Kybernetická bezpečnosť v poisťovníctve – hrozba i príležitosť

Matúš Medvec[1]
Národná banka Slovenska

V článku Poistenie kybernetických rizík uverejnenom v časopise BIATEC v júni 2015 sme sa venovali charakteristike kybernetického poistenia a jeho základným parametrom. V tomto čísle sa zameriame na jeho najnovší vývoj z pohľadu európskych krajín a medzinárodných organizácií.

Poistenie kybernetického rizika sa prvýkrát objavilo v druhej polovici deväťdesiatych rokov, no jeho rozšírenie sa zaznamenalo približne pred desiatimi rokmi. V tom období sa vyskytli prvé rozsiahlejšie kybernetické útoky jednak na štáty, respektíve na štátne orgány, ale aj na súkromné spoločnosti. Práve vtedy sa začal používať pojem kybernetická kriminalita.[2]

Dnes sa vývoj posunul ďalej a problematikou sa zaoberá široké spektrum verejných či súkromných inštitúcií. Medzinárodná organizácia pre spoluprácu a rozvoj (OECD), Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (EIOPA), Medzinárodná organizácia pre poisťovníctvo (IAIS) a centrálne banky členských krajín EÚ či orgány dohľadu stále pozornejšie sledujú tému kybernetického rizika. Je nepochybné, že s trendom informatizácie, práce s veľkými databázami, analytickými nástrojmi na vyhodnocovanie a prispôsobovanie predaja, ako aj s poskytovaním finančných služieb cez internet a prostredníctvom rôznych druhov aplikácií sa tlak na kybernetickú bezpečnosť zvyšuje. Obzvlášť je to badať v takom citlivom sektore na ochranu osobných údajov, akým je finančný sektor.

Kybernetické riziko ako výzva i hrozba pre poistný sektor

V sektore poisťovníctva sa téma kybernetickej bezpečnosti skloňuje ešte intenzívnejšie. Hlavným dôvodom je, že poisťovne sú nielen subjekty, ktoré sú vystavené možným kybernetickým útokom, ale sú aj poskytovateľmi ochrany voči takýmto útokom. V neposlednom rade sú aj predmetom dohľadu orgánov verejnej moci, v našom prípade Národnej banky Slovenska, pri riadení operačného rizika, pod ktoré spadá aj bezpečnosť informačných systémov.

Ak to rozmeníme na drobné, možno konštatovať, že je vo vlastnom záujme finančnej inštitúcie, aby sa chránila pred akoukoľvek vonkajšou hrozbou. Tým, že v dnešnej dobe sa informačné systémy využívajú stále intenzívnejšie a obsahujú stále viac údajov (databáza klientov, správa portfólia, finančné toky, účtovníctvo, elektronické verzie dokumentov a pod.), sa priamoúmerne zvyšuje aj riziko, že tieto údaje budú vystavené kybernetickej hrozbe. Tá má rôzne implikácie, no najvýraznejšou môže byť pozastavenie vnútorných procesov, napr. ak sa prelomí systém na uzatváranie nových kontraktov, čo má priame dôsledky na ziskovosť subjektu. Z nepriamych dôsledkov je najvýraznejšie reputačné riziko. Strata alebo sprístupnenie finančných či osobných údajov o klientoch bude mať dozaista negatívny vplyv na subjekt, čím, prirodzene, môže utrpieť aj dôvera zo strany jeho obchodných partnerov.

Kybernetické incidenty sa však netýkajú len poisťovní samotných, ale akéhokoľvek podnikateľského subjektu. To, samozrejme, vytvára prirodzený dopyt po poistnom produkte, ktorý by firmy proti rôznorodým rizikám, ktoré z kybernetických hrozieb vyplývajú, chránil. Ako príklad možno uviesť najrozšírenejšie predmety poistenia: 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 a ďalšie. Problémom naďalej zostáva upisovanie rizika. Inými slovami, z dôvodu nedostatku historických dát sa ťažšie podľa matematicko-poistných modelov vypočíta poistné. To je jedným z hlavných dôvodov relatívne vysokej ceny produktu (poisťovne nevedia exaktne produkt ohodnotiť, a teda z dôvodu obozretnosti majú tendenciu nastavovať cenu na vyššiu úroveň), čo robí produkt menej dostupným a utlmuje jeho rast. Dokonca sa odhaduje, že práve z tohto dôvodu je dnes cena produktu trojnásobná oproti hypotetickej, ak by sme poznali exaktné dáta za dlhšie časové obdobie.

