Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-71-76

OSIGURANJE INTERNET RIZIKA

Jasna Pak
Univerzitet Singidunum, Beograd

Abstract:
Razvoj informacione tehnologije doveo je do potrebe razvoja adekvatne osiguravajuće zaštite kako bi se odgovorilo novonastalim rizicima iz upotrebe interneta. U tradicionalne polise osiguranja unose se nove klauzule o proširenju pokrića na štete koje su posledica oštećenja ili uništenja računara ali osiguravači nude i posebne polise koje se odnose samo na internet rizike. Oni nastoje da pokriće iz osiguranja prilagode potrebama svakog osiguranika ali je često teško zadovoljiti te potrebe i proceniti rizik zbog stalnog razvoja informatičke tehnologije i njene složenosti. Još uvek se traže adekvatna rešenja koja bi bila u skladu sa propisima u oblasti osiguranja i propisima o sigurnosti informatičkih sistema i ličnih podataka. U članku se ukazuje na probleme sa kojima se suočavaju osiguravači i mogućim rešenjima na tržištu osiguranja u Srbiji u cilju razvoja novog proizvoda koji bi bio u najboljem interesu onih koji su nesumnjivo izloženi internet rizicima.

Key words:
polisa osiguranja,
osigurani rizik,
zaštita ličnih podataka,
građanska odgovornost,
hakerski napadi,
prekid rada.

UVOD

Poverenje u internet i njegovu efikasnost imperativ je zdravog poslovanja, očuvanja državnih, privrednih i širih društvenih interesa i normalnog života pojedinaca i porodice. Povrede pohranjenih ličnih i drugih podataka i poslovnih informacija koje su dostupne preko interneta mogu dovesti do ogromnih imovinskih šteta. Širom sveta su svakodnevni kriminalni napadi na informatičke sisteme kao što su krađa podataka, iznuda, prevare ili privredna špijunaža. Veliki broj preduzeća su žrtve čestih hakerskih napada. U novije vreme prodavci i kupci preko interneta zbog slučajeva prevara trpe milionske štete o čemu mediji stalno izveštavaju.[1] U ugrožene od rizika vezanih za internet spadaju ne samo velike kompanije, javne i državne ustanove već i mala i srednja preduzeća i pojedinci koji često nisu u stanju da procene kakvom su riziku izloženi.

Da bi se učvrstilo poverenje u poslovanje zasnovano na informacionim tehnologijama države donose propise o zaštiti ličnih podataka. Konvencija Saveta Evrope zahteva od država članica da prihvate pravne standarde o zaštiti podataka o ličnosti što je učinila i Srbija koja je potpisala i ratifikovala ovu Konvenciju.[2]

U Evropskoj uniji je još 1995. godine doneta Direktiva o zaštiti fizičkih lica u vezi obrade ličnih podataka kao i njihovom slobodnom protoku.[3] Međutim, smatra se da je za sigurnost jedinstvenog informacionog tržišta potrebna veća zaštita od one koju predviđa Direktiva. Evropska komisija radi na daljem usaglašavanju propisa država članica o zaštiti podataka što će imati značajan uticaj na osiguravače i potrošače.[4] U izradi propisa učestvuju i predstavnici osiguravača i njihovih profesionalnih udruženja koji imaju podatke o osiguranim štetnim događajima za koje su isplaćene velike naknade iz osiguranja. Evropsko udruženje osiguravača smatra, međutim, da bi predlog uredbe o zaštiti podataka koji je izradila Komisija ograničio mogućnost osiguravača da obrađuju i koriste podatke od značaja za procenu rizika a time i utvrđivanje adekvatne premije.[5]

U većem broju zemalja doneti su i propisi o merama tehničke sigurnosti podataka, njihovoj stalnoj kontroli i unapređenju. Posebna državna tela sprovode nadzor nad primenom ovih propisa. Osnivaju se organizacije od javnog značaja čiji je zadatak da sprovode nadzor nad zaštitom informacionih tehnologija koje izdaju periodična obaveštenja i preporuke da bi se rizik upada u baze podataka sprečio.[6] Međunarodnim standardom se utvrđuje

1 Videti više u: M.E. Meinl, Eletronic Complaints: An Empirical Study on British English and German Complaints on eBay, disertacija (Rheinischen Fridrich-Wilhelms-Universität Bonn, 2010 /hss.ulb.uni-bonn.de/2010/2122/2122.htm/.

2 Pravo na zaštitu podataka je osnovno ustavom zagarantovano ljudsko pravo zasnovano na čl. 24 Povelje Saveta Evrope o ljudskim i manjinskim pravima i Konvenciji o zaštiti lica u odnosu na automatsku obradu podataka. U Srbiji je ovo pravo predviđeno u čl. 42. Ustava (Sl. Glasnik R. Srbije 98/2006) na osnovu koga je donet Zakon o zaštiti podataka o ličnosti (Sl. Glasnik R. Srbije 97/2008).

