INFORMACIJA

o potpisivanju Ugovora o zakupu poslovnog prostora, namijenjenog za rad Vladinog bezbjednosno operativnog centra (GSOC)

UVOD

U skladu sa Reformski definisanim obavezama iz oblasti sajber bezbjednosti i informacionih tehnologija, Ministarstvo javne uprave podnosi ovu informaciju s ciljem iniciranja postupka produženja zakupa poslovnog prostora koji koristi Vladin centar za bezbjednosne operacije (G-SOC), čiji aktuelni zakup **ističe 1. avgusta 2025. godine.**

G-SOC predstavlja centralni tehničko-operativni mehanizam za 24/7 praćenje i odgovor na sajber prijetnje u okviru državne informaciono-komunikacione infrastrukture. Njegov značaj posebno dolazi do izražaja u kontekstu sve učestalijih i sofisticiranijih sajber incidenata, te potrebe za jačanjem digitalne otpornosti države u skladu sa evropskom NIS2 direktivom i Zakonom o informacionoj bezbjednosti.

Strateški značaj G-SOC-a u kontekstu reformske agende

Osnivanje Vladinog centra za bezbjednosne operacije (G-SOC) predstavlja neposrednu realizaciju mjere 2.4.4. Reformske agende Crne Gore, kojom je predviđeno uspostavljanje sveobuhvatnog i funkcionalnog nacionalnog sistema sajber otpornosti. Ova mjera uključuje harmonizaciju zakonodavnog okvira sa Direktivom NIS2 Evropske unije, unapređenje institucionalne strukture, kao i sistemsko jačanje tehničkih i kadrovskih kapaciteta tijela nadležnih za sajber bezbjednost.

G-SOC je operativno jezgro Vladinog CIRT-a, uspostavljeno radi nadzora, prevencije, detekcije i odgovora na sajber prijetnje koje se odnose na državne informacione sisteme. U okviru sprovođenja reformskih aktivnosti, G-SOC je već prepoznat kao ključna komponenta digitalne bezbjednosne arhitekture.

Stručna analiza sprovedena u okviru međunarodnih projekata tehničke pomoći – realizovanih uz podršku Vlade Ujedinjenog Kraljevstva i Evropske unije – pokazala je da je za efikasan i održiv rad G-SOC-a i Vladinog CIRT-a neophodno obezbijediti minimalno 34 stalno angažovanih visoko kvalifikovanih stručnjaka, uz tehnički stabilnu, zaštićenu i profesionalno opremljenu infrastrukturu u skladu sa međunarodnim normama i bezbjednosnim standardima.

Do sada, G-SOC je uspješno uspostavio ključne funkcionalnosti, uključujući:

- Mehanizme za detekciju, analizu i odgovor na sajber incidente u realnom vremenu;
- Operativnu saradnju sa međunarodnim partnerima i CIRT tijelima iz regiona;

- Kontinuirani nadzor nad digitalnim servisima državne uprave, sa fokusom na zaštitu podataka i infrastrukture od visokorizičnih sajber prijetnji.

Funkcionisanje G-SOC-a direktno je vezano za ispunjavanje jasno definisanih pokazatelja uspješnosti iz Reformske agende. Njegova operativna održivost i kadrovska stabilnost predstavljaju preduslov za povlačenje značajnih finansijskih sredstava iz instrumenata podrške Evropske unije.

U tom smislu, posebno se ističe da je za oblast digitalne transformacije i sajber bezbjednosti, u okviru Plana rasta Evropske unije za Zapadni Balkan, za 2025. godinu opredijeljeno ukupno **9.268.742,40 eura** za Crnu Goru. Korišćenje ovih sredstava uslovljeno je postojanjem funkcionalnih institucija, operativnih kapaciteta i sprovođenjem reformskih mjera definisanih nacionalnim i međunarodnim dokumentima.

Ukoliko bi se ugrozio kontinuitet rada G-SOC-a, odnosno ukoliko ne bi bila obezbijeđena njegova operativna stabilnost – uključujući tehničku infrastrukturu, prostor i stručne resurse – Crna Gora bi mogla ostati uskraćena za korišćenje ovih finansijskih sredstava, što bi imalo direktne negativne posljedice po ukupnu realizaciju digitalnih reformi.

Shodno tome, unapređenje G-SOC-a nije samo tehničko-operativna potreba, već strateška obaveza u okviru Reformske agende, čije ispunjavanje ima neposredan uticaj na finansijsku održivost planiranih aktivnosti i kredibilitet Crne Gore u procesu evropskih integracija.

