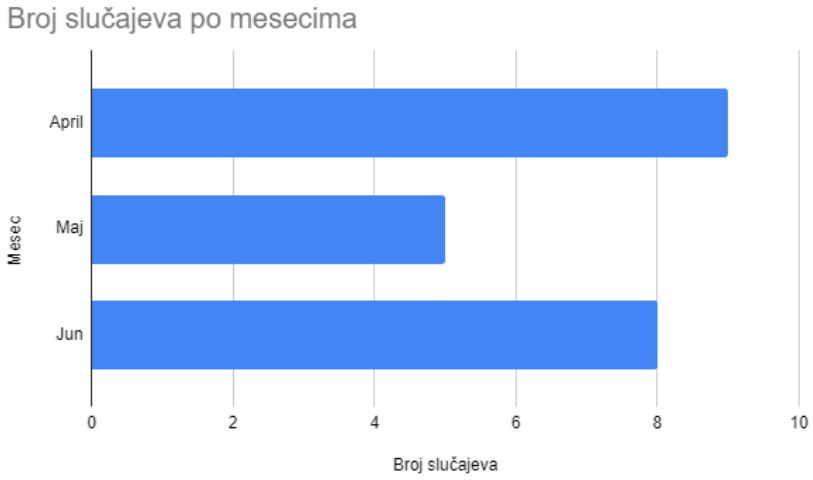
Monitoring izveštaj april - jun 2021: nespretna digitalizacija, fišing i pritisci

Novi kvartalni monitoring izveštaj obuhvata stanje digitalnih prava i sloboda u Srbiji za period od aprila do kraja juna 2021. U ovom periodu naročito su se istakli problemi nespretno uvedene digitalizacije, prevare građana kroz fišing kampanje, kao i pritisci u vidu strateških tužbi protiv medija, pretnji, a u jednom slučaju čak i privođenja zbog tvita.



SHARE FOUNDATION

Opasnosti nespretne digitalizacije

U želji da se građanima omogući i olakša obavljanje administrativnih obaveza, digitalizacija javne uprave u Srbiji poslednjih godina postaje jedno od dostignuća kojima se država naročito hvali. Međutim, iskustvo je pokazalo da kada se digitalizacija sprovodi nespretno, odnosno bez uzimanja u obzir rizika po podatke građana i informacionu bezbednost sistema, šteta postaje evidentna a koristi nesigurne.

Posle prošlogodišnjeg incidenta sa curenjem pristupnih kredencijala za Informacioni sistem Covid-19, najosetljiviju bazu podataka u državi u trenutku kada je pandemija korona virusa bila u jeku, stekao se utisak da se ovakvi incidenti uglavnom dešavaju zbog pojedinačnih propusta. Odgovornost gotovo po pravilu izostaje, a najveće žrtve nespretne digitalizacije su svaki put građani, koji ne samo što su žrtve kompromitacije podataka i informacionih sistema, već su takođe prinuđeni da refrešuju stranice, besomučno pokušavaju da se uloguju ili odustanu od "digitalizacije" i krenu po šalterima sa fasciklama i papirima.

Najnoviji incident sa podacima o ličnosti pogodio je naročito ranjivu populaciju, maturante osnovnih škola. U prelasku na digitalno školstvo, kreiran je portal Moja srednja škola, sa ciljem da objedini sve informacije i postupke u vezi sa upisom u srednje škole u Srbiji. Sajt je najpre postao nedostupan u nedelju 27. juna usled preopterećenja, pa je rok za prigovore na rezultate završnih ispita morao da bude produžen. Onlajn zajednica je istražila malo dublje sajt radi mogućih uzroka nefunkcionalnosti i tada je otkriveno da se kroz kod moglo pristupiti imenima i prezimenima osnovaca, te nazivu osnovne škole koju su pohađali, njihovim ocenama u 6, 7. i 8. razredu i rezultatima završnog ispita. U slučaju da neko dođe na ideju da neovlašćeno formira bazu sa svim ovim podacima, mogao bi da

profiliše čitavu jednu generaciju, recimo prilikom konkurisanja za poslove u budućnosti. Još jednom se pokazalo da su bezbednost podataka i integritet državnih informacionih sistema naknadna misao, koja postaje aktuelna tek kada se dogode incidenti.

