Iva Tošić, master[1]

OSIGURANJE OD INTERNET RIZIKA

Apstrakt

Razvoj i sve veća upotrebakompjutera iinterneta pored ogromnih prednosti kao što je ušteda vremena i sredstava, sa sobom nose i određene rizike. Ti rizici se odnose pre svega na internet napade koji su sve učestalijii koji mogu doneti ogromne troškove pogođenoj kompaniji. Upravo iz tih razloga u visokorazvijenim zemljama javilo se osiguranje od internet rizika, koje za cilj ima da smanji troškove koji bi pogodili kompaniju u slučaju da bude meta internet napada i omogućili njeno dalje poslovanje, jer bi u suprotnom propast pogođene kompanije bila gotovo izvesna. U prvom delu rada autor se bavi pre svega značajem tj prednostima interneta alii njegovima manama, kao i pojmom internet rizika. Dalje u drugom delu rada, obradiće se pojam osiguranja od internet rizika, kao vid imovinskog osiguranja i kao vid osiguranja od odgovornosti, uz kratak osvrt na osiguranje od internet rizika u Republici Srbiji.

Ključne reči: *rizik, internet, osiguranje, napad, imovinsko osiguranje, osiguranje od odgovornosti.*

1. Uvod

Razvoj digitalne tehnologije krajem 20. i početkom 21. veka doprineo je ubrzanjuprotoka informacija prevashodno zahvaljujući globalnoj računarskoj mreži – internetu.Najrazličitiji sadržaji postali su putem interneta globalno dostupni. Internet utiče na gotovo sve segmente privrede i društva[2], što je omogućilo lakšu i bržurazmenu ideja, obrazovanje i zadovoljenje širokog dijapazona potreba savremenog čoveka.[3]Internet utiče na gotovo sve segmente privrede i društva. Razvoj i primena računara, računarskih mreža iinterneta, u svim društvenim segmentima, nesporno doprinosi unapređenju kvaliteta poslovanja.Ideja postojanja

[1] Istraživač saradnik, Institut za uporedno pravo Beograd; mail: *i.tosic@iup.rs*

[2] J. Ćeranić (2016), „Povreda žiga na sajtovima za aukcijsku prodaju robe“, *Intelektualna svojina i Interent* (ur. D. Popović), 48.

[3] J. Ćeranić Perišić (2020), *Odgovornost internet posrednika za povredu žiga,* Beograd, 9.

interneta je da bude pouzdan i koristan i da doprinese olakšanju obavljanja određenih radnji. Upotreba interneta u privatne svrhe ubrzo se proširila na poslovanje privrednih društava.[4] Na taj način dolazi do smanjenje troškova i uštede vremena, čime se doprinosi produktivnosti, kvalitetu aliipovećanju zarade. U savremenom vremenu je praktično nemoguće zamisliti funkcionisanje društva bez interneta, a pre svega Imajući u vidu,količinu informacija koje se prenose putem Interneta i brzinu njihovog protoka.[5] Međutim, bez obzira na brojne prednosti koje nam njegovo korišćenje donosi, kao i nespornuuštedu vremena i novca, on sa sobom nosii određene rizike, kako za pojedince tako i za privredna društva. Ostvarenje nekog od tih rizika može imati razorne posledice i ogroman uticaj na poslovne subjekte, a samim tim i njihove zaposlene, korisnikei treća lica. Te radnje mogu dovesti do krađe intelektualne svojine[6], ugrožavanja korporativne strategije, pronevere, manipulisanja sa poverljivim i ličnim podacima, a u nekim slučajevima mogu ugroziti dalje postojanje samog društva. Nesporno je da internet rizici predstavljaju svakodnevnu pretnju kontinuiranom poslovanju i pružanju usluga kako u javnom, tako i u privatnom sektoru, a njihovo nastupanje može dovesti do katastrofalnih posledica. Prema rečima Roberta S. Muellera "postoje dve vrste firmi, one koje su hakovane, i one koje će biti hakovane".[7]

