ECOLOGICA, Vol. 30, No 109 (2023), 115-120
https://doi.org/10.18485/ecologica.2023.30.109.16
Originalni naučni rad
UDC: 351.817:004.738.5]:640.4

Uticaj sajber bezbednosti na hotelijerstvo i životnu sredinu

The impact of cyber security on the hotel industry and the environment

Jelena Petrović[1], Dragan Živković[2], Jovan Rudež[3]*

[1] Univerzitet Singidunum, Danijelova 32, 11000 Beograd, Srbija /
Singidunum University, 32 Danijelova, 11000 Belgrade, Serbia

[2]Alfa BK Univerzitet, Fakultet za finansije, bankarstvo i reviziju, Palmira Toljatija 3, Beograd, Srbija /
Alfa BK University, Faculty of Finance, Banking and Auditing, Palmira Toljatija 3, Belgrade, Serbia

[3]MUP RS Sektor za vanredne situacije, Uprava Novi Sad, Srbija /
Ministry of Internal Affairs RS, Department for Emergency Situations, Administration Novi Sad, Serbia

*Autor za prepisku / Corresponding author

Rad primljen / Received: 18.01.2023, Rad prihvaćen / Accepted: 20.02.2023.

Sažetak: U uslovima globalnog turističkog poslovanja, turizam se neprekidno suočava sa krizama koje utiču na njegov razvoj. Turizam je za posledicu imao pad turističkog prometa i prihoda, sa manjim ili većim uticajima na svetska turistička kretanja. Sa visokom tehnologijom dolazi i visokotehnološki kriminal poznat kao sajber kriminal koji se izvršava u sajber (računarskom) prostoru. On obuhvata sve radnje koje nisu dozvoljene u "realnom" svetu. U radu se objašnjava značaj sajber bezbednosti u poslovanju rada hotela ali i uticaja na ekološku sredinu u turizmu. U sajber napadima koriste se inovativne tehnike koje su sve teže za otkrivanje napadača sa opštom tendencijom u povećanju automatizacije napada. To znači da rezultati dejstva mogu imati različite vrste posledica po ciljne sisteme, koji se mogu manifestovati na fizičkom, logičkom i informacionom nivou. Destinacija ili poslovni brend mogu da pretrpe veliku štetu.

Ključne reči: Bezbednost, IKT tehnologija, zloupotrebe, računarske mreže, hotelijerstvo.

Abstract: In terms of global tourism business, tourism constantly faces crises that affect its development. Tourism has resulted in the decline in tourism traffic and tourism receipts, with major or minor impacts on global tourism trends. With high technology comes high-tech crime known as cybercrime that is committed in cyberspace. It covers all actions that are not allowed in the "real" world. The paper explains the importance of cyber security in the operation of the hotel, but also the impact on the ecological environment in tourism. Cyber attacks use innovative techniques that are increasingly difficult to detect attackers with a general tendency to increase attack automation. This means that the results of the action can have different types of consequences for the target systems, which can be manifested on the physical, logical and informational level. A destination or business brand can suffer great damage.

Keywords: Security, ICT technology, misuse, computer networks, hotel industry.

[1]orcid.org/0000-0002-8908-6431, e-mail: jelena1902@gmail.com
[2]orcid.org/0000-0002-5022-2651, e-mail: dragan.zivkovic@alfa.edu.rs
[3]orcid.org/0000-0003-4910-4946, e-mail:jovan.rudez@gmail.com

UVOD / INTRODUCTION

Zahvaljujući Internetu, mobilnim telefonima, WiFi, i ostalim pametnim tehnologijama, pojedinci, kompanije i institucije su umreženiji nego ikad do sada. Međutim, tehnologija koja olakšava življenje, ujedno ga mnogo i komplikuje. Savremena era globalne informaciono-tehnološke i komunikacijske povezanosti odnosno visoke tehnološke zavisnosti iziskuje adekvatnu zaštitu, a izgradnja sigurnog sajber okruženja dolaze u prvi plan internet komunikacija. Stoga se na međunarodnom i nacionalnom nivou usvajaju normativni i strateški dokumenti sa ciljem unapređenja stanja bezbednosti i redukcije heterogenih rizika po pojedince, organizacije i države. To upućuje da je problem bezbednosti u sajber prostoru postao tema od globalnog značaja zbog narastajućih potreba čoveka u virtualnom svetu i zavisnosti funkcionisanja čoveka od informaciono-komunikacionih tehnologija, koje su povećale brzinu i obim interakcija. Sajber kriminal kao i hibridni rat deluje na sve pore društvenog i privrednog života. Međutim, u ovom radu posmatraćemo njihov uticaj na turistička kretanja i rad hotela kao i uticaj na životnu sredinu. Napadači sve češće biraju ne samo tehnike i metode napada već i ciljeve i vreme napada. Napadi na turističke objekte uključujući i hotele sve su češći, a potencijalna ugroženost turista i gostiju postaje sve veća. To ostavlja teške posledice po mobilnost turista i njihovu bezbednost ali i na adekvatnu zaštitu životne sredine, koje posledično utiče na popunjenost hotelskih kapaciteta.