3 Direktiva 95/46/EZ od oktobra 1995, OJ L 281/95, 23.11.1995.

4 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) / COM/2012/011 final - 2012/0011 (COD) /

5 Insurance Europe key messages on the European Commission's proposed General Data Protection Regulation, SMC-DAT-12-064, 3.09.2012.

6 Namačko udruženje osiguravača je dalo veliki doprinos izradi propisa o tehničkoj zaštiti informacionih sistema. Videti u: „Stellungname des Gesamtverbandes der Deutschen Versicherungswirtschaft

kako preduzeča i drugi subjekti mogu da zaštite svoje internet mreže i baze podataka.[7] Uputstva se stalno dopunjuju i usavršavaju.

Obaveza primene adekvatne tehničke zaštite uticala je na shvatanje da je zaštita od internet rizika putem osiguranja samo nepotreban trošak. Naročito oni koji ne prodaju svoje proizvode i usluge preko interneta ne smatraju osiguranje naročito korisnim. Međutim, ne može se osporiti činjenica da internet rizici ne mogu da se izbegnu ni kod onih koji primenjuju najsavremenije mere zaštite zbog čega se shvatanje o potrebi osiguranja menja. Sve više se prihvata da ono ima ključnu ulogu u zaštiti od finansijskih gubitaka. Opasnost da nastane velika šteta koja čak može da ugrozi dalji opstanak privrednog subjekta govori u prilog zaključka da će uskoro izdatak za premiju biti normalan poslovni trošak. Kada nastane šteta postavlja se složeno pitanje kako je naknaditi, ko je odgovoran i za šta. Broj dela je svake godine sve veći kao i broj sudskih sporova tako da je potreba za osiguranjem od finansijskih gubitaka koji su posledica njihove povrede sve izraženija. Koliko je u XX veku bila značajna uloga osiguravača u zaštiti od industrijskih rizika toliko je danas ta uloga značajna za korisnike informacione tehnologije. Nije dovoljno samo investiranje u sigurnosne sisteme već je i osiguranje put da se izađe na kraj sa posledicama novih rizika.[8] Prenos rizika na osiguranje sve više postaje sastavni deo posla upravljanja rizicima. Propisi direktno utiču na povećanje interesovanja za osiguranjem i razvoja portfelja osiguravača.[9]

POSEBNE POLISE ZA OSIGURANJE INTERNET RIZIKA

Internet rizici su izričito isključeni ili ograničeno pokriveni nekim tradicionalnim osiguranjima (požara, građanske odgovornosti iz delatnosti, krađe, loma mašina, transportnih rizika).[10] Kod osiguranja stvari ako je računar predmet osiguranja uključeni su fiksno instalirani nosači podataka i programi koji su navedeni u ponudi osiguranja. Novčane štete usled gubitka podataka, prekida rada ili gubitka zarade mogu biti osigurane ako se to posebno ugovori Međutim, da bi ove štete usled bile pokrivene osiguranjem moraju biti posledica oštećenja ili uništenja hardvera. Na savremenom tržištu osiguranja postoje različite internet polise koje pokrivaju štete prouzrokovane nestankom, oštećenjem ili manipilacijom podataka i kada hardver nije oštećen. Mogućnost proširenja pokrića na novčane štete koje nisu posledica oštećenja ili uništenja računara i nosača podataka daje novu dimenziju klasičnoj imovinskoj polisi.

Savremeno tržište osiguranja se prilagođava novim zahtevima ali još nije uspelo da pruži dovoljno dobru zaštitu pojedinim osiguranicima. Postoji značajna praznina u pokriću imovinskih rizika kako osiguranja stvari tako i osiguranja od građanske odgovornosti.[11] Na nekim tržištima osiguravaju se rizici koji se na drugim smatraju neosigirljivim.[12]

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. Rizici su osigurani nezavisno od toga šta je uzrok, propust osiguranika, propust zaposlenih ili hakerski napad. Danas su neka pokrića internet rizika standardizovana ali zbog njihove osobenosti nije moguće koristiti iste 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 delatnosti i internet rizici različiti stoga nije isto pokriće koje nude pojedini osiguravači. Ono je nestandardno, „kroji" se prema osobenosti izloženosti riziku (suma osiguranja, premija, franšiza, isključenja iz osiguranja). Osiguravajuća zaštita se pruža za od dve grupe rizika koji nastaju u nematerijalnoj, sajber sferi. To su rizici koji dovode do direktnih imovinskih gubitaka kao što su troškovi utvrđivanja uzroka štete, obaveštavanja zaintresovanih strana, otklanjanja nedostataka i ponovnog uspostavljanja kompjuterskog sistema, umanjenje prihoda i troškovi usled prestanka rada i gubitka poslova[13], troškovi zbog povrede i gubitka podataka, novčani iznosi isplaćeni na ime ucene kao i troškove pružanja pravne pomoći. Pokriće šteta usled prekida rada osiguravači nerado prihvataju iako postoji interes, naročito posle učestalih hakerskih napada posle

sowie des Verbandes der privaten Krankenversicherung zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, Berlin, 28.03.2013 / www.gdv.de/.

