Poistenie kybernetických rizík

Matúš Medvec a Júlia Čillíková[1]
Národná banka Slovenska

Elektronizácia a internetový fenomén majú za následok, že pravdepodobnosť kybernetického útoku v akejkoľvek z jeho podôb je často vyššia ako pravdepodobnosť poistnej udalosti, akou je klasická dopravná nehoda. Jedným z dôvodov je aj fakt, že počet osôb s prístupom k internetovým službám a technológiám je vyšší ako počet vlastníkov osobných motorových vozidiel. Štandardné poistné produkty síce poistenie kybernetických rizík poznajú, zväčša však v časti výluk z poistenia. To znamená, že poistné krytie pri klasických produktoch (napríklad pri poistení zodpovednosti za škodu a poistení majetku) nezahŕňa kybernetické riziká. Práve z dôvodu existencie tejto „diery na trhu" sa vytvára nová oblasť poistenia, ktorou je práve poistenie kybernetického rizika[2].

Cieľom útokov sa stávajú aj bežní používatelia, a to práve pre ich slabšie zabezpečenie. Inokedy sa môžeme stretnúť so sofistikovanými útokmi na veľké spoločnosti, ktorých cieľom môže byť know-how alebo obchodné tajomstvo konkurencie. Treba však poznamenať, že bezpečnostný systém subjektu je taký dokonalý, ako je voči útokom odolný jeho najslabší článok, a preto je potrebné vyhnúť sa situáciám, keď menej zabezpečená časť spôsobí nabúranie do celého systému.

Z tohto pohľadu bude nadobúdať oblasť poistenia kybernetického rizika čoraz väčšiu dôležitosť, a teda tlak nebude len na nové a lacnejšie produkty, ale aj na zákonodarcu, aby sa tomuto poisteniu dali mantinely, ktoré by sa inak mohli prekračovať. Význam kybernetického rizika umocňuje aj fakt, že dnes dôsledok kybernetického útoku môže byť oveľa vážnejší ako dôsledky izolovaného teroristického útoku na hardvérové vybavenie (ak porovnávame škodu výlučne na nehmotnom majetku).

História

Prvé vírusy sa masovejšie rozšírili začiatkom nového milénia, neskôr sa hekovanie a kybernetické útoky začali využívať na diskrétne zásahy do informačných systémov medzi štátmi a približne od roku 2010 sa rozšírili komplexnejšie útoky z rôznych dôvodov (či už to bola špionáž, získanie konkurenčnej výhody, know-how, podvody, sabotáž alebo terorizmus). Inými slovami, vystavenie fyzických či právnických osôb uvedeným hrozbám má rapídne rastúcu tendenciu, ktorá má priamoúmerný charakter s technologickým pokrokom a inováciami.

Rozsah a aktuálnosť tejto problematiky možno demonštrovať najviac pertraktovanými prípadmi v celosvetovom meradle. Ich dôsledky hovoria práve v prospech existencie kybernetického poistenia. Za zmienku stojí prípad spoločnosti Sony z roku 2011, keď boli odcudzené dáta viac než 77 miliónov užívateľov (prostredníctvom známej hracej konzoly). V súvislosti s týmto útokom spoločnosť Sony vynaložila prostriedky v objeme 171 miliónov dolárov. Napokon bola nútená prerušiť sieť komunikujúcu s konzolami na viac než jeden mesiac a vyrovnať sa so stratou dôvery zo strany zákazníkov.

Ďalším známym prípadom je Irán a tzv. operácia olympijské hry. Uvedená sabotáž sa týka samotného štátu a nie súkromného subjektu. V roku 2010 mal kybernetický útok za následok zásah do riadenia vývoja a používania nukleárnych zariadení v krajine. Zaujímavosťou je, že napriek vysokej ostražitosti a izolovanosti serverov od vonkajšieho sveta sa útočníkom podarilo prepašovať vírus zvnútra organizácie prostredníctvom USB kľúča.

