Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 007.52
DOI: https://doi.org/10.24867/09GI13Stajsic

OSIGURANJE KAO NAČIN UPRAVLJANJA SAJBER RIZICIMA

INSURANCE AS A WAY TO MANAGE CYBER RISKS

Nada Stajšić Golijanin, *Fakultet tehničkih nauka, Novi Sad*

Oblast – INŽENJERSKI MENADŽMENT

Kratak sadržaj – *U radu su prikazane osnovne karakteristike novih rizika, među kojima se ističu rizici vezani za upotrebu digitalnih tehnologija, objedinjeni nazivom sajber rizici. Pitanja izloženosti i otpornosti, te pitanje upravljanja sajber rizicima su sagledana iz različizih perspektiva: od institucija od nacionalnog značaja, preko IT eksperata do osiguranja. Poseban akcenat je stavljen na akumulaciju sajber rizika i analizu adekvatnosti zaštite pomoću postojećih osiguravajućih pokrića.*

Ključne reči: *Rizik, upravljanje rizikom, sajber rizik, osiguranje, akumulacija rizika, procena i preuzimanje rizika*

Abstract – *The paper presents the basic characteristics of new risks, among which are the risks associated with the use of digital technologies, united by the name of cyber risks. Issues of exposure and resilience, as well as the issue of cyber risk management are viewed from different perspectives: from institutions of national importance, through IT experts to insurance. Special emphasis is placed on the accumulation of cyber risk and the analysis of the adequacy of protection with the help of existing insurance coverage.*

Keywords: *Risk, risk management, cyber risk, insurance, risk accumulation, underwriting.*

1. UVOD

Društvo XXI veka podvrgnuto je sveobuhvatnoj digitalnoj transformaciji. Bezmalo svi aspekti modernog života trpe promene prouzrokovane prisutnošću i napretkom tehnologije. Oslonjenost na nove tehnologije i internet servise, dostupnost i sigurnost tih servisa, posebno finansijskih, osnov je stabilnosti i uslov bez kog se ne može zamisliti moderno poslovanje i svakodnevni život pojedinaca.

Ogromne količine podataka koji se generišu korišćenjem tehnologije su platforma za dalje napredovanje i razvoj, ali i izvor bezbednosnih rizika. Izloženost pretnjama i rizicima je stanje stvari, a upravljanje rizicima izazov koji je postavljen pred eksperte za nove tehnologije i osiguravače, ravnopravno. Posmatrajući stvari iz svog ugla, osiguravači su postali svesni da su oštećenje podataka, narušavanje njihovog integriteta i (ne)dostupnost IT servisa osnovna područja u kojima treba sagledati i dimenzionisati rizik, i na kraju proceniti mogućnosti njegovog preuzimanja.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Đorđe Ćosić, vanr. prof.

2. OSIGURANJE, KARAKTERISTIKE I ZNAČAJ

Sa aspekta pojedinca, uloga osiguranja je dvostruka: zaštita osiguranika i zaštita trećih lica. U oba slučaja, i kod zaštite osiguranikovog telesnog integriteta i njegove imovine ili odgovornosti za štete pričinjene trećim licima, kroz naknadu štete nastale realizacijom osiguranog slučaja štiti se materijalni položaj osiguranika. Uporediv pristup je moguć i sa aspekta privrede, s tim što se uvećanjem subjekta uvećava i veličina mogućih gubitaka, pa se značaj osiguranja ogleda u sposobnosti da nadoknadi štete koje bi mogle ugroziti funkcionisanje privrede jedne države [1].

Osiguravači predstavljaju bitne aktere u inovacijama i napredovanju mnogih oblasti nauke i tehnologije: medicine, industrije, novih tehnologija, jer obezbeđuju preuzimanje rizika i tako omogućavaju nove poduhvate. U svetskim razmerama, osiguravači se pojavljuju kao bitni investitori, budući da raspolažu značajnim fondovima

Osiguranje omogućava transferisanje potencijalnih pojedinačnih šteta na zajednicu rizika a potom predviđene ukupne troškove svih šteta, utvrđivanjem premija osiguranja kao cene osiguravajućeg pokrića, podjednako raspoređuje na sve članove zajednice rizika. Precizna procena rizika, ukupnog iznosa šteta koje mogu nastati i premija koje su potrebne za pokriće svih potencijalnih ostvarenja rizika, predstavaljaju osnovne zadatke tehničke organizacije osiguranja.

