Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 005:368
DOI: https://doi.org/10.24867/18GI04Saramandic

OSIGURANJE SAJBER RIZIKA

CYBER RISK INSURANCE

Dušan Saramandić, Bogdan Kuzmanović, *Fakultet tehničkih nauka, Novi Sad*

Oblast – INŽENJERSKI MENADŽMENT

Kratak sadržaj - *Kao novi proizvod, sajber pokriće ima sve važniju ulogu u zemlji i svetu i predstavlja nezaobilaznu instancu kad god se razmatra budućnost osiguranja. Do koje mere sajber osiguranje dobija na značaju, pokazuje veliki broj novih regulativa koje regulišu upravo ovu sferu privrede i poslovanja u digitalnom svetu uopšte. Istraživanje u ovom Master radu ima za svrhu prvenstveno da uvede pojam sajber osiguranja a zatim i pokaže značaj koji danas ima u svetu. Osnovni zadatak ovog rada jeste prikaz postojećih proizvoda osiguranja u momentu pisanja rada i analiza njhovih rezultata.*

Ključne reči: *Osiguranje, Analiza rizika, Sajber pokriće.*

Abstract - *As a new product, cyber coverage has an increasingly important role in the country and abroad and is an unavoidable instance whenever the future of insurance is considered. The extent to which cyber insurance has gained importance is shown by a large number of new regulations that regulate this sphere of economy and business in the digital world in general. The research in this Master thesis aims primarily to introduce the concept of cyber insurance and then to show the importance it has in the world today. The main task of this paper is to present the existing insurance products at the time of writing and analyze their results.*

Ključne reči: *Osiguranje, Analiza rizika, Sajber pokriće.*

1. UVOD

Predmet istraživanja ovog rada jeste sajber osiguranje i sajber rizik. Sajber rizik kao pojam predstavlja svaki rizik u organizaciji, koji za posledicu može imati gubitak, kvar ili pogrešno korišćenje svog ili informaciono tehnološkog sistema trećeg lica, izazvanog slučajnim ili zlonamernim akcijama.
Kao novitet na našem tržištu, ovo pokriće predstavlja novi izazov sa kojim moraju da se susretnu domaći osiguravači. Iako i dalje predstavlja neistraženo područje u potpunosti, javlja se obaveza sagledavanja inostranih iskustava po ovom pitanju kako bi se naš region adekvatno spremio za ono što čeka svako tržište.

NAPOMENA:
Ovaj rad nastao je iz master rada čiji mentor je bio prof. dr Bogdan Kuzmanović.

2. POJAM OSIGURANJA

Reč osiguranje u našem jeziku predstavlja zaštitu i obezbeđenje. Sama svrha osiguranja jeste pružanje sigurnosti. Koliko ta dodatna sigurnost znači može se ustanoviti sagledavanjem činjenice da nijedan ni veći ni manji infrastrukturni projekat se više ne gradi bez osiguranja. To pokazuje da bi veliki deo, ako ne i celokupna privreda u današnjem obimu koji poznajemo stala preko noći, ukoliko nestane i osiguranja. Ako sagledamo i iz ugla pojedinca, sama činjenica da su u razvijenijim zemljama obavezni različiti oblici osiguranja, ukazuje na nužnost njegovog postojanja kao institucije. Osiguranje i dodatna sigurnost koja proizilazi ist istog, omogućava neometano razvijanje privrede, društva pa i čitave civilizacije. Ono omogućava brzo saniranje posledica katastrofalnih događaja, što ranije tokom istorije nije bilo moguće.
Mogućnost otklanjanja dodatne neizvesnosti koju priža osiguranje postaje pretpostavka za dalji razvoj i brži napredak.

