SorS

31. susret
osiguravača i
reosiguravača
Sarajevo

Mr. sc. BRANKO PAVLOVIĆ, dipl. ing. el.*
VESNA MINIĆ PAVLOVIĆ, dipl. mat.**

POLISA SAJBER OSIGURANJA KAO VAKCINA PROTIV POVEĆANE IT RANJIVOSTI

Sažetak

Popularnost i masovnost rada od kuće, koju je uslovila pandemija, donosi kompanijama nove IT rizike i pojačava brigu zbog povećanja intenziteta poznatih rizika, kao što su npr. virusi, ransomware, phishing i slično. Postoje objektivne okolnosti koje utiču na niži nivo IT bezbednosti rada zaposlenih nego inače. Pojedini zaposleni su prinuđeni da koriste sopstvenu računarsku opremu i vezu ka Internetu prilikom rada od kuće. Na taj način izlažu kompanijske podatke raznim sajber opasnostima, jer kućni kompjuteri po pravilu nemaju ažuran anti-virus softver, niti zakrpe operativnog sistema. Takođe, poslovni podaci koje šalju običnom, nekriptovanom elektronskom poštom putem Interneta, mogu biti presretnuti i kompromitovani. Zaposleni koji imaju prenosne računare često dolaze u iskušenje da rad od kuće pretvore u rad iz kafića ili sa plaže i pri tom koriste javne Wi-Fi mreže što nosi veliki rizik od hakerskog napada i gubitka ličnih ili kompanijskih podataka.

U novim okolnostima, u cilju zaštite od rizika rada od kuće, poslodavci bi trebalo da što pre obezbede zaposlenima specifične smernice za podizanje svesti o sajber bezbednosti i obuku namenjenu zaštiti od pomenutih potencijalnih rizika. Ipak sve to nije dovoljna zaštita, pa je polisa sajber osiguranja jedina prava prevencija za velike finansijske gubitke kompanije usled povećanih IT rizika usled i nakon pandemije.

Ključne reči: sajber osiguranje, IT rizici, virus

* Globos osiguranje a.d.o., kontakt: pavlovic.branko@gmail.com
** Generali osiguranje Srbija a.d.o., kontakt: vesna.minic.pavlovic@generali.rs

Summary

The popularity and mass work from home, which was caused by the pandemic, brings new IT risks to companies and increases the concern due to the increase in the intensity of known risks, such as, e.g., viruses, ransomware, phishing, and the like. There are objective circumstances that affect the lower level of IT security of employees than usual. Some employees are forced to use their computer equipment and Internet connection when working from home. In that way, they expose company data to various cyber hazards because home computers, as a rule, do not have up-to-date antivirus software or operating system patches. Also, business data sent by plain, unencrypted e-mail over the Internet can be intercepted and compromised. Employees who have laptops are often tempted to turn work from home into work from a coffee shop or the beach while using public Wi-Fi networks, which carries a high risk of hacker attack and personal or company data loss.

In the new circumstances, to protect against the risks of working from home, employers should provide employees as soon as possible with specific guidelines for raising awareness about cybersecurity and training designed to protect against these potential risks. However, all this is not enough protection, so the cyber insurance policy is the only real prevention for significant financial losses of the company due to increased IT risks due to the pandemic.

Keywords: Cyber insurance, IT risks, virus

Uvod

Popularnost i učestalost rada od kuće, masovna upotreba mobilnih uređaja i konstantni napredak infrastrukture pojačano izlažu i pojedinca i kompanije IT rizicima, kao što su npr. virusi, ransomware, phishing i slično. Onoliko koliko je kompanija sposobna da se odupre pretnjama i napadima ovih malicioznih programa, toliko je IT bezbedna. Danas svaki pojedinac koji koristi elektronske uređaje i Internet suočen je sa ovim izazovom. Međutim IT bezbednost je mnogo veći i složeniji zadatak koji kompanije treba da reše, kako bi osigurale svakog zaposlenog i kompaniju u celini.

IT bezbednost je skup mera koje omogućavaju da podaci kojima se rukuje budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti poverljivost, integritet i raspoloživost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica.

Kada se govori o poverljivosti podataka, govori se o zaštiti od izlaganja neovlašćenim licima. Svaka informacija koju kompanija poseduje ima vrednost, posebno u današnjem svetu. Bilo da se radi o finansijskim podacima, brojevima kreditnih kartica, poslovnim tajnama ili pravnim dokumentima, sve zahteva odgovarajuću poverljivost. Drugim rečima, samo ljudi koji su za to ovlašćeni

mogu imati pristup odgovarajućim podacima. Najčešći se sajber napadi odnose baš na kršenje ovog pravila. Primeri velikih svetskih kompanija koje su bile mete ovakvih napada u 2020. godini i suočile se sa krađom klijentskih podataka su Marriott hoteli, EasyJet, Zoom, itd.[1]

Integritet podrazumeva očuvanost izvornog sadržaja i kompletnost podatka. To znači da se podaci ne mogu menjati na neovlašćen način. Na primer, ukoliko bi napadač narušio integritet podataka, bilo u izvornoj bazi podataka ili presretanjem sadržaja od izvora do konačnog izveštaja koji se prezentuje korisniku, posledica bi mogla biti da menadžment kompanije donese loše odluke na osnovu pogrešnih informacija ili da prezentovan sadržaj bude kompromitujući po kompaniju ili da podaci jednostavno postanu neupotrebljivi. Narušavanje integriteta je najteže prepoznati, jer se najčešće izvodi tako da podaci ne budu dramatično izmenjeni već dovoljno da izazovu željenu reakciju kompanije.

Raspoloživost je svojstvo podataka da budu dostupni i upotrebljivi na zahtev ovlašćenih lica onda kada su im potrebni. Ova osobina takođe ima veliku vrednost i često je povezana sa napadima koji izazivaju blokiranje rada informacionog sistema. Na taj način kompaniji je zaustavljeno ili značajno otežano funkcionisanje dok se sistem ne oporavi, a prekid kontinuiteta poslovanja nužno izaziva finansijske gubitke.

Evolucija informacione bezbednosti

Već nekoliko decenija u nazad, bezbednost informacionog sistema je važna oblast, ali je u početku bila značajno jednostavnija i više fokusirana na fizičku bezbednost opreme.

Tokom šezdesetih godina prošlog veka kompanije postaju svesne da je potrebno da zaštite svoje računare. U to vreme nije bilo Interneta ili mreže pa je sigurnost bila, uglavnom, usredsređena na fizičke mere zaštite i sprečavanje pristupa ljudima koji su imali dovoljno znanja u radu na računaru. Da bi se to postiglo, uređajima su dodavane lozinke i višestruki slojevi sigurnosne zaštite. Osim toga, primenjivane su protivpožarne mere, kako bi se podaci što kompletnije zaštitili.

Istorija sajber bezbednosti počinje sedamdesetih godina istraživačkim projektom ARPANET[2] (eng. The Advanced Research Projects Agency Network) koji je preteča Interneta. ARPANET je osmišljen kao vojni projekat. Početna ideja je bila da se povežu američke vojne baze. Kasnije, uvidevši mogućnosti ovog projekta, ideja o povezivanju samo vojnih baza je prerasla u ekonomski isplativu investiciju koja se danas naziva jedinstvenim imenom Internet. Istraživač po imenu Bob Thomas stvorio je računarski program koji je mogao da se kreće po

1 http://www.keepnetlabs.com/the-biggest-data-breaches-in-the-first-half-of-2020

2 Featherly, K. (2021). *ARPANET United States defense program*. www.britannica.com/topic/ARPANET

ARPANET-ovoj mreži, ostavljajući mali trag gde god bi prošao. Program je nazvao Creeper, zbog odštampane poruke koja je ostajala prilikom putovanja mrežom: „Ja sam Creeper: Uhvati me ako možeš!“. Nekoliko godina kasnije, Raymond Samuel Tomlinson, čovek koji je izmislio elektronsku poštu, dizajnirao je program koji je Creeper podigao na viši nivo, čineći ga samoreplicirajućim i prvim računarskim crvom. Tada je napisao i drugi program pod nazivom Reaper koji je jurio Creeper i brisao ga, pružajući prvi primer antivirusnog softvera. Programi Tomasa i Tomlinsona su bili eksperimentalni radovi entuzijasta, ali zapravo su služili veoma važnoj svrsi, za otkrivanje brojnih nedostataka u mrežnoj bezbednosti ARPANET-a. To je bio veliki izazov u to vreme, jer su mnoge organizacije i vlade povezivale svoje računare putem telefonskih linija, kako bi stvorile sopstvene mreže. Određene grupe ljudi prepoznale su priliku da se uvuku u ove mreže i ukradu važne podatke. Tako su nastali prvi hakeri.

Tokom godina koje su usledile računari su počeli da se povezuju sve više, računarski virusi postajali su sve napredniji, a sistemi za zaštitu informacija nisu mogli da prate stalni napredak inovativnih pristupa hakovanju.

Posebno važna je 1987. godina, jer je to trenutak nastanka prvih komercijalnih antivirus programa. Kako postoje konkurentske tvrdnje ko je zaista prvi proizveo antivirus program, može se reći da su sledeće tri inicijative začetnici ove neizostavne komponente svakog pametnog elektronskog uređaja današnjice.