7 ISO 27001 o bezbednosti u oblasti informatike u cilju zaštite mreže, računara, programa i podataka od napada, štete i neovlašćenih upada. Ovaj standard koji definiše kako upravljati informatičkom bezbednošću popularan je u EU i sve više u istočnoj Aziji i SAD.

8 Ukupni gubici u V. Britaniji koji su posledica internet rizika su 20 mrld funti godišnje. Ceni se da je prosečna šteta većeg sajber napada 500 000 funti. Limit pokrića iz osiguranja je od 5 do 10 miliona funti. Premija ze pokriće od 1 milion je oko 30 000 funti, za pokriće od 10 miliona 150 000 funti. U SAD u 2011 godini na tržištu internet osiguranja premija je bila oko 800 m $. Očekuje se da će iznos premje usledećim godinama biti iznad milion US $. U SAD u nekim delatnostima i 75% preduzeća ima ovo osiguranje (Airmic Review of Recent Developments in the Cyber Insurance market and commentary on the increased availability of cyber insurance product, 8. juni 2012. str 11, dostupno na: www.airmic.com/.../airmic-rewiev-recent-developments-cyber-insurance.

9 Cybersecurity Insurance Workshop Readout Report National Protection and Programs Directorate US Department of Homeland Security (https://www.dhs.gov/.../cybersecurity-insurance). Zakon SAD o zdravstvenom osiguranju iz 1996. godine koji je predvideo stroge sigurnosne standarde zaštite sigurnosti i privatnosti za lične identifikacione informacije doveo je do ogromnog povećanja tržišta. Kalifornijski zakon o zaštiti podataka (2003) imao je za posledicu veliki broj zainteresovanih subjekata koji u svojoj delatnosti imaju baze podataka da se osiguranju od odgovornosti zbog krađe podataka.

10 U uslovima za kombinovano osiguranje elektronskih računara, procesora i sličnih uređaja koje primenjuju neki osiguravači na tržištu osiguranja u Srbiji se predviđa da samo ako je ugovorom o osiguranju dogovoreno i obračunata odgovarajuća premija, predmet osiguranja mogu biti i materijalna vrednost nosača spoljnih podataka (npr. magnetne trake i diskovi) i vrednost podataka na nosačima podataka (Uslovi a.d.o. „Dunav", juli 2003).

11 Danas virusom može da se prouzrokuje ne samo čisto novčana već i šteta na stvarima. Elektronski uzrok može npr. prouzrokovati eksploziju i oštećenje i uništenje stvari. Takav virus je stvoren (Stuxnet) za napad na nuklearno postrojenje. To je otvorilo nove mogućnosti za teroriste jer više ne treba da budu fizički prisutni na mestu događaja da bi izveli teroristički napad. Osiguravači već razmišljaju kako da se postave, da li da se ovakve štete apsolutno isključe iz osiguranja ili da se osiguraju pod posebnim uslovima uz pomoć države.

12 T. Grzebiela, Insurability of Electronic Commerce Risks / www,computer.org/csdl/proceedings/ hicss/2002/1435/07/14350185-obs.html Proceedings of the 35th Hawaii international Conference on System Sciences-2002/ str. 5. Postoji tzv. siva zona koja uključuje rizike koje svi osiguravači ne žele da osiguraju ali koje neki ipak osiguravaju. Zato je nemoguće dati prihvatljivu definiciju o neosigurljivim rizicima.

13 Osiguranje prihoda i vanrednih troškova pokriva gubitak neto dobiti i operativnih troškova koje pretrpi osiguranik usled prestanka delatnosti u vreme otklanjaja posledica osiguranog slučaja (ISO Form CP 00 30 06 07 /2007).

kojih nije bilo moguće duže vreme nastaviti delatnost.[14] Drugu grupu rizika čine izvori opasnosti građanske odgovornosti za štete koje je osiguranik prema propisima građanskog prava dužan da nadoknadi trećim licima. Pored odgovornosti za štete usled povrede ličnih podataka, pokrivena je i odgovornost za štete usled povrede časti i ugleda i povreda prava intelektualne svojine (autorskih i srodnih prava, zaštičene oznake robe ili usluga, poslovne tajne). Najveći značaj se daje osiguravajućoj zaštiti od rizika odgovornosti zbog povrede ličnih poverljivih podataka koje osiguranik prikuplja, obrađuje i prenosi.

