Od virtualne države do obrane u praksi

portal DOT | 7 svibnja, 2026

Hrvatska prvi put na najvećoj NATO-ovoj kibernetičkoj vježbi

Sudjelovanje Hrvatske na najvećoj NATO-ovoj kibernetičkoj vježbi Locked Shields važan je pokazatelj sazrijevanja nacionalnog pristupa kibernetičkoj sigurnosti. Riječ je o vježbi koja ne testira samo tehničku spremnost timova, nego i sposobnost koordinacije, donošenja odluka pod pritiskom, upravljanja kriznom komunikacijom te suradnje između različitih institucija i stručnjaka.

Digitalne usluge danas čine temelj svakodnevice: od obrazovanja i zdravstva do javne uprave, financijskih usluga i komunikacijskih platformi. Upravo zato svaka vježba koja simulira realne napade i testira obrambene mehanizme ima izravnu vrijednost za sigurnost građana i institucija.

Kibernetička sigurnost kao pitanje javnog interesa

U praksi, kibernetički napadi rijetko pogađaju samo jedan sustav. Često se šire na više povezanih servisa, prekidaju dostupnost podataka, usporavaju rad institucija i stvaraju dodatni pritisak na timove koji moraju reagirati u vrlo kratkom vremenu. Zbog toga su vježbe poput Locked Shields važne ne samo za vojni i sigurnosni sektor, nego i za cijeli ekosustav koji održava digitalne javne usluge. One omogućuju provjeru procedura, komunikacijskih kanala i razine pripravnosti svih uključenih dionika.

Posebna vrijednost ovakvih vježbi leži u tome što se ne testira izolirana tehnička obrana, nego ukupna sposobnost sustava da izdrži složen, višeslojni napad. To uključuje obranu mrežne infrastrukture, rad servisa, zaštitu podataka, koordinaciju između operativnih timova i upravljačke razine te pravodobno informiranje relevantnih tijela. U takvim okolnostima postaje jasno da je kibernetička sigurnost istodobno tehničko, organizacijsko i strateško pitanje.

Hrvatski pristup u tom kontekstu pokazuje važnost povezivanja institucija koje imaju različite uloge, ali zajednički cilj: zaštititi ključne digitalne sustave. Upravo zato su sudjelovanje CARNET-a, Nacionalnog CERT-a i drugih stručnjaka iz javnog i privatnog sektora važni elementi šireg sigurnosnog modela.

Uloga CARNET-a i Nacionalnog CERT-a

CARNET i Nacionalni CERT imaju posebnu ulogu u jačanju kibernetičke otpornosti u Hrvatskoj jer djeluju na sjecištu tehnologije, obrazovanja, prevencije i operativne sigurnosti.

U kontekstu vježbe Locked Shields razgovarali smo s Jakovom Kišem iz CARNET-a o tome kako iskustva stečena u takvom okruženju doprinose jačanju zaštite e-usluga koje građani svakodnevno koriste.

“Sudjelovanje u međunarodnoj kibernetičkoj vježbi Locked Shields pruža Nacionalnom CERT-u praktično iskustvo koje jača vještine i poboljšava procese u slučaju kibernetičkog napada. Simuliranjem realističnih kibernetičkih incidenata, naši stručnjaci mogu uvježbavati postupke odgovora, identificirati nedostatke i poboljšati koordinaciju prije nego što dođe do stvarnog napada. Osim u tehničkoj skupini, naši stručnjaci sudjelovali su u radu skupine za krizno komuniciranje i skupine za strateško odlučivanje. Tako je vježba obuhvatila najvažnije aspekte pripreme i odgovora u slučaju kibernetičke krize.”

Suradnja javnog i privatnog sektora

Jedna od najvažnijih poruka koju ovakve vježbe šalju jest da se kibernetička sigurnost ne može učinkovito graditi bez partnerstva javnog i privatnog sektora. U kriznim situacijama, osobito pri

velikim i koordiniranim napadima, potrebno je brzo okupljanje različitih vrsta stručnosti: od analitičara i inženjera do administratora sustava, pravnih i komunikacijskih stručnjaka te osoba koje mogu donositi odluke u realnom vremenu. Upravo zato sudjelovanje 135 stručnjaka u hrvatskom timu nije samo broj, nego pokazatelj načina na koji se gradi otpornost.

O važnosti takve suradnje, osobito u kriznim situacijama koje zahtijevaju brzo okupljanje različitih profila stručnjaka, više nam je rekao Jakov Kiš:

"Suradnja između javnog sektora i privatnih IT stručnjaka ključna je u slučaju značajnog kibernetičkog incidenta. Kibernetičke prijetnje često ciljaju sustave i usluge koji su međusobno povezani i zahtijevaju suradnju više javnih institucija i privatnih tvrtki. Javni sektor igra ključnu ulogu u nacionalnoj koordinaciji, upravljanju krizama i zaštiti bitnih javnih usluga, dok stručnjaci iz privatnog sektora često pružaju specijalizirano tehničko znanje, obavještajne podatke o prijetnjama, forenzičke sposobnosti i izravnu operativnu podršku. Kada se te snage kombiniraju, odgovor postaje brži, učinkovitiji i bolje koordiniran."

U stvarnoj krizi, ključna je upravo prethodno uspostavljena suradnja. Ako institucije i privatni stručnjaci već imaju definirane procese, kontaktne točke i razumijevanje svojih uloga, odgovor na napad može biti znatno brži. To je osobito važno u trenucima kada minute odlučuju o dostupnosti usluga, očuvanju podataka i povjerenju korisnika.

Što ovakve vježbe otkrivaju o spremnosti?

Locked Shields je i test i ogledalo. Testira tehničku zrelost, organizacijsku strukturu i sposobnost tima da djeluje pod velikim pritiskom, ali istodobno pokazuje gdje su snage, a gdje postoje područja za daljnje unaprjeđenje.

Kroz vježbu hrvatski su stručnjaci radili u uvjetima koji vjerno simuliraju složene kibernetičke napade – s velikim brojem sudionika, različitim ulogama i višeslojnom obranom. Takvo okruženje testira ne samo tehničke sposobnosti, nego i komunikaciju, donošenje odluka te međusobno povjerenje.

Koliko je hrvatski tim bio spreman, pojašnjava Jakov Kiš:

"Budući da je ovo prvo sudjelovanje Republike Hrvatske u vježbi Locked Shields, naši stručnjaci pokazali su zavidnu razinu znanja i vještina potrebnih za suočavanje s naprednim kibernetičkim napadima. Iako brojka od 135 sudionika zvuči velika, hrvatski tim je među manjima u vježbi, a sama kompleksnost i opseg vježbe pokazao je potrebu za uključivanjem više sudionika. Hrvatska je pokazala veliki napredak i sposobnost brze prilagodbe već u dva dana vježbe, a kao senior partner u skupini zajedno s Makedonijom, stekli smo veliko iskustvo koje nastavljamo nadograđivati u svakodnevnom radu i budućim sudjelovanjima u NATO vježbama."

Širi značaj za digitalnu otpornost

U vremenu kada se digitalne usluge sve više koriste u svakodnevnom životu, otpornost na kibernetičke incidente postaje sastavni dio javnog interesa. Građani možda ne vide pozadinsku infrastrukturu, ali itekako osjećaju posljedice njezina zastoja. Zato je važno da institucije koje je održavaju budu pripremljene ne samo za uobičajeni rad, nego i za izvanredne sigurnosne situacije.