Andreas Luning je započeo ovu misiju tako što je pronašao dva virusa na disketi za oporavak operativnog sistema svog kompjuteru Atari ST. On je napisao program koji detektuje i uklanja virus i o tome obavestio svog budućeg poslovnog partnera Kai Figgea. Ubrzo nakon toga njihova kompanija G Data proizvela je prvi komercijalni antivirus AntiVirenKit (AVK).

Iste godine dva Čehoslovaka Peter Paško i Miroslav Trnka kreirali su prvu verziju antivirus programa NOD, što je akronim od češkog naziva „Nemocnica na Okraji Disku“, a u prevodu znači „Bolnica na kraju diska“. Kasnije je slovačka kompanija ESET nastavila proizvodnju ovog programa poznatog danas kao ESET NOD32.

John McAfee bio je englesko-američki programer i biznismen, koji je sedamdesetih godina bio zaposlen kao programer u NASA Institutu za proučavanje svemira. Kasnije je promenio još nekoliko kompanija gde je od programera izrastao u softver arhitektu i konsultanta. On je 1987. godine osnovao kompaniju McAfee Associates koja se bavila proizvodnjom kompjuterskog antivirus programa. Osnivač je ubrzo posle toga napustio kompaniju, ali je McAfee postao lider u oblasti bezbednosnog softvera.

Devedesete su donele novi koncept zaštite podataka pomoću softvera poznatog kao zaštitni zid (eng. firewall). Kako je Internet postao dostupan javnosti, sve više ljudi je počelo da stavlja svoje lične podatke na udaljene servere i deli informacije preko mreže. Organizovane kriminalne grupe su to videle kao potencijalni izvor prihoda i počele da kradu podatke od ljudi i organizacija. Sredinom

devedesetih pretnje mrežnoj bezbednosti eksponencijalno su se povećale tako da su zaštitni zidovi i antivirusni programi morali masovno da se proizvode, da bi zaštitili javnost. NASA-in istraživač stvorio je prvi dizajn programa zaštitnog zida, nakon napada na računarski sistem u njihovoj bazi u Kaliforniji. Tim eksperata je istraživao i konačno stvorio virtuelni zaštitni zid po uzoru na fizičke strukture koje sprečavaju širenje stvarnih požara u zgradama ili objektima.

Međutim, dok su ovi zaštitni zidovi i antivirusni programi na neki način minimizirali rizik od napada, računarski virusi i crvi su dolazili još brže, tako da su hakeri u to vreme ipak imali prednost.

Početkom dvehiljaditih vlasti su počele da suzbijaju hakovanje, pomoću mnogo strožije kaznene politike, uključujući zatvor i velike novčane kazne. Bezbednost informacija nastavila je da napreduje, kako je rasla i popularnost Interneta. Međutim, i hakeri su nastavili da pojačavaju svoje prisustvo, tako da su brzo postali sposobni da stvore viruse koji nisu namenjeni samo napadu određene organizacije, već i čitavih gradova, država, pa čak i kontinenata.

Dvehiljadedesete su era velikih krađa podataka. Zbog stalnog napretka tehnologije, hakovanje je postajalo sve komplikovanije tokom godina koje su sledile, ali se i sigurnost informacija neprestano poboljšavala, tako da su mnoge kompanije implementirale širok spektar alata za sprečavanje i ublažavanje napada.

Ovaj trend se nastavlja i danas. U prilog tome govori statistika učestalosti ransomwere napada. U toku 2019. godine, svake četrnaeste sekunde neka kompanija je bila žrtva ransomware napada, dok je predviđanje da će se 2021. godine ta učestalost pojačati na svakih jedanaest sekundi sa očekivanom štetom od oko 20 milijardi dolara.[3]

Sajber bezbednost

Kao odgovor na veliku izloženost poslovanja ovim rizicima u digitalnom svetu, poslednjih godina snažno se razvija jedna grana informacione bezbednosti – sajber bezbednost. Dok se klasična IT bezbednost bavi svim aspektima zaštite informacionog sistema, počevši od fizičke bezbednosti opreme i mreže, zaštite od nenamernih ili namernih oštećenja sistema pa do zaštite informacija, sajber bezbednost je njen podskup koji je posebno fokusiran na zaštitu podataka, uređaja i mreže od zlonamernih uticaja koji dolaze digitalnim putem. Kao glavni akteri ove borbe su, sa jedne strane sajber napadači poznati kao hakeri, dok su sa druge strane čitavi timovi koje kompanije razvijaju kako bi što delotvornije štitili informacione sisteme. Sajber bezbednost nije više samo stvar IT stručnjaka. To je jedan holistički koncept koji podrazumeva spremnost čitave organizacije, kako u tehnološkom smislu tako i u obrazovnom usavršavanju svakog pojedinca.

3 Shakeel, I. (2016). *Evulution in the World of Cyber Crime*. https://resources.infosecinstitute.com/topic/evolution-in-the-world-of-cyber-crime

Sajber bezbednost predstavlja zaštitu sistema, mreža i programa od digitalnih napada čiji je cilj uglavnom pristup, izmena ili uništenje poverljivih podataka, zatim iznuda novca od korisnika, ili prekid normalnih poslovnih procesa.

Sajber napadači – hakeri

Kao i svaki drugi oblik kriminala i sajber kriminal je traženje zadovoljenja lične potrebe kroz socijalno disfunkcionalno ponašanje. Motivi mogu biti različiti, od finansijskih i reparacionih do ideoloških. U zavisnosti od vrste motiva razlikuju se oblici ili kategorije hakovanja.

Haktivizam (eng. hacktivism) je zloupotreba kompjutera i kompjuterskih mreža radi promovisanja neke političke organizacije ili socijalne promene, često povezane sa slobodom govora, ljudskim pravima ili slobodom informacija. Posebno poznate organizacije ovog tipa su WikiLeaks i Anonymous.

Sajber kriminal podrazumeva krađu finansijskih informacija, krađu identiteta ili neovlašćeno pristupanje računarskim sistemima.

Insajdersko odavanje informacija je čest slučaj hakovanja. U pitanju su zaposleni ili bivši zaposleni koji pokušava neovlašćeno da priđu kompanijskim podacima i sistemima kako bi ih oštetili. Obično je podržan spoljašnjim interesnim stranama radi postizanja finansijske koristi ili iznuđivanja.

Sajber ratovanje je aktivnost podstaknuta državnom organizacijom u nameri da probije odbranu nacionalnih kompjutera druge države, kako bi izazvali štetu ili prekid rada.[4]

Sajber terorizam ima osobinu da koristi kompjutere, mrežu i javni Internet, kako bi napravio razaranje i štetu radi postizanja političkih ciljeva kroz zastrašivanje.

Sajber špijunaža ima za cilj da dobije i čuva zaštićene osetljive kompanijske informacije konkurencije, kao što su poslovne tajne, klijentski podaci, finansijske informacije i marketinške informacije.

Posledice napada hakera

Bilo koji od ovih motiva napada izazivaju tri osnovne posledice kod žrtve. Ekonomski uticaj je najčešća i uvek prisutna posledica, zatim reputacioni pad i na kraju regulatorni problemi.

Finansijski gubici, zbog napada hakera, sastoje se od troškova za oporavak opreme i podataka kao i troškova prekida poslovanja. Ukoliko je u pitanju ransomwer napad, dodatno postoje i troškovi otkupa kako bi napadač otključao napadnut računar.

Povređena reputacija dovodi do gubitka klijenata i poverenja zainteresovanih strana, što posledično utiče na slabljenje brenda i narušavanje biznisa u celini. Na taj način i napad na reputaciju kompanije takodje ima i značajan finansijski uticaj.

4 Sheldon, J. (2016). *Cyberwar*. www.britannica.com/topic/cyberwar

Kompanija koja se nije oduprela sajber napadu, najčešće je izložena nekoj vrsti penala od strane regulatora. Osim toga biznis je u obavezi da se u što kraćem roku uskladi sa novom regulativom i implementira odgovarajuće bezbednosne mere. Takodje, sve te aktivnosti zahtevaju ozbiljne investicije.

Tehnike sajber napada

Hakeri retko kada primenjuju jednu tehniku prilikom izvođenja napada. Najčešće se napad odvija u nekoliko faza kombinujući različite tehnike koje nisu isključivo programerske prirode. Neizostavni deo je i psihološka ili socijalna priprema gde napadač najpre dobro prouči slabosti kompanije u kadrovskom i organizacionom pogledu, što predstavlja komponentu poznatu kao socijalni inženjering.

Kada govorimo isključivo o programerskim veštinama, sledećih 5 tehnika je najzastupljenije u današnjim sajber napadima.

