 Ministrstvo za javno upravo 69
4.3.1 Spremljanje zagotavljanja pogojev in izvajanja nalog 69
4.3.2 Prilagajanje ukrepov 70
5. Mnenje 71
6. Zahteva za predložitev odzivnega poročila 73
7. Priporočila 75

1. Uvod

Revizijo učinkovitosti zagotavljanja kibernetske varnosti v Republiki Sloveniji smo izvedli na podlagi Zakona o računskem sodišču[1] (v nadaljevanju: ZRacS-1) in Poslovnika Računskega sodišča Republike Slovenije[2] ter v skladu z mednarodnimi revizijskimi standardi, ki jih določa Napotilo za izvajanje revizij[3].

S sklepom o izvedbi revizije[4] so bili za revidirance določeni Vlada Republike Slovenije, Urad Vlade Republike Slovenije za varovanje tajnih podatkov in Ministrstvo za javno upravo. Revizija je obsegala obdobje od 1. 1. 2016 do 30. 9. 2019.

Naša pristojnost je na podlagi izvedene revizije podati opisno mnenje o učinkovitosti zagotavljanja kibernetske varnosti v Republiki Sloveniji. Revizijo smo načrtovali in izvedli tako, da smo pridobili zadostna in ustrezna zagotovila za izrek mnenja.

1.1 Opredelitev revizije

Predmet revizije je bila učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji.

Cilj revizije je bil izrek mnenja o učinkovitosti poslovanja vlade, urada za varovanje tajnih podatkov in ministrstva pri zagotavljanju kibernetske varnosti v Republiki Sloveniji.

Da bi lahko izrekli mnenje, smo si zastavili glavno revizijsko vprašanje, **kako Republika Slovenija zagotavlja kibernetsko varnost.** Odgovor na glavno revizijsko vprašanje smo pridobili z odgovori na naslednja podvprašanja:

- ali sta vlada in ministrstvo vzpostavila in zagotovila pogoje za zagotavljanje kibernetske varnosti;
- ali so revidiranci učinkovito izvajali naloge za zagotavljanje kibernetske varnosti;
- ali so revidiranci spremljali izvajanje ukrepov za zagotavljanje kibernetske varnosti in jih po potrebi prilagajali.

V reviziji smo mnenje o učinkovitosti revidirancev oblikovali na podlagi vnaprej določenih sodil. Ocena je temeljila na presoji, ali sta vlada in ministrstvo vzpostavila in zagotovila pogoje za zagotavljanje kibernetske varnosti, ali so revidiranci učinkovito izvajali naloge, spremljali izvajanje ukrepov in po potrebi prilagajali ukrepe za zagotavljanje kibernetske varnosti. Vlada in ministrstvo sta vzpostavila pogoje, če je vlada oblikovala ustrezen strateški in pravni okvir, vzpostavila ustrezno organizacijsko strukturo za zagotavljanje kibernetske varnosti in je ministrstvo pripravilo ustrezne pravne podlage za zagotavljanje kibernetske varnosti. Vlada, urad za varovanje tajnih podatkov in ministrstvo so učinkovito izvajali naloge, spremljali izvajanje ukrepov in po potrebi prilagajali ukrepe za zagotavljanje

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. 320-2/2019/2 z dne 25. 1. 2019.

kibernetske varnosti, če so izvajali naloge, ki so bolj podrobno za vsakega revidiranca navedene v nadaljevanju.

Ker ni enotne terminologije za izraz kibernetska varnost in obstajajo različne definicije in razumevanje tega pojma tako v predpisih kot tudi med strokovnjaki, uporabljamo za namene tega revizijskega poročila pojem **kibernetska varnost** kot skupek dejavnosti, ki so potrebne za zaščito in varovanje omrežij in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje. Izraz **kibernetska grožnja** pa pomeni vsako potencialno okoliščino, dogodek ali dejanje, ki bi lahko poškodovalo, prekinilo ali drugače škodljivo vplivalo na omrežja in informacijske sisteme, uporabnike takih sistemov in druge osebe.

1.2 Področje revizije

1.2.1 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. Državni zbor Republike Slovenije (v nadaljevanju: državni zbor) je leta 2010 sprejel Resolucijo o strategiji nacionalne varnosti Republike Slovenije[5] (v nadaljevanju: ReSNV-1), v katero je pod točko 5.3.5 Odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov vključil tudi področje kibernetske varnosti ter določil, da:

- bo Republika Slovenija na področju kibernetske varnosti izdelala nacionalno strategijo za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij ter sprejela potrebne ukrepe za zagotovitev učinkovite kibernetske obrambe, v katero bosta v največji možni meri vključena javni in zasebni sektor;
- je ena od prioritetnih nalog na področju zagotavljanja kibernetske varnosti tudi ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost.

Državni zbor je konec septembra 2019 sprejel posodobljeno Resolucijo o strategiji nacionalne varnosti Republike Slovenije[6] (v nadaljevanju: ReSNV-2), ki navaja, da se bodo v mednarodnem varnostnem okolju pojavljale številne grožnje, med katerimi med najpomembnejše spadajo hibridne in informacijsko-kibernetske grožnje. ReSNV-2 navaja tudi, da je zagotavljanje suverenosti Republike Slovenije v kibernetskem prostoru izrednega pomena.

1.2.1.1 Strateške usmeritve

Prvi večji premik na področju normativnega urejanja kibernetske varnosti se je zgodil na začetku leta 2016, ko je vlada v februarju sprejela Srednjeročni obrambni program Republike

5 Uradni list RS, št. 56/01 in 27/10 – ReSNV-1.

6 Uradni list RS, št. 59/19.

Slovenije 2016–2020[7], 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 bila do leta 2020 v Slovenski vojski vzpostavljena enota za kibernetsko varnost.

Vlada je v februarju 2016 sprejela tudi Strategijo kibernetske varnosti – vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti[8] (v nadaljevanju: strategija kibernetske varnosti), ki predstavlja prvi korak za sistemsko ureditev področja in okrepitev zagotavljanja kibernetske varnosti. Okrepitev celotnega sistema informacijskih sistemov in omrežij je bila nujna zaradi vedno večjega pomena kibernetske varnosti za nemoteno delovanje sistemov, od katerih je v nekaterih pogledih odvisno delovanje celotne družbe. 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[9]. Strategija kibernetske varnosti vsebuje pregled obstoječega stanja na področjih, ki so pomembna za zagotavljanje kibernetske varnosti, opredeljuje vizijo in določa cilje na področju zagotavljanja kibernetske varnosti v Republiki Sloveniji. Strategija kibernetske varnosti opredeljuje tudi področja, na katerih se bo udejanjala, in tveganja, ki nastopajo v kibernetskem prostoru. Vizija strategije kibernetske varnosti določa, da bo Republika Slovenija do leta 2020 vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in tudi odpravljal posledice varnostnih incidentov.

V strategiji kibernetske varnosti je vlada opredelila tudi deležnike, ki sodelujejo v sistemu zagotavljanja kibernetske varnosti, in sicer so to organizacije iz javnega in zasebnega sektorja. Po sprejemu strategije kibernetske varnosti pa je vlada dopolnila tudi strokovne naloge in organizacijo urada za varovanje tajnih podatkov na področju kibernetske varnosti (več v točki 2.2 tega poročila).

V marcu 2016 je vlada potrdila dokument Digitalna Slovenija 2020 – Strategija razvoja informacijske družbe do leta 2020[10] (v nadaljevanju: Digitalna Slovenija 2020), ki določa ključne strateške razvojne usmeritve, skupaj s strategijo kibernetske varnosti in Načrtom razvoja širokopasovnih omrežij naslednje generacije do leta 2020[11] pa to področje povezuje v enovit strateški okvir.

1.2.1.2 Zakon o informacijski varnosti

Sprejemu strategije kibernetske varnosti je sledil še sprejem Zakona o informacijski varnosti[12] (v nadaljevanju: ZInfV) v letu 2018, s katerim je Republika Slovenija prvič celovito in sistemsko

7 [URL: http://mo.arhiv-spletisc.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/predpisi/obramba/SOPR2016_2020.pdf], 26. 2. 2021.

8 Sprejeta na 76. redni seji vlade z dne 25. 2. 2016, [URL: http://uvtp.arhiv-spletisc.gov.si/fileadmin/uvtp.gov.si/pageuploads/Startegija_KV.pdf], 26. 2. 2021.

9 Povzeto po strategiji kibernetske varnosti.

10 [URL: http://mju.arhiv-spletisc.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/DSI_2020.pdf], 26. 2. 2021.

11 [URL: http://mju.arhiv-spletisc.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/NGN_2020.pdf], 26. 2. 2021.

12 Uradni list RS, št. 30/18.

uredila področje informacijske varnosti. Republiko Slovenijo so k zakonski ureditvi področja informacijske varnosti spodbujali in zavezovali že sprejeti strateški nacionalni in mednarodni dokumenti, predvsem ReSNV-1, Strategija kibernetske varnosti Evropske unije – "Odprt, varen in zavarovan kibernetski prostor"[13], strategija kibernetske varnosti in Direktiva (EU) 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji[14] (v nadaljevanju: NIS direktiva). Države članice so jo morale v svoj pravni red prenesti do 9. 5. 2018, kar je Republika Slovenija storila s sprejemom ZInfV. NIS direktiva je določila tudi, da morajo države članice Evropske unije do 9. 11. 2018 določiti izvajalce bistvenih storitev s sedežem na svojem ozemlju.

ZInfV 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.

Z ZInfV so bili med drugim v pravni red preneseni in določeni tudi naslednji ključni pojmi:

- **informacijska varnost** – kot zaščita, varovanje in obramba informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti;
- **informacijsko okolje** – kot skupek družbenih omrežij in kibernetskega prostora vključno z informacijami;
- **kibernetska varnost** – kot sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi;
- **kibernetski prostor** – kot globalno informacijsko okolje, ustvarjeno s pomočjo elektronskih komunikacijskih omrežij in informacijskih sistemov; kibernetski prostor omogoča nastanek, obdelavo in izmenjavo informacij.

1.2.2 Kibernetska varnost v svetu

Področje kibernetske varnosti ni novost in se v zadnjem desetletju vse hitreje razvija. Kljub globalni povezanosti kibernetskega prostora in pogosto nadnacionalnega značaja groženj pa imajo države po svetu zelo različen pristop do regulacije ter izvajanja aktivnosti na tem področju. Posledično zagotavljajo kibernetsko varnost na različne načine in v različnem obsegu. Razvite države in Evropska unija se vse bolj zavedajo pomena kibernetske varnosti za demokracijo, gospodarstvo in življenja posameznikov, zato se to področje tudi v okviru strateškega urejanja in zakonodaje v zadnjih letih pospešeno razvija. Kibernetski kriminal naj bi po oceni družbe McAfee svet v letu 2017 stal kar 600 milijard USD oziroma 0,8 % globalnega BDP[15]. Po podatkih inštituta Ponemon pa naj bi

13 [URL: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf], 26. 2. 2021.

14 UL L št. 194 z dne 19. 7. 2016, str. 1.

15 [URL: https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html], 26. 2. 2021.

kibernetski napad v letu 2019, pri katerem je prišlo do nepooblaščenega dostopa do podatkov, v povprečju stal 3,92 milijona USD[16].

Tudi Svetovni gospodarski forum v svojem poročilu o globalnih tveganjih za leto 2019[17] ugotavlja, da so v zadnjih letih kibernetski napadi vse višje na lestvici globalnih tveganj, in sicer so tako po verjetnosti nastanka kot po učinku uvrščeni v prvo deseterico. V poročilu so bili kibernetski napadi po verjetnosti uvrščeni na 5. mesto, takoj za krajo podatkov, po učinku pa so bili na 7. mestu, tik pred prenehanjem delovanja kritične infrastrukture. V skupni oceni so kibernetski napadi med najvišje uvrščenimi grožnjami[18]. Škoda oziroma stroški, povezani s kibernetskimi napadi, so na ravni držav zelo različni, saj nanje vplivajo številni in različni dejavniki. Prav tako države zelo različno načrtujejo višino finančnih sredstev za izboljšanje kibernetske varnosti. Velika Britanija, kot ena izmed vodilnih držav na področju kibernetske varnosti, je za obdobje 2016–2021 načrtovala 1,9 milijarde GBP[19]. Evropsko računsko sodišče v svojem obvestilu[20] poudarja, da je globalno ocenjeno, da države za kibernetsko varnost namenjajo 0,1 % svojega BDP. Enak delež namenja tudi Zvezna vlada Združenih držav Amerike, kar je za leto 2019 znašalo 21 milijard USD. Sicer pa Združene države Amerike skupaj z zasebnim sektorjem za to področje namenjajo 0,35 % BDP. Evropske države zaenkrat za to področje načrtujejo mnogo manj sredstev, nekatere zgolj desetino ameriškega zneska, druge pa še manj.

V času priprave tega poročila ni obstajala enotna metodologija za ocenjevanje pripravljenosti posameznih držav na kibernetske napade oziroma njihovo odpornost na kibernetske nevarnosti. V mnogih različnih ocenah pa so na vrhu seznamov najbolje pripravljenih večje države, kot so Velika Britanija, Združene države Amerike, Francija, Ruska federacija, Kitajska, Kanada, kakor tudi nekaj manjših, kot so Izrael, Latvija, Estonija in Gruzija. Slovenija na lestvicah običajno zaseda položaje med 30. in 50. mestom.

Agencija Evropske unije za kibernetsko varnost[21] (v nadaljevanju: ENISA) vsako leto pripravi poročilo o kibernetskih grožnjah[22]. V poročilu za leto 2018 je kot nekatere glavne trende na področju kibernetske varnosti navedla, da:

- elektronska pošta in zvabljanje[23] kot načina izrabe človeškega faktorja spadata med primarne vektorje okužbe s škodljivo kodo;
- je vse več kibernetskih napadov, ki so vodeni oziroma sponzorirani s strani tujih držav, usmerjenih v banke;

16 [URL: https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/], 26. 2. 2021.

17 The Global Risks Report 2019, [URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf], 26. 2. 2021.

18 Poročilo kot najbolj verjetne in najbolj vplivne navaja tveganja, povezana z ekstremnimi vremenskimi dogodki, neprilagajanje na klimatske spremembe in naravne nesreče.

19 Progress of the 2016-2021 National Cyber Security Programme, [URL: https://www.nao.org.uk/wp-content/uploads/2019/03/Progress-of-the-2016-2021-National-Cyber-Security-Programme.pdf], 26. 2. 2021.

20 Challenges to effective EU cybersecurity policy, Briefing Paper, [URL: https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=49416], 26. 2. 2021.

21 Angl.: European Union Agency for Cybersecurity.

22 ENISA Threat Landscape Report 2018, 15 Top Cyberthreats and Trends, [URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018], 26. 2. 2021.

23 Angl.: *phishing.*

- bodo države in proizvajalci morali v prihodnosti obravnavati vprašanje odsotnosti oziroma pomanjkanja rešitev za kibernetsko varnost, namenjenih manjšim organizacijam, podjetjem in končnim uporabnikom.

ENISA vsako leto v poročilu predstavi tudi 15 najpogostejših kibernetskih groženj. Tabela 1 prikazuje stanje in trende 15 najpogostejših kibernetskih groženj v letih 2017 in 2018.

Tabela 1: Najpogostejše kibernetske grožnje v letih 2017 in 2018

Najpogostejše grožnje 2017	Trendi 2017	Najpogostejše grožnje 2018	Trendi 2018	Sprememba na lestvici
1. Škodljiva koda (angl.: *malware*)	→	1. Škodljiva koda	→	→
2. Spletni napadi (angl.: *web based attacks*)	↑	2. Spletni napadi	↑	→
3. Napadi na spletne aplikacije (angl.*: web application attacks*)	↑	3. Napadi na spletne aplikacije	→	→
4. Zvabljanje (angl.: *phishing*)	↑	4. Zvabljanje	↑	→
5. Neželena elektronska pošta (angl.: *spam*)	↑	5. Onemogočanje storitev	↑	↑
6. Onemogočanje storitev (angl.: *denial of service*)	↑	6. Neželena elektronska pošta	→	↓
7. Izsiljevalsko programje (angl.: *ransomware*)	↑	7. Botneti	↑	↑
8. Botneti (angl.: botnets)	↑	8. Kršitve podatkov	↑	↑
9. Grožnje od znotraj (angl.: *insider threat*)	→	9. Grožnje od znotraj	↓	→
10. Fizična manipulacija/poškodba/kraja/ izguba (angl.*: physical manipulation/ damage/theft/loss*)	→	10. Fizična manipulacija/ poškodba/kraja/izguba	→	→
11. Kršitve podatkov (angl.: *data breaches*)	↑	11. Odtekanje informacij	↑	↑
12. Kraja identitete (angl.: *identity theft*)	↑	12. Kraja identitete	↑	→
13. Odtekanje informacij (angl.: *information leakage*)		13. Kraja procesorske moči (angl.: cryptojacking)	↑	Novo
14. Kompleti za izkoriščanje (angl.: *exploit kits*)	↓	14. Izsiljevalsko programje	↓	↓
15. Kibernetsko vohunjenje (angl.: *cyber espionage*)	↑	15. Kibernetsko vohunjenje	↓	→

Legenda: ↑ – trend rasti; ↓ – trend upadanja; → – nespremenjeno.
Vir: podatki ENISA[24].

Kibernetska varnost je bila v zadnjih letih tudi vse bolj pogosto na agendi institucij Evropske unije. Prizadevajo si, da bi bil skupni kibernetski prostor Evropske unije odprt, stabilen in varen. Predsednik Evropske komisije je leta 2017 v govoru o stanju v Evropski uniji poudaril, da lahko kibernetski napadi bolj ogrožajo stabilnost demokracij in gospodarstev kot orožje in tanki. V letu 2016 je bilo v Evropi dnevno več kot 4.000 napadov z izsiljevalskim programjem, 80 % podjetij

[24] Tako kot sprotna opomba 22.

pa je bilo žrtev vsaj enega kibernetskega incidenta, zato je v imenu Evropske komisije napovedal nova orodja in ukrepe[25].

Evropska unija je na področjih, ki so povezana s kibernetsko varnostjo, sprejela več strateških dokumentov. Med njimi izpostavljamo:

- Evropsko varnostno strategijo[26] (angl.: *European Security Strategy – A secure Europe in a better world*), december 2003;
- posodobitev Evropske varnostne strategije[27] (angl.: *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*), november 2010;
- Globalno strategijo Evropske unije[28] (angl.*: Shared Vision, Common Action: A Stronger Europe; A Global Strategy for the European Union's Foreign And Security Policy*), junij 2016;
- Varnostno agendo Evropske unije[29] (angl.: *EU Agenda on Security*), april 2015;
- Strategijo za enotni digitalni trg za Evropo[30] (angl.: *A Digital Single Market Strategy for Europe*), maj 2015.

Evropska unija je poleg NIS direktive sprejela tudi več drugih predpisov, dogovorov in aktov za zaščito skupnega kibernetskega prostora. Pri tem velja omeniti zlasti sprejem medinstitucionalnega dogovora[31], s katerim je bila decembra 2017 ustanovljena stalna skupina za odzivanje na računalniške grožnje[32] na ravni Evropske unije, v letu 2019 pa je bil sprejet akt o kibernetski varnosti[33], s katerim je bila med drugim okrepljena in razširjena tudi vloga ENISA. Pomemben korak v boju proti kibernetskim napadom pa je Svet Evropske unije storil, ko je maja 2019 sprejel Sklep o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice[34]. S tem sklepom je Evropska unija vzpostavila okvir, ki ji omogoča tudi, da naloži sankcije pravnim ali fizičnim osebam, ki so odgovorne za kibernetske napade ali poskuse kibernetskih napadov, zagotavljajo finančno, tehnično ali materialno podporo za kibernetske napade ali so kako drugače vpletene. Pomembno pa je, da se navedeni okvir lahko uporablja tudi pri kibernetskih napadih, usmerjenih zoper tretje države, ki niso članice Evropske unije, ali zoper mednarodne organizacije, če se omejevalni ukrepi zdijo potrebni za doseganje ciljev skupne zunanje in varnostne politike[35].

25 [URL: https://europa.eu/rapid/press-release_SPEECH-17-3165_sl.htm], 26. 2. 2021.

26 [URL: https://www.cvce.eu/content/publication/2004/10/11/1df262f2-260c-486f-b414-dbf8dc112b6b/publishable_en.pdf], 26. 2. 2021.

27 [URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF], 26. 2. 2021.

28 [URL: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf], 26. 2. 2021.

29 [URL: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf], 26. 2. 2021.

30 [URL: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:52015DC0192], 26. 2. 2021.

31 [URL: https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:32018Q0113(01)], 26. 2. 2021.

32 Angl.: *Computer Emergency Response Team*.

33 Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (v nadaljevanju: akt o kibernetski varnosti; UL L št. 151 z dne 7. 6. 2019, str. 15).

34 Sklep Sveta (SZVP) 2019/797 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice (UL L št. 129/13 z dne 17. 5. 2019, str. 1).

35 [URL: https://www.consilium.europa.eu/sl/policies/cybersecurity/], 26. 2. 2021.

Nacionalni odzivni center za kibernetsko varnost[36] (v nadaljevanju: nacionalni CSIRT) je v letnem poročilu o kibernetski varnosti[37] opozoril, da se je v Sloveniji opazno povečalo število napadov na podjetja, ki so vse pogosteje tarča kibernetskih kriminalcev. Nacionalni CSIRT poroča, da so napadi na manjša in srednje velika podjetja vse bolj pogosti, saj ta podjetja ne namenjajo zadostne pozornosti informacijski varnosti, kar spletni goljufi uspešno izkoriščajo. Najbolj pomembne vrste kibernetskih napadov na podjetja, ki jih je nacionalni CSIRT obravnaval v letu 2018, so bile: direktorska prevara, vrivanje v poslovno komunikacijo in okužbe z izsiljevalskimi virusi. Pri tem poudarja, da gre za napade, ki lahko povzročijo znatno finančno škodo[38] ter za več dni onemogočijo poslovanje[39].

1.3 Predstavitev revidirancev

1.3.1 Vlada Republike Slovenije

Vlada je v skladu z Zakonom o Vladi Republike Slovenije[40] organ izvršilne oblasti in najvišji organ državne uprave Republike Slovenije, ki določa, usmerja in usklajuje izvajanje politike države. V ta namen izdaja predpise in sprejema druge pravne, politične, ekonomske, finančne, organizacijske in druge ukrepe, ki so potrebni za zagotovitev razvoja države in za urejenost razmer na vseh področjih iz pristojnosti države. Vlado sestavljajo ministrice ali ministri, vodi in usmerja jo predsednik vlade, ki skrbi za enotnost politične in upravne usmeritve vlade, usklajuje delo ministrov, predstavlja vlado ter sklicuje in vodi njene seje. Ministri morajo obveščati vlado o vseh vprašanjih, ki so pomembna za odločanje in izvajanje vladne politike. Za delo vlade so skupno odgovorni vsi njeni člani, za delo posameznega ministrstva pa pristojni minister.

Vlada je odgovorna za izvajanje zakonov in drugih predpisov državnega zbora ter za celotno delovanje državne uprave. Vlada usmerja državno upravo prek ministrov, nadzoruje delo ministrstev, jim daje smernice za izvajanje politike in za izvrševanje zakonov, drugih predpisov in splošnih aktov ter skrbi, da ministrstva usklajeno izvršujejo svoje naloge.

Republika Slovenija je NIS direktivo v slovenski pravni red prenesla z uveljavitvijo ZInfV maja 2018. V skladu z ZInfV vlada med drugim:

- določi seznam bistvenih storitev iz predpisa, ki ureja standardno klasifikacijo dejavnosti;

36 Angl.: *Computer Security Incident Response Team,* [URL: https://www.cert.si/], 26. 2. 2021.

37 Poročilo o kibernetski varnosti za leto 2018, [URL: https://www.cert.si/wp-content/uploads/2019/09/Poročilo-o-kibernetski-varnosti_2018_splet.pdf], 26. 2. 2021.

38 Po podatkih nacionalnega CSIRT je povprečno oškodovanje v direktorjevi prevari v letu 2018 znašalo 40.000 EUR, oškodovanje tujega partnerja pri vrivanju v poslovno komunikacijo pa 178.000 EUR.

39 V avgustu 2019 je javni zavod Lekarna Ljubljana, največji javni lekarniški zavod v Sloveniji, ki svojo dejavnost opravlja v 52 lekarnah in lekarniških podružnicah v Ljubljani in okolici, doživel kibernetski napad z izsiljevalskim virusom, kar je začasno onemogočilo delovanje informacijskega sistema v vseh enotah zavoda ter spletni lekarni. Reševanje incidenta je trajalo več dni, najprej je zavod odprl enote za izdajo zdravil na papirni recept, nekaj dni kasneje pa je ponovno vzpostavil informacijski sistem in aktiviral 1 lekarno, kjer je potekala izdaja zdravil na elektronski recept. Zavod je postopoma aktiviral posamezne lekarne, šele po tednu dni pa so znova delovale vse enote razen spletne lekarne.

40 Uradni list RS, št. 24/05-UPB1, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14 in 55/17.

- določi posameznega izvajalca bistvenih storitev;
- določi metodologijo za določitev izvajalcev bistvenih storitev;
- določi organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti;
- sprejme strategijo informacijske varnosti.

Vlada je 19. 4. 2018 sprejela Uredbo o informacijski varnosti v državni upravi[41] (v nadaljevanju: uredba o IVvDU), ki med drugim določa minimalne skupne zahteve glede informacijske varnosti, ki jih sestavljajo enotni okviri upravljanja informacijske varnosti in temeljna nadzorstva za zagotavljanje informacijske varnosti v državni upravi.

