KIBERNETIČKA SIGURNOST U HRVATSKIM MEDIJIMA

Svan Hlača *

UDK: 007:004.056(497.5)
004.738.5(497.5)
Primljeno: 1. II. 2015.
Prihvaćeno: 8. II. 2019.

SAŽETAK

U ovom je radu analizirano stanje kibernetičke sigurnosti u Republici Hrvatskoj s posebnim težištem na prikazu računalno-sigurnosnih incidenata koji su imali izvorište ili metu unutar hrvatskog IP adresnog prostora ili .hr domene. Analizom članaka objavljenih na pet najpopularnijih hrvatskih portala utvrdit će se u kakvom su oni odnosu sa stvarnim brojem računalno-sigurnosnih incidenata. Također, da bi se opisao razvoj kibernetičke sigurnosti riječi će biti o razvoju interneta, cyberkulture i kibernetičkog prostora. Uz pomoć koncepata sekuritizacije, ali i hipersekuritizacije svakodnevnih sigurnosnih praksi, te tehnifikacije prikazat će se na koji se način stvara slika o kibernetičkoj sigurnosti u javnosti te kakvu poziciju akteri sekuritizacije predviđaju običnom korisniku.

Ključne riječi: kibernetička sigurnost, sigurnost, sekuritizacija, incidenti, hakeri.

UVOD

Danas je pristup internetu kao potpuno otvorenom sustavu omogućen gotovo svakom računalu ili mobilnom telefonu, a broj uređaja koji se mogu spojiti na internet je sve veći. Internet je omogućila tehnologija koja je nastala kao vojna tehnologija, ali je izašla iz okvira onoga za što je inicijalno zamišljena i postala je temelj informacijskog društva. S rastom i razvojem internet je sve više dolazio u ruke znanstvenika koji su željeli izgraditi utopijski sistem besplatne komunikacije za sve. Gradeći za sebe, u početku internet nisu željeli napraviti mjestom sigurnosnih propisa, već lako dostupnim mjestom koje je namijenjeno svima.

Takav pristup, potpomognut globalizacijom, otvorio je put za mnoge ranjivosti sustava. Ranjivost može biti smještena u operacijskom sustavu, ali i u bilo kojoj od bezbroj aplikacija koje se svakodnevno koriste. U vrijeme kada postoji mnogo proizvođača elektroničkih uređaja ne postoji mogućnost stvaranja adekvatnog sustava

* Svan Hlača (svan.hlaca@gmail.com) je magistar edukacije sociologije te etnologije i kulturne antropologije. Rad je proizašao iz istoimenog diplomskog rada kojeg je autor izradio i obranio na Filozofskom fakultetu Sveučilišta u Zagrebu u prosincu 2018.

obrane koji može odvratiti napad prije nego što do njega dođe. Ovo djeluje zastrašujuće, ali valja se zapitati je li zaista tako. Stručnjaci, mediji i ostali akteri govore o apokaliptičnim scenarijima koji samo čekaju da se dogode, međutim, nakon nešto manje od pola stoljeća od početaka razvoja interneta, on još uvijek postoji i jači je nego ikad.

S druge strane, pojedini autori govore o hipersekuritiziranosti i o tome da stručnjaci tehnificiraju diskurs čineći ga neshvatljivim običnim korisnicima interneta koje se primorava na poduzimanje svakodnevnih sigurnosnih praksi da ne bi postali žrtve i time ugrozili sebe, svoje bližnje i okolinu. Tehničke sposobnosti za izvedbu takvih napada svakako postoje, ali potrebno je odrediti kolika je stvarna mogućnost da običan korisnik bude meta pomno isplaniranog napada kojeg je visoko educirana osoba pripremala više mjeseci.

Ovim se radom želi ustanoviti kako mediji u Hrvatskoj sudjeluju u stvaranju atmosfere straha pišući o mogućim prijetnjama po stanovnike. Također, analizirat će se o kakvim je tipovima prijetnji riječ, tj. kakve prijetnje mediji prikazuju. Svaka od prikazanih prijetnji će se dodatno ispitati na temelju relevantne taksonomije da bi se ustanovilo o kojem je tipu i ozbiljnosti incidenta riječ. Svi obrađeni incidenti bit će podijeljeni na one koji su imali izvorište ili metu napada unutar hrvatskog IP adresnog prostora, te će oni koji to imaju biti detaljnije analizirani. Također, na temelju relevantnih izvora bit će prikazan broj računalno-sigurnosnih incidenata u hrvatskom IP adresnom prostoru, a svaki od podtipova će biti detaljno pojašnjen na temelju relevantnih taksonomskih dokumenata.

TEORIJSKI DIO

Temeljna ideja iza stvaranja interneta bila je ideja o komunikacijskom sustavu koji je otporan na nuklearni napad, tj. sustavu koji se temelji na komunikacijskoj tehnologiji prebacivanja paketa, što je omogućavalo da mreža bude neovisna o upravnim i kontrolnim centrima jer su paketi, jedinice poruke, sadržavale upute kako doći do primatelja i na koji način se trebaju spojiti da bi prikazale inicijalnu poruku (Castells 2001: 10). Međutim, uz napore Pentagona i onoga što Castells naziva velike znanosti u uspostavi javno dostupne računalne mreže, u Sjedinjenim se Državama pojavila i kontrakultura koja se može povezati s odjecima pokreta 1960-ih, a karakterizirao ju je slobodnjački i gotovo utopijski svjetonazor. Modem je izravan rezultat rada dvojice pripadnika te kontrakulture, Warda Christensena i Randyja Suessa, koji su tehnologiju prenošenja podataka bez korištenja *host* sustava dijelili besplatno jer su vjerovali u koncept besplatnog i javno dostupnog komunikacijskog kanala (Castells 2000: 381). Internet je obilježila činjenica da je on oblikovan tako da bude otvoren svima i omogući širok javni pristup te otežava regulaciju prometa državnim ili komercijalnim akterima. Castells (2000: 384) zasluge za ovakav oblik vidi u činjenici da su na razvoju radili „znanstvenici koji su htjeli postaviti novi sustav, pun tehnološke hrabrosti i svojevrstan utopijski pothvat". Također, Castells (2000: 384) navodi da otvorenost sustava proizlazi iz neprekidnog procesa inovacija i slobodnog pristupa

koji su potaknuli rani računalni hakeri koji su njegovali metodu „otvorenog koda". Međutim, ovakva otvorena arhitektura ostavila je mrežu ranjivom na najezde sofisticiranih uljeza. Slučaj kojeg Castells izdvaja, a predstavlja kanon među hakerima i stručnjacima za kibernetičku sigurnost, slučaj je Kevina Mitnicka (Castells 2000: 385; Littman 1996). Strah i potpuno nerazumijevanje formalno odgovornih službi za sigurnost zaslužni su za eksploziju važnosti kibernetičke sigurnosti u svijetu. Hakeri odjednom od štrebera koji vole popularnu kulturu postaju najtraženiji svjetski zločinci koji su sposobni fućkanjem uzrokovati potpuno uništenje svijeta.

Taj novi i opasni internet bilo je potrebno diskurzivno odrediti kao prijetnju, tj. sekuritizirati. Naime, sekuritizaciju se može definirati kao proces u kojem akter proglašava pojedini fenomen, odnos ili aktera egzistencijalnom prijetnjom za određeni referentni objekt. Ako relevantna publika prihvati stav da nešto treba sekuritizirati, dolazi do suspenzije „uobičajenih" političkih procesa i uspostave izvanrednih mjera kojima se odgovara na prikazanu prijetnju (Buzan, Wæver i de Wilde 1998: 25). Sigurnost u ovom smislu predstavlja polje pregovora između govornika i publike, koje je u velikoj mjeri uvjetovano pozicijom moći koju govornik ima unutar određene grupe. Wæver zaključuje da uspješna sekuritizacija uključuje artikulaciju prijetnje s „određenog mjesta, institucionalnim glasom, od elita" (Wæver prema: McDonald 2008: 69). Prijetnja prolazi tri stadija, tj. iz polja nepolitiziranosti ulazi u polje politiziranosti i potom u polje sekuritizacije.

