VODIČ:

KROZ RIZIKE I MEHANIZME ZAŠTITE NEZAVISNOSTI I BEZBEDNOSTI ONLAJN MEDIJA

HOD PO DIGITALNOJ IVICI

SHARE FOUNDATION - 2015

vodič

"VODIČ KROZ RIZIKE I MEHANIZME ZAŠTITE NEZAVISNOSTI I BEZBEDNOSTI ONLAJN MEDIJA"
SHARE FONDACIJA
OKTOBAR 2015
UREDNICI: ĐORĐE KRIVOKAPIĆ, VLADAN JOLER
TEKSTOVI: NEVENA KRIVOKAPIĆ, BOJAN PERKOV, MILICA JOVANOVIĆ
LEKTURA: MILICA JOVANOVIĆ
DIZAJN I PRELOM: OLIVIA SOLIS VILLAVERDE

ŠTAMPARIJA: NS PRESS DOO NOVI SAD
TIRAŽ : 200

PODRŠKA PROJEKTU:

FONDACIJA ZA OTVORENO DRUŠTVO, SRBIJA
OPEN SOCIETY FOUNDATION, SERBIA

CIP - Каталогизација у публикацији
Библиотека Матице српске, Нови Сад
34:[070:004.738.5(036)
КРИВОКАПИЋ, Невена
Pravni položaj online medija u Srbiji : vodič namenjen online i građanskim medijima kao korisnicima / [tekstovi Nevena Krivokapić, Ognjen Colić, Marija Maksimović]. - Novi Sad : Share fondacija, 2015 (Novi Sad : NS press). - 40 str.; 16 cm
Tiraž 200.
ISBN 978-86-89487-02-2
a) Електронски медији - Правни аспект - Србија - Водичи
COBISS.SR-ID 295461895

APSTRAKT

U poslednje vreme sajber napadi na onlajn medije i novinare u Srbiji postaju sve učestaliji. Veb portali su bili meta DDoS napada kojima se onemogućavao pristup njihovom sadržaju, ali i napada u kojima se utiče na integritet baza podataka. Ove slučajeve nadležni organi još uvek nisu rešili. Novinari su bili suočeni sa izazovima društvenog inženjeringa, oduzimanja i lažiranja onlajn identiteta i neovlašćenog pristupanja privatnim komunikacijama. Građanske novinare i aktivne učesnike u javnim debatama su pogodile manipulacije javnim mnjenjem, zastrašivanja putem anonimnih pretnji, ali i dvostruki aršini nadležnih prilikom procesuiranja slučajeva eventualnog prekoračenja slobode izražavanja.

Da bismo bolje pojasnili i predstavili ove probleme, procenićemo trenutnu poziciju onlajn medija i novinara u digitalnom okruženju, uzimajući u obzir činjenicu da oni čuvaju naročito poverljive i osetljive informacije ne samo na svojim uređajima već i širom mreže. Ovaj izveštaj će stoga posebnu pažnju posvetiti digitalnim rizicima, npr. gubitku ili otkrivanju podataka, kao i mehanizmima za smanjenje i izbegavanje rizika, odgovornim akterima ali i odnosu među suprostavljenim vrednostima (npr. privatnost v. bezbednost).

Konačno, analizom rizika koji ugrožavaju ostvarivanje osnovnih ljudskih prava i slabosti postojećeg sistema predložićemo niz mera koje bi Republika Srbija trebalo da preduzme kako bi povratila poverenje javnosti da može obezbediti zaštitu.

KLJUČNE REČI: onlajn mediji, novinari, digitalna bezbednost, sajber napadi, rizici

UVOD

U protekle dve godine, bili smo svedoci velikog porasta slučajeva kršenja ljudskih prava u onlajn okruženju u Srbiji. Mogli smo da vidimo da sadržaj kojim se kritikuju vlasti misteriozno nestaje, blogovi i onlajn portali odjednom postaju nedostupni dok privatni mejlovi izlaze u javnost a policija privodi građane na ispitivanje zbog izražavanja sopstvenog mišljenja na Internetu.

Posebni slučajevi kršenja onlajn prava i sloboda koje je Share fondacija zapazila vršeći monitoring jesu:

- Arbitrarno blokiranje ili filtriranje sadržaja
- Sajber napadi na nezavisne onlajn i građanske medije
- Hapšenja i sudski postupci protiv korisnika društvenih mreža i blogera
- Manipulisanje javnim mnjenjem upotrebom tehnologije
- Nadgledanje elektronskih komunikacija, kršenje prava na privatnost i zaštitu podataka o ličnosti
- Pritisci, pretnje i ugrožavanje bezbednosti onlajn i građanskih medija, novinara i pojedinaca

KLJUČNI NALAZI

Share fondacija je od maja 2014. godine počela da se bavi monitoringom digitalnih prava i sloboda na Internetu. U ovom izveštaju fokusiraćemo se na period od septembra 2014. do septembra 2015. godine, ali ćemo u delu koji sledi ukratko prikazati i nalaze za ceo period monitoringa, radi što celovitije slike.

- Oko 20 različitih sajtova onlajn medija je bilo pod DDoS napadima, koji su rezultirali prekidom ili suspenzijom rada sajtova. Neki od njih (kao što su Peščanik i Telepromter) bili su pod napadima češće i na duži vremenski period.
- Tokom vanredne situacije za vreme poplava u maju 2014, najmanje 13 članaka i blogova je uklonjeno. Ipak, takav slučaj masovnog ukidanja sadržaja više nije zabeležen.
- Do kraja leta 2015, oko 30 osoba je ispitivano, privođeno ili su sprovedeni sudski procesi zbog njihovih izjava na društvenim mrežama ili blogovima. Takođe, zabeležene su pretnje onlajn medijima i aktivistima koje državni organi nisu adekvatno procesuirali, iako je postojao jasan javni interes.
- Zabeležili smo različite obike napada koji su kompromitovali baze podataka onlajn medija, kao i njihove računare (malware, SQL injection).
- Novinari i pojedinci su bili žrtve neovlašćenog upada u njihove privatne komunikacije.
- Pojavile su se informacije o softveru i upustvima navodno proizvedenim za

potrebe vladajuće partije, za manipulaciju percepcijom javnog mnjenja i preplavljivanje glavnih informativnih portala pozitivnim ili negativnim komentarima i lajkovima/dislajkovima, u zavisnosti od teme.

- Tokom aprila 2015. bili smo svedoci najintruzivnijeg napada na jedan onlajn medij u Srbiji, koji je obuhvatio preuzimanje 4 mejl naloga, hostinga i 2 naloga na društvenim mrežama koji su ključni kanali medija. Iako je onlajn medij imao solidne sigurnosne procedure (različite šifre, dvostruku verifikaciju itd) preuzimanje naloga je izvedeno veoma efikasno. Na osnovu samog napada može se zaključiti da je cilj bio uništenje čitavog sadržaja i obeshrabrivanje daljeg rada tog onlajn medija (što se nije desilo).
- Pravni tim Share fondacije je zastupao i dalje zastupa onlajn medije i organizacije civilnog društva koji su bili pod napadima, pokrenuvši desetak pravnih procesa (uglavnom krivičnih). Svi postupci su još uvek u toku. Dodatno je pružena pravna podrška onlajn medijima, aktivistima i građanima u desetinama drugih slučajeva.