Da bi se pojedinačnim rizikom moglo upravljati putem transfera na osiguranje, rizik mora biti osigurljiv [2]. Na strani osiguranika mora postojati volja da se rizik kontroliše, kao i potpuno odsustvo namere da se podstiče njegovo ostvarenje.

Sa druge strane, sam rizik mora biti merljiv u smislu verovatnoće njegovog nastanka i obima posledica, kako bi bila odrediva njegova cena i prihvatljivost, kako za osiguranika tako i za osiguravača.

3. SAJBER RIZICI – ODREĐENJE POJMA

Iako je **sajber rizik** postao široko rasprostranjen termin, njegova definicija je i dalje predmet stalnog istraživanja i promena. U najširem smislu, sajber rizik se definiše kao rizik od obavljanja posla u sajber okruženju („risk of doing business in the cyber environment“ [3]). Budući da je usko povezan sa primenom novih tehnologija, spada u grupu rizika na čije ostvarenje prevashodno utiče ljudski faktor.

Ipak, nije nemoguće da do poremećaja i/ili gubitka u digitalnom okruženju dođe usled ostvarenja nekog od prirodnih rizika. Npr. prirodna katastrofa kao što je

zemljotres ili vetar izvanredne jačine kao posledicu mogu imati nedostupnost digitalnih resursa.

Infrastruktura u kojoj nastaju napadi su mreže, bilo kompanijske ili globalne, zasnovane na internet tehnologijama i/ili telekomunikacijama.

Gubici kao uzrok imaju sajber napad u najširem smislu, a mogu se manifestovati na različite načine: pražnjenja bankovnih računa, prevare počinjene usled zloupotrebe podataka, odgovornost za skladištenje podataka, izlaganja poverljivih podataka posetiocima sajta od strane nepažljivog zaposlenog, dostupnost, integritet i poverljivost elektronskih informacija.

3.1. Uzroci nastanka sajber rizika

Iako sajber rizik postoji u gotovo neograničenom broju oblika, podela na osnovu namere i porekla rizika predstavlja široku platformu u koju je moguće smestiti sve pojedinačne, međusobno veoma različite, slučajeve.

Unutrašnji i zlonamerni: Uglavnom namerno delo sabotaže ili krađe od strane nekoga iz kompanije.

Unutrašnji i nenamerni: Greške koje počine zaposleni. Čak se i dobronamernim ekspertima mogu desiti propusti, da npr. obore firewall ili onemoguće back-up podataka.

Spoljni i zlonamerni: Za najozbiljnije se smatraju napadi koji dolaze izvana, od zlonamernih pojedinaca ili grupa. Najčešći cilj napada su baze podataka, preopterećenje sistema ili isključenje kritične opreme.

Spoljni i nenamerni: Slučajni uticaj na vaš sistem. Softverska greška ili prirodne katastrofe mogu prouzrokovati nedostupnost sistema.

Očigledno, rizici i uticaji mogu biti posledica ljudskih ili sistemskih grešaka, ali i sajber kriminala koji je često vođen tradicionalnim kriminalnim motivima, poput krađe ili sabotaže, koja se može izvršiti bez potrebe za fizičkom blizinom. Rasprostranjena je upotreba zlonamernog softvera (ransomware, malware), sabotaže, napadi usamljenih hakera, preko sofisticiranih mreža ili hakiranje uz podršku države.

Zanimljivost sajber sveta očituje se i u činjenici da se uporediva „oružja“ koriste nezavisno od mete, bilo da se radi o pojedincu, kompaniji ili vladi neke države.

Ipak, ne postoji ravnopravnost u efektima napada: sa znatno ozbiljnijim posledicama rezultiraju napadi čija je meta npr. sistem za podršku izborima na bilo kom nivou (lokalnom, saveznom), upravljački sistem nekog industrijskog postrojenja, koji kao implikaciju mogu imati i znatne fizičke štete, ili baza podataka koja sadrži delikatne podatke o kompanijama i ličnostima.