Malware je maliciozni softver koji napada računarsku mrežu i uređaje na mreži pokušavajući da dospe u sam informacioni sistem. Kada konačno dostigne ciljnu poziciju malware obično blokira neke ključne komponente sistema ili instalira sledeći malware koji može dodatno oštetiti sistem. Malware napad se odvija kroz nekoliko faza. Najpre jednostavan fajl nekako dospe na mašinu „domaćina", bilo da je korisnik računara otvorio maliciozni mail sa malicioznim fajlom ili kliknuo na link ili posetio web sajt na kome je taj fajl bio sakriven i čekao žrtvu. Nakon što sistem prihvati uljeza, automatski se pokreće proces preuzimanja napadačevih kompletnih datoteka gde se nalaze alati za napad sistema. Kada je kompletan set alata isporučen na napadnuti računar, tada je sve spremno da napad može da počne. Malware uspostavlja vezu sa napadačem i šalje konfirmaciju da napadnuti kompjuter može udaljeno da se kontroliše. Tada napadač stupa na scenu i preduzima akcije kao što su krađa ili uništenje podataka, zaključavanje sistema itd.

Paleta malwarea je jako bogata. Tu spadaju virusi, trojanci, crvi, koinmajnersi i trenutno posebno dominantni ransomware.

Kompjuterski virusi, kao i ljudski virusi, imaju osobinu da jako lako mutiraju i jako brzo se prenose sa mašine na mašinu u jednoj računarskoj mreži. Iako dugo postoje, antivirus programi na dnevnom nivou moraju ažurirati svoje baze prepoznatih virusa kako bi pružali adekvatnu zaštitu.[5]

Crvi su slični virusima, vrlo brzo se šire kroz mrežu i imaju sličan ciljni zadatak. Međutim, glavna razlika je što virus mora nekako biti aktiviran od strane napadnutog računara, tako što korisnik nešto otvori ili klikne, dok je crv samoaktivirajući softver i nije potreban nikakav okidač kako bi njegova aktivnost krenula. Iz tog razloga on se još brže širi od virusa i često dospe na mašinu potpuno neopaženo tako što pronađe slabost sistema u pozadini.

5 Scientific American (2001). *When did the term 'computer virus' arise?* www.scientificamerican.com/article/when-did-the-term-compute

Trojanci imaju tu osobinu da često deluju kao legitiman softver, ali u nekom trenutku mogu da se aktiviraju i preuzmu kontrolu nad sistemom. Oni se ne repliciraju kao virusi ali mogu imati jako velike posledice u oštećenja podataka ili blokiranju rada same mašine.

Coinminersi su postali aktuelni dolaskom kriptovaluta i rudarenja. Zapravo je reč o softveru koji nema zadatak da uništi svog domaćina, međutim on koristi, ili bolje reći krade, snagu mašine koju zarazi (procesor, memoriju, mrežne resurse) da bi rudario kriptovalutu za nečiji tuđi račun.

Posebnu pažnju poslednjih godina privlači malware pod imenom ransomware. Koncept ovog napada je da napadač preuzme kontrolu nad sistemom, a zatim zaključa mašinu tako što uradi enkripciju fajlova. Da bi fajlovi i mašina ponovo postali operabilni, haker zahteva određeni iznos novca za otkup, kako bi dao instrukcije i šifru za otključavanje sistema. Za ovu vrstu napada je karakteristično da je obavezno inicirana nekom od tehnika socijalnog inženjeringa.

Kako je u našem digitalnom dobu sve više podataka u oblaku, broj napada i uspeh ransomware napada raste. Otprilike 58% žrtava ransomwarea platilo je otkup u 2020. godini, u poređenju sa 39% koji je plaćen 2017. godine.[6] Cena otkupa kreće se od nekoliko stotina do nekoliko miliona dolara i plaća se nekom od kriptovaluta npr. bitcoinom. Među ovim napadima najpoznatiji je svetski napad WannaCry u maju 2017. godine, a ciljna grupa su bili računari sa starijim Microsoft operativnim sistemom. Iako je Microsoft u međuvremenu objavio zakrpe kojima su mašine bile zaštićene od ovakvog napada, ipak je postojao ogroman broj mašina koje, zbog komplikovanih procedura ažuriranja operativnog sistema, nisu bile zaštićene. Procena je da je bilo zaraženo više od 200.000 računara u 150 zemalja, a ukupna šteta kretala se od nekoliko stotina miliona do milijardu dolara. U toku 2020. godine ransomware nastavlja da napreduje pa su najpoznatiji napadi bili NetWalker, REvil, Maze i WastedLocker.

DDoS (eng. Distributed Denial of Service) je jedna od starijih tehnika napada. Napadač pokušava da blokira rad sistema tako što odjednom pošalje ogroman broj zahteva serveru koja pruža neku on line uslugu. Na taj način server postaje prebukiran zahtevima pa mu padaju performanse dok na kraju biva potpuno blokiran i nije u mogućnosti da prihvati bilo kakav novi zahtev.

Čovek u sredini (eng. Man in the middle) je vrsta napada gde napadač presretne online komunikaciju između dve strane i to iskoristi da dobije informacije koje su u toj komunikaciji razmenjene.

Probijanje lozinke je takođe dugo primenjivana tehnika. Haker pokušava da dobije pristup nekim resursima tako što otkrije lozinku. Načini kako to radi se različiti, od pogađanja lozinke na osnovu činjenica o osobi koja je vlasnik, isprobavanja često korišćenih lozinki (npr. admin, test, sa...), pravljenja svih

6 Johnson, J. (2021). *Number of ransomware attacks per year 2014-2020*. www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide

mogućih kombinacija brojeva, slova i karaktera do pokušaja prevare korisnika da sami daju svoju lozinku.

Botnet (eng. robot-network) je tehnika napada koja podrazumeva stvaranje velikog broja zaraženih kompjutera kojima upravlja napadač. Na taj način on kreira tzv. „vojsku zombija" kojom upravlja radi daljeg napada na neku sledeću žrtvu. Ovo je često pripremna faza za izvođenje DDoS napada velikih razmera.

Socijalni inženjering je set tehnika kojima se napadaju korisnici sistema kako bi odali lozinke, poverljive podatke ili otvorili prolaz za maliciozne programe. Ova oblast podrazumeva psihološku manipulaciju žrtve, kako bi kombinujući uz to tehnička znanja, napadač došao do konačnog cilja. Najpoznatija tehnika u ovoj oblasti je phishing.

Phishing ili prevara krađom identiteta je napad u kojem se meta ili ciljevi kontaktiraju elektronskom poštom ili nekim internet sadržajem, od strane nekoga ko se predstavlja kao legitimna institucija, da bi namamio pojedince da pruže osetljive lične podatke. To mogu biti podaci za identifikaciju u informacionom sistemu, detalji bankarske i kreditne kartice i lozinke. Informacije se zatim koriste za pristup važnim resursima i mogu rezultirati krađom identiteta i finansijskim gubitkom.

Postoji i opcija kontaktiranja žrtve telefonom, pri čemu je proces i konačan cilj isti. Ukoliko je pojedinac kontaktiran pozivom, to se onda naziva Vishing (eng. voice phishing). Ukoliko je kontaktiranje obavljeno SMSom, tu vrstu napada nazivamo Smishing (SMS phishing)

Phising, ili u prevodu pecanje, patentiran je 1995. godine u američkoj kompaniji America On Line (AOL) koja je bila broj jedan provajder za Internet usluge.[7] Tamo su hakeri na početku kreirali lažne naloge generišući random brojeve kreditnih kartica, a zatim koristeći te naloge počeli da napadaju ostale korisnike sistema. Predstavili bi se kao zaposleni kompanije tražeći da im korisnici potvrde svoje korisničke podatke i slično. Kako je to bilo nepoznato do tada, mnogo ljudi je naselo na prevaru i kompromitovalo svoje podatke. Pecanje se nije mnogo promenilo od njegovog lansiranja u AOL-u do danas. Međutim, 2001. godine hakeri su pažnju usmerili na sisteme za plaćanje putem Interneta. Iako se prvi napad, koji je bio na E-Gold u junu 2001. godine, nije smatrao uspešnim, zasadio je važno seme. Krajem 2003. hakeri su registrovali desetine domena koji su izgledali vrlo slično kao legitimni sajtovi poput eBaya i PayPala. Koristili su programe za crve elektronske pošte da bi lažno slali poštu kupcima PayPala. Te kupce vodili su do lažnih lokacija i tražili da ažuriraju detalje o kreditnoj kartici i druge podatke za identifikaciju. Početkom 2004. počeli su napadi na bankarske sajtove i njihove kupce. Između maja 2004. i maja 2005. godine, oko 1,2 miliona korisnika u SAD je pretrpelo gubitke prouzrokovane krađom identiteta, što ukupno iznosi približno 929 miliona dolara. Organizacije godišnje gube oko 2 milijarde dolara zbog phishinga.

7 www.phishing.org

Posebno popularna tehnika je postavljanje mamaca (eng. baiting). Mamac može biti neka besplatna otvorena mreža ili sajt za besplatno preuzimanje zanimljivog sadržaja ili USB uređaj koji je neko ostavio ili besplatno deli na javnom mestu. Onog trenutka kada se maliciozni fajl prebaci na mašinu žrtve, bilo preko mreže ili USB memorije, ta maština postaje zaražena i dozvoljava napadaču da nad njom preuzme kontrolu.