PET STUDIJA SLUČAJA

1. TELEPROMPTER - PRVI SLUČAJ

Iako na glasu kao politički nekorektan sa povremenim nacionalističkim ispadima, privatni blog Teleprompter prerastao je u tipičan građaski onlajn medij, kakvi su u Srbiji još uvek retkost. Jedan od najposećenijih sajtova ove vrste, Teleprompter je poslednjih godina dosledno fokusiran na kritiku stranke na vlasti, kao i njenih koalicionih partnera.

Budući izvan kruga konvencionalnih medija, Teleprompter se u vladajućem javnom diskursu označava kao nevažan, nepouzdan, sumnjivih namera i izvora. Ipak, predstavnici vlasti uključujući i najviše funkcionere više puta su se upuštali u javnu diskusiju sa tvrdnjama iznetim u različitim tekstovima na ovom sajtu, demantujući neke od tih navoda i prilikom zvaničnih obraćanja javnosti.

Različiti oblici tehničkih napada na Teleprompter zabeleženi su i prethodnih godina, ali se dva napada u januaru i aprilu 2015. izdvajaju kao atipični i otkrivaju neke procedure kojima se napadači služe za pripremu glavnog napada.

2. TELEPROMPTER - DRUGI SLUČAJ

Početkom godine vlasnik i urednik Telepromptera primetio je čudne aktivnosti na sajtu. Preko kontakt forme namenjene čitaocima pristiglo je preko 300 mejlova neobične sadržine. Pokazalo se da je reč o SQL injection napadu, odnosno pokušaju ubacivanja malicioznog koda u bazu.

Iz dostupnih dokaza, tehnički analitičar Share fondacije zaključio je da je napad pokrenut ne naročito efikasnim automatskim alatom (Acunetix Web Vulnerability Scanner), inače legalnim softverom za proveru bezbednosti sajtova. Upotrebljen na ovaj način, softver koristi cross-site scripting (XSS) nedostatke sistema kako bi se zaobišle bezbednosne prepreke i ubacio maliciozni kod.

Najjednostavnija prevencija ove vrste napada jeste korišćenje verifikacionog sistema reCAPTCHA za dijalog sa čitaocima, kao i primena funkcije 'escapeshellcmd()' u kodu, a koja sistemu omogućava da izbegne tzv. metakaraktere unete u odeljke sajta otvorene za čitaoce. Zbog ovog napada, Teleprompter je sredinom januara podneo krivičnu prijavu nadležnom tužilaštvu sa predlogom da se sprovedu istražne radnje i inicira krivični postupak.

Sledeći napad na Teleprompter odigrao se u aprilu ove godine, i zasad predstavlja najsloženiji tehnički napad zabeležen u medijskoj onlajn zajednici Srbije.

Napadači su preuzeli kontrolu nad četiri imejl adrese urednika Telepromptera, obezbeđene dvostepenom zaštitom koja podrazumeva slanje verifikacionog koda SMS porukom na mobilni telefon. Iz priloženih dokaza i s obzirom na utvrđenu proceduru logovanja sa verifikacijom, tehnički analitičar Share fondacije nije mogao da utvrdi na koji način su napadači došli do pristupnih šifri za imejl adrese. U krivičnoj prijavi, advokat urednika Telepromptera izneće pretpostavku da su napadači verovatno presreli SMS poruku sa verifikacionim kodom, što prevazilazi forenzička sredstva i ovlašćenja koja su na raspolaganju građanima.

Pošto su na ovaj način preuzeti imejl nalozi, izbrisan je celokupan sadržaj elektronske pošte, promenjene su šifre i druga podešavanja za obnovu pristupa u slučaju blokade, kao i broj telefona koji je korišćen za verifikaciju. Preko imejl naloga, napadači su zatim pristupili Telepromptervim profilima na društvenim mrežama

3. DRAGANA PEĆO

kao i privatnim nalozima urednika sajta. Jedan od četiri imejl naloga sa ovlašćenjem za pristup kontrolnom panelu servera na kom je hostovan Telepromter, iskorišćen je za brisanje tekstova i drugih sadržaja koji su se u tom trenutku nalazili na sajtu. Konačno, izmenama u sistemu, pristupni saobraćaj preusmeren je na sajt kosovske Vlade.

Uz tehničku pomoć, urednik Telepromptera je uspeo da povrati kontrolu nad sajtom, za čiji je sadržaj postojala ažurna rezervna kopija. Pristup na četiri naloga elektronske pošte takođe je obnovljen, a izbrisane poruke nađene su u folderu 'trash', osim na jednom nalogu koji je temeljno ispražnjen.

Iz logova na serveru bilo je moguće locirati bar taj segment napada na sajt, dok pitanje o načinu na koji su napadači došli do pristupnih šifri a posebno eventualnom presretanju SMS poruke sa verifikacijom - ostaje otvoreno.

Tužilaštvo za visokotehnološki kriminal pokrenulo je postupak po službenoj dužnosti, dok je uz pravnu pomoć Share fondacije vlasnik i glavni urednik Telepromptera podneo dopunu krivične prijave 12. maja 2015. godine. Postupak je u toku.

Centar za istraživačko novinarstvo Srbije (CINS), neprofitnu nevladinu organizaciju, osnovalo je Nezavisno udruženje novinara Srbije kao samostalnu platformu oslobođenu komercijalnih pritisaka. Teme kojima se bavi Centar pretežno su vezane za političku korupciju iz vrhova vlasti, finansijski i privredni kriminal.

CINS je izgradio profil modernog tima, svesnog bitno drugačijeg okruženja u kom radi, i koji koristi različita tehnička rešenja za zaštitu saržaja, uključujući i enkripciju u komunikaciji.

Na metu napada u javnosti došli su serijom istraživanja o kriminalnom miljeu kockarske industrije, vođi balkanskog narko-kartela, kao i brojnim napisima o propustima nadležnih u vreme poplava, netransparentnim procedurama tokom obnove i slično.

Sredinom januara, Draganu Pećo, u to vreme novinarku CINS-a, kontaktirala je predstavnica javnog preduzeća kojem se novinarka navodno obratila sa zahtevom za pristup informacijama od javnog značaja. Narednih dana pokazaće se da je identičan zahtev sa njenim potpisom poslat na više adresa državnih institucija, javnih i privatnih preduzeća. Za slanje zahteva korišćena je adresa otvorena na javnom gmail servisu, koju novinarka nikada nije koristila. Pritom, jedini autentičan dokument bio je standardni elektronski formular za slanje zahteva sa potpisom, koji je novinarka uobičajeno koristila.