Na sajtu Kancelarije Vlade Srbije za informacione tehnologije i elektronsku upravu početkom juna je objavljeno saopštenje o "Pametnoj Srbiji", novoj državnoj platformi za masovnu obradu podataka, donošenje odluka i osmišljavanje strategija. Ono što je naročito zanimljivo jeste da najava nije bila previše propraćena u javnosti, iako je reč o potencijalno veoma osetljivom sistemu koji može da sadrži razne zbirke podataka o građanima koje država može da prikupi. "Cilj je integrisati sve višestruke tokove informacija iz različitih organa javne uprave na lokalnom i državnom nivou", navodi se u saopštenju.

"Pametna Srbija" će koristiti tehnologije kompanije Majkrosoft i nalaziće se u Državnom data centru u Kragujevcu, što ponovo podstiče na razmišljanje o rizicima u vezi sa centralizacijom podataka koje država ima o građanima, kako ti podaci mogu da se koriste i šta sve može da pođe naopako ako dođe do bezbednosnih propusta.

Internet prevare

Kategorija narušavanja informacione bezbednosti broji nekoliko slučajeva i to iz potkategorije računarskih prevara. Javnost je krajem maja saznala za šemu izdavanja lažnih potvrda o negativnom rezultatu PCR testiranja na prisustvo korona virusa. Novinari N1 su stupili u kontakt sa osobom koja je navodno mogla

da im “završi” negativan test. Ubrzo su dobili odgovor da pošalju ime, prezime, JMBG i datum za koji je potreban test i uplate 4000 dinara na račun fizičkog lica. Vladina Kancelarija za informacione tehnologije i elektronsku upravu (ITE) ubrzo je potvrdila da su potvrde dobijene na taj način lako proverivi falsifikati. Samo nekoliko dana nakon otkrivene prevare, uhapšen je muškarac osumnjičen da je izdavao lažne potvrde o PCR testiranju i registrovao lažne domene servisa eUprava i Republičkog fonda za zdravstveno osiguranje.

Građani su se kao mete računarskih prevara našli kada su dobili lažne mejlove od Pošte Srbije, u kojima se navodi da je nastao zastoj u isporuci paketa zbog neplaćene carine, te je poslat link do stranice na kojoj je trebalo uneti podatke sa platne kartice radi plaćanja lažne carine, sa ciljem krađe finansijskih informacija od građana. Fišing kampanja iznude usmerena na korisnike u Srbiji desila se i kada je građanima na lošem srpskom stigao mejl u kome napadač tvrdi da je dobio pristup uređaju primaoca poruke i kamerom snimio intiman video te osobe. Napadač je zatim tražio novčanu naknadu u bitkoinima da ne objavi video. Rajfajzen banka takođe je upozorila svoje klijente u Srbiji na prevaru mejlovima koji navodno dolaze sa adrese podrške banke. U lažnom mejlu zatraženo je da korisnici ažuriraju njihove podatke u bankarskom sistemu zbog “neobičnih aktivnosti” na njihovom računu.

Pored prevara mejlovima, građani su targetirani i SMS porukama, u kojima su dobijali linkove ka navodno “najboljem porno sadržaju u regionu”. Ovakve poruke se tipično koriste za prevare i naplaćivanje dodatnih usluga koje korisnici nisu tražili. Još jedan slučaj kompjuterske prevare, zajedno sa nedozvoljenom obradom podataka o ličnosti, jeste i slučaj zloupotrebe podataka bivšeg ministra na Fejsbuku. Naime, lažni Fejsbuk nalozi kreirani sa fotografijom bivšeg ministra

odbrane Srbije Dragana Šutanovca su korišćeni za takozvane “romansa prevare”, u kojima su žene navođene na onlajn veze radi iskorišćavanja.

Suspendovanje stranica, neproverene informacije i širenje zavera

Kada je reč o manipulacijama u digitalnom okruženju, zapažena su četiri slučaja iz te kategorije, od čega su se dva slučaja ticala suspendovanja stranica na društvenim mrežama, a nakon organizovanog prijavljivanja. Tako je Jutjub kanal Danas konferens centra, koji vodi novinar Željko Pantić, suspendovan nakon neosnovanih prijava za kršenje autorskih prava koje je podnela Arena sport, sportska TV mreža u okviru grupe Telekoma Srbija. Pantić je poznat po kritici predsednik Srbije Aleksandra Vučića i vladajuće stranke. Još jednom kritičaru vlasti, karikaturisti Dušanu Petričiću, Fejsbuk je nakon prijavljivanja nepovratno ukinuo stranicu “Karikature Dušana Petričića”. Iako je stranica i dalje vidljiva na toj mreži, Petričić je naveo da ni on ni njegova saradnica više ne mogu da joj pristupe.

