Iva Tošić, master*

UTICAJ PANDEMIJE VIRUSA KOVID 19 NA OSIGURANJE OD INTERNET RIZIKA

Sažetak

Sa pojavom pandemije virusa kovid 19 veliki broj kompanija je sa ciljem zaštite zdravlja svojih zaposlenih prešao na rad od kuće. Međutim, pored prednosti koje ima za zaštitu zdravlja i života ljudi u ovakvoj situaciji, rad od kuće, tj. poslovanje putem interneta i onlajn platformi nosi veliki rizik za kompaniju. Taj rizik se odnosi pre svega na internet napade koji su sve učestaliji i koji mogu doneti ogromne troškove pogođenoj kompaniji. Pored toga, internet kriminalci su spremni da zloupotrebe zainteresovanost za ažurne informacije o virusu kovid 19 kao način da izvrše internet napad protiv korisnika interneta. Kao vid zaštite od ovih napada koristi se osiguranje od internet rizika, koje za cilj ima da smanji troškove koji bi pogodili kompaniju u slučaju da bude meta internet napada i omogući njeno dalje poslovanje, jer bi u suprotnom u velikom broju situacija propast pogođene kompanije bila gotovo izvesna.

U prvom delu rada autorka se bavi rizicima koje je nastupanje pandemije virusa kovid 19 donelo poslovanju kompanija, a u drugom delu pojmom i značajem osiguranja od internet rizika kao i analizom uticaja koji je na povećanje značaja ove vrste osiguranja imalo nastupanje pandemije.

Ključne reči: rizik, internet, osiguranje, kovid 19, imovinsko osiguranje, osiguranje od odgovornosti.

1. UVOD

Ideja postojanja interneta je da bude pouzdan i koristan i da doprinese olakšanju obavljanja određenih poslova. Upotreba interneta u privatne svrhe ubrzo se proširila na poslovanje privrednih društava.[1] Na taj način dolazi do smanjenja troškova i uštede vremena, čime se doprinosi produktivnosti, kvalitetu, ali i povećanju zarade. Upravo u svetlu pandemije virusa kovid 19, koji je iznenada i neplanirano potresao svet, a time stvorio ogromne probleme kompanijama u sprovođenju svojih svakodnevnih poslova, internet je odigrao značajnu ulogu. Usled pandemije, zaposleni, kompanije i klijenti nisu u mogućnosti da normalno obavljaju svoju delatnost, pa su zbog toga kompanije bile sprečene da obavljaju uobičajene poslovne operacije.[2] Globalna pandemija virusa

* Istraživač saradnik u Institutu za uporedno parvo, e-mail: *i.tosic@iup.rs*

[1] Za više vid.: *Internet i društvo*, Srpsko sociološko društvo, Univerzitet u Nišu – Filozofski fakultet, Institut za uporedno pravo, Beograd, 2014.

[2] A. Louaas *et al.*, "A pandemic business interruption insurance", 2020, 2, tekst dostupan na: https://hal.archives-ouvertes.fr/hal-02941948, 5. 1. 2021.

kovid 19 jedinstvena je u dosadašnjoj istoriji u pogledu obima, odnosno broja država koje su njom bile pogođene u istom vremenskom periodu, kao i u pogledu njenog uticaja na različite segmente i oblasti društvenog života.[3]

Usled postojanja i razvoja interneta, kao i različitih platformi za održavanje *online* sastanaka, rad od kuće je predstavljao najpodobniju opciju u svetlu novonastalih okolnosti za sprovođenje redovnog poslovanja kompanija širom sveta. Međutim, pored prednosti, takvo poslovanje nosi i velike rizike, pre svega rizike od internet napada i prevara. Ostvarenje nekog od tih rizika može imati razorne posledice i ogroman uticaj na poslovne subjekte, a samim tim i njihove zaposlene, korisnike i treća lica. Te radnje mogu dovesti do krađe intelektualne svojine, ugrožavanja korporativne strategije, pronevere, manipulisanja poverljivim i ličnim podacima, a u nekim slučajevima mogu ugroziti dalje postojanje samog društva. Prema rečima Roberta S. Milera (*Robert S. Mueller*) „postoje dve vrste firmi, one koje su hakovane, i one koje će biti hakovane".[4]

S obzirom na sve intenzivniju upotrebu interneta[5] i sveprisutnu opasnost od nastanka štete usled internet napada,[6] kao vid zaštite javlja se osiguranje od internet rizika koje pomaže smanjenju finansijskog opterećenja društva, jer bi osiguravajuća kompanija nadoknadila gubitak. U vremenu kada internet predstavlja neizostavan deo kako privatnog (individualnog) tako i poslovnog života, pogotovo u situaciji u kojoj se ceo svet sada nalazi, ova vrsta osiguranja postaje jedna od najznačajnijih vrsta osiguranja radi obezbeđenja materijalne sigurnosti pojedinaca (fizičkih lica), pravnih lica, kako većih tako i manjih,[7] ali i samih država.