Trh a jeho vývoj

Poistenie kybernetického rizika sa prvýkrát objavilo v druhej polovici deväťdesiatych rokov, no jeho rozšírenie sa zaznamenalo približne pred desiatimi rokmi. V tomto období sa vyskytli prvé rozsiahlejšie kybernetické útoky jednak na štáty, respektíve na štátne orgány, ale aj na súkromné spoločnosti (najmä v zbrojárskom priemysle). Práve vtedy sa začal používať pojem kybernetická kriminalita.

Najväčší trh je, prirodzene, v USA, keďže práve tam spoločnosti čelili najväčšiemu počtu útokov. Aj z tohto dôvodu má trh poistenia kybernetických rizík v USA hodnotu viac ako miliardu dolárov s ročným rastom nad úrovňou 20 %.[3] Napriek tomu aj dnes zostáva fragmentovaný. Legislatíva v Spojených štátoch na to už stihla aspoň sčasti zareagovať a všetky porušenia bezpečnostných pravidiel súvisiace s osobnými údajmi podliehajú oznamovacej povinnosti príslušným orgánom.

Donedávna mal v USA klient kupujúci obdobné produkty príjem od 100 miliónov do 1 miliardy dolárov. Dnes sa však tieto produkty stávajú populárnymi aj medzi menšími klientmi (poistenie kybernetických rizík má zatiaľ približne 31 % firiem v USA). Na druhej strane si treba uvedomiť, že strojcovia kybernetických útokov svoje ciele nachádzajú aj medzi malými a strednými spoločnosťami, keďže často práve tie nemajú dostatok prostriedkov na pasívne či aktívne odvrátenie útokov.

Podľa Washington Times sa škody spôsobené počítačovou kriminalitou vyšplhajú len v USA ročne na 24 až 120 miliárd dolárov. To má za následok, že na zamedzenie počítačovej kriminality celosvetovo investuje 300 až 400 miliárd dolárov.[4]

Legislatíva vo Francúzsku dovoľuje uložiť sankciu do výšky 5 % z ročného obratu spoločnosti

1 *Názory a postoje autorov v tomto článku nemusia odrážať stanoviská a postoje NBS.*
2 *OECD, Cybersecurity Policy Making at a Turning Point. Dostupné na http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf*
3 *Rundesová, T. Poistite sa proti hackerom. Ide to aj u nás. Dostupné na: http://hnporadna.hnonline.sk/clanky-168/poistite-sa-proti-hackerom-ide-to-aj-u-nas-611750*
4 *Washington Times, Cybercrime costs the U.S. economy billions of dollars annually: study. Dostupné na: http://www.washingtontimes.com/news/2013/jul/23/cybercrime-costs-us-economy-billions-dollars-annua/*

v prípade porušenia zabezpečenia dát. Taktiež v Nemecku môžu úrady za obdobné porušenie uložiť pokutu do výšky 300 tisíc EUR. Ochranu kybernetickej bezpečnosti na Slovensku, respektíve sankčné mechanizmy zo strany orgánov štátnej správy poznáme len prostredníctvom vynucovania pravidiel ochrany osobných údajov Úradom na ochranu osobných údajov. Ten v prípade, že sú porušené pravidlá nakladania s osobnými údajmi iných osôb, môže ukladať sankčné opatrenia. Oblasť ochrany iných druhov dát a vôbec ochrana pred kybernetickými útokmi nie je v našej legislatíve detailne rozpracovaná.

Európa a jej inštitúcie sa tejto oblasti aktívne venujú.[5] Vnímajú ju ako nevyhnutnú na zabezpečenie rastu internetovej ekonomiky. Podľa prieskumu Európskej komisie sa dnes pri elektronických platbách cíti bezpečne len 12 % finančných spotrebiteľov.