3. EKONOMSKI ZNAČAJ SPROVOĐENJA OSIGURANJA

Čovek se u svojoj svakodnevnici suočava sa velikom moći prirode i pokušava je prilagoditi svom lagodnom i konfornom životu. Neretko je svedok njene velike razorne moći i nije uvek u mogućnosti da pronađe pravi odgovor na tu vrstu problema. Rušilačka moć prirodnih katastrofa po pravila sa sobom nosi i velike finansijske i ljudske gubitke. Način kojim čovek može da se bori protiv takvih problem jeste osiguranje. Osiguranje omogućava sanaciju i nadoknadu štete uzrokovanu nesrećnim slučajem. Nesrećni slučaj može da podrazumeva imovinsku štetu usled prirodne katastrofe ili životnu nezgodu (invaliditet, smrt itd.), što znači da postoje više vrsta rizika koje osiguranje kao vid sanacije nezgode, može da pokrije.
Način na koji osiguranje uspeva da prevaziđe ovu vrstu problema leži u principu uzajamnosti. Princip uzajamnosti predstavlja osnov udruživanja kapitala kao preventivnu meru. Naime, ukoliko se pokazalo da na svakih par godina dođe do prirodne nepogode ljudi mogu unapred prikupljati i odvajati sredstva namenjena sanacijii događaja kojim su svi ugroženi. Time, ukoliko katastrofa kao što je na primer zemljotres pogodi deset kuća, i napravi potpunu štetu, ta šteta neće biti toliko velika za svaku poredicu pojedinačno, već će celo naselje raspodeliti tu štetu prikupivši prethodno sredstva za sanaciju, prilozima daleko manjim nego što je iznos potpune štete. Ovakav vid zajedničkog nošenja tereta doprinosi opštem blagostanju društva i stabilnijeg okruženja za život.

Opasnost kao takvu možemo podeliti u dve grupe: na one koje se dešavaju bez ikakve kontrole čoveka poput mraza ili uragana; i na one koje čovek može da predupredi u nekoj meri kao što su požar. Kod druge grupe, čovek svesnim akcijama može smanjiti šansu nastanka događaja i zato se visokorizične radnje, poput paljenja cigarete na benzinskoj pumpi, izbegavaju.
Kao što vidimo u svakodnevnom životu, čovek nastoji da smanji svoju izloženost stihijama koje mu prete, preduzimanjem preventivnih mera. Čak i za slučajeve gde je gubitak neminovan, kao što je primer razornih zemljotresa, institucija osiguranja omogućava brz oporavak i relativno mali gubitak za društvo, obnavljajući sve što je uništeno. S te tačke gledišta, osiguranje je civilizacijsko dostignuće jer omogućava neometani napredak društva, ne dozvoljavajući dugoročne posledice stihije, bile one u industrijskom ili privatnom sektoru. S tim u vidu, osiguranje je obezbedilo potpuno neutralisanje nesrećnih događaja bar u finansijkom smislu, izuzimajući humanitarne katastrofe.

3.1. Tehnička osnova funkcionisanja osiguranja

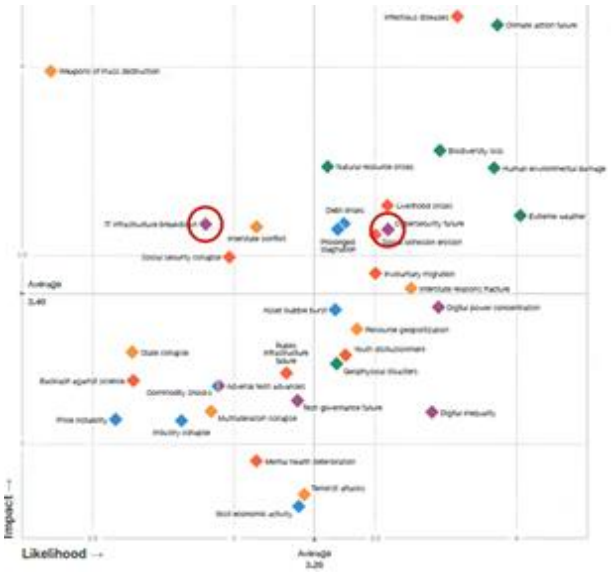
Kako bi osiguranje kontinuirano funkcionisalo, neophona je akumulacija novčanih sredstava. Kako bi se oformirala unapred određena količina novca koji će se koristiti za obnovu svih nastalih šteta, potrebno je odvajanje unapred namenjenih sredstava koja će služiti u tu svrhu. Iz tog razloga, obrazuje se osiguravajući fond.
Kako bi se obnova uništenih dobara odvijala kontinuirano, odmah nakon štete, potrebno je da u tom osiguravajućem fondu ne manjka novčanih sredstava, kako bi se izbegao svaki zastoj. Zastoj funkcionisanja osiguranja kao institucije, bi direktno uticao na zastoj celokupne privrede, što bi za krajnju posledicu imalo pogoršanje društvenog blagostanja.
Imajući u vidu kapitalnu ulogu, koju osiguravajući fond ima u funkcionisanju samog osiguranja, jedna od važnijih tema je i način njegove organizacije.