S obzirom na sve intenzivniju upotrebu interneta (prema procenama 2020. godine će hiljadu milijardi- trilion uređaja biti umreženo)[8]i sveprisutnu opasnost od nastanka štete usled internet napada potreba za osiguranjem od štetnih posledica raste.[9]Iz svih navedenih razloga u razvijenim zemljama se kao odgovor na pomenute problem javlja osiguranje od internet rizika. Upotreba osiguranja služi kao dopunsko sredstvo za smanjenje mogućih finansijski gubitaka sa kojim bi se određeno privredno društvo susrelo zbog internet rizika. Ovo bi pomoglo smanjenju finansijskog opterećenjadruštva, jer bi osiguravajuća kompanija nadoknadila gubitak. Zapravo,rizik organizacije prelazi

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

[5] J. Ćeranić (2017), „Pravni okvir odgovornosti za povredu žiga na internetu u Evropskoj uniji i Republici Srbiji", *Privredna krivična dela* (ur. I. Stevanović, V. *Čolović*), Beograd, 189.

[6] Npr. neretko je da se na interentu protivzakonito koristi tuđa žigom zaštićena oznaka, za više videti: J. Ćeranić (2016), „Odgovornost internet posrednika za povredu žiga u pravu Evropske unije", *Pravo i privreda*, 7-9, 413-428.

[7] „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.", https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies, 08.06.2020.

[8] Allianz Global Corporate & Specialty,, „A guide to Cyber risk- Managing the Impact of Increasing Interconnectivity", 2015, 5.

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

na drugu stranuusled plaćanja premije. Na ovaj način se smanjuje zabrinutost kompanije o „samoosiguravanju" i sprečava se da ogromninovčaniiznosiu slučaju nastupanja rizika odlazeu nepredviđene svrhe.[10] U vremenu kada internet predstavlja neizostavan deo kako privatnog (individualnog), takoi poslovnog života, nesporno je da će ova vrsta osiguranja postati jedna od najznačajnijih vrsta osiguranja radi obezbeđenje materijalne sigurnosti pojedinaca (fizičkih lica), pravnih lica, kako većih, tako i manjih[11], alii samih država.

Mediji nas skoro svakodnevno obaveštavaju o primerima organizacija koje su pretrpele ogromne finansijske gubitke i narušavanje reputacije kao rezultat problema koji proizilaze iz njihovih sistema informacione tehnologije,bez obzira da li je to rezultat ljudske greške, namernog pogrešnog postupanja ili neki drugi oblik kvara tehnoloških sistema. Vlade i regulatori postaju sve više zainteresovanii pozivaju kompanije da preduzmu mere za zaštitu kako sopstvene imovine, takoi nacionalne infrastrukture.

Udruženje Britanskih osiguravača smatra da osiguranje od internet rizika do 2025. godine treba da postane uobičajno, a navodeći sledeće razloge:

1. Internet kriminal je jedan od oblika kriminala koji najbrže raste na svetu. Deluje preko međunarodnih granica i privlači organizovane kriminalne grupe.
2. Internet pretnje su visokotehnološke prirode. Priroda pretnji se menja tako brzo da je skoro nemoguće dakompanije to isprate.
3. Kompanije su sve više zavisne od internetau svakodnevnom poslovanju. Nisu samo informacije pohranjene na mreži, kompanije sve više koriste telefonske i platne sisteme putem računarskih tehnologija.
4. Internet napadii neuspesi mogu dovesti do zatvaranja kompanijeili potrebe da bitnopromeni način obavljanja delatnosti. Poslednje istraživanje Vlade Velike Britanije utvrdilo je da je 10% pogođenih organizacija moralo promeniti prirodu svog poslovanja.[12]

[10] A. Mukhopadhyay *et al*., „Insurance for Cyber-risk- A Utility Model", https://www.researchgate.net/publication/236576735_Insurance_for_Cyber-risk_A_Utility_Model, 15.04.2020.

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

[12] Association of British Insurers, „Cyber insurance to become a business essential within the next decade", 2015, https://www.politicshome.com/members/article/cyber-insurance-to-become-a-business-essential-within-the-next-decade , 14.04.2020.

2. Pojam internet rizika

Sve intenzivnija upotreba interneta u svetu i činjenica da savremeno društvo praktično ne bi moglo da funkcioniše bez upotrebe interneta nesporno su uticali na unapređenje kvaliteta rada.