Neki osiguravači nude osiguranje fizičkim licima kao korisnicima interneta. Osiguranje se pruža u okviru osiguranja pravne zaštite ili putem posebnih polisa koje su prilagođene internet opasnostima.[15] Pokrivaju se troškovi analize i otklanjanja uzroka koji na društvenoj mreži mogu da ugroze nečiji ugled, zatim šteta zbog zloupotrebe identiteta, pomoć kod zaključenja ugovora i prevare kod online kupovine, obezbeđuje pravna zaštita kod povrede ličnih podataka, autorskog i srodnih prava, posledica napada hakera i dr.

Na savremenom tržištu osiguranja internet rizici koji mogu dovesti do katastrofalnih šteta, koji nastaju u ratnim okolnostima, kao posledica terorizma ili ugrožavanja infrastrukturnih sistema teško se mogu osigurati. Smatra se da država treba da utvrdi mehanizme za njihovo pokriće.

OSIGURLJIVOST INTERNET RIZIKA

Osiguravač mora unapred da zna kakvom je riziku izložen u budućnosti. Procena internet rizika je vrlo složena. Nema dovoljno statističkih podataka na osnovu kojih bi mogla da se utvrdi verovatnoća nastanka i prosečan iznos šteta. Radi se i o riziku čiji nastanak u najvećoj meri zavisi od ljudskog faktora zbog čega je upravljanje rizicima složeno. Zato osiguravači nastoje da pronađu nove mehanizme da bi mogli da pruže zadovoljavajuće pokriće. U tom cilju posebno je značajno direktno finasiranje preventivnih mera kao i izrada poslovnih akata, uslova i tarifa, koji motivišu osiguranika da sam preduzima mere sprečavanja nastanka rizika. Da obaveze ne bi izmakle kontroli u ugovore o osiguranju unesu odredbe kojima se ograničava pokriće po štetnom događaju i u godini osiguranja, predviđa učešće osiguranika u svakoj šteti i predviđa bonus za dobar tehnički rezultat. Ove preventivne mere kao i razvoj tehnologije i novih načina zaštite doprinosi osigurljivosti rizika o čemu svedoče podaci o stalnom porastu broja ugovora.

Okolnosti od značaja za procenu rizika

Sa stanovišta tehnike osiguranja potrebno je utvrditi veličinu i obim opasnosti i s tim u vezi cenu osiguranja. Mora se imati saznanje o prirodi i značaju rizika i merama tehničke zaštite koje osiguranik primenjuje. Poštovanje zakonom utvrđenih mera sigurnosti je osnovni uslov za prijem rizika u osiguranje. Standardi sigurnosti se brzo menjaju, ne retko zastarevaju čim su objavljeni. Često je teško utvrditi uzrok štetnog događaja što otežava izvršenje obaveze osiguravača.[16] O ovim činjenicama osiguravači stalno moraju da vode računa i zato oni koji rade na poslovima osiguranja internet rizika moraju da budu dobro obučeni i da se stalno usavršavaju.

Učestalost internet rizika i obim štetnih posledica teško je utvrditi korišćenjem tradicionalnih metoda. Na ovo osiguranje ne mogu se u potpunosti primeniti standardna pravila tehnike osiguranja.[17] Nezavisnost pojedinačnih rizika je osnovni uslov za ravnotežu zajednice rizika. Ako veliki broj osiguranika pretrpi štete u isto vreme tada pojedinačni slučajevi ne predstavljaju nezavisne događaje. Priroda informatičkih sistema uzrokuje njihovu međusobnu povezanost što može da dovede do kumulacije velikog broja šteta i opasnost insolventnosti osiguravača.[18] Pravilo o disperziji rizika teško se može primeniti.Virusi mogu da se prošire sa jednog mesta na neodređeni broj računara bilo gde u svetu u kratkom vremenskom periodu. Reosiguranje je takođe u nemogućnosti da odgovori stvarnim potrebama zaštite osiguravača. Povezanost informacionih sistema preko interneta na globalnom nivou dovodi do toga da cela zemaljska kugla je mesto potencijalne kumulacije rizika. Mehanizmi reosiguranja su tada nemoćni (za razliku od prirodnih katastrofa gde je rizik ograničen na neku geografsku oblast).[19] Problem se rešava i tako što država pomaže u oblasti preventive (posebno donošenjem propisa kojima se obavezuju privredni i drugi subjekti na donošenje poslovnih akata o upravljanju informacinim sistemima i osposobljavanju zaposlenih) ali i ulogom poslednjeg reosiguravača.