4. UPRAVLJANJE SAJBER RIZIKOM

Stavljanje pod kontrolu sajber rizika, ublažavanje posledica napada i uopšte povećanje stepena sigurnosti u sajber svetu tema je koja zaokuplja široki skup aktera: doneti su nacionalni programi za zaštitu u sajber svetu, veliki broj kompanija razvija sisteme zaštite od sajber napada, a osiguravači svoje mesto traže u „pukotinama“ i nedorečenostima navedenih sistema. Budući da ne postoje neprobojni sistemi zaštite, mesto za osiguranje izvesno postoji.

U potrazi za najboljom praksom u zaštiti od kibernetičkih rizika na području SAD i EU angažovano je više nacionalnih institucija, uključujući Nacionalni institut za standarde i tehnologiju (NIST) u SAD i GCHQ (UK Government Communications Headquarters) u Velikoj Britaniji. Pored institucija od nacionalnog značaja, ovoj temi je posvećeno i niz organizacija koje nadilaze granice država, kao i kompanija koje razvijaju sisteme zaštite kao vlastite proizvode.

Rezultat ovih nastojanja jeste skup propisa različitih nivoa (uredbe, direktive, zakoni), na osnovu kojih su od strane eksperata predloženi okviri za upravljanje sajber rizicima. Nezavisno od nivoa ne kome je prisutna potreba za definisanjem mera za zaštitu od sajber rizika, sve prikazane regulative sugerišu da je za dimenzionisanje adekvatne zaštite neophodno da organizacije, bez obzira na njihovo poreklo i oblast rada, razmotre šta su ključne vrednosti koje treba zaštiti, bilo da se radi o podacima ili sistemima. Identifikacija kritičnih podataka i sistema omogućava kompanijama da razumeju njihovu izloženost riziku i ranjivost.

Garantovanje potpune sigurnosti nemoguće je usled usložnjavanja sistema, njihove međusobne povezanost i uslovljenosti napretkom tehnologije, ali i usled činjenice da postojeće statistike ukazuju da je veći broj sajber rizika uslovljen ljudskim ponašanjem. Slabosti tehnologije i nedostaci sistema su lakše sagledivi, a time i pogodniji za upravljanje od predviđanja delovanja ljudi.

Da bi se odgovorilo na rastuće potrebe svih subjekata koji su izloženi sajber rizicima, identifikovan je radni okvir koji za cilj ima jačanje otpornosti i osmišljavanje adekvatnog risk-menadžmenta, a koji se temelji na četiri stuba: pripremi, zaštiti, otkrivanju i poboljšanju.

Prepoznati svoju kritičnu imovinu i procese, osigurati dobro utemeljenu i ponovljivu spremnost za sajber napade, razviti mogućnosti otkrivanja i kontinuiranog nadgledanja sposobnosti prepoznavanja nedostataka sistema i vanjskih pretnji imovini, izgraditi sveobuhvatnu bazu podataka bezbednosnih incidenata koji podržavaju kontinuirano učenje i na kraju, omogućiti oporavak od incidenata u što kraćem vremenskom periodu [3], siže je okvira.

5. ULOGA OSIGURANJA U UPRAVLJANJU SAJBER RIZICIMA

Značaj industrije osiguranja, kada je reč o novim rizicima, pre svega je viđen u kvantifikovanju rizika i upravljanju njima [4]. Kvantifikovanje rizika je veoma opterećeno nespremnošću kompanija, uključujući i osiguravače, da u potpunosti podele informacije o posledicama ostvarenja rizika. Ukupni troškovi koje kompanije imaju u vezi sa malicioznim sajber napadima je teško proceniti zbog toga što je jedan broj incidenata neotkriven, nije moguće pribaviti podatke o svim izdacima, a ponajpre zbog toga što se ovi napadi žele držati u tajnosti, budući da imaju direktan uticaj na reputaciju žrtve napada.

Ali, da li osiguravači vide jasno svoje mesto u svetu sajber rizika? Da li su procenjive maksimalno moguće štete (MPL)? Da li je jasno na koje sve linije biznisa bi imao uticaj jedan isti napad? Kakve fondove treba da ima osiguravač koji može da nosi ovakve rizike i, konačno, da li je moguće pružiti sigurnost drugima ako ne možete biti sigurni u svoju poziciju?

