INFORMACIJA O POTREBI HITNOG OBEZBJEĐIVANJA ADEKVATNIH PROSTORNIH KAPACITETA ZA AGENCIJU ZA SAJBER BEZBJEDNOST RADI USPOSTAVLJANJA PUNE OPERATIVNE SPREMNOSTI

Na sjednici Savjeta Agencije za sajber bezbjednost održanoj 25.02.2026. godine usvojena je informacija kojom je direktor Agencije za sajber bezbjednost zadužen da, u saradnji sa Ministarstvom javne uprave, pripremi informaciju za Vladu Crne Gore radi hitnog rješavanja pitanja prostornih kapaciteta za službenike Agencije. Potreba za hitnim postupanjem proizilazi iz zakonskih obaveza Agencije, obaveza iz Reformske agende Crne Gore 2024–2027, kao i iz činjenice da bez adekvatnog prostora nije moguće uspostaviti punu operativnu funkciju Agencije u traženom roku.

Polazeći od Zakona o informacionoj bezbjednosti, pitanje smještaja Agencije nije pitanje standardnog administrativnog prostora, već pitanje ispunjavanja uslova za zakonito i efikasno vršenje poslova iz oblasti sajber bezbjednosti. Zakon uspostavlja sistem upravljanja sajber prijetnjama, incidentima i sajber krizama, uz jasno definisanu međuinstitucionalnu koordinaciju i operativno postupanje. U tom smislu, zakonski okvir neposredno podrazumijeva obavezu obezbjeđivanja prostora koji omogućava fizičku, tehničku i organizacionu zaštitu, kontrolisan pristup, kontinuitet rada i bezbjednu obradu informacija. Ujedno, Zakon propisuje da se sredstva za rad Agencije obezbjeđuju u budžetu Crne Gore, a da Agencija mora ispunjavati tehničke i druge uslove propisane zakonom. Konkretno, član 60 Zakona propisuje da Agencija mora da ispunjava tehničke i druge uslove iz člana 39 stav 2 Zakona, što potvrđuje da su tehničko-infrastrukturni uslovi rada zakonska obaveza, a ne stvar organizacione procjene.

Posebno je važno istaći zakonsku obavezu operativne saradnje Agencije sa državnim strukturama nadležnim za reagovanje na incidente. Zakon o informacionoj bezbjednosti u odredbama koje uređuju postupanje kod incidenata visokog nivoa i sajber krize propisuje međusobno obavještavanje i zajedničko učešće Agencije i Vladinog bezbjednosno operativnog centra GOSC-a u rješavanju incidenata (član 34), kao i dalje koordinisano postupanje u slučaju sajber krize (član 35), dok član 38 stav 1 tačka 8 propisuje saradnju sa Agencijom radi razmjene informacija o sajber prijetnjama, ozbiljnim sajber prijetnjama i incidentima i rješavanja tih prijetnji, incidenata i sajber krize. U operativnom smislu, ova saradnja se danas neposredno reflektuje i kroz saradnju sa Vladinim bezbjednosno-operativnim centrom GSOC, što dodatno uslovljava zahtjev za prostornom blizinom radi efikasne koordinacije, razmjene informacija i brze reakcije.

U odnosu na reformske obaveze, Reformskom agendom Crne Gore 2024–2027, u okviru reforme 2.4.4 „Cybersecurity - Setting up a comprehensive framework for cyber resilience (introducing requirements of NIS2 Directive and strengthening relevant institutions)“, kao jedan od ključnih koraka definisan je indikator pod tačnim nazivom: **„Establishment of a competent authority and list of entities. The Cybersecurity Agency (acting as competent authority as defined in the NIS2) is operational: sufficiently staffed, equipped with supervisory powers, performing supervisory checks. List of entities in scope of the national law corresponding to the NIS2 Directive is finalized“**, sa rokom realizacije decembar 2025. godine u Reformskog agendi, odnosno kao referentni reformski indikator za operativnost Agencije. Ovaj indikator je suštinski vezan za dokazivu operativnu funkcionalnost Agencije (kadrovski, nadzorno i organizaciono), što objektivno nije moguće bez obezbijeđenih prostornih kapaciteta i adekvatnih tehničkih uslova rada.

REFORMSKA AGENDA

U kontekstu realizacije Reformske agende, hitnost obezbjeđivanja prostora dodatno je pojačana činjenicom da se u martu očekuje posjeta review misije Evropske komisije, te da su od Agencije za sajber bezbjednost i Ministarstva javne uprave već tražene aktivnosti na ispunjavanju uslova za punu operativnu funkciju Agencije, uključujući organizacione i planske pretpostavke (plan rada i plan nadzora), kao i demonstriranje realnih kapaciteta za sprovođenje nadzornih i operativnih funkcija. Takođe, u samoj Reformskoj agendi reforma 2.4.4 i pripadajući koraci izričito vezuju operativnost Agencije za izvršavanje nadzornih provjera i funkciju nadležnog organa u smislu NIS2 okvira.

U tom smislu, ispunjenje indikatora koji se odnosi na operativnost Agencije predstavlja osnov za povlačenje sredstava po Reformskog agendi u skladu sa finansijskim prilozima i aneksima koji prate sprovođenje reformskih koraka, pri čemu se finansijska realizacija veže za dokazivo ispunjenje kvalitativnih i kvantitativnih koraka. Istovremeno, prateći dokumenti za sprovođenje Facility mehanizma naglašavaju potrebu dostavljanja dokaza da je sistem/usluga uspostavljen i operativan, što dodatno potvrđuje da se pitanje prostora mora riješiti bez odlaganja kako bi se obezbijedila puna upotrebljivost kapaciteta Agencije.

