Informaciona bezbednost - među-sektorska saradnja: normativni i strateški okvir

Irina Rizmal
Ženevski centar za demokratsku kontrolu oružanih snaga (DCAF)

Imajući u vidu širinu zahvata oblasti kao što je informaciona bezbednost, broj aktera koje ona obuhvata kao i razmere izazova i pretnji koje sa sobom nosi, među-sektorska saradnja i javno-privatna partnerstva su postala model koji sve veći broj država u svetu prepoznaje kao neizbežan odnosno poželjan. Javni sektor uglavnom ima ograničene kapacitete u smislu ljudskih i finansijskih resursa; privredi je neophodan jasan normativni i strateški okvir u kojem dalje razvija svoje poslovanje; značajan broj operatora IKT sistema od posebnog značaja (kritične infrastrukture) je u rukama privatnog sektora; akademski sektor doprinosi u smislu istraživanja i razvoja; civilno društvo ukazuje na pitanja i izazove koje nose nove tehnologije kao i normativni okviri koji se razvijaju a koja nisu uvek primarni fokus prethodno navedenih aktera i slično.

Srbija je prepoznala potrebu za među-sektorskom saradnjom i ona se donekle odražava u samom Zakonu, ali i mnogo više u Strategiji razvoja informacione bezbednosti. Naime, usvajanjem Zakona o informacionoj bezbednosti 2016. godine, osnovano je Telo za koordinaciju poslova informacione bezbednosti pod okriljem Vlade Srbije. Telo ima savetodavnu ulogu i primarni članovi su predstavnici ministarstava nadležnih za poslove informacione bezbednosti, odbrane, unutrašnjih poslova, pravde, predstavnici službi bezbednosti, Kancelarije Saveta za nacionalnu bezbednost i zaštitu tajnih podataka, Generalnog sekretarijata Vlade, Centra za bezbednost IKT sistema (CERT-a) u organima vlasti i Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalnog CERT-a). Nedavnim izmenama Zakona (u oktobru 2019. godine), osnovnom članstvu Tela za koordinaciju dodati su i predstavnici Narodne banke. Zakon međutim ostavlja i mogućnost formiranja stručnih radnih grupa Tela za koordinaciju u koje se uključuju i predstavnici drugih organa vlasti, ali i *privrede, akademske zajednice i nevladinog sektora*.

Pomenuta zakonska mogućnost ostvarivanja među-sektorske saradnje pominje se i u Strategiji razvoja informacione bezbednosti kao potencijal za uspostavljanje sveobuhvatnijeg okvira informacione bezbednosti u zemlji (usvojenoj 2017. godine). Uspostavljanje stalne saradnje između javnog i privatnog sektora, kao osnov za razvoj i unapređenje strateških prioriteta, navedeno je kao jedan od sedam principa razvoja informacione bezbednosti. Učešće nevladinog sektora, akademske zajednice i drugih subjekata u ovoj oblasti prepoznato je kao značajno u naporima usmerenim na podizanje svesti o bezbednosnim rizicima i važnosti primena mera zaštite.

Konkretno, Strategija između ostalog navodi da je za održavanje adekvatnog nivoa informacione bezbednosti u zemlji potrebno, pored države, učešće drugih sektora, uključujući privredu, građane, nevladin sektor, akademsku zajednicu i ostale relevantne aktere. U tom smislu, uspostavljanje saradnje javnog i privatnog sektora koja će omogućiti efikasnu komunikaciju i optimizaciju planiranih budućih aktivnosti, odnosno blagovremenu razmenu informacija i deljenje resursa, prepoznato je kao jedan od polaznih prioriteta za unapređivanje ove oblasti u Srbiji. Akcenat je stavljen na izgradnju trajnog poverenja među ovim akterima,

uključujući tu javni sektor, odnosno predstavnike državnih institucija, privatni sektor, odnosno privredu, i građane organizovane u civilno društvo. Kao polazni mehanizam za uspostavljanje ovakve saradnje navedeno je pomenuto Telo za koordinaciju i prostor koji je ostavljen za formiranje stručnih radnih grupa u okviru istog.

Na kraju, operativniji vid javno-privatne saradnje koji zakonski okvir omogućava je i formiranje takozvanih Posebnih CERT-ova. Poseban CERT je pravno lice ili organizaciona jedinica u okviru pravnog lica koje obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično. U praksi, ovo ostavlja prostor za formiranje mreže Posebnih CERT-ova koji se upisuju u evidenciju koju vodi Nacionalni CERT i koji mogu biti, na primer, u okviru konkretnog preduzeća ili organizacije i usmereni samo na jedan sistem, ili sektorski i usmereni na grupu srodnih aktera (npr. bankarski CERT, CERT telekomunikacionih operatora, medijski CERT i sl). Sektorski CERT-ovi su tako uže specijalizovani za posebnu ciljnu grupu (ne-državnih) aktera, a upisom u evidenciju Nacionalnog CERT-a uključuju se u mrežu CERT-ova na nacionalnom nivou koja se zasniva na principima među-sektorske, javno-privatne saradnje.