Međutim, upravo usled nastupanja pandemije, potreba za ovom vrstom osiguranja kao rezultata sve učestalijh internet napada postaje sve veća, a, s druge strane, spremnost osiguravajućih društava da zaključe ugovor o osiguranju od internet rizika postaje sve manja.

2. RIZICI OD INTERNET NAPADA USLED NASTUPANJA PANDEMIJE

Pandemija virusa kovid 19 povećala je rizike od nastanka internet napada i prevara, pre svega iz razloga što je veliki broj kompanija prešao na rad od kuće,[8] kao

[3] A. Čović, „Pravo na privatnost i zaštita ličnih podataka u doba pandemije COVID-19", *Sociološki pregled*, br. 3/2020, 671.

[4] "There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.", tekst dostupan na: https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies, 08.06.2021.

[5] Prema procenama 2020. godine je hiljadu milijardi - trilion uređaja bilo umreženo, Allianz Global Corporate & Specialty, "A guide to Cyber risk- Managing the Impact of Increasing Interconnectivity", 2015, 5.

[6] S. Jovanović, „Osiguranje od informatičkih rizika", *Teme*, 2017, 829.

[7] Veličina određenog privrednog društva najčešće nije merilo kojim se vode lica koja izvršavaju internet napade, mnogo su značajnije informacije koje određeno društvo poseduje.

[8] Za više o radu od kuće vid.: T. Kaur, P. Sharma, "A Study on Working Women and Work from Home Amid Coronavirus Pandemic", *Journal of Xi'an University of Architecture & Technology*, 2020, 1400-1408; M. Dockery, S. Bawa, "Working from Homein the COVID-19 Lockdown", *Bankwest Curtin Economics Centre Research Brief COVID-19,* 2020; S. Bradaš, M. Reljanović, I. Sekulović, *Uticaj epidemije Covid-19 na položaj i prava radnica i radnika u Srbiji uz poseban osvrt na radnike i radnice na prvoj liniji i u neformalnoj ekonomiji i višestruko pogođene kategorije*, Fondacija Centar za demokratiju, Beograd, 2020.

i usled zloupotrebe aktuelnosti vesti vezanih za pandemiju. „Virus korona" je sada među najtraženijim rečima na internetu, a razlog je očigledan. Samim tim, želja za pristupom ažuriranim informacijama povezanim sa širenjem virusa dovodi do povećanja šansi za širenje zlonamernih kodova pod maskom autentične informacije o virusu korona. Zlonamerni kodovi koji uspešno pronađu put u slabo zaštićenom računarskom sistemu mogu dovesti do velikog broja štetnih ishoda, uključujući krađu poverljivih informacija, izlaganje osetljivih i privatnih finansijskih podataka, špijuniranja korisnikovih mrežnih transakcija ili instaliranja niza drugih zlonamernih kodova koji se mogu aktivirati naknadno. Kompanije koje poseduju veliki broj ličnih podataka vezanih za svoje zaposlene, klijente i treća lica mogu se naći u nezavidnoj situaciji ukoliko neka od tih informacija „procuri" na ovaj način.