Na kraju, čak i digitalno smeće kao što je stari smartfon ili laptop mogu biti izvori informacija za hakere. Ta oblast se često naziva ronjenje po kontejnerima (eng. dumpster diving). Ukoliko se uređaji koji se više ne koriste neadekvatno odlažu, bez kompletnog brisanja sadržaja sa diskova, hakeri vrlo jednostavno dolaze do naloga i lozinki, kontakt listi iz telefona i raznih drugih korisnih dokumenata. Ova tehnika nije samo stvar sajber bezbednosti već i fizičke bezbednosti, ali je često prisutna u mnogom napadima baziranim na socijalnom inženjeringu. Poznat slučaj korišćenja ove tehnike je Jerry Schneider iz Kalifornije koji se obogatio skupljajući elektronski otpad iz kontejnera Pacific Bell Telephone Company koja pruža usluge telefonije u Kaliforniji.

Odgovor kompanija na IT ranjivosti

Kako bi se odbranile od mnogobrojnih napadača, kompanije moraju da obezbede kompleksne sisteme odbrane svoje imovine. Organizacije razvijaju i sprovode politiku bezbednosti informacija kako bi nametnule jedinstveni skup pravila za rukovanje i zaštitu osnovnih podataka. Politika treba da se odnosi na celokupnu IT strukturu i sve korisnike u mreži. Određuje ko ima pristup različitim vrstama podataka, kako se identitet potvrđuje i koje se metode koriste za obezbeđivanje informacija u svakom trenutku. Dobra politika zaštite informacija takođe treba da sadrži etičke i zakonske odgovornosti kompanije i njenih zaposlenih kada je reč o zaštiti podataka klijenata.

Većina politika bezbednosti informacija usredsređena je na zaštitu tri ključna aspekta: poverljivost, integritet i dostupnost (eng. Confidentiality, Integrity, Availability). Zato se često ovo naziva CIA modelom informacione sigurnosti.

Politika bezbednosti informacija je krovni dokument koji definiše smernice a njega prati set procedura, uputstava i vodiča koji detaljno opisuju svaki segment zaštite: uspostavljanje organizacione strukture, identifikacija i klasifikacija informacija, zaštita nosača podataka, bezbednost rada na daljinu, kontrola pristupa sistemu, enkripcija, fizička zaštita, zaštita od zlonamernog softvera, zaštita komunikacionih kanala, prevencija i reagovanje na bezbednosne incidente, kontinuitet obavljanja posla i druge.[8]

Uspostavljeni procesi zaštite imaju neizostavno dve komponente, jedna je tehnička opremljenost a druga edukovani i obučeni zaposleni. Sajber bezbednost

8 Krivokapić, D., Petrovski, A., Malinović, S. (2017). *Mere za zaštitu IKT sistema od posebnog značaja*. Share fondacija: Vodič za IKT sisteme od posebnog značaja, informaciona bezbednost, p. 19.

se u praksi sprovodi se kroz tri osnovne faze, identifikacija potencijalnih načina napada i zaštita imovine, detekcija i odbrana i na kraju oporavak sistema.

Za identifikaciju mogućih napada važno je imati kvalitetne i ažurne informacije o trenutnim aktivnostima hakera i pokušajima napada na kompanije sličnog profila ili članica grupe. Na osnovu toga koriguju se i ažuriraju mere zaštite, proveravaju pravila pristupa informacijama tako da svaki zaposleni imam minimum dozvola koje su mu potrebne za obavljanje posla, kontroliše se ažurnost odbrambenog softver na serverima, mrežnim uređajima, aplikacijama i bazama podataka i neizostavno sprovode obuke koje poboljšavaju razumevanje ovog problema.

Detekcija je proces koji se odvija u kontinuitetu tako što se neprekidno prati saobraćaj na mreži, primenjuje malware analiza i blagovremeno reaguje ukoliko se primeti neka anomalija. Reakcija na primećen napad treba da bude jako brza kako bi se blokirao dalji rad napadača, stopirali procesi koji vode daljem širenju problema i ublažile posledice.

Oporavak sistema je završna faza kada se rade provere da su sve funkcije oporavljene i da su propusti zbog kojih je došlo do napada sanirani, kako se ne bi dogodili slični incidenti.

Kultura sajber bezbednosti

Dugoročna strategija borbe protiv opasnosti koje vrebaju u IT svetu može biti stvaranje kulture sajber bezbednosti. Ovo je posvećenost zaštiti podataka u celoj organizaciji u kojoj su tehnologija, politike i procesi dizajnirani uzimajući u obzir bezbednosne pretnje. Stvaranje ove kulture nije lako. Bitno je da postoji strukturirani pristup kao na primer ISO 27001, međunarodni standard za informacionu sigurnost.

Praksa govori da je ipak jednostavnije postići tehničku spremnost nego zadovoljiti socijalnu komponentu. Ne retko se događa da kompanije koje su imale najmoderniju opremu za sajber zaštitu budu žrtve napada, tako što je neki zaposleni prekršio bezbednosne smernice a da toga nije bio svestan. Puno se ulaže u edukaciju svakog pojedinca, međutim to otežava činjenica da neki ljudi nemaju osnovnu digitalnu pismenost a ipak moraju da funkcionišu u digitalnom svetu. Osnovni principi sigurnog rada u informacionom sistemu moraju biti usvojeni, kako bi kompanija imala šansu da se odupre napadima. Primeri tih pravila, kod kojih najčešće dolazi do propusta su: odgovorno upravljanje nalozima i lozinkama (birati lozinke koje su dovoljno kompleksne da ih nije lako pogoditi, ne koristiti iste lozinke za različite vrste pristupa, nikome ne davati svoju lozinku i redovno menjati lozinke), adekvatno upravljanje uređajima (zaključavanje ekrana, ne pozajmljivanje uređaja drugima bez ličnog nadzora i redovno ažuriranje softvera operativnog sistema), siguran udaljeni rad i anti-phishing pravila (ne verovati nepoznatim korisnicima koji pokušavaju da uspostave komunikaciju, voditi

računa o „hitnim“ zahtevima jer se tako najčešće krije prevara, uvek pažljivo proveriti adresu pošiljaoca elektronske poruke).

Edukacija zaposlenih je ciklični proces koji zahteva kontinuitet i strpljenje. Kompanije su svesne da je potrebno još mnogo rada i vremena dok pravila sajber bezbednosti ne postanu ugrađena u sve procese kompanije, tako da ih svaki pojedinac obavlja na rutinskom nivou. Do tada će rad timova za IT bezbednost biti nepotpun, a kompanije konstantno imati nezanemarljiv rizik od sajber napada, koji nije adekvatno zbrinut.

Zna se da hakeri neće spavati dok organizacije sprovode digitalnu transformaciju i svoj biznis prebacuju na online i colud servise. Naprotiv, i oni će biti vredni i pronalaziti nove i inovativne načine za sledeće talase napada. Ono što ostaje kao rešenje je osiguranje od sajber napada. Jedino na taj način kompanije mogu biti sigurne da, čak i ako se ne odbrane od hakera, neće imati velike finansijske gubitke.

Istorijski razvoj sajber osiguranja

Sajber rizici su isključeni ili delimično pokriveni tradicionalnim osiguranjima imovine. Kod osiguranja stvari, ako je računar predmet osiguranja, uključeni su hard diskovi i programi koji su navedeni u ponudi osiguranja. Štete nastale usled gubitka podataka, prekida rada ili gubitka zarade mogu biti posebno ugovorene. Kod tradicionalnog osiguranja imovine, da bi ove štete bile pokrivene osiguranjem, moraju nastati kao posledica oštećenja ili uništenja hardvera. Na savremenom tržištu osiguranja postoje različite polise koje pokrivaju štete prouzrokovane nestankom, oštećenjem ili manipulacijom podataka i za slučajeve kada hardver nije oštećen.

Prvi ugovori za pokriće sajber rizika su zaključeni pre četrdesetak godine u SAD i obezbeđivali su naknadu za slučaj novčanih gubitaka nastalih usled 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.[9] Rizici su osiguravani bez obzira na uzrok koji je doveo do štete.

Na savremenom tržištu osiguranja sajber 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.

Veliki broj autora u svetu se bavio sajber osiguranjem u poslednjih dvadesetak godina. Bohme i Kataria su među prvima objavili rad[10] o sajber osiguranju 2006. godine u kome su dokazivali da tržište sajber osiguranja ne može da

9 Pak, J. (2014). *Osiguranje Internet rizika*. Međunarodna naučna konferencija Univerziteta Singidunum Sinteza, s. 71-76

10 Bohme, R., Kataria, G. (2006). *Models and Measures for Correlation in Cyber-insurance*. Workshop on Economics of Information Security – WIES

bude uspostavljeno u uslovima velike korelisanosti klijenata. Bandyopadhyay[11] je 2009. godine tvrdio da je premija sajber osiguranja obično viša nego što je potrebno za pokriće rizika, jer osiguravači precenjuju eventualne štete zbog gubitka reputacije. Bolot i Lelarge[12] su iste godine tvrdili da sajber osiguranje može da uspostavi veliki podsticaj za kompanije da unaprede svoju informatičku bezbednost. Bohme i Schwartz[13] su 2010. godine objavili okvir koji uključuje različite modele i pretpostavke o sajber osiguranju iz tada dostupne literature. Novija literatura nudi empirijsku studiju o provalama u baze podataka[14], pregled tržišta sajber osiguranja u Švedskoj[15], optimizaciju pokrića sajber osiguranja pomoću bezbednosnih kontrola[16], itd.