Lažnom predstavljanju tako je obezbeđena uverljivost, te je dvadesetak institucija kojima je zahtev upućen sa lažnog naloga na njega zaista i odgovorilo. Elektronski formular sa potpisom verovatno je preuzet iz stvarne prepiske koju je novinarka vodila.

Zabluda u koju su dovedene državne institucije kojima je zahtev upućen, govori o nesumnjivom slučaju lažnog predstavljanja koje pritom narušava poslovni ugled novinarke i medijske organizacije za koju radi. Takođe, reč je i o prikupljanju ličnih podataka u nameri da oni budu predati nepozvanom licu.

Uz pomoć pravnog tima Share fondacije, krajem januara podneta je krivična prijava protiv NN lica, zbog sumnje da su izvršili krivična dela narušavanja poslovnog ugleda ili kreditne sposobnosti (član 239 KZ), odavanja poslovne tajne (član 240 KZ), računarske prevare (člana 301 KZ) ili drugo krivično delo za koje se gonjenje preduzima po službenoj dužnosti.

4. PEŠČANIK

Pokrenut kao onlajn glasilo udruženja građana, sajt Peščanik oslanja se na dugogodišnju tradiciju istoimene emisije koju su urednice samostalno realizovale na Radiju B92. Kao format proširen tekstovima i video-emisijama, zadržao je antinacionalističku platformu, što ga je često dovodilo u sukob sa vlastima i većinskom klimom u javnosti.

Raniji slučajevi sistematskog ometanja radijskog signala u vreme emitovanja, pretnje i napadi iz 'analogne' faze Peščanika ostali su u prošlosti, bez epiloga. Od prelaska u onlajn okruženje, sajt trpi stalne napade koji se tehnički unapređuju i intenziviraju od majskih poplava prošle godine, a naročito od objavljivanja analize plagiranih doktorata nekoliko visokih funkcionera na vlasti u junu 2014. Mesec dana kasnije, tokom napada malicioznim softverom izbrisan je sadržaj sa naslovne strane i zamenjen porukom "Stop lažima", koja je postavljena umesto naslova, tekstova i naziva rubrika. U novembru 2014. izbrisana su tri teksta o spornim doktorskim disertacijama, kao i njihovi prevodi na engleski jezik.

Aprila ove godine, nepoznate osobe postavile su na sajt Peščanika dva teksta od kojih se jedan

istovremeno pojavio i na sajtu dnevnog lista Danas. Uredništvo je zbog ovog napada podnelo krivičnu prijavu protiv N.N. lica zbog neovlašćenog pristupa serveru, falsifikovanja sadržaja i lažnog predstavljanja.

U junu ove godine, sajt je pretrpeo najteži DDoS napad u svojoj istoriji. Prema podacima tehničkog administratora, napad je počeo 'brute force' pretragom SSH protokola – odnosno automatizovanim pokušajima razbijanja sistemske enkripcije kojima se štite kanali između servera i sajta. Iz analize logova administrator je ustanovio da je SSH servis trpeo konstantan napad sa oko 2000 IP adresa. Redakcija je ukazala da je, poređenja radi, u prethodnom velikom napadu na sajt dva meseca ranije učestvovalo 280 IP adresa.

Ovog puta, istovremeno sa napadom na SSH, sa nekoliko stotina IP adresa napadani su i drugi servisi na serveru kao što su FTP, Postfix i mySQL (sistemski protokoli odnosno programi, neophodni za bezbedan rad sajta).

Prema obrazloženju krivične prijave koju je pravni tim Peščanika podneo nadležnom tužilaštvu, zbog nekoliko slojeva zaštite (firewall), svaka IP adresa sa koje je server napadan blokirana je posle trećeg pokušaja. Ceo saobraćaj sajta prolazi kroz mitigacioni centar koji filtrira sve maliciozne pokušaje koje prepozna. Rad sajta nije bio usporen, niti je ovoga puta došlo do upada na sajt, brisanja ili izmene sadržaja, što se desilo prethodna tri puta.

Redakcija je zaključila da cilj umnoženih zahteva kojima je ovom prilikom opterećen server nije mogao doći usled povećane posete redovnim pristupanjem sajtu, već isključivo radi onemogućavanja njegovog rada.

Inače, ovog leta je pravni tim Peščanika dobio prvi odgovor na jednu od tri tužbe podnete protiv NN lica zbog napada na sajt prošle godine, posle objavljivanja tekstova o plagiranim doktoratima i poplavama.

Više javno tužilaštvo je obavestilo pravne zastupnike redakcije da je do sada "uputilo 5 zahteva za prikupljanje potrebnih obaveštenja MUP-u Republike Srbije - SBPOK - Odeljenju za borbu protiv visokotehnološkog kriminala; 2 predloga za izdavanje naloga za lociranje mesta sa kog se obavlja komunikacija". U obaveštenju se dodaje i da je "na osnovu predloga tužilaštva, a po naredbama Višeg suda u Beogradu, izvršen pretres stanova na 2 lokacije u Beogradu i od korisnika stanova je oduzeta elektronska oprema koja je upućena na veštačenje Službi za specijalne istražne metode MUP-a Republike Srbije". U svom obaveštenju, tužilaštvo naglašava da u ovom predmetu "nije doneta Naredba o sprovođenju istrage".

5. MILJANA RADIVOJEVIĆ

Arheološkinja na postdoktorskim studijama u Kembridžu koja predvodi međunarodni tim istraživača arheometalurgije na lokalitetima vinčanske kulture u Srbiji, široj javnosti je postala poznata prošlog leta po analizi doktorske teze tadašnjeg rektora Univerziteta Megatrend, privatne visokoškolske institucije za koju postoje osnovane indicije da je usvajala plagirane doktorate istaknutih funkcionera na vlasti.

Analiza je ukazala da doktorske teze zapravo - nema, a detalji neuspešne potrage objavljeni su na sajtu Peščanika, gde je i započeto otkrivanje plagiranih doktorata sa Megatrenda i drugih fakulteta.

U svoju odbranu, tadašnji rektor Megatrenda optužio je naučnicu za učešće u zaveri protiv njega i ustanove na čijem je čelu, kao i funkcionera čiji su doktorati analizirani, u cilju "urušavanja državnog vrha". Kao dokaz, u emisijama na dve televizije sa nacionalnom frekvencijom javno je čitao delove autorkine prepiske sa njenog privatnog mejla.

Ispostavilo se da je neko neovlašćeno ušao na privatni mejl naučnice, prikupio delove prepiske i sa istog naloga ih poslao na adrese nekoliko većih novinskih agencija. Tadašnji rektor je u emisijama tvrdio da je prepisku dobio od srbijanske sekcije međunarodne hakerske grupe Anonymous. Nekoliko dana kasnije, grupa "Anonymous Srbija" oglasila se demantujući bilo kakvu vezu sa hakovanjem imejl adrese.

Proverom logova o aktivnosti na nalogu elektronske pošte, otkrivena je lokacija sa koje je pristupljeno mejlu kao i da je neovlašćen pristup ostvaren tri puta.