Najnovší vývoj na trhu

Potenciál trhu je však silný, čo deklaruje nielen rast informatizácie a automatizácie vo všetkých

1 *Názory autora prezentované v tomto článku sa nemusia nutne zhodovať s oficiálnymi stanoviskami a postojmi NBS.*
2 *Medvec, M. a Čillíková, J.: Poistenie kybernetických rizík. Dostupné na: http://www.nbs.sk/_img/Documents/_PUBLIK_NBS_FSR/Biatec/Rok2015/06-2015/04_biatec_15-6_Medvec-Cilikova.pdf*

oblastiach spoločnosti, ale aj rast kybernetických incidentov na jednej strane, ako aj rast počtu predaných poistných produktov na strane druhej.[3] Aktuálne sa odhaduje, že ročné poistné[4] v USA v tomto segmente dosahuje 2,75 miliardy USD, no podľa spoločnosti PwC má poistné v oblasti kybernetického rizika dosiahnuť v roku 2020 viac než 7 miliárd USD.

Čo sa týka frekvencie, aj tá ma rastúci trend: v roku 2014 sa konal prieskum na vzorke 9 700 účastníkov, na základe ktorého sa odhadlo, že došlo k 43 miliónom incidentov (čo je viac ako 100 tisíc denne). Oproti predchádzajúcemu roku išlo o nárast o 48 %. Za rok 2015 došlo k nárastu o 38 %.[5] Podľa ďalšej analýzy sa odhaduje, že denne sa vo svete stane viac než 200 tisíc kybernetických incidentov a ročná strata spôsobená kybernetickou kriminalitou je viac než 400 miliárd USD.[6] I keď exaktné čísla nie sú k dispozícii a analýzy a odhady sa rôznia, pri ich porovnaní si vieme predstaviť rozsah, v akom sa pohybujú škody. Napríklad nedávna štúdia Lloyd's a University of Cambridge odhaduje, že straty plynúce z kybernetických incidentov sa pohybujú v rozmedzí od 243 miliárd do 1 bilióna eur.[7]

Podľa prieskumu Európskej agentúry pre informačnú bezpečnosť sa kybernetické riziko dostalo v priebehu troch posledných rokov z pätnásteho na tretie miesto[8] z pohľadu potenciálu narušiť chod podnikateľského subjektu, čo poukazuje na jeho značne rastúcu tendenciu. Rovnako aj prieskum spoločnosti Allianz[9] zaradil kybernetické riziko do prvej desiatky (tretie miesto) rizík, ktoré majú priamy vplyv na výkon podnikateľskej činnosti. Na druhej strane, podľa uvedených prieskumov je kybernetické riziko na prvom mieste spomedzi oblastí, na ktoré sú spoločnosti pripravené najmenej. To len dokresľuje priestor na trhu a nutnosť intenzívnejšie sa touto témou zaoberať. Spomedzi dôvodov sa najčastejšie uvádza nepochopenie bezprostrednosti hrozby, chybné vnímanie, že sa to týka len veľkých spoločností, iné priority a pod.

Priemerný poistný produkt na krytie kybernetického rizika má limit krytia v objeme od 5 do 25 miliónov USD[10] a poistné sa pohybuje od 7 do 50 tisíc USD v závislosti od toho, o akú veľkú spoločnosť ide, v akej oblasti pôsobí a aké činnosti vykonáva.[11] Treba však dodať, že nejde o produkt „a la carte" a jeho konkrétnej ponuke takmer vždy predchádza komplexné vyhodnotenie informačného zabezpečenia a procesov, ktoré konkrétna spoločnosť vykonáva.

Kybernetické riziko z pohľadu orgánu EIOPA

Objem hrubého predpísaného poistného v EÚ sa odhaduje na 150 až 200 miliónov eur,[12] a preto je prirodzené, že sa uvedenou problematikou EIOPA zaoberá. Európsky orgán definuje kybernetické riziko ako časť operačného rizika spôsobeného zlyhaním informačných technológií alebo systémov, ktoré nevyhnutne vyústi do finančnej straty, prerušenia prevádzky, nabúrania dát alebo reputačnej straty spoločnosti. EIOPA sa teda začína na túto oblasť pozerať cez prizmu operačného rizika. To môže prirodzene vyústiť do odporúčaní, ktoré budú v tomto smere pretavené na národnú úroveň.