Pored normativnog i reformskog aspekta, postoje i jasna tehnička ograničenja koja uslovljavaju izbor lokacije. Imajući u vidu da se data centar nalazi u prostorijama u zgradi „Vektre“, izbor prostora za rad Agencije objektivno mora biti ograničen na radijus do 1 km od navedene lokacije. Ovaj uslov ne predstavlja administrativno opredjeljenje, već proizilazi iz potrebe za operativnom efikasnošću, logističkom održivošću, brzim tehničkim intervencijama, pouzdanim održavanjem povezanosti, minimizovanjem rizika po kontinuitet rada i obezbjeđivanjem stabilnog funkcionisanja u uslovima pojačane operativne dinamike.

Dodatno, činjenica da se Vladin bezbjednosno-operativni centar GSOC nalazi u Atlas Capital Centru dodatno potvrđuje opravdanost i nužnost prostornog ograničenja u istom radijusu, budući da takva lokacijska blizina neposredno utiče na brzinu reakcije, kvalitet koordinacije i efikasnost zajedničkog operativnog postupanja u obradi prijetnji, incidenata i kriznih situacija. Imajući u vidu zakonom propisanu intenzivnu saradnju i zajedničko postupanje, predmetni radijus predstavlja objektivno uslovljen bezbjednosno operativni kriterijum, a ne fakultativni element izbora lokacije.

Prostor koji se obezbjeđuje za potrebe Agencije mora, pored uslova lokacije, ispunjavati i posebne funkcionalne, tehničke i bezbjednosne zahtjeve koji proizilaze iz prirode poslova, zakonskih nadležnosti i međunarodno prihvaćenih standarda dobre prakse u oblasti sajber bezbjednosti i upravljanja informacionom bezbjednošću. To podrazumijeva da prostor mora omogućiti organizaciju rada u jasno razdvojenim bezbjednosnim cjelinama (zone sa različitim režimima pristupa), uz mogućnost uspostavljanja kontrolisanog ulaza i izlaza, fizičkog odvajanja administrativnih, operativnih i tehničkih funkcija, prostora sa ograničenim pristupom za obradu osjetljivih informacija, prostorija za koordinaciju i odgovor na incidente, kao i prostora za sastanke i međuinstitucionalnu saradnju.

Posebno se ukazuje da prostor mora imati adekvatnu mrežnu i telekomunikacionu infrastrukturu, uključujući optički pristup, kao i mogućnost uspostavljanja redundantnog linka radi obezbjeđivanja kontinuiteta rada i otpornosti komunikacionih veza. Ovaj zahtjev proizilazi iz operativne prirode posla, potrebe za neprekidnim pristupom sistemima i brze razmjene podataka u postupanjima po incidentima i prijetnjama, kao i iz principa kontinuiteta poslovanja i otpornosti koji su sastavni dio savremenih okvira sajber bezbjednosti.

Takođe, prostor mora raspolagati kapacitetima za sprovođenje edukacija i koordinacionih aktivnosti sa subjektima od posebnog značaja, uključujući subjekte kritične infrastrukture, imajući u vidu nadzornu, koordinacionu i preventivnu ulogu Agencije u sistemu nacionalne sajber bezbjednosti. Bez obezbjeđivanja ovakvih prostornih uslova, Agencija ne može u punom obimu ostvariti funkciju institucionalne podrške, nadzora, koordinacije i podizanja spremnosti relevantnih subjekata.

Navedeni zahtjevi usklađeni su i sa međunarodno prihvaćenim standardima i okvirima. Standardi ISO/IEC 27001 i ISO/IEC 27002 insistiraju na upravljanju rizicima, fizičkoj bezbjednosti, kontroli pristupa, zaštiti opreme i sigurnim operativnim uslovima, dok ISO 22301 (kontinuitet poslovanja) dodatno potvrđuje potrebu za infrastrukturnom pouzdanošću i planiranjem kontinuiteta rada. NIS2 pristup, na kojem je zasnovan reformski okvir, polazi od institucionalne spremnosti, koordinacije i sposobnosti nadležnih organa da efektivno vrše nadzor i reagovanje, što podrazumijeva realno funkcionalan i bezbjednosno adekvatan prostor.

Analizom tržišta poslovnih prostora na lokacijama koje zadovoljavaju navedene uslove (radijus do 1 km, tehničko-infrastrukturni kriterijumi, mogućnost organizacije bezbjednosnih cjelina i potrebna funkcionalnost prostora), utvrđeno je da se cijena zakupa kreće u rasponu do 24 eura po m². Imajući u vidu potrebu budžetske racionalnosti, predlaže se da se aktivnosti usmjere na pronalaženje prostora po cijeni zakupa do visine od 20 eura po m², uz ispunjenje svih navedenih tehničkih, funkcionalnih i bezbjednosnih uslova. Ograničenje cijene ne smije dovesti do ugrožavanja minimuma uslova potrebnih za zakonit i operativno održiv rad Agencije.

Imajući u vidu zakonske obaveze, reformske rokove, tehnička ograničenja lokacije, potrebu bliske operativne saradnje sa Vladinim bezbjednosno-operativnim centrom GSOC, kao i objektivnu neophodnost uspostavljanja bezbjednosnih cjelina i pouzdane komunikacione infrastrukture (optički pristup i redundantni link), proizilazi da je hitno obezbjeđivanje adekvatnih prostornih kapaciteta neposredan preduslov za uspostavljanje pune operativne spremnosti Agencije za sajber bezbjednost. Dalje odlaganje rješavanja ovog pitanja predstavlja institucionalni i operativni rizik, jer umanjuje vrijeme potrebno za adaptaciju, tehničko opremanje, uspostavljanje bezbjednosnih režima, organizaciju rada i dokazivanje pune funkcionalnosti Agencije u skladu sa zakonskim i reformskim obavezama.