INFORMACIJA O PRIJEDLOGU AKTIVNOSTI KOJE JE NEOPHODNO PREDUZETI U ORGANIMA DRŽAVNE UPRAVE U CILJU PODIZANJA SAJBER BEZBJEDNOSTI NA VEĆI NIVO

Vlada Crne Gore je na sjednici održanoj 29. decembra 2021. godine donijela novu, treću po redu, Strategiju sajber bezbjednosti Crne Gore za period 2022-2026 godine. Tokom izrade Strategije uzeta su obzir prethodna iskustva i izazovi sa kojim se Crna Gora susretala u sajber domenu, kao i preporuke, najbolje prakse i globalni bezbjednosni izazovi, sa posebnim osvrtom na hibridne prijetnje koje se u velikoj mjeri kanališu kroz sajber prostor i koje ugrožavaju ili mogu ugroziti različite aktere, od državnih institucija, privatnog sektora, prije svih banaka i internet servis provajdera, pa do samih pojedinaca.

Većina ključnih aktera, odnosno zainteresovane strane koje kreiraju strategije, politike i viziju razvoja sajber bezbjednosti u Crnoj Gori, saglasni su da su u prethodnom periodu najveći izazovi bili ljudski i organizacioni resursi. Ovi resursi predstavljaju osnov za sprovođenje strateških ciljeva, zakona, standarda, operativnih i tehničkih procedura i koordinaciju na nacionalnom i međunarodnom nivou.

Sa druge strane, posljednjih nekoliko godina privatni i javni sektor su izdvajali u određenoj mjeri finansijska sredstva za nabavku i primjenu savremenih tehnoloških rješenja u cilju adekvatne zaštite informacionih sistema od sajber prijetnji, odnosno umanjenja nivoa sajber rizika. Međutim, tehnološka rješenja za zaštitu informacionih sistema, kritične infrastrukture od sve prisutnijih sajber prijetnji, nijesu sama po sebi nikad dovoljna, pogotovo ukoliko njima ne upravljaju dobro obučeni sajber eksperti ili timovi, koji su dio organizacija sposobnih da obavljaju zadatke u okviru svojih nadležnosti. Takođe, moramo biti svjesni da je covid pandemija ostavila traga, kako na mogućnost izdvajanja sredstava za nabavku tehničke opreme, tako i na nivo obuka koje su organizovane u manjoj mjeri i u online formatu. Stoga bi bilo neophodno intenzivirati obuke IT kadrova, kako po pitanju sajber bezbjednosti, tako i svih drugih obuka iz oblasti IT-a.

Savjet za informacionu bezbjednost (Savjet), koji je između ostalog zadužen za monitoring implementacije Akcionog plana (AP) Strategije, ukazuje na neophodnost da se u što kraćem roku realizuju aktivnosti iz AP i druge ad-hoc mjere, kako bi svi akteri bili sposobni da odgovore trenutnim i budućim izazovima. Naime, AP Strategije definisane su aktivnosti u pravcu formiranja Agencije za sajber bezbjednost (Agencija), koja će predstavljati krovno tijelo po pitanju sajber i informacione bezbjednosti na nacionalnom nivou. Agencija bi trebalo da otkloni organizacijske prepreke i obezbijedi dovoljan nivo autoriteta za sprovođenje strategija, politika i operativnih zadataka, što sada nije slučaj, s obzirom na činjenicu da su premještanjem CIRT-a iz MJUDDM u Direkciju za zaštitu tajnih podataka (DZTP), mehanizmi zaštite ostali kao dio informatičke infrastrukture MJUDDM, a ljudski resursi su postali dio DZTP. U tom smislu, a kako je predviđeno AP Strategije, potrebno je u što kraćem roku pristupiti izmjenama i dopunama Zakona o informacionoj bezbjednosti i podzakonskih akata, Zakona o tajnosti podataka i Uredbe organizaciji i načinu rada državne uprave, čime bi u 2022. godini bio stvoren formalni preduslov za uspostavljanje Agencije, koje je planirano za 2023. godinu.

Kao jedan od modela prevazilaženja nedostatka resursa za prevenciju sajber prijetnji u institucijama koje su odgovorne za zaštitu kritičnih informacionih sistema državnih organa i saradnju sa zainteresovanim stranama (privatni sektor, akademska zajednica i međunarodni partneri), nameće se model združivanja operativnih, tehničkih i ljudskih kapaciteta, što bi povećalo nivo sposobnosti za odgovore na sajber incidente i optimizovalo potrošnju finansijskih sredstava. Ovakav model saradnje, između ostalog je od koristi i za CIRT, koji usljed nedostatka resursa ne može odgovoriti svim zadacima. Stoga, AP Strategije sajber

bezbjednosti predviđeno je formiranje Interresornog operativnog tima, sastavljenog od predstavnika relevantnih državnih institucija. Operativni tim bi imao zadatak da, u vremenu globalne bezbjednosne krize koja može uticati na Crnu Goru kao članicu NATO i permanentno prisutnih sajber napada na mrežu državnih organa i njene servise, u slučaju incidentnih situacija bude tehnička podrška CIRT-u i Savjetu za informacionu bezbjednost u cilju obezbjeđivanja optimalnih mehanizama za odgovore na sajber incidente i umanjenje sajber opasnosti i rizika. Dodatno, ohrabruju se institucije koje upravljaju informaciono-komunikacionim sistemima da u saradnji sa CIRT-om ulože dodatne preventivne napore u dijelu edukacije krajnjih korisnika, kao jednom od najefikasnijih mjera sajber bezbjednosti.