Sajber napadi mogu poteći od širokog spektra aktera, uticati na sve industrije i rezultirati različitim nivoima oštećenja podataka, kritičnih sistema, fizičke svojine, pa čak i prekidom poslovanja. Iz tog razloga sajber rizici mogu aktivirati razna osiguranja, kao što su: opšta i profesionalna odgovornost, osiguranja prekida rada, imovinska osiguranja zbog npr. fizičkog oštećenja izazvanog požarom kome je prethodio sajber napad, D&O, odgovornost za proizvode usled neispravnosti u kibernetičkom proizvodu, koja može biti uzrokovana sajber napadom (npr. cloud computing), profesionalna odgovornost, (greška u programiranju ili propust u održavanju, profesionalna odšteta).

Ipak postojanje rizika i izloženost njima je samo ishodište puta na čijem kraju je adekvatno osiguravajuće pokriće, do koga se dolazi nakon procene održivosti određene vrste osiguranja, akumulacije rizika i njegove cene.

5.1 Preduslovi održivosti osiguranja od sajber rizika

Na osnovu studije sprovedene od strane vodećeg međunarodnog istraživačkog centra u oblasti osiguranja, The Geneva association, pod nazivom „Unapređeno upravljanje akumulacijom rizika u sajber osiguranju“ [5], postoje tri preduslova za održivost tržišta sajber osiguranja:

Prvo, na izvoru rizika mora biti dovoljno otpornosti, tj. moraju biti sprovedene odgovarajuće mere zaštite. Da vlasnici kuća ne zaključavaju svoje domove, krađa ne bi mogla biti osigurana. Prvi koraci u sagledavanju bilo kog rizika su: proceniti, meriti i upravljati njime. Višak rizika, koji preostaje nakon svih preduzetih mera i nije sadržan u izvoru rizika, može se ublažiti kroz osiguranje.

Drugo, osiguravači moraju ostvariti prihvatljiv povrat kapitala. Ovo zahteva disciplinovanu i efektivnu procenu rizika.

Treće, raspoloživi kapital mora da izdrži udare akumuliranih događaja i da obezbedi adekvatne naknade osiguranicima nakon takvog događaja – u slučaju sajber rizika, upravo je akumulacija rizika, tj. njena absorbcija i upravljanje njome glavna briga osiguravača.

5.2. Akumulacija rizika – izazov za eksperte i istraživače

U istraživanju koje je sproveo Risk Management Solutions, Inc. i Centre for Risk Studies Cembridge university [6] razmotreno je pitanje akumulacije sajber rizika i upravljanja njime.

Istraživanja ukazuju da potražnja za sajber osiguranjem značajno premašuje trenutno kapacitet obezbeđen od strane osiguravača. Primarni razlog zbog koga je većina osiguravača na pojačanom oprezu kada je sajber rizik u pitanju je akumulacija rizika. Osiguravačima je teško proceniti da li bi veliki sajber incident izazvao gubitke kod mnogih njihovih osiguranika istovremeno.

Do sada industrija osiguranja ima iskustvo sa visokim odštetnim zahtevima pojedinačnih kompanija, ali ne postoji slučaj 'katastrofalnog događaja' koji je pogodio veliki broj kompanija i prouzrokovao velike štete po polisama sajber osiguranja.

Bez sposobnosti da proceni PML, osiguravači se povlače na sigurno, uz pretpostavku da bi jedan ozbiljan napad iscrpio njihov samopridržaj za tu grupu rizika, što je pogubno polazište za razvoj tržišta sajber osiguranja, budući da ograničava kapacitet osiguravača u prihvatanju rizika, kao i u efikasnosti korišćenja rizičnog kapitala.

Upravo ovde leži značaj istraživanja pitanja akumulacije sajber rizika i uspostavljanja važnih koncepata koji pomažu u kvantifikovanju akumulacije rizika. Uočljivo je da se primenom opisanih okvira za upravljanje sajber rizicima značajno podiže nivo kontrole nad akumulacijom rizika, tj. mere opreza kojima se rizik može sprečiti i/ili umanjiti utiče i na umanjenje akumulacije.