Domaći autori su objavljivali radove na temu sajber osiguranja poslednjih nekoliko godina. Najsvežije, javno dostupne radove, objavili su prošle godine Petrović,[17] na temu pravnih aspekata sajber osiguranja, i Stajšić Golijanin[18] o upravljanju sajber rizicima iz različitih perspektiva.

Upravljanje uvećanim IT rizicima kao posledicom pandemije

Postoje brojne definicije sajber rizika, koje su prilagođene određenim namenama ili aktivnostima pojedinih organizacija koje ih donose. Definicija CRO Foruma glasi[19]: „Sajber rizik predstavlja opasnost od upotrebe elektronskih podataka i njihovog prenošenja, uključujući i tehnološka sredstva kao što su internet i telekomunikacione mreže." Institut za upravljanje rizicima iz Londona je dao sledeću definiciju[20]: „Informatički rizik podrazumeva finansijsku štetu, gubitak ili narušavanje reputacije organizacije zbog neke vrste kvara njenih sistema informatičke tehnologije." Može biti zanimljiva i definicija sa besplatne enciklopedije Wikipedia[21]: „Sajber rizik je svaka vrsta ofanzivnog

11 Bandyopadhyay, T., Mookerjee, V. S., Rao, R. C. (2009) Why IT managers don't go for cyber-insurance products. *Communication of ACM 52(11)*, p. 68–73.
12 Bolot, J., Lelarge, M. (2009). *Cyber Insurance as an Incentive for Internet Security*. Springer: Managing information risk and the economics of security, p. 269–290.
13 Böhme, R., Schwartz, G. (2010). *Modeling Cyber-Insurance: Towards a Unifying Framework*. Workshop on Economics of Information Security – WEIS
14 Edwards, B., Hofmeyr, S., Forrest, S. (2015). *Hype and heavy tails: a closer look at data breaches*. Workshop on the Economics of Information Security (WEIS)
15 Franke, U. (2017). The Cyber Insurance Market in Sweden. *Computers & Security 68*, p. 130-144.
16 Uuganbayar, G. (2021). Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security 101*, p. 102-121.
17 Petrović, S. (2020). Sajber osiguranje. *Pravo i privreda 1/2020*, p. 206-217.
18 Stajšić Golijanin, N. (2020). Osiguranje kao način upravljanja sajber rizicima. *Zbornik radova fakulteta tehničkih nauka, god. 35, br. 10*.
19 CRO Forum. (2014). *Cyber resilience: The cyber risk challenge and the role of insurance*. Amsterdam: CRO Forum & KPMG Advisory N. V.
20 The Institute of Risk Management. (2014). *IRM Cyber Risk: Executive Summary*. London: The Institute of Risk Management
21 https://en.wikipedia.org/wiki/Cyber-attack

ponašanja pojedinaca ili organizovanih kompjuterskih programera, usmerenog na ciljane računarske informacione sisteme, infrastrukturu, računarske mreže i/ili lične računare radi krađe, izmene ili uništavanja, po pravilu sa nepoznatih lokacija". Domaću definiciju informatičkog rizika dao je Jovanović[22] kao opasnost od štetne upotrebe i manipulacije digitalnim instrukcijama i informacijama koje mogu da prouzrokuju finansijsku štetu na stvarima i licima i štetu u vezi sa ispunjavanjem zakonskih obaveza.

Jedan od najefikasnijih načina upravljanja uvećanim IT rizicima je osiguravajuće pokriće i zaštita u slučaju nastanka štete. Svaka kompanija koja koristi Internet ili cloud tehnologiju izložena je sajber opasnostima. Primeri sajber rizika mogu biti: iznude usled zloupotrebe podataka, hakerski napadi koji neovlašćeno uzimaju novac bankovnog računa, druge vrste sajber krađe, odgovornost za skladištenje podataka, obelodanjivanje poverljivih podataka posetiocima sajta, kršenje integriteta i poverljivosti elektronskih informacija, proboj kompjuterske sigurnosti, industrijska špijunaža, sajber terorizam, narušavanje ugleda i reputacije kompanije, prekid u lancu snabdevanja, itd.

Meta sajber napada može biti svaka kompanija koja koristi savremene informatičke tehnologije. Ipak, informacionu imovinu osigurava samo oko 15% kompanija, dok je udeo osiguranih kompanija znatno veći kod osiguranja od požara i iznosi 59%, pri čemu je verovatnoća ostvarenja osiguranog slučaja požara manja nego verovatnoća realizacije sajber rizika.[23]

Osiguravajuća zaštita se pruža za od dve grupe rizika koji nastaju u sajber prostoru. Prvu grupu čine rizici koji dovode do direktnih imovinskih gubitaka kao što su troškovi utvrđivanja uzroka štete, obaveštavanja zainteresovanih strana, otklanjanja nedostataka i ponovnog uspostavljanja kompjuterskog sistema, umanjenja prihoda usled prestanka rada, troškovi zbog povrede i gubitka podataka, novčani iznosi isplaćeni na ime ucene kao i troškovi pružanja pravne pomoći. Drugu grupu rizika čine izvori opasnosti iz odgovornosti za štete koje je osiguranik dužan da nadoknadi trećim licima usled povrede ličnih podataka, povrede časti i ugleda i prava intelektualne svojine.

Polisa sajber osiguranja nudi sledeća pokrića:

1. Odgovornost za profesionalne IT usluge[24] – ukoliko kompanija pruža IT usluge, polisa sajber osiguranja omogućava finansijsku zaštitu od profesionalne odgovornosti, odnosno odgovornost kompanije za usluge zasnovane na tehnologiji, za IT proizvode, za bezbednost informacija, i sl. Sajber polisa obezbeđuje podršku u sledećim slučajevima kršenja ugovora: nemar u izvršenju obaveza, greška ili propust u pružanju profesionalnih tehnoloških usluga ili propuštanje da se one

22 Jovanović, S. (2017). Osiguranje od informatičkih rizika. *Teme, g. XLI, br. 3*, p. 823-837.
23 Filipović, Z. (2018). *Cyber rizici – Izazovi digitalnog doba*. Drugi srpski dani osiguranja, Aranđelovac
24 http://respect-serbia.rs/cyber-i-it-osiguranje/

pruže; nenamerno kršenje ugovora; kleveta, narušavanje reputacije, nanošenje duševne boli; plagiranje, piraterija ili lažno prisvajanje ideja.

2. Odgovornost za multimedijalne sadržaje[25] – ako je multimedija deo usluge kompanije, npr. dizajn i izrada web sajtova, polisa sajber osiguranja pružiti pokriće za nastale troškove u slučaju nastanka tužbe zbog: klevete, narušavanja reputacije, nanošenja duševne boli; narušavanja, kršenja ili ometanja prava na privatnost ili povrede prava osobe u javnosti; plagiranje, piraterije ili lažnog prisvajanja ideja; kršenja autorskih prava, naziva domena, naslova ili slogana; nemara pružaoca usluge u vezi sa objavljivanjem multimedijalnog sadržaja na internetu ili u štampanim medijima; nelojalne konkurencije.
3. Odgovornost za bezbednost i privatnost podataka trećih lica – bezbednosti ličnih podataka na Internetu je izložena brojnim rizicima kao što su: neovlašćeno pristupanje ili neovlašćeno korišćenje računarske mreže; propust da se spreči fizička krađa ili gubitak informacija ili hardverske opreme; bezbednosni propusti; propust da se spreči lažna komunikacija osmišljena sa ciljem da se od korisnika na prevaru dobiju lične informacije, itd. Polisa sajber osiguranja nadoknađuje troškove tužbe zbog nemara ili neadekvatnog čuvanja i deljenja podataka.
4. Odgovornost za širenje virusa ili drugog zlonamernog programskog koda – pokrivaju se troškovi koji nastaju trećim licima usled potraživanja naknade štete od virusa za koji se dokaže da potiče iz kompanijske mreže.
5. Troškovi koje prouzrokuje krađa kompanijskih podataka – hakerski upadi u računarsku mrežu kompanije mogu da dovedu do krađe raznih vrednih poverljivih podataka koji se čuvaju na lokalnim serverima. Jedan od primera je krađa podataka o tehnološkom razvoju proizvoda kompanije, odnosno industrijska špijunaža.
6. Troškovi neophodnih radnji koje nameću propisi – u slučaju sajber incidenta u kompaniji ili kompromitacije podataka klijenata, regulativa zahteva sprovođenje određenih procedura, npr. u vezi sa propisima o zaštiti privatnosti. Realizacija takvih aktivnosti obično zahteva izvesne troškove, te je polisa sajber osiguranja pouzdan način da se pomenuti troškovi nadoknade.
7. Troškovi zastupanja na sudu i kazne nadležnih državnih organa – mogu biti osigurane advokatske usluge odbrane na sudu i sve naknade po odlukama donesenim od strane, pravosudnih organa ili regulatornih tela.
8. Troškovi obaveštavanje korisnika i upravljanja kriznom situacijom koji nastaju kao posledica povrede privatnosti podataka – jedna od obaveza kompanije koja se suoči sa sajber incidentom je i reagovanje na povredu privatnosti, odnosno obaveštavanje korisnika i upravljanje kriznom

25 https://vib.rs/sajber-osiguranje/

situacijom. Često takve situacije ne prolaze bez troškova angažovanja eksperata, kao i troškova medijskih obaveštenja. Polise sajber osiguranja pokrivaju ove troškove.

