KIBERNETIČKA SIGURNOST I NATO

Na koji način Sjevernoatlantski savez štiti svoj kibernetički prostor

Kibernetički napadi predstavljaju sve veću opasnost, ne samo za obezbjeđenje odbrane i sigurnosti država članica NATO-a nego i za ukupno funkcionisanje društva i ekonomije. Kibernetički napad može imati razornije posljedice od tradicionalnog napada, a istovremeno je povoljniji i brže izvodiv. Takođe, napad na jednu države se vrlo lako može proširiti i obuhvatiti i druge saveznike. Pored navedenog, kibernetički prostor i informacijske tehnologije danas obezbjeđuju funkcionalnost velikog dijela oružanih snaga i ujedno povezuju sve ratne oblasti.

Sjevernoatlantski savez je zato svrstao kibernetički prostor u „Operativne domene", a razvoj sposobnosti za kibernetičku odbranu se danas smatra jednako važnim korakom kao što je razvoj odbrane na zemlji, na moru, u vazduhu i u bliskom svemiru. Države članice su se obavezale da će, prije svega, jačati bezbjednost svojih nacionalnih mreža, te da će povećavati otpornost na kibernetičke napade (tzv. Cyber Defence Pledge iz 2016. god.). Sa aspekta bezbjednosti, značajno je da se na kibernetičke napade primjenjuje članak 5 Vašingtonskog ugovora, odnosno da se napad na jednog saveznika može smatrati napadom na cijeli Savez.

Uloga NATO-a u oblasti kibernetičke odbrane

1) Zaštita savezničkih mreža protiv napada

Na mrežnu infrastrukturu NATO-a se oslanjaju desetine hiljada osoba na više od 60 različitih lokacija – ne samo u Briselu u centrali Saveza, već i u savezničkim komandnim mjestima u Evropi i u SAD-u ili na mjestima gdje su u toku operacije NATO-a. Sistemi NATO saveza se susreću sa stotinama napada mjesečno. Radi se kako o napadima na niskom nivou tako i o tehnološki razrađenim napadima. Većina napada se evidentira i automatski rješava, međutim, neki napadi zahtijevaju analizu i uključenje ekspertnog tima.

2) Kako NATO pomaže državama članicama?

- podrškom u dijeljenju informacija o prijetnjama u realnom vremenu, uključujući razmjenu provjerenih procedura,
- NATO raspolaže timovima za kibernetičku odbranu (NATO Cyber Rapid Reaction teams) koji mogu saveznici ma brzo pomoći pri rješavanju kibernetičkih napada,
- određivanjem ciljeva za razvoj kibernetičke sposobnosti država članica, što olakšava saradnju na nivou cijelog Saveza i dalji razvoj sposobnosti (npr. posredstvom tzv. NATO Defence Planning Process),
- podrškom u edukaciji i obrazovanju (npr. preko NATO škola u Njemačkoj, Portugalu i Italiji), kao i organizacijom vježbi (npr. godišnja međunarodna vježba Cyber Coalition) koje saveznicima pružaju mogućnost da poboljšaju svoje sposobnosti.

Da li vam je pozNATO?

Bezbjednost i odbrana kibernetičkog prostora

Trend digitalizacije ili robotizacije u mnogim segmentima olakšava život, ali istovremeno donosi nove rizike i prijetnje. Ovisnost društva o digitalnim informacijskim sistemima se konstantno povećava, a kibernetički napadi su učestaliji, sofisticiraniji i ozbiljniji. Pri tome, narušavanje komunikacije ili zloupotreba podataka može uticati na procese odlučivanja, a potom i na ugrožavanje npr. života ili imovine stanovnika ili same države. Zaštita informacijskih sistema od softverske ili hardverske zloupotrebe ili zloupotrebe otuđenja podataka koji su pohranjeni u ovim sistemima jeste ključno rješenje u pružanju sigurnosti kibernetičkog prostora. Pružanjem bezbjednosti i odbranom kibernetičkog prostora, odnosno zaštitom informacija, sistema i infrastrukture, sve intenzivnije se bave kako stručne ustanove tako i pojedine vlade na najvišem nivou, kao i sam Sjevernoatlantski savez.

Glavni mehanizmi kibernetičke odbrane pod nadzorom NATO-a

Saveznu politiku u oblasti kibernetičke odbrane provode politička, vojna i tehnička tijela NATO-a, ali NATO za svoje operacije može koristiti i nacionalne kibernetičke kapacitete.

