Pregled oblasti sajber osiguranja

Sajber osiguranje kao tehnika upravljanja rizikom

Jelena Sekulić, Imre Lendák
Departman za energetiku, elektroniku i telekomunikacije
Fakultet tehničkih nauka
Novi Sad, Srbija
jelena.sekulic@uns.ac.rs, lendak@uns.ac.rs

Apstrakt — **Sajber osiguranje je skupni termin za sve polise osiguranja koje adresiraju rizike u sajber prostoru i nude finansijsku pomoć u slučaju pojave tih rizika. Cilj ovog rada je da istakne značaj koji posedovanje ovakve polise ima u pogledu jačanja sajber otpornosti. To se postiže iznošenjem motiva za bavljenje temom sajber osiguranja, navođenjem benefita po društvo u celini, kao i pojašnjenjem samog termina i elemenata pokrića. U nastavku se navode faktori koji utiču na cenu same polise i objašnjava kako se radi smanjenja cene podiže nivo bezbednosti u preduzećima. Na kraju su navedeni izazovi sa kojima se susreće tržište sajber osiguranja, kao i potencijalni pravci daljeg razvoja. Kako bi se ovaj proizvod pojavio i razvijao u regionu, neophodna je saradnja stručnjaka za osiguranje i informacionu bezbednost, kao i svest o značaju proaktivnog pristupa sajber bezbednosti.**

Ključne reči - sajber bezbednost; upravljanje rizikom; transfer rizika; sajber osiguranje

I. UVOD

Tržište sajber osiguranja je i dalje relativno nerazvijeno, iako vodi poreklo još iz 1990-ih [1]. Ne postoji jedna zvanična definicija sajber osiguranja, kao ni jedan, standardni paket usluga. Dok se definicije razlikuju u manjoj meri, polise osiguranja mogu imati značajnijih razlika u pogledu toga šta pokrivaju, a šta ne. Istorijski, prve ponude sajber osiguranja nisu bile samostalni paketi, već su se nudile kao dodaci na već postojeće polise. To su uglavnom bile polise razvijene za firme koje su se bavile tehnologijom, medijima masovne komunikacije ili telekomunikacijom, ili su pak pružale neke profesionalne usluge, te su svakako rukovale podacima o ličnosti svojih korisnika. Polise koje osiguravaju od odgovornosti usled grešaka, propusta, loše pružene usluge ili potpunog izostanka iste, spadaju pod osiguranje od profesionalne odgovornosti i ne mogu pokriti odgovornost za loše implementirane mere bezbednosti informacionog sistema, niti troškove forenzičke istrage. Tako se vremenom pojavila potreba za posebnom vrstom osiguranja - tzv. sajber osiguranjem, zvanim još i osiguranjem od sajber rizika ili od sajber/IT odgovornosti. Po poslednjim procenama, vrednost tržišta sajber osiguranja je 2021. godine iznosila 10.3 milijarde američkih dolara, 2022. godine 12.8 milijardi, dok se za 2029. godinu predviđa iznos od 63.6 milijardi. Prosečna godišnja stopa rasta je 2020. iznosila 22.4% [2]. Činjenica je da povećanjem obima i cene rizika, kao i sve strožim zakonima koji regulišu sajber prostor, ovaj tip osiguranja stiče sve veću popularnost.

A. *Cena narušene bezbednosti podataka*

Ako rizik definišemo kao mogućnost da dođe do neke štete, onda je incident pojava tog rizika, odnosno realizovani rizik. Svaki incident ima svoj uticaj, koji se meri kroz ozbiljnost posledica iskorišćavanja ranjivosti sistema, a izražava najčešće kroz finansijske gubitke. Tako se za svaki poznati sajber incident navodi i trošak koji je prouzrokovao.