2.1. *Internet prevare povezane sa virusom kovid 19*

Usled pomenute promene načina poslovanja veliki broj kompanija postao je meta internet napada,[9] pre svega takozvanih *phishing* prevara. Sprovodeći ovu vrstu prevara, internet kriminalci praktično koriste vest koja je izuzetno aktuelna u određenom trenutku kako bi „navukli" korisnike interneta da otvore link putem kojeg preuzimaju njihove lične podatke. Kada je u pitanju jedna kompanija, curenje podataka vezanih za njeno poslovanje ili klijente moglo bi naneti ogromnu štetu sa kojom vrlo verovatno ne bi bila u mogućnosti da se nosi, usled čega bi bila primorana da prekine svoje poslovanje. Iz tih razloga je pre svega neophodno da zaposleni koji rade od kuće imaju svest i znanje o *phishing* prevarama, najbrže rastućoj vrsti internet kriminala, od kojih se mnoge u ovom trenutku sprovode upravo zloupotrebom straha od virusa kovid 19.[10] Nažalost, internet kriminalci su iskoristili pandemiju za prevaru ljudi širom sveta,[11] a pored toga može se očekivati da još uvek planiraju brojne načine prevare zloupotrebom novonastale situacije. Naime, internet kriminalci koriste strah i neizvesnost stvorene ovom situacijom, nastojeći da iskoriste želju javnosti da nađe neki način zaštite i sigurnosti. Oni koriste aktuelnost vesti u vezi s pandemijom kako bi namamili potencijalne žrtve da preuzmu zaražene datoteke putem sumnjivih linkova. Na ovaj način oni zloupotrebljavaju obimne pretrage i radoznalost povezanu s virusom. Napravili su zlonamerne programe koji su sakriveni iza datoteka povezanih sa virusom korona.[12]

[9] Za više vid.: T. Weil, S. Murugesan, "IT Risk and Resilience - Cybersecurity Response to COVID-19", *ComputingEdge*, 2020, 12-18.

[10] Hakeri su se prilagodili novonastaloj situaciji u vezi s radom na daljinu često se predstavljajući kao pouzdane tehnološke platforme. Korisnici *Skype*-a, *Zoom*-a i *Google Meet*-a sada su meta manipulativnog internet kriminala. Nedavno istraživanje *Check Point*-a otkrilo je da je za samo tri nedelje registrovano više od 1700 domena povezanih sa *Zoom*-om, a 4% njih je sumnjivih ili moguće zlonamernih. Hakeri koriste ove lažne domene za slanje obaveštenja o sastancima preko ove aplikacije i stvaranje lažnih upozorenja na temu COVID-19 putem e-pošte. Pojedinci koji odgovore na ova upozorenja obično preuzmu malver ili na drugi način ugrožavaju sigurnost podataka.

[11] Prema podacima Nacionalnog centra za internet bezbednost Ujedinjenog Kraljevstva, početkom maja 2020. godine je prijavljeno više od 160.000 „sumnjivih" e-adresa i do kraja maja izgubljeno je 4,6 miliona funti usled internet prevara, sa oko 11.206 žrtava krađe identiteta. Nacionalni centar za sajber bezbednost (NCSC) srušio je 471 lažnu internet prodavnicu i 292 lažne internet stranice. Ovi podaci su zaista zabrinjavajući. H. S. Lallie *et al.*, "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic", 2020, 6, tekst dostupan na: https://arxiv.org/abs/2006.11929, 8. 12. 2020.

[12] S. Murugesan, N. Chidambaram, "Recent trends on online scams and frauds: COVID-19 Pandemic", *Journal of Seybold Report*, 2020, 43–44.

Uzimajući u obzir da rad od kuće postaje nova „normalnost“, internet kriminalci pokušavaju da iskoriste široko rasprostranjenu paniku i nažalost u tome uspevaju. Internet kriminal je najveća pretnja svakoj kompaniji i jedan od najvećih problema s kojima se suočava čovečanstvo. Uticaj na društvo može se videti u zvaničnom izveštaju o internet kriminalu koji svake godine objavljuje *Cibersecurity Ventures.*[13] Najefikasniji *phishing* napadi oslanjaju se na emocije, zabrinutost i želju da se putem interneta što pre dobiju nove informacije o virusu korona zbog čega je tim porukama teško odoleti. Prema navodima iz ovog izveštaja, internet kriminal koštaće svet 6 milijardi dolara godišnje od 2021. godine, u poređenju sa 3 milijarde dolara u 2015. Ovo predstavlja najveći transfer ekonomskog bogatstva u istoriji.[14]

Google-ova Grupa za analizu pretnji izvestila je sredinom aprila da su svakodnevno vršili blokadu 18 miliona prevarnih mejlova sa temom COVID-19. Zabeležen je porast od 50% broja zaposlenih koji su prijavili da su bili meta prevara i *phishing* napada otkako su naređenja da se rad sprovodi od kuće prvi put stupila na snagu. Nažalost, ove prevare su brojne.[15]