9. Izgubljena poslovna dobit usled prekida poslovanja – posledica sajber incidenta može biti izgubljena poslovna dobit usled ometanja normalnog režima rada kompanije i pojave eventualnih dodatnih troškova poslovanja. Polisa sajber osiguranja obezbeđuje finansijsku podršku za oporavak od sajber incidenta i tako smanjuje vreme potrebno za ponovno uspostavljanje normalnog režima rada kompanije, a takođe i nadoknađuje izgubljenu poslovnu dobit u toku trajanja sajber incidenta. Polisa pokriva direktan trošak osigurane kompanije, ali ne i štete zbog tužbi oštećenih trećih lica.
10. Troškovi za obnavljanje podataka – jedna od posledica sajber incidenta je i trošak ponovnog uspostavljanja poslovanja. Polisa sajber osiguranja pokriva sledeće troškove sprovođenja procedure obnavljanja podataka: za ponovno vraćanje, sakupljanje ili zamenu podataka, uključujući troškove za materijal i radno vreme; za korišćenje rentirane opreme; za prekovremeni rad zaposlenih; za angažovanje eksternih stručnjaka, istražitelja, forenzičara,...
11. Troškovi sajber iznude – iznuda određenog iznosa za povratak kompromitovanih, oštećenih ili uništenih podataka kompanije u prethodno stanje, jedan je od najskupljih sajber incidenata. Najčešće je posledica širenja kompjuterskog virusa, zlonamernog programskog koda ili onemogućavanja korišćenja informatičkih usluge (DoS). Polisa sajber osiguranja nudi neophodnu finansijsku zaštitu čak u slučaju ovako velike štete.
12. Odgovornost za sprovođenje elektronskog plaćanja – pokrivaju se troškovi krađe novca sa računa klijenata, ukoliko dođe do kompromitovanja njihovih podataka npr. o kreditnim karticama koje su koristili za plaćanje usluga osigurane kompanije ili osigurane banke koja procesira uplate preko Internet sajtova.

Uobičajeno je da fizičko oštećenje nastalo usled sajber napada nije pokriveno polisom, slično kao što je fizička šteta iz sajber napada isključena i po imovinskim polisama. Isključenje se uvek javlja i za štetu koja nastane usled kriminalnih aktivnosti osiguranika, kao i terorističkih napada. Često se sreće i isključenje za nedozvoljeno prikupljanje podataka klijenata, kao i isključenje za štetu koja može nastati usled nepoštovanja ugovora iz informatičke delatnosti od strane osiguranika, jer su troškovi koji nastaju usled ovih slučajeva izazvani aktivnostima osiguranika koje nisu u skladu sa zakonom ili ugovorom.

Najveća verovatnoća kod malih i srednjih preduzeća, od oko 5%, je za realizaciju sledećih rizika: prekid poslovanja, sajber kriminal i prevare i ugrožavanje privatnosti ličnih podataka.[26]

Polise sajber osiguranja nude najveće svetske i evropske osiguravajuće kompanije kao što su: AIG, Chubb, CNA, Allianz, Zurich, itd.

Premija sajber osiguranja

Tržište sajber osiguranja u regionu je nerazvijeno, tako da postoji vrlo mala istorija šteta koje su platile osiguravajuće kompanije. Zbog toga je određivanje premije zasnovano više na kvalitativnim nego kvantitativnim metodama.

Premija zavisi od velikog broja faktora koji manje ili više utiču na veličinu rizika, a samim tim i na cenu osiguranja.[27] Očekivano, veličina prihoda kompanije direktno je srazmerna veličini rizika. Delatnost osiguranika je jedan od najvažnijih faktora rizika. Npr. poznato je da sajber napadi naprave najveću štetu u zdravstvu, malim i srednjim preduzećima, kao i kompanijama koje imaju veliki broj plaćanja kreditnim karticama. Geografska zastupljenost je takođe bitan faktor rizika, jer je internacionalnim kompanijama teže da ispune sve zahteve različitih lokalnih regulativa, kao i da sačuvaju svoje podatke koji mnogo putuju s kraja na kraj sveta. Kao i kod ostalih vrsta osiguranja, limit pokrića koji ugovara osiguranik utiče na cenu polise, jer što je veći limit i rizik je veći, dok s druge strane ukoliko se ugovori učešće osiguranika u šteti, premija se smanjuje. Nivo informatičke bezbednosti kompanije takođe značajno utiče na premiju. Kompanije koje zadovoljavaju npr. ISO 27001 standard za upravljanje bezbednošću informacija, imaju manji rizik od sajber napada. Na kraju, kao kod drugih vrsta osiguranja, tehnički rezultat kompanije iz prošlosti utiče i na cenu sajber osiguranja.

Nedovoljna količina podataka o sajber štetama se jedino može prevazići uključivanjem reosiguravača u proces određivanja premije, pošto oni imaju znatno više iskustva po ovom pitanju od pojedinačnih osiguravača. Tipična premijska stopa koju preporučuju velike svetske reosiguravajuće kompanije ima red veličine 1%. Ovo osiguranje je relativno skupo u poređenju sa drugim vrstama osiguranja npr. oko tri puta skuplje od opšte odgovornosti i oko šest puta skuplje od osiguranja imovine.[28]

---

26 Bara, D., Ćorić, S., Jurišić, G. (2015). *The role of cyber insurance in managing and mitigating cyber security risk with special emphasis on the potential of Croatia and Serbia cyber insurance market*. Proceedings from IT/ICT Conference Kladovo 14-16.05.2015.

27 Franke, U. (2017). The Cyber Insurance Market in Sweden. *Computers & Security 68*, p. 130-144.

28 Paunović, M., Ralević, N. (2019). *Cyber-risk management and actuarial analyses*. XVII međunarodni simpozijum „Osiguranje na pragu IV industrijske revolucije", Zlatibor

Metoda ALE

Najčešće se u praksi koristi metoda ALE (engl. Annualized Loss Expected), odnosno određuje se premijska stopa, koja se zatim koriguje određenim faktorima. Kod ove metode obračuna premije osiguranja koristi se sledeća formula za očekivanu godišnju štetu (ALE):

*ALE = ARO * SLE*

gde je:

ARO – od engl. Annuualised Rate of Occurences – prosečni godišnji broj događanja štete

SLE – od engl. Single Loss Expectancy – prosečan iznos štete po realizaciji jednog rizika

Ova formula predstavlja tehničku premiju, na koju je potrebno dodati i režijski dodatak, koji je za ovu vrstu osiguranja obično oko 30%.

Ovako dobijena osnovna premija, koriguje se određenim faktorima, koji se odnose na delatnost poslovanja kompanije, veličinu kompanije i godišnje prihode. [29] Sledeći podaci o IT performansama osiguranika su važan pokazatelj izloženosti riziku koji utiče na eventualnu korekciju premija: da li je razvoj informacionog sistema poveren drugim kompanija, da li se koristi tehnologija računarstva u oblaku, da li se obrađuju i čuvaju osetljivi lični podaci, da li se pristupa podacima preko Interneta, itd. Važni faktori koji utiču na premiju su i limit osiguranja, učešće u štetama, kao i dostupni podaci o štetama i incidentima u prethodnom periodu. Na kraju korektivni faktori se formiraju na osnovu elemenata vezanih za procenu IT ranjivosti i sigurnosti. Uticaj pojedinačnih faktora rizika se procenjuje pomoću matrice rizika.

Matrica rizika

Matrica rizika je kvalitativni model koji kombinuje klasifikaciju verovatnoće pojave rizika sa klasifikacijom intenziteta posledica nastanka rizika, kako bi se utvrdila klasifikacija nivoa rizika. Kod ove matrice važi princip da veća verovatnoća i veći intenzitet podrazumevaju veći rizik. Matrica rizika može da se koristi i kao pseudo-kvantitativni metod, jer se klasifikacija verovatnoće može izraziti brojevima. Ključne prednosti korišćenja matrice rizika su pouzdano identifikovanje izvora pretnji, smanjenje troškova na duži rok usled sprovođenja preventivnih aktivnosti, povećavanje sposobnosti kompanije za procenu sopstvenih slabosti što unapređuje sistem upravljanja rizikom kroz periodično

29 Romanosky S. et all (2017). Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? *SSRN Electronic Journal, January 2017*

preispitivanje, poboljšavanje usklađenosti sa propisima i eliminisanje prevelikog oslanjanja na subjektivnu procenu kompanijskih informatičara o sistemu kojim upravljaju.

Primer jedne matrice rizika je prikazan na Slici 1. Intenzitet posledice nastanka štete je prikazan u kolonama, a verovatnoća pojave rizika u redovima matrice. Verovatnoća je definisana kao mogućnost da se određena situacija dogodi ili da određeni događaj dovede do negativnih posledica i može da se kreće od „vrlo retko" do „nekoliko puta godišnje".[30] Intenzitet posledice realizacije rizika pokazuje koliko velika štetu će biti napravljena ako se realizuje rizik i može da se kreće od „male posledice" do „katastrofalne posledice".