Uz pomoć pravnog tima Share fondacije, nadležnom tužilaštvu podneta je krivična prijava protiv rektora i NN lica zbog krivičnih dela neovlašćenog pristupa zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302 KZ) kao i povrede tajnosti pisma i drugih pošiljki (član 142 KZ) - ili drugog krivičnog dela za koje se gonjenje preduzima po službenoj dužnosti.

RIZICI

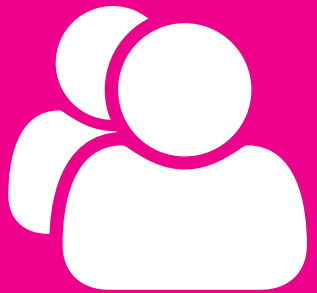
BEZBED-NOST NOVINARA I "DIGITALNA SENKA"

BEZBEDNOST NOVINARA I "DIGITALNA SENKA"

Novinari i građanski medijski akteri, poput blogera, suočavaju se sa različitim rizicima prilikom učešća u javnoj sferi, od pretnji, zastrašivanja i drugih formi uznemiravanja, do nasilja pa i ubistava. Ne samo da su ovi problemi i dalje relativno česti u fizičkom svetu, naročito u manje demokratskim zemljama, već prate medijske aktere i u digitalnom okruženju. Rezolucija Saveta Evrope o bezbednosti novinara, usvojena u Beogradu u novembru 2013. godine, strogo osuđuje "...fizičke napade i nasilje, zastrašivanje, zloupotrebu moći države, uključujući nezakonito nadgledanje komunikacija, i druge oblike maltretiranja novinara, kao i drugih koji doprinose oblikovanju javne debate i javnog mnjenja uživanjem prava na slobodu izražavanja i informisanja"[1]. Ugrožavanje fizičkog i "digitalnog" intergriteta novinara predstavlja veliki izazov, ali je važno napomenuti da fizička zaštita izgleda prilično lako u odnosu na zaštitu nečijih digitalnih poseda. Naime, bilo da ste novinar, bloger, aktivista za ljudska prava, pravnik ili samo "običan" građanin, vi ste mašina koja proizvodi podatke. Ovi podaci koje ljudi proizvode su raštrkani po Internetu, mrežama mobilne telefonije, privatnim IT sistemima, sistemima za video-nadzor i tako dalje, kao "digitalni tragovi"[2] koji mogu da otkriju mnogo detalja o nečijem profesionalnom i privatnom životu ukoliko se vrši njihova agregacija i zajednička obrada. Stoga se može reći da pojedinci poseduju dualni identitet, koji se sastoji od dve "ličnosti", oflajn i onlajn, iako zapravo postoji samo jedna osoba. Ova onlajn ličnost nije pod punom kontrolom osobe koju predstavlja, jer sa njom svako može da stupi u interakciju bez njene dozvole ili znanja. Digitalni identitet i bezbednost je teže

1 Rezolucija Saveta Evrope o bezbednosti novinara, usvojena na Konferenciji ministara za medije i informaciono društvo, Beograd, Srbija, 7-8. novembar 2013, para. 11 (b): https://www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted _ en.pdf

2 Za detaljnije objašnjenje, posetite Me & My Shadow vebsajt: https://myshadow.org/



zaštititi, jer ne postoje samo mnogi izazovi u stvarnom svetu, već i "Pandorina kutija" puna potencijalnih pretnji u sajber prostoru.

Suština digitalne bezbednosti je zaštita istih poseda koje biste inače štitili - za novinare, to su poverljive informacije koje se mogu odnositi na identitet njihovih izvora, procureli poverljivi materijali, planovi za istraživanje itd. Iz toga sledi da su najčešći rizici u digitalnom okruženju, ne samo za novinare, već i za sve koji rade sa osetljivim informacijama (blogeri, aktivisti za zaštitu ljudskih prava, državni funkcioneri, diplomate):

- TRAJNI GUBITAK PRISTUPA PODACIMA. Slučajevi kada vam se hard disk pokvari, telefon slomi ili kada izgubite memorijsku karticu iz kamere. Ovi slučajevi takođe uključuju upade u onlajn naloge, promene šifri i brisanje podataka kako bi se vlasniku naloga onemogućio dalji pristup sadržajima i podacima.
- OTKRIVANJE POVERLJIVIH INFORMACIJA. Slučajevi kada neko dođe u pristup informacijama koje čuvate kao poverljive ili privatne.
- PREKID KOMUNIKACIJE. Slučajevi prekida pristupa sredstvima komunikacije, mreži ili onlajn identitetima, npr. kada dođe do prekida vaše Internet konekcije ili kada vaš telefon nema signal.

U nastavku ćemo dodatno objasniti probleme i predložiti rešenja za poboljšanje digitalne bezbednosti i informacione privatnosti. Treba imati na umu da postoje mnogi aspekti u vezi sa ovom temom, ali ćemo se u ovom izveštaju usredsrediti samo na najvažnije.

LIČNA V. ORGANI-ZACIONA BEZBEDNOST

LIČNA V. ORGANIZACIONA BEZBEDNOST

Kada je reč o digitalnoj bezbednosti novinara, ona se retko posmatra iz persprektive njihove mreže ljudi, tj. kruga osoba sa kojima komuniciraju, među kojima su izvori i kolege svakako najvažniji. Kada postoji samo jedna slaba karika u komunikacionom lancu, posledice po privatnost i bezbednost mogu biti ozbiljne i zbog toga organizaciona bezbednost takođe mora da bude pitanje prioriteta za medije. Na primer, samo jedan upad u mejl nalog je dovoljan da ugrozi mnogo ljudi, zato uvek imajte na umu da se ne radi samo o vama.

Najčešći problemi sa praksama digitalne bezbednosti jesu:

- Tehnički upadi u privatne komunikacije i pristup podacima
- Krađa i oduzimanje opreme
- Nadzor elektronskih komunikacija koji vrše državni organi
- Socijalni inženjering
- Onemogućavanje pristupa sadržaju
- Ugrožavanje sigurnosti u onlajn prostoru

TEHNIČKI UPADI U PRIVATNE KOMUNIKACIJE I PRISTUP PODACIMA

Opšti bezbednosni rizici obuhvataju neovlašćene pristupe putem hakovanja, ubacivanja malicioznog softvera (malware), korišćenja tehnologije za nadzor digitalnih komunikacija u privatne svrhe ili takozvano "curenje" podataka usled neadekvatne zaštite infrormacionog sistema.

Glavne tačke napada, odnosno primarne mete koje napadači ciljaju jesu mejl serveri, uređaji (računari, mobilni telefoni, tableti), nalozi na onlajn platformama (društvene mreže, kolaborativni alati, čet aplikacije...), nosači informacija (fizički hard diskovi, fleš memorije, cloud platforme - Dropbox, Google Drive).

