REPUBLIKA SLOVENIJA
RAČUNSKO SODIŠČE

POREVIZIJSKO POROČILO

Popravljalni ukrepi pri reviziji učinkovitosti zagotavljanja kibernetske varnosti v Republiki Sloveniji

2021

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

POREVIZIJSKO POROČILO

Popravljalni ukrepi pri reviziji učinkovitosti zagotavljanja kibernetske varnosti v Republiki Sloveniji

Številka: 320-2/2019/42
Ljubljana, 14. julija 2021

1. Uvod

V revizijskem poročilu *Učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji*[1], št. 320-2/2019/31 z dne 3. 3. 2021 je Računsko sodišče Republike Slovenije (v nadaljevanju: računsko sodišče) izreklo mnenje, da Vlada Republike Slovenije (v nadaljevanju: vlada), Urad Vlade Republike Slovenije za varovanje tajnih podatkov (v nadaljevanju: urad za varovanje tajnih podatkov) in Ministrstvo za javno upravo (v nadaljevanju: ministrstvo) niso bili učinkoviti pri zagotavljanju kibernetske varnosti.

Ker vse razkrite nesmotrnosti niso bile odpravljene med revizijo, je računsko sodišče v revizijskem poročilu vladi in ministrstvu podalo zahtevo za predložitev odzivnega poročila.

Vlada je odzivno poročilo[2] računskemu sodišču predložila z zamudo. V odzivnem poročilu, ki ga je z varnim elektronskim podpisom potrdila odgovorna oseba mag. Janja Garvas Hočevar, vršilka dolžnosti generalnega sekretarja vlade, so predstavljeni popravljalni ukrepi.

Ministrstvo v predpisanem roku 90 dni odzivnega poročila ni predložilo, zato ga je računsko sodišče pozvalo k predložitvi odzivnega poročila in kasneje še k njegovi dopolnitvi. V odzivnem poročilu in njegovi dopolnitvi[3], ki ju je z varnim elektronskim podpisom potrdila odgovorna oseba Boštjan Koritnik, minister, so predstavljeni popravljalni ukrepi.

V porevizijskem postopku smo pregledali odzivni poročili ter preizkusili verodostojnost in zadovoljivost izkazanih popravljalnih ukrepov.

V tem poročilu:

- predstavljamo nesmotrnosti, ki so bile razkrite v revizijskem poročilu in so zahtevale ukrepanje,
- povzemamo popravljalne ukrepe in
- izrekamo mnenje o zadovoljivosti popravljalnih ukrepov.

1 [URL: https://www.rs-rs.si/revizije-in-revidiranje/arhiv-revizij/revizija/ucinkovitost-zagotavljanja-kibernetske-varnosti-v-republiki-sloveniji-2642/], 13. 7. 2021.

2 Št. 00602-1/2019/43 z dne 3. 6. 2021.

3 Št. 060-8/2019/103 podpisano dne 14. 6. 2021 in št. 060-8/2019/105 podpisano dne 16. 6. 2021.

2. Nesmotrnosti in popravljalni ukrepi

2.1 Vlada Republike Slovenije

2.1.1 Ozaveščanje s področja kibernetske varnosti

2.1.1.1 Opis nesmotrnosti

V točki 3.1.3 revizijskega poročila je navedeno, da SI-CERT[4] že od leta 2011 izvaja program ozaveščanja najširše slovenske javnosti Varni na internetu in sodeluje v programu Safe.si.[5] Oba programa sta se začela izvajati že pred sprejetjem Strategije kibernetske varnosti – vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti[6] (v nadaljevanju: strategija 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.

V točki 3.1.3 revizijskega poročila je navedeno tudi, da so se programi in projekti ozaveščanja izvajali že pred sprejetjem strategije kibernetske varnosti, pa vendar sta tako strategija in predlog Zakona o informacijski varnosti[7] opozorila, da obstaja velika podhranjenost na tem področju. Tudi Evropsko računsko sodišče je v informativnem dokumentu poudarilo, da je Agencija Evropske unije za kibernetsko varnost[8] 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.[9]

Vlada je morala v odzivnem poročilu izkazati, da je preverila, kakšne so potrebe po rednem oziroma dodatnem izvajanju programov ozaveščanja s področja kibernetske varnosti, in pripraviti načrt aktivnosti za izvajanje programov ozaveščanja, v katerem bo določila aktivnosti, nosilce in roke za izvedbo potrebnih aktivnosti.