5.3.Primeri pokrića u svetu

Istraživanje tržišta koje su 2018. godine sproveli Advisen i PartnerRe [7] pokazalo je da se pokrića za sajber rizike pomeraju iz sfere dodataka i proširenja u sferu samostalnih, celovitih proizvoda. Na svetskon tržištu postoji najmanje 35 osiguravača koji trenutno nude proizvode za osiguranje sajber rizika. Poseban izazov predstavlja činjenica da na tržištu ne postoje dva identična proizvoda za osiguranje sajber rizika, na šta je tržište naviknuto kod drugih vrsta osiguranja. U 26 analiziranih proizvoda nisu pronađena dva sa istim brojem i tipom pokrića: jednima je u fokusu bila zaštita imovine osiguranika, a drugima različite vrste odgovornosti.

Ipak, postoje i značajne sličnosti i dominantna pokrića kod svih proizvoda. Stepen prisutnosti pojedinačnih pokrića u proizvodima na tržištu je prikazan u Tabeli 1. Uočljivo je da dominiraju pokrića vezana za gubitke podataka, kršenje privatnosti, oštećenje softvera i troškove povezane sa odgovorom na incident.

5.4.Sajber osiguranje na domaćem tržištu

Za razliku od visokorazvijenih država, gde je tržište odgovorilo na pretnje ponudom konkretnih proizvoda koji se međusobno razlikuju, domaća društva još uvek nemaju u ponudi ovu vrstu osiguranja koja bi odgovarala sadržini uslova osiguranja stranih osiguravača [8]. Tradicionalne vrste osiguranja imovine ne pokrivaju ove vrste rizika, iako je moguće da se i po takvim polisama osiguranja pruža pokriće prilično ograničenog obima. Tako, na primer, tradicionalno osiguranje imovine pružalo bi osiguravajuće pokriće u slučaju da sajber napad dovede do nastanka nekog od osiguranih rizika kao što su požar ili eksplozija, koji prouzrokuju materijalnu štetu na osiguranim stvarima. Domaća društva za osiguranje prodaju „Kombinovano osiguranje elektronskih računara, procesora i sličnih uređaja", koje pruža pokriće samo od tzv. požarnih rizika i krađe, svojstvenih osiguranju imovine.

Kada je o odgovornosti reč, domaći osiguravači su uglavnom isključili sajber rizike iz pokrića. Kod osiguranja opšte odgovornosti, isključena su potraživanja koja proističu iz štete ili nemogućnosti upotrebe materijalnih ili nematerijalnih dobara, gubitka podataka, otkrivanja poverljivih informacija ili bilo kog drugog gubitka koji je direktno ili indirektno povezan sa prijemom ili prenosom kompjuterskog virusa ili drugog štetnog programa putem interneta ili na bilo koji drugi elektronski način, kao i putem neovlašćenog ometanja internetske veze, mreže, računara ili telekomunikacionog uređaja [9].

Tabela 1. *Najčešća pokrića koja se pojavljuju u proizvodima na tržištu osiguranja [6]*

Oznaka pokrića	Vrsta sajber pokrića	% proizvoda koji sadrže ovo pokriće (uzorak od 26 proizvoda)
1	Kršenje privatnosti	92%
2	Gubitak podataka i softvera	81%
6	Troškovi odgovora na incident	81%
15	Sajber iznuda	73%
4	Prekid poslovanja	69%
12	Odgovornost za multimedijalne sadržaje (kleveta i omalovažavanje)	65%
7	Troškovi zastupanja i taksi	62%
14	Narušavanje ugleda/reputacija	46%
3	Greške u mrežnim servisima, Odgovornost	42%
5	Prekid poslovanja zbog spoljnih uzroka	33%
9	Odgovornost - tehnološke greške i propusti	27%
10	Odgovornost - Greške i propusti u profesionalnim uslugama	23%
13	Finansijska krađa i prevara	23%
16	Krađa intelektualne svojine (IP theft)	23%
18	Oštećenje fizičke imovine	19%
19	Smrt I telesne povrede	15%
	- Sajber terorizam	12%
11	Odgovornost – D & O	13%
8	Odgovornost – Proizvodi i operacije	8%
17	Oštećenje životne sredine	4%

Identično isključenje je u svim uslovima za osiguranje profesionalnih odgovornosti: revizora, advokata, lekara, javnih beležnika, stečajnih upravnik, itd., kao i osiguranju od odgovornosti za proizvode. Jasna je namera osiguravača da osvesti temu sajber rizika i da isključi svoju obavezu u slučaju njegovog nastupanja.