1. HIBRIDNI RAT I UTICAJ NA HOTELIJERSTVO / HYBRID WAR AND ITS IMPACT ON THE HOTEL INDUSTRY

Hibridni rat nije potpuno definisan u teorijskom ali nije ni u praktičnom smislu. Ovo je relativno nova pojava koja se u turbulentnim nivoima brzo širi i deluje na sve oblike društvenog života, na pojedince i ustanove. Stratezima ove vrste agresije odgovara da se što manje zna o ovoj vrsti „ratovanja“, jer što se o njemu manje zna, njegove metode su uspešnije i razornije. U tom smislu, u prvi mah, malo su vidljive i njegove posledice po životnu sredinu. Tako i eksperti imaju problema da usaglase svoje stavove, a laici ga apsolutno ne prepoznaju (usavršavale su ga moćne obaveštajne službe SAD, kao proširenu verziju specijalnog rata). Formulisan je kao vojna strategija, idealna za agresiju na druge države, zato što su njegove metode delovanja, u toj meri podmukle i prikrivene da ne mogu biti sankcionisane međunarodnim zakonima. Njima se ostvaruju isti ciljevi kao konvencionalnim ratom, s tim što vojna agresija nailazi na osudu, a hibridna agresija prolazi tiho, kao da agresor nema nikakve veze s onim što se događa u državi koju napada. Praksa pokazuje da hibridni rat, gde se ciljevi postižu podrivanjem, „obojenim revolucijama“ i prevratom, daje dugoročno bolje rezultate od konvencionalne agresije, gde je situacija i nakon pobede rovita i neizvesna. Srbija je država koja ima najviše iskustva s hibridnim napadima. Osnovni problem kod suprostavljanja jeste blagovremeno prepoznavanje oblika i izvora bezbednosne pretnje jer je redovno dobro prikrivena i maskirana „dobrim namerama“. Pravi način odbrane je raskrinkavanje napada i napadača, edukacija stanovništva i operativni prodor u centre za vođenje hibridnog rata protiv Srbije, sa izuzetnom obuhvaćenošću i perfidnošću. Prikrivenost metoda delovanja omogućava projektovanje „istine“ i uticaj na politička i društvena zbivanja. Stoga, sajber-odbranu ne treba smatrati samo reakcijom na napade i naporima da se napadači iz sajber-prostora odvrate, odbiju napadi i da se, u slučaju potrebe, povrate vlastite sposobnosti i resursi u stanje pre napada. Sajber terorizam ugrožava čitavo čovečanstvo. Kada je u pitanju turizam, na meti su transportni sistemi (vodeni, kopneni, vazdušni), hotelsko-ugostiteljski kapaciteti, kongresi, festivali, karnevali, sportske priredbe, itd. Cilj je nanošenje materijalne štete i ljudskih žrtava. Inače, teroristički napadi se odlikuju sledećim karakteristikama (Štetić, 2017):

1) njihovi ciljevi su što veći broj ljudi zbog publiciteta i upoznavanja javnosti sa borbom koju vode;

2) izražena je isključivo politička pozadina napada i ukupnog odnosa (tzv. model Robin Hud);

3) nikakve žrtve, i posledice po životnu sredinu, nisu važne, bitan je postignut politički cilj;

4) što se daje veći publicitet događaju, to je veći značaj njihove ideje;

5) obučeni teroristi biraju vrstu turizma (domaći, međunarodni), i vrstu oružja (hemijsko, vatreno);

6) statistički podaci o žrtvama su vrlo važan podatak i pokazatelj snage terorista, pa je njihovo ponavljanje u medijima za njih veoma važno;

7) teroristima je potrebna reklama, a turizam ima mogućnost velikog publiciteta;

8) turizam i njegova masovnost su idealni za infiltraciju terorista;

9) pored štete koju nanosi turizmu, ima uticaja i na delatnosti koje su povezane sa turizmom.