---

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

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

6 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], 13. 7. 2021.

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

8 Angl.: *European Union Agency for Cybersecurity*.

9 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], 13. 7. 2021.

2.1.1.2 Izkazani popravljalni ukrep

Vlada je v odzivnem poročilu posredovala načrt aktivnosti za izvedbo zahtevanega popravljalnega ukrepa, kar prikazuje Tabela 1, z navedbo nosilca in roka za izvedbo aktivnosti.

Tabela 1: Načrt aktivnosti

Zap. št.	Aktivnost	Nosilec	Rok izvedbe
1	Spremljanje in nadgradnja programov ozaveščanja za javne uslužbence	ministrstvo, Uprava Republike Slovenije za informacijsko varnost (v nadaljevanju: URSIV)	december 2021
2	Uskladitev obstoječih vsebin za ozaveščanje z zahtevami za dostopnost oziroma razvoj novih vsebin za osebe s posebnimi potrebami	URSIV	junij 2022
3	Priprava naprednega izobraževalnega programa za kibernetsko varnost za IKT strokovnjake	URSIV	največ 22 mesecev od potrditve sofinanciranja s strani Javne agencije za raziskovalno dejavnost Republike Slovenije
4	Priprava izobraževalnih vsebin s področja kibernetske varnosti za osnovnošolsko in srednješolsko raven	URSIV	2022–2024
5	Sodelovanje na tekmovanju mladih talentov iz kibernetske varnosti European Cybersecurity Challenge	URSIV	oktober 2021

Vlada je v odzivnem poročilu med drugim navedla oziroma pojasnila, da redno spremlja aktivnosti ozaveščanja programov Varni na internetu pri SI-CERT in Safe.si. Vlada ocenjuje, da obstajata ciljni skupini, ki še nista dovolj naslovljeni s programi ozaveščanja. Gre za skupino starejših uporabnikov spleta in oseb s posebnimi potrebami. Področje ozaveščanja omenjenih dveh skupin bo po napovedi vlade v sodelovanju s pristojnimi ministrstvi naslovljeno tudi v novi strategiji kibernetske varnosti, ki jo pripravlja ministrstvo in bo vključevala akcijski načrt.

Za ciljno skupino javnih uslužbencev, ki v preteklosti tudi ni bila pokrita, je ministrstvo v letu 2020 pripravilo e-usposabljanje Informacijska varnost[10]. Usposabljanje obsega osnove informacijske varnosti, ki naj bi jih obvladoval vsak javni uslužbenec.

Februarja 2021 je bilo med predloge raziskovalnih tem ministrstva v okviru priprave Javnega razpisa Javne agencije za raziskovalno dejavnost Republike Slovenije "Ciljni raziskovalni programi 2021" uvrščeno in tudi zagotovljeno sofinanciranje 3 predlogov s področja kibernetske varnosti, med njimi tudi projekta Program usposabljanja za kibernetsko varnost.[11] Cilj slednjega je priprava naprednega izobraževalnega programa za kibernetsko varnost za IKT strokovnjake v podjetjih in institucijah, ki bi vključeval dejanske potrebe trga. Projekt bo izveden v sodelovanju s Sekcijo za kibernetsko varnost pri Gospodarski zbornici Slovenije, ki združuje deležnike iz javnega in zasebnega sektorja,

10 [URL: https://ua.gov.si/aktivnosti/detajli/?ID=ac505edf-e669-ea11-9c51-005056818ee6&Tag=459], 13. 7. 2021.

11 [URL: https://www.arrs.si/sl/progproj/crp/razpisi/21/razp-crp-21.asp], 13. 7. 2021.

izobraževalnih ter RRI[12] ustanov. Cilj projekta je, da tako pripravljen izobraževalni program kasneje dobi mesto na kateri od slovenskih fakultet. Odločitve o izboru projektov Javna agencija za raziskovalno dejavnost Republike Slovenije še ni sprejela. Prijavitelji bodo o izboru projektov obveščeni predvidoma avgusta 2021.