Neki od najskupljih incidenata vezuju se za kompanije *Uber*, *Target*, *Sony PlayStation* i *Epsilon*. U novembru 2016. godine, hakerskim napadom na *Uber* procureli su podaci 57 miliona vozača i klijenata. Nakon prvobitnog protivzakonitog pokušaja zataškavanja, kompanija je dve godine kasnije postigla sporazum sa državnim tužiocima i platila 148 miliona američkih dolara. Čitači kreditnih kartica u lancu prodavnica *Target* kompromitovani su 2013. godine, što je rezultovalo ukradenim podacima sa 110 miliona kartica. *Target* je snosio troškove ponovnog izdavanja kartica, što je uz prateće sudske troškove i pad prodaje usled izgubljenog poverenja koštalo kompaniju 290 miliona američkih dolara. Osiguranje je pokrilo 90 miliona, ali očekuje se još dodatnih troškova suđenja. Sto miliona zapisa korisničkih podataka ukradeno je sa *Sony*-jevog veb servisa, 2011. godine. Kompanija je izgubila 172 miliona američkih dolara i značajno joj je narušena reputacija. Tri godine kasnije, sa *Sony*-jevih servera ukradeno je sto terabajta podataka, za čiji je oporavak kompanija izdvojila novih sto miliona američkih dolara. *Epsilon* je prvi na listi, sa cifrom od čak četiri milijarde američkih dolara. *Epsilon* je kompanija koja pruža usluge marketinga putem elektronske pošte, te skladišti veliki broj imena i adresa elektronske pošte, od kojih je 60 miliona ukradeno u napadu 2011. godine. U pitanju su podaci korisnika veb servisa čak sedamdeset pet kompanija kojima je *Epsilon* pružao marketinške usluge. Sve troškove obaveštavanja korisnika, sudskih sporova i prekida u poslovanju u ime oštećenih kompanija snosio je *Epsilon* [3].

Najnoviji podaci za period od marta 2021. do marta 2022. godine, izneti u IBM-ovom izveštaju, koji je nastao kroz saradnju sa *Ponemon* institutom [4], govore da je prosečna cena curenja podataka porasla na 4.35 miliona američkih dolara, dostignuvši time novi maksimum. Ukupna cena se dobija kao zbir četiri faktora - izgubljeni prihod usled prekida poslovanja, cena detekcije, cena obaveštavanja i trošak koji nastaje posle napada. Cena detekcije, u koju spadaju forenzičke istrage, pregled sistema, procene, krizni menadžment, kao i komunikacija sa izvršnim i ostalim odborima, ove godine je imala najveći udeo u ukupnoj ceni, zamenivši cenu prekida poslovanja, koja je prethodnih šest godina bila na prvom mestu. U okviru ovog istraživanja, meren je i uticaj čak 28 faktora na povećanje/smanjenje ukupne cene incidenta. Među faktorima koji smanjuju cenu, pored upotrebe veštačke inteligencije, postojanja tima za reagovanje na incident (engl. *Incident Response* - IR) i drugih tehničkih i organizacijskih mera, našlo se i osiguranje.

B. Pravne regulative

Od prvog akta koji je donesen usled povećane upotrebe računara, Akta o privatnosti (engl. *Privacy Act*) donesenog u Sjedinjenim Američkim Državama, 1974. godine, pa do drugog dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu (engl. *Convention on Cybercrime*) potpisanog u maju 2022. godine, države širom sveta su radile na regulaciji IT sfere na nacionalnom, kao i internacionalnom nivou.