Utvrđivanje naknade iz osiguranja

Utvrđivanje naknade iz osiguranja je drugačije nego u osiguranju stvari. Visinu novčane štete koju je pretrpeo osiguranik ili treće lice često je teško odmeriti. To je materijalna šteta koja može biti velika (gubitak prihoda, povlačenje odobrenog zajma, gubitak započetih poslova).

Internet osiguranje je imovinsko osiguranje u kome je vladajući princip obeštećenje osiguranika. Naknada iz osiguranja treba da odgovara visini stvarno pretrpljene štete. Kako se ona u konkretnom slučaju teško može utvrditi postavlja se pitanje kako postupiti. Predvideti isplatu ugovorenog iznosa ne ulazeći u utvrđivanje visine štete suprotstavlja se principu obeštećenja. Nije isključeno da bi osiguranik mogao da dobije znatno više od pretrpljene štete i tako se obogatio. Ovaj problem je još otvoren i osiguravači različito postupaju.

14 U sporu NMS services Inc.v. Hartford, 62 Fed. APPx.511 (4th Cir. 2003), osiguranik je imao pokriće prekida rada i vanrednih troškova kao posledice sajber rizika. Zaposleni je ugradio dva hakerska programa u osiguranikov network sistem što mu je omogućilo upadne u sistem i prouzrokuje veliku štetu. (Insurance Coverage for Cyber Attacks, The Insurance Coverage Law, Bulletin, Vol. 12, No. 5, juni 2013, K&GATES, Legal Insight, dostupno na sajtu www.kigates.com).

15 Ovu polisu nudi jedna od najvećih multinacionalnih osiguravajućih grupa, AXA.

16 W. Karten, Zum Problem der versicherbarkeit und zur Risikopolitik des Versucherungsnehmers, betribswirtschaftliche Aspekte, Zeitschrift fur die gesamte Versicherungswissenschaft, 1972, str. 280.

17 A. Jagdham, op. cit., str. 2. Les conditions d'assurabilité des cyberrisques, Risques, Cahiers des Assurances, str. 2

18 T. Gabriele, op. cit. str. 7.

19 Isto.

Suma osiguranja

Da bi se utvrdio najviši iznos obaveze osiguravača prilikom zaključenja ugovora treba udrediti vrednost osiguranog interesa. Kada je prilikom zaključenja ugovora o osiguranju teško utvrditi vrednost predmeta osiguranja suma osiguranja se utvrđuje na više načina. Tako npr. ako je reč o umetničkim ili drugim vrednostima osiguravač i osiguranik sporazumno utvrđuju tu vrednost. Kada nastane osigurani slučaj osiguravač uvek može da ističe prigovor da je ugovorena vrednost iznad stvarne vrednosti i da prizna naknada koja je manja od ugovorene sume. Ima slučajeva kada se osiguranje može zaključiti i na deklarisanu vrednost, onu koju je odredio sam osiguranik, ali i ovde osiguravač naknađuje stvarno nastalu štetu. Poznato je da se u osiguranju od građanske odgovornosti limit pokrića utvrđuje po izboru osiguranika jer se ne može unapred znati koliku štetu on može da prouzrokuje drugome. 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 koji iznos sume osiguranja može da zadovolji njegove potrebe za osiguravajućom zaštitom. Ako se prilikom nastanka osiguranog slučaja može nesumnjivo utvrditi da je ugovorena suma manja od stvarne štete naknada može biti do ugovorene sume. U ovakvim osiguranjima primenu pravila proporcionalnosti treba isključiti jer ono ima puni smisao onda kada se u momentu zaključenja ugovora može utvrditi tačna vrednost osiguranog interesa.

Premija osiguranja

Jedan od razloga koji utiče na to da osiguranje internet rizika nije još uvek dovoljno razvijeno je visoka premija. Osiguravači su sve više svesni te činjenice i priznaju značajne popuste onim osiguranicima koji preduzimaju preventivne mere. Kada se radi o osiguranjima rizika na čiji nastanak utiče ponašanje osiguranika premija zavisi u dobroj meri od tehničkog rezultata. Osiguranicima koji u relevantnom periodu imaju dobar tehnički rezultat priznaje se popust na premiju, a onima koji imaju loš rezultat plaćaju veću premiju. To je slučaj i u osiguranju internet rizika koji ne retko nastaju usled radnji ili propusta zaposlenih. Osiguravaču su važni podaci o tome koji su sigirnosni sistemi ugrađeni kako bi se sprečio nastanak rizika ili ograničile njegove štetne posledice. Prate se aktivnosti osiguranika na poboljšanju sistema sigurnosti u osiguranoj delatnosti, zahtevaju preduzimanje određenih mera, od osiguranika se traži da vodi računa o usavršavanju i nadzoru zaposlenih koji mogu namerno ili slučajno da prouzrokuju nastanak rizika. U osiguranju internet rizika saradnja osiguravača i osiguranika je stalna. Primena zakonskih mera sigurnosti kao i mera koje zahteva osiguravač utiče značajno na smanjenje premije.

