Poistenie kybernetických rizík – globálne trendy a Slovensko

Útok na slovenský kataster nehnuteľností opäť pripomenul, aké vážne následky môžu mať kybernetické útoky. Hackeri dnes cielia na firmy, nemocnice, banky aj infraštruktúru, ich útoky spôsobujú miliardové škody a môžu paralyzovať celé odvetvia. Pritom až 87 % firiem si myslí, že voči kybernetickým rizikám nie sú dostatočne chránené, ukázala štúdia zaisťovne Munich Re z minulého roka.

Popri kúpe bezpečnostných softvérov či školení zamestnancov je jedným zo spôsobov, ako minimalizovať prípadné škody aj poistenie kybernetických rizík. Vo svete sa tento segment poisťovníctva rozvíja rýchlo, Slovensko však zaostáva. Kým globálny trh sa za posledných päť rokov strojnásobil a do roku 2027 môže dosiahnuť hodnotu 29 miliárd dolárov, u nás ostáva poistenie kybernetických rizík len okrajovou záležitosťou.

Poisťovne však pri úpise kybernetických rizík narážajú na problémy. Chýbajú historické dáta, útoky sú nepredvídateľné a veľa firiem kybernetickú bezpečnosť podceňuje. Na Slovensku sa odhodlali ponúkať tento produkt len niektoré poisťovne.

Je však zrejmé, že dopyt po ňom porastie. Rôzne regulácie ako GDPR ale hlavne rýchly vývoj a nárast rizika, nútia firmy zvýšiť bezpečnosť a poistenie sa môže stať dôležitým nástrojom ochrany. Otázkou už nie je, či sa kybernetické poistenie stane štandardom, ale kedy.

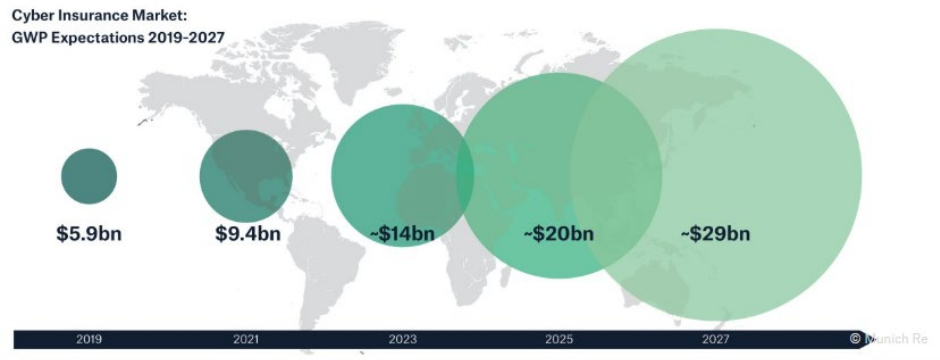
Tento text opisuje základné trendy na globálnom trhu s poistením voči kybernetickým rizikám. Vysvetľuje najčastejšie typy hrozieb a poistného krytia a ukazuje, ako sa poisťovne pri tvorbe týchto produktov snažia vysporiadať s otázkami poistiteľnosti rizika, s dostupnosťou dát, ale aj so skrytým poistením kybernetických hrozieb. Súčasne približuje aj pohľad regulátorov a prináša závery analýzy poistenia kybernetických rizík na Slovensku aj s príkladmi poistného krytia.

Globálny trh s poistením kybernetických rizík

Rýchly technologický pokrok dynamicky mení ľudskú spoločnosť a upriamuje pozornosť nie len na výhody, ktoré prináša, ale i riziká spojené s fungovaním v kybernetickom priestore. K spôsobom ochrany a zmiernenia dopadu kybernetických rizík je možné zaradiť nie len zavádzanie softwarovej ochrany či školenia zamestnancov, ale nepochybne i poistenie proti kybernetickým rizikám, ktoré chráni proti potenciálne až likvidačným následkom možných škôd spôsobených kybernetickými útokmi.

