Povzetek revizijskega poročila Učinkovitost zagotavljanja kibernetske varnosti v Republiki Sloveniji

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.

Ljubljana, 3. marca 2021