RIZICI VEZANI ZA „INTERNET OBLAK“

Neke organizacije podatke sa svojih računara ne čuvaju na vlastitim, nego na serverima kompanija koje ih čini dostupnim preko interneta. Podaci kompanije se ne nalaze u centralnom računaru kompanije, nego u “virtualnom oblaku”, serverima internetskih ponuđača. Postavlja se pitanja kako se obezbeđuje sigurnost pohranjenih podataka, da li o tome brine organizacija čiji su podaci ili internetska kompanije koje nude usluge pohranjivanja podataka. Podaci mogu da se nalaze na računarima u više zemalja pa se postavlja pitanje koji se propisi o zaštiti podataka primenjuju, da li zemlje subjekta čiji su podaci ili zemlje gde se server nalazi. Osiguravači o tome moraju da vode računa jer se propisi razlikuju od zemlje do zemlje i to direktno utiče na veličinu osiguranog rizika. Oni koji pohranjuju svoje podatke u “oblaku“(claud-u) trebalo bi da kontrolišu rad onoga kod koga se podaci pohranjeni. Najčešće se ugovorima između ova dva subjekta ne reguliše pitanje odgovornosti bezbednosti podataka kada je provajder renomirana kompanija, što nije dobro jer u svakom, pa i u najboljem sistemu, može biti slabosti. Unošenje klauzule o odgovornosti u ugovore u pružanju ovih specifičnih usluga često se ne unose jer mnogi korisnici nemaju dobru pregovaračku poziciju.[20] Osiguravači moraju da znaju ko je odgovoran za štete usled povrede podataka. Ako je na serveru internetske kompanije više korisnika može doći do kumulacije rizika, hiljade korisnika mogu biti istovremeno pogođeni i jedan napad može dovesti do insolventnosti osiguravača. Kada pitanje odgovornosti nije regulisano ugovorom osiguravač teško može da ostvari pravo na regres po osnovu subrogacije. Kako je primena opštih pravila građanskog prava o odgovornosti teško primeniti u ovakvim slučajevima zbog problema utvrđivanja uzročne veze između propusta i nastale štete i krivice uputno je da se pitanje odgovornosti reguliše ugovorom. Kada bi osiguranje zaključili i korisnik i provajder praznine u pokriću ne bi bilo. Ovaj bi problem mogao da se reši i posebnim propisom ali još nije bilo takvih pokušaja ni u razvijenim zemljama. Ima opreznih provajderam koji znaju da bi u nekim slučajevima mogla da se utvrdi uzročno-posledična veza između internet rizika i njihovog propusta i zaključuju osiguranje od opšte profesionalne odgovornosti (E&O).[21]

OSIGURANJE RIZIKA POVREDE LIČNIH PODATAKA

Propisi o zaštiti podataka obavezuju one koji sa njima raspolažu da preduzmu sve poznate mere zaštite a ako do povrede dođe o tome odmah obaveste one o čijim se podacima radi.[22] Troškovi ovog obaveštavanja mogu biti

20 Za utvrđivanje odgovornosti mogu pomoći ISO standardi o sigurnosti u oblasti informatičke tehnologije. Radi se na utvrđivanju standarda samo za cloud sigurnost. Međunarodno udruženje za računarsku sigurnost izradila je cloud sertifikat program, Cybersecurity Insurance Readout Report, op. cit. Str. 24.

21 E&O je osiguranje koje pokriva odgovornost za štete usled profesionalnih propusta osiguranika.

22 O značaju podataka o osiguranicima govori činjenica da je Savet Evrope doneo Preporuku u vezi zaštite ličnih podataka prikupljenih u okviru delatnosti osiguranja. Način na koji osiguravač dolazi do ličnih podataka mora da bude dozvoljen, a dobijeni podaci

izuzetno visoki. Rizik često nastaje namernim postupkom zaposlenih. U praksi osiguranja zabeleženi su slučajevi da službenici državnih organa kojima su podaci građana dostupni iste dostave osiguravačima i od njih dobijaju značajnu naknadu.[23] Poslednjih decenija, iskustvo u domenu zaštite podataka o ličnosti pokazalo je neophodnost određivanja organa koji će se brinuti o zaštiti podataka, bar kada je reč o velikim privrednim društvima. Društva mogu da upoznaju svoje zaposlene o odredbama zakona putem obuka. Osim toga, društva mogu da obavežu zaposlene da se pismenim putem obavežu na poštovanje službene tajne.[24]