Z pohľadu poisťovní predstavujú kybernetické riziká na jednej strane zvýšenú potrebu vlastnej ochrany, keďže i samotné poisťovne musia čeliť kybernetickým hrozbám a **na strane druhej, príležitosť ponúknuť na trh nový produkt a nové poistné krytie.**

Hoci trh s poistením kybernetických rizík predstavuje stále pomerne malé percento z celkového trhu s neživotným poistením, celosvetovo zaznamenáva veľmi rýchle tempo rastu. Podľa štúdie EIOPA stúpol trh s poistením kybernetických rizík v Európe v súvislosti so zavedením GDPR medzi rokmi 2017 a 2018 až o 71%. (2) Štúdie zaistných domov Munich Re a Swiss Re ukazujú, že za posledných 5 rokov sa celosvetový trh s poistením kybernetických rizík takmer strojnásobil. S rastúcim povedomím o hrozbách, kedy podľa štúdie Munich Re publikovanej v minulom roku, až 87% predstaviteľov firiem po celom svete si myslí, že ich spoločnosť nie je dostatočne chránená voči kybernetickým rizikám (7) a s rozširujúcou sa poistnou medzerou, teda zvyšujúcim sa rozdielom medzi potenciálnymi ekonomickými stratami spôsobenými kybernetickými hrozbami a škodami krytými kybernetickým poistením, existuje značný potenciál pre rast tohto odvetvia do budúcna. Zaisťovne očakávajú, že do roku 2027 by hodnota globálneho trhu s poistením kybernetických rizík mohla dosiahnuť až 29 mld. USD. (7,8)



Zdroj: Munich Re: Cyber risks. Cyber Insurance. Risks and Trends 2024

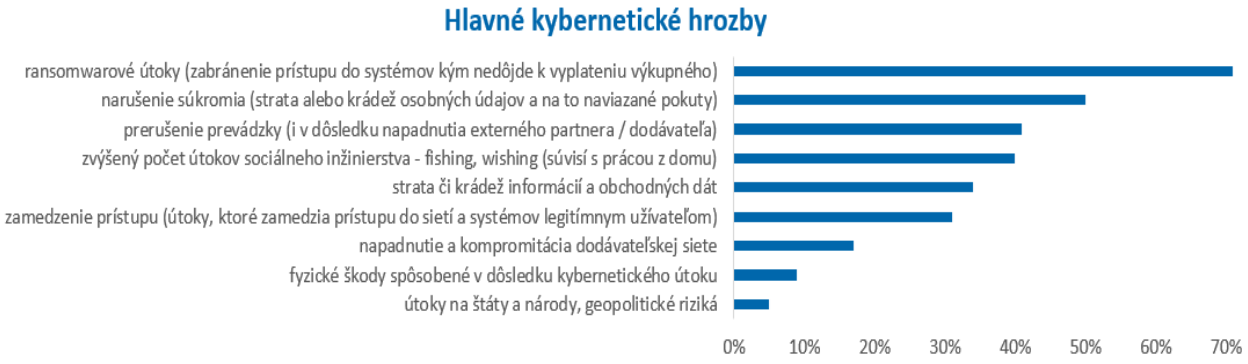
Zároveň je možné badať nerovnomerné rozdelenie celosvetového trhu s poistením kybernetických rizík. Až dve tretiny cyber poistného je upísaných na americkom kontinente, menej než jedna tretina v oblasti Európy a Afriky. (4) Aj napriek tomu, že čoraz viac poisťovní sa snaží do svojho produktového portfólia zahrnúť poistenie kybernetických rizík a to v rôznej miere a podobe, tento druh poistenia je z globálneho hľadiska stále pomerne koncentrovaný. Koncentráciu úpisu kybernetického rizika možno badať i v relatívne malom počte poisťovní / zaisťovní, o ktorých by bolo možné povedať, že sú pre tento druh poistenia globálne významné, s predpisom z poistenia kybernetických rizík vyšším ako 1 mil. USD.

Za celosvetovo zvyšujúcim sa upísaným poistným z poistenia kybernetických rizík nestojí len prirodzený rast, rýchly vývoj a nárast podkladového rizika, ale aj väčšia dostupnosť dát. Od svojich počiatkov prechádza i táto oblasť poistenia zmenami a hoci v porovnaní s tradičnými odvetviami neživotného poistenia je dostupnosť dát z poistenia kybernetických rizík stále nižšia a prirodzene chýbajú historické dáta, s postupujúcim časom majú poisťovne a najmä zaisťovne k dispozícii čoraz väčšie množstvo kvalitatívnych i kvantitatívnych údajov. To je základným predpokladom pre modelovanie kybernetických rizík a následné úpravy rizikových sadzieb používaných poisťovňami pre celkové ocenenie produktu.

