CYBER RIZICI – REOSIGURANJE I IZAZOVI DIGITALNOG SVIJETA

ŽIVOT JE NADIŠAO MAŠTU

U svijetu kakvog ga je George Orwell prikazao u romanu 1984, a izdao ga je sredinom 1949., svijet nije bio digitalan, ali je bio pod budnim okom Velikog brata. Nepunih 70 godina kasnije, u situaciji smo da nas ne promatra oko Velikog brata – ili bolje reći ne promatra nas samo ono – već zahvaljujući digitalizaciji sami snimamo i objavljujemo svoje fotografije, video-zapise, navike i misli, koje su dostupne cijelom svijetu. Po nekim studijama, prosječan korisnik pametnog mobilnog telefona u SAD pogleda u njega 150 puta dnevno[1], a dotakne ga 2.617 puta dnevno.[2] Broj mobilnih aparata u svijetu će preći 5 milijardi do 2019. godine[3]. Prednosti ovakve međusobne povezanosti su ogromne, omogućavaju znatno lakšu komunkaciju, informiranje, nabavku, poslovanje s bankama, pa čak u nekim naprednijim zemljama i komunikaciju s državnim organima, inače cijepljenim najjačim cjepivom protiv bilo kakvog progresa ili olakšavanja života svojim građanima. Jer se na taj način gubi moć. No, informiranje i kupovina su još uvijek, čini se, glavne preokupacije korisnika mobilnih telefona. Tako je prodaja preko web stranice draguljarnice Tiffany porasla 125% nakon što su stranicu prilagodili za mobilne telefone.[4] I nije nužno da sami objavimo svoje fotografije i druge informacije, uključujući i to da nismo u svom stanu, hakeri mogu pristupiti vašim kamerama i mikrofonu i iz najudaljenijeg kutka svijeta.

DIGITALNI SVIJET I MI

Naravno, digitalizacija svijeta ne staje samo na mobilnim telefonima, ona je općenita, i napreduje velikom brzinom, čak i kada je jasno da su brojna pitanja ostala otvorena. Od upravljanja proizvodnim procesima do toga da vaš frižider zna bolje od vas šta možete imati za ručak. Od vozila koja sama sobom upravljaju do distribucije robe. Od elektronskog bankarstva zahvaljujući kojem izbjegavate redove i neshvatljive procedure u bankama, koje začudo u elektronskom bankarstvu nisu tako stroge, te sami upravljate novcem i vršite plaćanja, do mogućnosti da haker počisti vaš bankovni račun zahvaljujući istom tom elektronskom bankarstvu. Uz pojavu tzv. kriptovaluta (1.110 njih[5], a broj im

[1] https://www.textrequest.com/blog/americans-check-their-cell-phones-150-times-a-day/
[2] https://www.networkworld.com/article/3092446/smartphones/we-touch-our-phones-2617-times-a-day-says-study.html
[3] https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/
[4] https://www.phonearena.com/news/Average-person-looks-at-his-phone-150-times-per-day_id26636
[5] https://venturebeat.com/2017/09/20/how-many-cryptocurrencies-does-the-world-need/

raste), uz virtualni svijet imamo i virtualne valute te i njihovo postojanje i nestanak predstavlja rizik.

Praktički nema oblasti života u kojoj digitalizacija nema primjenu. I to na način kojim se u potpunosti mijenja način života i zatvaraju stari a otvaraju novi poslovi, nestaju stari a nastaju novi proizvodi ili nove usluge. Tako su nestali fizički predmeti poput gramofonskih ploča (njihov povratak u proizvodnju i prodavnice ipak treba više vezivati uz nostalgiju i procjenu da se može na istom proizvodu još jednom zaraditi), audio kaseta, VHS kaseta i kaseta drugih formata, smanjuje se prodaja CD-ova i DVD-ova, a sve teže možete nabaviti uređaje za njihovu reprodukciju. Televizori se još uvijek prodaju, ali kako možete programe gledati i na svom mobilnom telefonu, tabletu ili računaru, bilo prenosnom ili desk-topu, a nivo pozornosti koji pojedinac obraća na video sadržaj je sve manji i koncentracija sve kraća, pitanje je do kada će se televizor smatrati potrebnim kućanskim aparatom. A ovo je samo jedan mali, izdvojeni segment promjena u životu.

OPASNOSTI DIGITALNOG SVIJETA

Uz ogromne mogućnosti koje digitalni svijet otvara, opasnosti koje su došle sa digitalnim svijetom su možda još i značajnije, a u svakom slučaju manje poznate.