Cilj ovih napada je da se otkriju informacije i podaci koje bi novinari, blogeri, aktivisti i medijske organizacije svakako želeli da zaštite. To može da podrazumeva sledeće informacije:

- NA ČEMU RADITE: planovi i nacrti istraživačkih priča ili kampanja, dokumenta, snimci, beleške itd.

- PODACI KOJE POSEDUJETE: poverljive informacije dobijene od izvora, potencijalni dokazi zloupotreba državnih službenika ili privatnih aktera (kompanije, kriminalci...)
- KO SU VAM SARADNICI: informacije o vašoj mreži kolega, izvora, urednika...
- KUDA SE KREĆETE: informacije o kretanju, dnevnim rutinama, planovima za putovanja u inostranstvo...
- DA LI NEŠTO KRIJETE: informacije iz privatne sfere koje drugi mogu da zloupotrebe.

KONFLIKT: Privatnost i poverljivost komunikacije v. tehnički napadi v. digitalna sigurnost kompanija koje čuvaju vaše podatke.

SREDSTVA ZAŠTITE: Digitalna pismenost, krivično-pravna zaštita kroz domaći pravni poredak i instrumente Budimpeštanske konvencije o visokotehnološkom kriminalu, pouzdani pružaoci i kvalitetne usluge informacionog društva, enkripcija sadržaja

KO JE ODGOVORAN: Internet i telekomunikacione kompanije, pružaoci usluga informacionog društva, organizacije nadležne za upravljanje Internetom (Internet governance), države, vaša organizacija i IT podrška, pojedinci za vlastiti sadržaj

KRAĐA I ODUZIMANJE OPREME

Jedan od mogućih scenarija čine krađa ili oduzimanje opreme po nalogu državnih organa (policije, tužilaštva, suda). Iako policijsko pretresanje redakcija nije toliko česta pojava u Srbiji, ne treba je potpuno isključiti. Ovo napominjemo zbog slučaja portala Klix.ba iz susedne Bosne i Hercegovine, čije je prostorije policija pretresla krajem prošle godine posle objavljivanja audio-snimka premijerke Republike Srpske Željke Cvijanović, i tom prilikom oduzela predmete i uništila deo opreme.[3] Kada je reč o krađi uređaja poput laptopova, tableta, telefona ili kamera, ukoliko počinilac poseduje dovoljna tehnička znanja, neće mu predstavljati problem da dođe do informacija zaštićenih običnom šifrom, poput one koju imate na log on ekranu operativnog sistema. Enkripcija hard diskova je stoga veoma važna ukoliko želite da pristup poverljivim podacima imaju samo ovlašćena lica, čak i u slučaju fizičke krađe.

SREDSTVA ZAŠTITE: napredne tehnike enkripcija, pravljenje rezervnih kopija podataka (data backup)

KO JE ODGOVORAN: Korporacije, IT podrška, pojedinci za svoje uređaje i podatke

3 O slučaju portala Klix.ba možete pročitati ovde: http://www.klix.ba/vijesti/bih/ko-su-glavni-akteri-koji-su-naredili-i-odobrili-pretres-portala-klix-ba/141230118

NADZOR ELEKTRONSKIH KOMUNIKACIJA KOJI VRŠE DRŽAVNI ORGANI

Rizik koga treba biti svestan prilikom rada sa poverljivim informacijama jeste moguće presretanje komunikacije od strane državnih organa (policija i bezbednosne službe). Prema pravnom okviru Srbije, tajnost sredstava komunikacije je zagarantovana Ustavom, i od te garancije se može odstupiti samo u slučajevima vođenja krivičnog postupka ili zaštite nacionalne bezbednosti, na način predviđen zakonom uz odluku suda. Takođe, nadzor putem video-kamera i sličnih sredstava u fizičkom prostoru može predstavljati narušavanje privatnosti, posebno jer oblast video-nadzora nije regulisana trenutno važećim Zakonom o zaštiti podataka o ličnosti.

Problem koji je neophodno što pre rešiti jeste potpuno odsustvo kontrole tržišta opreme za nadgledanje i presretanje elektronskih komunikacija. Privatni akteri mogu na jednostavan način i bez ozbiljne kontrole da nabave opremu i vrše aktivnosti nadgledanja za koje su nadležni isključivo državni organi, tj. bezbednosne agencije i policija u usko propisanim slučajevima na osnovu odluke Suda, čime je privatnost komunikacije građana Srbije dodatno ugrožena.

Međutim, podaci o komunikaciji koji zajedno otkrivaju daleko više informacija od samog sadržaja jesu tzv. metapodaci (metadata). Objašnjeno na primeru telefonskog razgovora, to su podaci o tome koji broj ste zvali, ko je vas zvao, u koje vreme, koliko je trajao razgovor i slično. Prema Zakonu o elektronskim komunikacijama, operatori su dužni da ove podatke čuvaju 12 meseci. Pažljivim kombinovanjem velike količine ovih podataka može se dobiti kompletan digitalni profil određene ličnosti: lokacija, dnevne rutine, mreža ljudi, izvori informacija, interesovanja. Pristup ovim podacima predstavlja veoma intruzivnu meru kojom se odstupa od garancije tajnosti sredstva komunikacije, te se zbog toga akteri u javnom i privatnom sektoru koji čuvaju ove podatke moraju pridržavati procedura propisanih Zakonom o zaštiti podataka o ličnosti. Poverenik za informacije od javnog značaja je 2012. godine u postupku sprovođenja nadzora nad operatorima mobilne i fiksne telefonije, došao je do zabrinjavajućih podataka o nezakonitom pristupanju državnih organa metapodacima. Tada je utvrđeno da je kod samo jednog operatora, tokom jedne godine, MUP direktno pristupio

podacima o komunikaciji korisnika više od 270 000 puta.[4]

KONFLIKT: Privatnost v. bezbednost

SREDSTVA ZAŠTITE: Međunarodni standardi ljudskih prava, watchdog inicijative [5]

KO JE ODGOVORAN: Države, policija, tajne službe, pravosuđe, operatori elektronskih komunikacija

SOCIJALNI INŽENJERING

Taktika koja se takođe može koristiti za prikupljanje poverljivih informacija od novinara ili njihovih izvora jeste socijalni inženjering, odnosno korišćenje psiholoških trikova i manipulacije kako bi se prikupile informacije ili na prevaru pristupilo informacionom sistemu. Često je to jedan od mnogih koraka u okviru složenijih planova za prevaru. Na primer, novinar[6] može dobiti mejl sa adrese koja naizgled deluje kredibilno i "dokumentom poverljive sadržine" u prilogu, koji zapravo predstavlja virus, ili mejl od lažnog izvora koji želi da sazna informacije od novinara u vezi sa njegovim radom. Anonimnost i neverifikovani kontakt podaci omogućavaju čak i da se pojedinac lažno predstavi kao novinar u cilju ispunjavanja skrivenih agendi. Neretko zbog niza različitih okolnosti može doći i do "zloupotrebe poverenja" (npr. "curenje" informacija od bivšeg nezadovoljnog kolege) što može da izazove posebne probleme.