Međutim, specifična priroda informacijsko-komunikacijskih tehnologija učinila je te tehnologije u 21. stoljeću temeljnim sigurnosnim uvjetom ostalih sigurnosnih sektora. Kibernetička sigurnost više nije samo sigurnost informacijsko-komunikacijskih sustava, već predstavlja temeljnu sastavnicu sigurnosti cjelokupnog opsega ljudskih djelatnosti u informacijskom društvu. O sekuritizaciji cyberprostora, tj. o kibernetičkoj sigurnosti počelo se govoriti nakon hladnog rata kao o odgovoru na niz tehnoloških inovacija i geopolitičkih promjena. Početkom 1990-ih pojam kibernetička sigurnost koristili su znanstvenici da bi označili niz nesigurnosti vezanih uz umrežena računala. Međutim, pojam je dobio šire značenje nakon što je ustanovljeno da prijetnje koje izviru iz digitalnih tehnologija mogu imati drastične posljedice za cjelokupno društvo (Hansen i Nissenbaum 2009: 1155).

Kod kibernetičke sigurnosti od presudne važnosti je činjenica da prijetnje ne dolaze isključivo namjerom agenata, već mogu biti sistemske prijetnje. Hundley i Anderson smatraju, a Hansen i Nissenbaum prenose (2009: 1160), da „kibernetička sigurnost ovisi o inherentnim nepredvidljivostima računala i informacijskih sustava koji, sami po sebi, stvaraju neželjenu, potencijalnu ili aktualnu, opasnu situaciju po sebe ili po fizički i ljudski okoliš u koji su ugrađeni". Prijetnje mogu proizaći iz grešaka u programskoj podršci (engl. *software*) i računalnoj sklopovskoj podršci (engl. *hardware*) i ne mogu biti otklonjene usavršavanjem digitalne tehnologije i programiranja. Edwards i Denning, prema Hansen i Nissenbaum (2009: 1160), zaključuju da unutar računalnih sistema postoji inherentna ontološka nesigurnost.

Međutim, Hansen i Nissenbaum (2009: 1163) navode da su kibernetičku sigurnost obilježila tri specifična, uz nju snažno vezana koncepta koji ju, odnosima između

sebe, definiraju. Svaki od ova tri koncepta snažno određuje odnos između sigurnosnih stručnjaka i aktera sekuritizacije s korisnicima informacijsko-komunikacijskih tehnologija, te dodatno produbljuje jaz između ove dvije skupine čime onemogućuje podizanje razine kibernetičke sigurnosti.

Hipersekuritizacija

Prvi koncept, hipersekuritizaciju, predstavlja Buzan (prema: Hansen i Nissenbaum 2009: 1163–1164), a opisuje ju kao „proširenje sekuritizacije izvan normalne razine prijetnji i opasnosti pomoću tendencije da se pretjeruje u prikazu prijetnji te uspostavlja velik broj protumjera". Uspjeh hipersekuritizacije određuje je li ona okarakterizirana kao pretjerivanje ili nije, tj. uspješna hipersekuritizacija ne smije biti okarakterizirana kao pretjerivanje.

Također, svi procesi sekuritizacije uključuju element hipotetskog u tome što stvaraju prijetnju na koju treba odgovoriti te na taj način „mobiliziraju ako-onda logiku" (Hansen i Nissenbaum 2009: 1164). Za razliku od sekuritizacije, hipersekuritizacija podrazumijeva trenutne i međusobno povezane efekte. Na primjer, dok sekuritizacija mreže govori isključivo o mreži kao takvoj, hipersekuritizacija prikazuje na koji način prijetnja mreži prijeti društvenom, financijskom i vojnom sektoru. Također, sekuritizacija uvijek promatra budućnost, ali zaključke temelji i na referencama iz prošlosti kao što su npr. Hirošima i Nagasaki. U kontekstu kibernetičke sigurnosti hipersekuritizacija nema tu mogućnost zbog toga što ne postoje povijesne reference, što za posljedicu ima preuveličavanje prijetnje jer ne postoji referentni okvir (Hansen i Nissenbaum 2009: 1164).

Svakodnevne sigurnosne prakse

Drugi koncept koji snažno oblikuje kibernetičku sigurnost su svakodnevne sigurnosne prakse koje uspostavljaju akteri sekuritizacije, državna tijela, privatne organizacije i tvrtke. Svakodnevnim se sigurnosnim praksama želi „mobilizirati" pojedince na dva načina: osiguravanjem partnerskog odnosa pojedinca prema akterima sekuritizacije i suglasnosti u održavanju visoke razine kibernetičke sigurnosti, te činjenjem hipersekuritiziranih scenarija plauzibilnijima povezivanjem elemenata scenarija katastrofe sa svakodnevnim iskustvima običnih korisnika. Uspjeh sekuritizacije uvelike ovisi o sposobnosti aktera sekuritizacije da poveže strah i prijetnje s osjećajima, potrebama i interesima običnih korisnika te činjenicom da dovodi iste u opasnost ne pridržavajući se svakodnevnih sigurnosnih praksi (Hansen i Nissenbaum 2009: 1165).

Cybersekuritizacija svakodnevnog života dodatno naglašava ulogu pojedinca kao partnera u borbi protiv nesigurnosti, ali naglašava i ulogu pojedinca kao izvora nesigurnosti, prijetnju ili, kako kaže Furedi, ranjivost. Naglašavanjem činjenice da se odbijanjem praćenja svakodnevnih sigurnosnih praksi narušava sigurnost cijelog sustava, u običnog se korisnika ugrađuje moralna odgovornost prema održavanju vlastite sigurnosti i, na koncu, sigurnosti cijelog sustava (Hansen i Nissenbaum 2009: 1166).

Tehnifikacija diskursa

Treći koncept koji obilježava kibernetičku sigurnost je tehnifikacija diskursa. Snažan naglasak na hipotetskim situacijama otvara prostor za tehnički, ekspertni diskurs. Nissebaum naglašava (Hansen i Nissenbaum 2009: 1166) da je znanje potrebno da se obuhvati cijelo polje kibernetičke sigurnosti impozantno i često nije dostupno široj javnosti. Ubrzani razvoj tehnologije donosi i nove metode napada, što dodatno potvrđuje privilegiranu poziciju stručnjaka za kibernetičku sigurnost. Ovakva privilegirana pozicija stručnjaka za kibernetičku sigurnost izvire upravo iz logike sekuritizacije: „ako je kibernetička sigurnost toliko važna, ne može biti prepuštena amaterima" (Hansen i Nissenbaum 2009: 1167). Upravo tehnifikacija diskursa u sekuritizaciji dopušta određivanje tehničkog kao domene koja zahtijeva stručnost koju javnost i većina političara nema. Na taj način stručnjaci postaju akteri sekuritizacije bez „politike" s potpunim legitimitetom i bez mogućnosti da budu izazvani ili da njihova procjena bude dovedena u pitanje (Hansen i Nissenbaum 2009: 1167).

METODOLOGIJA

U radu su korištene dvije metode iz korpusa kvalitativnih metoda društvenih znanosti. U prvom je koraku korištena analiza sadržaja članaka objavljenih na portalima 24sata, Dnevnik.hr, vecernji.hr i tportal, koji su prema istraživanju tvrtke Gemius najčitaniji hrvatski internetski portali.[1] Popisu je dodan i Index.hr, koji nije uvršten na popis tvrtke Gemius vlastitom zahtjevom, ali je jedan od najčitanijih internetskih portala u Hrvatskoj.

Pretraga je vršena prema ključnim riječima „cyber", „kibernetička", „računalna", „haker" i „hakeri", a obuhvatila je sve članke objavljene na spomenutim portalima 2017. godine. Na ovaj je način izdvojeno 1335 rezultata. Međutim, zbog preklapanja u ključnim riječima izdvojeno je 607 članaka.