Podaci ukazuju da je u svetu od januara do marta 2020. godine zabeleženo 300.000 jedinstvenih internet pretnji koje zloupotrebljavaju pandemiju i manipulišu potrebom ljudi da budu informisani. Najveći broj tih prevara odvija se putem zlonamernih poruka, zatim zlonamernih datoteka i URL adresa. Još jedan vid zloupotrebe pandemije svakako predstavlja i masovno registrovanje lažnih internet stranica. Za vreme trajanja pandemije, značajno je povećan broj lažnih internet stranica koje koriste temu virusa kovid 19, odnosno sadrže neki od pojmova pandemije u nazivu domena („Covid19/Coronavirus“). Pored distribucije internet napada, ove stranice se koriste za lažnu prodaju medicinske opreme, suplemenata, lekova, vakcina, na koji način prevarom korisnika „hakeri“ dolaze do protivpravno stečene imovinske koristi.[16]

Dodatni problem je da nijedna tehnologija ne može u potpunosti zaštititi pojedinca od trikova koji stoje iza *phishing* napada. Jedini siguran način za borbu protiv krađe identiteta i podataka, kao i ostalih vrsta prevara je edukacija zaposlenih i poboljšanje lične internet bezbednosti same kompanije. Osiguranje nastupa u onom trenutku kada je do prevare i štetnih posledica po kompaniju već došlo. Da bi zaštitili svoju privatnost, pojedinci na svim nivoima upravljanja moraju biti izuzetno oprezni pre otvaranja e-poruka ili upozorenja za koja se čini da dolaze od zdravstvenih stručnjaka, vladinih agencija ili kompanija. Takođe, zaposleni bi trebalo da budu podjednako oprezni kada odgovaraju na pozive za sastanke putem onlajn platformi.[17] Neophodno

[13] https://cybersecurityventures.com/annual-cybercrime-report-2020/, 17. 1. 2020.

[14] T. Ahmad, “Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity”, tekst dostupan na: https://ssrn.com/abstract=3568830, 1; zanimljivo je da se procenjuje da će ova vrsta internet kriminala biti profitabilnija od trgovine svim glavnim ilegalnim drogama zajedno, https://cybersecurityventures.com/annual-cybercrime-report-2020/ , 17. 1. 2021.

[15] Ugovarači prodaje koji rade za nemačke vlasti saglasili su se da će holandskom dobavljaču platiti 1,5 miliona evra za početnu isporuku milion maski, saopštio je Evropol, evropska policijska agencija za koordinaciju. Kada su dobavljačima rekli da njihova avansna uplata nije primljena, složili su se da pošalju dodatnih 880.000 evra kako bi osigurali isporuku maski. Holandski dobavljač u slučaju Evropol bio je legitiman, ali su prevaranti klonirali njegovu veb stranicu i svi dokazi o dve uplate su nestali, rekla je agencija, vid. detaljnije: Million-Mask Fraud Foiled in Coronavirus Variant of Email Scam (bloombergquint.com), 25. 12. 2021.

[16] SRb-CERT, „Zloupotreba pandemije virusa covid-19 u sajber prostoru“, 2020, 2-3.

[17] How hackers are using COVID-19 to find new phishing victims | 2020-06-23 | *Security Magazine*, 22. 12. 2020.

je da se zaposleni koji rade od kuće što pre edukuju o svojoj internet privatnosti i sigurnosti, pre svega imajući u vidu da globalna šteta od internet kriminala može biti čak duplo veća krajem ove godine.

2.2. *Internet bezbednost*

Internet bezbednost se fokusira na sprečavanje neovlašćenih promena podataka i zaštitu korisnika od internet prevara koje ugrožavaju poverljivost, integritet i dostupnost digitalnih informacija na internetu i u čitavom sajber prostoru.[18] Internet bezbednost je proces osiguranja imovine, programa i podataka od neovlašćenog pristupa ili napada. Sve veći broj internet napada čini internet bezbednost jednim od izazovnijih istraživačkih područja.[19] Činjenica je da je internet kriminal jedna od grana koja se najbrže razvija i da i pored edukacije i svih bezbednosnih protokola kompanije često neće biti u mogućnosti da izbegnu internet napade i prevare. Upravo u ovim situacijama, kao vid zaštite od posledica prouzrokovanih internet napadom, javlja se osiguranje od internet rizika.