Sveobuhvatan politički nadzor na najvišem nivou pruža Sjevernoatlantsko vijeće čiji je savjetodavni organ u predmetima kibernetičke odbrane Komitet za kibernetičku odbranu (Cyber Defence Committee – CDC).

KIBERNETIČKA SIGURNOST I NATO

Na koji način Sjevernoatlantski savez štiti svoj kibernetički prostor

Savjet za upravljanje kibernetičkom odbranom (Cyber Defence Management Board – CDMB) koordinira odbranu na radnom nivou. Sastoji se od zastupnika svih glavnih tijela u oblasti kibernetičke bezbjednosti u okviru NATO-a. CDMB pored ostalog potpisuje sa državama članicama i tzv. Memorandum o razumijevanju s ciljem olakšavanja razmjene informacija, pobojšanja prevencije incidenata i koordinacije eventualne pomoći.

NATO Computer Incident Response Capability (NCRIC) je grupa od dvije stotine stručnjaka u Monsu u Belgiji sa zadatkom da obezbijedi zaštitnu mrežu NATO-a i pruži državama članicama i saveznicima aktuelne informacije i analizu kibernetičkih izazova.

NATO Cyberspace Operations Centre je operativni centar u pripremi, koji će od 2023. godine pojačavati kibernetičku odbranu NATO saveza i pružati vojnoj komandi informacije potrebne za podržavanje operacija i misija Saveza. Centar bi trebalo da koordinira operativno djelovanje NATO-a u kibernetičkom prostoru i da pojača otpornost operacija na kibernetičke prijetnje.

Centar excelence NATO-a za kibernetičku odbranu (CCDCOE) u Estoniji, koji nakon iskustava sa kibernetičkim napadima 2007. godine danas nastupa kao vodeći lider u Savezu po pitanju kibernetičke bezbjednosti. Centar realizuje istraživanja, edukacije ili konsultativne aktivnosti. Njegov temelj su stručnjaci iz 29 država, a uključene su i neke države koje nisu članice, npr. Japan. Pošto centri excelence nisu u lancu komandne strukture Saveza, nemaju mandat za izvršavanje operacija tako da je omogućeno i učešće nečlanskih država, npr. u kibernetičkim vježbama,.

Primjeri kibernetičkih napada

Kibernetički napadi su usmjereni na razne ciljeve, od vojnih (npr. napadi na kompletnu državu), kriminalnih (npr. krađe), do ekonomskih (npr. kibernetička špijunaža) i drugih, i često su uzajamno povezani. Mogu imati ozbiljne posljedice i na svakodnevni život (npr. onesposobljavanje državne uprave u Estoniji 2007. godine, prekid isporuke električne energije za stotine hiljada stanovnika Ukrajine 2015. i 2016. godine) ili ciljano na specifične sposobnosti (oštećenje iranskog nuklearnog programa malver Stuxnet oko 2010. godine). Napadi nisu zaobišli ni Republiku Češku, organi vlasti su 2019. godine rješavali preko dvije stotine napada protiv institucija i firmi. Po život opasni su i napadi na kompjuterske mreže zdravstvenih ustanova, a posebno u periodu pandemije, što je NATO posebno osudio (u ČR pogledajte primjere u Benešovu i Brnu).

Bosna i Hercegovina

U kontekstu saradnje sa NATO-om, Bosna i Hercegovina je načine zaštite svog kibernetičkog prostora u najvećoj mjeri definisala u Programu reformi BiH 2021.
U ovom dokumentu, usvojenom od strane Predsjedništva BiH nakon što je BiH primljena u MAP, u okviru Sigurnosnih pitanja posebna pažnja posvećena je „cyber sigurnosti" koja „ostaje prioritet za BiH i nastavit će se fokusirati na jačanje institucionalnih, tehničkih i operativnih sposobnosti BiH Tima za odgovor na kompjuterske incidente (CERT) na putu ostvarenja svojih strateških ciljeva".
Uz navedeno, u Programu reformi za 2021. godinu podvučeno je da će se definisati načini komunikacije i koordinacije između relevantnih institucija za „cyber sigurnost" i izraditi strateški okvir za „cyber sigurnost" u BiH.