V tabeli 2 so navedene odgovorne osebe vlade v obdobju, na katero se nanaša revizija, in med izvajanjem revizije.

Tabela 2: Odgovorne osebe vlade v obdobju, na katero se nanaša revizija, in med izvajanjem revizije

Odgovorna oseba	Obdobje odgovornosti
dr. Miroslav Cerar, predsednik vlade	do 13. 9. 2018
Marjan Šarec, predsednik vlade	od 13. 9. 2018 do 13. 3. 2020
Janez Janša, predsednik vlade	od 13. 3. 2020

1.3.2 Urad Vlade Republike Slovenije za varovanje tajnih podatkov

Urad za varovanje tajnih podatkov je vladna služba, ki opravlja naloge nacionalnega varnostnega organa na področju določanja in varovanja tajnih podatkov. V letu 2017 je vlada poverila uradu za varovanje tajnih podatkov dodatne naloge, in sicer kot nacionalnemu organu za področje zagotavljanja kibernetske varnosti. Vzpostavitev nacionalnega organa za kibernetsko varnost je kot eno izmed prioritetnih nalog predvidela že ReSNV-1 v letu 2010. Vzpostavitev nacionalnega organa za kibernetsko varnost so zahtevali tudi strategija kibernetske varnosti, NIS direktiva in ZInfV, z njegovo vzpostavitvijo pa je Republika Slovenija izpolnila tudi zavezo, dano zvezi[42] NATO.

Urad za varovanje tajnih podatkov je v letu 2017 dobil naslednje pristojnosti za opravljanje nalog na področju kibernetske varnosti[43]:

- usklajevanje zmogljivosti za zagotavljanje kibernetske varnosti;
- sodelovanje z ustreznimi organi Evropske unije, zveze NATO in organi drugih mednarodnih organizacij in držav ter skrb za izvajanje sprejetih mednarodnih obveznosti in mednarodnih pogodb na področju kibernetske varnosti;

41 Uradni list RS, št. 29/18.

42 [URL: http://uvtp.arhiv-spletisc.gov.si/si/medijsko_sredisce/novica/1360/], 26. 2. 2021.

43 Sklep o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljevanju: sklep o uradu za varovanje tajnih podatkov 2017; Uradni list RS, št. 17/17).

- usklajevanje izvajanja strategije kibernetske varnosti;
- sodelovanje pri načrtovanju postopkov in ukrepov na področju tveganj ter varnosti omrežij in informacijskih sistemov;
- vključevanje v izobraževalni proces na področju kibernetske varnosti;
- sodelovanje pri načrtovanju postopkov in ukrepov za obvladovanje kibernetskih incidentov;
- sodelovanje z znanstvenoraziskovalnimi ustanovami in zasebnim sektorjem pri spodbujanju in krepitvi kibernetske varnosti in odpornosti ključne informacijsko-komunikacijske infrastrukture;
- spremljanje zmogljivosti za zagotavljanje kibernetske varnosti na državni ravni;
- sodelovanje pri organizaciji in usklajevanju državne vaje iz kibernetske varnosti ter pri usklajevanju mednarodnih vaj iz kibernetske varnosti;
- sodelovanje pri spremljanju kibernetskih incidentov na državni ravni;
- sodelovanje pri usklajevanju in usmerjanju delovanja skupin za odzivanje na kibernetske incidente v Republiki Sloveniji;
- sodelovanje pri zagotavljanju zgodnjega obveščanja, opozarjanja in informiranja vseh deležnikov o tveganjih in kibernetskih incidentih;
- sodelovanje v mednarodni mreži organov, pristojnih za odzivanje na kibernetske incidente.

ZInfV je predvidel ustanovitev pristojnega nacionalnega organa kot novega organa za področje kibernetske varnosti ter določil, da bo ta z delovanjem začel najkasneje do 1. 1. 2020. ZinfV je določil, da do začetka delovanja pristojnega nacionalnega organa v prehodnem obdobju naloge na področju kibernetske varnosti opravlja urad za varovanje tajnih podatkov, razen nalog upravnega odločanja in nadzora, ki jih opravlja ministrstvo.

Pristojni nacionalni organ oziroma do njegove vzpostavitve urad za varovanje tajnih podatkov med drugim izvaja naslednje naloge:

- koordinira delovanje sistema informacijske varnosti;
- razvija zmogljivosti za izvajanje kibernetske obrambe;
- vsem zavezancem pri izvajanju njihovih nalog nudi strokovno podporo na področju informacijske varnosti;
- zagotavlja analize, metodološko podporo in preventivno delovanje na področju informacijske varnosti ter daje mnenja s področja svojih prisotnosti;
- sodeluje z organi in organizacijami, ki delujejo na področju informacijske varnosti, predvsem z nacionalnim CSIRT in skupino za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave (v nadaljevanju: CSIRT organov državne uprave), z varnostno-operativnimi centri, z regulatorji oziroma nadzorniki področij iz drugega odstavka 5. člena ZInfV, z Agencijo za komunikacijska omrežja in storitve Republike Slovenije (v nadaljevanju: AKOS), z Informacijskim pooblaščencem in z organi kazenskega pregona ter s ponudniki varnostnih rešitev;
- zavezance ozavešča o pomembnosti prijave incidenta z vsemi znaki kaznivega dejanja, ki se preganja po uradni dolžnosti, organom kazenskega pregona skladno s Kazenskim zakonikom[44];

[44] Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20 in 91/20.

- koordinira usposabljanje, vaje in izobraževanje na področju informacijske varnosti ter skrbi za dvig zavedanja javnosti o informacijski varnosti;
- spodbuja in podpira raziskave in razvoj na področju informacijske varnosti;
- izvaja testiranja informacijsko-komunikacijskih tehnologij na področju informacijske varnosti;
- skrbi za pripravo in izvajanje strategije informacijske varnosti;
- izdela nacionalni načrt odzivanja na incidente ob upoštevanju strategije informacijske varnosti, načrtov nacionalnega CSIRT in CSIRT organov državne uprave, drugih pristojnih organov ter varnostne dokumentacije zavezancev;
- pregleduje ustreznost določitve izvajalcev bistvenih storitev in organov državne uprave vsaj vsaki 2 leti ter vladi lahko predlaga posodobitev določitev;
- za namene pregleda NIS direktive Evropsko komisijo vsaj vsaki 2 leti obvešča o ukrepih za določitev storitev izvajalcev bistvenih storitev, njihovem številu ter pomenu, o seznamu bistvenih storitev ter pragih za določitev ustrezne ravni opravljanja storitev izvajalcev bistvenih storitev glede na število uporabnikov ali glede na pomen zadevnega izvajalca bistvenih storitev;
- je enotna kontaktna točka za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic Evropske unije ter z mrežo skupin CSIRT in s skupino za sodelovanje, v katero prispeva svojega predstavnika;
- izpolnjuje druge obveznosti obveščanja Evropske komisije in skupine za sodelovanje, obveznosti obveščanja in notifikacije preostalih mednarodnih organizacij;
- izvaja druge naloge mednarodnega sodelovanja.

V tabeli 3 so navedene odgovorne osebe urada za varovanje tajnih podatkov v obdobju, na katero se nanaša revizija, in med izvajanjem revizije.

Tabela 3: Odgovorne osebe urada za varovanje tajnih podatkov v obdobju, na katero se nanaša revizija, in med izvajanjem revizije

Odgovorna oseba	Obdobje odgovornosti
Boris Mohar, direktor	do 16. 2. 2017
mag. Dobran Božič[45], direktor	od 17. 2. 2017 do 13. 9. 2018
mag. Nataša Dolenc[46], direktorica	od 13. 9. 2018 do 21. 7. 2019
Igor Eršte, direktor[47]	od 22. 7. 2019

1.3.3 Ministrstvo za javno upravo

Ministrstvo v skladu s 34.a členom Zakona o državni upravi[48] opravlja naloge na področju javne uprave, sistemskega urejanja organiziranosti in delovanja javnega sektorja, sistema javnih

45 Mag. Dobran Božič je bil v obdobju od 17. 2 2017 do 6. 10. 2017 v. d. direktorja.

46 Mag. Nataša Dolenc je bila v obdobju od 13. 9. 2018 do 8. 3. 2019 v. d. direktorice.

47 Igor Eršte je bil v obdobju od 22. 7. 2019 do 9. 1. 2020 v. d. direktorja.

48 Uradni list RS, št. 113/05-UPB4, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14 in 51/16.

uslužbencev, plačnega sistema v javnem sektorju, javnih naročil, volilne in referendumske zakonodaje, sistemskega urejanja splošnega upravnega postopka, sistemskega urejanja upravnih taks, upravnega poslovanja, upravljanja z informacijsko-komunikacijskimi sistemi in zagotavljanja elektronskih storitev javne uprave, zagotavljanja delovanja državnega portala eUprava, varnih predalov, centralne storitve za spletno prijavo in elektronski podpis, informacijske družbe, elektronskih komunikacij, dostopa do informacij javnega značaja, delovanja nevladnih organizacij, lokalne samouprave, kakovosti javne uprave, boljše zakonodaje ter odprave administrativnih ovir in naloge na področju sistemskega urejanja ravnanja s stvarnim premoženjem države in lokalnih skupnosti, centraliziranega ravnanja s stvarnim premoženjem države, načrtovanja in koordiniranja prostorskih potreb organov državne uprave ter druge naloge na področju ravnanja s stvarnim premoženjem v skladu s predpisi ali aktom vlade[49].

V skladu z ZInfV minister, pristojen za informacijsko družbo, podrobneje določi vsebino in strukturo varnostne dokumentacije, ki jo izvajalci bistvenih storitev vzpostavijo in vzdržujejo za zagotavljanje informacijske varnosti ter visoke ravni varnosti omrežij in informacijskih sistemov, ter minimalen obseg in vsebino varnostnih ukrepov, ki jih na podlagi varnostne dokumentacije pripravijo in izvajajo izvajalci bistvenih storitev. Minister predpiše tudi metodologijo za pripravo analize obvladovanja tveganj ter za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov v zvezi s politiko neprekinjenega poslovanja z načrtom njegovega upravljanja in seznamom ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so ključnega pomena za delovanje bistvenih storitev. V okviru ministrstva je v skladu z ZInfV 1. 1. 2019 začel delovati CSIRT organov državne uprave, ki ima predvsem naslednje pristojnosti:

- sprejema, obravnava in ocenjuje priglasitve incidentov, ki mu jih posredujejo organi državne uprave[50], za katere je pristojen, ter te podatke evidentira, hrani in varuje;
- organom državne uprave nudi metodološko podporo, pomoč in sodelovanje ob pojavu incidenta;
- sodeluje z nacionalnim CSIRT in s pristojnim nacionalnim organom ter jima na poziv na varen način nudi informacije o izvajanju svojih pristojnosti;
- objavlja opozorila o tveganjih in ranljivostih na področju informacijske varnosti organov državne uprave.

S 1. 7. 2019 je začela delovati Uprava Republike Slovenije za informacijsko varnost (v nadaljevanju: uprava za informacijsko varnost) s sedežem na ministrstvu, kar je pomenilo začetek vzpostavljanja pristojnega nacionalnega organa. Uprava za informacijsko varnost ima kot pristojni nacionalni organ naslednje pristojnosti[51]:

- odloča o sprejemu ukrepov ob težjem ali kritičnem incidentu ali kibernetskem napadu kot tudi stanju povečane ogroženosti;

---

49 Do 22. 7. 2016 je naloge na področju informacijske družbe in elektronskih komunikacij v skladu z 39. členom Zakona o državni upravi (Uradni list RS, št. 90/14) opravljalo Ministrstvo za izobraževanje, znanost in šport (v nadaljevanju: MIZŠ).

50 V skladu z 18. členom ZInfV organi državne uprave brez nepotrebnega odlašanja CSIRT organov državne uprave priglasijo incidente s pomembnim vplivom na neprekinjeno izvajanje storitev organov državne uprave, tisti organi državne uprave, ki imajo lastne zmogljivosti vsaj na ravni varnostno-operativnega centra, pa pristojnemu nacionalnemu organu.

51 Uredba o spremembah in dopolnitvah Uredbe o organih v sestavi ministrstev (Uradni list RS, št. 52/18).

- odloča v postopkih nadzora v skladu z zakonom, ki ureja informacijsko varnost;
- vodi seznam kontaktnih podatkov zavezancev ter skupni seznam incidentov in kibernetskih napadov;
- obvešča javnosti o incidentih in v zvezi z njimi sprejetih ukrepih;
- izpolnjuje mednarodne obveznosti in opravlja naloge mednarodne izmenjave podatkov, vključno z izvajanjem nalog enotne kontaktne točke in sodelovanja s pristojnimi organi s področja informacijske varnosti v Evropski uniji, določene z zakonom, ki ureja informacijsko varnost;
- opravlja koordinacijske, strokovno-tehnične, organizacijske in razvojne naloge na področju informacijske varnosti in kibernetske obrambe, določene z zakonom, ki ureja informacijsko varnost, in njegovimi podzakonskimi predpisi;
- izvaja naloge spremljanja in poročanja na podlagi zakona, ki ureja dostopnost spletišč in mobilnih aplikacij;
- odloča v postopkih nadzora skladno z zakonom, ki ureja dostopnost spletišč in mobilnih aplikacij.

V tabeli 4 so navedene odgovorne osebe ministrstva v obdobju, na katero se nanaša revizija, in med izvajanjem revizije.

Tabela 4: Odgovorne osebe ministrstva v obdobju, na katero se nanaša revizija, in med izvajanjem revizije

Odgovorna oseba	Obdobje odgovornosti
Boris Koprivnikar, minister za javno upravo	do 13. 9. 2018
Rudi Medved, minister za javno upravo	od 13. 9. 2018 do 13. 3. 2020
Boštjan Koritnik, minister za javno upravo	od 13. 3. 2020

1.3.4 Drugi deležniki revizije

Na področju kibernetske varnosti v Republiki Sloveniji je več drugih deležnikov, ki pa jih v reviziji nismo določili kot revidirance. Med drugim so sodelovali pri pripravi strategije kibernetske varnosti (več v točki 2.1.1.b tega poročila):

- Agencija za energijo,
- AKOS,
- Ministrstvo za finance,
- Ministrstvo za gospodarski razvoj in tehnologijo,
- Ministrstvo za infrastrukturo,
- MIZŠ,
- Ministrstvo za notranje zadeve,
- Ministrstvo za notranje zadeve – Policija,
- Ministrstvo za obrambo,
- Ministrstvo za zdravje,
- Ministrstvo za zunanje zadeve,

- SI-CERT[52],
- Slovenska obveščevalno-varnostna agencija (v nadaljevanju: SOVA),
- Svet za nacionalno varnost.

1.4 Revizijski pristop

Za pridobitev informacij, potrebnih za presojo **učinkovitosti** vlade, urada za varovanje tajnih podatkov in ministrstva **pri zagotavljanju kibernetske varnosti v Republiki Sloveniji,** smo uporabili kvalitativne in kvantitativne metode ter tehnike revidiranja, in sicer:

- proučevanje pravnih, strateških in drugih podlag, ki opredeljujejo obravnavano področje revizije, ter javno dostopnih podatkov s področja revizije;
- zbiranje, pregled in presojo dokumentacije revidiranega področja;
- pregled pridobljenih podatkov in informacij o vsebini ter poteku dosedanjih aktivnosti revidiranega področja;
- intervjuje pri revidirancih in drugih subjektih, ki so ali so bili (ne)posredno vključeni v revidirano področje ali pa so strokovnjaki na področju kibernetske varnosti;
- pisna vprašanja revidirancem;
- pregled spletnih strani, medijskih poročil in drugih javno dostopnih virov, ki so povezani s področjem revizije.

52 SI-CERT – nacionalni center za obravnavo omrežnih incidentov je bil ustanovljen leta 1995 pri javnem zavodu Akademska in raziskovalna mreža Slovenije (v nadaljevanju: Arnes).

2. Vzpostavitev pogojev za zagotavljanje kibernetske varnosti

2.1 Strateški in pravni okvir

Odgovor na vprašanje, **ali je vlada oblikovala ustrezen strateški in pravni okvir,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je vlada:

- sprejela strategijo za področje kibernetske varnosti;
- državnemu zboru posredovala predlog zakona za prenos NIS direktive v slovenski pravni red;
- sprejela podzakonske predpise za področje kibernetske varnosti;
- sprejela akcijski načrt oziroma drug operativni dokument za izvedbo ukrepov za zagotavljanje kibernetske varnosti;
- vloge, naloge in pristojnosti na področju kibernetske varnosti jasno opredelila v zakonodaji, podzakonskih predpisih in potrebnih operativnih dokumentih, kar pomeni, da je nedvoumno določeno, katere so naloge, ki jih je treba opraviti, kdo so deležniki ter do kdaj jih je treba opraviti.

2.1.1 Strateški okvir

Vlada je februarja 2016 sprejela strategijo kibernetske varnosti, marca 2016 strategijo Digitalna Slovenija 2020, v naslednjem letu pa določila urad za varovanje tajnih podatkov kot pristojni nacionalni organ za kibernetsko varnost. Na srečanju zveze NATO v Varšavi so članice 8. 7. 2016 podpisale zavezo o kibernetski obrambi[53].

2.1.1.a Digitalna Slovenija 2020

Digitalna Slovenija 2020 je krovna strategija, ki vključuje tudi področje kibernetske varnosti in določa, da je vizija Republike Slovenije izkoristiti razvojne priložnosti informacijsko-komunikacijske tehnologije in interneta, ki jih prinaša razvoj digitalne družbe, in tako postati napredna digitalna družba ter referenčno okolje za uvajanje inovativnih pristopov pri uporabi digitalnih tehnologij. V okviru Digitalne Slovenije 2020 je ministrstvo v okviru analize nacionalnega konteksta pripravilo tudi analizo prednosti, pomanjkljivosti, priložnosti in nevarnosti (grožnje)[54] tudi za področje kibernetske varnosti, kar je prikazano v tabeli 5.

53 [URL: https://www.nato.int/cps/en/natohq/official_texts_133177.htm], 26. 2. 2021.

54 Angl.: *SWOT – Strengths, Weaknesses, Opportunities and Threats.*

Tabela 5: Analiza SWOT kibernetske varnosti v nacionalnem kontekstu

Lastnosti	Opis – ocena analize
Prednosti	• Delujoča operativna raven sistema zagotavljanja kibernetske varnosti z dobro usposobljenimi, čeprav nezadostnimi kadrovskimi viri. • Dobre izkušnje s sodelovanjem na skupnih mednarodnih vajah iz kibernetske varnosti.
Pomanjkljivosti	• Sistemska neurejenost področja zagotavljanja kibernetske varnosti na strateški ravni brez ustreznih virov (osrednja koordinacija zmogljivosti, enotna kontaktna točka za mednarodno sodelovanje).
Priložnosti	• Sistemska ureditev zagotavljanja kibernetske varnosti in zaščite kritične IT infrastrukture, dvig zaupanja v kibernetski prostor. • Varovanje človekovih pravic v digitalni družbi.
Nevarnosti (grožnje)	• Nezaupanje v kibernetski prostor, varnost in zasebnost ter s tem v uporabo e-storitev na internetu – oslabitev komercialnega potenciala digitalizacije ter nižja stopnja zaupanja državljanov v državo. • Nezadostno zavedanje o pomembnosti zagotavljanja visoke ravni kibernetske varnosti.

Vir: Digitalna Slovenija 2020.

Cilji Digitalne Slovenije 2020 za uresničitev razvojne vizije so:

- dvig splošnega zavedanja o pomenu informacijsko-komunikacijske tehnologije in interneta za razvoj družbe;
- vzdržno, sistematično in osredotočeno vlaganje v razvoj digitalne družbe;
- splošna digitalizacija po načelu privzeto digitalno (angl.: *digital by default*);
- konkurenčno digitalno podjetništvo in digitalizirana industrija za digitalno rast;
- intenzivna in inovativna uporaba informacijsko-komunikacijske tehnologije in interneta v vseh segmentih družbe;
- visokohitrostni dostop do odprtega interneta za vse;
- vključujoča digitalna družba;
- varen kibernetski prostor;
- zaupanje v kibernetski prostor in varovanje človekovih pravic;
- Slovenija – referenčno okolje za uvajanje inovativnih pristopov pri uporabi digitalnih tehnologij.

Digitalna Slovenija 2020 je za spodbujanje razvoja informacijske družbe v Republiki Sloveniji do leta 2020 predvidela ukrepe na naslednjih prednostnih področjih:

- širokopasovna in druga infrastruktura elektronskih komunikacij;
- inovativne podatkovno vodene storitve;
- digitalno podjetništvo;
- kibernetska varnost;
- vključujoča informacijska družba.

V zvezi s področjem kibernetske varnosti je Digitalna Slovenija 2020 določila strateški cilj, in sicer naj bi Slovenija do leta 2020 vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in tudi odpravljal posledice varnostnih incidentov. Z vzpostavitvijo celovitega sistema zagotavljanja kibernetske varnosti naj bi Republika Slovenija prispevala k zagotovitvi odprtega,

varnega in varovanega kibernetskega prostora, ki naj bi bil temelj za nemoteno delovanje infrastrukture, pomembne za delovanje državnih organov in gospodarstva, pa tudi za življenje vsakega posameznika. Digitalna Slovenija 2020 predvidena naslednje ukrepe na področju kibernetske varnosti:

- vzpostavitev osrednje koordinacije nacionalnega sistema zagotavljanja visokega nivoja kibernetske varnosti in zagotovitev pogojev za njeno delovanje;
- kadrovska in tehnološka okrepitev organov na operativni ravni sistema zagotavljanja kibernetske varnosti skupaj z vzpostavitvijo CSIRT organov državne uprave;
- redna udeležba na mednarodnih vajah s področja kibernetske varnosti ter izvedba nacionalnih vaj;
- postopna nadgradnja omrežja državnih organov z opremo, ki je ustrezno potrjena s strani slovenskih organov kot varna in primerna za uporabo;
- vzpostavitev kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novovzpostavljenih organov;
- redno izvajanje programov ozaveščanja na področju kibernetske varnosti;
- uvedba vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja;
- spodbujanje razvoja in vpeljave novih tehnologij na področju kibernetske varnosti;
- redno izvajanje programov ozaveščanja na področju kibernetske varnosti za gospodarske subjekte;
- redno ocenjevanje tveganj za delovanje kritične infrastrukture sektorja informacijsko-komunikacijske podpore, načrtovanje ustreznih ukrepov za zaščito ter posodabljanje ocene tveganj na tem področju;
- implementacija ustreznih kibernetskih zmogljivosti za varovanje informacijskih in komunikacijskih sistemov policije;
- redno usposabljanje s področja kibernetske varnosti za organe pregona, ki sodelujejo pri razvoju kibernetskih zmogljivosti za področje javne varnosti in pri zatiranju kibernetskega kriminala;
- redno posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij;
- razvoj ustreznih kibernetskih zmogljivosti za varovanje obrambnih komunikacijskih in informacijskih sistemov;
- zagotovitev pogojev za nemoteno delovanje ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah;
- zagotovitev pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti.

Digitalna Slovenija 2020 pomembno ugotavlja tudi, da v Sloveniji stopnja razvitosti informacijske družbe v primerjavi s tujino že desetletje in pol vztrajno pada, kar se negativno izraža tudi na drugih razvojnih področjih. Po oceni avtorjev je tako stanje posledica bistveno prenizkih vlaganj v razvoj informacijske družbe in premajhnega splošnega zavedanja o pomenu informacijsko-komunikacijske tehnologije in interneta za razvoj gospodarstva, države in celotne družbe.

2.1.1.b Strategija kibernetske varnosti

Namen strategije kibernetske varnosti je, da Republika Slovenija okrepi svoj sistem zagotavljanja kibernetske varnosti in sistemsko uredi področje. Potreba po okrepitvi celotnega sistema zagotavljanja kibernetske varnosti je nujna zaradi vedno večjega pomena, ki ga ima za nemoteno

delovanje sistemov, od katerih je odvisno delovanje celotne družbe. Cilj strategije kibernetske varnosti je, da bo Republika Slovenija do leta 2020 vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in odpravljal posledice varnostnih incidentov. Ta cilj obsega tudi naslednje podcilje:

- okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti;
- varnost državljanov v kibernetskem prostoru;
- kibernetska varnost v gospodarstvu;
- zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore;
- zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala;
- razvoj obrambnih kibernetskih zmogljivosti;
- zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah;
- krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem.

2.1.2 Prenos NIS direktive v slovenski pravni red

Evropska unija je 6. 7. 2016 sprejela NIS direktivo, s katero določa ukrepe za doseganje visoke skupne ravni varnosti omrežij in informacijskih sistemov v Evropski uniji, z namenom izboljšanja delovanja notranjega trga. V skladu z NIS direktivo mora vsaka država članica sprejeti nacionalno strategijo za varnost omrežij in informacijskih sistemov, v kateri določi strateške cilje ter ustrezne ukrepe politike in regulativne ukrepe. V skladu z NIS direktivo so morale države članice določiti tudi enega ali več pristojnih nacionalnih organov za varnost omrežij in informacijskih sistemov, ki med drugim spremljajo tudi uporabo NIS direktive na nacionalni ravni. Države članice so morale določiti enotno kontaktno točko za komunikacijo in sodelovanje z relevantnimi organi v drugih državah članicah ter enega ali več nacionalnih odzivnih centrov CSIRT. Prav tako so morale države članice določiti tudi izvajalce bistvenih storitev, ki so ključnega pomena za vzdrževanje in nemoteno delovanje gospodarskih in družbenih dejavnosti. Osnovno merilo za določitev izvajalca bistvenih storitev je bilo, da je nemoteno delovanje storitev izvajalca odvisno od delovanja omrežja in informacijskih sistemov ter da bi varnostni incident prekinil ali resno okrnil delovanje storitev, ki jih izvajalec zagotavlja. Stopnja resnosti incidenta naj bi upoštevala število prizadetih uporabnikov, trajanje incidenta in geografsko razširjenost oziroma doseg incidenta.