Ključne riječi su odabrane na temelju više kriterija. Na početku stoljeća terminologija koja se koristila u kontekstu onoga što se danas naziva kibernetička sigurnost sastojala se od pojmova kao što su „računalna sigurnost" (engl. *computer security*), „IT sigurnost" (engl. *IT security*) i „informacijska sigurnost" (engl. *information security*) (Schatz, Bashroush i Wall 2017: 53). Međutim, krajem prvog desetljeća pojam „kibernetička sigurnost" (engl. *cyber security*) se sve češće spominje, a pravi uzlet doživljava 2009. kada predsjednik SAD-a Barack Obama poziva građane na prepoznavanje kibernetičke sigurnosti kao važne sastavnice nacionalne otpornosti i sigurnosti. Otad pojmovi računalna sigurnost, informacijska sigurnost i IT sigurnost gube na značaju, dok kibernetička sigurnost sve više jača (Schatz, Bashroush i Wall 2017: 54).

U Hrvatskoj je pojam „kibernetički" uveden u pravni poredak 2002. godine ratifikacijom Konvencije o kibernetičkom kriminalu (Vojković i Štambuk-Sunjić 2006:

[1] 24sata (https://www.24sata.hr/), Dnevnik.hr (https://dnevnik.hr/), vecernji.hr (https://www.vecernji.hr/), tportal (https://www.tportal.hr/) i Index.hr (https://www.index.hr/).

124) te predstavlja prilagodbu engleskog prefiksa *cyber-* hrvatskom jeziku. Govoreći o ratifikaciji Konvencije, Vojković navodi da je pojam „računalni kriminal", koji je dotad bio u Hrvatskoj najrazumljiviji i općenito prihvaćen termin, zamijenjen, i to prema njegovu mišljenju pogrešno, terminom „kibernetički kriminal" (Vojković i Štambuk-Sunjić 2006: 125). Praksa prevođenja prefiksa *cyber-* u pridjev „kibernetički", a ne „kiber", karakteristična je za slavenske jezike kao što su slovenski i češki jezik (*kibernetska varnost*, *kybernetická bezpečnost*) te se odrazila i na hrvatsko zakonodavstvo. Međutim, zbog globalnog dosega prefiksa *cyber-*, ali i njegove uloge u popularnoj kulturi i *cyberpunk* pokretu, on se i dalje koristi u hrvatskom jeziku. Dakle, termin „kibernetička sigurnost" je danas zakonski određen, prefiks *cyber-* je oblik iz kojeg je izveden termin „kibernetički", a „računalni" je 2002. godine ratifikacijom Konvencije zamijenjen terminom „kibernetički", ali je i dalje ostao snažno prisutan u hrvatskom jeziku kao doslovni prijevod pojma *computer security*, čija je popularnost počela padati tek 2009. godine (Schatz, Bashroush i Wall 2017: 54).

Pojam „haker" korišten je u jednini i množini zbog različitih rezultata koje je pretraga po ovim ključnim riječima davala. Na primjer, portal vecernji.hr pretragom po ključnoj riječi „haker" daje 6 rezultata, dok „hakeri" daju 91 rezultat. Portal 24sata pretragom po ključnoj riječi „haker" daje 15, a „hakeri" 89 rezultata. I tportal pretragom ključne riječi „haker" daje 15, a „hakeri" 104 rezultata. Dnevnik.hr pretragom po ključnoj riječi „haker" daje 5, a „hakeri" 27 rezultata. Najmanju razliku pokazuje Index.hr, koji pretragom po ključnoj riječi „haker" daje 192 rezultata, dok ključna riječ „hakeri" daje 202 rezultata.

Iz na ovaj način prikupljenih članaka izdvojeno je deset članaka koji se odnose na sedam računalno-sigurnosnih incidenata čije je izvorište ili objekt napada u hrvatskom IP adresnom prostoru, te se u daljnjoj analizi koristi metoda studije slučaja, tj. analiza svih računalno-sigurnosnih incidenata u Hrvatskoj 2017. godine kroz njihove opise u medijskom prostoru.

Studija slučaja je kvalitativna istraživačka metoda koja se često definira kao „studija malog broja slučajeva ili jednog slučaja u opreci sa studijama velikog broja slučajeva" (Jožanc 2015: 38). Budući da je ustanovljeno da se vrlo malo članaka odnosi na incidente koji su imali izvorište ili objekt napada u hrvatskom IP adresnom prostoru, studijom slučaja je opisan svaki od promatranih incidenata, ali je i klasificiran na temelju VOUND taksonomije te napadom prouzročene materijalne štete. Također, Schramm navodi da je „esencija studije slučaja, centralna tendencija svih tipova studije slučaja, osvjetljavanje odluke ili niza odluka: zašto su donesene, kako su implementirane i s kojim rezultatom" (prema: Yin 1984: 12), što u kontekstu prikaza računalno-sigurnosnih incidenata omogućava sagledavanje šire slike i detaljniju obradu manjeg broja slučajeva, što dalje omogućava analizu odnosa između empirijskog i normativnog u kontekstu računalno-sigurnosnih incidenata.

Usto, posebno je obrađen i slučaj značajnog incidenta zaraze zlonamjernim *ransomware*[2] sadržajem WannaCry koji je odjeknuo u svijetu, ali i u Hrvatskoj. Prikazano

[2] *Ransomware* je naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze, *ransomware* može šifrirati datoteke ili onemogućiti korištenje

je što je prethodilo napadu, na koji način je izveden, koji je doseg imao i koji je trag ostavio u Hrvatskoj.

Sav medijski sadržaj vezan uz računalno-sigurnosne incidente u Hrvatskoj podijeljen je s obzirom na izvorište računalno-sigurnosnog incidenta, opseg napada i vrstu napada, po uzoru na klasifikacijsku shemu Nacionalne taksonomije računalno-sigurnosnih incidenata koja sigurnosno-računalne incidente dijeli prema:

1) vektoru napada
2) operativnom učinku napada
3) učinku napada na informacije
4) objektu napada
5) dosegnutoj fazi napada.

Uz navedeni kriterij medijski sadržaj je kategoriziran prema dosegnutom broju žrtava i uzrokovanoj materijalnoj šteti.

Komparativnom analizom utvrđena je i razlika između medijskog prikaza računalno-sigurnosnih incidenata i službene evidencije istih koja se nalazi u okviru Statističkog pregleda temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini Ministarstva unutarnjih poslova te Godišnjeg izvještaja Nacionalnog CERT-a[3] za 2017. godinu.

Analizom su obuhvaćene sve kategorije računalno-sigurnosnih incidenata prema Godišnjem izvještaju Nacionalnog CERT-a, te samo one kategorije koje se odnose na kibernetičku sigurnost u ostalim izvorima. Pod tim se kategorijama podrazumijeva neovlašten pristup, ometanje rada računalnog sustava, oštećenje računalnih podataka, neovlašteno presretanje računalnih podataka, računalno krivotvorenje i računalna prijevara.

Komparativna analiza pokazala je o koliko je računalno-sigurnosnih incidenata, prema službenim izvještajima nadležnih tijela, u 2017. godini riječ, prati li broj i sastav medijskih članaka te brojke, u kojoj se mjeri računalno-sigurnosni incidenti obrađeni u medijima odnose na računalno-sigurnosne incidente krajnjeg korisnika, te koja je uloga prosječnog korisnika u incidentu. Ovom se analizom nastojalo odgovoriti na pitanje u kojem odnosu stoji stvarna situacija računalno-sigurnosnih incidenata krajnjih korisnika i prikaz računalno-sigurnosnih incidenata u medijima, te se nastojalo odgovoriti i na pitanje može li se govoriti o hipersekuritiziranosti ove teme u Hrvatskoj.

Analizom sadržaja odabranih članaka koji govore o incidentima koji su imali cilj ili izvorište napada unutar hrvatskog IP adresnog prostora istraženo je na koji način mediji kao glavni izvor informacija o sigurnosnim incidentima, ali i jedan od aktera

tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Od korisnika zaraženog računala traži se otkupnina u zamjenu za daljnje normalno korištenje računala.