KONFLIKT: Poverenje v. anonimnost

SREDSTVA ZAŠTITE: Nacionalno krivično pravo, verifikacija identiteta (enkripcija/potpisivanje mejlova)

KO JE ODGOVORAN: Države, korporacije, IT podrška, pojedinci

ONEMOGUĆAVANJE PRISTUPA SADRŽAJU

U većini slučajeva, sigurnost sadržaja objavljenog na nekoj onlajn platformi je povezana sa bezbednosnim praksama same platforme. Najčešći rizici su opterećivanje servera DDoS (Distributed Denial of Service) napadima, tj. zagušivanje servera na kome je sajt onlajn medija hostovan slanjem ogromnog broja zahteva za pristup u isto vreme.[7] Još jedan od načina da se naruši integritet sadržaja njegovom izmenom ili uklanjanjem jesu napadi na baze podataka sajta onlajn medija ubacivanjem malicioznog koda, kako bi se kompromitovao sadržaj baze (tzv. SQL Injection). [8]

Dodatni načini da se određeni sadržaj donekle učini nedostupnim a koji su legalni, za razliku od opisanih, jesu podnošenje zahteva po osnovu "prava na zaborav" (right to be forgotten) ili procedure za uklanjanje sadržaja po prijavi (notice-and-takedown). "Pravo na zaborav" je za sada moguće na teritoriji Evropske unije na osnovu odluke Suda pravde EU u predmetu poznatom kao Gugl protiv Španije.[9] Ova presuda omogućava građanima EU da od servisa za pretraživanje (npr. Gugl) zatraže uklanjanje informacija koje nisu istinite ili relevantne, doduše samo iz rezultata pretrage a ne sa samih sajtova gde su objavljene. Kada je reč o proceduri za uklanjanje sadržaja po prijavi, ona se najčešće primenjuje u slučajevima kada se od neke platforme traži da ukloni određeni sadržaj po nekom pravnom osnovu (npr. kršenje autorskih prava).

KONFLIKT: Slobodan pristup informacijama v. arhitektura mreže

SREDSTVA ZAŠTITE: Budimpeštanska konvencija o visokotehnološkom kriminalu, nacionalni pravni okvir

KO JE ODGOVORAN: Organizacije nadležne za upravljanje Internetom (Internet governance), države, korporacije, Hosting & IT podrška

UGROŽAVANJE SIGURNOSTI U ONLAJN PROSTORU

Ugrožavanje sigurnosti novinara, koje se u oflajn svetu manifestuje

4 Istraživanje dostupno na: http://labs.rs/sr/nevidljive-infrastrukture-elektronski-nadzor-i-zadrzavanje-podataka-sa-mobilnih-telefona/

5 Kao primer izdvajamo 12 međunarodnih principa primene standarda ljudskih prava na nadzor komunikacija, koji su dobili podršku više od 400 organizacija širom sveta među kojima je i Share fondacija: https://en.necessaryandproportionate.org/

6 Treba spomenuti slučaj novinarke Dragane Pećo, u čije ime je nepoznato lice slalo zahteve za pristup informacijama od javnog značaja sa lažne mejl adrese: http://www.cins.rs/srpski/news/article/saopstenje-za-javnost-783

7 Za više o DDoS napadima videti: http://www.digitalattackmap.com/understanding-ddos/

8 Za više o SQL Injection napadima videti: https://www.acunetix.com/websitesecurity/sql-injection/

9 Tekst odluke dostupan na: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

10 IWMF, Violence and Harassment against Women in the News Media: A Global Picture / Intimidation, Threats, and Abuse: http://www.iwmf.org/intimidation-threats-and-abuse/

pretnjama, sve više uzima maha na Internetu, a posebno na društvenim mrežama, usled mogućnosti da se pretnje upute anonimno. Procenjuje se[10] da se više od četvrtine pretnji i zastrašivanja novinarima upućuje onlajn, dok su novinarke tri puta više izložene verbalnom nasilju na internetu od svojih kolega. Predstavnica OEBS za slobodu medija Dunja Mijatović pozvala je zemlje članice[11] da preduzmu ozbiljne korake za stvaranje bezbednijeg okruženja za rad onlajn novinarki. Glavni ciljevi ove vrste napada jesu zastrašivanje radi odvraćanja od izveštavanja o određenim temama, javno izlaganje poruzi i podsticanje ili opravdavanje fizičkih napada na novinare. Ovo se može postići otvorenim pretnjama, objavljivanjem privatnih informacija, poput adrese, imena ili fotografija članova porodice, govorom mržnje, uvredama koje podstiču na nasilje, uznemiravanjem na društvenim mrežama i sl. Kada govorimo o nešto "suptilnijim" taktikama, treba spomenuti narušavanje reputacije novinara i angažovanje hakera.

KONFLIKT: Sloboda izražavanja i anonimnost v. prava ličnosti i kvalitet informacija

SREDSTVA ZAŠTITE: Međunarodni standardi ljudskih prava, nacionalni pravni okvir, samoregulacija

KO JE ODGOVORAN: Internet zajednica, države, korporacije, pojedinci

KO TREBA DA UŽIVA ZAŠTITU? KO VRŠI NOVINARSKU FUNKCIJU U DRUŠTVU?

Iako se do skoro nije uzimalo u obzir da bi pored profesionalnih novinara, i drugi akteri koji imaju značaju ulogu u javnom diskursu trebalo da uživaju dodatnu zaštitu od napada i pretnji, nedavni događaji[12] ukazuju na potrebu da se ozbiljno razmisli o tome. Takođe, kada govorimo isključivo o zakonskom okviru, u Srbiji ne postoji definicija novinara, te u formalno-pravnom smislu ne možemo definisati profesionalnog novinara. Upravo ta činjenica dodatno otežava zauzimanje stava o tome ko treba da uživa zaštitu. Smatramo da su pored profesionalnih novinara akteri koje treba uzeti u obzir onlajn i građanski mediji, blogeri, watchdog organizacije i civilno društvo, ali pod određenim okolnostima i građani Interneta prepoznatljivi u onlajn zajednici. U prilog tome govori i stav Saveta Evrope da i akterima koji nisu u potpunosti kvalifikovani kao mediji, a mogu se smatrati delom medijskog ekosistema koji doprinosi društvenoj funkciji medija, mogu biti priznate određene privilegije karakteristične za novinare. [13]

11 Videti communique Predstavnice OEBS za slobodu medija o porastu ugrožavanja sigurnosti novinarki u onlajn okruženju: http://www.osce.org/fom/139186?download=true

12 Stiče se utisak da u Srbiji postoji "selektivna zaštita" pojedinaca od pretnji na internetu: http://www.shareconference.net/sh/blog/selektivna-zastita

13 Rezolucija Saveta Evrope o bezbednosti novinara, usvojena na Konferenciji ministara za medije i informaciono društvo, Beograd, Srbija, 7-8. novembar 2013, para. 9: https://www.coe.int/t/dghl/standardsetting/media/belgrade2013/Belgrade%20Ministerial%20Conference%20Texts%20Adopted _ en.pdf