Svi se sjećamo tzv. Millenium buga, znanog i kao Y2K, kada se smatralo da stariji software-i u kojima je godina iskazana samo sa dvije zadnje cifre neće prepoznati da se radi o prelazu sa 1999. na 2000. godinu, te da neće prepoznati da je nastupajuća godina prestupna. Skoro svi, od pojedinih vlada do velikog broja privrednih društava, uključujući i ona iz oblasti osiguranja i reosiguranja, su uložili ogromne napore i novac da se pripreme za taj sudbonosni trenutak. Po današnjim cijenama, na rješavanje problema je utrošeno 438 milijardi USD[6]. Iako je moje mišljenje da je tada bilo puno, puno više dima nego što je realno bilo vatre, i da je to u konačnici bio dobar posao za informatičare, ovaj period bi se mogao označiti kao period pojave prvog globalnog cyber rizika. Danas, dvadesetak godina kasnije, cyber rizici vrebaju u digitaliziranom svijetu iza svakog binarnog ugla.

I iz vlastitog iskustva mogu reći da cyber rizik može utjecati na sve. Tako je novokupljeni automobil kasnio 10 dana u isporuci zbog navodnog hakerskog napada na Luku Koper, tako da se u tom periodu nije moglo znati gdje treba isporučiti robu. Ili je promućurni

[6] https://en.wikipedia.org/wiki/Year_2000_problem

trgovac na taj način opravdao zakašnjenje nastalo iz nekog drugog razloga. U svakom slučaju, za moje prijatelje je to bila zanimljiva priča.

No, prekid lanca snabdijevanja teško da bi se mogao opisati kao zanimljiva priča. Ili ne samo kao zanimljiva priča. On može dovesti do nestašica, velikih poslovnih gubitaka, pa i propasti pojedinih poduzeća.

Potencijalna šteta može nastati bilo kada i bilo gdje. Podjednako su ugroženi kako vlade pa čak i vojske, bez obzira na značajna sredstva, ljudstvo i tehniku kojima se štite, tako i proizvodni pogoni, transport, zdravstvo, edukacija, financijski sektor, razni drugi poslovi.

Segment koji je možda i najčešće pogođen cyber rizicima su baze podataka. Prema podacima organizacije Identity Theft Resource Center u 2017. je bilo oko 1.300 proboja u podatke, u kojima je 174 miliona podataka bilo izloženo. Godinu ranije zabilježeno je 1.093 poboja. Poslovni sektor je pretrpio najviše udara, 50,5%, zdravstveni sektor 28,3%, edukacioni sektor 8,8%, vlada/vojni sektor 5,3% od broja svih incidenata. Bankarski i financijski sektor 7,1%. Procjenjuje se da se podaci po osobi prodaju u prosjeku za 8 USD, a da mogu porasti u nekim specifičnim slučajevima na 15, pa i 30 USD[7]. Pri tome, broj dobijenih podataka, čak 91,4%, potiče iz upada u sisteme poslovnog sektora. Stoga je jasan financijski interes onih koji pokušavaju preoteti podatke. S druge strane, procijenjeni trošak po ukradenom ili izgubljenom zapisu za njihovu obnovu u prosjeku je u 2013. godini iznosio 188 USD[8].

Cyber rizici su još 2014. ušli među 10 najvećih globalnih poslovnih rizika, a u zadnje vrijeme se porede sa iznosima šteta koje nastanu usljed prirodnih katastrofa. Prema Allianz Risk Barometer Survey, anketi u kojoj je sudjelovalo 824 ispitanika iz 44 države, u 2016. su bili na 3. mjestu, a u Ujedinjenom Kraljevstvu na prvom[9]. Svjetska ekonomija gubi zbog cyber kriminala 445 milijardi USD godišnje[10].

[7] http://247wallst.com/technology-3/2017/12/23/2017-data-breach-total-nears-1300-easily-a-new-record/
[8] https://www.ponemon.org/local/upload/file/Cyber%20Insurance%20white%20paper%20FINAL%207.pdf
[9] http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf
[10] http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf

Posebno zastrašujuće zvuči izjava general-majora njemačkog ratnog vazduhoplovstva Ansgara Riksa, koji je upozorio da po jednom istraživanju hakeri mogu preuzeti kontrolu nad vojnim avionima uz pomoć opreme vrijedne 5.000 EUR[11].

RAZVOJ CYBER OSIGURANJA

Razvoj pokrića cyber rizika osiguranjem (tj. razvoj „proizvoda“ osiguranja) u SAD je počeo 1996., kada se cyber osiguranje prvi put pojavilo. U Kaliforniji su 2003. donijeti zakoni o obavještavanju o kršenju privatnosti (Privacy breach notice laws) kojima je povećana tražnja cyber osiguranja. Nakon toga, ukupno 47 od 50 država SAD je uvelo zakone o obaveznom obavještavanju o kršenju, te je zakonodavstvo tako postalo glavni pokretač razvoja ovog osiguranja. 2014. preko 60 društava je preuzimalo cyber rizike u osiguranje, s premijom od preko 1 milijarde USD.

