Monitoring digitalnih prava u Srbiji

januar-mart 2018.

Tehnički napadi na onlajn sadržaje ponovo preuzimaju primat u monitoringu stanja digitalnih prava i sloboda. Od 15 slučajeva povreda digitalnih prava i sloboda koje je SHARE Fondacija zabeležila u periodu januar – mart 2018, bilo je 6 slučajeva u kojima je onemogućen pristup sadržaju ili je na druge načine ugrožena informaciona bezbednost. Trend porasta pokazuje da smo od početka aprila već zabeležili tri tehnička napada. Među njima su prevara građana na Fejsbuku sa platnim karticama, tehnički napad na sajt Komiteta pravnika za ljudska prava (YUCOM) sa ciljem obaranja sajta i neovlašćeni pristup nalozima organizacije "Da se zna" na Instagramu i Tviteru.

Tehnički napadi kao metoda ugrožavanja digitalnih prava i sloboda, uglavnom sa ciljem činjena sadržaja medija nedostupnim, bili su na vrhuncu sredinom 2014. godine, kada je zbog afera sa plagiranim doktoratima u više navrata "obaran" sajt Peščanika. "Rušenja" Peščanika privukla su veliku pažnju javnosti i medija, te je zanimljivo da se kasnije nije javljao toliki broj slučajeva tehničkih napada na sajtove onlajn medija i organizacija civilnog društva, osim nekoliko sporadičnih primera.

Najupečatljiviji slučaj dogodio se krajem februara, kada su nepoznati počinioci preuzeli Fejsbuk stranicu Nezavisnog udruženja novinara Srbije (NUNS), uklonili administratore koji su upravljali stranicom i objavili neprikadan sadržaj. Tim SHARE Fondacije za prevenciju rizika po informacionu bezbednost SHARE CERT je uradio analizu incidenta i kontaktirao predstavnike Fejsbuka za Srednju i Istočnu Evropu, koji nisu reagovali povodom ovog slučaja, odnosno nisu povratili administratorski pristup zaposlenima u NUNS. Kao posledica neovlašćenog pristupa, dotadašnja Fejsbuk stranica NUNS je ugašena, te je udruženje moralo da napravi novu stranicu.

Slučaj Fejsbuk stranice NUNS pokazao je koliko je postalo rizično oslanjati se na postavljanje sadržaja na platforme nad kojima nemamo kontrolu u pogledu skladištenja (hostinga) podataka. Sve objave koje ste godinama postavljali, lajkovi i pratioci mogu nestati u trenutku, a u obzir treba uzeti i sredstva ulagana u promovisanje objava da bi dostigle više korisnika. Platforme u vlasništvu moćnih kompanija sa sedištem u Kaliforniji, kao što su Fejsbuk i Gugl, mogu da kontrolišu sadržaj i naloge korisnika pod uslovima korišćenja koji se mogu tumačiti veoma široko.

Kada je reč o ostalim incidentima u vezi sa kompromitovanjem informacione bezbednosti tehničkim metodama, važno je napomenuti da su mete u ovom periodu bile organizacije civilnog društva, za razliku od ranijih perioda kada su najviše napadani sajtovi medija. Sajtovi Centra za evroatlantske studije (CEAS), Fondacije "Budi human" i novinske agencije Tanjug bili su pod napadima, a posebno je zanimljivo da se Tanjug oglasio saopštenjem da se napad vrši sa "preko 50 IP adresa iz Srbije" sa ciljem "da se sruši informacioni sistem agencije". Napadi "zagušivanjem" ili "preplavljivanjem" servera se najčešće vrše sa više desetina hiljada adresa iz celog sveta, kao što je to bilo u slučaju sajta CEAS – korišćeno je oko 27000 IP adresa, od kojih gotovo sve potiču iz Holandije. Ostaje nejasno kakve su bezbednosne mere primenjene ukoliko slanje zahteva za pristup sajtu sa svega 50 IP adresa može da ugrozi informacioni sistem, i o tome mediji moraju posebno da vode računa.