[3] engl. *Computer Emergency Response Team*

na društvenopolitičkoj poziciji koja definira rizik, sudjeluju u definiranju računalno-sigurnosnog incidenta, kako te incidente prikazuju, te na koji je način i u kojem kontekstu prikazan ljudski faktor, tj. na koji je način čovjek utjecao na ranjivost sustava i je li i na koji način zaslužan za sigurnosni incident. Također, odgovoreno je na pitanje vladaju li diskursom sigurnosni stručnjaci i je li on pretjerano „tehnificiran", te na koji način akteri uvjetuju korisnika obvezujući ga na prihvaćanje svakodnevnih sigurnosnih praksi. Istraživanjem se nastojalo odgovoriti i na pitanje tretira li se korisnika kao najveću ranjivost sustava, te postoji li za to temelj kada govorimo o kibernetičkoj sigurnosti u Hrvatskoj.

ANALIZA

Prema službenim podacima nadležnih tijela – Nacionalnog CERT-a i Ministarstva unutarnjih poslova – u Hrvatskoj su 2017. zabilježena ukupno 732 incidenta u nadležnosti Nacionalnog CERT-a, te 755 incidenata u nadležnosti Ministarstva unutarnjih poslova, a koji su imali izvorište ili objekt napada unutar hrvatskog IP adresnog prostora ili .hr domene.

Pod nadležnošću Nacionalnog CERT-a 2017. godine bili su sljedeći računalno-sigurnosni incidenti: *web defacement* (kompromitiran web-poslužitelj s izmijenjenim izgledom i sadržajem web-stranice) – 370 slučajeva; *phishing* URL (kompromitiran web-poslužitelj s postavljenom lažiranom stranicom čija je svrha krađa podataka) – 127 slučajeva; *phishing* (navođenje korisnika na odavanje podataka putem raznih komunikacijskih kanala (najčešće elektroničke pošte)) – 59 slučajeva; *malware* URL (kompromitiran web-poslužitelj s postavljenim zlonamjernim kodom) – 42 slučaja; *spam* (neželjena elektronička poruka reklamnog sadržaja) – 29 slučajeva; nedozvoljene mrežne aktivnosti (neovlašteno automatizirano prikupljanje informacija o računalnim mrežama i sustavima) – 28 slučajeva; *spam* URL (kompromitiran web-poslužitelj s neovlašteno postavljenim reklamnim sadržajem) – 26 slučajeva, *bot* (računalo ili neki drugi uređaj zaražen zlonamjernim kodom, a koji djeluje kao *bot* unutar *botnet* mreže) – 20 slučajeva; ostale vrste napada i zloporaba za koje korisnik smatra su računalno-sigurnosni incidenti – 12 slučajeva; DoS[4] (volumetrički napad koji se izvodi slanjem velikog broja IP paketa s ciljem zagušenja mrežne propusnosti) – 10 slučajeva; *malware* domene (kompromitirano web-sjedište s postavljenim zlonamjernim kodom) – 4 slučaja; ostala kompromitirana računala – 3 slučaja; te C&C (kontrolni poslužitelj za nadzor i upravljanje računalima koja su dio *botnet* mreže) – 2 slučaja (Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu).

Pod nadležnošću Ministarstva unutarnjih poslova 2017. godine bili su sljedeći računalno-sigurnosni incidenti: neovlašten pristup (višestruko pogađanje zaporki ili iskorištavanje ranjivosti da bi se ostvario neovlašteni pristup računalu) – 5 slučajeva; ometanje rada računalnog sustava (uskraćivanje dostupnosti računalnog sustava) – 11 slučajeva; oštećivanje računalnih podataka – 7 slučajeva; neovlašteno

[4] engl. *Denial-of-Service*

presretanje računalnih podataka (prikupljanje informacija *sniffing*[5] metodom) – 1 slučaj; računalno krivotvorenje – 10 slučajeva; računalne prijevare (razne vrste prijevara na internetu (lažno predstavljanje, prijevare prilikom trgovine na internetu i sl.)) – 721 slučaj.[6]

Kada je riječ o značajnim incidentima u 2017. godini valja izdvojiti zlonamjerni *ransomware* sadržaj WannaCry, prvi globalni incident ovakvog intenziteta, zabilježen 12. svibnja 2017., u kojem je pogođeno više od 400.000 računala u 150 zemalja. Prema podacima objavljenim na stranicama Ureda vijeća za nacionalnu sigurnost, u Hrvatskoj je zabilježeno 205 slučajeva računala zaraženih zlonamjernim *ransomware* sadržajem WannaCry.

S druge strane, kada je riječ o računalno-sigurnosnim incidentima koji su imali ili izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni, analiza članaka objavljenih na portalima 24sata, Dnevnik.hr, vecernji.hr, tportal i Index.hr, koji su prema istraživanju tvrtke Gemius najčitaniji hrvatski portali, pokazuje značajno drugačiju sliku.

Pretraga članaka povezanih s ključnim riječima „cyber", „kibernetička", „računalna", „haker" i „hakeri", koji su objavljeni 2017. godine, dala je mnoštvo rezultata, ali i različite rezultate za svaki portal: Index.hr najviše članaka, njih 202, prikazuje pretragom pojma „haker", portal 24sata najviše članaka (89) prikazuje pretragom pojma „hakeri", Dnevnik.hr najviše članaka (30) prikazuje pretragom pojma „cyber", vecernji.hr najviše članaka (91) prikazuje pretragom pojmova „hakeri" i „cyber", a tportal najviše članaka (166) prikazuje pretragom pojma „računalna".

Kada se izdvoje samo članci koji se odnose na konkretan računalno-sigurnosni incident koji je imao ili izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni, tj. članaka koji govore o stvarnim slučajevima računalno-sigurnosnih incidenata, a ne o prijetnjama koje bi mogle pogoditi Hrvatsku i njezine stanovnike, broj povezanih članaka drastično pada. Naime, od svih relevantnih članaka 2017. godine konkretnim primjerima računalno-sigurnosnih incidenata koji su imali ili izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni posvećeno je svega deset članaka, ne računajući WannaCry[7] koji je zasebno obrađen zbog velikog broja članaka o njemu. Svaki od relevantnih računalno-sigurnosnih incidenata obrađen je prema VOUND taksonomiji[8] da bi se utvrdilo u koju skupinu određeni incident spada i o kojoj je razini prijetnje riječ, te su na temelju tih podataka incidenti analizirani.

---

5 Presretanje mrežnog prometa *snifferom*, posebno razvijenom aplikacijom koja presreće mrežne pakete.

6 Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini Ministarstva unutarnjih poslova, siječanj 2018.

7 Detaljnije u: Analiza WannaCry *ransomwarea*, NCERT-PUBDOC-2018-1-354, CERT.hr, https://www.cert.hr/wp-content/uploads/2018/02/WannaCry.pdf (pristupljeno u listopadu 2018.).

8 Akronim VOUND dobiven korištenjem početnih slova ključnih riječi pet atributa predloženih za opis računalno-sigurnosnih incidenta u Republici Hrvatskoj: vektor napada (V); operativni učinak napada (O); učinak napada na informacije (U); objekt napada (N); dosegnuta faza napada (D) (Nacionalna taksonomija računalno-sigurnosnih incidenata, 2018).

Analizom opisanih računalno-sigurnosnih incidenata u člancima ustanovljeno je da dva članka[9] pišu o različitim slučajevima krađe povjerljivih bankovnih podataka, tj. *skimming* napada. Prema VOUND taksonomiji, vektor napada je fizički napad jer je riječ o instalaciji zlonamjernog uređaja na fizički izložen uređaj, u ovom slučaju bankomat. Operativni učinak napada je prikupljanje informacija, točnije: skeniranje koje podrazumijeva neovlašteno i automatizirano prikupljanje povjerljivih korisničkih podataka. Učinak napada na informacije je otkrivanje informacije jer napadač prikuplja podatke s magnetne trake bankovne kartice i PIN-ove. Objekt napada je za ove incidente sam korisnik jer je cilj napada prikupljanje korisnikovih osobnih informacija. Dosegnuta faza napada je potpuna kompromitacija jer je napadač ostvario svoj cilj i motivaciju za napad. Prema članku „Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe" u tom je sigurnosnom incidentu ukupna materijalna šteta bila manja od 10.000 kuna, a u članku „Lopovi imaju sve naprednije metode za varanje građana, ali zaštititi se možete na prilično jednostavan način" takva se informacija ne navodi.

