Povzetek revizijskega poročila
Učinkovitost upravljanja kibernetske varnosti za področje kritične infrastrukture v ELES

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

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

ELES je zaznavanje kibernetskih groženj izvajal učinkovito, in sicer z različnimi dokumentiranimi aktivnostmi, imel je opredeljene vloge in odgovornosti za odkrivanje varnostnih dogodkov ter je izvajal različne aktivnosti odkrivanja. ELES je imel vpeljane postopke posredovanja informacij o odkritih dogodkih, prav tako pa je nenehno izboljševal postopke zaznavanja in ustvarjal različne zbirke znanja, povezane z varnostnimi dogodki. ELES je pri upravljanju odzivanja na kibernetske grožnje uporabljal načrt odzivanja. Zaposleni so bili usposobljeni za odzivanje ter so poročali o dogodkih in posredovali informacije o dogodkih prejemnikom tako znotraj kot tudi izven ELES. Z nekaterimi organizacijami so imeli vpeljano prostovoljno izmenjavo informacij o incidentih. ELES je upravljanje odzivanja izvajal tudi z analiziranjem obvestil ter razumevanjem vpliva incidentov na organizacijo kakor tudi z razvrščanjem incidentov. ELES je imel vpeljane procese za spremljanje, analize in odzivanje na ranljivosti kakor tudi za omejevanje in blažitev incidentov. ELES ni imel posebne strategije za področje kibernetske varnosti, je pa imel vzpostavljene politike za vse segmente integriranega sistema upravljanja, ki so se prek vodstvenega pregleda redno pregledovale in ustrezno dopolnjevale. ELES ima še možnosti za izboljšave, ki se jih zaveda in jih tudi uvaja.

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

Ljubljana, 23. avgusta 2021