Jedan od najvažnijih evropskih zakona je Opšta uredba o zaštiti podataka o ličnosti (engl. *General Data Protection Regulation*). Iako je kreiran od strane Evropske unije, odnosi se na sve organizacije širom sveta koje barataju podacima stanovnika Unije. Ova uredba je zasnovana na Direktivi o zaštiti podataka iz 1995. godine, sastavljana je u periodu 2011-2016. godine, a 25. maja 2018. godine je stupila na snagu. Kazne za kršenje dostižu 20 miliona eura ili 4% godišnjih prihoda, šta god je veće [5]. Podaci o ličnosti su, po definiciji, sve informacije koje su u vezi sa individuom, koje je mogu direktno ili indirektno identifikovati. Od očiglednih primera, kao što su lična imena i adrese elektronske pošte, preko lokacijskih informacija, informacija o polu, nacionalnosti, religijskim i političkim opredeljenjima, pa do čisto tehničkih podataka kao što su kolačići veb pregledača, sve se smatra podacima o ličnosti [5]. Iz ovoga se da zaključiti da svaka kompanija koja je prisutna na internetu i ima bilo kakav vid interakcije sa korisnicima, zapravo čuva podatke o ličnosti i za njih odgovara po ovoj uredbi. Za četiri godine primene ove regulative, izdato je preko 900 kazni. Najskupljih pet iznosi 746 miliona eura, 225 miliona eura, 90 miliona eura i na četvrtom i petom mestu 60 miliona eura. Odgovorne kompanije su redom *Amazon*, *WhatsApp*, *Google*, *Facebook* i na petom mestu ponovo *Google*, koje su u sklopu propisanih kazni morale da donesu ozbiljne izmene u svojim politikama privatnosti i poslužile su kao dobar primer za druga preduzeća [6].

U Srbiji je rukovanje podacima o ličnosti regulisano Zakonom o zaštiti podataka o ličnosti. Međutim, zakon koji direktno adresira bezbednosne rizike u informaciono-komunikacionim (IKT) sistemima jeste Zakon o informacionoj bezbednosti, donesen 2016. godine, sa poslednjom dopunom iz 2019. godine. Ovim zakonom se uređuju mere zaštite od bezbednosnih rizika u IKT sistemima, odgovornosti pravnih lica prilikom upravljanja i korišćenja IKT sistema i određuju se nadležni organi za sprovođenje mera zaštite, koordinaciju između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite. Takođe, definisano je i značenje pojmova kao što su informaciona bezbednost, incident, rizik, upravljanje rizikom itd.

C. Motivacija za mala i srednja preduzeća

Na prvi pogled može delovati da samo velika preduzeća imaju koristi od sajber osiguranja, jer su ona češće mete, usled veće potencijalne finansijske dobiti. Međutim, velika preduzeća imaju i više sredstava na raspolaganju za ulaganje u tehničke mere bezbednosti, ali i tim stručnjaka, kao i edukaciju zaposlenih. S druge strane, mala i srednja preduzeća, iako ne privlače napadače toliko velikim profitom, mogu biti laka meta, jer često nemaju dovoljan nivo zaštite, kao ni svest zaposlenih na odgovarajućem nivou. A kada se uzme u obzir i činjenica da mala i srednja preduzeća čine 99% evropskih i domaćih preduzeća [7, 8], jasno je da će većina njih pre ili kasnije doživeti neki sajber incident, ukoliko već nisu.

Dok u svetu sajber osiguranje polako postaje normala, preduzeća u R. Srbiji su još neodlučna. Kod dela zainteresovanih kompanija postoji stav da ne žele da otkrivaju detalje o svom poslovanju ili sigurnosnim procedurama koje imaju, ili stav da je uz sve mere zaštite sajber osiguranje nepotrebno. Ti stavovi će se neminovno menjati, jer će preduzeća usled saradnje sa inostranim partnerima bivati uslovljena posedovanjem polise sajber osiguranja, te će taj porast potražnje dovesti i do rasta ponude i promena na tržištu. Pre nego do toga dođe, bilo bi dobro razumeti prednosti posedovanja ove polise, koje su svakako šire od mogućnosti poslovanja sa inostranstvom.

Analizom stepena rizika i cene sajber incidenta, može se uvideti prvi benefit sajber osiguranja, a to je pokrivanje dela troškova. Pored finansijske podrške, osiguraniku može biti dostupna pomoć u odnosima sa javnošću, tim tehničkih stručnjaka za analizu i savetovanje, kao i tim pravnih savetnika. Ovi elementi čine drugi sloj benefita, te se uopšteno može reći da osiguranje pomaže u fazi oporavka od sajber napada.