Ogromna brzina, laka dostupnost, manipulativnost, i praktično neograničene mogućnosti skladištenja koje internet pruža, otvaraju neviđene mogućnosti za najrazličitije upotrebe novih tehnologija koje su omogućile čoveku da donosi veliki broj brzih, potpunih i sveobuhvatnih odluka. U tom moru informacija nezamislivo je da se bilo ko snađe bez postojanja informacionih sistema. Međutim, da bismo bili u stanju da sve to ostvarimoi pored mogućnosti koju nam pruža informatička tehnologija, potrebno je ispuniti odgovarajuće preduslove za njeno efikasno funkcionisanje. Sa jedne strane računari su doneli mnoge koristi ali su sa druge strane ugrozilineke od najvažnijih vrednosti, kao što su sigurnost, funkcionalnost i privatnost podataka.[13]U poslovanju klijenata koji upotrebljavaju internet postoji određena doza straha kada treba da proslede poverljive informacije.[14]

Kao što je već pomenuto upotreba računara iinterneta pored nebrojenih dobrih strana koje dovode do ogromne uštede vremena i novca ipak sa sobom nosi određene rizike.Definisanje internet rizika nije jednostavno, što se vidiiz velikog broja definicija koje su prilagođene određenim namenama ili aktivnostima pojedinih organizacija.

Izraz „internet rizik" se odnosi na mnoštvo različitih izvora rizika koji utiču na imovinu firme. Neke istaknute primere internet rizika je istakla Nacionalna asocijacija poverenika osiguranja i uključuju krađu identiteta, otkrivanje osetljivih informacija iprekid poslovanja. Učinjeno je mnogo pokušaja da se definiše internet rizik. Neki od njih koriste prilično uske koncepte: na primer, neki autoriinternet rizik nazivaju rizikom povezanim sa zlonamernim elektronskim događajima koji uzrokuju poremećaje poslovanja i finansijskegubitke.[15] Ostali zauzimaju širu perspektivudefinišući ga kao rizik sigurnostiinformacija[16]ili rizik koji nastaje neuspehom informacionih

[13] Mirko Kosanović, Miloš Kosanović (2017), „Internet rizici", 10th International Scientific Conference "Science and Higher Education in Function of Sustainable Development" 06 – 07 October 2017, Mećavnik – Drvengrad, Užice, Serbia, 76.

[14] Za više videti: G. Manojlović *et al.* (2013) „Osiguranje poslova na internetu", *Konferencija o bezbednosti informacija BISEC*, 44.

[15] A. Mukhopadhyay *et al.* (2013), "Cyber-Risk Decision Models: To Insure IT or Not?", *Decision Support Systems,* 1.

[16] H. Ögüt *et al.* (2011), "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection," *Risk Analysis*,497.

sistema.[17]Izraz „ciber" je skraćenica za reč *ciberspace*, koja se uglavnom shvata kao interaktivni domen sastavljen od svih digitalnih mreža koje se koriste za čuvanje, modifikaciju i komunikaciju informacije. To uključuje sve informacione sisteme koji se koriste za podršku kompanijama, infrastrukturu i usluge. Uzimajući to u obzirneki autori daju još širu definiciju internet rizika definišući ga kao „operativne rizike zainformaciona i tehnološka sredstva čije posledice utiču na poverljivost, dostupnost iliintegritet informacija iliinformacionih sistema", kategorišući ga u četiri klase:

1) radnje ljudi
2) kvarovi sistema i tehnologija,
3) neuspeli unutrašnji procesii
4) spoljni događaji.[18]

Prema definiciji radne grupe CRO forum internet rizik je najbolje razumeti kao rizik poslovanja u internet okruženju. Međutim, tako široko određenje pojma internet rizika je neadekvatno, a i neophodno je posmatrati ga u odnosu na druge vrste rizika. Internet rizik pokriva sve rizike koji nastaju iz korišćenja elektronskih podataka i njihovog prenošenja, uključujućitehnološka sredstva kao što su internet i telekomunikacione mreže. Takođe obuhvata štetu koja može biti prouzrokovana internet napadima, prevarama počinjenim zloupotrebom podataka, iz odgovornosti koja je proizašla iz skladištenja podataka i dostupnostii poverljivosti elektronskih informacija - bilo da su one vezane pojedinca, kompanije ili vlade.[19] Dalje, Institut za upravljanje rizicima iz Londona pod internet rizicima podrazumeva finansijsku štetu, gubitak, ili narušavanje reputacije organizacije zbog neke vrste kvara njenih sistema informacione tehnologije.[20]Prema stavovima domaćih autora internet rizik se definiše kao opasnost od štetne upotrebe i manipulacije digitalnim instrukcijama iinformacijama koje mogu da prouzrokuju finansijsku štetu na licima i stvarima i štetu u vezi sa ispunjavanjem zakonskih obaveza.[21]

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

[17] R. Böhme, K. Gaurav (2006), "Models and Measures for Correlation in Cyber-Insurance.", *WEIS*, 1.