Republika Slovenija je NIS direktivo v slovenski pravni red prenesla z uveljavitvijo 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. ZInfV določa tudi minimalne varnostne zahteve in zahteve za priglasitev incidentov za izvajalce bistvenih storitev, ponudnike digitalnih storitev[55] in organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo

55 Vsaka fizična ali pravna oseba, ki zagotavlja digitalno storitev.

informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti. Prav tako ureja tudi pristojnosti, naloge, organizacijo in delovanje pristojnega nacionalnega organa za informacijsko varnost, enotne kontaktne točke za informacijsko varnost, nacionalnega CSIRT ter CSIRT organov državne uprave. ZInfV je določil prehodno obdobje, da:

- vlada določi posamezne izvajalce bistvenih storitev v 6 mesecih od uveljavitve uredbe, ki določa seznam bistvenih storitev, in uredbe, ki določa metodologijo za določitev izvajalcev bistvenih storitev; glede na to, da navedeni uredbi nista bili sprejeti v roku 6 mesecev od uveljavitve ZInfV (to je do 11. 11. 2018), je 6-mesečni rok za določitev posameznih izvajalcev začel teči kasneje, in sicer 22. 6. 2019, ko je vlada sprejela Uredbo o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev[56] (v nadaljevanju: uredba o določitvi bistvenih storitev); NIS direktiva je sicer določila, da naj bi se izvajalci bistvenih storitev v posamezni državi članici Evropske unije določili že do 9. 11. 2018;
- morajo ponudniki digitalnih storitev v 9 mesecih od uveljavitve ZInfV (to je do 11. 2. 2019) izpolniti varnostne zahteve in zahteve za priglasitev incidentov, ki ogrožajo varnost njihovih omrežij in informacijskih sistemov, na ponujane storitve, ki jih zagotavljajo v Evropski uniji, da bi zagotovili neprekinjeno izvajanje teh storitev;
- vlada v 9 mesecih od uveljavitve ZInfV (to je do 11. 2. 2019) določi organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti; CSIRT organov državne uprave se ne določi, če imajo organi državne uprave v svoji notranji organizacijski strukturi zagotovljene lastne zmogljivosti vsaj na ravni varnostno-operativnega centra;
- morajo organi državne uprave izvesti aktivnosti, vezane na varnostne zahteve, varnostno dokumentacijo in varnostne ukrepe ter priglasitev incidentov, v 12 mesecih od njihove določitve.

ZInfV je v prehodnih določbah določil tudi naslednje:

- uprava kot pristojni nacionalni organ začne z delovanjem najkasneje do 1. 1. 2020;
- do pričetka delovanja uprave opravlja naloge urad za varovanje tajnih podatkov, razen nalog upravnega odločanja in nadzora, ki jih opravlja ministrstvo, pristojno za informacijsko družbo;
- uprava z dnem začetka delovanja od urada za varovanje tajnih podatkov prevzame naloge, arhive in dokumentacijo, ki se nanašajo na informacijsko varnost, ter javne uslužbence, pravice proračunske porabe, opremo in druge zbirke podatkov oziroma evidence s prevzetega delovnega področja;
- vlada uskladi sklep o uradu za varovanje tajnih podatkov 2017 z ZInfV v 3 mesecih od njegove uveljavitve (to je do 11. 8. 2018);
- nacionalni CSIRT začne z delovanjem po ZInfV 1. 1. 2019;
- CSIRT organov državne uprave se vzpostavi na ministrstvu, pristojnem za upravljanje informacijsko-komunikacijskih sistemov državne uprave, 1. 1. 2019;
- do vzpostavitve CSIRT organov državne uprave njegove naloge glede obravnave incidentov izvaja nacionalni CSIRT;

56 Uradni list RS, št. 39/19.

- vlada sprejme strategijo informacijske varnosti iz 26. člena ZInfV v letu dni od uveljavitve tega zakona (to je do 11. 5. 2019).

2.1.3 Podzakonski predpisi

Vlada je 19. 4. 2018 sprejela uredbo o IVvDU, ki med drugim določa minimalne skupne zahteve glede informacijske varnosti, ki jih sestavljajo enotni okviri upravljanja informacijske varnosti in temeljna nadzorstva za zagotavljanje informacijske varnosti v državni upravi. Uredba o IVvDU določa, da ministrstvo v 6 mesecih po njeni uveljavitvi (to je do 11. 11. 2018) na svoji spletni strani objavi enotno metodologijo upravljanja tveganj informacijske varnosti in enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi.

Vlada je v uredbi o določitvi bistvenih storitev, ki jo je sprejela junija 2019, določila 9 področij[57], na katerih se izvajajo bistvene storitve, ter 3 podpodročja[58] na področju energije ter 4 podpodročja[59] na področju prometa.

2.1.4 Operativni dokumenti za izvajanje aktivnosti

Vlada do konca obdobja, na katero se nanaša revizija, ni sprejela akcijskega načrta oziroma drugega operativnega dokumenta za izvedbo ukrepov za zagotavljanje kibernetske varnosti.

MIZŠ, ki je bilo v času priprave strategije kibernetske varnosti v prvi polovici leta 2016 pristojno za informacijsko družbo, je 12. 5. 2016 predlog akcijskega načrta za uresničevanje strategije kibernetske varnosti (v nadaljevanju: akcijski načrt) skupaj z oceno potrebnih virov (23 novozaposlenih in 16 prerazporeditev) za obdobje 2016–2018 posredovalo Strateškemu svetu Sveta za razvoj informatike (v nadaljevanju: strateški svet), ki je deloval v okviru MIZŠ in je bil pristojen za njegovo potrditev. V predlogu je MIZŠ poleg predloga akcijskega načrta in ocene potrebnih virov predlagalo tudi, da koordinacijo področja kibernetske varnosti na nacionalni ravni prevzame urad za varovanje tajnih podatkov, kar je bilo kasneje tudi določeno v ZInfV in sklepih vlade. Po pojasnilih MIZŠ je bil predlog kasneje v maju 2016 tudi predstavljen članom strateškega sveta. Na predstavitvi so pojasnili cilje, potrebne ukrepe za njihovo izpolnitev in oceno potrebnih virov. Predlagani akcijski načrt ni bil potrjen.

Pojasnilo vlade

Vlada se zaveda, da akcijski načrt v preteklosti ni bil sprejet, vendar poudarja, da se vse predvidene aktivnosti izvajajo tudi brez akcijskega načrta. Vendar pa to ne pomeni, da vlada ne ve, katere aktivnosti potekajo oziroma kaj je treba v naslednjem obdobju izvesti. Vlada ima na tem področju zelo jasno vizijo.

[57] Energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura finančnega trga, preskrba s hrano in varstvo okolja.

[58] Elektrika, nafta in plin.

[59] Zračni, železniški, vodni in cestni promet.

2.1.5 Opredelitev vlog, nalog in pristojnosti

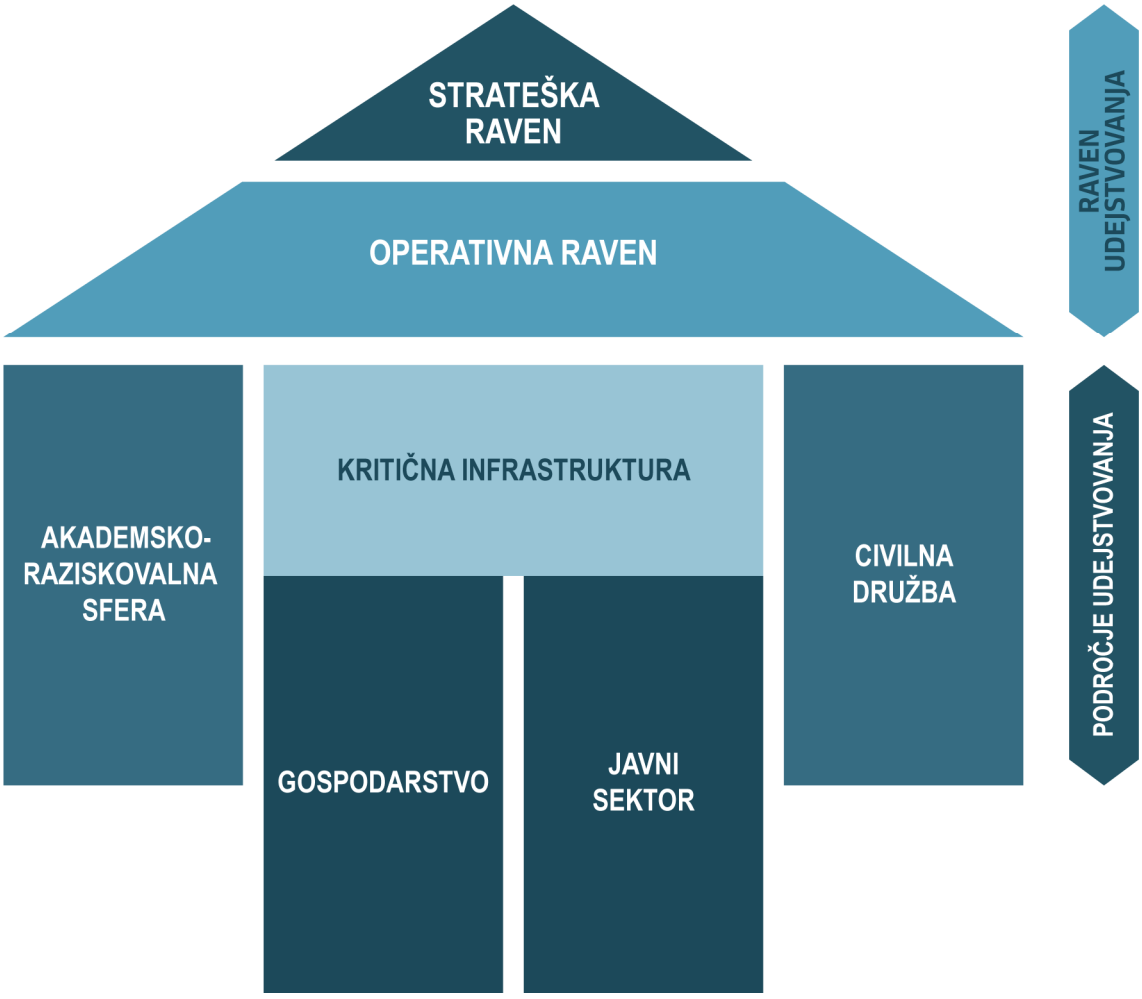
Vloge, naloge in pristojnosti na področju kibernetske varnosti je vlada opredelila v zakonodaji in operativnih dokumentih. V času priprave in sprejema strategije kibernetske varnosti ni bilo koordinacijskega telesa, ki bi deležnike povezovalo na strateški ravni, operativne zmogljivosti pa so bile v letu 2016 porazdeljene med različne deležnike, in sicer:

- SI-CERT;
- sektor za informacijsko varnost v okviru Direktorata za informatiko na ministrstvu;
- Ministrstvo za obrambo za sisteme na področju obrambe in varstva pred naravnimi in drugimi nesrečami;
- SOVA za področje protiobveščevalnega delovanja ter
- Policija, Urad za informatiko in telekomunikacije in Uprava kriminalistične policije, predvsem v Centru za računalniško preiskovanje z zmogljivostmi za zatiranje kibernetskega kriminala.

Vlada je navedene deležnike opredelila tudi v strategiji kibernetske varnosti (slika 1) ter poudarila, da v sistemu zagotavljanja kibernetske varnosti sodelujejo organizacije javnega in zasebnega sektorja. Strategija kibernetske varnosti določa, da bodo imeli, poleg predvidene osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti ter odzivnih centrov za zagotavljanje kibernetske varnosti, pomembno vlogo tudi AKOS, telekomunikacijski operaterji in upravljavci telekomunikacijske infrastrukture, ponudniki storitev informacijske družbe, akademsko-raziskovalna sfera ter stanovska in strokovna združenja. Prav tako naj bi imeli pomembno vlogo tudi proizvajalci programske opreme, ki nudijo podporo državnim organom.

Strategija kibernetske varnosti med deležnike šteje tudi organizacije v tujini, predvsem partnerje v okviru Evropske unije in zveze NATO, še posebej v primerih, kadar se skupaj s slovenskimi deležniki odzivajo na varnostne incidente.

Slika 1: Shematski prikaz sistema zagotavljanja kibernetske varnosti



Vir: strategija kibernetske varnosti.

Po sprejemu ZInfV je vlada s Sklepom o dopolnitvi Sklepa o ustanovitvi, nalogah in organizaciji Urada Vlade Republike Slovenije za varovanje tajnih podatkov[60] (v nadaljevanju: sklep o uradu za varovanje tajnih podatkov 2018) določila, da bo urad za varovanje tajnih podatkov naloge s področja informacijske in kibernetske varnosti opravljal vse do pričetka delovanja pristojnega nacionalnega organa za informacijsko varnost v skladu z ZInfV.

ZInfV določa zavezance, ki se delijo na:

- izvajalce bistvenih storitev;
- ponudnike digitalnih storitev;

60 Uradni list RS, št. 52/18.

- organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

ZInfV je predvidel vzpostavitev naslednjih organov:

- pristojni nacionalni organ;
- enotna kontaktna točka za informacijsko varnost;
- nacionalni CSIRT in
- CSIRT organov državne uprave.

ZInfV določa tudi, da vlada za namen določitve izvajalcev bistvenih storitev določi seznam bistvenih storitev. Vlada je seznam bistvenih storitev določila z uredbo o določitvi bistvenih storitev, medtem ko izvajalcev bistvenih storitev do konca obdobja, na katero se nanaša revizija, ni določila.

Ukrep vlade

Vlada je:

- 17. 10. 2019 določila 12 izvajalcev bistvenih storitev,
- 7. 11. 2019 določila 6 izvajalcev bistvenih storitev,
- 28. 11. 2019 določila 3 izvajalce bistvenih storitev,
- 5. 3. 2020 določila 1 izvajalca bistvenih storitev in
- 12. 3. 2020 določila 5 izvajalcev bistvenih storitev.

Pri pripravi metodologije in pragov v sklopu uredbe o določitvi bistvenih storitev ter določitvi seznama storitev Republika Slovenija ni sodelovala s sosednjimi državami pri čezmejnem usklajevanju niti ni bila povabljena k sodelovanju s strani sosednjih držav. NIS direktiva sicer spodbuja države članice k sodelovanju na tem področju, med drugim določa, da skupina za sodelovanje v skladu s svojimi nalogami, med katere spadata tudi izmenjevanje informacij in najboljših praks o ozaveščanju in usposabljanju ter izmenjevanje informacij in najboljših praks o raziskavah in razvoju v zvezi z varnostjo omrežij in informacijskih sistemov, podpira države članice, da pri določanju izvajalcev bistvenih storitev uporabijo usklajen pristop.

Evropska komisija je 28. 10. 2019 izdala poročilo Evropskemu parlamentu in Svetu o oceni skladnosti pristopov držav članic za določitev izvajalcev bistvenih storitev v skladu z NIS direktivo[61] (v nadaljevanju: poročilo o določitvi IBS). Vlada izvajalcev bistvenih storitev ni določila v roku, ki ga je predvidela NIS direktiva. Evropska komisija v poročilu med drugim navaja, da je 6 državam 25. 7. 2019 poslala opomin, med njimi tudi Republiki Sloveniji. Iz opomina izhaja, da je 24. 5. 2019 Evropska komisija Republiko Slovenijo opozorila, naj predloži vse potrebne informacije, zato ji je ministrstvo 21. 6. 2019 odgovorilo z dodatnimi informacijami, vendar hkrati ni posredovalo seznama izvajalcev bistvenih storitev. Evropska komisija je z opominom pozvala vlado, naj ji v 2 mesecih od

61 Poročilo Komisije Evropskemu parlamentu in Svetu o oceni skladnosti pristopov držav članic za določitev izvajalcev bistvenih storitev v skladu s členom 23(1) Direktive 2016/1148/EU o varnosti omrežij in informacijskih sistemov, oznaka: COM(2019) 546 final, z dne 28. 10. 2019.

prejema opomina predloži pripombe. Ministrstvo je Evropski komisiji 1. 8. 2019 posredovalo prošnjo za 2-mesečno podaljšanje roka za odgovor na uradni opomin oziroma do 26. 11. 2019, kar je Evropska komisija odobrila.

Ukrep ministrstva

Ministrstvo je obveščalo Evropsko komisijo o procesu določevanja izvajalcev bistvenih storitev. Evropska komisija je na podlagi predloženega seznama izvajalcev bistvenih storitev julija 2020 sprejela odločitev, da zaključi postopek ugotavljanja kršitve prava Evropske unije.

Poročilo o določitvi IBS navaja, da je NIS direktiva prvi instrument notranjega trga, namenjen izboljšanju odpornosti Evropske unije proti tveganjem kibernetske varnosti. V poročilu so navedene tudi posamezne storitve, ki so jih države članice določile v podsektorju elektrike ter v podsektorju železniškega prometa.

Republika Slovenija ima ločeno urejeno področje kibernetske varnosti v ZInfV in področje kritične infrastrukture, ki 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 in gospodarstvo, ter druge ključne družbene funkcije ter zdravje, varnost, zaščito in blaginjo ljudi v Zakonu o kritični infrastrukturi[62] (v nadaljevanju: ZKI). To pomeni, da je treba kritično infrastrukturo in njene upravljavce ter izvajalce bistvenih storitev določiti ločeno v posebnih postopkih, saj jo oziroma jih vladi v določitev predlagata različni ministrstvi. Vlada je v juliju 2018 najprej določila nosilce sektorjev kritične infrastrukture in z njimi sodelujoče državne organe, v februarju 2019 pa je določila še upravljavce kritične infrastrukture.

Republika Slovenija je s sprejemom strategije kibernetske varnosti februarja 2016 v svojih dokumentih prvič uvedla pojem kibernetska varnost. Ko je to področje 2 leti kasneje uredila v ZInfV, pa je uvedla pojem informacijska varnost in ga uporabila tudi v uredbi o IVvDU. Republika Slovenija je z ZInfV v slovenski pravni red prenesla NIS direktivo, ki pa pojmov kibernetska in informacijska varnost ne ureja, ampak določa le ukrepe za doseganje visoke skupne ravni varnosti omrežij in informacijskih sistemov v Evropski uniji. Revidiranci so v obdobju, na katero se nanaša revizija, v različnih sprejetih dokumentih, delovnih dokumentih in poročilih nedosledno uporabljali oba pojma. Evropska unija je v letu 2019 začela dosledno uporabljati pojem kibernetska varnost, med drugim v poročilu o določitvi IBS in aktu o kibernetski varnosti. Premik od pojma informacijska varnost k uporabi pojma kibernetska varnost pa je razviden tudi pri nacionalnem CSIRT, ki je v letu 2019 izdal Poročilo o kibernetski varnosti za leto 2018, pred tem pa so imela njegova poročila naslov Poročilo o omrežni varnosti. Pojem kibernetska varnost uporablja, vendar ga posebej ne opredeljuje, tudi ReSNV-2, ki med drugim določa, da bo vzpostavljen nacionalni organ za kibernetsko področje za podporo strateškemu odločanju na podlagi podatkov vseh subjektov nacionalnovarnostnega sistema pripravljal analize in ocene o grožnjah in stanju na področju kibernetske varnosti. Prav tako ReSNV-2 določa, da bo Republika Slovenija zagotovila učinkovit sistem zagotavljanja kibernetske varnosti s povezanimi ukrepi na področju preprečevanja in odzivanja ter ozaveščanja vseh delov družbe. Enotna in jasna terminologija omogoča lažjo izmenjavo

62 Uradni list RS, št. 75/17.

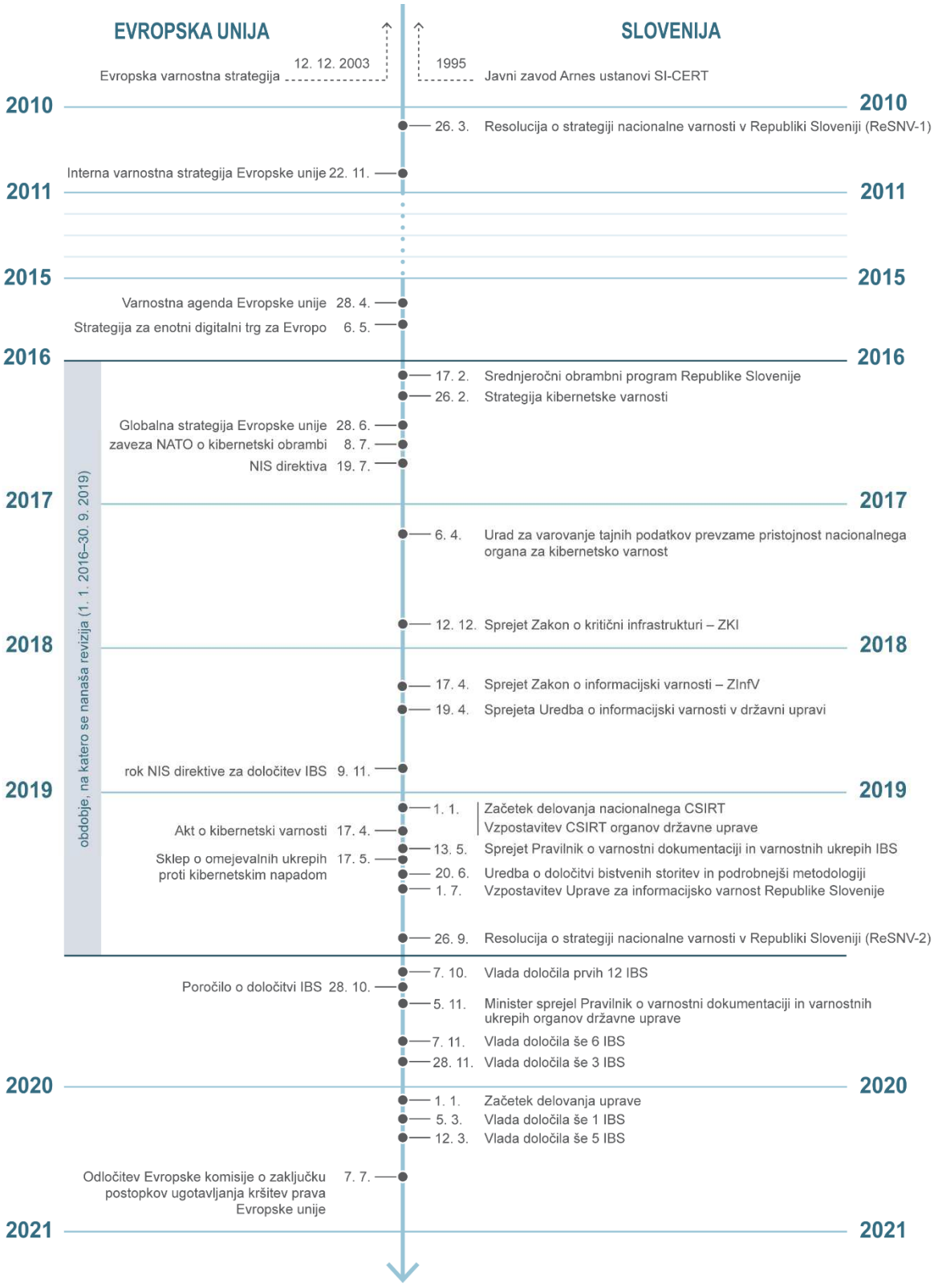
podatkov in poročanje med deležniki na področju kibernetske varnosti v Republiki Sloveniji in na mednarodni ravni.

Priporočilo

Vladi priporočamo, naj v pravnih in strokovnih dokumentih jasno definira, poenoti in dosledno uporablja ustrezno terminologijo in pri tem sledi trendom na ravni Evropske unije.

Slika 2 prikazuje dogodke na področju kibernetske varnosti v Evropski uniji in v Sloveniji med letoma 2010 in 2020.

Slika 2: Pregled dogajanj na področju kibernetske varnosti med letoma 2010 in 2020 v Evropski uniji in Sloveniji



Opomba: IBS – izvajalci bistvenih storitev.

Ocenjujemo, da je vlada v pretežni meri oblikovala ustrezen strateški in pravni okvir. Vlada je leta 2016 sprejela strategijo kibernetske varnosti in z njo zastavila strateške usmeritve na tem področju, vendar pa strategije kasneje ni prenovila oziroma sprejela nove, kot je to določal ZInfV. Vlada bi morala že v maju 2019 sprejeti novo strategijo na tem področju, kar pa se do konca obdobja, na katero se nanaša revizija, ni zgodilo. Republika Slovenija je NIS direktivo v slovenski pravni red prenesla z uveljavitvijo ZInfV. Vlada je sicer sprejela uredbo o določitvi bistvenih storitev, vendar je pri tem zamujala. Glede na oceno iz strategije kibernetske varnosti, da je okrepitev celotnega sistema nujna zaradi vedno večjega pomena kibernetske varnosti za nemoteno delovanje sistemov, od katerih je odvisno delovanje celotne družbe, je po naši oceni tako ravnanje zaskrbljujoče, saj se s tem roki za implementacijo in izvajanje aktivnosti le še podaljšujejo. Vlada je zamujala tudi z določitvijo izvajalcev bistvenih storitev, za kar je prejela opomin Evropske komisije. Vlada je prvi seznam izvajalcev bistvenih storitev določila v oktobru 2019. Pravočasen sprejem podzakonskih predpisov in drugih aktov je pomemben za celovito izvajanje določb ZInfV in učinkovito zagotavljanje kibernetske varnosti v Republiki Sloveniji. Vlada ni sprejela akcijskega načrta oziroma drugega operativnega dokumenta na področju kibernetske varnosti, pristojna resorna ministrstva so sicer pripravila določene osnutke, ki pa na vladi nikoli niso bili potrjeni.