Međutim, postoji i treći sloj, o kom govore autori Pregleda sajber osiguranja [1]. Navode četiri prednosti sajber osiguranja, među kojima je pre svega mogućnost da se organizacije podstaknu da ulažu više u svoju zaštitu, u cilju smanjivanja premije. Finansijski motiv bi doveo do toga da se sa reaktivnog pristupa bezbednosti pređe na proaktivni, a da se na osiguranje gleda kao na poslednju liniju odbrane, a ne prvu, niti najvažniju i svakako ne jedinu. Dalje, poboljšanjem sveukupnog nivoa sajber bezbednosti, veruje se da se postiže i viši nivo društvene dobrobiti. Treće, sajber osiguranje može služiti kao indikator kvaliteta zaštite

neke kompanije. I poslednje, može dovesti do novih i naprednijih standarda u sajber bezbednosti, jer bi posedovanje sertifikata ili ispunjavanje nekog standarda bio najjednostavniji način da osiguravači procene nivo rizika kom je osiguranik izložen. Primer dobre prakse se može naći u Ujedinjenom Kraljevstvu, gde je vlada donela standard pod nazivom engl. *Cyber Essentials* [9]. Ovaj standard definiše bazične bezbednosne mere, kako bi svako preduzeće imalo minimum zaštite i napravilo prvi korak ka sajber otpornosti. Takođe, moguće je sertifikovati se po ovom standardu, što osiguravačima (ali i klijentima, investitorima i ostalim zainteresovanim stranama) može dati jasniju sliku o nivou sajber bezbednosti kompanije koju procenjuju.

II. PREGLED STANJA U OBLASTI

A. *Definicija i elementi pokrića*

Američka osiguravajuća kuća *Embroker* definiše sajber osiguranje kao finansijski proizvod koji omogućava preduzećima da prenesu troškove oporavka nastalih usled narušavanja sajber bezbednosti [10]. Britanska kompanija, *Hiscox*, navodi da sajber osiguranje pomaže u zaštiti preduzeća protiv različitih digitalnih rizika, pružajući finansijsku podršku usled sajber napada [11].

Posrednik u osiguranju, Osiguranik, smatra da je sajber osiguranje bitan aspekt u održanju stabilnosti poslovanja, koje može biti ugroženo usled sajber napada i drugih hakerskih pretnji. Naglašavaju da sajber osiguranje ne može i neće sprečiti sajber napad, ali može da pomogne u minimiziranju posledica i pokrivanju finansijskih troškova. Od elemenata pokrića navode troškove narušavanja bezbednosti, uključujući i povrate podataka, sistemsku forenziku, kao i troškove pravne odbrane i pravljenje naknada za kupce [12].

U radu koji je nastao kao posledica analize preko stotine polisa sajber osiguranja na američkom tržištu, daje se sledeća definicija: "Sajber osiguranje je skupni pojam za sve polise osiguranja koje se bave direktnim gubicima, kao i gubicama treće strane, koji su posledica računarski baziranog napada ili ispada kompanijskog informacionog sistema" [13].

Ista analiza pokazala je mnogo veću konzistentnost među polisama nego što bi se očekivalo. U prvih pet polisa su identifikovani zajednički faktori koji su uključeni u pokriće. Primeri ovih faktora koji su svrstani u direktne troškove su:

- troškovi istrage uzroka incidenta,
- troškovi ponovnog uspostavljanja poslovnih usluga,
- troškovi obaveštavanja oštećenih strana,
- usluge kreditnog monitoringa,
- troškovi usluga odnosa sa javnošću i medijima,
- plaćanje iznuda i otkupa i
- gubici vezani za prekid poslovanja.

U indirektne troškove spadaju troškovi sudskih postupaka, kao i sve kazne određene u tim postupcima. Kao uzroke sporova navode pozivanje na odgovornost usled:

- kompromitovanja podataka o ličnosti,
- kompromitovanja poslovnih informacija,
- nenamerne propagacije zlonamernog softvera,
- nedostupnosti sistema autorizovanim korisnicima, i
- narušavanja privatnosti, klevete i prekršaja autorskih prava.