Už počas roku 2014 vypracovalo Jednotné výskumné centrum Európskej komisie dokument, ktorý sa ako prvý zaoberal otázkou kybernetickej bezpečnosti z pohľadu EÚ. Dnes tvorí základ pre stratégiu kybernetickej bezpečnosti EÚ[6] v rámci digitálnej agendy európskych inštitúcií. Jej cieľom je vytvorenie priestoru najvyššieho svetového štandardu elektronickej bezpečnosti (výmenou informácií, spoločným riešením a koordináciou proti masívnym kybernetickým útokom a pod.).

Dôvody na existenciu uvedeného druhu poistenia

Informatizácia spoločnosti so sebou priniesla nielen uľahčenie života, ale aj s tým spojené nové druhy hrozieb. Patria k nim kybernetické riziká, ktoré sa týkajú najmä firiem pracujúcich s veľkým objemom dát, teda aj finančné inštitúcie, ktoré tieto dáta spracúvajú ako nevyhnutnú súčasť svojho biznisu.

Elektronické služby, internet, počítačové databázy a zdieľanie dát má v ostatných rokoch rapídne rastúcu tendenciu. Ako každá nová technológia, i tieto so sebou priniesli nové hrozby. Dnes už drvivá väčšina obyvateľov rozvinutých krajín používa smartfóny so sociálnymi médiami (Facebook, Twitter, Google plus), cez ktoré sa dostávajú k svojim osobným údajom. Priestorom pre hekerov, ktorí sa snažia o prístup k uschovaným údajom, sú aj cloudové služby.

V súkromných spoločnostiach dochádza k optimalizácii nákladov a lepšiemu vykazovaniu dát pre kvalifikovanejšie manažérske rozhodnutia prostredníctvom tzv. *Big Data*, čiže spracúvaním dát do využiteľných a porovnateľných prehľadných výstupov. Je preto nepochybné, že takéto databázy v sebe ukrývajú obrovské možnosti, ale sú najmä zaplnené citlivými údajmi pre konkrétnu spoločnosť.

Faktom však je, že drvivá väčšia kybernetických útokov sa realizuje prostredníctvom veľmi jednoduchých spôsobov využívajúcich minimálne zabezpečenie obetí.

S rozvojom elektronizácie a širokým využívaním elektronických systémov a databáz nielen na vnútorné použitie organizácie, ale aj na komunikáciu s tretími stranami sa hrozba kybernetického útoku stáva čoraz reálnejšou a dôsledok takéhoto útoku môže mať v určitých prípadoch až likvidačné následky.

Riziká, pred ktorými sa treba chrániť

Kybernetická kriminalita môže mať rôzny pôvod a príčinu. Stručne možno poznamenať, že rozlišujeme jednoduché útoky hekerov na málo zabezpečené subjekty a potom rafinované a oveľa zložitejšie útoky, ktoré cielene prelomia aj pokročilé zabezpečenie. Toto rozdelenie je dosť zjednodušené a keďže kybernetické zločiny sa objavili vo viacerých podobách, v súčasnosti možno identifikovať nasledujúce druhy:

- organizovaná kriminalita – charakterizuje ju veľká pokročilosť a rafinované taktiky na prelomenie zabezpečených sietí. Cieľom je získať majetkový prospech;
- drobní hekeri – ich cieľom je získať prospech predajom ukradnutých dát alebo duševného vlastníctva. Ide o najbežnejšiu formu kybernetickej kriminality;
- tzv. hektivisti[7] – hekeri, ktorí útočia na oficiálne kontá inštitúcií s cieľom poukázať na slabú ochranu; charakterizuje ju výrazne menšia nebezpečnosť ako v prípade vyššie uvedených druhov. Do tejto kategórie spadajú aj aktivisti bojujúci proti testovaniu liekov na zvieratách a pod.;
- kybernetická kriminalita zo strany štátov (napr. totalitné režimy) – príkladom je nedávny útok na spoločnosť Sony. Ciele útokov sú často politicko-ekonomické. Sú známe prípady, keď sa pri cezhraničnom zlúčení alebo splynutí spoločností stratili elektronicky prevádzané finančné prostriedky;
- terorizmus – útok s cieľom poškodiť a destabilizovať, a nie získať materiálny prospech. Terčom sú často laboratória alebo vojenské výskumné zariadenia.