Ovaj problem postoji odavno. Činjenica je da je kultura osiguranja od internet rizika na jako niskom nivou, ali sa nastupanjem pandemije virusa kovid 19, kompanije su u još većoj meri izložene ovim rizicima, pre svega zbog toga što su veliki deo svog poslovanja prenele na onlajn poslovanje, potom i zbog želje da dobijaju aktuelne informacije o pandemiji. Sve navedeno stvara povoljne uslove za internet napade putem linkova i veb stranica koje navodno sadrže informacije o virusu.

3. OSIGURANJE OD INTERNET RIZIKA

Svakodnevna sve veća upotreba interneta, a samim tim i veći broj internet prevara zahtevaju da se omogući neki način zaštite za korisnike interneta. Jedan od tih načina je svakako osiguranje od internet rizika, kojim se plaćanjem premije osiguranja rizik prenosi na osiguravača.[20] Naravno, treba imati u vidu da ova vrsta osiguranja ne štiti od samog internet napada, ali predstavlja vrlo značajnu zaštitu od posledica koje jedan takav napad može izazvati pogođenoj kompaniji. Pandemija virusa kovid 19, koja je potresla ceo svet, samo je potvrdila potrebu za ovom vrstom osiguranja, koja je sada potrebnija nego ikada pre. Zapravo, uzimajući u obzir činjenicu da se internet svakodnevno razvija i postaje sve veći deo svakodnevnice, ova vrsta osiguranja će svakako postati budućnost tržišta osiguranja. Pored toga, ovo je vreme kada kompanije treba da podsete zaposlene na opasnosti otvaranja priloga i linkova koji dolaze od nepouzdanih izvora.[21]

[18] K. Okereafor, O. Adebola, "Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety", *International Journal in IT & Engineering*, 2020, 3.

[19] S. Hakak *et al*., "Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies"*, IAEE Access, Special section on internet-of-things attacks and defenses: recent advances and challenges*, 2020, 2.

[20] Za više vid.: L. Asaf, "The insurability of cyber risk", tekst dostupan na SSRN 3452833 (2019).

[21] AON Empowe results, Cyber Risk Implications of the Coronavirus Outbreak.

3.1. *Problemi koji se javljaju kod osiguranja od internet rizika*

Osiguranje od internet rizika, ukoliko ga kompanija poseduje, može predstavljati ključ opstanka poslovanja kompanije nakon internet napada. Međutim, ono sa sobom nosi i određene probleme, štete koje u tim slučajevima mogu nastati često su nemerljive, tj. ne može se unapred utvrditi kolika je šteta koje će neko lice ili privredno društvo pretrpeti u slučaju internet napada. Procena internet rizika, tj. kolika će biti potencijalna šteta, je vrlo složena. Da obaveze ne bi izmakle kontroli, u ugovore o osiguranju bi mogle da se unesu odredbe kojima se ograničava pokriće po štetnom događaju i u godini osiguranja, predviđa učešće osiguranika u svakoj šteti, ali i bonus za dobar tehnički rezultat.[22] Osiguranje od internet rizika spada u imovinska osiguranja u kojima je vladajući princip obeštećenje osiguranika.[23] Naknada iz osiguranja treba da odgovara visini stvarno pretrpljene štete.

Ukoliko je prilikom zaključenja ugovora o osiguranju teško utvrditi vrednost predmeta osiguranja, suma osiguranja se može utvrditi na više načina.[24] Princip obeštećenja se primenjuje na taj način što se trećem oštećenom licu ne može priznati naknada koja je veća od štete koju je pretrpeo. Da bi se izbeglo da se prilikom zaključenja ugovora utvrđuje stvarna vrednost osiguranog interesa, osiguranje internet rizika se po pravilu zaključuje na vrednost koju odredi osiguranik koji najbolje zna koji iznos sume osiguranja može da zadovolji njegove potrebe za osiguravajućom zaštitom. Ako se prilikom nastanka osiguranog slučaja može nesumnjivo utvrditi da je ugovorena suma manja od stvarne štete, naknada može biti do ugovorene sume. U ovakvim osiguranjima primenu pravila proporcionalnosti treba isključiti jer ono ima puni smisao onda kada se u momentu zaključenja ugovora može utvrditi tačna vrednost osiguranog interesa.[25]

Osiguranje treba da se prilagodi svakom osiguraniku jer su kod različitih delatnosti i internet rizici različiti, stoga nije isto pokriće koje nude pojedini osiguravači.[26] Iako su danas neka pokrića internet rizika standardizovana, zbog njihove osobenosti nije moguće koristiti iste uslove za veliki broj osiguranika (model uslove), kao što je to slučaj kod osiguranja drugih imovinskih rizika.