2.2 Organizacijska struktura za zagotavljanje kibernetske varnosti

Odgovor na vprašanje, **ali je vlada vzpostavila ustrezno organizacijsko strukturo za zagotavljanje kibernetske varnosti,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je vlada:

- zagotovila ustanovitev v ZInfV predvidenih organov za posamezna področja zagotavljanja kibernetske varnosti;
- opravila analizo, v kateri je natančno ugotovila obseg potreb po kadrovski in tehnološki okrepitvi;
- v skladu s predhodno analizo zagotovila sredstva za kadrovsko in tehnološko okrepitev organov na operativni ravni sistema zagotavljanja kibernetske varnosti;
- vzpostavila kompetentno preverjanje varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novovzpostavljenih organov.

2.2.1 Ustanovitev organov

Vlada je zagotovila, da so bili v zakonskih rokih ustanovljeni pristojni nacionalni organ, ki je hkrati tudi enotna kontaktna točka, nacionalni CSIRT in CSIRT organov državne uprave.

2.2.1.a Pristojni nacionalni organ in enotna kontaktna točka

Vlada je po sprejemu ZInfV v letu 2018 s sklepom o uradu za varovanje tajnih podatkov 2018 naloge urada za varovanje tajnih podatkov uskladila z ZInfV in določila, da urad za varovanje tajnih podatkov do začetka delovanja pristojnega nacionalnega organa v skladu z ZInfV opravlja tudi naslednje naloge:

- ministrstvu, pristojnemu za informacijsko družbo, predlaga sprejetje ukrepov v primeru težjega ali kritičnega incidenta ali v primeru kibernetskega napada ter v primeru stanja povečane ogroženosti na podlagi zakona, ki ureja informacijsko varnost;

- vodi seznam kontaktnih podatkov zavezancev ter skupni seznam incidentov in kibernetskih napadov;
- obvešča javnosti o incidentih in ukrepih, sprejetih v zvezi z njimi;
- izpolnjuje mednarodne obveznosti in opravlja naloge mednarodne izmenjave podatkov, vključno z izvajanjem nalog enotne kontaktne točke in sodelovanja s pristojnimi organi s področja informacijske varnosti v Evropski uniji, določene z zakonom, ki ureja informacijsko varnost;
- opravlja koordinacijske, strokovno-tehnične, organizacijske in razvojne naloge na področju informacijske varnosti in kibernetske obrambe, določene z zakonom, ki ureja informacijsko varnost, in predpisi, izdanimi na njegovi podlagi.

Vlada je 26. 7. 2018 izdala Uredbo o spremembah in dopolnitvah Uredbe o organih v sestavi ministrstev, s katero je določila pristojnosti urada za varovanje tajnih podatkov tudi na področju kibernetske varnosti. Urad za varovanje tajnih podatkov je s sklepoma vlade postal pristojni nacionalni organ, vendar pa vlada uradu za varovanje tajnih podatkov do leta 2019 ni zagotovila dodatnih sredstev za opravljanje nalog s področja kibernetske varnosti. Da bi pridobil sredstva za opravljanje novododeljenih nalog, se je urad za varovanje tajnih podatkov med drugim prijavil tudi na razpis Evropske komisije – razpis CEF[63].

Minister je 15. 4. 2019 imenoval delovno skupino za zagotovitev začetka delovanja uprave za informacijsko varnost in pri tem določil njene naloge, in sicer da delovna skupina:

- zazna in določi znanja in kompetence javnih uslužbencev, zaposlenih na upravi za informacijsko varnost;
- zazna in določi potrebno število javnih uslužbencev za opravljanje nalog uprave za informacijsko varnost;
- pripravi naloge in predlog organizacije za akt o notranji organizaciji in sistemizaciji delovnih mest v upravi za informacijsko varnost (besedilni del s predlogom posameznih delovnih mest);
- določi dinamiko zaposlovanja javnih uslužbencev;
- zazna in določi prostorske potrebe uprave za informacijsko varnost ter druga materialna sredstva, potrebna za delovanje uprave za informacijsko varnost, kot sta pisarniška in programska oprema in podobno;
- oceni finančne potrebe uprave in pripravi osnutek proračuna oziroma izhodišča za pripravo proračuna uprave za informacijsko varnost;
- pripravi druge predloge in ukrepe, potrebne za začetek delovanja uprave za informacijsko varnost.

Do vzpostavitve delovanja pristojnega nacionalnega organa je njegove naloge opravljal urad za varovanje tajnih podatkov, razen nalog upravnega odločanja in nadzora, ki jih je opravljalo ministrstvo.

Ministrstvo v obdobju, na katero se nanaša revizija, ni izvajalo nadzora, saj zato ni bilo pogojev, ker vlada še ni določila izvajalcev bistvenih storitev, prav tako pa tudi ni določila organov državne

63 European Commission, Connecting Europe Facility 2014-2020, Telecom calls for proposal 2018, [URL: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/], 26. 2. 2021.

uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

S 1. 7. 2019 je bila v okviru ministrstva vzpostavljena uprava za informacijsko varnost kot pristojni nacionalni organ, ki naj bi v nadaljevanju postopoma prevzel naloge od urada za varovanje tajnih podatkov kot začasnega pristojnega nacionalnega organa.

Ukrep vlade

Vlada je 25. 10. 2019 objavila Odlok o Svetu za nacionalno varnost[64], v katerem je določila tudi članstvo direktorja uprave za informacijsko varnost v sekretariatu Sveta za nacionalno varnost (v nadaljevanju: SSNAV) ter določila članstvo predstavnika uprave za informacijsko varnost v Operativni skupini sekretariata Sveta za nacionalno varnost (v nadaljevanju: OS SSNAV).

Vlada je 16. 3. 2020 objavila nov Odlok o Svetu za nacionalno varnost[65], iz katerega izhaja, da direktor uprave za informacijsko varnost ni več član SSNAV.

2.2.1.b Nacionalni CSIRT

Nacionalni CSIRT je odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. SI-CERT je bil 1. 1. 2019 imenovan za nacionalni CSIRT. Na podlagi ZInfV med drugim izvaja naslednje naloge:

- zavezancem, za katere je pristojen, nudi metodološko podporo, pomoč in sodelovanje ob pojavitvi incidenta;
- sprejema podatke o tveganjih in ranljivostih na področju informacijske varnosti, jih posreduje skrbnikom prizadetih sistemov in objavlja opozorila;
- sodeluje v mreži skupin CSIRT, lahko pa tudi v drugih mednarodnih mrežah za sodelovanje;
- sodeluje s skupinami CSIRT in varnostno-operativnimi centri v Republiki Sloveniji ter skupinami CSIRT v drugih državah članicah Evropske unije;
- izvaja ozaveščanje uporabnikov na področju informacijske varnosti;
- objavlja opozorila o tveganjih in ranljivostih na področju informacijske varnosti;
- sodeluje s pristojnim nacionalnim organom in mu na poziv nudi informacije o izvajanju svojih pristojnosti na podlagi ZInfV.

2.2.1.c CSIRT organov državne uprave

Na podlagi ZInfV naloge CSIRT organov državne uprave izvaja ministrstvo, pristojno za upravljanje informacijsko-komunikacijskih sistemov državne uprave. Med drugim izvaja naslednje naloge:

- sprejema, obravnava in ocenjuje priglasitve incidentov, prejete od organov državne uprave, za katere je pristojen, ter te podatke evidentira, hrani in varuje;

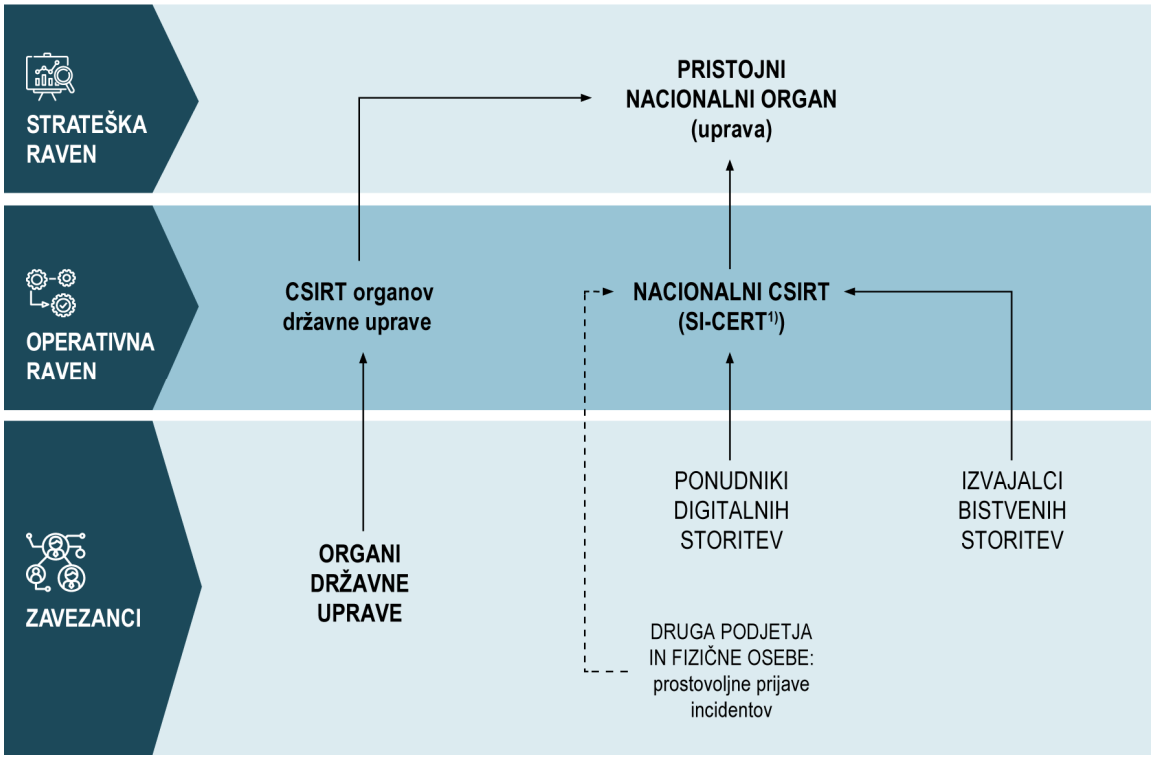
64 Uradni list RS, št. 64/19.

65 Uradni list RS, št. 26/20.

- organom državne uprave nudi metodološko podporo, pomoč in sodelovanje ob pojavu incidenta;
- sodeluje z nacionalnim CSIRT in s pristojnim nacionalnim organom ter jima na poziv na varen način nudi informacije o izvajanju svojih pristojnosti na podlagi tega zakona;
- objavlja opozorila o tveganjih in ranljivostih na področju informacijske varnosti organov državne uprave.

Ministrstvo je s 1. 1. 2019 na ministrstvu v sklopu Direktorata za informatiko vzpostavilo CSIRT organov državne uprave, ki deluje v okviru sektorja za informacijsko varnost. CSIRT organov državne uprave je izvajal aktivnosti, ki so bile navedene v nalogah operativnega centra informacijske varnosti, med njimi je tudi sprejemal, obravnaval in analiziral varnostne incidente ter svetoval prijaviteljem. Slika 3 prikazuje povezanost navedenih organov pri poročanju o kibernetskih incidentih.

Slika 3: Shema poročanj o incidentih po ZInfV



Opomba: [1] SI-CERT je bil ustanovljen v letu 1995, s 1. 1. 2019 pa je postal nacionalni CSIRT.
Vir: Poročilo o kibernetski varnosti za leto 2018.

2.2.2 Analiza potreb in zagotavljanje kadrovske in tehnološke okrepitve

Vlada je že v predlogu Zakona o informacijski varnosti[66] (v nadaljevanju: predlog ZIV) ugotovila, da so organi na obeh ravneh sistema, tako strateški kot operativni, podhranjeni na kadrovskem, materialno-tehničnem in organizacijskem področju. V predlogu ZIV je vlada med drugim navedla tudi oceno finančnih posledic predloga tega zakona za državni proračun in druga javna finančna sredstva. Tabela 6 prikazuje skupne ocenjene stroške vzpostavitve in delovanja pristojnih organov, ki so v predlogu ZIV v obdobju od leta 2018 do leta 2021 znašali 4.318.400 EUR.

Tabela 6: Skupni ocenjeni stroški vzpostavitve in delovanja pristojnih organov ter pogojev za delovanje CSIRT organov državne uprave in SI-CERT oziroma nacionalnega CSIRT

v EUR

	Kategorija/leto	2018	2019	2020	2021
1.	Število zaposlitev kumulativno	8	14	24	24
2.	Stroški vzpostavitve/delovanja delovnih mest	40.000	46.000	78.000	48.000
3.	Stroški plač in nadomestil (bruto 2)	120.000	420.000	720.000	720.000
4.	Službene poti in izobraževanja	6.000	16.800	28.800	28.800
5.	Investicije v strojno in programsko opremo	300.000	300.000	300.000	300.000
6.	Nakup/pridobitev prostorov	/	/	/	/
7.	Stroški SI-CERT (v letu 2018) oziroma nacionalnega CSIRT (od leta 2019 naprej)	64.000	238.000	272.000	272.000
	Skupaj	**530.000**	**1.020.800**	**1.398.800**	**1.368.800**

Vir: predlog ZIV.

Ministrstvo ni vodilo oziroma posebej beležilo stroškov za kibernetsko varnost, prav tako tudi ne za informacijsko varnost, zato nima točnih podatkov o tem, koliko sredstev je za to porabilo. Ministrstvo je za namene revizije pripravilo podatke o realizaciji med 1. 1. 2016 in 31. 12. 2018, 1. 1. 2019 in 30. 9. 2019 ter o finančnih elementih predobremenitev za leto 2019, ki so prikazani v tabeli 7.

66 Zakon o informacijski varnosti, predlog, EVA: 2017-3130-0029, prva obravnava.

Tabela 7: Ocena realizacije proračuna za namen kibernetske varnosti med 1. 1. 2016 in 30. 9. 2019

v EUR

Proračunska postavka		2016	2017	2018	Finančni elementi predobremenitev 2019	Realizacija 30. 9. 2019
153377	Investicije, podpora in vzdrževanje strojne, komunikacijske in licenčne programske opreme, lokalnih računalniških omrežij upravnih enot in državnih organov	98.960	98.960	98.960	49.480	49.480
153380	Razvoj ter vzdrževanje in upravljanje skupne informacijske infrastrukture (strežniške in licenčne)	23.180	65.051	65.051	1.848.417	66.490
153381	Razvoj ter vzdrževanje in upravljanje skupne komunikacijske infrastrukture (strežniške in licenčne)	89.086	15.131	87.222	232.568	63.434
170089	Razvoj, vzdrževanje in upravljanje informacijske varnosti	0	888.010	570.006	848.426	592.432
170090	Vzpostavitev in vzdrževanje sistema upravljanja s podatki	0	2.873	28.774	43.732	3.599
170093 170095	Informacijska varnost Razvoj in podpora delovanja interneta		384.153	384.000	448.000	163.154
SKUPAJ		**211.226**	**1.454.178**	**1.234.013**	**3.470.623**	**938.589**

Vir: podatki ministrstva.

Pojasnilo ministrstva

Tabela 7 ne vključuje celotne vrednosti posameznih proračunskih postavk, temveč so vključeni le zneski, ki se po oceni ministrstva nanašajo na področje kibernetske varnosti. Za področje kibernetske varnosti ne obstaja ločena proračunska postavka, lahko pa kibernetska varnost predstavlja del drugih proračunskih postavk, kot na primer postavke za razvoj, vzdrževanje in upravljanje informacijske varnosti, postavk s področja informacijsko-komunikacijske infrastrukture, strojne in programske opreme in podobno.

Vlada je v letu 2016 sicer pripravila podrobno oceno kadrovskih potreb pri pripravi osnutka akcijskega načrta za uresničevanje strategije kibernetske varnosti, ki pa ni bil nikoli sprejet. Kasneje ni izvedla analize potreb za vse deležnike na področju kibernetske varnosti, s katero bi ocenila kadrovske in tehnološke potrebe. Ministrstvo in urad za varovanje tajnih podatkov sta sicer opravila posamezne analize potreb, a s strani vlade niso bile potrjene. Vlada tudi ni zagotovila sredstev v skladu s predhodnimi analizami, ki so bile opravljene za potrebe postopka sprejema ZInfV in proračunskega načrtovanja. Vlada je v predlogu sklepa o uradu za varovanje tajnih podatkov 2018 predvidela, da bo imel pristojni nacionalni organ v letu 2018 5 zaposlenih, za kar naj bi potreboval 103.750 EUR, v letu 2019 pa 9 zaposlenih, za kar naj bi potreboval 410.800 EUR. Vlada uradu za varovanje tajnih podatkov, ki je v letu 2018 in prvi polovici leta 2019 opravljal naloge pristojnega nacionalnega organa, teh finančnih sredstev ni zagotovila, prav tako tudi ni odobrila povečanja predvidenega števila zaposlenih. Urad za varovanje tajnih podatkov je tako šele s 1. 6. 2019 zaposlil 1 javnega uslužbenca izključno za področje kibernetske varnosti.

Ukrep ministrstva

Omenjeni zaposleni na uradu za varovanje tajnih podatkov je bil novembra 2019 premeščen na upravo za informacijsko varnost.

Delovna skupina ministrstva (več v točki 2.2.1.a tega poročila) je pripravila oceno potrebnih virov na področju kibernetske varnosti za delovanje uprave za informacijsko varnost v predlogu Akta o notranji organizaciji in sistemizaciji delovnih mest v Ministrstvu za javno upravo, Upravi Republike Slovenije za informacijsko varnost (v nadaljevanju: akt o notranji organizaciji), h kateremu je vlada julija 2019 dala soglasje. Vlada je junija 2019 potrdila spremembe Skupnega kadrovskega načrta organov državne uprave za leti 2018 in 2019 in s tem ministrstvu za potrebe uprave za informacijsko varnost odobrila povečanje števila zaposlenih javnih uslužbencev za 3 zaposlene. Akt o notranji organizaciji je predvideval, da bo uprava za informacijsko varnost konec leta 2021 imela 27 zaposlenih, potrebna finančna sredstva pa so bila predvidena v proračunih za leti 2020 in 2021. Ob koncu obdobja, na katero se nanaša revizija, je uprava za informacijsko varnost imela 6 zaposlenih.

Ukrep ministrstva

Od začetka septembra 2020 je uprava za informacijsko varnost imela 9 zaposlenih.

Vlada je 16. 7. 2019 dala soglasje k aktu o notranji organizaciji. Ocenjeno je bilo, da naj bi stroški dela uprave za informacijsko varnost za leto 2019 znašali 84.164 EUR.

ReSNV-2 predvideva tudi novost glede vlaganj v kibernetsko varnost, saj navaja, da si bo Republika Slovenija prizadevala doseči raven obrambnih izdatkov skladno s prevzetimi mednarodnimi zavezami, s čimer bo zagotavljala celovit razvoj obrambnih zmogljivosti države, vključno z zmogljivostmi za soočanje z vojaškimi, informacijsko-kibernetskimi in hibridnimi grožnjami.

Glede na izkušnje, ki jih je imel urad za varovanje tajnih podatkov z dolgotrajnim postopkom zaposlitve novega sodelavca, ocenjujemo, da je popolnitev delovnih mest v skladu z aktom o notranji organizaciji zelo ambiciozna in jo bo težko realizirati.

2.2.3 Preverjanje varnosti in funkcionalnosti informacijske opreme

V obdobju, na katero se nanaša revizija, vlada ni vzpostavila kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novovzpostavljenih organov.

Pojasnilo ministrstva

Testiranje informacijsko-komunikacijskih tehnologij na področju informacijske varnosti je naloga sektorja za skupne zadeve, v katerem je po sistemizaciji predvidenih 5 delovnih mest. Ministrstvo je predlogu proračuna 2020/21 za omenjeno področje že predvidelo 30.000 EUR.

Vlada je zagotovila ustanovitev v ZInfV predvidenih organov za posamezna področja zagotavljanja kibernetske varnosti, vendar ni pravočasno in za vse organe zagotovila ustreznih sredstev. Vlada je v predlogu ZIV pripravila analizo, v kateri je ugotovila obseg potreb po kadrovski in tehnološki okrepitvi. Nove, podrobnejše analize obsega potreb po kadrovski in tehnološki okrepitvi vlada kasneje ni več pripravila, prav tako ni preverila, ali so potrebe še vedno enake. Odsotnost akcijskega

načrta oziroma drugega operativnega dokumenta je po naši oceni ključno vplivala na (ne)izvajanje aktivnosti na področju kibernetske varnosti, ki pa se do leta 2019 niso začele. Vlada je vloge, naloge in pristojnosti na področju kibernetske varnosti opredelila v zakonodaji, podzakonskih predpisih in nekaterih operativnih dokumentih, vendar pa jih ni v celoti medsebojno uskladila, prav tako jih ni pravočasno posodobila in ni zagotovila virov, ki bi omogočali izvajanje predpisanih nalog. Vlada v obdobju, na katero se nanaša revizija, še ni vzpostavila kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novovzpostavljenih organov. Ocenjujemo, da bi morala vlada za vzpostavitev ustrezne organizacijske strukture pravočasno zagotoviti tudi zadostna sredstva za kadrovsko in tehnološko okrepitev na področju kibernetske varnosti, česar pa v obdobju, na katero se nanaša revizija, ni storila.

2.3 Pravne podlage za zagotavljanje kibernetske varnosti

Odgovor na vprašanje, **ali je ministrstvo pripravilo ustrezne pravne podlage za zagotavljanje kibernetske varnosti,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je ministrstvo:

- na podlagi analize področja kibernetske varnosti pripravilo predloge strateških in operativnih dokumentov za ureditev področja kibernetske varnosti;
- pripravilo vse podzakonske akte in druge dokumente na podlagi ZInfV.

2.3.1 Strateški in operativni dokumenti

V skladu z ZInfV bi morala vlada do 11. 5. 2019 sprejeti strategijo informacijske varnosti. Ministrstvo pa bi moralo kot pristojno resorno ministrstvo prej pripraviti predlog strategije informacijske varnosti in jo vladi predložiti v sprejem. Ministrstvo predloga strategije informacijske varnosti ni pripravilo pravočasno, zato strategija v zakonskem roku ni bila sprejeta.

Pojasnilo ministrstva

Ministrstvo se zaveda zamude pri pripravi nove strategije kibernetske/informacijske varnosti, do katere je prišlo iz objektivnih razlogov. Ob kadrovski podhranjenosti je bilo treba prioritizirati naloge in prednostno izvesti tiste, povezane s podzakonskimi akti ZInfV in določitvijo izvajalcev bistvenih storitev, ker je Sloveniji pretila kazen Evropske komisije. Sočasno je bilo treba izvesti vse potrebne postopke, povezane z organizacijo, pravnimi, kadrovskimi in tehničnimi zadevami za vzpostavitev uprave za informacijsko varnost. Nekateri od teh postopkov v septembru 2020 še vedno potekajo.

Ministrstvo v obdobju, na katero se nanaša revizija, akcijskega načrta ali drugega operativnega dokumenta za izvajanje nalog na področju kibernetske varnosti ni pripravilo oziroma sprejelo (več v točki 2.1.4 tega poročila).

2.3.2 Akti na podlagi ZInfV

V skladu z ZInfV minister podrobneje določi vsebino in strukturo varnostne dokumentacije, ki jo vzpostavijo in vzdržujejo izvajalci bistvenih storitev, ter minimalen obseg in vsebino varnostnih ukrepov, ki jih izvajalci bistvenih storitev pripravijo in izvajajo na podlagi omenjene dokumentacije. Minister pri tem predpiše tudi metodologijo za pripravo analize obvladovanja tveganj ter za določitev

ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki izhajajo iz politike neprekinjenega poslovanja, z načrtom njegovega upravljanja in za pripravo seznama njegovih ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov, ki so bistvenega pomena za delovanje bistvenih storitev.

Ministrstvo je pripravilo uredbo o določitvi bistvenih storitev, ki določa tiste storitve iz Uredbe o standardni klasifikaciji dejavnosti[67], ki se za potrebe izvajanja ZInfV štejejo za bistvene, določa pa tudi metodologijo za določitev izvajalcev bistvenih storitev, vključno z vrednotenjem medpodročnih in področnih dejavnikov. Vlada je v uredbi o določitvi bistvenih storitev določila 9 področij, na katerih se izvajajo bistvene storitve, ter 3 podpodročja na področju energije ter 4 podpodročja na področju prometa. Priloga k uredbi o določitvi bistvenih storitev vsebuje seznam bistvenih storitev po področjih in podpodročjih, na katerih se izvajajo bistvene storitve. V uredbi o določitvi bistvenih storitev so za vsako področje opredeljeni parametri za motnjo in za incident. Nekatere vrednosti teh parametrov za posamezno motnjo in incident pri zagotavljanju storitve so po naši oceni nastavljene previsoko. Kot primer navajamo motnje pri:

- zagotavljanju preskrbe s hrano, ki bi prizadele več kot 100.000 uporabnikov in lahko povzročile prekinitev storitve za več kot teden dni;
- zagotavljanju storitve železniškega potniškega prometa, ki bi prizadele vsaj 10.000 fizičnih oseb in lahko povzročile prekinitev za najmanj teden dni;
- zagotavljanju storitve bolnišnične dejavnosti, ki bi prizadele več kot 1.000 fizičnih oseb, oziroma dejavnosti nujne medicinske pomoči za več kot 100.000 oseb in lahko povzročile prekinitev za več kot teden dni;
- zagotavljanju storitve pitne vode, ki bi prizadele več kot 100.000 uporabnikov in lahko povzročile prekinitev za več kot teden dni;
- zagotavljanju storitev prodaje motornih goriv, ki bi prizadele vsaj 100.000 uporabnikov in lahko povzročile motnjo za več kot teden dni;
- zagotavljanju storitev prenosa ali distribucije električne energije, ki bi prizadele vsaj 100.000 uporabnikov in lahko onemogočile napajanje z električno energijo uporabnikom za vsaj 3 ure.