[18] C. Biener, M. Eling, J. H. Wirfs (2015), „Working papers on finance", Institute of insurance economics, 3, 2-3.

[19] Cro forum (2014), „Cyber resilience - The cyber risk challenge and the role of insurance", 5.

[20] The Institute of Risk managment (2014), „Cyber risk- Executive Summary", 8.

[21] S. Jovanović, 825.

od tih načina je svakako osiguranje od internet rizika, kojim se plaćanjem premije osiguranja rizik prenosi na osiguravača.[22] Ono što je svakako veliki problem kod osiguranja internet rizika jeste to što su štete koje u tim slučajevima mogu nastati često nemerljive, tj ne može se unapred utvrditi kolika je šteta koje će neko lice iliprivredno društvo pretrpeti u slučaju neke od internet prevara ili neke vrste internet kriminala.To je svakako i jedan od razloga zbog kog je osiguranje od internet rizika još uvek nedovoljno razvijeno bez obzira na ogromnu potrebu za ovom vrstom osiguranja.

Međutim, koliki je značaj ove vrste osiguranja potvrđuje i činjenica da je su u 2020. godiniinternet rizici prvi put ocenjeni kao najvažniji svetski poslovni rizici prema Allianz-ovom barometru rizika za 2020. godinu (39% odgovora), navodeći da su internet rizicii klimatske promene dva značajna izazova koja društva treba da pomno prate u sledećoj deceniji.[23]Osiguranje od internet rizika je deo poslovne strategije i poslovne kulture svake ozbiljne organizacije. Nemati odgovarajuću zaštitu od sve učestalijih i sve izvesnijih incidenata poput curenja podataka iliinterenetiznuda govori o tome da kompanija ne shvata ozbiljno svoje poslovanje.

Tri elementasu neophodna da bi se omogućilo funkcionisanje tržišta osiguranja od internet rizika alii procena ovih rizika:

1) Klasifikacija i kodifikacija internet rizika- Ovo podrazumeva promovisanje razmatranja internet rizika u tradicionalnim linijama poslovanja.
2) Razumevanje izloženostiinternet riziku-Ovo je kritično područje za uspešno tržište osiguranja. Ključna komponenta je razvoj scenarija za izloženost internet riziku kako bi se mogao razumeti rizik izloženosti, aimajući u vidu faktore koji će uticati na verovatnoću / ozbiljnost gubitaka.
3) Snažani dobro osmišljen okvir za upravljanje rizikom - Nakon što se razvije pristup kodifikacijii akumulacijiizloženostiriziku, kompanije će biti bolje opremljene da utvrde parametre tolerancije na rizik i da odrede alokaciju kapitala.

Sve veća složenost, međusobna povezanost i međuzavisnost tehnologije čine zagarantovanu zaštitu od internet rizika nemogućom. Nijedan sistem nije nesavladivi zato postoji uvek rizik da je nešto prodre ili ugroziučinak sistema i tehnologije kompanije.

Četiri stuba identifikovana su kao okvir za povećanje postojećeg upravljanja rizicima i uspostavljanje procesainternet otpornosti:

---

[22] Za više videti: A. Lubin (2019), „The insurability of cyber risk", dostupno na SSRN 3452833., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452833, 29.04.2020.

[23] https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, 28.04.2020.

1. Priprema-razumevanje svoje kritične imovine; razviti sposobnosti za rešavanje različitih nivoa rizika; utvrditi sklonost riziku i ugraditi upravljanje rizikom u celu organizaciji.
2. Zaštitita- Osigurati utemeljenu i ponovljivu internet spremnost; sprovesti ocenjivanje pretnji: omogućiti i osnažiti upravljanje incidentima i mogućnosti reagovanja; razvitii sprovesti plan za reagovanje na incident, kontinuirano se obrazovatii obučavati.
3. Otkrivanje- Razviti mogućnosti otkrivanja i neprekidnog praćenja sposobnosti za rešavanje nepravilnostii pretnjiimovini kompanije.
4. Poboljšanje- Izgraditi sveobuhvatnu bazu podataka sigurnosnihincidenata koji podržavaju kontinuirano učenje i konačno omogućitioporavak od incidenta u najkraćem vremenskom roku.[24]