Razvoj u Europi je započeo 1995. donošenjem Direktive EU o zaštiti podataka, kada je zaštita podataka ustanovljena kao pravo građana EU. Sredinom 2000. povećana zavisnost od infromacione tehnologije i veliki hakerski skandali su doveli do povećane tražnje cyber osiguranja. EU je 2013. najavila Direktivu EU o cyber sigurnosti, kojom se određuju minimalne mjere zaštite u poslovanju. 2013./2014. društva za osiguranje daju ponude na širem tržištu, a u Londonu postoji 25-30 tržišta za ovo osiguranje. 2015. se očekivala primjena reforme zakonodavstva o zaštiti podataka, ali je to pomaknuto za kasnije[12].

Procjene su da tržište cyber osiguranja generira 700 miliona EUR premije, a da će u 2018. godini dosegnuti 800 miliona EUR[13].

Donošenjem strožijih zakona o zaštiti ličnih podataka, trošak rješavanja cyber upada je povećan, kroz troškove obavještavanja vlasti unutar 72 sata, klijenata, troškove odnosa sa javnošću i pravnih troškova. U Europi se očekuje stupanje na snagu European Global Data Protection Regulation u maju 2018., odredbe koja je donijeta 2016. Ukoliko bi neko društvo propustilo da ispuni odredbe ove regulative, može biti kažnjeno sa 2% do 4%

[11] Oslobođenje, 14.07.2017
[12] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf
[13] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf

njihovog globalnog prihoda, zavisno od vrste aktivnosti i uz primjenu monetarnih ograničenja (maksimum od 20 miliona EUR). Donošenje ove regulative moglo bi donijeti daljnji ubrzani rast cyber osiguranja[14] u EU.

ŠANSA ZA OSIGURANJE

Nesumnjivo mnogi misle da je u situaciji kada premije osiguranja (i reosiguranja) padaju u uobičajenim vrstama osiguranja, okretanje osiguranju cyber rizika dobra orijentacija i šansa za povećanje premijskog prihoda. U periodu od 2012. do 2015. premija je porasla sa 1 milijarde USD na 2 milijarde USD, a očekuje se utrostručenje premije do 2020.[15], a po nekim procjenama skok na 20 milijardi USD do 2025. godine[16].

U rijetko kojoj oblasti je moguće očekivati ovakav rast premije, štoviše može se reći ni u jednoj drugoj. No bez dužeg iskustva u osiguranju cyber rizika i preciznijih statistika nemoguće je reći kakav efekt tako uvećana premija može imati na rezultate poslovanja pojedinih društava ili općenito, na statistike pojedinih tržišta. Poredeći sa ukupnim ekonomskim štetama (445 milijardi USD), ako ništa drugo treba ukazati na oprez kod preuzimanja ovakvih rizika, jer je izloženost očito vrlo visoka.

Zanimljivo je da je stopa osiguranih društava puno veća kod imovinskih osiguranja (npr. od požara (59%), iako je vjerojatnoća ostvarenja događaja požara manja od vjerojatnoće ostvarenja cyber napada. Nekih 15% društava osigurava svoju informatičku aktivu[17].

PROSJEČNI TROŠKOVI CYBER NAPADA NA UZORKU OD NEKOLIKO STOTINA KOMPANIJA

Dostupni podaci pokazuju da su društva u SAD izložena većem riziku financijskih gubitaka preko 1 milion USD usljed cyber kriminala. Tako prema nekim studijama 7% društava u SAD je izgubilo 1 milion USD ili više, dok je na svjetskom nivou taj postotak 3%. Dodatno na to, nekih 19% organizacija u SAD su izgubile između 50.000 USD i 1 miliona USD, naprema 8% organizacija na svjetskom nivou. Krađa informacija dovodi do

[14] http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
[15] https://www.darkreading.com/operations/average-breach-falls-below-cyber-insurance-policy-deductible-study-shows/d/d-id/1324652
[16] http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf
[17] http://www.aon.com/attachments/risk-services/cyber/2017-Global-Cyber-Risk-Transfer-Report-Final.pdf

najvećeg vanjskog troška po društva koja pretrpe cyber napad, a troškovi vezani uz poremećeno poslovanje ili izgubljenu produktivnost su drugi najveći vanjski trošak, a kojeg čine faktori poput kazni, sudskih postupaka, utrživosti ukradene intelektualne imovine itd. Rješavanje problema nastalih cyber napadima, ukoliko nije brzo, dovodi do povećanja troškova. Tako je prosječno vrijeme za rješavanje cyber napada bilo 32 dana, a prosječni trošak društava iz SAD koja su bila uključena u godišnju studiju iz 2013. Ponemon Instituta je prelazio 1 milion USD. Godinu ranije studija je pokazivala period od 24 dana potrebna da se riješe problemi cyber napada, a prosječni trošak je bio 591.780 USD[18].