Najčešća isključenja su ona koja nisu u direktnoj vezi sa sajber prostorom, već se odnose na krivična dela, greške i propuste, namerno kršenje zakona, autorskih prava i otkrivanje poslovnih tajni ili poverljivih informacija, zatim na krivične istrage koje su već u toku, kao i fizičke povrede, neke aspekte odgovornosti i gubitke vezane za sisteme koji su van kontrole osiguranika. Posledice nastale usled terorizma, rata ili vojnih akcija su takođe uglavnom isključene iz pokrića [13].

B. *Procena rizika i određivanje cene*

Prilikom kupovine sajber osiguranja, kompanija biva temeljno analizirana po pitanju izloženosti sajber rizicima. Ukoliko su bezbednosne mere na niskom nivou, osiguravač može odbiti da pruži usluge osiguranja ili ih pak prodati po znatno višoj ceni. U cilju obezbeđenja povoljne polise sajber osiguranja, važno je da kompanija ima implementirane osnovne bezbednosne kontrole, među koje spadaju: višefaktorska autentifikacija, detekcija pretnji na krajnjim tačkama sistema i reagovanje na iste, bezbedno uskladištene rezervne kopije podataka (tj. bekap), upravljanje pristupom zasnovano na privilegijama, filtriranje mejlova, postojanje i testiranje plana za reagovanje na incident, redovni treninzi i testiranja zaposlenih u pogledu svesti o sajber bezbednosti, nadgledanje sistema i beleženje svih relevantnih aktivnosti i konačno, kontrola partnera i trećih strana, kako bi se minimizovala mogućnost pojave i propagacije incidenta preko njihovih sistema [14].

Osim količine implementiranih bezbednosnih mera, na cenu sajber osiguranja utiču i drugi faktori na koje kompanija može da utiče u manjoj meri. Pre svega, u obzir se uzimaju veličina kompanije i industrija kojoj pripada. Porastom broja zaposlenih raste i potencijal za uspešne napade socijalnim inženjeringom, kao i opasnost od ljudske greške - u vidu korišćenja zastarelih softvera, slabih lozinki, nepoštovanja procedura za korišćenje interneta i rukovanje opremom kompanije itd. Industrija igra još važniju ulogu. Lokalni biznis sa ograničenom bazom potrošača, kao niskorizično preduzeće, plaćaće manju premiju. Već će lanac maloprodajnih radnji biti okarakterisan kao srednjerizično preduzeće, usled čuvanja podataka o kreditnim karticama, koje možda dodatno prikupljaju i preko neke internet prodavnice. Visokorizične će biti kompanije iz npr. zdravstvenog sektora, jer se medicinski podaci smatraju posebno osetljivim podacima o ličnosti. Što

je veći godišnji prihod, biće skuplja i polisa sajber osiguranja, jer se kompanije sa velikim prihodima smatraju pogodnim za ucenjivanje i iznude. Konačno, cena se koriguje spram odabranog limita pokrića i iznosa franšize, tj. sume koju osiguranik sam plaća u slučaju incidenta [14].

Da bi se rizici mogli kvantifikovati, te odrediti visina premije za svako preduzeće, potrebno je te rizike prvo identifikovati i analizirati. Ključna tehnika koja se koristi za identifikaciju i analizu rizika kompanije, pre pisanja ugovora o osiguranju jeste upitnik koji kompanija popunjava, kao i sastanci predstavnika kompanije i osiguravača. Ukoliko se postave prava pitanja sa jedne strane i iskreno se odgovori na njih sa druge, dobiće se realna slika stanja u kompaniji, te će ono moći i da se popravi. Kroz nekoliko takvih iteracija, kompanija postaje bezbednija i još se dodatno štiti kupovinom sajber osiguranja.