4. SAJBER RIZIK

Sajber osiguranje je isprepleteno sa drugim granama i vrstama osiguranja. Razlog za to je što svaka vrsta poslovanja prelazi u digitalnu sferu, što samim tim znači da je podložna sajber rizicima. Imajući to u vidu, neki drugi proizvodi osiguranja mogu obezbediti i određena sajber pokrića. Imovinska polisa na primer može pružati kao dodatak specifična sajber pokrića. Dodavanjem teksta klauzula koje uključuju sajber pokriće, izbegava se zaključivanje posebnih polisa i smanjuje birokratija. Kao što smo već naveli, nekada posebno naglašavanje nije ni potrebno jer imovinska polisa obično nadoknađuje svaku imovinsku štetu bilo ona izazvana sajber napadom ili ne.
Sajber proizvodi osiguranja mogu biti namenjeni nadoknadi troškova licu koje zaključuje osiguranje ili nadoknadi troškova trećim licima. Sajber pokriće nije pravljeno kao paket proizvoda gde se više pokrića uzima od jednom, kao kod imovinskih polisa požara i zemljotresa, već su podložni proširivanju i sužavanju pokrića u zavisnoti od potreba korisnika. Sa druge strane, podzraumevano pokriće može varirati u zavisnoti od tržišta, te je potrebno dobro proučiti šta je obuhvaćeno a šta ne. Što se tiče limita, uglavnom se određuje na agregatnoj osnovi, i to po gubitku, a u nekim ređim slučajevim i po godini. Sajber pokrića većinom imaju više okidača, koji pokreću polisu, a to su najčešće**:**

- prijavljene štete od strane trećih lica
- opažanje i otkriće upada u sistem kao i troškova vezanih za isto (troškovi IT forenzičara, obaveštenja ugroženih korisnika, troškovi pravne pomoći itd.). Obično je potrebno par nedelja, ili par meseci da se uopšte otkrije da je došlo do hakerskog napada. To znači da tek po otkriću će se pokrenuti polisa, iako je moguće da je šteta nastala mnogo ranije
- prinudno stopiranje poslovanja