Studija Ponemon Instituta iz 2017.[19], Cost of Data Breach Study (sponzorirana od strane IBM-a, te stoga dostupna na toj stranici), pokazuje koje su se promjene desile. Na uzorku od 419 kompanija iz 13 zemalja, prosječni trošak je dosegao 3,62 miliona USD, što je ipak nekih 10% manje u odnosu na prethodnu godinu. Prosječan trošak po izgubljenom podatku je bio 141 USD, a šanse za ponovni napad su bile 27,7% u periodu od naredne dvije godine.

NEKI VEĆI CYBER NAPADI

Već je rečeno da se cyber napadi mogu desiti u bilo kojoj oblasti ljudske aktivnosti. Evo nekih od takvih događaja, prema brošuri Aon-a Global Cyber Market Overview[20] i nekim drugim izvorima:

Hunter Water - Negdje 2000. nezadovoljni radnik upao je u sistem vodovoda i oslobodio 264.000 litara otpadnih voda na različitim lokacijama, u periodu od 3 mjeseca. Napad je doveo do značajnog onečišćenja okoline.

Los Angeles City Hall – 2006. Uprava grada je bila odgovorna zbog prekida poslovanja jer su hakeri ušli u sistem i na nekoliko dana zakrčili 4 glavne raskrsnice.

TJX (maloprodaja) – 2006., 2007., 90 miliona USD troškova, ukadeni podaci o kreditnim i debitnim karticama klijenata.

[18] https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf
[19] https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/security-ibm-security-services-se-research-report-sel03130wwen-20180122.pdf
[20] http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf

Heartland (financijske usluge – procesori za plaćanje) – 2008., 2009., 110 miliona USD troška. Ukradeni podaci su uključivali i magnetne zapise učitane na magnetne trake kreditnih i debitnih kartica, koje su hakeri mogli onda duplirati na lažne kartice.

Lodz City Tram system – 2010. poljski tinejdžer je premostio daljinski upravljač TV-a te je njim upao u bežični sistem upravljanja skretnicama. Jedan tramvaj je iskočio zbog toga iz tračnica i udario u drugi, prouzrokovavši lakše povrede nekolicine putnika, što je prvi cyber napad koji je doveo do povreda.

2010. napadnut je razvojni nuklerani program Irana, kada je virus Stuxnet ubrzao 1/5 nuklearnih centrifuga i doveo do njihovog raspada. Nema procjene visine štete.

Saudi Aramico – 2012., hakeri su prouzrokovali uništavanje 30.000 desktop kompjutera i 2.000 servera, a informatički sistem kompanije je bio isključen 2 sedmice.

Zappos (internet prodaja) – 2012., 500 miliona USD troška zbog preuzimanja podataka o klijentima.

Adobe (tehnologija) – 2013., bez procjene troška. Ukradeni podaci o kreditnim i debitnim karticama 3,1 miliona klijenata, lozinke 33 miliona korisnika, kao i izvorni kod za razne pakete, uključujući i Adobe Photoshop.

Kompanija JP Morgan Chase (financijske usluge/bankarstvo) napadnuta je 2014. Iako nema iznosa štete, plan je napravljen da se godišnje na digitalnu sigurnost troši 250 miliona USD.

Ebay (internet trgovina) – napadnuti 2014., smanjili su planirani godišnji prihod za 200 miliona USD zbog napada.

Target (maloprodaja) – 2014., trošak incidenta 162 miliona USD, ukradeno 40 miliona podataka o kreditnim i debitnim karticama i lični podaci 70 miliona kupaca.

LOT – 2015. poljska aviokompanija je zbog hakiranja hardware-a koji izdaje planove leta morala otkazati desetak letova.

Kompanija Anthem (djelatnost: zdravstvo) je 2015. Imala štetu od 100 miliona USD zbog pristupa hakera ličnim informacijama.

Equifax (kreditni registar) je u cyber napadu 2017. imao preko 160 miliona kompromitiranih ličnih podataka. Napad je započeo u martu, ali se nisu oglašavali, a glavni napadi su bili u maju i junu mjesecu. Prvi izvještaj o obavještenjima je datiran 18.09.2017. Prvog dana po objavi napada, vrijednost dionica je pala 13%, a ukupno 25%, dok su u dvije tzv. klasne tužbe potrošači iz Kanade potraživali odštetu u visini od 450

milijardi USD, a iz SAD 70 milijardi USD[21]. Konačna šteta se zasigurno neće moći znati godinama. Osiguranje koje je Equifax ugovorio pokriva između 100 i 150 miliona USD[22].

2017. WannaCry ransomware je inficirao stotine hiljada računara, a napadači su tražili od žrtava iz više od 150 zemalja 300 miliona USD, plativo u bitcoinima.