U cilju motivacije državnih službenika koji su odgovorni za informaciono-komunikacione sisteme, informacionu i sajber bezbjednost, potrebno je pronaći održivi model povećanja zarada. Na ovaj način, povećaće se efikasnost IT i sajber stručnjaka, smanjiti zavisnost od eksternih ugovarača i otvoriti vrata za priliv novih talenata i stručnjaka iz privatnog sektora. Takođe, jedan od modela motivacije službenika je i organizovanje kvalitetnih obuka IT kadra po pitanju informacione i sajber bezbjednosti koja je u svijetu vrlo aktuelna. Tako obučen kadar bi se uslovio ugovorima na 3-4 godine obaveznog rada u državnom organu nakon plaćenih obuka.

S obzirom na to da su procjena i registar rizika neophodni mehanizmi pripreme strategije odbrane od sajber napada na nivou države, neophodno je da sva ministarstva u sklopu Registra rizika procijene rizike za informacione sisteme i rade njihovu reviziju na godišnjem nivou, u skladu sa legislativom.

Kroz iskustva u radu Savjeta može se uočiti da se sajber incidenti ne prijavljuju relevantnim institucijama. Profesionalno je prijaviti incident jer svi mogu biti žrtve sajber napada.

Visokim procentom realizacije Strategije, uz dodatne programe edukacije, koji će izmedju ostalog biti ponudjeni i kroz program koji Vlada Francuske planira da ponudi regionu kroz Regionalni centar za obuke iz oblasti sajber bezbjednosti, Crna Gora bi trebalo da stvori održivi model sajber otpornosti na svim nivoima. Riječ je o centru koji će biti ishod Sajber Balkan projekta Francuskog centra za ekspertizu bezbjednosti u Jugoistočnoj Evropi, koji je iniciralo francusko Ministarstvo za Evropu i vanjske poslove. S tim u vezi, potpisano je pismo namjere između Univerziteta Crne Gore i Vlade Crne Gore u kojem je iskazana spremnost i želja Vladi Francuske da Regionalni centar za borbu protiv sajber kriminala i za sajber bezbjednost bude u Crnoj Gori.

Cijeli svijet, pa i Crna Gora, se nalazi na putu digitalizacije i virtuelizacije, pa se iz tog razloga mora posvetiti posebna pažnja zaštiti digitalnih servisa, koji pružajući usluge i koristeći lične podatke, preko kojih se vrši razmjena osjetljivih podataka, obavljaju finansijske transakcije i slično. U tom smislu, sajber bezbjednost još više dobija na značaju, a neminovno je očekivati da će zlonamjerni akteri iskoristiti sve ranjivosti sistema, kako bi ostvarili dobit, vršili ucjene ili došli u posjed informacija.

Shodno navedenim dešavanjima, kao i trenutnoj bezbjednosnoj krizi, evidentan je povećan intenzitet sajber napada, te je stoga Savjet za informacionu bezbjednost, dao preporuke da se intenzivira realizacija aktivnosti iz Akcionog plana Strategije, kao i da se preduzmu određeni koraci kako bi svi akteri bili spremniji da odgovore na prijetnje i izazove.

S tim u vezi, na posljednoj sjednici Savjet za informacionu bezbjednost donio je sljedeće preporuke:

1. Direkcija za zaštitu tajnih podataka, u skladu sa AP za implementaciju Strategije sajber bezbjednosti 2022-2026, ažurira listu lokalnih CIRT timova i dostavi članovima Savjeta podatke o imenovanim kontakt osobama iz organa državne uprave;
2. Direkcija za zaštitu tajnih podataka u saradnji sa Ministarstvom javne uprave, digitalnog društva i medija pripremi materijale za obuke iz oblasti sajber bezbjednosti sa pratećim uputstvima do kraja aprila 2022. godine;
3. Direkcija za zaštitu tajnih podataka pripremi predlog realizacije prve sajber vježbe do naredne sjednice Savjeta;
4. Agencija za elektronske komunikacije i poštansku djelatnost, do naredne sjednice Savjeta, dostavi svim članovima informaciju o problemima koje postoje u rješavanju zahtjeva organa državne uprave prema telekomunikacionim operatorima, kako bi se povećao nivo operabilnosti i bezbjednosti;
5. Ministarstvo javne uprave, digitalnog društva i medija formira interesorni operativni tim za podršku u rješavanju sajber incidenata u skladu sa AP za implementaciju Strategije sajber bezbjednosti 2022-2026, do 20. aprila 2022 godine.