Analizom članka „Nova prijetnja: Poruke iz lažne Porezne žele do vaših podataka" (24sata, 1. prosinca 2017.) i „Ne nasjedajte na ovaj lažni mail iz porezne, mogli biste ostati bez podataka" (tportal, 1. prosinca 2017.) je ustanovljeno da je u njima riječ o *phishing* kampanji. Vektor napada je socijalni inženjering[10] jer je riječ o *phishing* poruci u kojoj se korisniku savjetovalo preuzimanje zlonamjernog sadržaja s *phishing* URL-a koji se nalazio na lažnoj domeni porezna-uprava.net. Prema operativnom učinku napada ovaj incident pripada *phishing* URL tipu kompromitacije. Učinak napada na informacije je otkrivanje jer preuzimanjem zlonamjernog sadržaja na računalo žrtva omogućava napadaču pristup računalu i povjerljivim informacijama. Objekt napada je lokalno računalo jer je riječ o napadu u kojem dolazi do kompromitacije lokalnog računala pojedinačnog korisnika preuzimanjem zlonamjernog sadržaja. Prema dosegnutoj fazi napada riječ je o fazi isporuke, a do ostvarivanja pristupa nije došlo zbog pravovremene reakcije nadležnih službi koje su onemogućile vezu s kompromitiranog računala s napadačem. Članci ne otkrivaju koliko je pojedinaca pogođeno i kolika je materijalna šteta uzrokovana ovim incidentom. Međutim, budući da su nadležne službe prijetnju vrlo brzo otklonile, može se pretpostaviti da je riječ o neznačajnoj šteti, tj. ni uređaji ni podaci nisu oštećeni u napadu, a sanacija podrazumijeva instalaciju antivirusnog programa.

Sljedeći incident opisan je u člancima „Hakeri srušili sustav KBC-a Sestara milosrdnica, pacijenti ostali bez snimaka lomova" (vecernji.hr, 12. siječnja 2017.) i „Hakeri napali Traumatologiju: Srušio se sustav s podacima" (24sata, 12. siječnja 2017.). Prema vektoru napada ovaj se incident svrstava u skupinu napada na dostupnu mrežnu i računalnu opremu, napada koji iskorištavaju ranjivosti računalnih mreža,

[9] „Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe" (24sata, 27. studenog 2017.) i „Lopovi imaju sve naprednije metode za varanje građana, ali zaštititi se možete na prilično jednostavan način" (Dnevnik.hr, 2. studenoga 2017.).

[10] Socijalni inženjering je niz tehnika pomoću kojih pojedinac, iskorištavanjem ljudskih pogrešaka i slabosti, utječe na drugog pojedinca da bi ga naveo da učini nešto što nije u njegovom interesu.

ranjivih mrežnih uređaja i javno dostupnih poslužitelja ili računala. Operativni učinak napada je sustav zaražen zlonamjernim kodom, a učinak napada na informacije je uništenje informacija. Objekt napada je upravljačka infrastruktura jer je riječ o napadu na kritične dijelove sustava koji koordiniraju aktivnosti i upravljaju resursima informacijskog sustava. Dosegnuta faza napada je potpuna kompromitacija jer je došlo do uništenja podataka i privremenog uskraćivanja usluge. U člancima se ne navodi koliko je bilo pogođenih korisnika i kolika je materijalna šteta, ali piše da su svi podaci vraćeni iz sigurnosne kopije i smješteni na novi poslužitelj, pa se može pretpostaviti da je materijalna šteta u ovom slučaju gotovo zanemariva.

Sljedeći članak je „Lažni bankar prevario dvije žene, uzeo im 3.900 kuna za klađenje" (Index.hr, 8. travnja 2017.). Vektor ovog napada je socijalni inženjering jer je napadač naveo žrtve na kršenje uobičajenih sigurnosnih procedura, tj. lažnim predstavljanjem je došao do povjerljivih informacija. Operativni učinak napada je prijevara, a učinak napada na informacije je otkrivanje jer je napadač ostvario pristup informacijama kojima u normalnim okolnostima ne bi imao pravo pristupa. Objekt napada su korisnice jer su napadom prikupljane osobne informacije korisnika, a dosegnuta faza napada je potpuna kompromitacija jer je došlo do ostvarivanja ciljeva i motivacije za napad, tj. došlo je do krađe novca s računa žrtava. Ovim su napadom dvije osobe oštećene za 3900 kuna.

Članak „Hakeri od Cro Copa tražili otkupninu: 'Bolje mu je da ga ne nađu, ako ga nađe policija – jadna mu majka'" objavio je Index.hr 28. travnja 2017. Vektor napada nije opisan, ali se može pretpostaviti da je riječ o socijalnom inženjeringu ili o napadu na web-tehnologije koje podrazumijevaju *brute force* napade na autentifikacijske mehanizme web-aplikacija kao što su zaporke. Prema operativnom učinku napada postoje dvije mogućnosti, kompromitacija korisničkog računa na temelju podataka prikupljenih socijalnim inženjeringom ili pokušaj neovlaštenog pristupa koji podrazumijeva višestruko pogađanje lozinke za pristup. Učinak napada na informacije je uništenje jer napad za konačni cilj ima uklanjanje pristupnih prava žrtvi. Objekt napada je korisnik, a dosegnuta faza napada je potpuna kompromitacija. U članku se navodi da je pogođena samo jedna žrtva, a materijalne štete nije bilo jer žrtva nije platila traženu otkupninu za povrat korisničkog računa, već joj je nadležna služba nakon prijave incidenta vratila pristup korisničkom računu.

U članku „OPREZ Nova prijevara putem maila na bizarno jednostavan način izvlači novac od naivnih ljudi" (Index.hr, 26. svibnja 2017.) riječ je o dvije tvrtke s područja Karlovca koje se razlikuju po tome što je jedna uplatila novac napadaču, a druge nije. Vektor napada je socijalni inženjering jer se napadač predstavio kao direktor obje pogođene tvrtke te je tražio da mu se isplati novac na privatan račun u Španjolskoj. Operativni učinak napada je prijevara, a učinak napada na informacije nije zabilježen, tj. nema ga. Objekt napada je u oba slučaja bio korisnik, tj. djelatnica u tvrtki. Dosegnuta faza napada je dvojaka. Naime, u slučaju tvrtke koja nije isplatila novac riječ je o fazi isporuke iza koje nije slijedila faza ostvarivanja pristupa i kompromitacije, dok je u slučaju tvrtke koja je isplatila novac riječ o potpunoj kompromitaciji. Napadom su pogođene dvije tvrtke, a materijalna šteta, koja nije navedena u članku, prouzrokovana je u samo jednoj tvrtki.

Članak „Oprez na društvenim mrežama: Lažni general ženu iz Gruda koštao 20.000 kuna" objavio je tportal 6. rujna 2017. Prema vektoru napada riječ je socijalnom inženjeringu jer je lažnim predstavljanjem napadač na društvenoj mreži Facebook nagnao žrtvu na isplatu veće svote novaca. Operativni učinak napada je prijevara jer je riječ o lažnom predstavljanju napadača. Učinak napada na informacije nije zabilježen, tj. nema ga. Objekt napada je korisnik, a dosegnuta faza napada je potpuna kompromitacija jer je došlo do uplate na račun napadača. Ovom je prijevarom pogođen jedan korisnik, a materijalna šteta iznosi 20.000 kuna.

DISKUSIJA

Analizom i usporedbom računalno-sigurnosnih incidenata koji su imali izvorište ili objekt napada u hrvatskom IP adresnom prostoru ili .hr domeni, a o kojima su vijesti prenijeli internetski portali, te smještanjem tih incidenata u kontekst ukupnog broja sličnih incidenata u Hrvatskoj, jasno se može zaključiti kako incidenti, da bi ih se prikazalo u medijima, moraju uključivati značajnu novčanu štetu, moraju rezultirati prestankom rada nekog vitalnog sustava ili moraju biti povezani sa stvarnom osobom koja je žrtva. Podaci nadležnih službi pokazuju potpuno drugačiju situaciju i mediji naprosto cijeli jedan vid računalnih ugroza ne prikazuju.