Prostorni kapaciteti i značaj lokacije

Prostor koji trenutno koristi Vladin centar za bezbjednosne operacije (G-SOC) predstavlja tehnički i infrastrukturno optimizovano okruženje koje je u potpunosti prilagođeno zahtjevima rada visoko specijalizovanih sajber timova u režimu 24/7 operativnog nadzora. Riječ je o prostoru koji je prethodno, uz finansijsku i tehničku podršku međunarodnih partnera, temeljno adaptiran i opremljen u skladu sa najvišim bezbjednosnim, tehničkim i infrastrukturnim standardima koji se primjenjuju u radu savremenih centara za upravljanje sajber bezbjednošću.

Posebno je značajno istaći da se navedene prostorije (Atlas Capital) nalaze u neposrednoj blizini Data centra Ministarstva javne uprave, čime se ostvaruje višestruka strateška prednost:

- Blizina Data centra omogućava G-SOC-u brz i siguran pristup ključnim sistemima i servisima u vlasništvu države.
- Zahvaljujući fizičkoj blizini i direktnoj mrežnoj povezanosti, tehnički timovi mogu intervenisati u realnom vremenu, bez oslanjanja na udaljene konekcije ili vanjske resurse, čime se obezbjeđuje visok stepen otpornosti na sajber napade i brzi oporavak u slučaju incidenata;
- Infrastruktura u prostoru je konfigurisana za rad sa visokom dostupnošću, uz primjenu sigurnosno izolovanih kanala, enkripcije podataka i fizičke kontrole

pristupa, čime se garantuje integritet i kontinuitet u radu informaciono-komunikacionih servisa od posebnog značaja.
- Prostor je već opremljen redundantnim napajanjem, UPS sistemom što predstavlja osnovni tehnički uslov za nesmetan rad servera, mrežnih komponenti i ostale visokospecijalizovane opreme.

Zbog kompleksnosti postojeće tehničke infrastrukture – uključujući sofisticirane nadzorne sisteme, mrežne uređaje visoke propusnosti, centralizovane sigurnosne platforme i specijalizovane radne stanice – eventualna migracija G-SOC-a u alternativni prostor bi podrazumijevala:

- Višemjesečne tehničke pripreme, uključujući ponovno projektovanje sistema, planiranje selidbe, testiranje i konfiguraciju nove lokacije;
- Značajne sigurnosne i operativne rizike, jer bi tokom faze migracije došlo do prekida u praćenju, analizi i odgovoru na sajber prijetnje, što otvara prostor za potencijalne napade ili gubitak podataka;
- Visoke finansijske izdatke, jer bi izmještanje opreme zahtijevalo nova ulaganja u infrastrukturu, kabliranje, klimatizaciju, energetske instalacije, fizičku bezbjednost i redundantne sisteme;
- Privremenu ili djelimičnu obustavu nadzora nad ključnim digitalnim servisima, uključujući one koji podržavaju funkcionisanje javne uprave, zdravstva, poreske uprave, sistema socijalne zaštite i drugih institucija koje osiguravaju stabilnost državnih funkcija.

U kontekstu navedenog, jasno je da lokacija koju trenutno koristi G-SOC nije samo tehnički pogodna, već strateški nezamjenjiva u pogledu čuvanja kontinuiteta rada i realizacije ključnih obaveza iz oblasti sajber bezbjednosti. Svaki pokušaj preseljenja nosio bi visok nivo operativne, pravne i reputacione neizvjesnosti, te bi bio direktno suprotan principima efikasnog i bezbjednog upravljanja kritičnom informaciono-komunikacionom infrastrukturom.

Dosadašnje finansiranje i potreba za preuzimanjem obaveza od strane države

Zakup poslovnog prostora do sada je u potpunosti bio finansiran kroz donatorske aranžmane, prije svega iz sredstava Evropske unije. Imajući u vidu završetak finansijske pomoći u avgustu 2025. godine, neophodno je da država preuzme finansiranje troškova zakupa i održavanja prostora putem budžetskih sredstava Ministarstva javne uprave.

U Budžetu za 2025. godinu već su planirana sredstva za ovu namjenu, a dalja neizvjesnost u vezi zakupa može direktno ugroziti kontinuitet rada G-SOC-a i realizaciju međunarodno prepoznatih obaveza iz oblasti sajber bezbjednosti.

Posljedice eventualnog prekida zakupa

Ukoliko se zakup ne produži, posljedice bi bile višestruko negativne, uključujući:

- Prekid rada G-SOC-a, odnosno suspenziju mehanizma za odgovor na sajber prijetnje;

- Diskontinuitet u nadzoru i upravljanju sigurnosno-kritičnim sistemima;
- Gubitak pristupa fondovima EU usljed neispunjavanja operativnih uslova;
- Odlaganje realizacije planiranih reformskih i infrastrukturnih projekata za najmanje godinu dana;
- Povećani rizik od sajber napada i kompromitacije informaciono-komunikacione infrastrukture.