Iako upitnici predstavljaju najbolji način da se prikupljeni podaci organizuju i analiziraju, u tehnike procene rizika spada i analiza poslovne dokumentacije, provere usaglašenosti sa standardima i eventualnih sertifikacija, kao i korišćenje postojeće baze znanja i istorijskih podataka. [1]

C. Izazovi i dalji razvoj

Specifičnosti sajber osiguranja mogu da se posmatraju i po koracima procesa, od identifikacije rizika do potpisivanja ugovora, a opciono i rešavanja primljenih obaveštenja o šteti [1]. U nastavku se navode ti koraci, kao i izazovi koji se javljaju u svakom:

- Identifikacija rizika. S obzirom na to da je sajber osiguranje novi tip osiguranja, osiguravači nemaju dovoljno iskustva i još nemaju razvijene standardizovane procedure. Takođe, računarski sistemi brzo evoluiraju, pojavljuju se nove tehnologije, a menja se i sistem unutar kompanije.
- Određivanje verovatnoće. Postoji niz prepreka koje osiguravačima stoje na putu procene rizika kompanije: zaposleni ne žele da otkrivaju primenjene metode, kao ni da pristanu na prinudno uvođenje novih mera; instalirani bezbednosni softveri nisu efikasni ako se neispravno konfigurišu i održavaju; bezbednost je proces, te se ne može fiksno odrediti i očekivati da ostane nepromenljiva. Sledeća prepreka se ogleda u evoluciji napada. Napadači stalno menjaju tehnike i brzo se prilagođavaju, što ih čini veoma nepredvidivima. Takođe, teško je odrediti stvarni doprinos mera i standarda nivou bezbednosti kompanije. Dodatno otežava i činjenica da su sistemi međuzavisni u pogledu bezbednosti, kao i da postoje barijere u deljenju informacija o napadima.
- Određivanje uticaja. Teško je kvantifikovati ukupnu štetu koju nanese sajber napad, zbog toga što se nematerijalne štete poput narušenog ugleda ili oštećenja i gubitka osetljivih podataka teško procenjuju.
- Procena rizika. Praktično je skoro nemoguće verifikovati donetu procenu rizika.
- Određivanje pokrića. Teško je precizirati pokriće, i dalje postoji veliki broj izuzetaka od pokrića i limit nadoknade može biti nizak za velike kompanije.
- Proračun premije. Usled nedostatka reosiguranja u ovoj oblasti, sličnosti među sistemima širom sveta i činjenice da su napadi lako i jeftino izvodljivi, pojava povezanih rizika predstavlja posebnu opasnost u sferi sajber osiguranja. Npr. usled masovnog širenja nekog zlonamernog softvera, ili distribuiranog napada uskraćivanjem usluga, može se desiti da jednom osiguravaču u kratkom periodu veliki broj klijenata traži odštetu. Uzevši to u obzir, izuzetno je teško odrediti cenu polise.
- Sastavljanje i potpisivanje ugovora. Jezik za pisanje ugovora je još neprecizan, kompanije misle da postoje preklapanja sa postojećim polisama i utvrđivanje odgovornosti često nije jednostavno - mogu biti odgovorni vlasnici sistema, proizvođači softvera ili pružaoci internet i drugih usluga.
- Rešavanje prijave o šteti. Postoji šansa da se napad ne detektuje pravovremeno ili uopšte, ili pak da on traje dugo, pa i mesecima. U ovom slučaju treba utvrditi kako osiguravači nadoknađuju štetu. Uz to, da bi se šteta prijavila, uglavnom je potrebno sprovesti forenzičku istragu, što je dodatni trošak oštećenoj strani, a i narušava reputaciju, jer incident često više ne ostaje u tajnosti.

Uz dalji razvoj polisa, nazire se i razvoj u pogledu načina pružanja usluge osiguranja. Na ovo ukazuje partnerstvo koje su sklopile kompanije *Allianz*, *Apple* i *Cisco*, u svrhu pružanja boljih paketa sajber osiguranja od strane kompanije *Allianz*, ukoliko osiguranici koriste *Apple* i *Cisco* proizvode. Procene su da će se u budućnosti sajber osiguranje prodavati kao proizvod za sajber bezbednost, direktno nadležnima za tu oblast u kompanijama [15].