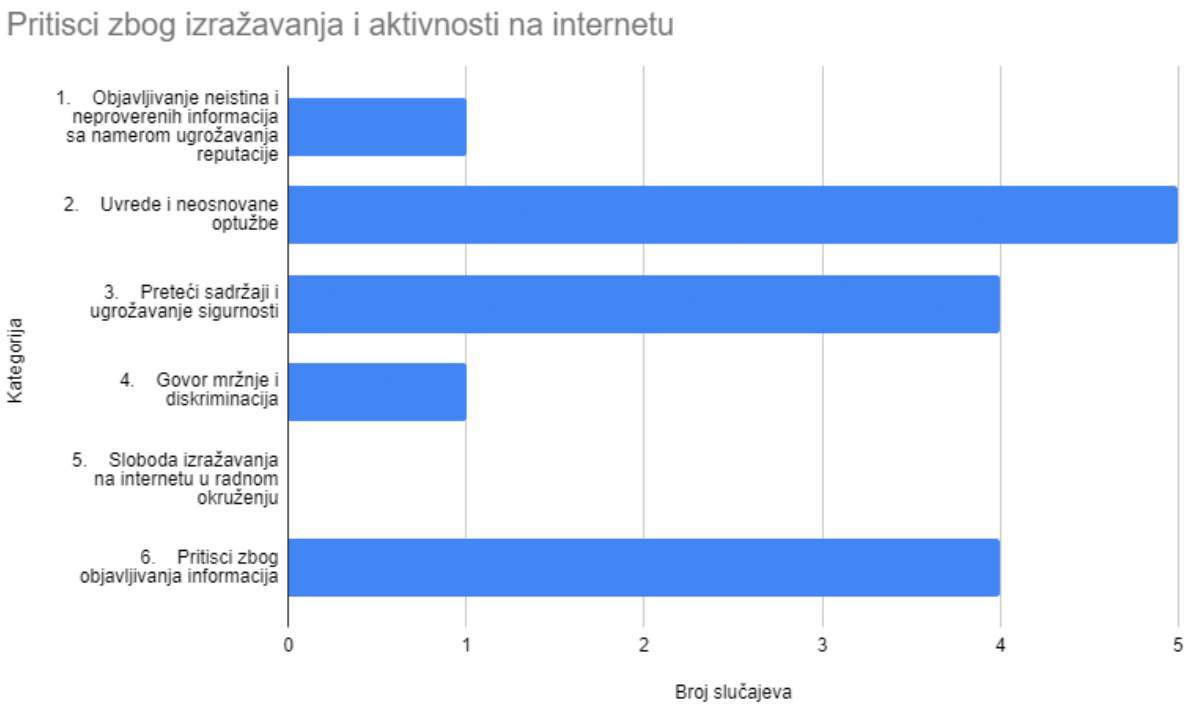
Dva slučaja koji spadaju u potkategoriju drugih manipulacija ticala su se prenošenja satire kao vesti u mnogim onlajn medijima i teorija zavere. Brojni mediji u Srbiji preneli su kao vest tekst o navodnom lažnom svešteniku koji je varao ljude širom Bosne, a izvor informacije bila je Bijeljina njuz, satirični portal. Pored ovog, u spomenutu potkategoriju spada i slučaj širenja zavera o COVID-19 vakcini. Naime, bivša ministarka zdravlja Nada Kostić je na Fejsbuku objavila

teoriju zavere o COVID-19 vakcini proizvođača Fajzer-Biontek, tvrdeći da je u pitanju “vojno oružje”.

Konstantne pretnje novinarima i pritsci na medije

Najčešće zabeležena kategorija povreda u monitoringu, pritisci zbog izražavanja i aktivnosti na internetu, uglavnom se ticala pretnji i pritisaka na novinare i redakcije. Tako su pojedinim novinarima upućivane pretnje smrću na Instagramu, pretnje na Fejsbuk postovima, kao i brojne uvrede i pretnje putem društvenih mreža.

Jedan oblik pritiska zbog objavljivanja informacija, primećen i u prethodnom periodu monitoringa, jesu tužbe upućene medijima. Ono što je tipično za ove tužbe jeste da su strateški podnete da zastraše medije i druge aktere koji deluju u javnom interesu da odustanu od izveštavanja o nekom problemu ili angažmana po nekom društvenom pitanju i u svetu su poznate kao SLAPP tužbe. Privatna kompanija Milenijum tim tužila je nekoliko medija, uključujući Jugpress, Info Vranjske, N1 i Nova.rs, nakon što su preneli izjave sa dve konferencije za medije opozicione Narodne partije održane u februaru. Milenijum tim u svakoj od tužbi traži naknadu štete od po 100.000 evra za povredu ugleda.