Prvi ugovori za pokriće internet rizika su zaključivani u SAD početkom osamdesetih godina XX veka i obezbeđivali su naknadu iz osiguranja za slučaj novčanih gubitaka koji su posledica povrede ličnih i poslovnih podataka, prekida rada usled hakerskog napada ili drugog uzroka, gubitka poslovnog ugleda, odgovornosti za štete trećim licima i pravne zaštite osiguranika. U ovim ugovorima rizikje bio osiguran nezavisno od toga šta je uzrok nastanka štetnog događaja, propust osiguranika, propust zaposlenih ili hakerski napad.

Iako su danas su neka pokrića internet rizika standardizovana zbog njihove osobenosti nije moguće koristitiiste uslove za veliki broj osiguranika (model uslove) kao što je to slučaj kod osiguranja drugih imovinskih rizika. Osiguranje treba da se prilagodi svakom osiguraniku jer su kod različitih delatnostiiinternet rizici različiti stoga nije isto pokriće koje nude pojedini osiguravači.[25]

Osiguranje od internet rizika predstavlja novu vrstu osiguranja koja se pojavila u visokorazvijenim državama. U osiguranju od internet rizika se javljaju mnogi problemi i iz tog razloga osiguravači često nisu spremni da zaključe ugovor. Nesporno je da osiguravač mora unapred da zna kakvom je riziku izložen u budućnosti, a procena internet rizika, tj kolika će biti potencijalna štetaje vrlo složeno. Osiguravači pre svega ne raspolažu sa dovoljno statističkih podataka na osnovu kojih bimogla da se utvrdi verovatnoća nastanka i prosečan iznos šteta, a takođe se radii o riziku čiji nastanak u najvećoj meri zavisi od ljudskog faktora.Da obaveze ne biizmakle kontroli u ugovore o osiguranju bi mogleda se unesu odredbe kojima se ograničava pokriće po štetnom događaju i u godiniosiguranja, predviđa učešće osiguranika u svakoj štetialiibonus za dobar tehnički rezultat.[26]Takođe, visinu novčane štete koju je pretrpeo osiguranik ili treće lice cesto je teško odmeriti. To je materijalna šteta koja može biti velika

[24] Cro forum, 3.

[25] J. Pak (2014), „Osiguranje internet rizika", *Sinteza*, 72.

[26] *Ibidem*, 73.

(gubitak prihoda, povlačenje odobrenog zajma, gubitak započetih poslova).

Jedan od razloga koji nesporno utiče na to da osiguranje internet rizika nije još uvek dovoljno razvijeno je visoka premija osiguranja. Kako osiguravači postaju sve više svesni te činjenice, oni priznaju popuste onim osiguranicima koji preduzimaju preventivne mere. Osiguranicima kojiimaju dobar tehnički rezultat u određenom periodu umanjuje se premija, dok oni kojiimaju loš rezultat plaćaju veću premiju. Prate se aktivnosti osiguranika na poboljšanju sistema sigurnosti u osiguranojdelatnosti, zahteva preduzimanje određenih mera, kao što je usavršavanje zaposlenih alii nadzor nad njihovim radom kako ne bi namerno ili slučajno prouzrokovali nastanak rizika. U osiguranju internet rizika neophodna je kontinuirana saradnja osiguravača i osiguranika a primena zakonskih mera sigurnosti kao i mera koje zahteva osiguravač može značajno uticati na smanjenje premije.

Pored svih ovih problema, osiguranje od internet rizika će ubrzo postati neophodan vrsta osiguranja, pa se postavlja pitanje šta bi pokrivala takva vrsta osiguranja. Polisa osiguranja od internet rizika bipružala pokriće tako što bipre svega nadoknadila troškove angažovanja IT stručnjaka. Ti troškovi se uglavnom odnose na utvrđivanje obima štete, njenog limitiranja, povratka podatakaitd. Međutim, treba imati u vidu da je ovo najblaža finansijska posledica internet napada i samo mali deo pokrića internet osiguranja, te kao takav obično nije prvimotiv 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, sprečavanja neovlašćenog pristupa i korišćenja kompanijskih resursa i sprečavanje nastanka bezbednosnih propusta. 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 kazniizrečenih na osnovu prekršajnih naloga ovlašćenog državnog organa, troškova upravljanja kriznom situacijom, obaveštavanja korisnika i podrške klijentima, koji su takođe pokriveni polisom internet osiguranja.