Polisa osiguranja od internet rizika pre svega pokriva troškove angažovanja IT stručnjaka, ali treba imati u vidu da je ovo najblaža finansijska posledica internet napada i samo mali deo pokrića internet osiguranja, te kao takav obično nije prvi motiv kupovine polise internet osiguranja. Ono što predstavlja najveću odgovornost svake kompanije, i što joj može doneti i najveće troškove u slučaju internet napada, jeste obaveza čuvanja ličnih podataka[27] zaposlenih i svojih klijenata kao što su matični broj,

[22] *Ibid*., 73.

[23] „Iznos naknade ne može biti veći od štete koju je osiguranik pretrpeo nastupanjem osiguranog slučaja.“, čl. 925, st. 2 Zakona o obligacionim odnosima, *Sl. list SFRJ,* br. 29/78, 39/85, 45/89 - odluka USJ i 57/89*, Sl. list SRJ,* br. 31/93*, Sl. list SCG,* br. 1/2003 – Ustavna povelja *i Sl. glasnik RS,* br. 18/2020.

[24] Npr. ako je reč o umetničkim ili drugim vrednostima, osiguravač i osiguranik sporazumno utvrđuju tu vrednost. U trenutku kada nastupi osigurani slučaj, osiguravač može da ističe prigovor da je ugovorena vrednost iznad stvarne vrednosti i da prizna naknadu koja je manja od ugovorene sume. Postoje i slučajevi kada se osiguranje može zaključiti i na deklarisanu vrednost, vrednost koju je odredio sam osiguranik. Poznato je da se u osiguranju od građanske odgovornosti limit pokrića utvrđuje po izboru osiguranika jer se ne može unapred znati koliku štetu on može da prouzrokuje drugome.

[25] J. Pak, „Osiguranje internet rizika“, *Sinteza*, 2014, 74.

[26] *Ibid*., 72.

[27] Za više o pojmu i istorijatu podataka o ličnosti vid.: S. Andonović, *Zaštita podataka o ličnosti u elektronskoj javnoj upravi u Republici Srbiji – pravni aspekti,* doktorska disertacija na Pravnom fakultetu Univerziteta u Beogradu, 2019, 87–146.

adresa, brojevi kreditnih kartica, tekućih računa, podaci o zdravstvenim ispravama, podaci o vozačkoj dozvoli i svi ostali podaci koji se vezuju za identitet određene osobe ili njeno finansijsko i zdravstveno stanje (podaci o mejl adresama, brojevima telefona, poštanskim adresama itd.), sprečavanja neovlašćenog pristupa i korišćenja kompanijskih resursa i sprečavanja nastanka bezbednosnih propusta. U ovakvim slučajevima ta lica imaju pravo da pozovu društvo na odgovornost kada bi ono pored naknade pretrpljene štete bilo u obavezi da plati prateće sudske, administrativne i druge troškove. Za većinu malih ili srednjih biznisa, čak i najmanji trošak internet incidenta može trajno da zatvori kompaniju. Upravo u ovoj situaciji se ogleda najveći značaj osiguranja od internet rizika, čija bi polisa pokrila sve finansijske posledice u nekom od navedenih slučajeva. Ukoliko ipak, i pored preduzetih mera, dođe do povrede privatnosti, društvo će najčešće biti izloženo i plaćanju novčanih kazni izrečenih na osnovu prekršajnih naloga ovlašćenog državnog organa, troškova upravljanja kriznom situacijom, obaveštavanja korisnika i podrške klijentima, koji su takođe pokriveni polisom internet osiguranja.[28]

Još jedan od problema koji se javlja kod osiguranja od internet rizika, a koji pogađa sve vrste osiguranja jeste problem moralnog hazarda. Kao i kod drugih vrsta osiguranja, kao najbolje rešenje javlja se predviđanje manje premije za one kompanije koje imaju razvijene bezbednosne protokole i koje ulažu u edukaciju zaposlenih, tj. određivanje premije na osnovu rizika. Dalje kao rešenje može se javiti i koosiguranje i ograničavanje pokrića po štetnom događaju.[29]