III. ZAKLJUČAK

Pod terminom sajber osiguranje smatra se osiguranje od sajber rizika, ali i od sajber odgovornosti. To znači da bi osiguravači trebalo da pokrivaju i direktne i indirektne gubitke, ili da pružaju mogućnost prilagođavanja polise potrebama preduzeća. Direktno ili pokriće prve strane (engl. *first-party coverage*) bi štitilo samu kompaniju u slučaju sajber incidenta. Osmišljeno je tako da pokriva troškove prekida poslovanja, povrata izgubljenih podataka, ponovnog uspostavljanja poslovnih procesa, obaveštavanja korisnika, odnosa sa javnošću i forenzičke istrage. Indirektno pokriće se odnosi na rizike vezane uz poslovanje sa trećim licima (engl. *third-party coverage*). Ukoliko se sajber napadom na osiguranu kompaniju otkriju podaci o ličnosti, poslovne tajne ili druge poverljive informacije drugih lica, te ta lica podignu tužbe, osiguranje će pokriti sudske troškove, kao i sve kazne propisane zakonom, do limita određenog ugovorom.

Usled sve češćih i ozbiljnijih sajber napada, rizici su postali preveliki da bi se jedno preduzeće samo nosilo sa njima. Uz razvoj zakonodavstva koji je doneo milionske kazne za kompanije koje ne uspeju da sačuvaju tuđe podatke kojima rukuju, postalo je neophodno prebaciti deo rizika osiguravaču i obezbediti finansijsku podršku. Osim toga, proces kupovine sajber osiguranja bi trebalo da od kompanije zahteva implementaciju osnovnih bezbednosnih kontrola, kako bi rizik koji osiguravač preuzima bio prihvatljiv.

U ovom procesu bi obema stranama trebalo da pomažu IT stručnjaci, a naročito stručnjaci za sajber bezbednost. S jedne strane, oni vode digitalnu transformaciju, kroz koju još uvek prolazi veliki broj preduzeća u regionu, te bi u tom procesu bezbednost trebalo da bude prioritet. To bi svakako podrazumevalo implementaciju tehničkih (višefaktorska autentifikacija, kontrola pristupa, pravljenje bekapa, zapisi ključnih aktivnosti, detekcija i reagovanje na pretnje itd) i organizacionih (procedure za rukovanje eksternim uređajima, korišćenje interneta i rad na daljinu, plan za reagovanje na incident itd) mera, kao i podizanje svesti zaposlenih o sajber bezbednosti, ali i podizanje svesti o značaju sajber osiguranja, kao poslednje linije odbrane.

Trenutni doprinos autora ogleda se u razvoju veb aplikacije putem koje bi se vršila procena nivoa rizika privatnih lica, te i okvirni proračun visine premije sajber osiguranja. Aplikacija bi bila besplatno dostupna svim zainteresovanim kompanijama, te bi kao prvi takav proizvod na domaćem tržištu trebalo da podstakne interesovanje za kupovinu sajber osiguranja. Dalji rad će se fokusirati na simulacije čestih sajber napada, radi preciznije ocene uticaja koji imaju po sistem kompanije. Ako bi kompanije imale konkretne informacije o tome koliko bi im dana sistem bio van funkcije, odnosno poslovanje stopirano, kao i kolike bi finansijske troškove zahtevao oporavak od sajber incidenta, pretpostavlja se da bi motivacija za ulaganje u bezbednosne mere, među kojima se nalazi i sajber osiguranje, značajno porasla. Ukoliko bi se kompanijama savetovalo da potraže paket osiguranja od sajber rizika, domaće tržište bi moralo da odgovori na tu potražnju i poveća ponudu. Kako bi ponuda od strane osiguravajućih društava bila konkurentna, oni bi takođe trebalo da sarađuju sa stručnjacima za sajber bezbednost. Paketi osiguranja koji uz pokriće nude i inicijalnu procenu ranjivosti sistema, savetnike za proces implementacije bezbednosnih mera, predavače koji bi obučavali zaposlene u osiguranoj kompaniji, kao i tim koji bi vršio redovnu kontrolu sistema i ukoliko do incidenta ipak dođe, reagovao i sproveo forenzičku istragu bili bi daleko popularniji.