Zaključci i preporuke

Evidentna je potreba za daljim jačanjem svesti i širenjem digitalne pismenosti. Iako možda zvuči kao kliše, činjenica je da čovek jeste i dalje najslabija karika sistema. Samim tim, jačanje svesti o 'sajber higijeni' (osnovama individualne sajber bezbednosti) je prvi korak ka izgradnji otpornih struktura bilo kojeg okvira/sektora. U ovim naporima, mediji igraju značajnu ulogu. Kao forumi za diseminaciju informacija, mediji su jedan od ključnih izvora znanja šire javnosti. Preduslov za adekvatno vršenje ove uloge su 'digitalno pismeni' i osvešćeni novinari koji dovoljno poznaju oblast i razumeju potencijalne rizike u sajber sferi. U tom smislu, potrebno je razviti različite alate koji bi poslužili kao izvor osnovnih znanja i veština za održavanje individualne 'sajber higijene' najpre predstavnika medija i civilnog društva u cilju podrške daljeg 'opismenjavanja' u ovoj oblasti. Tematski prilagođene radionice i simulacione vežbe takođe mogu da pomognu u ovim naporima kako bi se na realnim scenarijima pokazalo šta i kako može da se desi u praksi i kako izgraditi veću otpornost pojedinaca i samim tim i sistema kojima oni pripadaju. Na ovaj način, podržava se razvoj odgovornog izveštavanja javnosti o ovoj oblasti i posledično jačanje svesti šire javnosti.

Kada je u pitanju dolaženje do adekvatnih informacija u cilju izveštavanja, prevencije i/ili prevazilaženja izazova ili posledica napada, najčešća zamerka je vreme potrebno za filtriranje podataka koji su dostupni kroz različite mehanizme za razmenu informacija. Razvijene platforme za razmenu podataka funkcionišu po principu zajednice jednakih. Pretpostavlja se da će svi članovi zajednice koji su uključeni u datu platformu ne samo koristiti informacije koje su kroz nju dostupne, već i dodavati informacije i iskustva do kojih oni dođu kroz svoj rad ili kroz druge slične platforme u kojima su aktivni. Kao rezultat toga, opšt(ij)e, odnosno, sveobuhvatnije platforme za razmenu informacija koje obuhvataju veliki broj različitih aktera sadrže pregršt informacija koje nisu sve jednako relevantne za sve članove. U tom smislu, sektorski CERT-ovi, kao što je Share, imaju značajnu ulogu kao potencijalna tačka za informisanje o sektorski-prilagođenim izazovima i incidentima. Dodatno, sektorski CERT-ovi takođe već dobijaju informacije kroz članstvo u različitim nacionalnim, regionalnim i globalnim forumima CERT timova, što znači da imaju pristup različtim izvorima znanja i informacija u ovoj oblasti koje mogu da prenesu svojim konstituentima.

Osim informacija, sektorski CERT-ovi mogu da pomognu i 'na terenu' u vidu tehničke podrške u uklanjanju posledica napada, ali i prilikom preduzimanja daljih koraka (poput prikupljanja

digitalnih dokaza radi podnošenja prijava Odeljenju za visokotehnološki kriminal Ministarstva unutrašnjih poslova u slučaju krivičnog dela, na primer). Ovako nešto se ne može očekivati od Nacionalnog CERT-a koji je nadležan za vrlo širok spektar nacionalnih aktera i čija je uloga primarno usmerena na prikupljanje i razmenu informacija, obaveštavanje i upozoravanje, kao i na podizanje svesti na nacionalnom nivou. Pomoć koju sektorski CERT-ovi mogu da pruže će zbog same činjenice da su *sektorski* biti i bolje prilagođena zbog jasnije definisane ciljne grupe (sektora) i boljeg poznavanja izazova i problema sa kojim se data grupa suočava. Sektorski CERT-ovi su tako primarni alat za podršku akterima koji pripadaju ciljnoj grupi datog CERT-a.

Ipak, iako akteri koji nisu Zakonom definisani kao operatori IKT sistema od posebnog značaja nisu u obavezi da prijavljuju incidente Nacionalnom CERT-u, ovo je dobra praksa koja se preporučuje radi statističke analize stanja u nacionalnom sajber prostoru. Naime, jedna od Zakonom utvrđenih aktivnosti Nacionalnog CERT-a je i kontinuriana izrada analiza rizika i incidenata na osnovu uočenih problema i primljenih informacija (prijava). Prijavljivanje incidenata koje su mediji i civilno društvo pretrpeli generisaće statistiku na nacionalnom nivou i ukazati na razmere izazova sa kojima se ovi akteri suočavaju u sajber prostoru. Imajući u vidu (još uvek) relativno mali broj prijava koje Nacionalni CERT primi na godišnjem nivou, značajniji broj prijava iz jednog sektora bi potencijalno mogao da pomogne u smislu opšteg podizanja svesti o tome kakva je situacija u ovim sektorima.

Konačno, učešće u, i povezivanje sa, među-sektorskim forumima dodatno doprinosi naporima usmerenim na razmenu informacija sa relevantnim akterima kao i specifičnih iskustava u prevenciji i prevazilaženju rizika i posledica napada u sajber prostoru. Iako su motivi napada na, na primer, bankarski sektor značajno drugačiji od motiva napada na medije ili organizacije civilnog društva, načini na koji se napadi izvode i razvijaju, kao i njihove posledice su isti, ili makar dovoljno slični, za svaki sektor. U tom smislu, razmena informacija, znanja i iskustava u među-sektorskim forumima može samo dodatno pomoći u uspostavljanju otpornih sistema i prevenciji, ali i u otklanjanju mogućih posledica napada kroz širu mrežu kontakata i podrške.