Od 370 slučajeva *web defacementa*, najpopularnije vrste računalno-sigurnosnog incidenta, ne spominje se niti jedan. Doduše, incidenti ovog tipa ne uzrokuju gotovo nikakvu materijalnu štetu, napadaju ranjive i zastarjele internetske stranice, te ih, obično, izvode mladi hakeri željni uzbuđenja. Najčešće je riječ o upozorenjima poput „*We are anonymous*" i „*You have been hacked*", koja hakerima služe da pokažu svoje znanje i umješnost te postave dokaze o kompromitaciji na servisu pastebin.com, svojevrsnoj oglasnoj ploči na kojoj zlonamjerni hakeri opisuju napade koje su izveli.

Incidenata koji uključuju slanje *phishing* URL-ova bilo je 2017. godine 127, a o njima govore dva članka koja se odnose na isti incident. Štoviše, članci daju savjete za obranu od ove prijetnje nakon što je ona već otklonjena. Može se zaključiti da je vijest prenesena zbog toga što su je kao važnu označile nadležne službe koje su putem svojih komunikacijskih kanala upozorile korisnike, te zbog toga što je riječ o incidentu u kojem se napadač predstavljao kao upravna organizacija Ministarstva financija. Može se pretpostaviti da je šteta, iako nije službeno objavljena, bila zanemariva. Iz ovoga se može zaključiti da računalno-sigurnosni incidenti u Hrvatskoj nisu dovoljno zanimljivi da bi ih mediji prikazivali u istoj mjeri u kojoj su zastupljeni u pokazateljima nadležnih službi.

Iako je relativno velik broj članaka povezan s kibernetičkom sigurnošću, o incidentima u Hrvatskoj se govori veoma malo. Sagledaju li se ostali članci, može se zaključiti da prevladava diskurs koji govori o potencijalnim prijetnjama koje se kriju u svijetu oko nas. Naslovi poput „Roditelji, ako ste djeci kupili ovu lutku, odmah ju uništite!" (24sata, 18. veljače 2017.) i „Avione više ne rušimo kao nekad, dovoljan nam je iPad" (Express, 5. rujna 2018.) kod običnog korisnika izazivaju strah. Međutim, onima koji svakodnevno prate vijesti o kibernetičkoj sigurnosti ovakve vijesti nisu

novost. Usporedbe radi, dok 24sata govori o špijunskoj lutki, relevantni sigurnosni portali pišu o prijenosu signala putem zvuka koji proizvodi računalni ventilator (Greenberg 2018), očitavanju raspoloženja korisnika pomoću Wi-Fi signala (Murnane 2016) i hakiranju *pacemakera*[11]. Međutim, veoma je važno napomenuti, a to je ono što mediji ne spominju, da je riječ o teoretskim konceptima (engl. *Proof of Concept*) koje razvijaju vrhunski sigurnosni stručnjaci u kontroliranim okruženjima s jasnim ciljem osmišljavanja novih tehnika napada.

Možda najbolje glad medija za stvarnim računalno-sigurnosnim prijetnjama pokazuje situacija oko kampanje zlonamjernim *ransomware* sadržajem WannaCry. Službeni računi napadača koji je izveo napad javno su dostupni i prikazuju da je u cijeloj kampanji zarađeno svega 49,96959529 bitcoina (Collins 2017), što je tada iznosilo 120.055,58 američkih dolara, a zaraženo je više od 400.000 računala. Također, Kaspersky navodi da je 98% računala koristilo operativni sustav Windows 7, koji je pušten u javnost 2009. godine (Perekalin 2017). Valja ponovno napomenuti da je zakrpa koja je onemogućavala napad bila objavljena 91 dan prije globalne zaraze, a Julian Assange je u objavi ranjivosti koja je omogućila izvedbu ovog napada na stranici Wikileaks kazao:

> Postoji velik rizik od proliferacije kada govorimo o razvoju kibernetičkog „oružja". Nekontrolirana proliferacija takvog „oružja" je posljedica nemogućnosti da ga se ograniči i visoke cijene koju postiže na globalnom tržištu oružja. Značaj događaja „Year Zero" nadilazi mogućnost izbora između kibernetičkog rata i mira. Ova objava je izvanredna iz političke, pravne i forenzičke perspektive. (Vault 7: CIA Hacking Tools Revealed, 2017)

Međutim, iako je WannaCry bio idealan kandidat za izvedbu „kibernetičkog Pearl Harbora", zapravo je u svom dosegu i posljedicama podbacio. Nekako je za očekivati od tajnog kibernetičkog oružja koje razvijaju američke tajne službe da uzrokuje padove aviona i eksplozije nuklearnih elektrana, a ne da onemogući pristup zdravstvenim kartonima pacijenata i prekid prikazivanja voznog reda njemačke željeznice na kolodvorskim zaslonima. Napad je prekinuo MalwareTech, dvadesetdvogodišnji britanski stručnjak za kibernetičku sigurnost, koji je veoma povoljno kupio domenu koja je unutar koda samog sadržaja bila postavljena kao *kill switch* ili prekidač, te time zaustavio širenje zaraze. Takvo što ne može biti vezano uz globalnu prijetnju.

Hrvatski su se mediji također bavili zlonamjernim *ransomware* sadržajem WannaCry kao globalnom prijetnjom, iako je u Hrvatskoj zabilježeno svega 205 slučajeva zaraze. Štoviše, iz Ureda vijeća za nacionalnu sigurnost je kazano da WannaCry nije bio ozbiljna prijetnja. Međutim, o ovom su incidentu generirana 44 članka na pet najvećih portala, a i televizijske su kuće objavile izjave stručnjaka koji su pojasnili o čemu je točno riječ, zašto se trebamo bojati i na koji način se možemo zaštititi. Iako su objavljene složene upute za zaštitu računala, zapravo je trebalo napraviti redovnu nadogradnju operativnog sustava da bi se zaraza onemogućila.

[11] „Pronađene mnoge ranjivosti u pacemaker uređajima", CERT.hr, 6. lipnja 2017.

Mjesec dana kasnije odvijala se slična kampanja zlonamjernim *ransomware* sadržajem NotPetya, koju su mediji ponovno proglasili globalnim kibernetičkim napadom, a Index.hr je 27. lipnja 2017. objavio članak naslovljen „NOVI VELIKI CYBER NAPAD Hakirane tvrtke diljem svijeta, napadnut i Černobil". Napadom je pogođeno svega 16.500 uređaja, a u Černobilu je pogođen sustav za nadzor radijacije, ali opasnosti od radijacije nije bilo. Napad je iskorištavao potpuno iste ranjivosti kao i WannaCry, koje su bile zakrpane gotovo četiri mjeseca prije napada.

Uzme li se sve u obzir, možemo reći da je kibernetička sigurnost hipersekuritizirana, tj. da se naglašava mogućnost „cyber Pearl Harbora", iako dosadašnji podaci i slučajevi to ne pokazuju. Mediji u Hrvatskoj najčešće o kibernetičkoj sigurnosti govore kao o izvoru velikih prijetnji prenaglašavajući činjenicu da je riječ o globalnom problemu, pa tako svaku potencijalnu prijetnju prikazuju kao prijetnju koja može poremetiti život u Hrvatskoj. Međutim, činjenica je da je stvarna situacija zapravo medijski nezanimljiva, a mediji koriste svaku priliku da prijetnju uvećaju do krajnjih granica i izazovu još veći strah korisnika koji potom grozničavo slijede savjete tih istih medija kako bi se osjećali barem malo sigurnije.