4.1. Nastanak i karakteristike

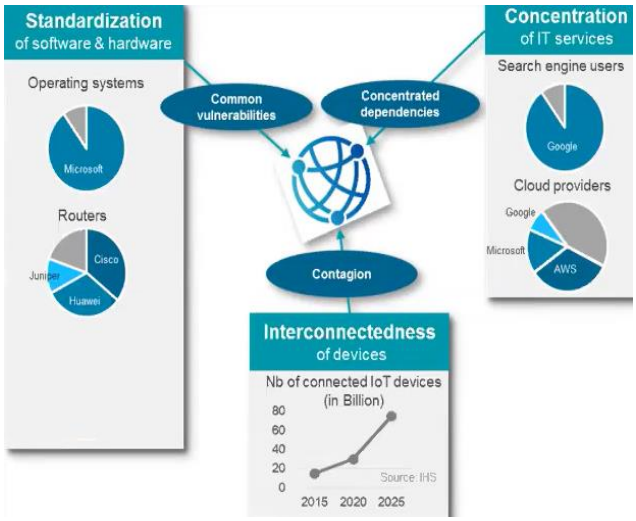


Slika 1. *Izveštaj o globalnim rizicima - Svetski ekonomski forum 2021.*

Na slici 1. prikazan je grafikon iz Izveštaja o globalnim rizicima sa Svetksog ekonomskog foruma 2021. godine gde grafikon pokazuje da sajber rizici konstantno zauzimaju veliki udeo u ukupnom procentu potencijalnih opasnosti.
Pored toga što sajber napadi ostavljaju veliki stepen štete, takođe predstavljaju kategoriju rizika koja ima najveću verovatnoću da se desi. Na prikazanom grafikonu na trećoj poziciji odmah nakon rizika prenosivih bolesti (što je razumljivo imajući u vidu Corona virus) i rizika katastrofalnih događaja (usled klimatskih promena) vidimo sajber rizik. Imajući to u vidu i ukoliko se Corona virus sagledava kao kratkoročni problem, sajber zaštita će imati još važniju ulogu u društvu.
Prethodnih godina sama percepcija sajber rizika se menja u celom svetu. Usled tehnoloških promena koje civilizacija trpi kontinuirano, normalno je neprekidno adaptiranje i na nove vrste ovakvog rizika. Trenutna pandemija ubrzala je proces digitalizacije i dodatno promenila način funkcionisanja celokupne planete. Kako u pogledu poslovanja tako i u sferama obrazovanja pa čak i razonode. Takođe, koren takvih promena predstavlja povećanu međuzavisnot čoveka i digitalnih tehnologija.

4.2. Delovanje ovog rizika i uticaj na savremenu ekonomiju

Ubrzavanjem procesa digitalizacije, mnoge kompanije su se zatekle nespremne i još uvek pokušavaju da se priviknu na novi vid funkcionisanja. Veliki sistemi i korporacije su pravljenjem dodatnih podsistema, uspeli u nekoj meri da digitalizuju poslovanje, ali manja i srednja preduzeća se i dan danas bore sa tim izazovom. Imajući u vidu veliku količinu posla koju je potrebno uraditi, neretko se zanemaruje adekvatna sigurnost, zaštita i čuvanje rezervnih podataka. To dalje prouzrokuje mnoge nove slabosti u svakom privrednom subjektu. Kada se na to još doda faktor ljudske greške, usled nedovoljnog znanja ili adekvatne obuke za korišćenje digitalnih alata lako se može objasniti zašto je sajber rizik sve veći. Sistemi koji pokazuju toliku ranjivost postaju baš iz tog razloga mete sve češćih hakerskih napada, kako kroz suptilne viruse, koji bivaju otvoreni kroz e-mail, ili kroz nedozvoljene upade u IT sistem.
Sajber okruženje predstavlja pojam koji se pojavljuje šezdestih godina prošlog veka za svojevrsno okruženje koje kreira čovek.
Iz navedenih primera izvodi se zaključak da što je tržište „koncentrisanije" u jednoj tački, dolazi do veće akumulacije i šteta je potencijalno veća.