Problem stvaranja bezbednog sajber okruženja je višedimenzionalan i zahteva koordinisano delovanje različitih faktora, odnosno institucija i tela. Normativna regulativa u sferi sajber bezbednosti je od velikog značaja, ali ako izostanu strategije, politike, akcioni planovi i mere kojima se implementiraju zakonska rešenja, svi napori zakonodavca ostaju uzaludni (Milošević, Putnik, 2017, str. 187). S druge

strane, treba imati u vidu da visok stepen tajnosti karakteriše rad na obaveštajno bezbednosnom prikupljanju i obradi podataka, uz poštovanje i načela efikasnosti i ekonomičnosti rada službi bezbednosti.

2. KRAĐA PODATAKA I KREDITNIH KARTICA: primer Revenge Hotels / DATA AND CREDIT CARD THEFT: example of Revenge Hotels

Kompanija Kasperski sprovela je istraživanje koje se odnosi na Revenge Hotels kampanju, usmerenu na sektor hotelijerstva, i konstatovala da je preko 20 hotela bilo pod udarom ciljanih sajber napada (Kovačević, 2019). Međutim, veliki broj hotela širom sveta postalo je žrtva velikih hakerskih napada. Neosporno, pod udarcima sajber kriminala, ugroženi su brojni hoteli širom sveta. Na primer, podaci kreditnih kartica koji se skladište u administrativnom sistemu hotela, uključujući i one dobijene od onlajn turističkih agencija (OATs), su pod rizikom da budu ukradeni i prodati kriminalcima širom sveta. Revenge Hotels je kampanja koja uključuje različite grupe koji koriste tradicionalne daljinske Trojance (RATs) kako bi inficirali hotelske kompanije koje se nalaze u vrlo osetljivom sektoru hotelijerstva. Kampanja je aktivna od 2015 godine, ali je povećala svoje prisustvo tokom 2019. godine. U doba zdravstvene krize tokom 2020 i 2021 godine aktivnosti su, gotovo, prepolovljene. Najmanje dve grupe, Revenge Hotels i ProCC, su identifikovane kao deo kampanje, međutim više sajberkriminalnih grupa je potencijalno uključeno. Glavni vektor napada u ovoj kampanji su i-mejlovi sa priloženim malicioznim Word, Excel ili PDF dokumentima. Neki od njih koriste exploit CVE-2017-0199, preuzimajući ga pomoću VBS i PowerShell skripti i zatim instalirajući prilagođene verzije raznih daljinskih trojanaca ili drugih prilagođenih malvera, poput ProCC, na uređaj žrtve kako bi kasnije mogli da izvršavaju komande i uspostave daljinski pristup inficiranim sistemima. Svaki fišing i-mejl je sastavljen sa posebnom pažnjom za detalje i uglavnom imitira prave ljude iz legitimnih organizacija koji prave lažni zahtev za rezervaciju za veliku grupu ljudi. Vredno je napomenuti da bi čak i oprezni korisnici mogli biti prevareni da otvore i preuzmu priložene materijale iz ovakvih mejlova jer oni sadrže brojne detalje (na primer, kopije pravnih dokumenata i razloge za rezervaciju) i izgledaju uverljivo. Jedini detalj koji može otkriti napadača bio bi pogrešno napisan domen organizacije (typosquatting). Međutim, kada se jednom inficira, računaru se može pristupiti daljinski ne samo od strane same sajberkriminalne grupe – dokazi prikupljeni od strane istraživača kompanije Kaspersky pokazuju da se daljinski pristup hotelijerskim recepcijama i podacima koje oni sadrže prodaju na kriminalnim forumima na pretplatničkoj osnovi. Malver sakuplja podatke sa klipborda hotelskih recepcija, kalemova štampača i zabeleženih skrinšotova (ova funkcija se aktivira korišćenjem određenih reči na engleskom ili portugalskom). Zbog toga što osoblje hotela često kopira podatke kreditnih kartica gostiju sa sajtova onlajn turističkih agencija kako bi im naplatili, ovi podaci mogu takođe biti kompromitovani. Međutim, prema podacima dobijenim sa Bit.ly, popularnog sajta za skraćivanje linkova koji koriste napadači da šire maliciozne linkove, istraživači kompanije Kaspersky pretpostavljaju da su i korisnici iz mnogih zemalja bar pristupili malicioznim linkovima – što znači da broj zemalja sa potencijalnim žrtvama može biti veći. „Kako korisnici postaju svesniji toga koliko su zaista njihovi podaci zaštićeni, sajber kriminalci se okreću malim preduzećima, koja često nisu dobro zaštićena od sajber napada i poseduju značajnu koncentraciju ličnih podataka. Hotelijeri i druga mala preduzeća koja rade sa korisničkim podacima moraju da budu oprezniji i primenjuju profesionalna bezbednosna rešenja kako bi izbegli curenje podataka koje potencijalno može uticati ne samo na korisnike već i ugroziti reputaciju hotela“ (Besthuzev, 2022). Kako bi ostali bezbedni, putnicima se preporučuje (Kovačević, 2019):