Coincheck je 2018. objavio gubitak 534 miliona USD vrijednih bitcoina u hakerskom napadu[23]. Procjene su da je do sada u takvim napadima izgubljeno na milijarde USD. Neka društva su spremna osigurati takve napade do 25 miliona USD, neka pokrivaju samo krađe koje počine zaposlenici kompanija, ali ne i od trećih osoba, a neki pak samo kriptovalute na tzv. „hladnim novčanicima“, ali ne i online račune („vrući novčanici“).

SISTEMSKA RJEŠENJA ZA POBOLJŠANJE CYBER SIGURNOSTI

Viđenje javnosti je da dvije trećine ispitanika smatra da su korporacije odgovorne za cyber napade, kada se oni dese, a 62% ispitanika iz SAD smatra da vlada SAD treba biti odgovorna za zaštitu američkih poslova od cyber napada[24].

Stoga ne čudi donošenje zakona iz ove oblasti, te je još 2013. predsjednik SAD Obama izdao izvršnu naredbu o cyber zaštiti kako bi se poboljšala cyber zaštita kritične infrastrukture u SAD i promoviralo dijeljenje informacija o cyber prijetnjama između vlade i privatnih društava koje nadgledaju te kritične sisteme. U SAD se niz takvih propisa nastavio. Nakon izvršne naredne predsjednika Obame, Nacionalni institut za standarde i tehnologiju je 2014. donio tzv. okvir za poboljšanje cyber sigurnosti kritične infrastrukture, koji obuhvata postojeće svjetske standarde i prakse koje pomažu društvima da shvate, prijave i kontroliraju svoje cyber rizike[25].

U tom svjetlu treba promatrati i već spomenutu EU regulativu, European Global Data Protection Regulation. Svakako, i svako pojedino društvo treba ozbiljno pristupiti procjeni izloženosti cyber rizicima i mjerama zaštite. I industrija osiguranja će zasigurno moći pomoći svojim savjetima, ali je sasvim izvjesno samo u manjem obimu i za značajne i velike klijente koje treba osigurati.

[21] Global Reinsurance, 14.12.2017
[22] Osiguranje.hr, 09.10.2017
[23] Poslovni dnevnik, 02.02.2018.
[24] https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf
[25] https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

U SAD se i na saveznom nivou razmatra donošenje regulative u oblasti osiguranja kojom će se obuhvatiti sigurnost podataka specifičnih za industriju osiguranja.

ŠTA SE MOŽE OSIGURATI

Industrija osiguranja je sve manje podložna standardiziranju, čak i kada bi to bilo potpuno opravdano. Osiguranje cyber rizika, čini mi se, je takva oblast gdje bi značajan stepen standardizacije bio prednost, no i mišljenje da se za svakog klijenta treba napraviti ponuda koja mu odgovara je legitimno. No, za veliki broj društava koja ne spadaju u red velikih uglavnom će uvjeti osiguranja i isključenja biti zbunjujuća i ponude od strane nekoliko osiguravača teško uporedive.

No najprije pogledajmo s kakvim rizicima se suočavaju privredna društva i vlade i njihove institucije u slučaju cyber napada:

- Zakonska odgovornost
- Proboj kompjuterske sigurnosti
- Narušavanje privatnosti
- Cyber krađa
- Cyber špijunaža i industrijska špijunaža
- Cyber ucjene
- Cyber terorizam
- Gubitak prihoda
- Namirenje troškova
- Narušeni ugled
- Kontinuitet poslovanja/prekidi u lancu snabdijevanja
- Cyber prijetnje infrastrukturi[26]

Allianz upozorava da utjecaj prekida poslovanja prouzrokovan tehničkom greškom često bude podcijenjen u odnosu na cyber napade, a također i gubitak reputacije nakon cyber incidenta[27].

Iako općenito postoji vjerovanje da stariji informatički uređaji mogu biti ranjiviji od novijih, nažalost moderni svijet pokazuje i ružnu stranu velikih korporacija koje namjerno ažuriraju

[26] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf
[27] http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

software za starije uređaje na način da ih usporavaju. I ovaj problem može utjecati na zatajenje ili lošiji rad starijih uređaja, makar oni bili potpuno funkcionalni. Uz to, dosta uređaja ima instalirani software koji se više ne podržava. Očito da moderni svijet prisiljava na kupovinu novih uređaja i novih software-a, te će svako za sebe morati donijeti odluku kako pristupiti rješavanju ovakvih problema.

Kako je Allianz jedno od najvećih svjetskih društava za osiguranje, nadam se da mi niko neće zamjeriti ili smatrati za reklamiranje to što ću navesti kakva osiguranja nude za cyber incidente, a prema njihovoj vrlo korisnoj brošuri A Guide to Cyber Risk[28]:

Cyber protect pruža:

Pokriće za proboj privatnosti i podataka – Troškovi odbrane i štete za koje su odgovorni Osiguranik ili vanjski pružatelj usluga, a koji proistječu iz gubitka podataka.