Komplexný prístup OECD

V OECD sa téme kybernetického rizika primárne venuje výbor pre poisťovníctvo a dôchodky (Insurance and Private Pensions Committee, IPPC), ktorý spracoval komplexný projekt pozostávajúci z troch samostatných častí. Možno ho uviesť ako vzor synergie a spolupráce medzinárodných organizácií, konkrétne IAIS a OECD. S realizáciou projektu sa plánuje začať koncom tohto roka a cieľom je detailnejšie mapovať aktuálny stav kybernetickej kriminality a poistného krytia. To má následne zabezpečiť lepšie regulačné rozhodnutia a tým prispieť k zdravšiemu rastu tejto oblasti finančného trhu. Výstupom by mali byť tri správy:

- prehľad trhu a charakteristika poistného krytia dostupného na trhu,
- informovanosť o kybernetickom riziku a možnostiach jeho zmiernenia a prevencie,
- regulačné nástroje, ktoré pomôžu zdravému rastu tohto produktu.

Keďže ide o veľmi komplexný projekt, možno očakávať, že táto analýza poskytne najucelenejší prehľad nových trendov v oblasti kybernetického rizika tak z pohľadu súkromného, ako aj verejného sektora. Najväčšou výzvou však zostane presnosť a heterogenita dát. Nie všetky krajiny majú zákonný mandát na zbieranie takého rozsahu údajov, aký navrhuje OECD. Ak by aj mali, metodika zberu dát v jednotlivých krajinách môže byť do istej miery odlišná od metodiky OECD a skresliť tak celkový výsledok. Treba si však počkať na rok 2017 a analyzovať potenciálne najkomplexnejší prehľad o tejto oblasti.

Aktivity IAIS v oblasti kybernetického rizika

Ďalšia z medzinárodných organizácií, ktorá sa venuje oblasti kybernetického rizika, je Medzinárodná organizácia pre poisťovníctvo.[13] Témou kybernetického rizika sa začala sa zaoberať najskôr vnútri organizácie a pred pár rokmi začala riešiť aj otázky poistenia voči tomuto riziku.

Keďže IAIS zbiera a vyhodnocuje veľké množstvo údajov od svojich členov v rôznych štátoch sveta, prostredníctvom výboru pre audit a posudzovanie rizika analyzovala spôsoby zabezpečenia proti uvedenému riziku vnútri organizácie. Uvedomuje si potenciálne riziko, a tak je téma ochrany pred kybernetickým útokom na programe pravidelného a komplexného monitorovania a posudzovania rizika.

Okrem toho sa IAIS venuje tejto téme aj z pohľadu novej produktovej línie. IAIS poistenie kybernetického rizika charakterizuje ako riziko, ktoré sa týka informačných technológií, a zároveň predpokladá, že k nemu existuje poistný produkt. Najmä členovia v krajinách, kde finančný sektor dosahuje väčšiu signifikantnosť (najmä v USA,

3 *World Economic Forum, The Global Risk Report 2016, 11th Edition.*
4 *The Betterley Report, Cyber/Privacy Insurance Market Survey 2015, June 2015.*
5 *Turnaround and Transformation in Cybersecurity: Key Findings from The Global State of Information Security Survey 2016, PwC, September 2015.*
6 *Economic impact of cybercrime, Mcaffee. Dostupné na http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.*
7 *Emerging Risk Report 2015, Business Blackout, Lloyd's of London, July 2015.*
8 *ENISA surveyed stakeholders in 23 European Union countries, plus Norway, Turkey and the United States.*
9 *Risk Barometer on Business Risks, Allianz, 2016.*
10 *U.S. Insurers Responding Cautiously to Soaring Cyber Coverage Demand, Carrier Management, Standard & Poor's, June 2015. Dostupné na http://www.carriermanagement.com/news/2015/06/12/141360.htm.*
11 *Cyber Insurance: One Element of Risk Management, Deloitte, March 2015, Dostupné na http://deloitte.wsj.com/riskandcompliance/2015/03/18/cyber-insurance-one-element-of-a-cyber-risk-managementstrategy/.*
12 *Promoting U.K. Cyber Prosperity, Long Finance, July 2015. Dostupné na http://www.longfinance.net/lfresearch.html?id=937.*
13 *Webové sídlo IAIS. Dostupné na http://www.iaisweb.org/.*

ktoré reprezentujú až 90 % svetového trhu v tejto oblasti[14], v Anglicku a Číne), sa tejto problematike venujú aj na zasadnutiach.