- Koristite virtuelne kartice za plaćanje rezervacija napravljenih preko onlajn turističkih agencija, jer ovakve kartice isteknu posle jednog plaćanja
- Kada plaćate za rezervaciju ili se odjavljujete sa recepcije hotela, koristite virtuelni novčanik, kao što je Apple Pay ili Google Pay, ili sekundarnu kreditnu karticu sa ograničenim dostupnim sredstvima

Vlasnicima hotela i menadžmentu se takođe savetuje da prate sledeće korake kako bi osigurali bezbednost korisničkih podataka (Kaspersky Endpoint Security for Business, 2022):

- Sprovođenje procene rizika postojeće mreže i implementacija regulacije o tome kako se upravlja korisničkim podacima.
- Korišćenje pouzdanog bezbednosnog rešenja sa veb zaštitom i funkcijom kontrole aplikacija, poput Kaspersky Endpoint Security for Business. Veb zaštita pomaže u blokiranju pristupa fišing i malicioznim veb sajtovima dok kontrola aplikacija (u modu bele liste) osigurava da nijedna aplikacija osim onih sa bele liste ne može biti pokrenuta na računarima hotelijerske recepcije.
- Uvođenje obuke podizanja svesti o bezbednosti za osoblje kako biste ih naučili kako da

uoče pokušaje fišinga i ukazali na značaj opreznosti tokom rada sa dolazećim i-mejlovima.

3. OBLICI SAJBER KRIMINALA / FORMS OF CYBER CRIME

Sajber terorizam najčešće se izvodi plasiranjem zlonamernih programa kroz računarske mreže, računare i uređaje za elektronsku obradu podataka. Odbrana od sajber terorista je izuzetno odgovoran i komplikovan zadatak. Sajber kriminal (kompjuterski kriminal) javlja se u raznim oblicima, koji imaju za cilj eksploataciju podataka, ali i nanošenje štete, ali posredstvom sajber prostora. Najčešće se realizuje putem malicioznih programa (malware). Reč je o štetnim programi koje sajber kriminalci koriste kako bi pristupili tuđim računarima i naneli štetu. Oni se javljaju u sledećim oblicima (Jonev, 2016, str. 206):

- *Virusi/trojanci* – prepoznaćete ih po promenama u radu računara, pojavljivanju prozora i poruka koje iskaču, ili po promenjenim ili obrisanim datotekama.
- *Spyware/Adware* – spyware služi za praćenje, odnosno „špijuniranje“ vaših aktivnosti dok koristite internet, a adware instalira prozore i poruke koje iskaču. Najčešće se javljaju zajedno.
- *Ransomware (sajber iznuda)* – nešto ozbiljniji oblik ugrožene sajber bezbednosti, gde gubite kontrolu nad vašim informacijama, a haker traži određena novčana sredstva da vam ih vrati nazad.
- *Scareware* – prevara korisnika gde se on uverava da je njegov računar napao virus, te mu se savetuje da kupi antivirus program koji uopšte ne postoji.
- *Krađa indentiteta* – često se javlja kao sledeći korak sajber kriminalaca nakon krađe podataka („curenje podataka“), a može biti ugrožena i fizička bezbednost osobe čiji je identitet preuzet. Posebno je česta preko društvenih mreža, što je bio jedan od glavnih razloga zašto je uvedena Opšta uredba o zaštiti podataka o ličnosti (GDPR), i njena paralela u našem zakonu – Zakon o zaštiti podataka o ličnosti.
- *Fišing (phishing)* – prevare putem mejla gde sajber kriminalci pokušavaju da dobiju poverljive informacije poput lozinki, broja računa, korisničkih imena, i slično. Najčešće se prevaranti predstavljaju kao neke kompanije, pojedinci u nevolji ili organizacije, kako bi delovali verodostojno.