V Načrt za okrevanje in odpornost[13] je bil umeščen predlog za financiranje priprave izobraževalnih vsebin s področja kibernetske varnosti, ki bi jih vključili v izobraževalne programe na osnovnošolski in srednješolski ravni. Namen je doseči, da bodo omenjene teme del kurikulov že v obveznem osnovnošolskem izobraževanju, kar bi pripomoglo k postopnemu ozaveščanju celotne populacije. Ob uspešni uvedbi vsebin v izobraževalne programe vlada pričakuje tudi multiplikativne učinke medgeneracijskega sodelovanja, ko bi mladi tako pridobljeno znanje širili tudi med svojimi starši in starimi starši. Predlog predvideva vključitev vsebin v izobraževalne programe najkasneje do konca leta 2024, pri čemer bodo sodelovali Ministrstvo za izobraževanje, znanost in šport (v nadaljevanju: MIZŠ), Zavod Republike Slovenije za šolstvo in URSIV.

URSIV je v letu 2021 prvič pristopila k sodelovanju države na tekmovanju mladih talentov med 13. in 26. letom iz kibernetske varnosti European Cybersecurity Challenge, za katero bo organizirala nacionalni izbor tekmovalcev ter zagotovila njihov trening, pripravo in udeležbo na tekmovanju na Češkem.

2.1.1.3 Ocena popravljalnega ukrepa

Izkazani popravljalni ukrep ocenjujemo kot **zadovoljiv.**

2.1.2 Strategija kibernetske varnosti

2.1.2.1 Opis nesmotrnosti

V točki 3.3.1 revizijskega poročila je navedeno, da bi morala vlada v skladu z Zakonom o informacijski varnosti[14] (v nadaljevanju: ZInfV) 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.

Vlada je morala v odzivnem poročilu izkazati, da je 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.

12 Angl.: *Responsible Research and Inovation*.

13 [URL: https://www.eu-skladi.si/sl/po-2020/nacrt-za-okrevanje-in-krepitev-odpornosti], 13. 7. 2021.

14 Uradni list RS, št. 30/18 in 95/21.

2.1.2.2 Izkazani popravljalni ukrep

Vlada je v odzivnem poročilu posredovala načrt aktivnosti za sprejem nove strategije kibernetske varnosti in akcijskega načrta, kar prikazuje Tabela 2, z navedbo nosilca in roka za izvedbo aktivnosti.

Tabela 2: Načrt aktivnosti

Zap. št.	Aktivnost	Nosilec	Rok izvedbe
1	Predstavitev dobrih praks pri implementaciji strategije, primer Estonije	URSIV	maj 2021
2	Pregled strategij kibernetske varnosti primerljivih držav	URSIV	junij 2021
3	Predlog strategije kibernetske varnosti	URSIV	september 2021
4	Predlog akcijskega načrta strategije kibernetske varnosti	URSIV	oktober 2021
5	Sprejem strategije in akcijskega načrta	URSIV	december 2021

Vlada je v odzivnem poročilu navedla oziroma pojasnila, da je 20. 10. 2020 v izvedbi ministrstva potekala delavnica Digitalni izziv – kibernetska varnost, na katero so bili povabljeni deležniki s področja kibernetske varnosti in kjer so bile predstavljene načrtovane aktivnosti v povezavi s pripravo nove strategije kibernetske varnosti. Delavnica je spadala v niz delavnic, organiziranih za različna področja informacijske družbe, ki jih pokriva krovna strategija Digitalna Slovenija. Na osnovi predlogov sodelujočih in pregleda uresničevanja obstoječe strategije kibernetske varnosti je bilo v aprilu 2021 področje kibernetske varnosti s svojim poglavjem vključeno tudi v predlog nove krovne strategije Digitalna Slovenija, ki jo kot nosilec pripravlja ministrstvo.

V okviru URSIV se nadaljujejo aktivnosti za pripravo strategije. Pri tem gre predvsem za pregled novejših strategij primerljivih držav, kamor spada tudi predstavitev dobrih praks pri implementaciji strategije v Estoniji. Delavnico je URSIV v sodelovanju s Sekcijo za kibernetsko varnost pri Gospodarski zbornici Slovenije organizirala v mesecu maju 2021.

Vlada je navedla, da pričakuje, da bo strategija pripravljena in posredovana v potrditev v letu 2021, kar je predvideno tudi v Načrtu za okrevanje in odpornost.