Oblasťou kybernetického rizika z pohľadu trhu sa začala IAIS venovať v roku 2014 a túto problematiku začlenila do programu pracovnej skupiny pre finančnú kriminalitu. Práce sa v posledných rokoch veľmi zintenzívnili a výsledkom je najmä spoločný projekt s OECD, ktorý ma ambíciu pripraviť komplexné mapovanie produktu, trhu, trendov aj ďalších možných regulačných nástrojov.

Čo sa týka regulačných nástrojov, IAIS ako jeden z normotvorcov vo finančnom sektore plánuje uvedené analýzy pretaviť do aktualizovania základných princípov[15] poistného sektora, konkrétne najmä tých, ktoré sa venujú systému správy a riadenia a operačnému riziku.

Aktivity vybraných krajín EÚ

Veľká Británia

Viaceré európske krajiny sa začali na oblasť kybernetického rizika pozerať detailnejšie. Ako prví sa začali touto oblasťou intenzívne zaoberať kolegovia z Veľkej Británie. To, samozrejme, súvisí s veľkosťou ich finančného sektora a s potenciálom dôsledkov, ktoré by kybernetické incidenty mohli mať. Aj z tohto dôvodu anglické inštitúcie (Bank of England, PRA, HM Treasury a FCA) na tejto téme úzko spolupracujú už od roku 2013. Výsledkom spolupráce je ucelený program predchádzania kybernetickým útokom, ktorý okrem iného obsahuje:

- zoznam hlavných databáz a systémov, ktoré sú vystavené kybernetickým hrozbám najintenzívnejšie,
- dotazník na mapovanie najnovšieho vývoja v uvedenej oblasti,
- testy odolnosti proti kybernetickým rizikám (stresové testovanie),
- fórum v jednotlivých sektoroch finančného trhu o najnovšom vývoji,
- vytvorenie koordinačnej skupiny spomedzi zástupcov verejných inštitúcií, ktoré majú na starosti kybernetickú bezpečnosť.

Výsledkom týchto iniciatív sú aj zistenia a odporúčania adresované subjektom finančného sektora. Týkajú sa najmä prispôsobenia systému správy a riadenia, testovania odolnosti informačných systémov, mapovania možných rizík, prípravy riešenia krízových situácií, schopnosti zabezpečiť kritické funkcie aj pri kybernetickom útoku a systému nezávislého hodnotenia príslušných opatrení.

Momentálne sa vo Veľkej Británii pracuje na ucelenej stratégii kybernetickej bezpečnosti vo forme jednotnej odpovede celého verejného sektora.

Slovinsko

Kybernetická bezpečnosť je aj v centre záujmu menších krajín. Ako príklad možno uviesť Slovinsko, ktoré sa touto témou aktívne zaoberá aj pri priamom výkone dohľadu nad poisťovňami pôsobiacimi na národnom trhu. Kontrola informačných systémov a databáz je zahrnutá do ročného inšpekčného plánu.

Dohľad na mieste vychádza z interného manuálu, ktorý vychádza zo štandardu pre správu a riadenie informačnej bezpečnosti COBIT 5.[16] Orgán dohľadu využíva pri výkone dohľadu aj externého audítora informačných systémov. Za rok je schopný v tejto oblasti vykonať dohľad nad pätinou subjektov pôsobiacich na trhu, čo umožňuje vykonať komplexnú kontrolu kybernetickej bezpečnosti počas rozumného časového horizontu.