Priporočilo

Vladi priporočamo, naj prouči parametre za posamezno motnjo in incident pri zagotavljanju storitve, ki so navedeni v prilogi k uredbi o določitvi bistvenih storitev, in jih po potrebi prilagodi.

Minister je 13. 5. 2019 sprejel Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev[68] (v nadaljevanju: pravilnik o varnostni dokumentaciji IBS), ki je pričel veljati s 1. 6. 2019. Pravilnik o varnostni dokumentaciji IBS določa, da morajo izvajalci bistvenih storitev vzpostaviti in vzdrževati dokumentiran sistem upravljanja varovanja informacij in sistem upravljanja

67 Uradni list RS, št. 69/07 in 17/08.

68 Uradni list RS, št. 32/19.

neprekinjenega poslovanja. Pravilnik med drugim določa tudi metodologijo za pripravo analize obvladovanja tveganj ter metodologijo za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov. Prav tako določa tudi minimalni obseg in vsebino varnostnih ukrepov.

Ministrstvo je marca 2019 tudi pripravilo osnutek Pravilnika o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave[69], ki je bil ob koncu obdobja, na katero se nanaša revizija, še v fazi medresorskega usklajevanja.

Ukrep ministrstva

Minister za javno upravo je 5. 11. 2019 sprejel Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave[70].

Ministrstvo je zagotovilo nekatere pravne podlage za zagotavljanje kibernetske varnosti, ki jih določa ZInfV. Vendar pa ministrstvo tudi po preteku zakonskega roka, v katerem bi morala vlada sprejeti novo strategijo informacijske varnosti, ni pripravilo predloga te strategije oziroma tudi ni preverilo, ali je treba spremeniti, dopolniti ali zamenjati strategijo kibernetske varnosti iz leta 2016, ki je bila še vedno v veljavi. Ministrstvo v obdobju, na katero se nanaša revizija, tudi ni pripravilo akcijskega oziroma drugega operativnega načrta, potrebnega za jasno in nemoteno spremljanje izvajanja in uresničevanja strategije kibernetske varnosti. Ministrstvo v obdobju, na katero se nanaša revizija, ni pripravilo in sprejelo vseh podzakonskih aktov in drugih dokumentov, ki bi jih sicer moralo pripraviti v skladu z ZInfV, oziroma jih je pripravilo in/ali sprejelo z zamudo. Zato ocenjujemo, da ministrstvo ni bilo uspešno pri pripravi vseh podzakonskih aktov.

69 Z dne 8. 3. 2019, [URL: https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/381179], 26. 2. 2021.

70 Uradni list RS, št. 68/19.

3. Izvajanje nalog za zagotavljanje kibernetske varnosti

3.1 Vlada Republike Slovenije

Odgovor na vprašanje, **ali je vlada učinkovito izvajala naloge za zagotavljanje kibernetske varnosti,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je vlada:

- sprejela strategijo informacijske varnosti oziroma sprejela posodobljeno strategijo kibernetske varnosti;
- preverila potrebe in v skladu z ugotovljenimi potrebami zagotavljala vire;
- skrbela za redno izvajanje programov ozaveščanja na področju kibernetske varnosti;
- uvedla vsebine s področja kibernetske varnosti v sistem izobraževanja in usposabljanja;
- spodbujala razvoj in vpeljavo novih tehnologij na področju kibernetske varnosti;
- redno posodabljala zakonodajo in postopke skladno z razvojem informacijsko-komunikacijskih tehnologij;
- zagotovila pogoje za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti.

3.1.1 Strategija informacijske varnosti

Vlada je februarja 2016 sprejela strategijo kibernetske varnosti. Kasneje sprejeti ZInfV pa določa, da bo vlada sprejela novo strategijo informacijske varnosti, ki bo obravnavala predvsem:

- cilje in prednostne naloge strategije;
- okvir upravljanja za dosego ciljev in prednostnih nalog strategije, vključno z vlogami in odgovornostmi državnih organov in drugih ustreznih deležnikov;
- opredelitev ukrepov v zvezi s pripravljenostjo, odzivanjem in ponovno vzpostavitvijo informacijske varnosti, vključno s sodelovanjem med javnim in zasebnim sektorjem;
- opredelitev programov izobraževanja, ozaveščanja in usposabljanja v zvezi s strategijo;
- opredelitev načrtov raziskav in razvoja v zvezi s strategijo;
- načrt ocene tveganja za prepoznavanje tveganj;
- seznam različnih subjektov, vključenih v izvajanje strategije.

Vlada strategije informacijske varnosti ni sprejela v zakonskem roku do 11. 5. 2019, kakor tudi ne do konca obdobja, na katero se nanaša revizija.

Pojasnilo vlade

Prioriteta vlade je bil sprejem ReSNV-2 in vzpostavitev uprave za informacijsko varnost. ReSNV-2 je podlaga za prenovljeno strategijo kibernetske varnosti, ki jo predvideva ZInfV, saj vsebuje poglavja oziroma točke, ki se pomembno nanašajo na informacijsko in kibernetsko varnost. Vlada se zaveda potrebe po čimprejšnjem sprejemu strategije informacijske varnosti. Kljub temu da je zakonski rok za

sprejem že potekel, pa je dejstvo, da tudi veljavna strategija kibernetske varnosti iz leta 2016 že predvideva vzpostavitev učinkovitega sistema zagotavljanja kibernetske varnosti do leta 2020.

Ocenjujemo, da zamude zakonskih rokov pri pripravi oziroma posodobitvah temeljnih dokumentov na področju kibernetske varnosti predstavljajo tveganje, da učinkovit sistem zagotavljanja kibernetske varnosti ne bo vzpostavljen pravočasno.

3.1.2 Preveritev potreb in zagotavljanje virov

Ob pripravi predloga strategije kibernetske varnosti je delovna skupina pripravila in posredovala predlog akcijskega načrta za uresničevanje strategije kibernetske varnosti. Predlagani akcijski načrt ni bil potrjen, prav tako pa ni bil kasneje pripravljen in potrjen noben drug načrt za uresničevanje strategije kibernetske varnosti (več v točki 2.1.4 tega poročila).

Pojasnilo vlade

Vlada je bila v obdobju, na katero se nanaša revizija, zelo aktivna s sprejemom resolucije (ReSNV-2) in vzpostavitvijo uprave za informacijsko varnost, pri čemer so bili roki skladni z odločitvami, sprejetimi na sejah SSNAV. Ti sklepi predstavljajo pristojnim organom vodilo za delo oziroma delovni akcijski načrt. Sprejem akcijskega načrta trenutno ni aktualen, bo pa sprejet skupaj oziroma po sprejemu nove strategije v letu 2020, ki bo začrtala aktivnosti za prihodnje obdobje[71]*.*

3.1.3 Programi ozaveščanja

SI-CERT že od leta 2011 izvaja program ozaveščanja najširše slovenske javnosti Varni na internetu in sodeluje v programu SAFE.si[72]. Oba programa sta se začela izvajati že pred sprejetjem strategije kibernetske varnosti. Vlada drugih novih programov, akcij oziroma aktivnosti za ozaveščanje različnih javnosti na področju kibernetske varnosti ni izvajala ali financirala in jih zaenkrat tudi ni predvidela v prihodnje.

Programi in projekti ozaveščanja so se izvajali že pred sprejetjem strategije kibernetske varnosti, pa vendar sta tako strategija in predlog ZInfV opozorila, da obstaja velika podhranjenost na tem področju. Tudi Evropsko računsko sodišče je v informativnem dokumentu poudarilo, da je ENISA opozorila na to, da imajo uporabniki kritično vlogo v boju proti kibernetskim napadom in da so pridobivanje znanja, izobraževanja in ozaveščanje ključni za vzpostavitev kibernetsko odporne družbe[73].

---

71 Povezava s pojasnilom vlade v točki 2.1.4 tega poročila.

72 Namenjen osveščanju o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje.

73 ECA, Challenges to effective EU cybersecurity policy, Briefing Paper, March 2019, [URL: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf], 26. 2. 2021.

3.1.4 Uvajanje vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja

Strategija kibernetske varnosti navaja, da je informacijska oziroma kibernetska varnost vključena v nekaj študijskih programov fakultet in v študijski program samostojnega visokošolskega zavoda, ki so jih ustanove samoiniciativno uvedle v svoje programe še pred objavo strategije. Strategija kibernetske varnosti med cilji navaja tudi ukrep uvedbe vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja. Vlada v reviziji ni izkazala dodatnih ukrepov za dosego tega cilja.

Pojasnilo vlade

Smiselno bi bilo, da bi se v programu usposabljanja o tajnih podatkih, ki ga izvaja urad za varovanje tajnih podatkov, poudarila vsebina glede informacijske/kibernetske varnosti. Vsekakor pa je področje izobraževanja ena ključnih nalog uprave za informacijsko varnost, v okviru katere bo deloval tudi Sektor za dvig odpornosti in z ministrstvom, pristojnim za izobraževanje, sodeloval pri uvedbi tem s področja informacijske/kibernetske varnosti v izobraževalne programe na osnovni in srednješolski ravni.

3.1.5 Spodbujanje razvoja in vpeljave novih tehnologij

Vlada je spodbujala razvoj in vpeljavo novih tehnologij na področju kibernetske varnosti, in sicer je v letu 2019 vzpostavljala informacijski sistem na državni ravni, imenovan Tajni državni računalniški oblak (v nadaljevanju: TDRO). Vlada je načrtovala, da bo s TDRO vsem ministrstvom, generalnemu sekretariatu vlade, kabinetu predsednika vlade, Stalnemu predstavništvu Republike Slovenije pri Evropski uniji v Bruslju in drugim omogočila elektronsko komuniciranje z dokumenti, ki so označeni do vključno stopnje tajnosti "TAJNO" po Zakonu o tajnih podatkih[74]. Vlada je še načrtovala, da bo projekt TDRO dokončan do konca leta 2019. Vlada ni spodbujala razvoja oziroma vpeljave drugih novih tehnologij.

3.1.6 Posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij

Ker je bil ZInfV sprejet šele leta 2018, vlada v obdobju, na katero se nanaša revizija, še ni predlagala nobenih sprememb ali dopolnitev. ZInfV je določil vrsto drugih aktivnosti, ki so jih morali vlada, minister oziroma ministrstvo, izvajalci bistvenih storitev in organi državne uprave izvesti v zakonsko določenih rokih. Vlada in ministrstvo sta pri večjem številu aktivnosti zamujala oziroma ob koncu obdobja, na katero se nanaša revizija, še vedno niso bile izvedene oziroma dokumenti še niso bili sprejeti.

Tabela 8 prikazuje nosilce, aktivnosti, roke, datume realizacije, zamudo v dnevih ter komentar, če določena aktivnost še ni bila zaključena do konca obdobja, na katero se nanaša revizija.

74 Uradni list RS, št. 50/06-UPB2, 9/10, 60/11 in 8/20.

Tabela 8: Status aktivnosti po ZInfV

Nosilec	Člen ZInfV	Aktivnost	Rok	Datum realizacije	Zamuda (št. dni)
Vlada	6. (1)	Določi seznam bistvenih storitev.	11. 11. 2018	22. 6. 2019	**223**
	6. (2)	Določi posameznega izvajalca bistvenih storitev.	22. 12. 2019[3)]	17. 10. 2019[4)]	
				7.11.2019[5)]	
				28.11.2019[6)]	
				5. 3. 2020[7)]	**72**
				12. 3. 2020[8)]	**84**
	6. (3)	Določi izvajalce kritične infrastrukture in nosilce obrambnega načrtovanja kot izvajalce bistvenih storitev.	11. 8. 2019[1)]		**> 50**
	7. (4)	Določi metodologijo za določitev izvajalcev bistvenih storitev.	11. 11. 2018	22. 6. 2019	**223**
	9. (1)	Določi organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.	11. 5. 2019[1)]		**> 142**
	26.	Sprejme strategijo informacijske varnosti.	11. 5. 2019[1)]		**> 142**
	27. (1)	Začetek delovanja pristojnega nacionalnega organa v sestavi ministrstva.	1. 1. 2020	1. 9. 2019	
	40. (4)	Uskladi sklep o uradu za varovanje tajnih podatkov 2018.	11. 8. 2018	26. 7. 2018	
	41. (1)	Začetek delovanja nacionalnega CSIRT.	1. 1. 2019	1. 1. 2019	
	41. (2)	Začetek delovanja CSIRT organov državne uprave.	1. 1. 2019	1. 1. 2019	
	42. (1)	Uskladi Uredbo o organih v sestavi ministrstev.	11. 8. 2018	26. 7. 2018	
Minister	12. (3)	Določi vsebino in strukturo varnostne dokumentacije za izvajalce bistvenih storitev.	11. 11. 2018	1. 6. 2019	**202**
	17. (3)	Določi vsebino in strukturo varnostne dokumentacije za organe državne uprave.	11. 11. 2018[2)]	30. 11. 2019	**384**
Izvajalci bistvenih storitev	43. (2)	Morajo izpolniti varnostne zahteve in zahteve za priglasitev.	8. 11. 2019		
Organi državne uprave	43. (5)	Morajo izpolniti varnostne zahteve in zahteve za priglasitev.	11. 8. 2020		

Opombe: [1)] Še ni bil določen do zaključka obdobja, na katero se nanaša revizija, to je do 30. 9. 2019.

[2)] Zaključeno po koncu obdobja, na katero se nanaša revizija.

[3)] V skladu z ZInfV bi morali biti izvajalci bistvenih storitev imenovani do 11. 5. 2019, vendar se je zaradi prepoznega sprejetja uredbe o določitvi bistvenih storitev ta rok podaljšal do 22. 12. 2019.

[4)] Vlada je določila prvih 12 izvajalcev bistvenih storitev.

[5)] Vlada je določila še 6 izvajalcev bistvenih storitev.

[6)] Vlada je določila še 3 izvajalce bistvenih storitev.

[7)] Vlada je določila še 1 izvajalca bistvenih storitev.

[8)] Vlada je določila še 5 izvajalcev bistvenih storitev.

Vlada in ministrstvo v obdobju, na katero se nanaša revizija, nista pripravila drugih zakonskih in podzakonskih aktov s področja kibernetske varnosti.

3.1.7 Zagotavljanje pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih

Predstavniki ministrstva, Ministrstva za obrambo Republike Slovenije in urada za varovanje tajnih podatkov sodelujejo v mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti[75]. Prav tako predstavniki organov sodelujejo na mednarodnih vajah[76] (več v točkah 3.2.3, 3.2.4 in 3.3.7 tega poročila).

Pojasnilo vlade

Vlada se seznanja z načrtovanimi vajami kot tudi s poročili o udeležbah na vajah.

Vlada je po sprejemu strategije kibernetske varnosti, prenosu NIS direktive v slovenski pravni red z ZInfV in z uredbo o IVvDU predvidela pripravo vrste podzakonskih aktov in drugih dokumentov, vendar pa ocenjujemo, da za izvedbo ni zagotovila vseh ustreznih virov. S tem ni bilo osnovnih predpogojev, da bi bili vsi načrtovani cilji strategije kibernetske varnosti in določila v ZInfV lahko doseženi. Razen že obstoječih programov ozaveščanja Varni na internetu in SAFE.si, vlada ni poskrbela za izvajanje drugih programov, kljub temu da je pomen ozaveščanja večkrat poudarila v svojih dokumentih. Vlada tudi ni uvedla programov s področja kibernetske varnosti v izobraževalne procese na katerikoli stopnji. Vlada je zagotavljala mednarodno sodelovanje predstavnikov Republike Slovenije v različnih delovnih telesih in sodelovanje pri vajah kibernetske varnosti. Vlada je na področju razvoja in vpeljave novih tehnologij začela z vpeljavo informacijskega sistema TDRO, namenjenega varni komunikaciji zaupnih informacij, ni pa vpeljala drugih tehnoloških novosti za dvig kibernetske odpornosti. Vlada je nekatere podzakonske akte, ki bi jih morala sprejeti na podlagi ZInfV, sprejela z zamudo, nekaterih pa kljub poteku rokov ob koncu obdobja, na katero se nanaša revizija, še ni sprejela. Vlada je bolj aktivno začela izvajati naloge na področju kibernetske varnosti konec leta 2018 in v letu 2019 na način, da je izvajanje aktivnosti na področju kibernetske varnosti koordinirala prek SSNAV. Ocenjujemo, da je vlada delno učinkovito izvajala naloge za zagotavljanje kibernetske varnosti.

75 Horizontalna delovna skupina za kibernetska vprašanja pri Evropski uniji, skupina za sodelovanje po NIS direktivi pri Evropski uniji, odbor za kibernetsko obrambo pri Evropski uniji, upravni odbor pri ENISA.

76 Cyber Europe 2016 in Cyber Europe 2018 (ENISA), EU Hybrid Exercise 2018, Cyber Coalition 2016, 2017, 2018 (NATO).

3.2 Urad Vlade Republike Slovenije za varovanje tajnih podatkov

Odgovor na vprašanje, **ali je urad za varovanje tajnih podatkov učinkovito izvajal naloge za zagotavljanje kibernetske varnosti,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je urad za varovanje tajnih podatkov:

- ustrezno opredelil področje v okviru svoje organizacije ter določil zadostno število zaposlenih za opravljanje teh aktivnosti;
- izvajal vse naloge na področju kibernetske varnosti v skladu z ZInfV in sklepom vlade;
- redno sodeloval na mednarodnih vajah s področja kibernetske varnosti;
- sodeloval v okviru mednarodnih delovnih teles in združenj s področja kibernetske varnosti;
- izvedel nacionalne vaje s področja kibernetske varnosti.

3.2.1 Organiziranost urada za varovanje tajnih podatkov in kadri

Urad za varovanje tajnih podatkov je manjši državni organ, ki ni razdeljen na notranje organizacijske enote. Urad za varovanje tajnih podatkov je z ZInfV, ki je pričel veljati 11. 5. 2018, dobil dodatne pristojnosti s področja kibernetske varnosti. Do vzpostavitve delovanja uprave za informacijsko varnost, ki je bilo predvideno s 1. 1. 2020, je bil urad zadolžen za opravljanje nalog nacionalnega organa kot začasni pristojni nacionalni organ. Naloge s področja kibernetske varnosti so poleg svojih rednih nalog s področja varstva tajnih podatkov opravljali 3 uslužbenci.

Pojasnilo urada za varovanje tajnih podatkov

2 javna uslužbenca sta poleg ostalih rednih nalog opravljala naloge s področja kibernetske varnosti v manjši meri (približno devetino delovnega časa), tretji pa je bil s področjem kibernetske varnosti obremenjen približno dve tretjini delovnega časa.

Predstavniki urada za varovanje tajnih podatkov so med 20. 4. 2017 in 31. 12. 2017 sodelovali v medresorski projektni skupini za kibernetsko varnost, katere namen je bil pripraviti predlog ZKI, ki je bil sprejet konec decembra 2017.

Kljub temu da so bile uradu za varovanje tajnih podatkov dodeljene naloge na področju kibernetske varnosti, pa mu niso bila dodeljena dodatna kadrovska in finančna sredstva. Predviden obseg kadrovskih in finančnih sredstev, ki naj bi bil za urad za varovanje tajnih podatkov zagotovljen iz finančnih postavk in kadrovskih kvot ministrstva, ni bil realiziran. Urad za varovanje tajnih podatkov je s strani ministrstva za potrebe službenih poti prejel finančna sredstva v znesku 3.750 EUR. Z rebalansom proračuna za leto 2019 so bila predvidena dodatna sredstva za zaposlitev 2 javnih uslužbencev na področju kibernetske varnosti.

Urad za varovanje tajnih podatkov je šele konec leta 2018 sistematiziral delovno mesto za področje kibernetske varnosti in decembra 2018 objavil javni natečaj za zasedbo prostega uradniškega delovnega mesta. S 1. 6. 2019 se je v uradu za področje kibernetske varnosti zaposlil 1 javni uslužbenec.

3.2.2 Izvajanje nalog

Urad za varovanje tajnih podatkov ni izvajal vseh nalog v skladu z ZInfV in za katere ga je vlada pooblastila, saj vlada ni sprejela vseh podzakonskih aktov, ki jih določa ZInfV. Prav tako je bil omejen pri izvajanju nalog, saj ni imel ustrezno usposobljenega kadra za izvajanje vseh nalog s področja kibernetske varnosti.

Tabela 9 strnjeno prikazuje našo oceno o realizaciji izvajanja nalog urada za varovanje tajnih podatkov.

Tabela 9: Ocena o realizaciji izvajanja nalog urada za varovanje tajnih podatkov

Naloge urada za varovanje tajnih podatkov na podlagi sklepa o uradu za varovanje tajnih podatkov 2017 in sklepa o uradu za varovanje tajnih podatkov 2018	Ocena
Usklajuje zmogljivosti za zagotavljanje kibernetske varnosti	da/delno po svojih zmožnostih
Sodeluje z ustreznimi organi Evropske unije, zveze NATO in organi drugih mednarodnih organizacij in držav ter skrbi za izvajanje sprejetih mednarodnih obveznosti in mednarodnih pogodb na področju kibernetske varnosti	da/delno po svojih zmožnostih
Usklajuje izvajanje strategije kibernetske varnosti	ne
Sodeluje pri načrtovanju postopkov in ukrepov na področju tveganj ter varnosti omrežij in informacijskih sistemov	da/delno po svojih zmožnostih
Dejavno se vključuje v izobraževalni proces na področju kibernetske varnosti	delno – ozaveščanje
Sodeluje pri načrtovanju postopkov in ukrepov za obvladovanje kibernetskih incidentov	ne[1)]
Sodeluje z znanstvenoraziskovalnimi ustanovami in zasebnim sektorjem pri spodbujanju in krepitvi kibernetske varnosti in odpornosti ključne informacijsko-komunikacijske infrastrukture	da
Spremlja zmogljivosti za zagotavljanje kibernetske varnosti na državni ravni	da/delno po svojih zmožnostih
Sodeluje pri organizaciji in usklajevanju državne vaje iz kibernetske varnosti ter pri usklajevanju mednarodnih vaj iz kibernetske varnosti	ne/delno
Sodeluje pri spremljanju kibernetskih incidentov na državni ravni	da – po svojih zmožnostih
Sodeluje pri usklajevanju in usmerjanju delovanja skupin za odzivanje na kibernetske incidente v Republiki Sloveniji	ne[1)]
Sodeluje pri zagotavljanju zgodnjega obveščanja, opozarjanja in informiranja vseh deležnikov o tveganjih in kibernetskih incidentih	ne[1)]
Sodeluje v mednarodni mreži organov, pristojnih za odzivanje na kibernetske incidente	da – po svojih zmožnostih
Ministrstvu, pristojnemu za informacijsko družbo, predlaga sprejem ukrepov v primeru težjega ali kritičnega incidenta ali v primeru kibernetskega napada ter v primeru stanja povečane ogroženosti na podlagi zakona, ki ureja informacijsko varnost	ni bilo takega incidenta in kibernetskega napada
Vodi seznam kontaktnih podatkov zavezancev ter skupni seznam incidentov in kibernetskih napadov	delno – seznam incidentov
Obvešča javnosti o incidentih in v zvezi z njimi sprejetih ukrepih	ni bilo takega incidenta in kibernetskega napada
Izpolnjuje mednarodne obveznosti in opravlja naloge mednarodne izmenjave podatkov, vključno z izvajanjem nalog enotne kontaktne točke in sodelovanja s pristojnimi organi s področja informacijske varnosti v Evropski uniji, določene z zakonom, ki ureja informacijsko varnost	da – po svojih zmožnostih
Opravlja koordinacijske, strokovno-tehnične, organizacijske in razvojne naloge na področju informacijske varnosti in kibernetske obrambe, določene z zakonom, ki ureja informacijsko varnost, in njegovimi podzakonskimi predpisi	ne[2)]
Je pristojen za kriptografsko zaščito podatkov	da

Opombi: [1)] Še niso bili vzpostavljeni ustrezni organi, ki bi vodili in usmerjali te aktivnosti.
[2)] V obdobju, na katero se nanaša revizija, urad za varovanje tajnih podatkov ni imel ustrezne zakonske podlage za izvajanje nalog, podzakonski predpisi pa še niso bili sprejeti.

Urad za varovanje tajnih podatkov med drugim ni izvajal nalog, ki se nanašajo na njegovo sodelovanje z izvajalci bistvenih storitev, saj teh izvajalcev vlada v obdobju, ko je urad za varovanje tajnih podatkov opravljal naloge pristojnega nacionalnega organa, še ni določila. Urad za varovanje tajnih podatkov je sodeloval pri pripravi predloga ReSNV-2 ter pripravi nekaterih podzakonskih aktov, ki jih določa ZInfV. S pripombami in mnenji je urad za varovanje tajnih podatkov sodeloval pri pripravi uredbe o določitvi bistvenih storitev, pravilnika o varnostni dokumentaciji IBS ter Pravilnika o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave.