Program reformi BiH za 2021. Godinu plan provedbe „cyber sigurnosti" dijeli na 6 aktivnosti:

- Ojačati CERT za institucije BiH,
- Ispuniti CERT strateške ciljeve,
- Izraditi i usvojiti odluku o uspostavljanju mreže CERT-ova u BiH kojom će se definisati metod komunikacije i koordinacije između CERT timova u BiH,
- Izraditi Nacrt zakona o informacionoj bezbjednosti i bezbjednosti mrežnih i informacionih sistema u institucijama BiH shodno NIS direktivi,
- Izraditi strateški okvir za „cyber sigurnost",
- Obezbijediti uslove koji će omogućiti prijem i zadržavanje IT stručnjaka u CERT-u za institucije BiH.

Nakon što je 17. 5. 2022. godine zamjenik generalnog sekretara NATO-a Mircea Geoana upozorio je da bi Rusija mogla pokušati napasti kritičnu digitalnu infrastrukturu Gruzije i Bosne i Hercegovine, kao što je učinila kada je napala Ukrajinu, samo dan kasnije, ministar odbrane BiH Sifet Podžić izjavio je da će NATO pomoći BiH u vezi sa mogućim „cyber napadima" iz Rusije.
Podžić je tom prilikom potvrdio da su sa NATO-om sastanci već obavljeni i određene mjere su poduzete, a sastanak između Političko-sigurnosnog komiteta NATO-a i delegacije Bosne i Hercegovine održan 21. 6. 2022. godine u sjedištu NATO-a u Briselu potvrdio je čvrstu saradnju BiH i Alijanse na polju zaštite kibernetičkog prostora naše zemlje.

KIBERNETIČKA SIGURNOST I NATO

Na koji način Sjevernoatlantski savez štiti svoj kibernetički prostor

Tako je paket pomoći BiH, pored ostalog, sadržao i podrazumijevao i pomoć u sigurnosnom kontekstu i to kroz jačanje kapaciteta za kibernetičku (cyber) odbranu.
Ekpsertski tim za sprečavanje „cyber" incidenata Ministarstva odbrane i Oružanih snaga BiH boravio je 27. 6. do 1. 7. 2022. godine u radnoj posjeti 169. timu za „cyber" zaštitu Nacionalne garde Maryland.
Cilj ove posjete bio je nastavak dosadašnje saradnje na uspostavljanju kapaciteta Ministarstva odbrane (MO) i Oružanih snaga (OS) BiH za uspješno uspostavljanje sistema „cyber sigurnosti" u MO i OS BiH. Tokom posjete realizovano je više aktivnosti iz oblasti kibernetička sigurnosti, te razmjena iskustava kroz naučene lekcije.

LINKOVI:

https://ekonsultacije.gov.ba/legislativeactivities/details/110879

https://www.klix.ba/vijesti/bih/upozorenje-iz-nato-a-rusija-bi-mogla-izvesti-velike-cyber-napade-u-bih-moramo-pomoci/220518002
https://ba.voanews.com/a/ministar-odbrane-bih-preduzima-mjere-u-vezi-sa-mogucim-cyber-napadom-iz-rusije/6579124.html

Tim za sprečavanje cyber incidenata MO i OS BiH u posjeti 169. timu za cyber zaštitu Nacionalne garde Maryland

Nacionalni ured za cyber i informacionu bezbjednost (https://www.nukib.cz/cs/) i bezbjednosne preporuke istog (https://www.nukib.cz/cs/infoservis/doporučeni/)
North Atlantic Treaty Organization (2020): Cyber defence. Nato.int, 25. 9. 2020. (https://www.nato.int/cps/en/natohq/ topics_78170.htm)
North Atlantic Treaty Organization (2020): NATO Cyber Defence Factsheet. (https://www.nato.int/nato_static_fl2014/assets/ pdf/2020/8/pdf/2008-factsheet-cyber-defence-en.pdf)
Fertasi, Nadja El – De Vivo, Diana (2016): Cyber resilience: protecting NATO's nervous system. NATO Review. (http://www. nato.int/docu/review/2016/Also-in-2016/nato-cyber-resilience-security/EN/index.htm)
Zaharia, Andra (2020): 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends. Comparitech.com, 29. 7. 2020. (https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Cost_of_cybercrime_stats)

Objavljivanje ovog teksta omogućeno je podrškom Ministarstva vanjskih poslova Republike Češke.
Tekst odražava stav njegovog autora, a ne nužno i stav Republike Češke.

Tekst je preuzet i preveden sa sajta natoaktual.cz.
Nova ideja RS 2030 je adaptirala i/ili dodala dijelove teksta koji se odnose na BiH.