Pri výkone dohľadu sa kontrola zameriava hlavne na plány predchádzania incidentom, na existenciu kontroly štyroch očí, softvérové zabezpečenie zabraňujúce externej penetrácii a na krízové plány. Okrem toho sa kontroluje zabezpečenie interných databáz a spolupráca so subjektmi, ktorým poisťovne potenciálne zverili výkon časti svojej činnosti. Pokiaľ ide o zverenie správy citlivých údajov, dohliada sa na to, aby spoločnosť, ktorej sa výkon správy dát zveril, používala minimálne rovnaké štandardy na ich ochranu ako samotný subjekt na finančnom trhu.

Slovinsko, ako každá krajina pôsobiaca na jednom trhu EÚ, má na svojom území aj rôzne pobočky spoločností z iných členských štátov. Pri týchto subjektoch sa zameriava najmä na to, či pobočka pôsobiaca v ich krajine správne a dostatočne proporčne implementuje systém celej skupiny. V tejto oblasti je nutné klásť dôraz na spoluprácu domáceho orgánu dohľadu s orgánmi dohľadu celej skupiny, najmä prostredníctvom výmeny informácií počas rokovaní kolégií orgánov dohľadu.

Pre zlepšenie povedomia na trhu a s cieľom poukázať na dobré príklady z praxe, ale aj na prípady porušenia IT štandardov slovinskí kolegovia organizujú workshopy pre účastníkov trhu.

Česká republika

V Českej republike sa tejto problematike venujú v posledných rokoch ešte intenzívnejšie. V minulom roku nadobudol účinnosť zákon o kybernetickej bezpečnosti. Jeho hlavným cieľom bolo stanoviť podmienky pre spoluprácu verejného a súkromného sektora s cieľom zvýšiť efektivitu riešenia kybernetických hrozieb.[17] Zákon vytvára podmienky aj na nastavenie systému prenosu informácií s cieľom prevencie ďalších potenciálnych hrozieb.

Kybernetický priestor zákon definuje ako digitálne prostredie umožňujúce vznik, spracovanie a výmenu informácií vytvorenými informačnými systémami, službami a sieťami elektronických komunikácií. Keďže zákon sa vzťahuje na významné informačné systémy, otázka znie, či doň budú spadať aj informačné systémy poisťovní. Jedným z prahových kritérií pre tzv. kritické informačné infraštruktúry je aj to, že ekonomický dopad útoku musí predstavovať stratu prevyšujúcu 0,5 % HDP. Kritériá však zatiaľ nespĺňa ani jeden subjekt pôsobiaci na českom poistnom trhu. Ak by sa tak stalo, bude to pre daný subjekt znamenať nové administratívne a operačné náklady.

14 *Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool, Long Finance, June 2015.*
15 *ICP IAIS. Dostupné na: http://www.iaisweb.org/page/supervisory-material/icp-on-line-tool.*
16 *Štandard COBIT V. Dostupné na http://www.isaca.org/cobit/pages/default.aspx.*
17 *Smejkal, V.: Poistné spektrum – zákon o kybernetickej bezpečnosti a informačné systémy poisťovní, Poistný obzor 2/2015.*

Okrem uvedeného nového prvku v právnom poriadku ČR sa tejto téme, síce všeobecnejšie, venuje aj zákon č. 277/2009 Sb. o poisťovníctve[18]. Zahŕňa požiadavky na zachovávanie mlčanlivosti pri práci s informáciami a systémami a obsahuje požiadavky na ich obozretné spravovanie ako súčasť systému správy a riadenia.

Česká národná banka sa tejto problematike venovala ešte hlbšie a vydala úradné oznámenie k výkonu činnosti na finančnom trhu – operačné riziko v oblasti informačného systému.[19] To stanovuje, že subjekt na finančnom trhu má vytvoriť, udržiavať a uplatňovať funkčný a efektívny riadiaci a kontrolný systém vrátane informačného systému. Subjekty sú ďalej povinné vypracovať interné zásady a postupy na vyhodnocovanie a ovplyvňovanie miery podstupovaného operačného rizika vrátane menej častých významných udalostí[20] (kam bezpochyby možno kybernetické riziko zaradiť). Subjekt pri riadení operačného rizika zabezpečí, že bude obsahovať minimálne tieto okruhy: vymedzenie operačného rizika, postupy jeho riadenia, právomoci a zodpovednosť konkrétnych ľudí a útvarov, informácie o významných udalostiach, miery akceptovateľného rizika, ako aj spôsob, ako incident odstrániť. Okrem toho má tzv. povinná osoba, teda napr. aj poisťovňa, pripraviť a vyhodnocovať plány pre mimoriadne krízové situácie, ktoré majú obsahovať postupy, ako udržať chod inštitúcie a limitovať straty.