Iako je osiguranje oblast ekonomije, ipak "sajber" u sajber osiguranje smešta ovu temu u interdisciplinarne, te zahteva i angažovanje stručnjaka za sajber bezbednost. Dok stručnjaci za osiguranje mogu ovom novom tipu osiguranja doprineti svojim iskustvom i metodologijama razvijenim u drugim oblastima osiguranja, stručnjaci za informacionu bezbednost mogu doprineti u "sajber" delu. Ukoliko bi se oni postavili kao spona između kompanija i osiguravajućih društava, saradnjom sa obe strane bi doprineli opštem podizanju nivoa bezbednosti, kako u poslovnom sektoru, tako i na privatnom planu, jer bi edukacija zaposlenih trebalo da ima za cilj stvaranje kulture sajber bezbednosti, što bi podrazumevalo primenu svega naučenog na svakodnevnom nivou.

IV. ZAHVALNICA

Rad je podržan od strane Pokrajinskog sekretarijata za obrazovanje i naučnoistraživačku delatnost Autonomne pokrajine Vojvodine (Republika Srbija) kroz projekat „Osiguranje protiv incidenata u sajber prostoru (OPISP)", broj: 142-451-2369/2022-01/01. Rad je podržan od strane Ministarstva prosvete, nauke i tehnološkog razvoja kroz projekat „Razvoj i primena savremenih metoda u nastavi i istraživačkim aktivnostima", broj: 451-03-68/2022-14/200156.

V. REFERENCE

[1] A. Marotta, F. Martinelli, S. Nanni, A. Orlando and A. Yautsiukhin, "Cyber-insurance survey", Computer Science Review, Maj, 2017.

[2] https://www.fortunebusinessinsights.com/cyber-insurance-market-106287 (pristupljeno u januaru 2023.)

[3] https://www.firmex.com/resources/blog/the-10-most-expensive-data-breaches-in-corporate-history/ (pristupljeno u januaru 2023.)

[4] Cost of a Data Breach Report 2022, IBM Security, Jul, 2022.

[5] https://gdpr.eu/what-is-gdpr/ (pristupljeno u januaru 2023.)

[6] https://www.tessian.com/blog/biggest-gdpr-fines-2020/ (pristupljeno u januaru 2023.)

[7] https://single-market-economy.ec.europa.eu/smes/sme-definition_en#modal (pristupljeno u januaru 2023.)

[8] https://www.privreda.gov.rs/lat/ministarstvo/organizaciona-struktura/sektor-za-razvoj-malih-i-srednjih-preduzeca-i-preduzetnistva (pristupljeno u januaru 2023.)

[9] https://www.ncsc.gov.uk/cyberessentials/overview (pristupljeno u januaru 2023.)

[10] https://www.embroker.com/coverage/cyber-insurance/ (pristupljeno u januaru 2023.)

[11] https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance (pristupljeno u januaru 2023.)

[12] https://www.osiguranik.com/blog/sta-je-sajber-osiguranje-sta-treba-da-znate-o-sve-popularnijoj-temi-u-sektoru-osiguranja/ (pristupljeno u januaru 2023.)

[13] S. Romanosky, L. Ablon, A. Kuehn and T. Jones, "Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?", SSRN Electronic Journal, Mart, 2017.

[14] https://www.embroker.com/blog/cyber-insurance-cost/ (pristupljeno u januaru 2023.)

[15] https://www.techtarget.com/searchsecurity/news/252434612/Cybersecurity-insurance-breaks-coming-for-Apple-Cisco-customers (pristupljeno u januaru 2023.)