Ovi oblici mogu se javljati i kod pravnih i kod fizičkih lica, s tim što ukoliko je u pitanju kompanija, to može dovesti i do ogromnih gubitaka.

Postoji, još uvek, problem međunarodne zajednice u potpunom definisanju i interpretaciji pojma sajber terorizma.

Naime, pojam se često zloupotrebljava a ponekad se ne objašnjava na pravi način. To znači, između ostalog, da svaki sajber napad ne mora biti okarakterisan kao terorizam (Denning, 2001). Vrlo tanka linija, između sajber vandalizma (ubačen virus na sajt), sajber incidenata, jačih sajber napada (upada na mrežu), i akata sajber terorizma često se ne adekvatno interpretira, što ne daje mogućnost da se bolje sagleda i analizira suština. Svakodnevni pristup društvenim mrežama, u bilo kom vidu (video, fotografije, vandalizam sajtova) omogućavaju da terorističke grupe, na globalnom nivou, to koriste u vidu svoje efikasne i efektivne propagandne aktivnosti. S druge strane, te aktivnosti se ne mogu uvek smatrati izvornim aktom sajber terorizma, odnosno jačim napadom kriminalnih aktivnosti. Ozbiljni napadi terorista na vitalne infrastrukture jedne države kao što su brane, vodovodni sistemi, snabdevanje električnom energijom, kontrola vazdušnog saobraćaja, nuklearna postrojenja, i drugi incidenti koji mogu narušavati prirodnu ravnotežu, te mogu dovesti do fizičkog oštećenja, uništenja i svih drugih oblika ugrožavanja životne sredine.

4. SEKJURITIZACIJA SAJBER PRETNJI / SECURITIZATION OF CYBER THREATS

Imajući u vidu da je poreklo sajber pretnji teško odrediti (najbolji primer za to je prijave podmetnutih bombi u škole i institucije u Srbiji u proleće 2022 godine), kao i da je njihove posledice teško predvideti, jedno od osnovnih pitanja koje se nameće je pitanje institucionalizacije reagovanja na ove pretnje. Stoga je neophodno skup sajber pretnji smestiti u bezbednosno relevantne okvire, odnosno obaviti njihovu sekjuritizaciju. Sekjuritizujući sajber pretnje, učesnik sekjuritizacije nastoji da ih predstavi kao pretnje koje ugrožavaju tačno određene vrednosti. Ukoliko se materijalizuju mogu izazvati katastrofalne posledice te je neophodno usvojiti određene mere kako bismo se na adekvatan način suprotstavili egzistencijalnim pretnjama. Stoga je neophodno usvojiti mere po hitnom postupku, koje nakon odobrenja od publike, postaju specijalne mere koje se usvajaju te postaju institucionalan, legalan način suočavanja sa pretnjama, čime se završava proces sekjuritizacije. U tom postupku postoji veći broj pristupa pomoću kojih se rešavaju osnovna pitanja bezbednosti sajber prostora i sajber pretnji, odnosno utvrđivanja načina kako su ta pitanja postala bezbednosno relevantna. U analizi mogu da se koristi osnovni,

bazični koncept sekjuritizacije, koncept frejminga i sajber sektorski pristup.