3.2. *Povećanje rizika usled nastupanja pandemije*

Uzimajući u obzir povećani broj internet napada usled nastupanja pandemije, može se zaključiti da će pandemija u još jednom aspektu imati uticaj na osiguranje od internet rizika u onim zemljama u kojima je ova vrsta osiguranja razvijena. Naime, radi se o tome da je usled nastupanja pandemije došlo do povećanja osiguranog rizika. Ako je povećanje rizika toliko da osiguravač ne bi zaključio ugovor da je takvo stanje postojalo u času njegovog zaključenja, on može raskinuti ugovor. Ali ako je povećanje rizika toliko da bi osiguravač zaključio ugovor samo uz veću premiju da je takvo stanje postojalo u času zaključenja ugovora, on može ugovaraču osiguranja predložiti novu stopu premije. Takođe, može se očekivati da će osiguravajuća društva zahtevati da im kompanije dostave dokaze da su preuzele sve mere za ostvarenje internet sigurnosti prilikom sprovođenja rada od kuće ili čak da odbiju da pokriju štetu koju bi internet napad prouzrokovao ukoliko nisu preduzete sve mere za ostvarivanje internet bezbednosti. Nažalost, u ovakvoj situaciji ne bi bilo iznenađujuće da, pored ionako slabo razvijenog tržišta osiguranja od internet napada, pojedina osiguravajuća društva koja su do sada obavljala ovu vrstu osiguranja odbiju da zaključe ugovor.[30]

[28] I. Tošić, „Osiguranje od internet rizika“, *Odgovornost za štetu, naknada štete i osiguranje*, Beograd–Valjevo, 2020, 444.
[29] Za više vid.: L. Bailey, “Mitigating Moral Hayard in Cyber-Risk Insurance”, *Journal of Law & Cyber Warfare,* 2014, 1–42.
[30] Za više vid.: https://www.getcyberresilient.com/threat-insights/the-impact-of-covid-19-on-cybersecurity-insurance, 22. 1. 2020, https://www.wsj.com/articles/cyber-insurers-get-tough-on-risk-assessments-amid-coronavirus-pandemic-11589794201, 22. 1. 2021.

U svakom slučaju, osiguranje od internet rizika bi trebalo da bude deo poslovne strategije i poslovne kulture svake ozbiljne kompanije jer, ukoliko kompanija nema odgovarajuću zaštitu od sve učestalijih i sve izvesnijih incidenata, poput curenja podataka ili internet iznuda, može se zaključiti da ne shvata ozbiljno svoje poslovanje. Zaštita podataka od strane zaposlenih u kompaniji i osiguranje od internet rizika idu „ruku pod ruku" i oba predstavljaju neizostavni deo poslovne politike svake ozbiljne kompanije. Stoga je neophodno omogućiti da se kontrola čuvanja podataka korisnika strože sprovodi unutar samih kompanija. Ipak, bez odgovarajuće strategije upravljanja internet rizicima, kompanije neće biti u stanju da se izbore sa internet rizicima, barem ne na duže staze.

S druge strane, treba imati u vidu da je tržište osiguranja od internet rizika jako slabo razvijeno, usled čega zaključenje ovog ugovora karakterišu visoke premije osiguranja i često nespremnost osiguravača da uopšte zaključi ugovor.[31] Sa razvojem tržišta osiguranja u ovoj oblasti, osiguravači bi bili u mogućnosti da ponude ovu vrstu osiguranja sa nižom premijom nego što ona iznosi u ovom trenutku, a neminovno je da je ovo vrsta osiguranja koja će svakodnevno biti sve potrebnija.[32]

3.3. *Osiguranje od internet rizika u Republici Srbiji i nastupanje pandemije virusa kovid 19*

Osiguranje od internet rizika u Republici Srbiji gotovo da uopšte nije razvijeno. Takva vrsta osiguranja je tek u razvitku i među prvima su je ponudili u kompaniji *Wiener Stadtische* osiguranje. Međutim, primeri internet napada su i u Srbiji mnogobrojni. Sa nastupanjem pandemije virusa kovid 19, i u Srbiji se pokazalo da je potreba za ovom vrstom osiguranja ogromna.