Gubitak podataka može dovesti do ogromne štete, kako direktne tako i štete licima o čijim se podacima radi koja mogu da podnesu zahtev za naknadu štete na osnovu zakona o zaštiti podataka.[25] Kada preduzeče izgubi poverljive podatke bilo putem upada hakera ili namere ili nepažnje zaposlenih klijenti gube poverenje i to dovodi do smanjenja njegovog ugleda.[26] Osnovno pokriće koje se se nudi za rizik povrede podataka je građanska odgovornost za štete koje su posledica povrede. Dalje pokriće obuhvata troškove u vezi upravljanja krizom. Hakerski napad ima za posledicu veliku štetu. Podaci mogu biti izmenjeni, oštećeni, obrisani ili uništeni. Pokriveni mogu biti i troškovi ponovnog uspostavljanja baze podataka. Ako sistem ne radi nastaje dalja šteta. Naknada gubitka prihoda i troškova može da se osigura kao osnovno ili dopunsko pokriće.27

ZAKLJUČAK

Na tržištu osiguranja razvijenih zemalja neki internet rizici se osiguravaju, neki delimično a neki se ne primaju u osiguranje. Ovi novi rizici su za neka privredna društva daleko veća opasnost od klasičnih industrijskih rizika i zato u razvijenim zemljama zahtevi za osiguranjem rastu. Države su zainteresovane za razvoj osiguranja jer osiguravači značajno doprinose preduzimanju preventivnih mera, a informacioni sistemi se posle nezgode brže uspostavljaju što je od velikog značaja za normalno obavljanje privrednih aktivnosti i državnih i javnih poslova. U Srbiji interesovanja za osiguranjem internet rizika nema iako je rizik prisutan. Raširena je pogrešno shvatanje da standardne polise za osiguranje stvari i građanske odgovornosti već pokrivaju i ove rizike. Ni domaći osiguravači ne pridaju značaj uvođenju i razvoju ovog savremenog osiguranja, a takav stav opravdavaju time da se radi o nepoznatom, teško procenjivom riziku. Dok se u razvijenim zemljama postavlja pitanje kako da se uklone prepreke koje sprečavaju osiguravače da nude relevantnije polise većem broju klijenata za nižu cenu u manje razvijenim zemljama se razmišlja da li da se uopšte krene sa ovim osiguranjem. Zato je pomoć države od značaja. Trebalo bi osnovati domaći pul reosiguranja sa učešćem države i doneti zakon koji bi utvrdio uslove za pokriće internet rizika. Na tome se u svetu uveliko radi. Značaj informatičke tehnologije je veliki i za Srbiju i mora se voditi računa o finansijskoj sigurnosti onih koji su izloženi novim rizicima.

LITERATURA

[1] A. Jaghdam, Les conditions d'assurabilite des caber-risques, Risques, Les cahiers de l'assurances, 77/2014.

[2] G. Allen, Cyber Risk and Insurance- A Reality Check, Wllis North America, Octobar 2004-White Paper,

[3] N. Ligtelijn/S. Favaretto, Assurance sur internet : La croissance en marche, Risques, Les cahiers de l'assurances, 77/2014.

[4] J. Behrends, Cyber-Versicherung haben eine grosse Zukunft, Versicherungs Wirtschaft 2/2013

[5] M.E. Meinl, Eletronic Complaints: An Empirical Study on British English and German Complaints on eBay (Rheinischen Fridrich-Wilhelm-Universitet Bonn (dostupno na: hss. ulb.uni-bonn.de/2010/2122/2122/htm

[6] M. Greisiger, Cyber Risks-Developing Layered Safeguard Controls, Business Insurance, White Paper, www.BusinessInsurance

[7] T. Grzebiela, Insurability of Electronic Commerce Risks

[8] /www.computer.org/csdl/proceedings/ hicss/2002/1435/07/14350185-obs.html Proceedings of the 35th Hawaii international Conference on System Sciences-2002/

[9] W. Karten, Zum Problem der versicherbarkeit und zur Risikopolitik des Versucherungsnehmers, betribswirtschaftliche Aspekte, Zeitschrift fur die gesamte Versicherungswissenschaft, 1972Internet Liability Exposures and the Insurance Response, www.nzila.org/.../Gary_Thomas_ technology.pdf

obrađivani u skladu sa pravilima struke osiguranja. Osiguranik mora na jasan način da bude informisan o svrsi korišćenja njegovih podataka, a osiguravač koji obrađuje podatke može da koristi dobijene informacije isključivo u cilju izvršenja radnji potrebnih za zaključenje, sprovođenje i izvršenje ugovora o osiguranju. /https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=543709&SecMode=1&DocId=295462&Usage=2/