Sa druge strane, postoje i kompanije koje ne dolaze u kontakt sa velikim brojem ličnih podataka trećih lica. One najpre strahuju od gubitaka poslovnih prihoda usled nemogućnosti poslovanja nakon internetincidenta. Uzročnik takvog prekida rada može bitikako širenje virusa postavljenog samo sa željom da se nanese šteta, tako i nemogućnost pristupa kompjuterskim sistemima i podacima usled želje da se izvršiiznuda finansijskih sredstava da bi se pristup

[27] Za više o pojmu i istorijatu podataka o ličnosti videti: S. Andonović (2019), *Zaštita podataka o ličnosti u elekronskoj javnoj upravi u RepubliciSrbiji- pravni aspekti,* doktorska disertacija, Pravni fakultet u Beogradu, 87-146.

omogućio. Polisa internet osiguranja u oba slučaja nadoknađuje utvrđenu izgubljenu dobit i plaća troškove iznude ukoliko angažovaniIT stručnjaci utvrde da je neophodno, a pod uslovom da su učinjeni svi razumni napori da se utvrdi da internetiznuda nije sama po sebi prevara, kao i napori da se izbegnu i umanje gubici.

Još jedan od problema koji se javlja kod osiguranja od internet rizika, a koji pogađa sve vrste osiguranja jeste problem moralnog hazarda.[28] Kao i kod drugih vrsta osiguranja kao najbolje rešenje javlja se predviđanje manje premije za one kompanije koje imaju razvijene bezbednosne protokolei 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]

- Osiguranje od internet rizika kao imovinsko osiguranje

Osiguranje od internet rizika spada u imovinska osiguranja u kome je vladajući princip obeštećenje osiguranika.[30] Naknada iz osiguranja treba da odgovara visini stvarno pretrpljene štete. Kako se ona u konkretnom slučaju teško može utvrditi postavlja se pitanje kako postupiti,s obzirom da je predvidetiisplatu ugovorenog iznosa bez utvrđivanja visinestvarno pretrpljene štete u suprotnosti sa principom obeštećenja.

Tradicionalne vrste osiguranja imovine ne pokrivaju ove vrste rizika, one bi eventualno pružale osiguravajuće pokriće u slučaju da internet napad dovede do nastanka nekog od osiguranih rizika kao što su požar ili eksplozija, koji prouzrokuju materijalnu štetu na osiguranim stvarima. Uzimajući u obzir sve veću upotrebu internetai svakodnevni razvoj tehnologije, kao i činjenicu da sve veći broj kompanija barem deo svog poslovanja obavlja preko interneta, detaljno regulisanje ove vrste osiguranja će postati neophodno.

Da bi se utvrdio najvišiiznos obaveze osiguravača neophodno je da se prilikom zaključenja ugovora odredi vrednost osiguranog interesa. Ukoliko je prilikom zaključenja ugovora o osiguranju teško utvrditi vrednost predmeta

[28] Rizik moralnog hazarda je rizik spremnosti jedne ugovorne strane da preuzima neuobičajene rizike, odnosno, da ne nastupa u ugovornim odnosima u dobroj veri. Može biti:
ex ante-kada se osiguranik upušta u rizičnije aktivnosti nego što bi inače činio
ex post- kada ne preduzima mere da smanji štetu koju proizvodi nastupanje osiguranog slučaja
„*Prevara*"- prijavljivanje veće štete kako bi ostvario veću nadokandu od osiguravajućeg društva

[29] Za više videti: L. Bailey (2014), „Mitigating Moral Hayard in Cyber-Risk Insurance",*Journal of Law & Cyber Warfare,* 1-42.