Pored razvoja osiguranja od internet rizika, u Srbiji je neophodna i edukacija zaposlenih o internet napadima, kako bi kompanije bile u mogućnosti da bar u određenoj meri spreče te napade. Čini se da je znanje o ovoj temi na jako niskom nivou. Kada se uzme u obzir činjenica da većina kompanija barem deo svog poslovanja obavlja preko interneta, a u svetlu novonastalih okolnosti sada i većina njih, kao i da obično raspolažu velikim brojem ličnih podataka što svojih zaposlenih, što klijenata, ako bi došlo do internet napada u kojem bi bili zloupotrebljeni ti podaci, vrlo je verovatno da ne bi mogle da nastave svoje poslovanje. Iz tih razloga u Srbiji je prvenstveno potrebna edukacija zaposlenih, unapređenje sigurnosnih protokola, a zatim i da se razvije tržište osiguranja od internet rizika.

[31] Kao što je prethodno pomenuto, nastupanje pandemije je dodatno doprinelo nespremnosti osiguravača da zaključe ugovor u ovoj vrsti osiguranja, a ono je sada potrebnije nego ikad.

[32] Koliki je značaj ove vrste osiguranja potvrđuje i činjenice da su u 2020. godini internet rizici prvi put ocenjeni kao najvažniji svetski poslovni rizici prema *Allianz*-ovom barometru rizika za 2020. godinu (39% odgovora), navodeći da su internet rizici i klimatske promene dva značajna izazova koja društva treba da pomno prate u sledećoj deceniji. U 2021. godini, očekivano, pandemija se popela na prvo mesto, ali internet rizici drže treće mesto na listi poslovnih rizika, https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, 24. 1. 2021.

4. ZAKLJUČAK

Jedan od najvećih rizika za privredna društva, usled svakodnevne sve veće upotrebe kompjutera i interneta, predstavlja internet napad koji u određenim slučajevima može dovesti i do propasti kompanije usled ogromnih troškova, gubitka reputacije i klijenata. Kao vid prevencije štete koju kompanija može pretrpeti usled internet prevara javlja se ideja o osiguranju od ove vrste rizika. Nastupanje pandemije virusa kovid 19 uticalo je na to da je osiguranje od internet rizika iz ugla osiguranika potrebnije nego ikada, ali iz ugla osiguravača došlo je do povećanja rizika usled čega postoji potreba za povećanjem premije, a u nekim slučajevima čak i za raskidom ugovora. Pored toga, pitanje je u kojoj meri će osiguravači biti spremni da zaključe ugovor o osiguranju od internet rizika u svetlu novonastale situacije.

Neophodno je najpre da se kompanije koje se bave prikupljanjem i obradom podataka o ličnosti posvete rešavanju problema internet bezbednosti. U suprotnom, čak i incident najmanjeg obima može naneti veliku štetu ne samo kompaniji već i njenim klijentima. Treba imati u vidu da osiguranje samo po sebi ne može biti zamena za konstantnu edukaciju zaposlenih unutar kompanije o mogućnostima i načinima koji dovode do internet napada, kao i načinima da se ti napadi spreče ili bar umanje. Potrebno je naglasiti da osiguranje od internet rizika kao pojedinačno rešenje deluje adekvatno tek kada nastupi štetni događaj, pa samim tim najbolji rezultat donosi kada je deo opšte strategije upravljanja rizicima. Pošto se radi o okruženju koje je u neprestanom razvoju, potrebno je biti u toku sa aktuelnim strategijama i dobrim praksama koje obezbeđuju podatke korisnika i smanjuju mogućnost da dođe do zloupotrebe.

Iva Tošić, MA
Research Assistant at the Institute of Comparative Law, Belgrade
e-mail: i.tosic@iup.rs

THE IMPACT OF THE COVID-19 PANDEMIC ON THE IMPORTANCE OF INTERNET RISK INSURANCE

Summary

With the outbreak of the Covid-19 pandemic, most of the companies have moved to work from home in order to protect the health of their employees. However, in addition to the advantages it has for protecting the health and lives of people in this situation, working from home carries a great risk for the company. This risk refers primarily to internet frauds. These frauds are becoming more frequent and they can bring huge costs to the affected company. In addition, cyber criminals are willing to abuse interest in up-to-date information about the virus as a way to carry out an internet attack against internet users. Internet risk insurance is used as a type of protection against these attacks. It aims to reduce the costs that would hit the company in case it is the target of an internet attack and enable its further business, because otherwise the collapse of the affected company would be almost certain.

In the first part of the paper, the author analyzes the risks that companies are obligated to deal with because of the onset of a pandemic, while the second part deals with the concept and importance of internet risks insurance as well as the analysis of the impact of the pandemic on the importance of this type of insurance.

Keywords: risk, internet, insurance, Covid-19, property insurance, liability insurance.