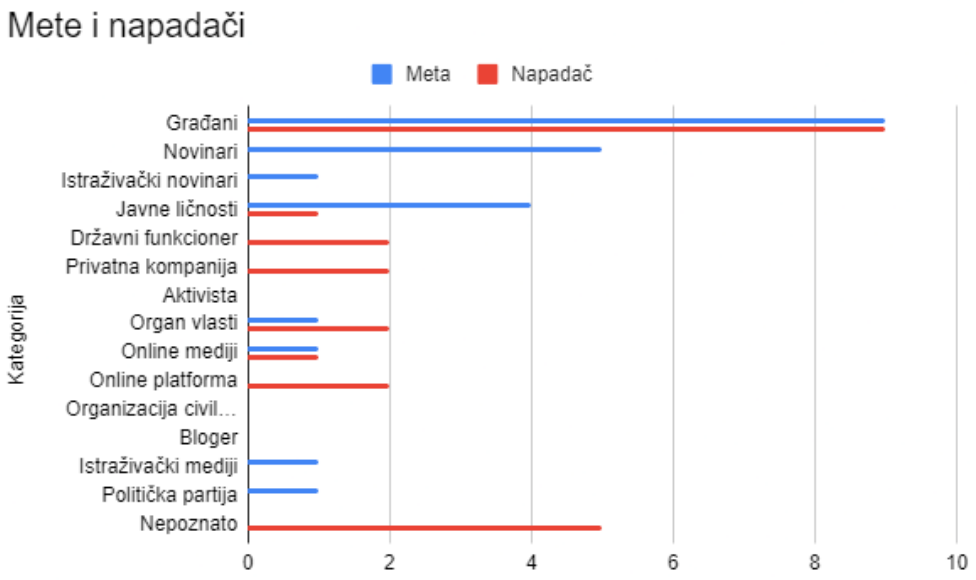
Predstavnici još jedne privatne kompanije, tj. Niveus tima, podneli su dve tužbe protiv portala Vojvođanski istraživačko-analitički centar (VOICE) u kojima se traži naknada štete u iznosu od po milion dinara. Tužbe su usledile nakon izveštavanja VOICE o ugovorima o uslugama socijalne zaštite koji su dodeljeni Niveus timu preko javnih nabavki. Portal KRIK takođe je bio meta tužbe, u ovom slučaju u iznosu od pola miliona dinara, koju je protiv portala podneo Bratislav Gašić, direktor Bezbednosno-informativne agencije (BIA) i visoko rangirani član vladajuće SNS. Tužba je usledila nakon što je KRIK nedavno objavio izveštaj sa suđenja na kome su navodi da je Gašić povezan sa kriminalnim licima.

Još jedna vrsta pritiska jeste i slučaj bivšeg političara Zorana Čička, koji je bio saslušan u policiji u vezi sa tvitom koji je objavio povodom skorašnjih izbora za mesne zajednice u Novom Sadu i ulozi SNS-a. Čičak je zbog tvita u pritvoru

zadržan 17 sati, nakon što su pripadnici Službe za borbu protiv organizovanog kriminala došli na njegovu kućnu adresu i odveli ga na saslušanje.

Ključni nalazi

SHARE Fondacija zabeležila je ukupno 22 povrede digitalnih prava za tromesečni period, od početka aprila do kraja juna 2021. godine. U aprilu je zabeleženo 9 slučajeva, u junu za jedan manje, a u maju 5 slučajeva povreda prava. Najučestaliji su bili pritisci zbog izražavanja i aktivnosti na internetu, u 15 slučajeva, dok je narušavanje informacione bezbednosti zabeleženo 6 puta, manipulacije i propaganda u digitalnom okruženju dogodile su se 4 puta, a kategorija povreda informacione privatnosti i zaštite podataka o ličnosti 3 puta.



Građani su bili najčešća meta napada, ali su i najčešće kršili digitalna prava – u oba slučaja po 9 puta. Novinari su bili žrtve napada 5, a javne ličnosti 4 puta. Pored građana, napadači su u najvećem broju slučajeva ostali nepoznati, 5 puta.

Monitoring baza SHARE Fondacije