Urad za varovanje tajnih podatkov je v okviru svojih pristojnosti sodeloval z novinarji (16 sodelovanj med 31. 3. 2017 in 14. 8. 2019), na okroglih mizah (26 dogodkov med 13. 4. 2017 in 29. 11. 2018) ter skliceval oziroma se udeleževal sestankov (28 sestankov med 13. 3. 2017 in 18. 4. 2019) s posameznimi organi v Sloveniji, pomembnimi za zagotavljanje kibernetske varnosti. Urad za varovanje tajnih podatkov je za potrebe nacionalnega sistema za zagotavljanje informacijske varnosti opravil informativne sestanke s SI-CERT, AKOS, SOVA, Ministrstvom za notranje zadeve, Ministrstvom za obrambo, ministrstvom ter Ministrstvom za zunanje zadeve. Urad za varovanje tajnih podatkov je 16. 1. 2019 sklical sestanek pomembnejših deležnikov za zagotavljanje kibernetske varnosti v Sloveniji z namenom izmenjave informacij v povezavi z aktualnimi mednarodnimi dogodki. V okviru projekta Cyber Interreg[77] je urad za varovanje tajnih podatkov sodeloval z Gospodarsko zbornico Slovenije[78] (v nadaljevanju: GZS). V okviru predstavitve predloga nove ReSNV-2 je urad za varovanje tajnih podatkov sodeloval tudi na posvetu oziroma javni obravnavi predloga na Fakulteti za družbene vede Univerze v Ljubljani. V državnem zboru je urad za varovanje tajnih podatkov sodeloval v razpravi Odbora za obrambo, in sicer o stanju na področju kibernetske varnosti. V organizaciji Inštituta za korporativno upravljanje je urad za varovanje tajnih podatkov ob sodelovanju Informacijskega pooblaščenca izvedel posvet o kibernetski varnosti v Državnem svetu s ciljem krepitve ozaveščanja[79]. Urad za varovanje tajnih podatkov je kot začasni pristojni nacionalni organ vodil seznam incidentov, ki mu jih posredujeta nacionalni CSIRT in CSIRT organov državne uprave. Tedenska poročila, ki jih je prejel od poročevalcev (tabela 10), je evidentiral v aplikaciji SPIS in jih za namen poročanja tudi zabeležil v preglednico.

Urad za varovanje tajnih podatkov je kot začasni pristojni nacionalni organ za informacijsko varnost o stanju na kibernetskem področju redno sodeloval v OS SNAV in SSNAV.

Urad za varovanje tajnih podatkov ni imel sredstev za vzpostavitev evidenc o incidentih, zato se je prijavil na razpis Evropske komisije – razpis CEF v upanju, da bo sredstva pridobil. Urad za varovanje tajnih podatkov je zaprosil za finančno pomoč v znesku 100.000 EUR, od katerega bi po oceni 30.000 EUR porabil za vzpostavitev računalniške podpore evidencam ter 70.000 EUR za izobraževanje. Urad za varovanje tajnih podatkov načrtov, kako bodo porabljena morebiti pridobljena sredstva, ni pripravil. Evropska komisija je 26. 4. 2019 sporočila, da uradu za varovanje tajnih podatkov ni bila odobrena finančna pomoč.

77 Regionalne politike za konkurenčna mala in srednja podjetja za kibernetsko varnost (angl.: *Regional policies for competitive cybersecurity SMEs*), [URL: https://www.interregeurope.eu/cyber/], 26. 2. 2021.

78 [URL: https://www.gzs.si/sekv/vsebina/cyber_interreg], 26. 2. 2021.

79 [URL: https://www.ics-institut.si/dogodki/nacionalni-posvet-kibernetska-varnost-republike-slovenije-v-luči-vedno-pogostejših-hekerskih-vdorov-kako-učinkovito-implementirati-rešitve-zakona-o-informacijski-varnosti], 26. 2. 2021.

V skladu s 13. členom ZInfV morajo izvajalci bistvenih storitev nacionalnemu CSIRT brez nepotrebnega odlašanja priglasiti incidente s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev, ki jih zagotavljajo. Nacionalni CSIRT o incidentu obvesti pristojni nacionalni organ. V Republiki Sloveniji v obdobju, na katero se nanaša revizija, ni bilo zaznanega kibernetskega incidenta s pomembnim vplivom na neprekinjeno izvajanje bistvenih storitev[80]. Od januarja 2019 je nacionalni CSIRT uradu za varovanje tajnih podatkov redno tedensko poročal o prijavljenih incidentih. CSIRT organov državne uprave in Enotni kontaktni center (v nadaljevanju: EKC) ministrstva sta šele v marcu 2019 pristojni nacionalni organ začela obveščati o incidentih. V tabeli 10 so navedene osnovne informacije o javljenih incidentih za obdobje od 1. 1. 2019 do 30. 9. 2019.

Tabela 10: Prikaz javljenih incidentov za obdobje od 1. 1. 2019 do 30. 9. 2019

Datum	Opis	Vir obvestila
8. 3. 2019	Obvestilo o zlonamerni elektronski pošti (WeTransfer)	CSIRT organov državne uprave, EKC
25. 3. 2019	Vidnost pacientov na spletnih straneh Splošne bolnišnice Izola	nacionalni CSIRT
25. 3. 2019	Zloraba sistema za nadgradnje podjetja Asus	nacionalni CSIRT
9. 5. 2019	Goljufiva elektronska sporočila z lažnim predstavljanjem	CSIRT organov državne uprave, EKC
10. 5. 2019	SPAM/Phishing abuse report	nacionalni CSIRT
20. 5. 2019	Obvestilo o pojavu zlonamerne elektronske pošte – direktorska prevara	EKC
10. 6. 2019	Google Incident Notification	irski NCSC[1)]
10. 6. 2019	Obvestilo o pojavu zlonamerne elektronske pošte – izsiljevalsko sporočilo "Tvoje skrivno življenje"	EKC
11. 6. 2019	Obvestilo o pojavu zlonamerne elektronske pošte – izsiljevalsko sporočilo "Tvoje skrivno življenje"	CSIRT organov državne uprave, EKC
12. 6. 2019	Obvestilo o pojavu zlonamerne elektronske pošte – Phishing	EKC
17. 6. 2019	Guidance for vulnerabilities – Intel	NATO
12. 7. 2019	Napad onemogočanja (DDoS) na spletno mesto Policije	nacionalni CSIRT
15. 7. 2019	Poročilo o incidentu informacijske varnosti	Policija
17. 7. 2019	Napad onemogočanja (DDoS) na bolgarsko Ministrstvo za finance	nacionalni CSIRT
9. 8. 2019	Poročilo o napadu v javnem zavodu Lekarna Ljubljana	nacionalni CSIRT
12. 8. 2019	Poročilo o napadu v javnem zavodu Lekarna Ljubljana	nacionalni CSIRT
28. 8. 2019	Obvestilo o pojavu zlonamerne elektronske pošte – Telekom Slovenije/Siol.net	EKC
September 2019	Priglasitev incidenta informacijske varnosti pristojnemu nacionalnemu organu in nacionalnemu CSIRT	CSIRT organov državne uprave, EKC

Opomba: [1)] Angl.: *National Cyber Security Centre.*
Vir: podatki urada za varovanje tajnih podatkov.

[80] Razen incidenta z izsiljevalskim virusom v javnem zavodu Lekarna Ljubljana (povezava z opombo 39).

Urad za varovanje tajnih podatkov v obdobju, na katero se nanaša revizija, ni imel izdelane metodologije za ocenjevanje incidentov in ni imel izdelanih navodil glede ukrepanja v primeru priglasitve incidenta.

> ***Priporočilo***
>
> *Ministrstvu priporočamo, naj pristojni nacionalni organ pripravi metodologijo za vrednotenje incidentov in navodila, ki bodo vsebovala procese ukrepanja v primeru različnih stopenj incidentov in te procese prične izvajati ob priglasitvi incidentov.*

Vlada je sprejela uredbo o določitvi bistvenih storitev v juniju 2019. Ker morajo izvajalci bistvenih storitev izpolniti varnostne zahteve in zahteve za priglasitev incidentov v 6 mesecih od njihove določitve, urad za varovanje tajnih podatkov zaradi prenosa nalog na upravo za informacijsko varnost v obdobju, na katero se nanaša revizija, še ni prejel priglasitve incidentov izvajalcev bistvenih storitev. Urad za varovanje tajnih podatkov še ni prejel priglasitve kibernetskega napada, ki bi imel večji medpodročni vpliv in ki bi ga priglasil nacionalni CSIRT ali CSIRT organov državne uprave. Urad za varovanje tajnih podatkov je kot pristojni nacionalni organ za informacijsko varnost o stanju na kibernetskem področju redno seznanjal OS SSNAV in SSNAV. Urad za varovanje tajnih podatkov je pisno obvestil OS SSNAV o vdoru z izsiljevalskim virusom v javni zavod Lekarna Ljubljana. Drugih kibernetskih incidentov, o katerih bi moral poročati OS SSNAV in SSNAV, urad za varovanje tajnih podatkov ni zaznal. Urad za varovanje tajnih podatkov je za OS SSNAV pripravili poročilo o stanju kibernetske varnosti v Republiki Sloveniji in kibernetskih incidentih v Evropi. Urad za varovanje tajnih podatkov se še ni soočil s primerom/incidentom, za katerega bi ocenil, da je o njem treba obveščati druge države članice Evropske unije. Urad za varovanje tajnih podatkov je skupaj z ministrstvom pripravil poročilo o stanju kibernetske varnosti za leto 2017 in ga posredoval Evropski komisiji. Do konca obdobja, na katero se nanaša revizija, urad za varovanje tajnih podatkov še ni posredoval poročila o stanju kibernetske varnosti za leto 2018 Evropski komisiji. O napredku kibernetske varnosti v državi je urad za varovanje tajnih podatkov skladno z zavezo o kibernetski obrambi poročal zvezi NATO za leti 2017 in 2018.

3.2.3 Sodelovanje na mednarodnih vajah

Urad za varovanje tajnih podatkov je na podlagi sklepov vlade sodeloval na več mednarodnih vajah:

- Cyber Europe 2016,
- Cyber Europe 2018,
- EU Hybrid Exercise – MULTILAYER 2018,
- NATO Cyber Coalition 2016,
- NATO Cyber Coalition 2017 in
- NATO Cyber Coalition 2018.

Urad za varovanje tajnih podatkov je sodeloval tudi na kibernetski vaji iz strateškega odločanja 2018[81], ki je bila izvedena v okviru Evropske obrambne agencije med 22. 5. 2018 in 24. 5. 2018 v Sloveniji. Poročilo o tej vaji je pripravilo Ministrstvo za obrambo. V poročilu, s katerim se je vlada seznanila novembra 2018, so navedena odprta vprašanja in predlogi za nadaljnje delo:

- povezava med kriznim odzivanjem in kibernetskimi incidenti (težji incident, kritični incidenti, kibernetski napad, stanje povečane ogroženosti) v ZInfV ni celovito opredeljena;
- preprečevanje kibernetskih incidentov in njihovih posledic v kriznih razmerah; ZInfV omogoča pristojnemu organu, da v stanju povečane ogroženosti zavezancem po ZInfV določi ukrepe za preprečitev ali zmanjšanje verjetnosti realizacije incidenta ter zmanjšanje škodljivih posledic; ni pa zakonske podlage za določitev ukrepov za ostale, ki niso zavezanci po ZInfV;
- komuniciranje z javnostmi oziroma pristojnosti in usklajevanje obveščanja javnosti med subjektom, ki je bil deležen kibernetskega incidenta, SI-CERT in ostalimi, ki sodelujejo pri preprečevanju in odpravi posledic incidenta, ni posebej opredeljeno;
- odgovorno prijavljanje ranljivosti na kibernetske incidente ni urejeno v ZInfV;
- vloga obrambnega resorja v primeru vsakodnevnega odzivanja na kibernetske incidente na subjekte izven obrambnega resorja ter vloga obrambnega resorja glede odzivanja na kibernetske incidente na subjekte izven obrambnega resorja v kriznih razmerah, vojni in primeru zaščite kritične infrastrukture, ki ni v pristojnosti obrambnega resorja, nista opredeljeni;
- delovanje Slovenske vojske v kibernetskem prostoru in v tradicionalnih domenah z upoštevanjem kibernetske domene kot prostora hibridnega in vojaškega delovanja v Sloveniji ni vzpostavljeno skladno z usmeritvami zveze NATO;
- umestitev urada za varovanje tajnih podatkov v prehodnih določbah ZInfV kot pristojnega nacionalnega organa se je izkazala kot zelo dobra.

3.2.4 Sodelovanje v mednarodnih delovnih telesih in združenjih

Urad za varovanje tajnih podatkov je sodeloval tudi v različnih mednarodnih delovnih telesih in združenjih:

- Na ravni Evropske unije je skupaj s predstavniki ministrstva sodeloval v horizontalni delovni skupini za kibernetsko varnost in skupini za sodelovanje po NIS direktivi. Predstavniki urada za varovanje tajnih podatkov so sodelovali tudi v delovni skupini za evropske zadeve. Nosilec aktivnosti (lastnik kibernetskega dosjeja) je bilo ministrstvo, urad za varovanje tajnih podatkov je po potrebi sodeloval pri pripravi stališč. Delovna skupina za evropske zadeve je obravnavala tematike, ki so bile kasneje obravnavane na odboru stalnih predstavnikov COREPER[82] I.
- V upravnem odboru ENISA je direktorica urada za varovanje tajnih podatkov zastopala Republiko Slovenijo.
- Na področju zveze NATO je urad za varovanje tajnih podatkov skupaj z ministrstvom za obrambo sodeloval v delovnih telesih Cyber Defence Committee ter Cyber Defence Management Board.

81 Angl.: *Comprehensive Cyber Strategic Decision Making Exercise 2018.*

82 Angl.: *Committee of the Permanent Representatives of the Governments of the Member States to the European Union.*

Intenzivnost delovanja urada za varovanje tajnih podatkov v posameznih mednarodnih delovnih telesih je bila različna:

- V okviru Sveta Evropske unije: horizontalna delovna skupina za kibernetska vprašanja, ki se sestaja tedensko. Primarno delovno skupino je pokrival ataše Republike Slovenije pri Stalnem predstavništvu Republike Slovenije pri Evropski uniji v Bruslju. Predstavnik urada za varovanje tajnih podatkov se je sestankov udeleževal občasno, skladno z dogovorom. Do sedaj se je urad za varovanje tajnih podatkov zasedanja delovne skupine udeležil 3-krat. V delovnih skupinah Sveta Evropske unije se poskuša doseči dogovor o čim več vprašanjih in pripravljajo predlogi političnih rešitev na višjih ravneh. Tu je bilo tudi prvič predstavljeno stališče Republike Slovenije do obravnavanih predlogov.
- V okviru Komisije Evropske unije: skupina za sodelovanje po NIS, ki se sestaja 2- do 3-krat letno. Primarno delovno skupino pokrivata predstavnika ministrstva in predstavnik urada za varovanje tajnih podatkov, ki je član omenjene delovne skupine od leta 2018. Do danes se je predstavnik urada za varovanje tajnih podatkov le 1-krat udeležil sestanka.
- V okviru zveze NATO: odbor za kibernetsko obrambo, ki se je sestajal mesečno. Trenutno delovno skupino pokriva obrambni predstavnik Republike Slovenije pri Stalnem predstavništvu Republike Slovenije pri zvezi NATO v Bruslju, katerega primarna naloga ni bilo pokrivanje področja kibernetske varnosti. Predstavnika urada za varovanje tajnih podatkov sta se udeležila sestankov na direktorski ravni, ki potekajo 1-krat do 2-krat na leto.

Direktor urada za varovanje tajnih podatkov se je udeležil 2 sestankov upravnega odbora ENISA, in sicer 11. 10. 2017 in 18. 7. 2018. Na sestankih oziroma tematskih sejah upravnega odbora[83] so bili obravnavani programski dokumenti. Roki za pripravo odzivov na gradivo, ki je v obravnavi na delovnih telesih Evropske unije in zveze NATO, so običajno zelo kratki, zato je komunikacija najpogosteje potekala prek telefona, v obliki avdiokonferenčnega klica ter prek elektronske pošte.

3.2.5 Nacionalne vaje

Strategija kibernetske varnosti predvideva, da bo Republika Slovenija izvajala vaje s področja kibernetske varnosti na nacionalni ravni. Med nalogami urada je bila tudi zadolžitev, da sodeluje pri organizaciji in usklajevanju državne vaje iz kibernetske varnosti ter pri usklajevanju mednarodnih vaj iz kibernetske varnosti. Ugotovili smo, da urad za varovanje tajnih podatkov v obdobju, na katero se nanaša revizija, ni sodeloval pri izvedbi ali izvedel nacionalne vaje s področja kibernetske varnosti. Z ustanovitvijo uprave za informacijsko varnost so se nanjo prenesle tudi naloge, povezane z aktivnostmi za izvajanje nacionalnih vaj s področja kibernetske varnosti.

Ocenjujemo, da je urad za varovanje tajnih podatkov s kadri in viri, ki so mu bili na voljo, izvajal predvsem naloge, ki so se nanašale na mednarodno sodelovanje na vajah kibernetske varnosti in sodelovanje v mednarodnih delovnih telesih in združenjih. Urad za varovanje tajnih podatkov kadrov, ki bi bili ustrezno usposobljeni prav za področje kibernetske varnosti, ni imel. Urad za varovanje tajnih podatkov je podajal različna mnenja o dokumentih, ki so se v tem obdobju pripravljali, in sodeloval pri ozaveščanju prek udeležbe na okroglih mizah in posvetih. Aktivno se je

83 Angl.: *Management Board Thematic Meeting.*

vključil tudi pri pripravi ZKI. Ocenjujemo, da je urad za varovanje tajnih podatkov delno učinkovito izvajal naloge za zagotavljanje kibernetske varnosti.

3.3 Ministrstvo za javno upravo

Odgovor na vprašanje, **ali je ministrstvo učinkovito izvajalo naloge za zagotavljanje kibernetske varnosti,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je ministrstvo:

- pravočasno pripravilo predloge strategije informacijske varnosti oziroma sprememb strategije kibernetske varnosti;
- pravočasno pripravilo podzakonske akte in druge dokumente v skladu z ZInfV;
- izvedlo analizo stanja na področju kibernetske varnosti in v skladu z njo ocenilo potrebe in zagotovilo vire;
- skrbelo za redno izvajanje programov ozaveščanja na področju kibernetske varnosti;
- uvedlo vsebine s področja kibernetske varnosti v sistem izobraževanja in usposabljanja na področju javne uprave;
- spodbujalo razvoj in vpeljavo novih tehnologij na področju kibernetske varnosti;
- sodelovalo v okviru mednarodnih delovnih teles in združenj s področja kibernetske varnosti;
- redno ocenjevalo tveganja za delovanje kritične infrastrukture sektorja informacijsko-komunikacijske podpore na področju javne uprave;
- načrtovalo ustrezne ukrepe za zaščito na podlagi ocen tveganj kibernetske varnosti javne uprave in posodabljalo ocene tveganj na tem področju.

3.3.1 Predlog strategije informacijske varnosti

V skladu z ZInfV bi morala vlada do 11. 5. 2019 sprejeti strategijo informacijske varnosti. Ministrstvo pa bi moralo kot pristojno resorno ministrstvo prej pripraviti predlog strategije informacijske varnosti in ga vladi predložiti v sprejem. Ministrstvo ni pravočasno pripravilo predloga nove strategije informacijske/kibernetske varnosti oziroma predloga sprememb obstoječe strategije kibernetske varnosti (več v točki 2.3.1 tega poročila).

Edini predlog akcijskega načrta za uresničevanje strategije kibernetske varnosti skupaj z oceno potrebnih virov je MIZŠ 12. 5. 2016 posredovalo strateškemu svetu, ki pa ga ni potrdil. Zato tudi niso bile izvedene nobene nadaljnje aktivnosti. Strateški svet se je na svoji 10. seji z dne 30. 5. 2016 seznanil s predlogom za vzpostavitev nacionalnega organa za kibernetsko varnost in ga potrdil. Seznanil se je z okvirno oceno potrebnih virov za uresničevanje strategije kibernetske varnosti in tudi z dejstvom, da ni mogoče zagotoviti predlaganih potrebnih virov. Strateški svet je zato predlagal:

- radikalno okrepitev omenjenega področja;
- pripravo operativnega programa konsolidacije človeških virov z imeni in priimki identificiranih oseb v državni upravi, ki imajo znanja na tem področju;
- preverjanje možnosti sodelovanja s slovenskimi sistemskimi integratorji;
- okrepitev SI-CERT, ki se v tem trenutku nahaja v kritičnem stanju;
- seznanitev vlade s stanjem na tem področju s strani predsednika strateškega sveta;

- pripravo vladnega gradiva, s katerim bo vlada seznanjena s kritičnim stanjem na tem področju s konkretnimi primeri in možnimi posledicami v primeru neukrepanja; pripravo gradiva koordinira ministrstvo – Direktorat za informatiko skupaj z Direktoratom za informacijsko družbo pri MIZŠ in uradom za varovanje tajnih podatkov.

MIZŠ je za podkrepitev izrednega pomena zagotovitve ustrezne ravni kibernetske varnosti pripravilo dokument Potencialni vpliv kibernetskih napadov na gospodarstvo in družbo. MIZŠ kasneje ni pripravilo novega akcijskega načrta oziroma drugega operativnega dokumenta za izvedbo ukrepov za zagotavljanje kibernetske varnosti.

Pojasnilo ministrstva

Akcijski načrt uradno ni bil nikoli potrjen, razlog je bil predvsem v virih, ki so potrebni za uresničitev akcijskega načrta, teh pa ni bilo na razpolago.

Uprava za informacijsko varnost bi kot pristojni nacionalni organ v skladu z zahtevo ZInfV morala začeti delovati najkasneje do 1. 1. 2020. Minister je 15. 4. 2019 sprejel sklep o imenovanju delovne skupine za zagotovitev začetka delovanja uprave za informacijsko varnost, ki je bila vzpostavljena s 1. 7. 2019. Ministrstvo in urad za varovanje tajnih podatkov se v obdobju, na katero se nanaša revizija, še nista dogovorila o prenosu nalog, sredstev, arhivov in dokumentacije, ki se nanašajo na kibernetsko varnost, z urada za varovanje tajnih podatkov na upravo za informacijsko varnost.

Ukrep ministrstva in urada za varovanje tajnih podatkov

Predstavniki uprave za informacijsko varnost in urada za varovanje tajnih podatkov so se 10. 10. 2019 sestali z namenom, da bi primopredaja poslov potekala čim bolj tekoče. Na sestanku so se dogovorili o 4 fazah postopnega prenosa nalog, sredstev, arhivov in dokumentov, ki se nanašajo na informacijsko varnost.

3.3.2 Priprava podzakonskih aktov in drugih aktov poslovanja

ZInfV med drugim določa, da mora minister določiti:

- vsebino in strukturo varnostne dokumentacije;
- metodologijo za pripravo analize obvladovanja tveganj ter metodologijo za določitev ključnih, krmilnih in nadzornih informacijskih sistemov in delov omrežja ter pripadajočih podatkov.

Ministrstvo je z več kot polletno zamudo pripravilo uredbo o določitvi bistvenih storitev, ki je po tem, ko jo je vlada sprejela, začela veljati 22. 6. 2019 (prikazano tudi v tabeli 8). Ministrstvo je v skladu z ZInfV pripravilo pravilnik o varnostni dokumentaciji IBS, ki je začel veljati 1. 6. 2019. Ministrstvo do konca obdobja, na katero se nanaša revizija, še ni pripravilo Pravilnika o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave, je pa po obdobju, na katero se nanaša revizija, izvedlo ukrep, naveden v točki 2.3.2 tega poročila. Na predlog ministrstva je vlada 19. 4. 2018 sprejela uredbo o IVvDU, ki določa roke za izvedbo ukrepov in posredovanje podatkov. Predvideni roki in realizacija aktivnosti v obdobju, na katero se nanaša revizija, so prikazani v tabeli 11.

Tabela 11: Roki in realizacija nalog iz uredbe o IVvDU

Nosilec	Člen	Aktivnost	Rok	Datum realizacije	Zamuda (št. dni)
Vlada	3. (3)	Imenuje odbora za upravljanje informacijske varnosti.	11. 11. 2018[1)]		> 323
Ministrstvo	9. (3)	Objavi metodologijo upravljanja tveganj informacijske varnosti v državni upravi.	11. 11. 2018	20. 12. 2019	404
		Objavi enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi.	11. 11. 2018	22. 5. 2019	192
		Pripravi gradiva za usposabljanje in ozaveščanje na področju informacijske varnosti.	ni roka		
Organi državne uprave	10. (1)	Popišejo informacijsko premoženje in informacijske sisteme v skladu z enotno metodologijo popisovanja informacijskega premoženja in informacijskih sistemov v državni upravi.	11. 5. 2019[1)]		

Opomba: [1)] Še ni bil določen do zaključka obdobja, na katero se nanaša revizija, to je do 30. 9. 2019.

Ministrstvo je aprila 2019 pripravilo tudi navodila za upravljanje z dogodki in incidenti informacijske varnosti (v nadaljevanju: navodila za informacijsko varnost), ki opisujejo proces in postopke z navodili za upravljanje dogodkov in incidentov informacijske varnosti, ki jih v okviru Direktorata za informatiko na ministrstvu izvajata storitveni center in sektor za informacijsko varnost. Ta dokument zelo podrobno opisuje aktivnosti (od zaznave, prijave dogodka in incidenta, evidentiranja in klasificiranja dogodka, odziva in zaključevanja aktivnosti) po prijavi dogodka ali incidenta prek e-pošte ali prek informacijskega sistema Maximo.