Pokriće prekida poslovanja i troškova obnove – Gubitak poslovnog prihoda (i troškova obnove) prouzrokovanih ciljanim napadom na kompjuterski sistem društva.

Pokriće za odštetne zahtjeve na osnovu sigurnosti mreže – Troškovi odbrane i štete za koje je Osiguranik dogovoran, a koji proistječu iz ciljanog cyber napada.

Pokriće odgovornosti po odštetnim zahtjevima zbog medija – Troškovi odbrane i štete za koje je Osiguranik odgovoran, a koji proistječu iz publiciranja ili emitiranja sadržaja digitalnih medija.

Pokriće troškova nametnutih od strane regulatora – Troškovi odbrane zbog zahtjeva postavljenog od strane regulatora, a koji proizilazi iz gubitka podataka.

Pokriće kazni i penala od strane regulatora – Novčane kazne i penali koje nametnu regulatori (u mjeri u kojoj su osigurljivi) a koji proizilaze iz gubitka podataka.

[28] http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf

Troškovi obavještavanja – U skladu sa zahtjevima po zakonu i od strane regulatora nakon gubitka podataka.

Troškovi odgovora – Naknade i troškovi za forenzičko istraživanje nakon gubitka podataka, identifikacija i prezervacija izgubljenih podataka, savjeti o zakonskim i regulatornim obavezama, određivanje obima obaveza naknade u ugovorima sa pružateljima usluga koji su treća strana, usluge kreditnog praćenja i druge akcije popravljanja situacije koje su neophodne nakon gubitka podataka.

Pokriće hakerske krađe – Naknada za ukradena sredstva usljed zlonamjerne aktivnosti treće strane.

Pokriće cyber ucjena – Naknada za rješenje stvarne prijetnje u pogledu kompromitiranja Osiguranikovih podataka ili sistema.

E-plaćanja – Troškovi odbrane, štete i ugovorni penali u pogledu kršenja standarda sigurnosti podataka industrije platnih kartica.

Pokriće za krizno komuniciranje – Troškovi odnosa s javnošću panela stručnjaka radi ublažavanja bilo kakvog negativnog publiciteta iz pokrivenog slučaja.

Pokriće konsultantskih usluga – Troškovi IT stručnjaka da bi se odredio iznos i obim štete pokrivene po ovoj polici.

Cyber Protect premium pruža dodatno pokriće kao što je prošireni prekid poslovanja.

Cyber protect Premium Plus pruža pokriće zasnovano na Allianz Cyber Protect prema zahtjevima specifičnog posla.

U pokrićima cyber osiguranja koja se zasebno prodaju, fizičko oštećenje uobičajeno nije pokriveno. Često je fizička šteta koja proizilazi iz cyber napada isključena i po imovinskom osiguranju, te na ovo treba obratiti pažnju.

Allianz može nositi do 100 miliona EUR cyber pokrića, ali ujedno upozorava na opasnost kumuliranja rizika (npr. malware koji obuhvati veći broj osiguranika, ili proboj ili prestanak rada tzv. clouda, ukoliko se radi o velikom pružatelju usluga). Kako se cyber rizici razvijaju i mijenjaju, teško je napraviti model koji bi bio primjenjiv na cyber rizike i služio kao mjerilo izloženosti za pojedinog osiguravača.

No, postoje ipak scenariji koje je napravio Lloyd's skupa sa firmom Cyence pod nazivom „Counting the cost: Cyber exposure decoded“[29] koji ukazuju da prekid u pružanju usluga putem tzv. clouda može koštati od 4,6 milijardi USD za veliki događaj do 53,1 milijardu USD za ekstremno veliki događaj, a za masovni događaj ranjivosti softwarea raspon je od 9,7 milijardi USD za veliki događaj do 28,7 milijardi USD za ekstremno veliki događaj. Pri tome, scenariji ukazuju na nedostatak pokrića osiguranjem, gdje bi osigurane štete bile od 620 miliona USD do 8,1 milijardu USD za incident koji uključuje cloud, a od 762 miliona USD do 2,1 milijardu USD za masovni događaj ranjivosti softwarea[30].

No već sljedeći izvještaj Lloyd'sa, ovaj put u suradnji sa Air Worldwide („Cloud Down – The impacts on the US economy) procjenjuje da bi poslovi u SAD pretrpjeli 15 milijardi USD ekonomske štete (3 milijarde USD osigurane štete) ako bi jedan od vodećih pružatelja usluga clouda prestao raditi na tri do šest dana[31].

Također, na tržištu se javljaju i osiguranja direktora i zvaničnika (D&O), kojim se pokriva širok spektar odgovornosti direktora i zvaničnika jednog društva, uključujući i cyber rizike[32].