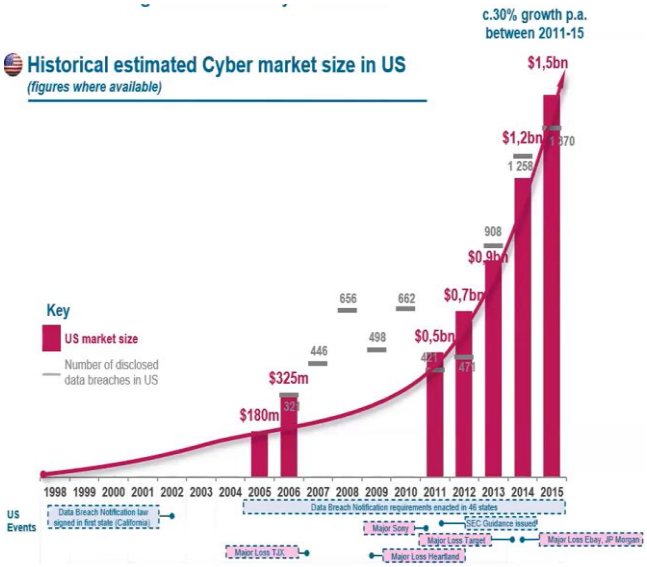


Slika 2. *SCOR; koncentracija tržišta*

IT tržište je veoma koncentrisano i nema puno diverzifikacije, već nasuprot izuzetno je centralizovano. Pored toga, postoji visok stepen standardizacije među tehnološkim rešenjima. Kao što se može videti na slici 2. kompanija Microsoft ima izuzetno visok procenat udela među svim operativnim sistemima. Takođe, samo 3 vodeća proizvođača prednjače na tržištu internet rutera i zauzimaju čak 75%. Ista situacija je takođe i kada su u pitanju IT usluge. Kompanija Google je ubedljivi lider na tržištu. Imajući u vidu visok nivou udela na tržištu pojedinih firmi, vrlo lako može doći do problema velikih razmera. Ako na sve to, dodamo još faktor međupovezanosti uređaja koji ubrzano raste, dolazimo do fenomena poznatog kao Cyber Cat. Ovaj naziv koristi se za sajber katastrofu razmera velike katastrofe usled prirodnih nepogoda.
Samo iskustvo ljudi koji se bave osiguranjem i procenom sajber rizika je veoma značajno. Sa trenutnim brzim promenama na tržištu, svaki tim ljudi koji se bavi sajber problematikom mora biti u stanju da precizno određuje pojmove i definiše svoju poslovnu strategiju. Moraju imati jasnu nameru u kom pravcu žele da oblikuju svoj portfolio. To obuhvata i uspostavljanje vodiča i pravila za maksimalni nivo samopridržaja po riziku osiguravača koji mora biti poznat svakom zaposlenom koji preuzima rizik. Kako nastaju novi proizvodi neprestano, javlja se i potreba za formiranjem upustava za preuzimanje rizika jer pokrića postaju sve preciznije određena. Neretko, potrebna je pomoć i sa strane osoba iz branši koje nisu nužno osiguranje, kao što su, IT stručnjaci, specijalni tehnički konsultanti itd., koji takođe učestvuju u formiranju upustava i pomažu svojom ekspertizom osiguravačima da bolje procene i na kraju donesu bolju odluku.
Kao nova vrsta osiguranja na tržištu, sajber osiguranje pruža mogućnost promene i same pozicije osiguravača i njegovog udela na tržištu. Takođe, daje mogućnost mlađim osiguravačima da se svojim znanjem i ekspertizom na vreme dobro pozicioniranju i nadmaše tradicionalno jake osiguravače. Kako bi se došlo do tog cilja potrebno je kontinuirano investiranje u znanje i ljudske resurse sa jedne strane kao i nove softvere za procenu i modelovanje rizika. Sam način na koji se budu modelovali rizici, proces ocenjivanja rizika i metod procene rizika uticaće dosta na samo poslovanje. Stoga i pored pomoći eksperata, potrebno je praviti redovne izveštaje i analize kako bi se obezbedilo da osiguravajuće društvo radi sve navedeno na dobar način ili bar bolje od konkurencije.

4.3. Tržište sajber osiguranja

Smatra se da je tržište sajber rizika brzorastuće i tržište koje se sve brže menja. Povećana digitalizacija i međuzavisnost direktno proporcionalno povećava nivo rizika i širi tržište. Još jedan motor razvoja je kontinuirano povećavanje zakonske regulative vezano za opšta pravila za zaštitu podataka. Kako manje razvijene zemlje prate druge zemlje koje prednjače u ovom pogledu, dolazi do teritorijalnog proširenja po svetu kao i do u unutrašnjeg proširenja po granama industrije. Što se tiče faktora koji utiču na stalno menjanje tržišta, možemo istaći konkurenciju na tržištu osiguranja koja oblikuje proces razvoja proizvoda u pravcu: proširenja obima pokrića, dodavanje i menjanje isključenja isl. Povećan obim regulative zahteva i veću ekspertizu i angažman menadžmenta u ovoj sferi, poboljšane veštine i opremu, radi adekvatnog odgovora na sajber rizike kao i preciznije definisanje osiguravajućeg proizvoda.
Da je jedan od vodećih faktora razvoja tržišta sajber osiguranja upravo zakonska regulativa, može se videti na grafikonu ispod. Striktnija legislativa, štetni događaji koji su izuzetno medijski propraćeni kao i povećana svest učesnika na tržištu, povečali su potražnju za sajber pokrićem u Americi.
Na slici 3. prikazan je pregled rasta premije sajber osiguranja u Americi koji pokazuje kako pojačane regulative zaštite podataka funkcionišu kao motor razvoja tržišta osiguranja.



Slika 3. *AonInpoint; pregled pojačane regulative kao motor razvoja*

5. ZAKLJUČAK

Na neki način, stvara se začarani krug, koji je pokrenut sve većim novcem koji se nalazi u IT sektoru, gde se generiše dodatni kapital kroz akumulaciju, dolazi do rasta tržišta osiguranja, stvaranja viška kapitala i stvaranje dodatnih fondova koji su opet izloženi sajber riziku. To dalje prouzrokuje novu zakonsku regulativu, koja je opet motor daljih inovacija što u pogledu borbe protiv sajber kriminala što u pogledu samog sajber kriminala.