[30] „Iznos naknade ne može biti veći od štete koju je osiguranik pretrpeo nastupanjem osiguranog slučaja.", Zakon o obligacionim odnosima, član 925, stav 2.

osiguranja suma osiguranja se može utvrditi na više načina.[31]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 i osiguranje internet rizika se po pravilu zaključuje na vrednost koju odredi osiguranik koji najbolje zna kojiiznos 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.[32]

- Osiguranje od internet rizika kao osiguranje od odgovornosti

Kao što je već pomenuto prilikom internet napada ogromnu štetu može pretrpeti samo društvo, međutim ono što se javlja kao dodatni problem je što štetu najčešće trpei klijenti kompanije ili zaposleni usled „curenja" ličnih podataka kao što su matični broj, adresa, brojevi kreditnih kartica, tekućih računa, podaci o zdravstvenim ispravama, podaci o vozačkoj dozvoliisvi ostali podaci koji se vezuju za identitet određene osobe ili njeno finansijsko i zdravstveno stanje (podaci o i-mejl adresama, brojevima telefona, poštanskim adresama, itd.).U ovakvim slučajevima ta licaimaju pravo dapozovu društvo na odgovornost kada bi onopored naknade pretrpljene štete bilo u obavezi da plati prateće sudske, administrativne i druge troškove. Za većinu malih ili srednjih biznisa, čak i najmanji trošak internetincidenta može trajno da zatvori kompaniju. Pored toga javlja se i sekundarna šteta: narušavanje reputacije, nezadovoljnii oštećeni klijenti, otpušteni zaposleni, ugrožene porodice.

Incidenti koji uključuju zloupotrebu ili krađu ličnih podataka nisu ni približno u opadanju, ali ono što još više zabrinjava jeste nedovoljna informisanost o načinima zaštite podataka u poslovnom okruženju. Pored toga što mnoge kompanije i dalje nemaju adekvatno obučeno osoblje i stručnjake koji bi se bavili praćenjem prikupljanja, čuvanja i deljenja podataka, jako je mali broj onih koji curenje podataka vide kao rizik za svoju kompaniju.

[31] Npr. ako je rec o umetničkim ili drugim vrednostima osiguravač i osiguranik sporazumno utvrđuju tu vrednost. U trenutku kada nastupi osigurani slučaj osiguravač može da istice 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 pokrica utvrđuje po izboru osiguranika jer se ne može unapred znati koliku štetu on može da prouzrokuje drugome.

[32] J. Pak, 74.

Svakako ogroman značaj za zaštitu podataka od ličnostiima novi Zakon o zaštiti podataka o ličnosti[33]i nova direktiva EU *General Data Protection Directive*(GDPR)[34]. Stalna edukacija i podizanje bezbednosnih protokola na više standarde omogućiće i širu svest zaposlenih o važnosti pravilnog čuvanja poverljivih informacija. Podjednako je važno podići stepen zaštite i u interneti u realnom okruženju, a neki od prvih koraka je izrada protokola o rukovanju poverljivim podacima unutar kompanije u kojem će se odrediti ko od zaposlenih može da dođe u dodir sa poverljivim informacijama. Pojedine kompanije uveliko zapošljavaju i lice zaduženo za zaštitu podataka o ličnosti(*Data Security Officer-a*), stručnjaka koji će biti zadužen za sprovođenje strategije zaštite podataka i za kontrolu poštovanja procedura unutar kompanije. Ovo pokazuje da zaštita podataka od strane zaposlenih u kompanijii osiguranje odinternet rizika idu „ruku pod ruku" i oba predstavljaju neizostavni deo poslovne politike svake ozbiljne kompanije. Stoga,neophodno je omogućiti da se kontrola čuvanja podataka korisnika strože sprovodi unutar samih kompanija. Ipak, bez odgovarajuće strategije upravljanjainternet rizicima, kompanije neće biti u stanju da se izbore sa internet rizicima, barem ne na duže staze.

4. Osiguranje od internet rizika u Republici Srbiji

Osiguranje od internet rizika, na žalost, u Srbijiskoro uopšte nije razvijeno. Takva vrsta osiguranja je praktično tek „provirila" među prvima su je ponudili u kompaniji Wiener Stadtische osiguranje. Međutim, primeri internet napada su i u Srbiji mnogobrojni, tako da je nesporno da potreba za ovom vrstom osiguranja svakako postoji. Na primer, Narodna banka Srbije bila je žrtva internetincidenta poznatijeg kao "fake president"[35], u kojem je zatraženo da se na lažni račun jedne strane firme uplati suma u iznosu od 175.500 eura. Nakon nekoliko dana od izvršenja transakcije, službenici Banke primetili su prevaru – račun na koji je novac uplaćen je zapravo nepostojeći, a i-mejl sa kojeg je poslat zahtev takođe nije validan.