Mediji daju savjete o tome što bi trebali poduzeti prilikom korištenja računala ili bilo kojeg elektroničkog uređaja, a mogu se odnositi na dodatnu provjeru identiteta osobe s kojom korisnici komuniciraju, nadogradnju antivirusnog programa, vanjsku provjeru uređaja poput bankomata, provjeru adresa kojima pristupaju, provjeru protokola koje koriste, provjeru adresa elektroničke pošte u tijelu zaglavlja, a ne u polju pošiljatelja jer se ono lako može lažirati. Međutim, mediji izbjegavaju napomenuti da je kod kibernetičke sigurnosti zdrav razum najbolja zaštita jer korisniku omogućava da na temelju dosadašnjih saznanja djeluje u novim situacijama i prepozna rizičnu situaciju.

Rječnikom teoretičara učenja, savjeti koje objavljuju mediji spadaju u pasivno učenje, tj. izravan transfer znanja, što je karakteristično za bihevioriste. S druge strane, kognitivisti učenje promatraju kao stvaranje kognitivnih struktura koje nam omogućavaju obradu novih informacija na temelju postojećih saznanja, te internalizaciju znanja kao aktivan proces. Ukratko, ne postoji popis koraka koje treba poduzeti da bi se prepoznala kibernetička prijetnja, nego treba naučiti prepoznati rizične situacije, što zahtijeva mnogo više truda, ulaganja, fleksibilnosti i, na koncu, sposobnost obrane od ugroza. Christopher Hadnagy, jedan od najpoznatijih sigurnosnih stručnjaka, utemeljitelj SECTF-a na DEFCON-u, smatra da kvalitetan sigurnosni program za osvještavanje važnosti pravilnog, odgovornog i opreznog pristupa ne čini objašnjavanje što je to dobra lozinka i od koliko bi se ona znakova trebala sastojati, već demonstracija koliko vremena hakeru treba da probije slabu lozinku (Hadnagy 2011: 343).

Krajnji korisnik bi trebao preuzeti tako definiran rizik te svoju kognitivnu suverenost, kako je naziva Beck (2001: 79), prepustiti stručnjacima jer je uzimanje sudbine u vlastite ruke nerealan i vrlo opasan potez (Furedi 2008: 107). Oni koji ne slijede te korake predstavljaju opasnost za sebe i cijeli sustav oko sebe, a pritisak se na njih vrši navođenjem najstrašnijeg scenarija uspješno izvedenog kibernetičkog napada.

Rizik svakako postoji, ali treba osvijestiti da običan korisnik jednostavno nije dovoljno atraktivna meta za potpunu demonstraciju moći kvalitetno izvedenog kibernetičkog napada. Stuxnet je između niza ostalih primjera pokazao što kibernetički napad zapravo može i da ne postoji zaštita od kvalitetno izvedenog kibernetičkog napada. S druge strane, Stuxnet je plod rada najviše razine sigurnosnih stručnjaka s gotovo neograničenim budžetom i ne bi bilo racionalno koristiti ga za iznudu novca ili krađu fotografija s računala.

Kada je riječ o sigurnosnim stručnjacima, svakako treba istaknuti da oni snažno utječu na tehnifikaciju diskursa i čine ga udaljenijim i nerazumljivijim običnom korisniku, što se vidi na temelju savjeta za zaštitu od računalno-sigurnosnih ugroza koje su objavile nadležne službe. Štoviše, oni su umnogome odvojeni od običnog korisnika i njegovih potreba. Koriste Linux, besplatan operativni sustav kojeg razvija zajednica računalnih stručnjaka i koji je nemjerljivo manje podložan kibernetičkim napadima od proizvoda tvrtke Microsoft. Usto oni sebe smatraju tehnološkom elitom koja običnim korisnicima pruža osnovne upute o tome kako se donekle zaštititi od najučestalijih trenutno aktivnih napada.

Razliku između računalno-sigurnosnih stručnjaka i običnog korisnika izvrsno ilustrira situacija kojoj je autor prisustvovao 2017. godine u Varaždinu na konferenciji o informacijskoj sigurnosti FSeC. Konferencija je bila podijeljena na izlagački dio i na službena predavanja i radionice. Predstavljajući Nacionalni CERT pokušalo se podijeliti promotivni materijal u obliku zapakirane USB memorije. Ubrzo je primijećeno da posjetitelji uzimaju sve promotivne materijale osim USB-ova. Kada je jedan od sigurnosnih stručnjaka posjetitelja upitan zašto je tome tako, odgovorio je: „Nikad ne uzimam nepoznat USB. Religija mi brani. Tko zna što se na njemu nalazi?"

ZAKLJUČAK

Kibernetička sigurnost svakako predstavlja značajan aspekt svakodnevnog života u informacijskom društvu, međutim važno je razlikovati svakodnevne slučajeve i dosege „uobičajenih dnevnih aktivnosti napadača" od korištenja posebno razvijenih kibernetičkih oružja koja se temelje na tajnim ranjivostima. Iako postoji mogućnost da kupac pametnog televizora bude prisluškivan i da se prikupljaju podaci o njemu, valja se zapitati kome bi bilo u interesu takvo što napraviti. Računalne prijevare se ne razlikuju, osim po mediju provedbe, od drugih prijevara, a napadač računa na lakovjernost i pohlepu žrtve, što se ne može anulirati doslovnim praćenjem općenito napisanih sigurnosnih praksi. Kibernetičko oružje ima stvaran potencijal za narušavanje sigurnosti, međutim takvi slučajevi su rijetki u svijetu, a pogotovo u Hrvatskoj. Mediji, s druge strane, svaku moguću prijetnju prikazuju kao hipersekuritiziranu, pretjeranu, gledajući samo krajnje posljedice uspješno izvedenog napada. Godine 2017. WannaCry je zbog 205 slučajeva zavrijedio čak 44 članka, dok su svi ostali računalno-sigurnosni incidenti medijski popraćeni u deset članaka.

Dobar je pokazatelj i broj registriranih *botova* u Hrvatskoj, koji se temelji na vanjskim izvorima koji dostavljaju informacije Nacionalnom CERT-u te prikazuju

okvir stvarnog stanja. Riječ je o broju zaraženih računala u Hrvatskoj, a koja su dio neke *botnet* mreže kojom upravlja zlonamjerni korisnik da bi izvodio DDoS i DoS napade. Ovaj tip zlonamjernog sadržaja ne ostavlja tragove na računalu, djeluje u pozadini i ni na koji način ne mijenja iskustvo korisnika na računalu. U Hrvatskoj je 2017. godine nekom vrstom zlonamjernog *botnet* sadržaja bilo zaraženo približno 320.000 uređaja koji su korišteni u izvedbi složenih napada. Međutim, zbog toga što ne postoji šteta za korisnika i riječ je o samo jednom uređaju koji čini milijunsku *bot* mrežu, ovaj podatak jednostavno nije dovoljno medijski atraktivan da bi se o njemu pisalo.

Činjenica je da je uređaja sve više i da s njima dolazi sve više prijetnji koje mogu biti ostvarene iskorištavanjem brojnih ranjivosti. Međutim, to što ranjivosti, a s njima i mogućnosti postoje, ne znači da će netko te ranjivosti stvarno i iskoristiti.

Nažalost, mediji stvaraju sliku u kojoj prijetnje izlaze iz svakog elektroničkog uređaja, ali se na temelju analize medijskog prostora može zaključiti da takvo što nije empirijski utemeljeno.

LITERATURA

B. S. 2017. Ne nasjedajte na ovaj lažni mail iz porezne, mogli biste ostati bez podataka. Tportal, 1. prosinca. https://www.tportal.hr/tehno/clanak/ne-nasjedajte-na-ovaj-lazni-mail-iz-porezne-mogli-biste-ostati-bez-podataka-20171201 (pristupljeno 5. rujna 2018.).

B. S. 2017. Oprez na društvenim mrežama: Lažni general ženu iz Gruda koštao 20.000 kuna. Tportal, 6. rujna. https://www.tportal.hr/tehno/clanak/oprez-na-drustvenim-mrezama-lazni-general-zenu-iz-gruda-kostao-20-000-kuna-20170906 (pristupljeno 5. rujna 2018.).

Beck, U. 2001. *Rizično društvo: u susret novoj moderni*. Beograd: Filip Višnjić.