Iako smo u prva tri meseca monitoringa imali važan društveni događaj sa aspekata političke aktivnosti na internetu – lokalne izbore u Beogradu – čini se da je ova kampanja prošla sa manje incidenata u digitalnom okruženju od nekih prethodnih. Međutim, kao slučajeve koji su se istakli možemo da izdvojimo kreiranje lažnog profila gradonačelnika Beograda Siniše Malog i pretnje predsedniku pokreta "Dveri" Bošku Obradoviću u Jutjub komentarima na emisiju u kojoj je gostovao tokom kampanje.

Pretnje i pozivi na nasilje, najbrojnija kategorija povreda digitalnih prava i sloboda, doživljavaju pad u broju slučajeva, ali ostaje problem neefikasne reakcije nadležnih organa. Pretnje novinaru Draganu Janjiću zbog stava da je ubistvo Olivera Ivanovića politički motivisano širene su putem sponzorisanih objava na Fejsbuk stranici "Srbija naša zemlja". Prvo osnovno javno tužilaštvo u Beogradu odbacilo je krivičnu prijavu koju je u Janjićevo ime podnelo NUNS, uz navode da "ne postoje osnovi sumnji da je učinjeno krivično delo za koje se goni po službenoj dužnosti".

Problemi sa zaštitom podataka o ličnosti nisu se u velikoj meri isticali u ranijim periodima monitoringa, ali je od januara do marta bilo tri slučaja, od kojih je svakako najgrublja povreda objavljivanje podataka učesnika protesta u Požegi koji su korisnici socijalne pomoći. Na Fejsbuku su se pojavile prepiske, transakcije sa privatnih računa građana, njihovi zahtevi i molbe Centru za socijalni rad Požega i drugi podaci. Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti je zbog slučaja u Požegi pokrenuo nadzor. Međutim, ovo nije izolovan slučaj objavljivanja podataka o primanju socijalnoj pomoći, koji po Zakonu o zaštiti podataka o ličnosti spadaju u naročito osetljive podatke. Poverenik je takođe pokrenuo postupak nadzora nad Ministarstvom za rad, zapošljavanje, boračka i socijalna pitanja i preduzetnikom na čijem sajtu su objavljeni podaci o žrtvama porodičnog nasilja i primaocima socijalne pomoći.

Ponovo se vraćamo na pitanje odnosa nadležnih organa prema ljudskim pravima u digitalnom okruženju, jer se čini da svaki pomak u pogledu rešavanja slučajeva pretnji, tehničkih napada i

drugih povreda prate (najmanje) dva koraka unazad. Sporazum o bezbednosti novinara koji su Republičko javno tužilaštvo i MUP potpisali sa medijskim i novinarskim udruženjima još krajem 2016. očigledno ne daje želje rezultate, naročito u kontekstu odbacivanja krivičnih prijava zbog ugrožavanja sigurnosti novinara i postupaka čiji se sudski epilog čeka dugo.

Da bi tehnički napadi na sajtove medija, civilnog društva i druge subjekte bili rešeni u najkraćem mogućem periodu, neophodno je pojačati kapacitete Tužilaštva za visoko-tehnološki kriminal, VTK odeljenja MUP-a, kao i unaprediti odnose sa velikim stranim kompanijama u čijem su vlasništvu najpopularnije platforme. Poverenik Rodoljub Šabić je nebrojeno puta u medijima ukazao na nedopustivo loš odnos države prema zaštiti podataka o ličnosti građana, što nedavni slučajevi potvrđuju.

Uloga civilnog sektora u rešavanju problema na najvećim i najpopularnijim onlajn platformama mora da bude podignuta na viši nivo, jer kada je reč o sadržajima na Fejsbuku, Tviteru ili Jutjubu, glavnu pregovaračku poziciju imaju privatne kompanije sa sedištem van Srbije i teško da policija i drugi državni organi mogu sami da sprovedu svoje zahteve. SHARE Fondacije će kroz SHARE CERT i članstvo u evropskoj koaliciji za digitalna prava EDRi nastaviti da uspostavlja direktan kontakt sa timovima platformi zaduženim za bezbednost, kako bi se zahtevi u pogledu prava korisnika iz Srbije razmotrili i efikasno rešavali.

Monitoring baza SHARE Fondacije