Možno spomenúť, že z pohľadu internej klasifikácie súkromných spoločností patrí ochrana pred kybernetickým rizikom medzi operačné riziká. Subjekt, resp. pôvodca kybernetického útoku môže byť veľmi rôznorodý, na druhej strane aj zásah a poškodenie, ktoré spôsobí, často variuje. V súvislosti s kybernetickou kriminalitou hrozia najčastejšie tieto riziká:[8]

- obmedzenie prístupu k informačným systémom spoločnosti alebo prerušenie poskytovaných webových služieb (kódovanie, výpadok siete, zlyhanie počítačov a vírusy, ktoré môžu zničiť dáta, poškodiť hardvér, ochromiť systémy alebo prerušiť prevádzku spoločnosti),
- krádež citlivých alebo osobných informácií alebo zdravotných záznamov, prípadne manipulácia s nimi,
- získanie neoprávneného prospechu (prevod elektronických peňazí),
- poškodenie dobrého mena a strata dôvery (autorské práva, obchodná značka).

5 *Európska Komisia. Digitálna Agenda. Dostupné na: https://ec.europa.eu/digital-agenda/en/cybersecurity*

6 *;Európska Komisia. Digitálna Agenda. Dostupné na: http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace*

7 *KPMG. Cyber crime: Insurers in the firing line. Dostupné na http://www.kpmg.com/global/en/issuesandinsights/articlespublications/frontiers-in-finance/pages/cyber-crime-insurers-firing-line-fs.aspx*

8 *Jarkovský, A. Poistenie kybernetických rizík. Dostupné na http://intranet1.renomia.cz/_sys_/FileStorage/download/8/7860/01_2014_it-systems_pojisteni-kybernetickych-rizik_final-pdf.pdf?nc=1*

Predmet poistenia

Predmet poistenia možno exaktne identifikovať až po analýze expertmi z oblasti informačných technológií. Problémom však zostáva upisovanie, teda odhadovanie rizika a následne výpočet poistného. To nerozlučne súvisí s faktom, že predmetný trh je nový, neexistuje dostatok historických dát a ak je aj určité penzum dát k dispozícii, môžu byť veľmi heterogénne (napr. odcudzenie údajov v banke môže mať oveľa väčšie dôsledky, ako keď sa to stane v športovom klube, ktorý eviduje len základné identifikátory svojich členov). Poisťovne tak majú ťažkú úlohu pri stanovovaní poistného z údajov dostupných na trhu. Môže to viesť buď k príliš drahým a nedostupným produktom, alebo na druhej strane k produktom, ktoré nebudú kryť dostatočný rozsah rizík a teda budú poskytovať obmedzený okruh poistných plnení.

Ak by sme mali charakterizovať poistenie kybernetického rizika, zaradili by sme ho medzi hybridné poistné produkty, teda produkty zložené z viacerých častí. Prvou je majetkové poistenie, čiže poistenie za škody spôsobenému poistenému. Druhou je poistenie zodpovednosti za škodu, ak vzniknú škody tretím osobám.

Poistenie môže v najširšom rozsahu zahŕňať identifikáciu úniku údajov, opatrenia na nápravu poškodení spôsobených kybernetickým zásahom, náhradu nákladov spojených s medializáciou, s vyšetrovaním zdroja úniku, náhradu právnych nákladov súvisiacich s únikom dát, ako aj nákladov na notifikáciu dotknutých subjektov, obnovenie prerušenia prevádzky v dôsledku útoku, straty na zisku, poistenie prípadného vydierania spoločnosti, nečestného konania zamestnanca, škody tretích strán súvisiace s kybernetickým útokom či poistenie pokuty udelenej orgánom dohľadu.