[29] Global Reinsurance, 17.07.2017
[30] Asia Insurance Review, 18.07.2017
[31] Global Reinsurance, 25.01.2018
[32] [32] https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

Većina društava za osiguranje preuzima cyber rizike i kao zasebno pokriće i kao dodatak postojećoj polici, posebno kao dodatak policama pokrića grešaka i propusta (E&O) i policama profesionalne odgovornosti (npr. D&O), ili policama opće odgovornosti, imovinskim ili policama dizajniranim za vlasnike poslova[33].

RAZUMIJEVANJE RIZIKA I TEŠKOĆE KOD PRODAJE CYBER OSIGURANJA

Osiguranje cyber rizika iziskuje dobro razumijevanje rizika koji se preuzimaju. Stoga je preuzimanje kod cyber rizika možda i važnije od preuzimanja kod nekih drugih vrsta osiguranja. Stoga ne čudi da je u jednoj anketi nedostatak shvatanja izloženosti naveden kao najveća prepreka prodaji cyber pokrića[34]. Jedan od brokera je prodajni proces nazvao vođenjem bitke uzbrdo, sa informatičarima koji ne prihvataju mogućnost da njihovi sistemi mogu biti kompromitirani, dosta klijenata srednjeg nivoa odbijaju mogućnost da su izloženi, ili prema riziku imaju stav „nikad mi se to nije desilo“[35].

Značajan broj klijenata nije u mogućnosti dostaviti dodatnu dokumentaciju potrebnu za postupak preuzimanja, a dostupne aplikacije su previše komplicirane za manje rizike[36].

Čini se da su brokeri značajan kanal za prodaju ovog osiguranja, te njihova specijalizacija u ovom smjeru može olakšati posao društvima za osiguranje.

Ipak, preporuka za društva za osiguranje koja su spremna dati veći kapacitet za cyber rizike je da uzmu u razmatranje kod pripreme proizvoda vanjske pružatelje usluga, definicije kompjuterskih sistema, kumule, mogućnosti odgovora osiguranika na proboj, kao i okidače za prekid poslovanja[37].

Stoga ne treba čuditi da je relativno mali broj društava za osiguranje spreman preuzimati cyber rizike.

---

[33] http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf
[34] http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf
[35] http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf
[36] http://www.partnerre.com/assets/uploads/docs/cyber-survey-results.pdf
[37] www.guycarp.com/.../AheadoftheCurve-UnderstandingEmergingRisks.pdf

REOSIGURANJE I IZAZOVI DIGITALNOG SVIJETA

Vidjeli smo ranije koji su to sve izazovi koje je informaciona tehnologija i ubrzana digitalizacija svih oblasti života donijela sa sobom.

Uloga reosiguranja je još uvijek, rekli bismo, u razvoju i to ranom. Jasno je da je kapacitet koji osiguranje nudi nedovoljan u odnosu na ukupne štete koje cyber rizici prourokuju u svijetu svake godine. Stoga je logično da se višak rizika prenese u reosiguranje. No, i u društvima za reosiguranje se javljaju iste dileme kao i u direktnom osiguranju. Neka društva za osiguranje su pokušala izbjeći isključenja cyber rizika, posebno u ugovorima o reosiguranju gdje je učešće cyber rizika bilo slučajno, dodatno na osnovno pokriće ili u neku ruku prikriveno. No, sa poboljšanjim shvatanjem cyber rizika, te sa pokušajima da se jasnije postave granice pokrića cyber rizika u direktnom osiguranju, i reosiguranje postaje otvorenije za preuzimanje cyber rizika. I nadalje dva izazova ostaju otvorena – nedostatak odgovarajućih podataka i kapaciteta za modeliranje kako bi se izračunala kumulirana izloženost i nedostatak znanja za preuzimanje koje bi omogućilo stvaranje i razvoj tržišta. Razvojem modela moći će se odrediti vjerojatnoća ostvarenja događaja i njegova veličina, no još uvijek podaci o dosadašnjim dešavanjima nisu dovoljni za to[38].

Arthur Wightman iz PwC-a, specijaliziran za osiguranje na Bermudama, je rekao da ukoliko se rizici općenito mjere svojom učestalošću i jačinom, onda cyber dolazi do kapaciteta koji zbunjuje[39]. Nije ni čudo, jer se događaji dešavaju često, i znaju biti vrlo veliki. No, on nadalje smatra da cyber rizik, ukoliko mu se pristupi kroz striktno preuzimanje i aktivno praćenje opasnosti, daje veliku mogućnost reosiguravačima da vode inovacije na tržištu i uhvate nove izvore prihoda na inače mekom tržištu. Strateška priroda ovih rizika znači da će priroda odgovora reosiguravača odrediti uspjeh, a u nekim slučajevima i opstanak učesnika na tržištu. Ukoliko reosiguravači uzmu pravi pristup nagrada će, po njemu, biti mogućnost uzimanja prihoda koji vremenom mogu postati jednaki ili čak i veći od vrijednosti premija za prirodne opasnosti[40].