23 Prema istraživanju časopisa Handelsblatt uključeno je bilo preko 10.000 službenika (policajaca, prosvetnih radnika, poreskih službenika i dr.) od kojih su dobijane informacije o fizičkim licima koji nisu kod njih osigurani (prezime, ime, adresa, lični podaci). Društvo za osiguranje je plaćalo je po 50 evra nastavnicima za informaciju o novom učeniku. Ukoliko bi došlo do zaključenja ugovora o zdravstvenom osiguranju, nastavnik bi bio nagrađen sa 150 evra, dok bi u slučaju zaključenja ugovora o osiguranju života dobijali po 600 evra.

24 Član 35. Zakona o zaštiti ličnih podataka, Službeni glasnik R. Srbije,

25 Savezni zakon o zaštiti podataka (čl. 43 st. 2) Nemačke predviđa kaznu od 300 000 evra u slučaju povrede podataka klijenata. Očekuje se da će uredba EU o zaštiti podataka biti doneta do kraja 2014 goine koja će uticati na poošterenje odgovornosti za gubtak podataka. To će nesumnjivo doprineti povećanju zahteva za osiguravajućom zaštitom. Postoji obaveza prijave nadležnom organu povrede podataka u roku od 24 sata od saznanja za povredu. Kazna koju predviđa uredba je do 2% od ukupnog prihoda (obuhvaćen je i prihod od poslova u inostranstvu). Član 57. Zakona o zaštiti podataka o ličnosti R. Srbije predviđa kaznu od 50.000 do 1.000.000 din. pravno i odgovorno lice u pravnom licu od 5.000 do 50.000 dinara što je znatno niža kazna od onih u pravu država članica EU.

26 Vodič za rukovanje podacima o ličnosti u privatnom sektoru (Poverenik za zaštitu podataka i transparentnost Švajcarske konfederacije, str. 10, izvor: http://www.edoeb.admin.ch/datenschutz/00628/00629/00633/index.html?lang=fr)

27 U Nemačkoj ima 450 miliona ugovora o osiguranju sa ličnim podacima. http://gdv.de/2012/07 das- krisen reaktionszentrum fur IT-Siherhaits der Versicherers. Saradnja države, privrednih preduzeća i društava za osiguranje doprinosi većoj bezbednosti podataka i omogućava sprovođenje osiguranja.

[10] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) /COM/2012/011 final - 2012/0011 (COD) /

[11] Airmic Review of Recent Developments in the Cyber Insurance market and commentary on the increased availability of cyber insurance product, 8. juni 2012. str 11, www.airmic.com/.../airmic-rewiev-recent-developments-cyber-insurance.

[12] Cyber Security Insurance Workshop Readout Report, National Protection and Programs Directorate US Department of Homeland Security, (https://www.dhs.gov/.../cybersecurity-insurance).

[13] Internet Liability Exposures and the Insurance Response www.nzila.org/.../Gary_Thomas_technology.pdf

[14] The Betterley Report, Coverage of Cyber Risk, www.betterley.com/blog

[15] Menaging Cyber Cecurity as a Business Risk:Cyber Insurance in the Digital Age, Ponemon Institute, www.ponemon.org

[16] Stellungnahme des Gesamtverbandes der Deutschen Versicherungswirtschaft sowie des Verbandes der Privaten Krankenversicherung zum Referentenentwurf des Bundesministerium des Innern fur ein Gesetz zur Erhohung der Sicherheit Informationstechnischer Systeme, Berlin 2013, www.gdv.de

INTERNET RISK INSURANCE

Abstract:
The development of information technology triggered the need to provide adequate insurance protection and cope with the consequences of newly emerged risks. The traditional insurance policies are written with new clauses expanding the coverage for damages that are the result of partial or total destruction of computer, but insurers also offer special policies that apply only to Internet risks. Insurers are trying to adapt the coverage to the individual needs of the insured, but is often difficult to meet the requirements and to carry out the risk assessment because of the continuous development of information technology and its complexity. The most adequate solutions that would be in accordance with existing regulations in the field of insurance and regulations on the protection of information systems and personal data are yet to be found. The article points out the problems that insurers meet in relation with specific risks and the possible solutions for the insurance market of Serbia in order to develop a new product that would be in the interest of those who are undoubtedly exposed to Internet risks.

Key words:
Insurance policy,
Risks insured,
Protection of private data,
Public liability,
Hackers attacks,
Business interruption.