Matrica rizika služi za određivanje prioriteta preventivnih aktivnosti usmerenih ka sprečavanju posledica realizacije različitih rizika. Na Slici 1. se vidi da je najvažnije upravljati rizicima koji spadaju u klasu ekstremnih intenziteta i srednje ili velike verovatnoće (polja 11 i 12), a zatim rizicima iz polja 7, 8, 9 i 10.

Slika 1. Matrica procene rizika

Ocene rizika		**NIZAK** **0 – prihvatljiv**	**SREDNJI** **1 – razumno nizak**	**VISOK** **2 – generalno neprihvatljiv**	**EKSTREMNI** **3 – neprihvatljiv**
INTENZITET					
VEROVATNOĆA		PRIHVATLJIV (bez efekata)	TOLERANTAN (efekti nisu kritični)	NEŽELJEN (veliki efekat)	NETOLERANTAN (može dovesti do katastrofe)
	NEVEROVATAN (najverovatnije se neće dogoditi)	NIZAK (1)	SREDNJI (4)	SREDNJI (6)	VISOK (10)
	MOGUĆ (verovatno će se rizik ostvariti)	NIZAK (2)	SREDNJI (5)	VISOK (8)	EKSTREMNI (11)
	VEROVATAN (rizik će se desiti)	SREDNJI (3)	VISOK (7)	VISOK (9)	EKSTREMNI (12)

Izvor: Draper, G. (2019). *Managing Cybersecurity Risks Using a Risk Matrix*. https://fortsafe.com/managing-cybersecurity-risks-using-a-risk-matrix/

30 Draper, G. (2019). *Managing Cybersecurity Risks Using a Risk Matrix*. https://fortsafe.com/managing-cybersecurity-risks-using-a-risk-matrix/

Tehnike analize rizika u sajber osiguranju

U Tabeli 1 prikazane su tehnike koje se koriste za identifikaciju i analizu rizika i specificiranje detalja ugovora o osiguranju. To su sledeće tehnike:

a) Analiza poslovne dokumentacije kompanije koja želi da se osigura, kao osnovni način za saznavanje najvažnijih detalja osiguraniku i riziku. Koriste se različiti dokumenti kompanije, akti poslovne politike, odluke, popisi, procedure, grafikoni;
b) Organizacija sastanaka i intervjua omogućava da se na najjednostavniji način sazna neka informacija, tako što će se pitati nadležna osoba iz kompanije koja želi da se osigura;
c) Popunjavanje upitnika i anketa od strane zaposlenih u kompaniji omogućava da se na organizovan način prikupe i kasnije analiziraju podaci koji su prethodno skupljeni u slobodnoj formi tokom intervjua;
d) Korišćenje baze znanja koju su kreirali eksperti i koja sadrži najbolju praksu i informacije koje se mogu koristiti u različitim prilikama, s ciljem identifikacije imovine, pretnji i ranjivosti i eventualnih mera za smanjenje rizika;
e) Formiranje stabla napada, kao i stabala pretnji i greški s ciljem preglednog predstavljanja i lakše analize napada na kompanijski sistem i mrežu. Primer stabla napada je prikazan na Slici 2.
f) Delfi metod omogućava da se grupno, zajedničko mišljenje eksperata u najvećoj meri što objektivnije sagleda, da se prevaziđu svi nedostaci prisutni kod generisanja mišljenja i uspostavljanja zajedničkog stava i mišljenja grupe po pojedinim pitanjima na otvorenim sastancima grupe;
g) Analiza istorije napada na sistem je najefikasniji način određivanja verovatnoće pojave budućeg incidenta na osnovu istorijskih podataka;
h) Sertifikati o standardima sajber bezbednosti koje kompanija ima, kao što je ISO 27001, govore o uspostavljenim kontrolama i procedurama u sistemu i mreži kompanije, što značajno smanjuje rizik da se sajber pretnja ostvari;
i) Metoda za određivanje očekivane godišnje štete (ALE) je opisana u prethodnom poglavlju;
j) Profilisanje rizika kompanije se koristi za prepoznavanje u koji od predefinisanih profila rizika se najbolje uklapa kompanija s ciljem pojednostavljivanja pojedinačnog proces preuzimanja rizika;
k) Teorija igara je moćan mehanizam za odlučivanje o specifikaciji pokrića tj. o delu rizika kompanije koji je najbolje preneti na osiguravača, dok osiguravaču pomaže da razume uticaj preuzetog rizika na profit;
l) Skeniranje ranjivosti sistema je organizovani pristup testiranju, identifikaciji, analizi i izveštavanju o potencijalnim sigurnosnim problemima na kompanijskoj mreži;

m) Testiranje penetracije u sistem je simulirani sajber napad na računarski sistem kompanije da bi se proverile i iskoristile potencijalne ranjivosti sistema. Testiranje se može vršiti na delove sistema kao što su web aplikacije ili na ceo sistem;
n) Matrica rizika je objašnjena u prethodnom poglavlju.

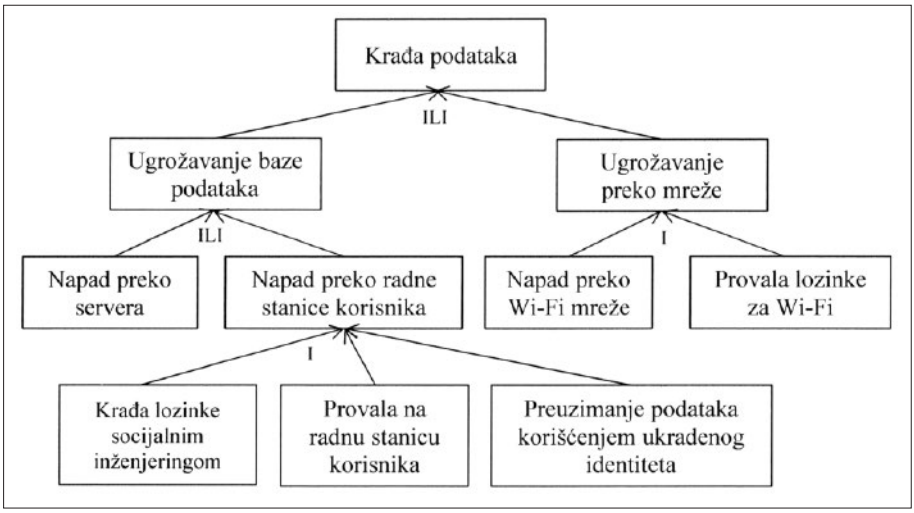
Tabela 1. Vodič za preuzimanje sajber rizika

Faza	Koraci	Tehnike
Identifikacija rizika	Identifikacija imovine	a) Analiza poslovne dokumentacije b) Organizacija sastanaka i intervjua c) Popunjavanje upitnika i anketa d) Korišćenje baze znanja
	Identifikacija pretnji	a) Analiza poslovne dokumentacije b) Organizacija sastanaka i intervjua c) Popunjavanje upitnika i anketa d) Korišćenje baze znanja e) Formiranje stabla napada
	Identifikacija ranjivosti	e) Formiranje stabla napada l) Skeniranje ranjivosti sistema m) Testiranje penetracije u sistem b) Organizacija sastanaka i intervjua c) Popunjavanje upitnika i anketa d) Korišćenje baze znanja f) Delphi metod za usaglašavanje h) Sertifikati o standardima bezbednosti
Analiza rizika	Određivanje verovatnoće realizacije rizika	g) Analiza istorije napada na sistem b) Organizacija sastanaka i intervjua c) Popunjavanje upitnika i anketa d) Korišćenje baze znanja f) Delphi metod za usaglašavanje
	Određivanje uticaja	b) Organizacija sastanaka i intervjua c) Popunjavanje upitnika i anketa d) Korišćenje baze znanja f) Delphi metod za usaglašavanje
	Očekivani rizik	n) Matrica rizika i) Određivanje očekivane godišnje štete (ALE)

Faza	Koraci	Tehnike
Ugovaranje osiguranja	Specifikacija pokrića	b) Organizacija sastanaka i intervjua k) Teorija igara
	Obračun premije	k) Teorija igara j) Profilisanje rizika kompanije

Izvor: Marotta, A. et all. (2017). Cyber-insurance survey. *Computer Science Review 24(2017)*, p. 35-61.

Slika 2. Primer stabla napada



Izvor: Marotta, A. et all. (2017). Cyber-insurance survey. *Computer Science Review 24(2017)*, p. 35-61.

Sajber reosiguranje

Sajber reosiguranje je prilično nerazvijeno, jer su dileme u razvoju proizvoda reosiguranja identične kao i u vezi osiguranja. Često su sajber rizici u imovinskim ugovorima o reosiguranju isključeni.

Ipak, pošto je kapacitet osiguravajućih kompanija nedovoljan, reosiguranje je u praksi često neophodno. Zato je učešće koje reosiguravači nude na kvotnoj osnovi često do 30%. Reosiguravači su konzervativni u pogledu ukupne izloženosti sajber riziku, pa često zahtevaju ograničenja po štetnom događaju za prekid poslovanja, kao i različite franšize (po iznosima ili po vremenu) i isključuju pokriće na određenim područjima koja smatraju

rizičnijim. Takođe, uvode i različita isključenja, kao npr. za uređaje poput USB memorija koji nisu kriptovani.