Uzatváranie poistnej zmluvy a jej špecifiká

Poistenie kybernetického rizika sa uzatvára tak ako ostatné klasické druhy poistenia poistnou zmluvou. Tá ustanovuje podmienky, predmet a rozsah poistenia. Zahŕňa tiež výluky z poistenia spolu s limitmi poistného krytia. Treba poznamenať, že väčšinou nejde o formulárovú zmluvu, ale o individuálne dohodnutý a pomerne zložitý kontrakt (vysoká individualizácia v dôsledku špecifických podmienok pri rôznych poistených subjektoch, a to aj z dôvodu, že ide o pomerne citlivý poistný produkt).

Pri uzatváraní poistnej zmluvy je najdôležitejšie uvedomiť si a riadne identifikovať potenciálne hrozby pre konkrétnu spoločnosť. Zovšeobecňovanie v tomto prípade vôbec nie je na mieste, a to najmä z dôvodu, že menšia spoločnosť, napríklad s piatimi zamestnancami, bude mať určite iné potreby ako spoločnosť so stovkami zamestnancov. Okrem toho pri zvažovaní poistného krytia môže mať ešte významnejší vplyv predmet činnosti spoločnosti (napríklad či ide o spoločnosť pôsobiacu v sektore informačných technológií alebo maloobchodnej spoločnosti, ktorá pôsobí v oblasti prevádzkovania občerstvenia). V oblasti informačných technológií a pri spracúvaní citlivých dát možno predpokladať značne vyššiu expozíciu kybernetickým útokom a s nimi súvisiacim rizikám. Je nutné pripomenúť, aby sa nezanedbala identifikácia potenciálnych hrozieb expertom v danej v oblasti; či už to bude interný zamestnanec oddelenia informačných technológií alebo externý spolupracovník, ktorý vypracuje audit a identifikuje oblasti, ktoré je vhodné zahrnúť do poistného krytia.

Potenciálne hrozby sa najčastejšie zaznamenajú v dotazníku pred podpisom poistnej zmluvy a najmä z toho dôvodu je dobré zabezpečiť si tieto údaje pred stretnutím so zamestnancom poisťovne alebo s finančným agentom. Predíde sa tak kúpe produktov, ktoré sú pre danú spoločnosť absolútne nadbytočné.

Pre výpočet poistného bude pravdepodobne poisťovňa zvažovať parametre ako predmet činnosti danej spoločnosti, typ a rozsah spracúvaných dát, rozsah programovej vybavenosti, úroveň ochrany dát (interné smernice upravujúce nakladanie s dátami a osobnými údajmi, použitie kryptografických nástrojov), rozsah outsourcovania služieb (cloud, platobné služby), technologické vybavenie (hardvér i softvér) a požadované limity plnení.

Ďalším dôležitým zmluvným dojednaním sú výluky z poistenia. Tie sú faktorom, ktorý významne ovplyvňuje, respektíve zužuje rozsah poistného krytia a má vplyv na konečnú cenu poistného produktu. Navyše pri tomto druhu poistenia a jeho technickej zložitosti by sa mal poistník a poistený o uvedenú časť poistnej zmluvy, respektíve poistných podmienok zaujímať ešte detailnejšie, keďže priamo ovplyvnia výšku možného poistného plnenia pri takej citlivej oblasti, akou informačné technológie bezpochyby sú. Najčastejšími výlukami v rámci poistenia kybernetických rizík by mohli byť:

- poistné krytie vzťahujúce sa výsostne na kybernetické útoky pri bežnom vykonávaní poskytovaných služieb (nezahŕňa outsorcované činnosti a pod.),
- krytie sa nevzťahuje na udalosti spôsobené internými zamestnancami,
- škoda spôsobená prenosom počítačového vírusu sa tiež vylučuje,
- krytie sa nevzťahuje na škody spôsobené klientmi poisteného,
- nepreplácajú sa škody, ktoré vznikajú vyrubením pokuty alebo inej administratívnej sankcie,
- pre poistné plnenie sa niekedy vyžaduje identifikácia páchateľa,
- krytie sa niekedy nevzťahuje na náhradu ušlého zisku.