Pojasnilo ministrstva

Navodila za informacijsko varnost predstavljajo tudi poslovnik CSIRT organov državne uprave in so objavljena na intranetu ministrstva.

Ocenjujemo, da so navodila za informacijsko varnost zelo podrobna, a namenjena predvsem zaposlenim na ministrstvu in ne celotni državni upravi. CSIRT organov državne uprave je namreč v skladu z ZInfV namenjen vsem organom državne uprave, za katere je med drugim tudi odzivni center. Vendar pa navodila niso dostopna vsem uporabnikom v državni upravi, saj so objavljena le na intranetnih straneh ministrstva.

Priporočilo

Ministrstvu priporočamo, naj prilagodi, posodobi in ustrezno objavi kratka in jasna navodila za upravljanje z dogodki in incidenti informacijske varnosti tako, da bodo uporabna za prijavo kibernetskega incidenta za vse organe državne uprave, ki nimajo svojih operativnih centrov informacijske varnosti in CSIRT. Navodila za informacijsko varnost naj tudi dopolni z navodili za uspešno in učinkovito odpravo težav in navodili, kako uporabljati druge storitve CSIRT organov državne uprave.

Uredba o IVvDU v 1. členu določa, da velja tudi za druge državne organe, organe lokalnih skupnosti, javne agencije in nosilce javnih pooblastil ter druge subjekte, ki se povezujejo s centralnim informacijsko-komunikacijskim sistemom, to je v sistem HKOM. Vendar pa ZInfV ne vključuje vseh subjektov, navedenih v 1. členu uredbe o IVvDU, saj je namenjen le organom državne uprave. S tem pomemben del javne uprave, ki je sicer vključen v sistem HKOM, izključuje iz priglasitve incidentov v CSIRT organov državne uprave in iz uporabe njegovih storitev.

EKC je prek elektronske pošte sicer obveščal in opozarjal tudi nekatere organe javne uprave o pojavu nevarnosti. V primeru ožje nevarnosti je obvestila pošiljal le posameznim organom. Ocenjujemo, da bi za učinkovitejše doseganje višje ravni kibernetske varnosti CSIRT organov državne uprave moral obveščati in opozarjati vse subjekte, ki so povezani v sistem HKOM.

Priporočilo

Ministrstvu priporočamo, naj prouči možnost, da bi storitve CSIRT organov državne uprave lahko uporabljali tudi povezani subjekti, navedeni v 1. členu uredbe o IVvDU.

3.3.3 Analiza stanja na področju kibernetske varnosti in zagotavljanje virov

Ministrstvo je septembra 2018 pripravilo oceno kibernetskih tveganj[84] na podlagi Uredbe o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite[85]. Podatki temeljijo na statistiki incidentov SI-CERT. V oceni niso navedene ocene potreb po kadrovskih virih ter konkretni predlogi posameznih nalog za izboljšanje kibernetske varnosti. Vlada in ministrstvo sta vire načrtovala v predlogu proračunov za leti 2020 in 2021, ki do konca obdobja, na katero se nanaša revizija, tako kot tudi akcijski načrt za področje kibernetske varnosti, še niso bili sprejeti. Ocena potrebnih dodatnih virov za uresničevanje strategije kibernetske varnosti iz leta 2016, ki je bila priloga osnutka akcijskega načrta, je predvidevala, da bo do konca leta 2018 v državnih organih 39 zaposlenih pokrivalo področje kibernetske varnosti, izvedeno naj bi bilo 16 prerazporeditev in 23 novih zaposlitev.

84 Ocena kibernetskih tveganj, št. 842-2/2018/11 z dne 26. 9. 2018, verzija 1.0, [URL: http://mju.arhiv-spletisc.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/ZKibP/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf], 26. 2. 2021.

85 Uradni list RS, št. 62/14 in 13/17.

Ministrstvo naj bi od tega izvedlo 10 prerazporeditev in dobilo 4 nove zaposlene. Načrtovane kadrovske rešitve se niso uresničile.

Pojasnilo ministrstva

Na delovni ravni se je poskušala ocena potrebnih virov vseh deležnikov za izvajanje ukrepov znižati na minimum tako, da so bili ohranjeni samo najnujnejši viri, ki bi jih bilo mogoče zagotoviti za izvajanje strategije kibernetske varnosti in ki bi bili zato namenjeni najnujnejšim aktivnostim – vzpostavitvi pristojnega nacionalnega organa in CSIRT organov državne uprave ter nujne okrepitve SI-CERT. Vendar pa kasneje ni bilo političnega konsenza niti za zagotovitev teh najnujnejših sredstev.

Ministrstvo je junija 2016 pripravilo osnutek gradiva za vzpostavitev nacionalnega organa za kibernetsko varnost in okrepitev nacionalnega sistema kibernetske varnosti, ki je vseboval oceno, da na nacionalnem organu potrebujejo 14 zaposlenih. Vendar pa je bilo v vladno proceduro posredovano gradivo, ki je opredeljevalo samo vzpostavitev nacionalnega organa na uradu za varovanje tajnih podatkov brez dodatnih zaposlitev. Sistemizacija ministrstva se je (v delu, ki se nanaša na Direktorat za informatiko, sektor za informacijsko varnost) v obdobju od začetka leta 2015 do septembra 2017 večkrat spremenila. Sprva je predvidevala 17 delovnih mest na področju kibernetske varnosti, na koncu pa le še 6. Zasedena so bila le 4 delovna mesta.

Naloge na področju informacijske/kibernetske varnosti so se na ministrstvu opravljale v okviru Direktorata za informatiko, sektorja za informacijsko varnost (operativne in upravljavske naloge), in v okviru Direktorata za informacijsko družbo. Delovna mesta s posebej navedenimi nalogami na področju informacijske/kibernetske varnosti v Direktoratu za informacijsko družbo na MIZŠ in kasneje na ministrstvu niso bila sistemizirana, temveč so te naloge opravljali zaposleni poleg ostalih delovnih nalog. V Direktoratu za informatiko na ministrstvu je imel sektor za informacijsko varnost poleg vodje še 2 zaposlena na operativnem področju informacijske varnosti za potrebe operativnega centra informacijske varnosti in 1 zaposlenega na področju upravljanja informacijske varnosti. Ministrstvo ni naredilo analize posledic zmanjšanja števila sistematiziranih delovnih mest. Na ministrstvu ocenjujejo, da so se tveganja informacijske varnosti zaradi tega zmanjšanja bistveno povečala.

Ministrstvo je v predlogu ZIV za zagotovitev pogojev za delovanje pristojnega nacionalnega organa predvidelo 17 dodatnih zaposlitev, za delovanje CSIRT organov državne uprave pa 4 dodatne zaposlitve, vendar do realizacije načrtovanih dodatnih zaposlitev do konca obdobja, na katero se nanaša revizija, še ni prišlo.

S 1. 1. 2019 je v sklopu ministrstva začel delovati CSIRT organov državne uprave, vendar je posloval le v delovnem času ministrstva. Vlada je za potrebe uprave za informacijsko varnost dovoljeno število zaposlenih na ministrstvu povečala za 3 zaposlene. Za to povečanje je moralo ministrstvo zagotoviti sredstva v svojem finančnem načrtu. Vlada je 16. 7. 2019 dala soglasje k aktu o notranji organizaciji, ki ga je pripravila delovna skupina za vzpostavitev uprave za informacijsko varnost na ministrstvu, kar naj bi omogočilo kadrovsko okrepitev CSIRT organov državne uprave. Ministrstvo je ob koncu obdobja, na katero se nanaša revizija, še vedno načrtovalo vključitev kadrov sektorja za informacijsko varnost v sistem pripravljenosti (dežurstva), s čimer naj bi se približalo standardom dosegljivosti in odzivnosti, ki veljajo za mreže CSIRT.

Sektor za informacijsko varnost na ministrstvu je izvajal naslednje naloge s področja informacijske varnosti[86]:

- pregled projektov za izvedbo – pregledal je več kot 70 projektov za izvedbo;
- preverjanje izvorne kode[87] – preveril je 122 programov izvorne kode z namenom preprečevanja varnostnih lukenj in pomanjkljivosti v programski kodi, ki je bila oziroma bo nameščena v državni računalniški oblak[88];
- penetracijsko testiranje[89] – izvedel je 64 penetracijskih testov;
- upravljanje ranljivosti v informacijskih sistemih[90] – spremljal in identificiral je 451 ranljivosti informacijskih sistemov;
- upravljanje in odzivanje na incidente v informacijskih sistemih – identificiral je 551 varnostnih incidentov;
- analiza incidentov v informacijskih sistemih;
- upravljanje z informacijsko varnostjo;
- upravljanje s sistemom vab[91] in
- ozaveščanje in usposabljanje uporabnikov in skrbnikov informacijskih sistemov – izvedel je usposabljanja za 161 uporabnikov ter usposabljanje za 16 skrbnikov informacijskih sistemov.

Ministrstvo je za izvajanje navedenih aktivnosti vključilo tudi zunanje izvajalce. V letu 2016 je sklenilo pogodbo z izvajalcem Viris, varnost in razvoj informacijskih sistemov, d.o.o. (v nadaljevanju Viris), v letu 2017 pa je sklenilo pogodbe z izvajalci Viris, Mikeji, Informacijske Tehnologije, d.o.o. in S&T SLOVENIJA, informacijske rešitve in storitve d.d., ki je pogodbene aktivnosti izvajal skupaj s podizvajalci[92]. Ministrstvo je v letih 2018 in 2019 pogodbo z S&T SLOVENIJA, informacijske rešitve in storitve d.d. letno podaljševalo. Stroški zunanjih izvajalcev operativnega centra informacijske varnosti na ministrstvu so leta 2016 znašali 33.306 EUR, v letu 2017 428.580 EUR, v letu 2018 479.546 EUR ter v letu 2019 (do 30. 9.) 512.722 EUR.

3.3.4 Izvajanje programov ozaveščanja

SI-CERT, ki deluje v okviru javnega zavoda Arnes, izvaja nacionalni program ozaveščanja Varni na internetu in sodeluje v projektu SAFE-SI (od leta 2005). Nacionalni program (projekt) Varni na internetu v celoti financira ministrstvo. Projekt SAFE-SI deluje v okviru projekta Center za varnejši internet, ki ga izvajajo Fakulteta za družbene vede Univerze v Ljubljani, javni zavod Arnes,

86 [URL: http://mju.arhiv-spletisc.gov.si/si/delovna_podrocja/informatika/informacijska_varnost/], 26. 2. 2021.

87 Angl.: *source code review.*

88 [URL: http://mju.arhiv-spletisc.gov.si/si/delovna_podrocja/informatika/drzavni_racunalniski_oblak/], 26. 2. 2021.

89 Angl.: *penetration testing*. Penetracijsko testiranje je testiranje učinkovitosti varovanja računalniškega sistema s simulacijo napadov, [URL: http://www.islovar.org/islovar], 26. 2. 2021.

90 Angl.: *vulnerability management.*

91 Angl.: *honeypot.*

92 IBM SLOVENIJA, Podjetje za proizvodnjo, marketing in storitve, d.o.o.; Unistar LC, zastopstvo, izdelava in vzdrževanje računalniške opreme in računalniških aplikacij d.o.o.; PRO ASTEC podjetje za sistemsko programsko podporo, svetovanje in zastopanje, d.o.o.; HIC SALTA d.o.o., Sistemska integracija in komunikacije, OSI sistemske integracije d.o.o.; Viris in SMART COM d.o.o. informacijski in komunikacijski sistemi.

Zveza prijateljev mladine Slovenije in Zavod MISSS (Mladinsko informativno svetovalno središče Slovenije), financirata pa ga Izvajalska agencija za inovacije in omrežja (INEA) pri Evropski komisiji (prek Instrumenta za povezovanje Evrope) in ministrstvo[93]. Drugih namenskih programov ozaveščanja, ki bi jih financiralo ministrstvo, v obdobju, na katero se nanaša revizija, ni bilo.

3.3.5 Uvedba vsebine s področja kibernetske varnosti v sistem izobraževanja in usposabljanja

Ministrstvo je prejelo pojasnila MIZŠ, da je bila v marcu 2019 objavljena raziskava o uporabi informacijsko-komunikacijske tehnologije v šolah[94], kjer je bilo ugotovljeno, da na nekaterih področjih uporabe informacijsko-komunikacijske tehnologije v Sloveniji nismo najbolj vešči[95]. Ministrstvo je pojasnilo, da se je vključilo v programski svet za informatizacijo izobraževanja pri MIZŠ z namenom, da se vsebine s področja kibernetske varnosti vključijo v obvezne izobraževalne programe na osnovni in srednješolski stopnji. Imenovana je bila delovna skupina za pripravo akcijskega načrta za področje izobraževanja do leta 2027. Programski svet se je v obdobju, na katero se nanaša revizija, sestal le maja 2019, vendar se sestanka predstavniki ministrstva niso udeležili. Na podlagi pregleda načrta izdelave Akcijskega načrta digitalnega izobraževanja 2021–2027 z uporabo inovativnih metod dela smo ugotovili, da področje kibernetske varnosti ni predvideno v novonastajajočih programih.

Ministrstvo je v letu 2018 pripravilo 3 spletne tečaje o informacijski varnosti za zaposlene v sistemu Moodle[96]. Zaradi zapletov v zvezi z obdelavo osebnih podatkov[97] spletni tečaji ob koncu obdobja, na katero se nanaša revizija, še niso bili v uporabi. Ministrstvo tudi še ni določilo časovnice oziroma rokov uvedbe spletnega izobraževanja za druge organe državne uprave.

Ukrep ministrstva

Vsi uslužbenci ministrstva so bili 15. 11. 2019 s sporočilom sekretariata pozvani, da opravijo oziroma obiščejo pripravljene tečaje. Do 16. 12. 2019 se je tečaja ozaveščanja o informacijski varnosti udeležilo 286, tečaja o splošni uredbi o varnosti podatkov pa 208 uslužbencev.

3.3.6 Razvoj in vpeljava novih tehnologij

Ministrstvo se je vključilo v Sekcijo za kibernetsko varnost v okviru Združenja za informatiko in telekomunikacije pri GZS z namenom povezovanja in lažjega sodelovanja z deležniki sistema kibernetske varnosti (javni in zasebni sektor, organizacije RRI[98], univerze). Sekcija za kibernetsko

93 [URL: https://safe.si/center-za-varnejsi-internet/o-centru], 26. 2. 2021.

94 2nd Survey of schools: ICT in Education, Final Report, [URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57894], 26. 2. 2021.

95 Na primer poglavje 1.2. Use (and non-use) of digital technologies.

96 Moodle je odprtokodni sistem za postavitev spletnih učilnic.

97 Mnenje Informacijskega pooblaščenca glede varovanja osebnih podatkov pri usposabljanju zaposlenih in hrambi dnevniških zapisov, št. 0712-3/2018/2645 z dne 24. 12. 2018.

98 Angl.: *Responsible Research and Innovation.*

varnost je kot deležnik sodelovala tudi pri pripravi osnutka ZInfV. V letu 2018 je sekcija pridobila sofinanciranje za projekt CYBER v okviru Interreg Europe. Projekt je razdeljen v 2 fazi, prva faza, ki se je začela 1. 6. 2018, bo trajala 3 leta, druga faza pa nadaljnji 2 leti. V projektu sodeluje 9 partnerjev iz 7 držav. GZS bo v okviru projekta pridobila 151.965 EUR.

Pojasnilo ministrstva

V Sekciji za kibernetsko varnost sodelujejo tudi predstavniki nekaterih državnih organov (na primer Ministrstvo za obrambo, Ministrstvo za notranje zadeve, Policija, urad za varovanje tajnih podatkov in ministrstvo). Ker so sodelujoči tudi iz zasebnega sektorja, izobraževalnih organizacij ter organizacij RRI, sekcija omogoča dobro priložnost za mreženje. Tako stkane povezave so se že izkazale kot koristne pri sodelovanju na nekaterih vajah iz kibernetske varnosti.

Ministrstvo je s pismi podpore podprlo Fakulteto za elektrotehniko, računalništvo in informatiko Univerze v Mariboru ter GZS pri pridobitvi sofinanciranja projektov kibernetske varnosti iz evropskih sredstev. Ministrstvo ni izvajalo drugih aktivnosti, povezanih z razvojem in vpeljavo novih tehnologij.

Pojasnilo ministrstva

Ministrstvo ocenjuje, da bo za razvoj novih tehnologij v prihodnje odgovorna uprava za informacijsko varnost, trenutno pa je to odvisno od posameznih državnih organov. Ministrstvo trenutno koordinira pripravo nacionalne ocene kibernetskih tveganj v omrežjih 5G.

3.3.7 Sodelovanje v mednarodnih delovnih telesih in združenjih

Ministrstvo je sodelovalo pri pripravi in izvedbi kibernetskih vaj Cyber Europe 2016 in 2018. Na vaji Cyber Europe 2016 je bil poudarek na kibernetski varnosti v sektorju ponudnikov dostopa do interneta. V Sloveniji je sodelovalo 10 organov/organizacij s skupaj 14 udeleženci. Na vaji Cyber Europe 2018 je bil poudarek na kibernetski varnosti v letalskem sektorju. V Sloveniji je sodelovalo 12 organov/organizacij s skupaj 24 udeleženci. Ministrstvo je sodelovalo tudi na EU Hybrid Exercise – Multilayer MULTILAYER 2018, NATO Cyber Coalition 2018 in nacionalni kibernetski vaji iz strateškega odločanja 2018 – EDA ter tudi na EU Hybrid Exercise – MULTILAYER 18 (Parallel and Coordinated Exercise) EU HEX-ML18 (PACE), ki je bila vaja kriznega upravljanja in je obsegala incidente z različnih področij ter je bila namenjena preverjanju sodelovanja in odzivanja različnih organov in organizacij. Omenjena vaja iz strateškega odločanja – EDA pa je bila namenjena povečanju zavedanja o pomenu kibernetske varnosti na ravni strateških odločevalcev, izboljšanju kulture kibernetske varnosti ter prek odzivanja na namišljen kibernetski incident tudi preverjanju nacionalnega modela zagotavljanja kibernetske varnosti. Ministrstvo je sodelovalo tudi na vaji NATO CMX 2017, kjer so vadili pripravo ukrepov in odzivanje v kriznih situacijah.

V času priprave in izvedbe vaj Cyber Europe so bili potrebni delovni obiski v Grčiji. Kot predstavniki Republike Slovenije so na delovnih obiskih sodelovali predstavniki SI-CERT, urada za varovanje tajnih podatkov in ministrstva. Pri vajah pa so sodelovali tudi strokovnjaki iz drugih organov in organizacij.

Ministrstvo je sodelovalo z ENISA. Predstavnik ministrstva se je redno udeleževal vaj kibernetske varnosti v okviru Evropske unije in zveze NATO. V preteklosti je funkcijo predstavnika za stike[99] z ENISA opravljal podsekretar/sekretar z MIZŠ, kasneje po potrebi tudi podsekretar z ministrstva. Frekvenca sodelovanja v obliki elektronske izmenjave dokumentov in telefonskih klicev je bila do 3-krat letno. V skupini za pripravo NIS direktive je sodeloval podsekretar/sekretar z MIZŠ. V času nastajanja te direktive je bila frekvenca sodelovanja v obliki sestankov približno na vsaka 2 meseca. Z oddelkom za nacionalne strategije kibernetske varnosti pri ENISA je vseskozi sodeloval podsekretar z MIZŠ oziroma ministrstva. Frekvenca sodelovanja v obliki elektronske izmenjave dokumentov in telefonskih klicev je bila do 3-krat letno. Ministrstvo je v okviru Evropske unije sodelovalo v horizontalni delovni skupini za kibernetska vprašanja.

3.3.8 Ocenjevanje tveganj za delovanje kritične infrastrukture

Ministrstvo je marca 2019 pripravilo osnutek metodologije upravljanja tveganj informacijske varnosti v državni upravi[100], ki pa do konca obdobja, na katero se nanaša revizija, še ni bil sprejet. V okviru priprave osnutka metodologije je ministrstvo preverilo nekaj orodij za upravljanje tveganj, ki ustrezajo pripravljeni metodologiji in podpirajo celoten cikel upravljanja tveganj (med drugimi Silver Bullet RM, Stream, EBIOS, Eramba).

Ukrep ministrstva

Metodologija obvladovanja tveganj informacijske varnosti v državni upravi je bila sprejeta 20. 12. 2019[101].

Ministrstvo je septembra 2018 pripravilo oceno kibernetskih tveganj (več v točki 3.3.3 tega poročila), vendar v njej ni podrobne ocene tveganj delovanja kritične infrastrukture sektorjev informacijske komunikacijske podpore na področju javne uprave. V skladu z oceno bi morala priprava podobnih pregledov in ocen postati stalna praksa pristojnega nacionalnega organa.

CSIRT organov državne uprave, ki je bil vzpostavljen 1. 1. 2019, mora na podlagi ZInfV objavljati opozorila o tveganjih in ranljivostih na področju informacijske varnosti organov državne uprave. V obdobju, na katero se nanaša revizija, je CSIRT organov državne uprave objavil vrsto opozoril in jih posredoval posameznim organom.

3.3.9 Načrtovanje ukrepov na podlagi ocen tveganj

Ministrstvo v obdobju, na katero se nanaša revizija, ni izvedlo analiz ocen tveganja, ni pripravilo in posledično tudi ni objavilo ocen tveganj za delovanje kritične infrastrukture sektorjev informacijske komunikacijske podpore na področju javne uprave. To je bil tudi razlog, da ni načrtovalo ukrepov za

99 Angl.: *liaison officer*.

100 [URL: https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/381178], 26. 2. 2021.

101 [URL: https://www.gov.si/assets/ministrstva/MJU/DI/Informacijska-varnost/Metodologija-obvladovanja-tveganj-informacijske-varnosti-v-drzavni-upravi.pdf], 26. 2. 2021.

zaščito pred kibernetskimi nevarnostmi. ZInfV določa tudi inšpekcijski nadzor nad izvajanjem njegovih določb, ki pa se v obdobju, na katero se nanaša revizija, še ni začel izvajati.

Ukrep ministrstva

Ministrstvo je na podlagi akta o notranji organizaciji uprave za informacijsko varnost predvidelo tudi inšpekcijski nadzor, ki vključuje naloge inšpekcijskega in upravnega nadzora na področju informacijske varnosti, elektronske identifikacije in storitev zaupanja ter dostopnosti spletišč in mobilnih aplikacij, s čimer je zapolnilo delovno mesto vodje inšpekcije. Uprava za informacijsko varnost je tudi sprejela strateške usmeritve in prioritete nadzora za leto 2020.

Ministrstvo ni pravočasno pripravilo predloga strategije informacijske varnosti oziroma sprememb strategije kibernetske varnosti. Prav tako ni pravočasno pripravilo vseh podzakonskih aktov, drugih dokumentov in zadolžitev, opredeljenih v ZInfV. Ministrstvo je izvedlo oceno kibernetskih tveganj, ni pa izvedlo analize stanja na področju kibernetske varnosti in v skladu z njo ocenilo potreb in zagotovilo virov. Ministrstvo ni izkazalo, da je analiziralo posledice zmanjšanja števila sistemiziranih delovnih mest na področju informacijske varnosti s 17 na 6 delovnih mest, vseeno pa ocenjuje, da so se tveganja informacijske varnosti zaradi tega zmanjšanja bistveno povečala. Ocenjujemo, da so se zaradi zmanjšanja predvidenega števila zaposlenih in s tem ohranitve (pre)majhnega števila zaposlenih, ki se ukvarjajo s področjem kibernetske varnosti, tveganja na tem področju bistveno povečala, še posebej, če upoštevamo tudi, da je državna uprava vsako leto bolj digitalizirana ter da število kibernetskih incidentov iz leta v leto skokovito narašča (več v točki 1.2.2 tega poročila). Na podlagi ocen tveganja ministrstvo tudi ni identificiralo (ali realiziralo) posameznih ukrepov za zaščito in dvigovanje odpornosti kibernetske varnosti. V letu 2017 je bilo za uslužbence ministrstva pripravljeno e-izobraževanje za področje informacijske varnosti. S tem ali drugimi programi ozaveščanja na področju ministrstva kot tudi javne uprave pa ministrstvo ni nadaljevalo. Ministrstvo je sodelovalo z GZS in nekaterimi akademskimi ustanovami na področju pridobivanja virov financiranja, a do kakšnih večjih vpeljav tehnologij na področju kibernetske varnosti ni prišlo. Ministrstvo je v letu 2019 sicer pospešilo izvajanje aktivnosti, vendar po naši oceni do konca obdobja, na katero se nanaša revizija, še ni vzpostavilo celovitega sistema, ki bi učinkovito izvajal naloge za zagotavljanje kibernetske varnosti. Ministrstvo je v mednarodnem okviru sodelovalo v delovnih telesih s področja kibernetske varnosti. Ministrstvo ni redno ocenjevalo tveganj za delovanje kritične infrastrukture in na podlagi analiz ni načrtovalo ustreznih ukrepov za zaščito pred kibernetskimi grožnjami. Ocenjujemo, da je ministrstvo delno učinkovito izvajalo naloge za zagotavljanje kibernetske varnosti.

4. Spremljanje izvajanja ukrepov za zagotavljanje kibernetske varnosti

4.1 Vlada Republike Slovenije

Odgovor na vprašanje, **ali je vlada spremljala izvajanje ukrepov za zagotavljanje kibernetske varnosti in jih po potrebi prilagajala,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi (se) je vlada:

- seznanjala s stanjem kibernetske varnosti;
- spremljala napredek na področju kibernetske varnosti;
- glede na stanje in napredek odločala o prilagajanju ukrepov za zagotavljanje kibernetske varnosti.