Kako će se naša zemlja i naš region suočiti sa ovom novom pojavom na tržištu osiguranja, ostaje da se vidi. Pozitivna stvar je što postoje primeri država koje koliko toliko uspevaju da se nose sa svim sajber opasnostima 21. veka.

Svakako treba imati na umu da se budućnost osiguranja krije u ovoj sferi i da postoje određene smernice i navike koje će morati biti usvojene kako bi se adekvatno odgovorilo na nove izazove.

Kao što je u drugim delovima sveta, ova promena će morati da dođe i kod nas i nema sumnje da će uticati na sve učesnike na tržištu i subjekte u osiguranju.

Sami osiguranici u obliku velikih korporacija, moraće da nauče da bolje upravljaju rizikom, lakše ga identifikuju, primene preporuke regulatornih tela i podignu svest svojih saradnika.

Osiguravači će morati ili sami da se izvešte u modelovanju svoje izloženosti, ili da prepisuju šta rade inostrana društva, što neće biti garant za uspeh imajući u vidu velike razlike na tržištima. Moraće sami raditi na razvoju proizvoda sajber pokrića relevantnih za svoje lokalno tržište, kako bi na adekvatan način ispunili buduće potrebe osiguranika, što će neminovno uključiti stručne konsultante u ovoj oblasti.

Na regulatornim telima ostaje zadatak pomnog praćenja razvoja situacije i pružanje adekvatnog odgovora u obliku uspostave relevantne regulative, kako bi sve strane bile zadovoljne.

6. LITERATURA

1. Allianz Risk Barometer 2021: Covid-19 trio tops global business risks, AGCS, 2021.
2. Defense Advanced Research Projects Agency: Internet Protocol, Information Processing Techniques Office, Virginia, USA, 1981.
3. Department of the Treasury: Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Washington D.C. 2020.
4. Guy Carpenter: Silent Cyber – No Longer Silent?, 2020.
5. Institute and Faculty of Actuaries': Silent Cyber Assessment Framework, Research Project, 2019.
6. Marović B., Kuzmanović, B., Njegomir, V.: „Osnovi osiguranja i reosiguranja", Princip Press, Beograd, 2008.
7. Marović B., Njegomir V., Purić R.: „Reosiguranje", Precision, Čačak, 2012.
8. NetDiligence: Cyber Claims Study, Ransomware Spotlight Report, 2021.
9. Palo Alto Networks: Ransomware Threat Report, Unit 42, 2021.
10. Parsoire D., Heon S.: Cyber Risk Insurance: Challenges & Opportunities, SCOR Campus, SCOR, 2021.
11. World Economic Forum: The Global Risks Report 2021 16th Edition, 2021

Web izvori:

12. dlapiperdataprotection.com/
13. unctad.org/page/cybercrime-legislation-worldwide

Kratka biografija:

Dušan Saramandić, rođen je u Novom Sadu 1996. godine. Osnovne akademske studije završio je 2019. godine na Ekonomskom fakultetu u Subotici, odeljenju u Novom Sadu.. Master rad na Fakultetu Tehničkih nauka iz oblasti Upravljanje rizikom i menadžment u osiguranju odbranio je 2021. godine u Novom Sadu, a od 2020. godine radi u praksi reosiguranja u kompaniji Dunav Re

Dr Bogdan Kuzmanović je više od 20 godina radio u praksi osiguranja u kompaniji »DDOR Novi Sad« gde je bio i generalni direktor. Vodio je sektor osiguranja imovine, poljoprivrede, transporta i kredita i predstavljao kompaniju u poslovima vezanih za inostranstvo (Rusija, Ukrajina, Grčka, Rumunija, Turkmenistan, Austrija, Velika Britanija, Francuska, Nemačka, Nigerija..). Osnivač je Srpske asocijacije menadžera i član predsedništva Saveza ekonomista Vojvodine. Završio je ekonomski fakultet Univerziteta u Novom Sadu, doktorirao je na FTN. Od 2012. do novembra 2019. godine direktor je ekonomske funkcije Transnafta AD, a od 2019. je generalni direktor.