Veliki deo sajber reosiguranja se plasira u Londonu i na Bermudama.

Sajber osiguranje u Srbiji

Wiener Städtische osiguranje u Srbiji nudi osiguranje od sajber rizika. Postoje određeni preduslovi koje mora da ispuni kompanija koja želi da sklopi ugovor o ovoj vrsti osiguranja sa Wienerom: na svakom kompjuteru u kompaniji mora biti instaliran anti-virus softver koji se redovno ažurira; ključni podaci se moraju redovno kopirati i skladištiti na udaljenoj bezbednoj lokaciji; mora biti uspostavljena kontrola mrežnog saobraćaja i mora postojati jasna kompanijska politika informatičke bezbednosti.

Pored ispunjenja preduslova, kompanija popunjava upitnik u kojem daje osnovne podatke o svom informacionom sistemu, primenjenoj zaštiti, načinu prenosa i skladištenja podataka, ali i finansijske podatke, informacije o uticaju na redovno poslovanje, o broju i prirodi ličnih podataka trećih lica, itd. Na osnovu tih informacija preuzimači rizika odlučuju o prijemu u osiguranje i određuju adekvatnu premiju.

Wienerova polisa[31] sajber osiguranja u Srbiji se može sklopiti s ciljem zaštite od krađe, zloupotrebe ili izmene kompanijskih podataka. Ova polisa pokriva troškove angažovanja IT stručnjaka za utvrđivanje obima štete, njenog limitiranja i povratka podataka, uklanjanja zlonamernog koda ili virusa i slično. Sajber osiguranje pokriva i štetu koju kompanija može pretrpeti usled ugrožavanja ličnih podataka klijenata, tako što nadoknađuje troškove angažovanja pravnih savetnika, savetnika za krizne situacije, za troškove obaveštavanja lica čiji su podaci ugroženi, kao i druge troškove nastale sa ciljem očuvanja reputacije kompanije. Sajber incident može indirektno pokrenuti odgovornost menadžmenta. Polisa osiguranja od odgovornosti menadžera služi da pokrije troškove odbrane menadžmenta na sudu, ali takođe i pokriva nadoknadu štete ukoliko sud utvrdi da je menadžment kriv. Direktne finansijske posledice sajber incidenta takođe ulaze u osigurano pokriće. Polisa sajber osiguranja nadoknađuje i novčane kazne koju kompanijama izreknu nadležni državni organi, troškove upravljanja kriznom situacijom, kao i troškove obaveštavanja korisnika i troškovi podrške klijentima. Polisa sajber osiguranja u slučaja širenja zlonamernog koda ili virusa koji nanosi štetu ili onemogućava pristup kompjuterskim sistemima i podacima usled želje da se izvrši iznuda nadoknađuje utvrđenu izgubljenu dobit i plaća troškove iznude ukoliko angažovani IT stručnjaci utvrde da je neophodno.

31 https://www.ekapija.com/news/3051143/wiener-staedtische-osiguranje-vazno-je-osigurati-se-od-sajber-rizika

Zaključak

Na tržištu Srbije osiguravači nemaju mnogo iskustva u pokriću ovih rizika. Razvoj novih proizvoda sajber osiguranja je veliki izazov za osiguravajuće kompanije, zbog rada sa novim konceptima i modelima. Nedostatak iskustva, statističkih podataka i alata, antiselekcija, moralni hazard, adekvatnost aktuarskih pretpostavki, dovoljnost premije za ispunjenje svih obaveza, kvalitetan program reosiguranja, itd. su ključne prepreke za obezbeđenje adekvatnog pokrića sajber rizika.

Utvrđivanje naknade u sajber osiguranju je drugačije nego u osiguranju imovine. Određivanje veličine štete koju je pretrpeo osiguranik ili treće lice je komplikovano. Materijalna šteta može biti velika, naročito usled gubitaka prihoda. Ipak i u sajber osiguranju, kao i u ostalim imovinskim osiguranjima, važi načelo obeštećenja osiguranika. Naknada iz osiguranja mora da odgovara visini stvarne štete koju ima osiguranik ili treće lice. Ugovaranje isplate ugovorenog iznosa, kao u osiguranju lica, bez utvrđivanja visine štete nije u skladu sa načelom obeštećenja, što znači da bi osiguranik mogao da dobije znatno više od pretrpljene štete. Problem utvrđivanja naknade u sajber osiguranju može da posluži kao jedan od pravaca daljeg istraživanja.

Usvajanje savremenih svetskih trendova razvoja regulative za sajber prostor, uvođenja odgovarajućih metoda analize sajber rizika i korišćenja naprednih informacionih tehnologija za analizu podataka, omogućiće brže uključivanje domaćih osiguravajućih kompanija u ovu brzorastuću vrstu osiguranja.

Literatura

1. Bandyopadhyay, T., Mookerjee, V. S., Rao, R. C. (2009) Why IT managers don't go for cyber-insurance products. *Communication of ACM 52(11)*, p. 68–73.
2. Bara, D., Ćorić, S., Jurišić, G. (2015). *The role of cyber insurance in managing and mitigating cyber security risk with special emphasis on the potential of Croatia and Serbia cyber insurance market*. Proceedings from IT/ICT Conference Kladovo 14-16.05.2015.
3. Insurance market, Proceedings from IT/ICT Conference Kladovo 14-16.05.2015.
4. Bohme, R., Kataria, G. (2006). *Models and Measures for Correlation in Cyber-insurance*. Workshop on Economics of Information Security (WIES)
5. Böhme, R., Schwartz, G. (2010). *Modeling Cyber-Insurance: Towards a Unifying Framework*. Workshop on Economics of Information Security (WEIS)
6. Bolot, J., Lelarge, M. (2009). *Cyber Insurance as an Incentive for Internet Security*. Springer: Managing information risk and the economics of security, p. 269–290.
7. CRO Forum. (2014). *Cyber resilience: The cyber risk challenge and the role of insurance*. Amsterdam: CRO Forum & KPMG Advisory N. V.
8. Draper, G. (2019). *Managing Cybersecurity Risks Using a Risk Matrix*. https://fortsafe.com/managing-cybersecurity-risks-using-a-risk-matrix/

9. Edwards, B., Hofmeyr, S., Forrest, S. (2015). *Hype and heavy tails: a closer look at data breaches*. Workshop on the Economics of Information Security (WEIS)
10. Featherly, K. (2021). *ARPANET United States defense program*. www.britannica.com/topic/ARPANET
11. Filipović, Z. (2018). *Cyber rizici – Izazovi digitalnog doba*. Drugi srpski dani osiguranja, Aranđelovac
12. Franke, U. (2017). The Cyber Insurance Market in Sweden. *Computers & Security 68*, p. 130-144.
13. Johnson, J. (2021). *Number of ransomware attacks per year 2014-2020*. www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide
14. Jovanović, S. (2017). Osiguranje od informatičkih rizika. *Teme, g. XLI, br. 3*, p. 823-837.
15. Krivokapić, D., Petrovski, A., Malinović, S. (2017). *Mere za zaštitu IKT sistema od posebnog značaja*. Share fondacija: Vodič za IKT sisteme od posebnog značaja, informaciona bezbednost, p. 19.
16. Marotta, A. et all. (2017). Cyber-insurance survey. *Computer Science Review 24(2017)*, p. 35-61.
17. Pak, J. (2014). *Osiguranje Internet rizika*. Međunarodna naučna konferencija Univerziteta Singidunum Sinteza, s. 71-76
18. Paunović, M., Ralević, N. (2019). *Cyber-Risk Management and Actuarial Analyses*. XVII međunarodni simpozijum „Osiguranje na pragu IV industrijske revolucije", Zlatibor
19. Petrović, S. (2020). Sajber osiguranje. *Pravo i privreda 1/2020*, p. 206-217.
20. Romanosky S. et all (2017). Content Analysis of Cyber Insurance Policies: How Do Carriers Write Policies and Price Cyber Risk? *SSRN Electronic Journal, January 2017*
21. Scientific American (2001). *When did the term 'computer virus' arise?* www.scientificamerican.com/article/when-did-the-term-compute
22. Shakeel, I. (2016). *Evulution in the World of Cyber Crime*. https://resources.infosecinstitute.com/topic/evolution-in-the-world-of-cyber-crime
23. Sheldon, J. (2016). *Cyberwar*. www.britannica.com/topic/cyberwar
24. Stajšić Golijanin, N. (2020). Osiguranje kao način upravljanja sajber rizicima. *Zbornik radova fakulteta tehničkih nauka, god. 35, br. 10*.
25. The Institute of Risk Management. (2014). *IRM Cyber Risk: Executive Summary*. London: The Institute of Risk Management
26. Uuganbayar, G. (2021). Optimisation of cyber insurance coverage with selection of cost effective security controls. *Computers & Security 101*, p. 102-121.
27. http://www.keepnetlabs.com/the-biggest-data-breaches-in-the-first-half-of-2020
28. http://www.phishing.org
29. http://respect-serbia.rs/cyber-i-it-osiguranje/
30. https://vib.rs/sajber-osiguranje/
31. https://en.wikipedia.org/wiki/Cyber-attack
32. https://www.ekapija.com/news/3051143/wiener-staedtische-osiguranje-vazno-je-osigurati-se-od-sajber-rizika