POSLEDICE

POSLEDICE

NESIGURNOST I STRAH

U prethodnom delu imali ste priliku da se upoznate sa slučajevima iz prethodne godine, kao i sa rizicima koji se mogu javiti u digitalnom okruženju. Postavlja se zatim pitanje koje su prave posledice sajber napada na onlajn medije i novinare u Srbiji. Većina slučajeva nestanka sadržaja sa Interneta i DDoS napada nije imala dugoročnije posledice na sam sadržaj, što ne znači da drugih vrsta posledica nema. Kao što je Džon Gilmor, jedan od osnivača organizacije Electronic Frontier Foundation (EFF), objasnio: "Mreža tumači cenzuru kao grešku i zaobilazi je". Sadržaj koji je uklonjen sa mreže se obično samo umnožava na različitim mestima, prenosi na drugim blogovima i onlajn medijima, pri čemu oznaka cenzurisanog ili na drugi način ugroženog sadržaja privlači još više pažnje i donosi još više čitalaca. U nastavku ćemo izneti moguće posledice opisanih napada i njihov uticaj na nezavisnost i sigurnost onlajn i građanskih medija.

Glavna posledica ovakvih napada jeste izazivanje nesigurnosti i straha, što stvara "chilling effect"[14] na slobodu izražavanja u onlajn okruženju. Činjenica da objavljivanje sadržaja kojim se kritikuju strukture moći (država, kriminalne grupe ili druge strukture) može da dovede do uništenja, blokiranja i privremenog nestanka sajtova, praćenih velikim stresom i količinom radnih sati potrošenih na popravljanje sistema, što svakako može uticati na volju za slobodom izražavanja. U sajber prostoru, troškovi odbrane su u većini slučajeva mnogo viši od troškova samog napada, stoga se može reći da verovatno ne postoji efikasan i pouzdan način zaštite od ovakvih vrsta napada koji se unapred mogu predvideti. To svakako može biti veoma obeshrabrujuće za male i nezavisne onlajn i građanske medije, koji nisu u mogućnosti da priušte skupe eksperte za sajber bezbednost i tehnička rešenja da se zaštite.

14 "Chilling efekat" je pravna kovanica koja se može objasniti kao obeshrabrivanje legitimnog i dozvoljenog ispoljavanja nekog prava pretnjom ili stavljanjem u izgled neke pravne sankcije. Nastala je u pravnoj teoriji SAD i vezuje se prevashodno za ugrožavanje slobode izražavanja: http://www.shareconference.net/sh/blog/ciling-efekat-presude-protiv-dva-forumasa-u-slucaju-malagurski-da-li-je-sloboda-izrazavanja-na

OBESHRABRIVANJE JAVNOG DIJALOGA - "CHILLING EFFECT"

Hapšenje pojedinaca zbog njihovih blogova, komentara ili drugih formi izražavanja u onlajn prostoru ima "chilling effect" ne samo na novinare i onlajn medije, već i na čitavu populaciju korisnika Interneta, što u Srbiji obuhvata oko 60% građana. Kod građana se stvara osećaj nedovoljnih sloboda i zaštite u digitalnom okruženju, što negativno utiče na slobodno izražava- nje mišljenja na Internetu. Fokusiranje tradicionalnih medija na slučajeve privođenja, pritvaranja i daljeg pravnog procesuiranja građana koji su na blogovima i društvenim mrežama kritikovali i komentarisali političku realnost, iz ugla državne sile a ne građanskih sloboda, svakako podstiče ovakvu percepciju u javnosti.

KRŠENJE PRAVA NA PRIVATNOST I NADGLEDANJE

Ciljani napadi na ličnu i profesionalnu komunikaciju, kao što su mejlovi, onlajn dokumenti i baze podataka, mogu da ugroze anonimnost izvora, otkriju istaživačke planove i budu zloupotrebljeni za ucenjivanje i diskreditaciju žrtve napada objavljivanjem privatnih informacija, kao i za krađu identiteta. Postizanje neophodnog stepena digitalne bezbednosti često zahteva kompleksne procedure, izmenu postojećih navika koje su povezane sa tehnologijom, što utiče na efikasnost novinarskog poziva i same medijske organizacije.

MANIPULACIJA JAVNIM MNJENJEM POMOĆU TEHNOLOGIJE

U digitalnom okruženju posebno su usavršene tehnike za manipulaciju javnim mnjenjem, zloupotrebom softvera i drugih alata za potrebe političkih partija ili komercijalnog sektora, i drugih interesnih krugova. Poplave komentara, statusa i lajkova na novinskim portalima i socijalnim mrežama, menjaju prostor otvoren za dijalog i slobodu izražavanja, čime se kreira lažna slika javnog mnjenja. Ovaj veštački izazvan "šum" dovodi do toga da se autentični glasovi pojedinaca ne mogu čuti, što obeshrabruje dijalog o temama koje su značajne za društvo.

Jedna od inicijativa Share fondacije, pokrenuta zajedno sa 200 uglednih nacionalnih organizacija i eksperata, jeste Deklaracija o poštovanju Internet sloboda u političkoj komunikaciji.[15] U Deklaraciji se ističe da slučajevi cenzure na Internetu, napadi na sajtove i privatne naloge predstavljaju kršenje ljudskih prava i da su u suprotnosti sa Ustavom Republike Srbije i njenim zakonima.

15 Tekst Deklaracije: http://deklaracija.net/

ZAKLJUČAK

ULOGA DRŽAVE

Neophodno je pozabaviti se i ulogom države u ovakvim slučajevima. Kakva je korelacija između sadržaja, političkog konteksta i samih napada? U većini slučajeva u Srbiji, napadnuti su sajtovi koji se kritički odnose prema vlasti, objavljuju tekstove koji otkrivaju korupciju i ističu neefikasnost vlade i članova vladajuće stranke.

Neophodno je naglasiti da ne postoje čvrsti dokazi koji ukazuju da bilo koje vladino telo ili politička partija stoje iza sajber napada na onlajn medije. Sama priroda tih napada i struktura mreže su takvi da je nezavisnim istraživačima gotovo nemoguće da proprate ovakve napade, dok se napadači obično kriju iza anonimnosti i mnoštva kompjutera korišćenih za napad tzv. bot mrežama iz drugih država. Čak i ukoliko postoji trag koji ukazuje na pojedinca, "black hat"[16] hakera ili organizacije, veoma je teško utvrditi ko je naručilac napada. Takođe, ovakvi napadi ne čine zvaničnu politiku cenzure Interneta koje sprovode vlade u obliku Internet filtriranja i blokiranja sadržaja, kao što je to slučaj u Kini ili Turskoj.