---

[33] *Sl. glasnik RS*, br. 87/2018

[34] UREDBA (EU) 2016/679 EVROPSKOG PARLAMENTA I VEĆA od 27. Aprila 2016.o zaštiti pojedinaca u vezi s obradom ličnih podataka i o slobodnom kretanju takvih podataka teo stavljanju van snage Direktive 95/46/EZ (Opšta uredba o zaštiti podataka)

[35] Ova vrsta prevara je jedna od najčešćih i sprovodi se obično tako što se kontaktira jedno lice koje je najčešće zaposleno u računovodstvu firme, navodno od strane nekog od lica koja imaju vodeću ulogu u kompaniji, i traži se od njega da izvrši hitnu uplatu na određeni račun davajući lažno ime primaoca i razlog uplate (npr. poverljive nabavke). Kada je izvršen transfer, novac se ubrzo skida uglavnom pre nego što lice upe da shvati da se radi o prevari da povuče transakciju.

Ovo je samo jedan od primera internet prevara, iz kog razloga potreba za razvojem ove vrste osiguranja sve više raste. Sa nastupanjem pandemije virusa COVID-19, pokazalo se da je potreba za ovom vrstom osiguranja ogromna. Naime,mnoge kompanije i preduzeća su usled pandemije prešla na rad od kuće, a takva situacija pružila je nove šanse internet kriminalcima da uđu u korporativne sisteme i dođu do podataka o poslovanju, računajući na radoznalost pojedinaca kojima se nude sadržaji poput „saznajte koji je lek protiv korona virusa".Otvaranjem zaraženih linkova ili priloga, omogućava se pristup podacima kompanije, odnosno krađa, zloupotreba iliizmena podataka.

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, a uzimajući u obzir činjenicu da većina kompanija barem deo svog poslovanja obavlja preko interneta, kao i da obično raspolažu velikim brojem ličnih podataka što svojih zaposlenih, što klijenata, ukoliko bi došlo do internet napada u kojem bi bili zloupotrebljeni ti podaci vrlo je verovatno da ne bi mogli da nastave svoje poslovanje. Iz tih razloga u Srbiji je prvenstveno potrebna edukacija zaposlenih, unapređenje sigurnosnih protokola, a dalje i da se razvije tržište osiguranja od internet rizika.

5. Zaključak

Svakodnevna sve veća upotreba kompjutera i interneta sa sobom nosi određene rizike. Jedan od najvećih rizika za privredna društva predstavlja internet napad koji u određenim slučajevima može dovesti i do propasti kompanije usled ogromnih troškova, gubitka ugleda i klijenata. Kao vid prevencije internet rizika javlja se ideja o osiguranju od ove vrste rizika. U slučaju nastanka štetnog događaja, nosioci polise mogu da računaju da će pretrpljena šteta biti ublažena i da će se njihovo poslovanje oporaviti od incidenta brže nego u slučaju nedostatka odgovarajućeg pokrića.

Međutim, pored niza problema kod ove vrste osiguranja, a koji su obrađeni u radu potrebno je naglasiti da osiguranje od internet rizika kao pojedinačno rešenje deluje adekvatno tek kada nastupi štetni događaj, pa samim tim najbolji rezultat donosi tek kada je deo opšte strategije upravljanja rizicima. Sve dok kompanije koje se bave prikupljanjem i obradom podataka o ličnosti ne posvete strukturnom rešavanju problema internet bezbednosti, čak iincident najmanjeg obima može naneti veliku štetu ne samo kompaniji, već i njenim klijentima. Takođe, 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 napadispreče ili bar umanje. 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.

* * *

CYBER RISK INSURANCE

Summary

The development and increasing use of computers and the internet, in addition to the huge benefits it brings us, such as saving time and money, also has certain risks. These risks relate primarily to internet attacks which are becoming more frequent and which can bring huge costs to the affected company. For these reasons, cyber risk insurance has appeared in highly developed countries, which aims to reduce the costs that would hit the company, because otherwise the collapse of the affected company would be almost certain. In the first part of the paper, the author deals primarily with the importance and the advantages of the Internet, but also its disadvantages, as well as the concept of internet risk. Further in the second part of the paper, author will analyze concept of cyber risk insurance, with a brief overview of cyber risk insurance in the Republic of Serbia.

Keywords: risk, internet, insurance, attack, property insurance, liability insurance.