Ako vidieť, rozsah výluk býva rôzny a môže byť veľmi široký, preto je nevyhnutné dôsledne sledovať obsah uvedeného zmluvného dojednania.

ISO štandard a príklad z Veľkej Británie

Štandard ISO 27001:2013[9] vydala Medzinárodná organizácia pre štandardizáciu v septembri 2013. Venuje sa práve základným zásadám v oblasti ky-

bernetickej bezpečnosti; inými slovami, ide vlastne o návod na riadenie bezpečnosti informácií, dát a osobných údajov. Organizácie, ktoré spĺňajú podmienky uvedené v tomto štandarde môžu získať certifikát. Tento štandard je novelou predchádzajúcej normy a líši sa najmä tým, že zohľadňuje nový trend v tejto oblasti – outsourcovanie služieb, čo ma zásadný vplyv na kybernetickú bezpečnosť.

Jedným z príkladov deklarujúcich dôležitosť poistenia kybernetických rizík je strategický dokument[10] schválený vládou Veľkej Británie, podľa ktorého má byť krajina jedným z najbezpečnejších miest na svete pre podnikanie v kybernetickom priestore. Zo strategického hľadiska ide o veľmi dobrý krok, keďže Londýn je najväčšie finančné centrum Európy. Podľa uvedeného dokumentu až 81 % veľkých a 60 % malých spoločností malo skúsenosť z nabúraním sa do zabezpečenia ich počítačových sietí. Zároveň sa uvádza, že náklady na jedno nabúranie sa do zabezpečenia spoločnosti sa medziročne zdvojnásobili.

V stratégii pre kybernetickú bezpečnosť sa ďalej uvádza, aké neblahé dôsledky môže mať narušenie bezpečnosti pre podnikateľský subjekt, jeho know-how a reputáciu. Vláda Veľkej Británie zdôrazňuje, že rast objemu poistenia kybernetického rizika bude mať významný pozitívny vplyv na rast poistného sektora. V súlade s tým sa zaviedol tzv. minimálny štandard pre malé i veľké podniky, ktorý obsahuje nevyhnutné prvky zabezpečenia.

Poistné produkty na slovenskom trhu

Keďže škody spôsobené kybernetickou kriminalitou sa vo svete odhadujú na 300 miliárd až bilión dolárov a majú rastúci trend, nepochybne to otvára trh s kybernetickým poistením aj na našom území. Podľa medializovaného vyjadrenia spoločnosti[11] sa v súčasnosti ponúkajú poistenia zodpovednosti za škodu v súvislosti s ochranou dát. Predstaviteľ inej spoločnosti pôsobiacej na našom trhu sa vyjadril,[12] že okrem samotného úniku dát bude možné kryť aj pokuty a penále udelené orgánmi dohľadu. Podľa jeho slov mnohí klienti využívajú aj možnosť pripoistiť si riziko prerušenia prevádzky následkom kybernetického útoku alebo vydieranie spoločnosti. Z uvedeného vyplýva, že aj v našich podmienkach začína byť po poistení kybernetického rizika dopyt a teda reakcia trhu je úplne prirodzená s vyhliadkou rastúcej tendencie v strednodobom a dlhodobom horizonte.