Na osnovu iskustva iz prethodne dve godine, možemo sa sigurnošću reći da država nije izgradila poverenje da može uspešno zaštititi onlajn medije i građanske novinare u Srbiji. Svesni smo da određeni državni organi imaju ograničene ljudske i organizacione kapacitete što utiče na efikasnu reakciju u pojedinim situacijama. Međutim, prava opasnost leži u diskreciji državnih organa (tužilaštva, policije i sudstva) da različito tretira slučajeve ugrožavanja prava u onlajn okruženju.

U većini slučajeva sajber napada na onlajn medije, istraživačke novinare i građanske medije koji kritikuju vladu, mogli smo da primetimo veoma sporo reagovanje ili potpuno odsustvo reakcije državnih organa. U protekloj godini, Share fondacija je preuzela aktivnu ulogu u monitoringu i sprovođenju sajber forenzičkih analiza napada na onlajn medije, čije rezultate dostavlja nadležnim organima i javno objavljuje kada to nije u suprotnosti sa interesima sprovođenja istrage. Međutim, nijedan od bitnijih slučajeva nije doveo do identifikacije i hapšenja osumnjičenih, dok su se očekivane

16 Hakeri koji traže bezbednosne propuste u informacionim sistemima kako bi ih iskoristili za ličnu finansijsku dobit ili u druge maliciozne svrhe: https://www.techopedia.com/definition/26342/black-hat-hacker

reakcije svodile na poneku izjavu nadležnih organa. Ovakva praksa sve više urušava poverenje građana i onlajn medija u zaštitu koju je država dužna da pruži.

S druge strane, nadležni organi su se pokazali kao veoma efikasni u slučaju hapšenja i samog sudskog postupka protiv korisnika društvenih medija i blogera (slučaj Malagurski i slučajevi izazivanja panike tokom poplava). Direktne posledice se ogledaju u nedostatku pravne sigurnosti u ovoj oblasti i nezadovoljavajućem nivou vladavine prava.

ŠTA BI TREBALO DA SE URADI?

Pretnje po slobodu govora i privatnost u digitalnom okruženju, kao i sigurnost novinara i pojedinaca moraju se posmatrati kao prioriteti. Republika Srbija je dužna da razvije efikasnije mehanizme za zaštitu novinara i medija, kao i da istovremeno izgradi kapacitete za onlajn medije kako bi se zaštitili od sajber napada, koliko god je to moguće.

Formalno i neformalno obrazovanje na temu sajber bezbednosti, privatnosti i slobode izražavanja u digitalnom okruženju za široku publiku i specifične ciljne grupe takođe su neophodni, kako bi se unapredila bezbednost i dosledno poštovala ljudska prava i u digitalnom okruženju.

Obuke u pravosuđu, harmonizacija zakona i regulatorna reforma neohodni su kako bi se akteri upoznali sa novim oblicima kršenja osnovnih ljudskih prava (sloboda izražavanja, pravo na slobodan pristup i razmenu informacija, pravo na privatnost) i novim formama pritiska na pojedince i medijske organizacije.

Potrebe države i bezbednosnog aparata (policija, službe bezbednosti...) da odgovore na nove vrste pretnji u sajber svetu ne bi smele da budu izgovor za uspostavljanje disproporcionalnih mera nadzora elektronskih komunikacija, Internet cenzuru ili neke druge forme sajber policijske države.

PREDLOŽENI KORACI

Da bi sloboda izražavanja u digitalnom prostoru Srbije bila unapređena i poštovana, svaki od relevantnih aktera bi trebalo da preduzme odgovarajuće korake, kako bi se rizici i njihove posledice svele na najmanju moguću meru. Za neke korake je neophodna kooperacija šireg kruga aktera, dok drugi zahtevaju samostalno angažovanje svakog pojedinca i organizacije u skladu sa sopstvenim resursima i organizacionim mogućnostima. Tako sama Republika Srbija treba da preuzme niz mera kako bi poboljšala postojeće stanje i unapredila našu digitalnu budućnost:

REGULATORNA REFORMA: HARMONIZACIJA I IMPLEMENTACIJA PROPISA

- Usvajanje Zakona o informacionoj bezbednosti i implementacija Budimpeštanske konvencije o visokotehnološkom kriminalu u skladu sa međunarodnim standardima ljudskih prava, a posebno Evropskom konvencijom o ljudskim pravima i odlukama Evropskog suda za ljudska prava;
- Unapređenje regulatornog okvira kontrole nad trgovinom opreme i softvera za nadzor elektronskih komunikacija;
- Uspostavljanje mehanizama kontrole sprovođenja mera elektronskog nadzora isključivo uz sudsku odluku;
- Implementacija u nastavku predloženih mera kroz Akcione planove za poglavlja 23 i 24.

IZGRADNJA KAPACITETA I PROMENA PRIORITETA

- Treninzi za pripadnike pravosuđa u oblasti primene međunarodnih standarda ljudskih prava u digitalnom okruženju;
- Podizanje ljudskih i organizacionih kapaciteta policije i tužilaštva za borbu protiv visokotehnološkog kriminala;
- Uspostavljanje funkcionalnog Nacionalnog centra za hitne slučajeve (CERT - Computer Emergency Response Team);
- Podrška uspostavljanju funkcionalne mreže CERT-ova i organizacija zaduženih za brzu reakciju i podršku različitim ciljnim grupama;
- Prioritetno rešavanje slučajeva ugrožavanja slobode izražavanja, informacione privatnosti i digitalne bezbednosti građanskih novinara i onlajn medija od strane policije i tužilaštva;
- Saradnja jedinica za borbu protiv visokotehnološkog kriminala sa ostalim jedinicama policije i upotreba redovnih istražnih tehnika zajedno sa prikupljanjem digitalnih dokaza.

MEĐUNARODNA SARADNJA I UČEŠĆE U SAMOREGULATORNIM I KOREGULATORNIM PROCESIMA

- Unapređenje saradnje na međudržavnom nivou u cilju rešavanja slučajeva visokotehnološkog kriminala;
- Izgradnja dobrih odnosa i saradnja sa međunarodnim regulatornim telima, organizacijama koje upravljaju Internetom i velikim Internet kompanijama;
- Unapređenje mehanizama koregulacije i dalje podsticanje samo-

regulacije u oblastima regulisanja sadržaja i upravljanja mrežama;

- Prepoznavanje i poštovanje Internet kulture i društvenih normi koje važe u Internet zajednici od strane pravosudnih organa u njihovom postupanju.

DIGITALNA PISMENOST

- Osposobljavanje pojedinaca i organizacija da se aktivno služe tehnologijom i sistemom zaštite osnovnih ljudskih prava u digitalnom okruženju, kako bi obezbedili slobodu izražavanja, okupljanja i organizovanja, zaštili informacionu privatnost i unapredili digitalnu bezbednost;
- Podsticanje upotrebe tehnoloških inovacija na osnovama aktivne participacije i kolaboracije radi osnaživanja kreativne i inovativne medijske i informacione produkcije.

MONITORING REZULTATI I ANALIZE

Detaljne monitoring izveštaje i analize možete pronaći na:

- www.sharedefense.org
- www.shareconference.net
- www.labs.rs

SHARE FOUNDATION - 2015