Može se pretpostaviti da za predstavljanje i konstrukciju bezbednosti nije neophodno postojanje objektivne pretnje već pokušaj njenog određivanja kroz proces sekjuritizacije. Znači da sekjuritizaciju treba sagledati kao sredstvo razumevanja i procesa konstrukcije onoga što se smatra pretnjom i kolektivno odgovoriti na nju (Buzan i dr., 1998). Kao osnovni elementi koncepta sekjuritizacije izdvajaju se (Gnjatović, 2018): sekjuritizirajući akteri, funkcionalni akteri, govorni čin, publika i specijalne mere. Publika predstavlja jedan od vodećih predmeta konstruktivnih kritika u periodu posle konačnog utemeljenja koncepta sekjuritizacije. Ona predstavlja one kojima se sekjuritizirajući akteri obraćaju i od nje zavisi da li će neki sekjuritizirajući potez biti uspešan i dobiti „titulu“ uspešno sprovedene sekjuritizacije ili će pak ostati na nivou sekjuritizirajućeg poteza. Publika u stvari ovlašćuje sekjutirizirajućeg aktera da primeni specijalne mere prihvatanjem njegovog poteza (Balzacq, 2010, p.12).

Sekjuritizacija je formulisana kao krajnje intersubjektivna kategorija, na tragu pitanja o uspešnosti odnosno neuspešnosti, kao praktičnog uzdizanja određenog pitanja na bezbednosnu agendu. Na osnovu određenih uslova, u okviru teorije govornih činova, kao intelektualne prethodnice koncepta sekjuritizacije, razvijeni su određeni olakšavajući uslovi za uspešan bezbednosni govorni akt (Waever, 2003):

(1) zahtev koji je u osnovi govornog čina mora ispoštovati bezbednosnu gramatiku i oformiti jaku vezu (tačku bez povratka ili mogućeg izlaza) sa egzestencijalnom pretnjom;

(2) Sekjuritizirajući akter, koji deluje sa pozicije autoriteta, mora posedovati socijalni kapital;

(3) Moraju postojati određene istorijske okolnosti u vezi sa pretnjom.

Ovo nisu neophodni uslovi, ali svakako olakšavaju sam proces konstruisanja pretnji, u smislu da bi trebalo da pozitivno utiču i na kraju dovedu do uspešnog procesa sekjuritizacije.

U savremenim uslovima, za razumevanje politike pretnje neophodno je koristiti koncept frejminga. On predstavlja simboličko takmičenje više društvenih značenja nekog domena pitanja, gde značenje implicira ne samo ono što je u pitanju, već i ono što treba učiniti. Koncept frejminga naglašava perceptivni, integrativni i reprezentativni aspekt bezbednosti. Pretnje, rizici, opasnosti – jesu slike sa negativnom konotacijom. Ovo korespondira sa određenjem pretnji u konceptu sekjuterizacije (Eriksson, 2001). Takođe, u konceptu frejminga pravi se razlika između dijagnostičke i prognostičke funkcije okvira. Naime, dijagnostička funkcija govori o dijagnozi posmatranog problema, koji se odnosi na identifikaciju uzroka problema. Prognostička funkcija govori o potrazi za rešenjima određenog problema. Stoga se određuju četiri uslova koji mogu poboljšati frejming određene pretnje, a to su (Petrović, 2019):

(1) *akter frejminga* – teži da određenu pojavu ili pitanje predstavi na način koji je prethodno utvrđen i koji ima određeni cilj (svako može biti akter – ali su to uglavnom političari, birokrate, eksperti, mediji, uticajne grupe i akademski radnici;

(2) *tip referentnog objekta* – ono što bi trebalo da se zaštiti i u fokusu egzistencijalnih pretnji;

(3) *karakteristike okvira/frama* kao deo bezbednosnih pretnji koje mogu biti ograničene, otvorene i orijentisane ka pretnji;

(4) *kontinuitet ili promena okvira* – pod uticajem stepena konsenzusa ili konflikta.