Buzan, B., O. Wæver i J. de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Castells, M. 2000. *Uspon umreženog društva. Informacijsko doba: ekonomija, društvo, kultura. Svezak 1*. Zagreb: Golden marketing.

Castells, M. 2001. *The Internet Galaxy: Reflexions on the Internet, Business, and Society*. Oxford University Press. [Usp. M. Castells, *Internet galaksija: razmišljanja o internetu, poslovanju i društvu*, Zagreb: Naklada Jesenski i Turk – Hrvatsko sociološko društvo, 2003.]

Collins, K. 2017. The hackers behind the WannaCry ransomware attack have finally cashed out. Quartz, 3. kolovoza. https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/ (pristupljeno 1. rujna 2018.).

D. M. 2017. Lažni bankar prevario dvije žene, uzeo im 3.900 kuna za klađenje. Index.hr, 8. travnja. https://www.index.hr/vijesti/clanak/lazni-bankar-prevario-dvije-zene-uzeo-im-3900-kuna-za-kladjenje/962246.aspx (pristupljeno 7. rujna 2018.).

Furedi, F. 2008. *Politika straha: s onu stranu ljevice i desnice*. Zagreb: Izdanja Antibarbarus.

Godišnji izvještaj Nacionalnog CERT-a za 2017. godinu. https://www.cert.hr/wp-content/uploads/2018/03/CERT.hr_godisnji_izvjestaj_2017.pdf.

Greenberg, A. 2018. Mind the gap: This researcher steals data with noise, light, and magnets. Wired, 2. srpnja. https://www.wired.com/story/air-gap-researcher-mordechai-guri/ (pristupljeno 28. kolovoza 2018.).

Hadnagy, C. 2011. *Social Engineering: The Art of Human Hacking*. Wiley.

Hakeri srušili sustav KBC-a Sestara milosrdnica, pacijenti ostali bez snimaka lomova. 2017. vecernji.hr, 12. siječnja. https://www.vecernji.hr/vijesti/hakeri-sruseli-sustav-kbc-a-sestara-milosrdnica-pacijenit-ostali-bez-snimaka-lomova-1141823 (pristupljeno 5. rujna 2018.).

Hansen, L. i H. Nissenbaum. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53(4): 1155–1175.

Hruškovec, I. 2017. Kriminalci u akciji: Kako ćete zaštititi svoju karticu od krađe. 24sata, 27. listopada. https://www.24sata.hr/tech/kriminalci-u-akciji-kako-cete-zastititi-svoju-karticu-od-kra-e-545891 (pristupljeno 6. rujna 2018.).

Hruškovec, I. 2017. Nova prijetnja: Poruke iz lažne Porezne žele do vaših podataka. 24sata, 12. siječnja. https://www.24sata.hr/tech/nova-prijetnja-poruke-iz-lazne-porezne-zele-do-vasih-podataka-550701 (pristupljeno 6. rujna 2018.).

I. G. 2017. Hakeri od Cro Copa tražili otkupninu: "Bolje mu je da ga ne nađu, ako ga nađe policija – jadna mu majka". Index.hr, 28. travnja. https://www.index.hr/sport/clanak/hakeri-od-cro-copa-trazili-otkupninu-bolje-mu-je-da-ga-ne-nadju-ako-ga-nadje-policija-jadna-mu-majka/966418.aspx (pristupljeno 7. rujna 2018.).

Jožanc, N. 2015. Studija slučaja u komparativnoj politici. *Politička misao* 52(3): 35–58.

Jurić, M. 2017. Lopovi imaju sve naprednije metode za varanje građana, ali zaštititi se možete na prilično jednostavan način. Dnevnik.hr, 2. studenoga. https://dnevnik.hr/vijesti/hrvatska/iako-su-pokusaji-prijevara-sve-napredniji-svijest-gradjana-jos-je-uvijek-jako-niska---494631.html (pristupljeno 5. rujna 2018.).

Littman, J. 1996. *The Fugitive Game: Online with Kevin Mitnick*. Little, Brown & Co.

M. V. 2017. OPREZ Nova prijevara putem maila na bizarno jednostavan način izvlači novac od naivnih ljudi. Index.hr, 26. svibnja. https://www.index.hr/vijesti/clanak/oprez-nova-prijevara-putem-maila-na-bizarno-jednostavan-nacin-izvlaci-novac-od-naivnih-ljudi/972860.aspx (pristupljeno 6. rujna 2018.).

McDonald, M. 2008. Constructivisms. U: *Security Studies: An Introduction*, ur. P. D. Williams i M. McDonald. Routledge. Str. 152–169.

Murnane, K. 2016. Scientists Can Use WiFi To Read Your Emotions. Forbes, 20. rujna. https://www.forbes.com/sites/kevinmurnane/2016/09/20/mits-csail-lab-creates-a-system-that-identifies-peoples-emotions-using-wireless-signals/#4ee06c866b53 (pristupljeno 1. rujna 2018.).

Nacionalna taksonomija računalno-sigurnosnih incidenata. 2018. https://www.cert.hr/wp-content/uploads/2018/06/Nacionalna-taksonomija-ra%C4%8Dunalno-sigurnosnih-incidenata.pdf.

Negovetić L. i B. Blotnej. 2017. Hakeri napali Traumatologiju: Srušio se sustav s podacima. 24sata, 12. siječnja. https://www.24sata.hr/news/hakeri-napali-traumatologiju-srusio-se-sustav-s-podacima-506981 (pristupljeno 7. rujna 2018.).

Perekalin, A. 2017. WannaCry: Are you safe? Kaspersky Lab, 13. svibnja. https://www.kaspersky.com/blog/wannacry-ransomware/16518/ (pristupljeno 10. rujna 2018.).

Pronađene mnoge ranjivosti u pacemaker uređajima. 2017. CERT.hr, 6. lipnja. https://www.cert.hr/31250/ (pristupljeno 10. rujna 2018.).

„Roditelji, ako ste djeci kupili ovu lutku, odmah ju uništite!" 2017. 24sata, 18. veljače. https://www.24sata.hr/tech/roditelji-ako-ste-djeci-kupili-ovu-lutku-odmah-ju-unistite-512186 (pristupljeno 6. rujna 2018.).

Schatz, D., R. Bashroush i J. Wall. 2017. Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law* 12(2): 53–74.

Statistički pregled temeljnih sigurnosnih pokazatelja i rezultata rada u 2017. godini Ministarstva unutarnjih poslova. Zagreb, siječanj 2018.

Vault 7: CIA Hacking Tools Revealed. 2017. WikiLeaks, 7. ožujka. https://wikileaks.org/ciav7p1/ (pristupljeno 10. kolovoza 2018.).

Vojković, G. i Štambuk-Sunjić, M. 2006. Konvencija o kibernetičkom kriminalu i kazneni zakon Republike Hrvatske. *Zbornik radova Pravnog fakulteta u Splitu* 43(1): 123–136.

Yin, R. K. 1984. *Case Study Research: Design and Methods*. SAGE Publications.

Ž. L. 2017. NOVI VELIKI CYBER NAPAD Hakirane tvrtke diljem svijeta, napadnut i Černobil. Index.hr, 27. lipnja. https://www.index.hr/vijesti/clanak/novi-napad-hakirane-tvrtke-diljem-europe-nikada-nece-prestati-ovako-previse-zaradjuju/979406.aspx (pristupljeno 5. rujna 2018.).

CYBER-SECURITY IN CROATIAN MEDIA

Svan Hlača

SUMMARY

This study gives an overview of cyber security in Republic of Croatia with special focus on cyber security incidents that had their point of origin or target in Croatian IP space or .hr domain. Analysis of relevant Internet articles of five most popular Croatian news portals will show in what relation does it stand to number of cyber security incidents. Furthermore, to describe progress of cyber security, evolution of Internet, cyber culture and cyber space will be shown. By concepts of securitization and especially hypersecuritization, everyday security practices and discourse techification, the picture of cyber security in public will be shown as will be the position of which actors of securitization predict for basic users.

Keywords: cyber security, security, securitization, incidents, hackers.