Takto koncipovaná podzákonná norma vytvára všeobecný rámec pre riadenie celého operačného rizika a ide do požadovanej miery podrobnosti. Nevenuje sa však konkrétne kybernetickému riziku a jednotlivé požiadavky boli vytvorené v roku 2011, teda pred tým, ako sa táto téma začala intenzívnejšie vyvíjať. Z toho pohľadu je vhodné zamerať sa na ňu pri výkone dohľadu a v tomto svetle aj príslušné úradné oznámenie vykladať. Časom však, podľa názoru autora, nastane potreba prijať osobitný dokument, ktorý bude postihovať výsostne tému kybernetického rizika a osobitosti, ktoré so sebou prináša.

Uvedený výpočet príkladov spomedzi členských štátov nie je zďaleka uzavretý, poukazuje však na trendy, akými sa jednotlivé štáty uberajú. Je prirodzené, že menšie krajiny, ktoré disponujú obmedzenejšími zdrojmi, sa nemôžu venovať problematike v takom rozsahu ako veľké krajiny, preto je nevyhnutná intenzívna spolupráca medzi členskými krajinami EÚ.

Situácia na Slovensku

Slovensko ako súčasť EÚ transponovalo v súčasnosti platnú a účinnú smernicu Solventnosť II. Tá je premietnutá do nového zákona o poisťovníctve č. 39/2015 Z. z.[21], ktorý okrem iného obsahuje aj časť týkajúcu sa systému správy a riadenia finančnej inštitúcie.

V § 23 citovaného zákona sa uvádza, že poisťovňa je povinná zaviesť a uplatňovať účinný systém správy a riadenia, ktorým sa zabezpečí spoľahlivé a obozretné riadenie činnosti. V zmysle tohto paragrafu má poisťovňa zohľadňovať a zmierňovať riziká, ktorým je vystavená, resp. ktorým by mohli byť vystavení jej klienti. To jednoznačne implikuje aj obozretnosť vzhľadom na hrozbu kybernetického rizika. Ako v celom režime Solventnosti II, tak aj v tomto zákone sa zdôrazňuje princíp proporcionality, teda že aj operačné riziko sa vyhodnocuje primerane povahe, rozsahu a zložitosti činnosti a rozsahu služieb poskytovaných subjektom pôsobiacim na finančnom trhu.

Okrem iného sa pri systéme správy a riadenia zakotvuje povinnosť prijať primerané opatrenia na zabezpečenie nepretržitého a pravidelného výkonu svojich činností vrátane vypracovania záložných plánov. Tieto plány by teda mali zvážiť aj prípad útoku z kybernetického prostredia, keďže ten môže spôsobiť vážnejšie škody a zasiahnuť do riadneho chodu poisťovne.

Ak sa posunieme o úroveň (v právnej sile) nižšie, usmernenie EIOPA o systéme správy a riadenia[22], ktoré bolo prijaté aj do nášho rámca pre fungovanie poisťovní, zdôrazňuje, že neexistuje jednotný systém riadenia rizík, ktorý by bol vhodný pre všetky podniky; systém sa musí prispôsobiť jednotlivým podnikom. To jednoznačne predpokladá nastavenie systému a jeho prispôsobenie nielen čo do veľkosti, ale aj čo do rizík, ktorým je vystavený. Samozrejme, orgán dohľadu by mal tieto osobitosti vedieť vyhodnotiť a aj aplikovať pri samotnom výkone dohľadu.

Usmernenie sa tiež venuje koncepciám, ktoré sú poisťovne v zmysle zákona povinné pripraviť. Jednou z nich je aj koncepcia riadenia rizík. Tá ma v súlade s usmernením č. 21 obsahovať aj:

- určenie operačných rizík, ktorým je alebo môže byť poisťovňa a zaisťovňa vystavená, a zhodnotenie možností ich zmierňovania,
- činnosti a vnútorné procesy na riadenie operačných rizík vrátane informačných systémov, ktoré ich podporujú,
- limity tolerancie rizík vzhľadom na hlavné oblasti operačných rizík poisťovne alebo zaisťovne.