2.1.2.3 Ocena popravljalnega ukrepa

Izkazani popravljalni ukrep ocenjujemo kot **zadovoljiv**.

2.1.3 Kibernetska varnost v sistemu izobraževanja in usposabljanj

2.1.3.1 Opis nesmotrnosti

V točki 3.3.5 revizijskega poročila je navedeno, da je ministrstvo prejelo pojasnila MIZŠ, da je bila v marcu 2019 objavljena raziskava o uporabi informacijsko-komunikacijske tehnologije v šolah[15], kjer je bilo ugotovljeno, da na nekaterih področjih uporabe informacijsko-komunikacijske tehnologije v Sloveniji nismo najbolj vešči[16]. 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.[17] Zaradi zapletov v zvezi z obdelavo osebnih podatkov[18] spletni tečaji ob koncu obdobja, na katero se nanaša revizija, še niso bili v uporabi.

Vlada je morala v odzivnem poročilu izkazati, da je 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.

2.1.3.2 Izkazani popravljalni ukrep

Vlada je v odzivnem poročilu posredovala načrt aktivnosti za vpeljavo vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja, kar prikazuje Tabela 3, z navedbo nosilca in roka za izvedbo aktivnosti.

15 2nd Survey of schools: ICT in Education, Final Report, [URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57894], 13. 7. 2021.

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

17 Moodle je odprtokodni sistem za postavitev spletnih učilnic.

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

Tabela 3: Načrt aktivnosti

Zap. št.	Aktivnost	Nosilec	Rok izvedbe
1	Priprava izhodišč za prenovo učnih načrtov	Zavod Republike Slovenije za šolstvo (v nadaljevanju: ZRSŠ)	december 2021
2	Smiselna umestitev vsebin kibernetske varnosti v prenovljene učne načrte	Strokovne skupine za prenovo učnih načrtov OŠ, SŠ pri ZRSŠ	2022–2024
3	Strokovno izpopolnjevanje vodstvenih in strokovnih delavcev v vrtcih in šolah za uporabniško in tehnično usposobljenost ter spletno varnost	ZRSŠ	od leta 2022 dalje
4	Izobraževanje strokovnih delavcev za organizacijo računalniško informacijske dejavnosti na šoli, vključno s kibernetsko varnostjo	ZRSŠ in fakultete	od leta 2022 dalje
5	Dodatno izpopolnjevanje strokovnih delavcev za organizacijo informacijske dejavnosti na šoli, vključno s kibernetsko varnostjo	ZRSŠ in fakultete	od leta 2022 dalje

Vlada je v odzivnem poročilu navedla oziroma pojasnila, da v Sloveniji obstaja projekt Varni na internetu[19], ki ga izvaja SI-CERT, ki deluje pod okriljem Arnes. SI-CERT predstavlja nacionalno kontaktno točko, ki opravlja posredniško in svetovalno vlogo ter prevzema tudi koordinacijo projekta osveščanja javnosti o informacijski varnosti. Vzporedno se izvaja tudi program Safe.si[20] kot točka osveščanja o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje. Glede na to, da v obstoječih učnih načrtih ni vključena vsebina kibernetske varnosti, ter glede na to, da tehnologija prodira v vse pore družbenega življenja, in glede na podatke iz raziskav o kibernetski varnosti, vlada ocenjuje, da potreba po uvajanju vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja obstaja. Prav tako vlada ocenjuje, da je izražena dovolj velika potreba, da se razišče sistemska rešitev izobraževanja iz temeljnih vsebin kibernetske varnosti vseh udeležencev izobraževanja ter tudi usposabljanja vodstvenih in strokovnih delavcev v vzgojno-izobraževalnih zavodih.

2.1.3.3 Ocena popravljalnega ukrepa

Izkazani popravljalni ukrep ocenjujemo kot **zadovoljiv.**

19 [URL: https://www.varninainternetu.si/], 13. 7. 2021.

20 [URL: https://safe.si/], 13. 7. 2021.

2.2 Ministrstvo za javno upravo

2.2.1 Okrepitev Uprave Republike Slovenije za informacijsko varnost

2.2.1.1 Opis nesmotrnosti

V točki 2.2.2 revizijskega poročila je navedeno, da je vlada 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 v letu 2018 pristojni nacionalni organ 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, ki pa je bil novembra 2019 premeščen na upravo za informacijsko varnost.