4.1.1 Seznanjanje s stanjem, spremljanje napredka in prilagajanje ukrepov

Vlada je v letih 2016 in 2017 področje kibernetske varnosti spremljala le v okviru svoje vloge pri sprejemanju ključnih dokumentov na tem področju, in sicer strategije kibernetske varnosti, ZInfV in podzakonskih aktov. Od jeseni 2018 pa je vlada aktivnosti na področju kibernetske varnosti izvajala in spremljala v skladu z navodili SSNAV.

Pojasnilo vlade

Sprejeti sklepi SSNAV predstavljajo pristojnim organom vodilo za delo oziroma delovni akcijski načrt. Sprejem akcijskega načrta trenutno ni aktualen, bo pa sprejet skupaj oziroma po sprejemu nove strategije v letu 2020, ki bo začrtala aktivnosti za prihodnje obdobje.

Vlada je ukrepe za zagotavljanje kibernetske varnosti, med drugimi vzpostavitev uprave za informacijsko varnost, soglasje k aktu o notranji organizaciji, sistemizacija delovnih mest na upravi za informacijsko varnost in zagotovitev virov, sprejela na podlagi predlogov urada za varovanje tajnih podatkov, ministrstva in poročanja OS SSNAV.

Vlada je izvajanje ukrepov za zagotavljanje kibernetske varnosti spremljala prek dokumentov, ki sta jih ministrstvo in urad za varovanje tajnih podatkov pripravila za sprejem na vladi, ter prek poročil OS SSNAV. Ocenjujemo, da vlada ni v celoti prilagajala ukrepov za izvajanje kibernetske varnosti glede na informacije, ki jih je prejela. Ugotovili smo namreč, da je vlada večkrat prejela informacije o nezadostnosti virov za zagotavljanje kibernetske varnosti. Ocenjujemo, da bi morala vlada glede na to, da akcijski načrt na podlagi strategije kibernetske varnosti ni bil sprejet in da prav tako niso bila sprejeta druga operativna navodila za področje kibernetske varnosti, zagotoviti jasne pisne usmeritve za področje kibernetske varnosti, ki bi zajemale vsaj aktivnosti, nosilce in časovnico za najnujnejše ter prioritetne naloge, ki jih je treba izvesti do sprejema nove strategije informacijske varnosti. Vlada je v lastnih dokumentih in dokumentih, ki sta jih pripravila ministrstvo ter urad za varovanje tajnih podatkov, ugotovila, da je stanje na področju kibernetske varnosti nezadovoljivo ter da bo treba veliko vložiti tako v kadre kot v tehnologijo. Vlada bi zato morala zagotoviti, da bi bili

podzakonski akti in dokumenti, ki jih je bilo treba sprejeti na podlagi ZInfV, sprejeti pravočasno. Prav tako bi morala vlada že ob sprejemu strategije kibernetske varnosti zagotoviti tudi vire za njeno izvajanje. Ocenjujemo, da se je vlada na različne načine seznanjala s stanjem in spremljala področje kibernetske varnosti, vendar pa ni vedno sprejela ustreznih ukrepov za nujno potrebno prilagajanje aktivnosti.

4.2 Urad Vlade Republike Slovenije za varovanje tajnih podatkov

Odgovor na vprašanje, **ali je urad za varovanje tajnih podatkov spremljal izvajanje ukrepov za zagotavljanje kibernetske varnosti in jih po potrebi prilagajal,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je urad za varovanje tajnih podatkov:

- spremljal delovanje sistema informacijske varnosti;
- spremljal pripravo in izvajanje strategije informacijske varnosti oziroma sprememb strategije kibernetske varnosti.

4.2.1 Spremljanje delovanja sistema

Urad za varovanje tajnih podatkov je spremljal področje kibernetske varnosti v Republiki Sloveniji in o stanju poročal OS SSNAV in SSNAV. Prav tako je svoje ugotovitve o stanju na področju kibernetske varnosti v obliki poročil letno posredoval Evropski komisiji in zvezi NATO. Urad za varovanje tajnih podatkov ni poročal o incidentih, ki bi lahko imeli večji medpodročni vpliv oziroma ki bi lahko ob daljšem trajanju povzročili slabšanje stabilnosti nacionalne varnosti Republike Slovenije, saj takšnih incidentov nihče ni priglasil. To je tudi razlog, da urad za varovanje tajnih podatkov o incidentih s področja kibernetske varnosti ni obveščal Policije oziroma Nacionalnega centra za krizno upravljanje.

Urad za varovanje tajnih podatkov je vsebino s področja kibernetske varnosti spremljal tudi s pomočjo komunikacije s predstavniki Republike Slovenije v Bruslju in se medresorsko usklajeval z deležniki v Republiki Sloveniji. Urad za varovanje tajnih podatkov je bil tudi član medresorske delovne skupine za evropske zadeve, v okviru katere je tedensko s predstavniki Republike Slovenije v Bruslju prek videokonferenčne povezave usklajeval odprta vprašanja.

4.2.2 Spremljanje priprave in izvajanja strategije informacijske varnosti

Urad za varovanje tajnih podatkov ni spremljal priprave in izvajanja strategije informacijske oziroma sprememb strategije kibernetske varnosti, saj ministrstvo strategije informacijske varnosti v obdobju, na katero se nanaša revizija, ni pripravilo in posredovalo v sprejem vladi, prav tako tudi ni pripravilo morebitnih sprememb strategije kibernetske varnosti. Urad za varovanje tajnih podatkov je v vlogi pristojnega nacionalnega organa na področju kibernetske varnosti deloval le kratko obdobje, v katerem so se aktivnosti šele vzpostavljale, zato je bilo spremljanje področja omejeno predvsem na poročanje vladi oziroma njenim delovnim telesom ter na poročanje

mednarodnim institucijam. Urad za varovanje tajnih podatkov je pojasnil, da aktivnosti ni prilagajal, saj zato še niso bili vzpostavljeni pogoji.

Urad za varovanje tajnih podatkov je redno spremljal in poročal o izvajanju aktivnosti in stanju na področju kibernetske varnosti. Pojasnil je, da je bil zaradi omejene kadrovske zasedbe zelo omejen pri izvajanju aktivnosti, ki mu jih je naložila vlada in ki jih je izvajal tudi v prehodnem obdobju v skladu z ZInfV. Ocenjujemo, da je urad za varovanje tajnih podatkov, kolikor so mu to omogočali viri, ki jih je imel na razpolago, spremljal področje kibernetske varnosti in o njem tudi redno poročal vladi oziroma njenim delovnim telesom. Urad za varovanje tajnih podatkov zaradi zamude vlade in ministrstva pri pripravi in sprejemu strategije informacijske varnosti ni mogel sodelovati, je pa sodeloval pri pripravi drugih dokumentov s področja kibernetske varnosti, ki so bili pripravljeni oziroma sprejeti (na primer ReSNV-2, ZKI in drugi podzakonski akti). Urad za varovanje tajnih podatkov v obdobju, na katero se nanaša revizija, ni poročal o morebitnih kibernetskih incidentih pri izvajalcih bistvenih storitev, saj jih vlada ni pravočasno določila.

4.3 Ministrstvo za javno upravo

Odgovor na vprašanje, **ali je ministrstvo spremljalo izvajanje ukrepov za zagotavljanje kibernetske varnosti in jih po potrebi prilagajalo,** smo pridobili na podlagi naslednjih sodil, v skladu s katerimi je ministrstvo:

- spremljalo zagotavljanje pogojev in izvajanje nalog na področju kibernetske varnosti v skladu z ZInfV in njegovimi podzakonskimi predpisi;
- prilagajalo ukrepe na področju zagotavljanja kibernetske varnosti glede na analize spremljanja zagotavljanja kibernetske varnosti.

4.3.1 Spremljanje zagotavljanja pogojev in izvajanja nalog

Ministrstvo je spremljalo zagotavljanje pogojev in izvajanje nalog na področju kibernetske varnosti tako, da je implementiralo direktivo NIS s pripravo ZInfV ter pripravilo strategijo kibernetske varnosti. V letu 2019 pa je bilo aktivno pri ustanavljanju uprave za informacijsko varnost ter vzpostavitvi CSIRT organov državne uprave. Ministrstvo je tudi spremljalo posamezne segmente področja kibernetske varnosti tako, da je spremljalo zakonodajo, ki je na ravni Evropske unije urejala posamezne segmente kibernetske varnosti. Glede na to, da je bila decembra 2018 sprejeta Direktiva o Evropskem zakoniku o elektronskih komunikacijah[102], je z namenom njene implementacije ministrstvo začelo s pripravo osnutka novega Zakona o elektronskih komunikacijah. V tem okviru je bila pozornost namenjena tudi ureditvi varnosti omrežij in storitev, pri čemer naj bi bila ponovno pretehtana tudi ustreznost rešitev glede poročanja operaterjev o incidentih. V septembru 2018 je ministrstvo izdalo oceno kibernetskih tveganj, kjer so opisani tudi 3 primeri kibernetskih napadov, od katerih sta bila 2 prisotna tudi v Sloveniji, in sicer kibernetski napad Anonymous v letu 2012 in kibernetski napad WannaCry

[102] UL L št. 321 z dne 17. 12. 2018, str. 36.

v letu 2017. Ministrstvo je v okviru operativnega središča za informacijsko varnost z zunanjimi izvajalci med drugim:

- pregledovalo projekte za izvedbo, a poročil o pregledih ni izdelalo;
- preverilo 122 programov izvorne kode z namenom preprečevanja varnostnih lukenj in pomanjkljivosti v programski kodi, ki je bila oziroma bo nameščena v državni računalniški oblak;
- izvedlo 64 penetracijskih testov;
- spremljalo in identificiralo 451 ranljivosti informacijskih sistemov;
- od vzpostavitve CSIRT organov državne uprave identificiralo 551 varnostnih incidentov;
- v 3 letih in pol izvedlo usposabljanja za 161 uporabnikov ter usposabljanje za 16 skrbnikov informacijskih sistemov.

Zaradi zamud pri določitvi izvajalcev bistvenih storitev in organov državne uprave v skladu s podzakonskimi akti kakor tudi zaradi dejstva, da do konca obdobja, na katero se nanaša revizija, še niso pretekli vsi roki za izpolnjevanje obveznosti, ministrstvo ni moglo izvajati nadzora. Prav tako ministrstvo ni prejelo informacij, da ponudniki digitalnih storitev niso izpolnjevali svojih obveznosti, zato tudi ni moglo ukrepati.

Služba za notranjo revizijo na ministrstvu še ni izvedla notranjega revizijskega pregleda, ki bi se nanašal na področje kibernetske varnosti.

Pojasnilo ministrstva

Služba za notranjo revizijo na ministrstvu je v letu 2019 izvedla redni notranji revizijski pregled upravljanja z identitetami in dostopi do aplikacij na ministrstvu.

Priporočilo

Ker izvedeni notranji revizijski pregled ni pokrival področja kibernetske varnosti, temveč širše področje informacijske varnosti, ministrstvu priporočamo, naj služba za notranjo revizijo pregleda aktivnosti izvajanja procesov zaščite in varnosti in preveri njihovo skladnost z internimi akti na področju kibernetske varnosti.

4.3.2 Prilagajanje ukrepov

Ministrstvo je konec leta 2018 pripravilo oceno kibernetskih tveganj. V obdobju, na katero se nanaša revizija, ministrstvo še ni izvedlo analize spremljanja zagotavljanja kibernetske varnosti, s katero bi identificiralo nove ukrepe, jih vpeljalo in spremljajo njihovo izvajanje. Ker ministrstvo ni vpeljalo novih ukrepov na podlagi predhodno izvedene analize, jih tudi ni prilagajalo.

Zaradi neizvedene analize spremljanja zagotavljanja kibernetske varnosti ministrstvo ni moglo pripraviti in izvajati ukrepov za dvigovanje kibernetske odpornosti niti jih ni moglo spremljati in prilagajati. Ocenjujemo, da ministrstvo ni bilo učinkovito pri pripravi, izvajanju in prilagajanju ukrepov za dvigovanje kibernetske odpornosti.

5. Mnenje

Revizijo smo izvedli, da bi izrekli mnenje o učinkovitosti **Vlade Republike Slovenije** (vlada), **Urada Vlade Republike Slovenije za varovanje tajnih podatkov** (urad za varovanje tajnih podatkov) ter **Ministrstva za javno upravo** (ministrstvo) pri zagotavljanju kibernetske varnosti v Republiki Sloveniji v obdobju od 1. 1. 2016 do 30. 9. 2019.

Da bi lahko izrekli mnenje o učinkovitosti revidirancev, smo si zastavili glavno revizijsko vprašanje, **kako Republika Slovenija zagotavlja kibernetsko varnost.** Odgovor na glavno vprašanje smo pridobili z odgovori na naslednja revizijska podvprašanja: ali sta vlada in ministrstvo vzpostavila in zagotovila pogoje za zagotavljanje kibernetske varnosti; ali so revidiranci učinkovito izvajali naloge za zagotavljanje kibernetske varnosti ter ali so revidiranci spremljali izvajanje ukrepov za zagotavljanje kibernetske varnosti in jih po potrebi prilagajali.

Vlada je februarja 2016 sprejela Strategijo kibernetske varnosti – vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti (strategija kibernetske varnosti), v aprilu 2018 pa Zakon o informacijski varnosti (ZInfV) in s tem v pravni red Republike Slovenije prenesla Direktivo (EU) 2016/1148/ES Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji. Vlada bi morala v skladu z ZInfV v roku 1 leta sprejeti strategijo informacijske varnosti oziroma sprejeti spremembe in dopolnitve strategije kibernetske varnosti, vendar tega ni storila. Vlada je določila seznam bistvenih storitev in določila metodologijo za določitev izvajalcev bistvenih storitev z več kot 7-mesečno zamudo. Prav tako do konca obdobja, na katero se nanaša revizija, ni določila izvajalcev bistvenih storitev, za kar je med drugim prejela tudi opomin Evropske komisije. Vlada tudi ni določila organov državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti. Kljub temu da je vlada strategijo kibernetske varnosti sprejela že na začetku leta 2016 in s sklepom urad za varovanje tajnih podatkov pooblastila za izvajanje nalog s področja kibernetske varnosti, pa ni sprejela akcijskega načrta oziroma drugega operativnega dokumenta za izvedbo ukrepov za zagotavljanje kibernetske varnosti. Prav tako bi morala vlada že ob sprejemu strategije kibernetske varnosti zagotoviti tudi vire za njeno izvajanje, česar pa ni storila. Vlada je v letu 2019 zagotovila pogoje za ustanovitev obeh v ZInfV predvidenih organov, vendar pa ni opravila analize potreb po kadrovski in tehnološki okrepitvi. Poleg tega tudi ni pravočasno zagotovila zadostnih sredstev za kadrovsko in tehnološko okrepitev na področju kibernetske varnosti ter ni vzpostavila kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novovzpostavljenih organov. V letu 2019 je vlada pospešila aktivnosti za vzpostavitev Uprave Republike Slovenije za informacijsko varnost in jo ustanovila že nekaj mesecev pred v ZInfV predvidenim rokom. Vlada ni uvedla novih programov ozaveščanja na področju kibernetske varnosti in tudi ni uvedla vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja. Vlada je v letu 2018 vzpostavila projekt, imenovan Tajni državni računalniški oblak, ni pa vpeljala drugih tehnoloških novosti za dvig kibernetske odpornosti. Vlada je zagotavljala pogoje za sodelovanje slovenskih strokovnjakov v mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti. Seznanjala se je s stanjem kibernetske varnosti ob sprejemanju dokumentov s tega področja, od jeseni 2018 pa tudi prek Operativne skupine sekretariata Sveta za nacionalno varnost in sekretariata Sveta za nacionalno varnost.

Urad za varovanje tajnih podatkov je v skladu s sklepom vlade področje kibernetske varnosti opredelil v okviru svoje organizacije, vendar pa je zaradi kadrovske in finančne podhranjenosti aktivnosti izvajal le v omejenem obsegu. Urad za varovanje tajnih podatkov je aktivno sodeloval na mednarodnih vajah s področja kibernetske varnosti in v okviru mednarodnih delovnih teles in združenj s področja kibernetske varnosti, vendar pa zaradi pomanjkanja virov ni izvedel nobene nacionalne vaje s področja kibernetske varnosti. Urad za varovanje tajnih podatkov je po januarju 2019 od Nacionalnega odzivnega centra za kibernetsko varnost in skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave (CSIRT organov državne uprave) začel prejemati informacije o incidentih na področju kibernetske varnosti. Urad za varovanje tajnih podatkov je o stanju na kibernetskem področju redno seznanjal Operativno skupino sekretariata Sveta za nacionalno varnost in sekretariat Sveta za nacionalno varnost. Urad za varovanje tajnih podatkov ni spremljal priprave in izvajanja strategije informacijske varnosti, saj ni bilo aktivnosti ministrstva na tem področju.

Ministrstvo je pripravilo in z večmesečno zamudo sprejelo Pravilnik o varnostni dokumentaciji in varnostnih ukrepih izvajalcev bistvenih storitev. Pravilnik o varnostni dokumentaciji in varnostnih ukrepih organov državne uprave je ministrstvo sprejelo z 12,5 mesečno zamudo. Ministrstvo ni pripravilo predloga strategije informacijske varnosti, katere sprejem je predvideval ZInfV, oziroma ni ugotovilo, ali bi bilo treba obstoječo strategijo kibernetske varnosti zaradi novosprejete zakonodaje posodobiti ali spremeniti. Ministrstvo je izvedlo oceno kibernetskih tveganj, ni pa izvedlo analize stanja na področju kibernetske varnosti, na podlagi katere bi ocenilo potrebe in zagotovilo ustrezne vire. Ministrstvo tudi ni poskrbelo za izvajanje programov ozaveščanja na področju kibernetske varnosti, zagotavljalo pa je vire za delovanje nacionalnega centra SI-CERT ter pripravilo interne tečaje za informacijsko varnost. Ministrstvo je sodelovalo z Gospodarsko zbornico Slovenije pri mednarodnih projektih in s priporočilnimi pismi podprlo nekaj akademskih projektov. Ministrstvo je pravočasno vzpostavilo CSIRT organov državne uprave. Sodelovalo je na mednarodnih vajah s področja kibernetske varnosti, prav tako je sodelovalo v okviru mednarodnih delovnih teles in združenj s področja kibernetske varnosti. Ministrstvo ni celovito spremljalo zagotavljanja pogojev in izvajanja nalog na področju kibernetske varnosti v skladu z ZInfV, saj izvajalci bistvenih storitev niso bili določeni. Ministrstvo je pripravilo oceno kibernetskih tveganj na podlagi Uredbe o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite. V oceni niso podane ocene potreb kadrovskih virov ter konkretni predlogi posameznih nalog za izboljšanje kibernetske varnosti. Ministrstvo ni prilagajalo ukrepov na področju zagotavljanja kibernetske varnosti, ki bi jih pripravilo na podlagi analize spremljanja zagotavljanja kibernetske varnosti.

Na podlagi navedenih ugotovitev menimo, da zagotavljanje kibernetske varnosti v obdobju od 1. 1. 2016 do 30. 9. 2019 kljub pospešenim aktivnostim v letu 2019 **ni bilo učinkovito.**

6. Zahteva za predložitev odzivnega poročila

Vlada Republike Slovenije in **Ministrstvo za javno upravo** morata v roku 90 dni po prejemu revizijskega poročila predložiti računskemu sodišču odzivno poročilo.

Odzivno poročilo mora vsebovati:

- navedbo revizije, na katero se nanaša,
- kratek opis nesmotrnosti v poslovanju, ki so bile razkrite z revizijo, in
- izkaz popravljalnih ukrepov.

Izkaz popravljalnih ukrepov mora obsegati navedbo popravljalnih ukrepov in ustrezna dokazila o izvedenih popravljalnih ukrepih za odpravo ugotovljenih nesmotrnosti.

Vlada Republike Slovenije mora v odzivnem poročilu izkazati, da je:

1. preverila, kakšne so potrebe po rednem oziroma dodatnem izvajanju programov ozaveščanja s področja kibernetske varnosti, in pripravila načrt aktivnosti za izvajanje programov ozaveščanja, v katerem bo določila aktivnosti, nosilce in roke za izvedbo potrebnih aktivnosti – točka 3.1.4;
2. pripravila načrt aktivnosti za sprejem nove strategije informacijske/kibernetske varnosti ali spremembe in dopolnitve strategije kibernetske varnosti, v katerem bo določila aktivnosti, nosilce in roke za izvedbo potrebnih aktivnosti – točka 3.3.1;
3. preverila, kakšne so potrebe po uvajanju vsebin s področja kibernetske varnosti, in pripravila načrt aktivnosti za vpeljavo vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja, v katerem bo določila aktivnosti, nosilce in roke za izvedbo potrebnih aktivnosti – točka 3.3.5.

Ministrstvo za javno upravo mora v odzivnem poročilu izkazati, da:

1. izvaja aktivnosti za finančno in kadrovsko okrepitev Uprave Republike Slovenije za informacijsko varnost v skladu z Aktom o notranji organizaciji in sistemizaciji delovnih mest v Ministrstvu za javno upravo, Upravi Republike Slovenije za informacijsko varnost – točka 2.2.2;
2. je začelo izvajati ocenjevanja tveganj za delovanje kritične infrastrukture sektorjev informacijsko-komunikacijske podpore na področju javne uprave – točka 3.3.8.

Po drugem odstavku 29. člena ZRacS-1 je odzivno poročilo uradna listina, ki jo potrdi odgovorna oseba uporabnika javnih sredstev s svojim podpisom in pečatom.

Računsko sodišče bo ocenilo verodostojnost odzivnega poročila, to je resničnost navedb o popravljalnih ukrepih, in po potrebi opravilo revizijo odzivnega poročila na podlagi četrtega odstavka 29. člena ZRacS-1. Prav tako bo ocenilo zadovoljivost sprejetih popravljalnih ukrepov.

Če odzivno poročilo ne bo predloženo v roku, določenem v tem revizijskem poročilu, stori odgovorna oseba uporabnika javnih sredstev prekršek po tretjem odstavku 38. člena ZRacS-1. Če uporabnik javnih sredstev, ki bi moral predložiti odzivno poročilo, niti v roku 15 dni po izteku roka za

predložitev odzivnega poročila računskemu sodišču ne predloži odzivnega poročila, se šteje, da uporabnik javnih sredstev krši obveznost dobrega poslovanja[103]. Opozarjamo, da se neresnične navedbe v odzivnem poročilu obravnavajo kot neresnične navedbe v uradni listini (drugi odstavek 29. člena ZRacS-1).

Če bo računsko sodišče v porevizijskem postopku ugotovilo, da Vlada Republike Slovenije oziroma Ministrstvo za javno upravo krši obveznost dobrega poslovanja, bo ravnalo v skladu s sedmim do štirinajstim odstavkom 29. člena ZRacS-1.

[103] 3. točka prvega odstavka 37. člena Poslovnika Računskega sodišča Republike Slovenije.

7. Priporočila

Vladi Republike Slovenije priporočamo, naj:

- v pravnih in strokovnih dokumentih jasno definira, poenoti in dosledno uporablja ustrezno terminologijo in pri tem sledi trendom na ravni Evropske unije;
- prouči parametre za posamezno motnjo in incident pri zagotavljanju storitve, ki so navedeni v prilogi k Uredbi o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev, in jih po potrebi prilagodi.

Ministrstvu za javno upravo priporočamo, naj:

- pristojni nacionalni organ pripravi metodologijo za vrednotenje incidentov in navodila, ki bodo vsebovala procese ukrepanja v primeru različnih stopenj incidentov in te procese prične izvajati ob priglasitvi incidentov;
- prilagodi, posodobi in ustrezno objavi kratka in jasna navodila za upravljanje z dogodki in incidenti informacijske varnosti tako, da bodo uporabna za prijavo kibernetskega incidenta za vse organe državne uprave, ki nimajo svojih operativnih centrov informacijske varnosti in odzivnih centrov za kibernetsko varnost; navodila za informacijsko varnost naj tudi dopolni z navodili za uspešno in učinkovito odpravo težav in navodili, kako uporabljati druge storitve skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave;
- prouči možnost, da bi storitve skupine za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij organov državne uprave lahko uporabljali tudi povezani subjekti, navedeni v 1. členu Uredbe o informacijski varnosti v državni upravi;
- služba za notranjo revizijo pregleda aktivnosti izvajanja procesov zaščite in varnosti in preveri njihovo skladnost z internimi akti na področju kibernetske varnosti.

Pravni pouk

Tega poročila na podlagi tretjega odstavka 1. člena ZRacS-1 ni dopustno izpodbijati pred sodišči in drugimi državnimi organi.

Tomaž Vesel,
generalni državni revizor

Poslano:

1. Vladi Republike Slovenije, priporočeno s povratnico;
2. Uradu Vlade Republike Slovenije za varovanje tajnih podatkov, priporočeno;
3. Ministrstvu za javno upravo, priporočeno s povratnico;
4. dr. Miroslavu Cerarju, priporočeno;
5. Marjanu Šarcu, priporočeno;
6. Borisu Moharju, priporočeno;
7. mag. Dobranu Božiču, priporočeno;
8. mag. Nataši Dolenc, priporočeno;
9. Borisu Koprivnikarju, priporočeno;
10. Rudiju Medvedu, priporočeno;
11. Državnemu zboru Republike Slovenije, priporočeno;
12. 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