ZAKLJUČAK / CONCLUSION

U savremenim uslovima poslovanja hoteli su ne retko izloženi sajber napadima. Stoga je neophodno preventivno delovanje i odbrana čiji je cilj da se zaštite i očuvaju vlastite operativne i funkcionalne sposobnosti, podaci i informacije, sistemi, kao i ljudi i sistemi koji zavise od njih. To iziskuje da u hotelu treba da postoji stručnjak koji je posebno zadužen za informacionu bezbednost i sajber-odbranu, a bira se iz redova inženjera, tehničara i drugih stručnjaka iz domena informacionih i drugih tehnologija. Neophodno je osposobljavati učesnike u elektronskom saobraćaju (pošti) da se mogu zaštititi od različitih cyber napada, i zaštiti različite IT sisteme u sve turbulentnijem okruženju. Ljudi treba da znaju da samostalno testiraju svoje sisteme da bi znali koliko su, zapravo, bezbedni kroz proces penetracionog testiranja. Edukovanje o sajber bezbednosti se odnosi na sve koji žele da uđu u svet sajber poslovanja. To su lica odgovorna za zaštitu poslovnih informacija, rukovodioci i zaposleni u službi za bezbednost informacionog sistema, odgovorna lica zadužena za IKT infrastrukturu i arhitekturu, svi koji imaju potrebu za zaštitom pristupa kao i zaštitom samih informacija. U 2022. godini, od početka ratnog stanja u Ukrajini, Srbija je bila podložna najezdi lažnih dojava o podmetnutim bombama, uglavnom kao posledica njene spoljne politike. S druge strane, za specijalističke timove za protivdiverzionu zaštitu nije bilo odmora – izvršili su na hiljade pregleda velikog broja evakuisanih. Bez izuzetka sve prijave su bile lažne. S razvojem interneta nastao je i termin hibridnog rata. Stoga je neophodno preduzimati niz preventivnih i zaštitnih mera kako bi se pretnje od sajber terorizma, kao i njegove posledice, svele na najmanju moguću meru. To je u cilju zaštite putovanja i smeštaja gostiju u hotelske kapacitete i osiguranja

njihove bezbednosti. S druge strane to obezbeđuje zaštitu životne sredine i pravilan ekološki tretman okruženja odnosno turističke destinacije.

LITERATURA / REFERENCES

[1] Balzacq, T. (2010). *Securatization theory: how security problems emerge and dislove*, Routledge. UK, p.12.

[2] Besthuzev, D. (2022). GreAT tim, www.kaspersky.org

[3] Buzan, B., Waever, O., & Wilde, J. (1998). *Security: A new framework for analysis*, Lynne Reinner Publishers, p.167.

[4] Denning, D. (2001). Activism, Hactivism, Cyberterrorism. In: J. Arquilla, D. Ronfelt, (eds), *Networks and Netwars: The future of terror, crime, and militancy*. RAND, (pp. 239-288). https://www.rand.org/pubs/monograph_reports/MR1382.html, dostupno 1.4.2022.

[5] Eriksson, J. (ed). (2001). *Threat Politics: New Perspectives on Security, Risk and Crissis Management*, Aldershot: Ashage Publishing.

[6] Gnjatović, M. (2018). Primena koncepta frejminga u sekuritizaciji sajber pretnji, *Godišnjak fakulteta bezbednosti*, Beograd, str.153-168.

[7] Jonev, K. (2016). Sajber terorizam i upotreba sajber prostora u terorističke svrhe, *Bezbednost*, Beograd, 58(2), 206-222.

[8] Kaspersky Endpoint Security for Business, 2022.

[9] Kovačević, N. (2019). Ne tako sigurna putovanja: sajber kriminalci kradu podatke kreditnih kartica gostiju hotela širom sveta. https://turizmarium.ogledalo.rs/2019/12/ne-tako-sigurna-putovanja-sajber-kriminalci-kradu-podatke-kreditnih-kartica-gostiju-hotela-sirom-sveta/, dostupno 1.4.2022.

[10] Milošević, M., Putnik, N. (2017). Sajber bezbednost i zaštita od visokotehnološkog kriminala u republici Srbiji – strateški i pravni okvir, *Kultura polisa*, Novi Sad, 14(33), 177-191.

[11] Petrović, P. (2019). *Srbija u novom društveno-ekonomskom sistemu*, Institut za međunarodnu politiku i privredu, Beograd, str. 321-331.

[12] Štetić, S. (2017). Uticaj terorizma na turističku destinaciju, *Turističko poslovanje*, br. 12/2017, Visoka turistička škola, Beograd.

[13] Waever, O. (2003). *Securitisation: Taking stock of a research programme in Security Studies*, Draft, 1-36. https://docplayer.net/62037981-Securitisation-taking-stock-of-a-research-programme-in-security-studies.html, dostupno 1.4.2022.

[14] Živković, D., Petrović, P., Ercegović, M. (2020). Način funkcionisanja malih i srednjih preduzeća u hotelijerstvu i eko-turizmu, *Ecologica*, 27(97), 75-81.