Procjena Aon-a je da je u 2015. tržište reosiguranja imalo premiju od 525 miliona USD po osnovu cyber rizika. Ot toga je oko 95% upisano na kvotnoj osnovi, što samo po sebi

[38] Inteligent Insurer, A New Age of Risk, November 2015
[39] Intelligent Insurer, Monte Carlo Today, 10.09.2017
[40] Intelligent Insurer, Monte Carlo Today, 10.09.2017

dovoljno govori o oprezu s kojim se ulazi u ove poslove, kako sa strane osiguravača, tako i reosiguravača. Nekih 15 reosiguravača aktivno su preuzimali cyber rizike kroz zasebne ugovore, a taj broj raste. Neki od reosiguravača su bili aktivni 10-tak godina na polju reosiguranja cyber rizika, a nude učešće od 20-30% na kvotnoj osnovi. Ipak, ostaju konzervativni u pogledu njihove ukupne izloženosti cyber rizicima i često zahtijevaju ograničenja po štetnom događaju za prekid poslovanja. Neka društva koja su relativno nedavno počela s preuzimanjem cyber rizika, čak i kad su voljna da daju ponudu, uglavnom ograničavaju svoje učešće na ispod 20%. Iako najveći dio premije osiguranja cyber rizika potječe iz SAD, značajan dio reosiguranja je plasiran van SAD, prvenstveno u Londonu i Bermudama[41].

O oprezu s kojim reosiguranje pristupa preuzimanju cyber rizika govori i poziv Christiana Mumenthalera, direktora Swiss Re-a, vladama da se uključe i podrže industriju u pogledu cyber rizika, gdje reosiguravači žele biti manje opterećeni. Na taj način bi vlade pomogle industriji osiguranja i reosiguranja da izbjegnu akumulaciju rizika i preveliku izloženost. Cyber rizike je povezao s terorizmom, te smatra kako bi pristup vlasti i kod cyber rizika trebao biti jednak onom kod pitanja šteta od terorizma. Ranije je iskazivao skepticizam u pogledu cyber rizika, smatrajući ih vjerojatno neosigurljivim[42], ali očito da ne bježe od preuzimanja ovih rizika.

Jedan od rijetkih dokumenata koji se dotiče pitanja reosiguranja cyber rizika je i Cyber Risks and Reinsurance iz 2016. Simona Cooka, preuzimača reosiguranja u XL Catlinu[43]. U njemu se navodi da je njihov pristup preuzimanju ovakvih rizika u potpunosti konzistentan. Žele znati imali li klijent posebno određenog preuzimača za cyber rizike, vlastiti tekst police i pokrića, te obrazac ponude. Također, poznaje li kakvi su zahtjevi u pogledu obavještavanja i zakoni na teritorijima koje žele pokriti. Bitna stavka je posjeduje li društvo zadovoljavajuće mogućnosti u pogledu odštetnih zahtjeva uključujući kreditni monitoring i forenziku podataka. Uz to, uključuju i pitanja upravljanja krizom i štetama.

Kao naredni izazov vidi nedostatak odgovarajućih isključenja za cyber rizike. Kako se cyber kriminal stalno mijenja, danas postavljeno isključenje već za šest mjeseci može biti prevaziđeno.

[41] http://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
[42] https://www.reinsurancene.ws/swiss-re-ceo-calls-government-support-cyber-risks/
[43] http://xlcatlin.com/fast-fast-forward/articles/cyber-risks-and-reinsurance

Na stvarnom primjeru pokrića kojeg smo plasirali, reosiguranje uključuje franšizu koja je iskazana i monetarno i vremenski. Limit je dat agregatno. Pokriće isključuje SAD i Kanadu. Prijenosni uređaji poput diskova, traka, USB ili flash memorija su isključeni iz pokrića, ukoliko nisu enkriptirani. Događaj se mora prijaviti u roku od 60 dana od otkrivanja. Neprofesionalna usluga je apsolutno isključenje. Gubici zbog fluktuiranja tržišta su isključeni. Pokriće je proporcionalno.

Ostali uvjeti su uobičajeni i kod reosiguranja drugih rizika.

Na kraju možemo zaključiti da cyber rizici pružaju velike mogućnosti za razvoj osiguranja i reosiguranja, ali također i da donose mnoštvo nepoznanica te da procjeni rizika i preuzimanju treba prisutpiti sa velikom opreznošću i uz potrebno poznavanje problematike.

Zlatan Filipović

Juni 2018.

(Tekst rađen za potrebe časopisa Svijet osiguranja u kojem je i objavljen te Okruglog stola o reosiguranju na SorS-u 2018.)