Práca orgánu dohľadu v súvislosti s kybernetickými rizikami, ktorým sú vystavené poisťovne

Samotné poisťovne sú tiež vyhľadávaným cieľom kybernetických útokov a teda je v ich imanentnom záujme chrániť sa proti takýmto rizikám. Na druhej strane orgán dohľadu si tiež plní úlohy voči poisťovniam, keďže jeho cieľom je zabezpečiť zdravé fungovanie finančného trhu a ochranu finančných spotrebiteľov. Z pohľadu orgánu dohľadu, teda v našej jurisdikcii Národnej banky Slovenska, sa už dnes pri výkone dohľadu kontrolujú oblasti, ktoré nevyhnutne súvisia s poistením kybernetických rizík. Treba poznamenať, že orgán dohľadu, ako aj samotné subjekty potrebujú istý čas na prípravu manuálov pre riadne a detailné hodnotenie tejto oblasti.

Ak však vychádzame z medzinárodných štandardov a dnešnej praxe, pri výkone dohľadu by sa mali posudzovať nasledujúce okruhy:

- úlohy a zodpovednosti vyššieho manažmentu poisťovne v súvislosti s kybernetickými rizikami (na základe interného predpisu, vnútorných pravidiel obsahujúcich monitoring potenciálneho rizika, miery tolerancie voči určitým druhom rizík a pod.),
- vzdelanie, skúsenosti a zručnosti zamestnancov zodpovedných za bezpečnosť informačných technológií,
- kontrola, či sa k zodpovedným pracovníkom dostávajú pravidelné správy týkajúce sa kybernetickej bezpečnosti a prípadných hrozieb,
- existencia základných prvkov elektronickej bezpečnosti (firewall, antivírusové vybavenie, anti-spam, anti-spyware a pod.),
- existencia kontrol kybernetickej bezpečnosti v rámci vnútorných procesov a softvérového vybavenia,
- ak sa vykonáva stresové testovanie kybernetickej bezpečnosti prípadne simulácie útokov, či je riadne zdokumentované a predložené zodpovedným pracovníkom manažmentu,
- využívanie nezávislého audítora kybernetickej bezpečnosti,
- risk manažment pre kybernetické riziko (monitorovanie, analyzovanie a včasná reakcia na prípadné hrozby),
- kontrola, či má subjekt vypracované koncepcie pre posudzovanie kybernetického rizika spôsobeného outsorcovaním určitých úloh,
- školenia zamestnancov na tému ako predchádzať a čeliť kybernetickým hrozbám,
- systém aktualizovania vnútorných predpisov v odpovedí na nové hrozby.

Spoločným menovateľom poistného trhu v Európe je, že subjekty nemajú špeciálnu stratégiu predchádzania kybernetickým hrozbám, ale jej časti sú zahrnuté medzi koncepcie v oblasti správy informačno-technických prostriedkov.

V našom regulatórnom režime zatiaľ chýba povinnosť oznamovať kybernetické incidenty orgánu dohľadu. S prihliadnutím na trend v iných členských štátoch, ako je napr. Francúzsko a Veľká Británia, kde táto povinnosť existuje a je vynútiteľná pod hrozbou administratívnej sankcie, však možno očakávať, že sa uvedené v strednodobom horizonte premietne aj do našej legislatívy, najmä s nárastom ponuky produktov v tejto oblasti.

Záverom možno konštatovať, že téma poistenia kybernetického rizika bude mať nepochybne rastúcu tendenciu. Vyplýva to najmä zo systematického nárastu kybernetických útokov a tiež dopytu po tomto druhu poistenia.

9 *Medzinárodná organizácie pre štandardizáciu. Štandard pre kybernetickú bezpečnosť. Dostupné na https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en*

10 *Stanovisko vlády Veľkej Británie z 5.11.2014 týkajúce sa kybernetickej bezpečnosti. Dostupné na: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf*

11 *Bližšie pozri http://www.allianzsp.sk/su-kyberneticke-utoky-nastraho-u-buducnosti*

12 *Mittaš, M. Proti hekerom sa dá chrániť aj poistiť. Dostupné na: http://www.nextfuture.sk/poistovne/clanky/proti-hekerom-sa-da-chranit-aj-poistit/*