Delovna skupina ministrstva 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.

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.

Resolucija o strategiji nacionalne varnosti Republike Slovenije[21] 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.

[21] Uradni list RS, št. 59/19.

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

Ministrstvo je moralo v odzivnem poročilu izkazati izvajanje aktivnosti za finančno in kadrovsko okrepitev URSIV v skladu z aktom o notranji organizaciji.

2.2.1.2 Izkazani popravljalni ukrep

Ministrstvo je v odzivnem poročilu izkazalo, da so bile v URSIV od leta 2020 realizirane 4 zaposlitve za nedoločen čas in 1 zaposlitev za določen čas do konca trajanja projekta Predsedovanje Republike Slovenije Svetu Evropske unije 2021 – z namenom napotitve na delo v Stalnem predstavništvu Republike Slovenije v Bruslju, kamor je bil v tem letu javni uslužbenec tudi napoten. V mesecu maju 2021 je bilo sklenjeno delovno razmerje za določen čas do konca trajanja projekta Predsedovanje Republike Slovenije Svetu Evropske unije 2021. Realizirana je bila tudi zaposlitev 1 javnega uslužbenca za čas nadomeščanja javne uslužbenke.

Ministrstvo v odzivnem poročilu ni izkazalo aktivnosti za finančno okrepitev URSIV.

2.2.1.3 Ocena popravljalnega ukrepa

Izkazani popravljalni ukrep ocenjujemo kot **delno zadovoljiv.**

2.2.2 Ocenjevanja tveganj za delovanje kritične infrastrukture

2.2.2.1 Opis nesmotrnosti

V točki 3.3.8 revizijskega poročila je navedeno, da je ministrstvo marca 2019 pripravilo osnutek metodologije upravljanja tveganj informacijske varnosti v državni upravi[22], 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

Ministrstvo je sprejelo Metodologijo obvladovanja tveganj informacijske varnosti v državni upravi 20. 12. 2019[23].

Ministrstvo je septembra 2018 pripravilo oceno kibernetskih tveganj, vendar v njej ni podrobne ocene tveganj delovanja kritične infrastrukture sektorjev informacijske komunikacijske podpore na

22 [URL: https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/381178], 13. 7. 2021.

23 [URL: https://www.gov.si/assets/ministrstva/MJU/DI/Informacijska-varnost/Metodologija-obvladovanja-tveganj-informacijske-varnosti-v-drzavni-upravi.pdf], 13. 7. 2021.

področju javne uprave. V skladu z oceno bi morala priprava podobnih pregledov in ocen postati stalna praksa pristojnega nacionalnega organa.

Ministrstvo je moralo v odzivnem poročilu izkazati, da je začelo izvajati ocenjevanja tveganj za delovanje kritične infrastrukture sektorjev informacijsko-komunikacijske podpore na področju javne uprave.

2.2.2.2 Izkazani popravljalni ukrep

Ministrstvo je v odzivnem poročilu izkazalo, da je skladno z Zakonom o kritični infrastrukturi[24] (v nadaljevanju: ZKI) v juniju 2020 opravilo oceno tveganj za delovanje kritične infrastrukture HKOM ter opredelilo ukrepe za obvladovanje tveganj. Ocena tveganj[25] je bila opravljena na podlagi sprejete Metodologije ocenjevanja tveganj kritične infrastrukture (HKOM).[26]

Ministrstvo je navedlo, da je ocenjevanje tveganj kritične infrastrukture redna naloga upravljalcev kritične infrastrukture, zato naj bi v juniju 2021 ponovno izvedlo letno oceno tveganj, v kateri bodo tveganja kibernetske varnosti ocenjena z vidika novonastalih groženj, verjetnosti in morebitnih posledic.

2.2.2.3 Ocena popravljalnega ukrepa

Izkazani popravljalni ukrep ocenjujemo kot **zadovoljiv.**

Pri pregledu odzivnega poročila in njegove dopolnitve smo ugotovili, da Metodologija ocenjevanja tveganj kritične infrastrukture (HKOM) odstopa od navodil in usmeritev, ki so jih poleg ministrstva podala pristojna ministrstva na podlagi 12. člena ZKI upravljalcem kritične infrastrukture. V oceni tveganj ni navedenega opisa stanja kritične infrastrukture v razmerah rednega delovanja, opisne analize in ovrednotenja virov tveganj za delovanje kritične infrastrukture v skladu z Navodili za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije.[27]

24 Uradni list RS, št. 75/17.

25 Preglednica v MS Excel, brez oznake verzije in datuma nastanka/posodobitve.

26 Št. 382-42/2017/145, z dne 10. 6. 2020.