U poslednje dve godine osiguravači koji posluju na području Republike Srbije nude proizvode stranih osiguravajućih kuća za osiguranje od IT i sajber rizika.Isrtaživanje sprovedeno u okviru master rada o stanju domaćeg tržišta osiguranja u kontekstu sajber rizika ukazuje da se kod nas sajber pokrića sagledavaju prevashodno iz ugla obaveze: osiguranje se skoro isključivo ugovara ako je osiguranik u obavezi da poslovnom partneru, kao preduslov saradnje, dokaže da ima ovo pokriće.

Najviši nivo poznavanja rizika je u IT sektoru, a i kada je svest o potencijalnim opasnostima u pitanju, prednjače kompanije iz korpusa novih tehnologija. Domaći osiguravači ističu da se izloženost sajber rizicima nikako ne ograničava na spomenute sektore, budući da svetska iskustva svedoče da su najugroženije finansijske institucije i zdravstvene ustanove, zbog obima i delikatnosti podataka kojima rukuju. Ako se ima u vidu ukupan portfelj neživotnih osiguranja i struktura pravnih subjekata, izvodi se zaključak da su osiguranici veoma slabo upoznati sa novim pretnjama.

6. ZAKLJUČAK

Transformacija poslovanja, koje je većim delom prebačeno na računarske mreže, donela je velike benefite, ali i bezbednosne rizike.

Prepoznavanje faktora koji utiču na sajber sigurnost i njihova kontrola preduslov je aktiviranja dodatnog društvenog instrumenta za upravljanje rizikom, osiguranja.

Pred osiguravačima je veliki izazov, budući da su pitanja akumulacije sajber rizika još uvek bez potpunog i pravog odgovora, pa je time i oprez na strani osiguravača na značajnom nivou.

I pored toga, tržište sajber osiguranja u svetu nastavlja da se razvija, pre svega pod uticajem visoko profilisanih napada na integritet podataka i regulatornih zahteva koji su sa tim u vezi. Privredni subjekti mogu značajno unaprediti upravljanje sajber rizikom odgovarajući na zahtev osiguravača i implementirajući najbolju praksu koja objedinjuje ljude, procese i tehnologije, a nadopunjuje se osiguranjem.

7. LITERATURA

[1] J. L. Athearn, *„Risk and insurance*“, New York, 1977.
[2] V. Njegomir, *“Upravljnje rizicima u osiguranju i reosiguranju”*, Zagreb, 2018.
[3] https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf (pristupljeno u oktobru 2019.)
[4] https://www.csis.org/events/managing-cyber-risk-and-role-insurance (pristupljeno u novembru 2019.)
[5] https://www.genevaassociation.org/sites/default/files/-research-topics-document-type/pdf_public/research_brief_-advancing_accumulation_risk_management_in_cyber_insurance.pdf (pristupljeno u januaru 2020)
[6] https://www.jbs.cam.ac.uk/fileadmin/user_upload/-research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf (pristupljeno u februaru 2020)
[7] https://partnerre.com/wp-content/uploads/2018/10/2018-Survey-of-Cyber-Insurance-Market-Trends.pdf (pristupljeno u februaru 2020)
[8] S. Jovanović, *„Osiguranje od informatičkih rizika*“, Teme, 2017.
[9] Uslovi za osiguranje opšte odgovornosti, Kompanija „Dunav osiguranje“ a.d.o. Beograd

Kratka biografija:

Nada Stajšić Golijanin je rođena u Sarajevu 1968. godine. Diplomirala je na Elektronskom fakultetu u Nišu 1993. godine. Master rad na Fakultetu tehničkih nauka iz oblasti Inženjerski mendažment – Upravljanje rizicima i menadžment osiguranja odbranila je 2020. god. Kontakt: stajsicnada@gmail.com