Z predchádzajúceho jednoznačne vyplýva, že súčasťou koncepcie by malo byť aj identifikovanie kybernetického rizika ako jednej z potenciálnych hrozieb. Koncepcia by tiež mala obsahovať limity tolerancie a možnosti zmierňovania týchto rizík. Ďalej možno uviesť, že významnou požiadavkou pre fungovanie poisťovní je aj nutnosť prehodnocovania koncepcií na ročnej báze. Vytvára sa tak priestor na ich aktualizáciu a zahrnutie nových hrozieb, ako aj procesov a postupov na ich mapovanie a prevenciu.

Poisťovne by mali zaviesť procesy na identifikáciu, analýzu a oznamovanie udalostí spojených s operačným rizikom, ktoré sú významným nástrojom pre prácu samotného orgánu dohľadu a na prípravu nových regulačných predpisov v tejto oblasti.

Ako ďalej s kybernetickým rizikom vo finančnom sektore SR

Napriek viacerým iniciatívam a konštantne intenzívnejšiemu záujmu o uvedenú oblasť stále absentuje komplexný medzinárodný štandard pre

18 *https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=69215&nr=277~2F2009&rpp=15#local-content*
19 *Český zákon o poisťovníctve. Dostupné na https://portal.gov.cz/app/zakony/zakonPar.jsp?idBiblio=69215&nr=277~2F2009&rpp=15#local-content.*
20 *Úradné oznámenie ČNB. Dostupné na https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/legislativa/vestnik/2011/download/v_2011_05_20811560.pdf.*
21 *Zákon o poisťovníctve. Dostupné na http://www.nbs.sk/_img/Documents/_Legislativa/_UplneZnenia-Zakonov/Z0392015.pdf*
22 *Usmernenia EIOPA. Dostupné na https://eiopa.europa.eu/GuidelinesSII/EIOPA_Guidelines_on_System_of_Governance_SK.pdf*

kybernetickú bezpečnosť a manažment či prevenciu s tým súvisiacich rizík prispôsobený osobitostiam finančných inštitúcií. Aj to je dôvodom, prečo sa môže prehodnocovať vytvorenie riešení na národnej úrovni.

Národná banka Slovenska ďalej sleduje najnovší vývoj v tejto oblasti a čerpá skúsenosti jednak z výstupov medzinárodných organizácií a jednak od okolitých európskych partnerov. V tejto súvislosti môže zvažovať aj vytvorenie tzv. okrúhlych stolov, kde by sa vymieňali skúsenosti medzi regulátorom, orgánom dohľadu, trhom a odborníkmi zo sektora informačných technológií. To môže následne vyústiť do interných postupov, prípadne podzákonných právnych nástrojov, ktoré sa tejto téme budú venovať.

Možno teda zhrnúť, že absencia medzinárodných či európskych štandardov v tejto oblasti nepriamo, ale prirodzene núti zvažovať aj čiastkové národné postupy, teda aspoň do ich schválenia.

Prezentácia regionálneho ekonomického výhľadu MMF v NBS

Začiatkom mája sa v Národnej banke Slovenska uskutočnila oficiálna prezentácia regionálneho ekonomického výhľadu Medzinárodného menového fondu pre región strednej, východnej a juhovýchodnej Európy – Regional Economic Issues (REI) Report on Central, Eastern and Southeastern Europe (CESEE). Správa podrobnejšie mapuje a analyzuje hospodársky vývoj CESEE regiónu, ako aj výhľad a riziká ďalšieho vývoja. Spracúva ju európsky odbor MMF dvakrát ročne a spolu s podobnými analytickými správami pre iné regióny nadväzuje na World Economic Outlook, jednu z nosných publikácií MMF. Regionálny ekonomický výhľad MMF prezentovali zástupcovia sekcie rozvíjajúcich sa trhov európskeho odboru MMF – Anna Ilyina, vedúca sekcie, a ekonómovia Ara Stepanyan a Jiří Podpiera. S úvodným slovom vystúpil guvernér NBS Jozef Makúch.

Zľava Jiří Podpiera, Anna Ilyina, Jozef Makúch, Ara Stepanyan a Marek Jakoby.
Foto: Roman Benický