27 Uradni list RS, št. 7/19.

3. Mnenje o izkazanih popravljalnih ukrepih

3.1 Mnenje o izkazanih popravljalnih ukrepih Vlade Republike Slovenije

Pregledali smo odzivno poročilo, ki ga je na podlagi zahteve iz revizijskega poročila Učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji izdelala Vlada Republike Slovenije. Ocenili smo, da je odzivno poročilo, ki ga je z varnim elektronskim podpisom potrdila mag. Janja Garvas Hočevar, vršilka dolžnosti generalnega sekretarja vlade, verodostojno.

Zadovoljivost izkazanih popravljalnih ukrepov smo ocenili na podlagi posredovanega opisa ukrepov in dokumentacije. Menimo, da smo pridobili zadostne in ustrezne podlage in dokaze, da lahko podamo oceno o zadovoljivosti izkazanih ukrepov.

Ocenjujemo, da so izkazani ukrepi, opisani v točkah 2.1.1.2, 2.1.2.2 in 2.1.3.2, ki jih je sprejela Vlada Republike Slovenije, **zadovoljivi.**

3.2 Mnenje o izkazanih popravljalnih ukrepih Ministrstva za javno upravo

Pregledali smo odzivno poročilo, ki ga je na podlagi zahteve iz revizijskega poročila Učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji izdelalo Ministrstvo za javno upravo. Ocenili smo, da je odzivno poročilo in njegova dopolnitev, ki ju je z varnim elektronskim podpisom potrdili Boštjan Koritnik, minister, verodostojno.

Zadovoljivost izkazanih popravljalnih ukrepov smo ocenili na podlagi posredovanega opisa ukrepov in dokumentacije. Menimo, da smo pridobili zadostne in ustrezne podlage in dokaze, da lahko podamo oceno o zadovoljivosti izkazanih ukrepov.

Ocenjujemo, da je izkazani popravljalni ukrep, opisan v točki 2.2.1.2, ki ga je sprejelo Ministrstvo za javno upravo, **delno zadovoljiv.**

Ocenjujemo, da je izkazani popravljalni ukrep, opisan v točki 2.2.2.2, ki ga je sprejelo Ministrstvo za javno upravo, **zadovoljiv.**

4. Ovrednotenje nezadovoljivo odpravljenih nesmotrnosti

4.1 Ovrednotenje nezadovoljivo odpravljene nesmotrnosti Ministrstva za javno upravo

Nesmotrnost, opisana v točki 2.2.1.1, za katero Ministrstvo za javno upravo ni izkazalo v celoti zadovoljivih popravljalnih ukrepov, se nanaša na aktivnosti za okrepitev Uprave Republike Slovenije za informacijsko varnost v skladu z aktom o sistematizaciji, pri čemer ni izkazalo aktivnosti za finančno okrepitev Uprave Republike Slovenije za informacijsko varnost.

Nesmotrnost, ki ni bila v celoti zadovoljivo odpravljena, ne presega pomembnosti, ki je bila upoštevana v reviziji.

5. Sklep o kršitvi obveznosti dobrega poslovanja

Ministrstvo javno upravo v odzivnem poročilu ni izkazalo v celoti zadovoljivega popravljalnega ukrepa za odpravo nesmotrnosti, opisanega v točki 2.2.1.2.

S tem je Ministrstvo za javno upravo v skladu z določbami petega odstavka 29. člena Zakona o računskem sodišču[28] in prvega odstavka 37. člena Poslovnika Računskega sodišča Republike Slovenije[29] kršilo obveznost dobrega poslovanja.

Tomaž Vesel,
generalni državni revizor

Poslano:

1. Vladi Republike Slovenije, priporočeno;
2. Ministrstvu za javno upravo, priporočeno;
3. Državnemu zboru Republike Slovenije, priporočeno;
4. arhivu.

28 Uradni list RS, 11/01 in 109/12.

29 Uradni list RS, 91/01.

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