Prvé, na mieru šité poistné zmluvy, ktoré poskytovali ochranu pred špecificky pomenovaným kybernetickým rizikom naviazaným na riziko obchodovania na internete, boli upísané ešte v 90. rokoch minulého storočia. I napriek tomu sa v rámci poisťovníctva stále jedná o pomerne nové i keď rýchlo sa rozvíjajúce odvetvie.

Kybernetické hrozby a škody, ktoré spôsobili

Najčastejšie pretaveným rizikom a ťahúňom kybernetických škodových štatistík sú ransomwarove útoky, teda útoky vydieračským softvérom, ktorých rozsah, zložitosť a komplexnosť s technologickým pokrokom rastie. Medzi najčastejšie ponúkané poistné krytia patria dôvernosť údajov, zodpovednostné krytie a prienik do systémov.



Zdroj: IAIS, Global Insurance Market Report (GIMAR) April 2023 (Marsh and Microsoft study 2022)
Tabuľka zobrazuje podiel kybernetických rizík s najvyšším potenciálom spôsobiť poistnú udalosť podľa poisťovní a zaisťovní, ktoré sa zúčastnili štúdie Marsh and Microsoft, 2022

V súvislosti s poistením kybernetických rizík sa poisťovne zamýšľajú i nad otázkou, čo všetko je ešte poistiteľné riziko. Teda zvažujú nie len mieru rizika, pravdepodobnosť vzniku škody, ale napríklad i praktické otázky riešenia poistných udalostí. Nie každé riziko, ktoré vyplýva z kybernetický hrozieb, sú jednotlivé poisťovne ochotné vziať do krytia. Zatiaľ, čo napríklad boj s dezinformáciami v rozsahu odstránenia klamlivého a zavádzajúceho obsahu z internetu a marketingové náklady spojené s napravením dobrého mena, alebo oprava hackerským útokom zablokovaného systému, či obnova dát sú pomerne uchopiteľné riziká, samotná manipulácia volebného výsledku, jej preukázateľnosť je už iným orieškom a môže byť rizikom nepoistiteľným.

najčastejšie typy poistených rizík podľa údajov poisťovní / zaisťovní, ktoré sa zúčastnili štúdie pre GIMAR 2023	
dôvernosť údajov a dát	88%
zodpovednosť	88%
preniknutie do systémov	88%
bezpečnosť sietí	84%
prerušenie prevádzky	84%
kybernetické vydieranie	84%
komunikácia a mediálna zodpovednosť	84%
technologické prerušenie	68%
kybernetický podvod alebo krádež	68%
následné prerušenie prevádzky	52%
iné	12%

Zdroj: IAIS, Global Insurance Market Report (GIMAR) April 2023

Medzi zatiaľ najväčšie kybernetické útoky patrili útoky z roku 2017 WannaCry ransomware, ktorého výsledkom boli škody v hodnote 8 mld. USD alebo NotPetya útok, ktorý po celom svete spôsobil škody v hodnote viac ako 10 mld. USD, z ktorých približne len 3 mld. USD boli poistením kryté. Na to, aby bol hackerský útok pre firmu likvidačný, alebo jej prinajmenšom spôsobil značné škody a komplikácie, ale nemusí mať hneď tak gigantické rozmery.

Podľa štúdie IAIS dosiahla celková hodnota čistých poistných udalostí spôsobených kybernetickými rizikami na konci roku 2021 sumu 4,2 mld. USD reportovanú členskými krajinami IAIS zapojenými do štúdie. (4) Zatiaľ čo rozloženie celkových škôd kopíruje celosvetové rozloženie poistného, štúdia prezentuje záver, že celková ziskovosť z poistenia kybernetických rizík na vzorke najvýznamnejších poisťovateľov v tomto odvetví má tendenciu byť nižšia ako ich ziskovosť z neživotného poistenia ako celku.[1]

Dostupnosť dát a modelovanie kybernetických rizík

Udržateľnosť odvetvia poistenia kybernetických rizík nevyhnutne predpokladá neustále zlepšovanie upisovacích postupov, teda zberu informácií, merania, odborného posúdenia a

[1] Pomer čistých škôd z kybernetického poistenia uvádzaných touto skupinou poisťovateľov a zaisťovateľov k nimi predpísanému poistnému z kybernetických rizík predstavoval 68%, zatiaľ čo v prípade neživotného poistenia to bolo len 55%. (4) Pri bližšom pohľade na rozloženie hodnôt škodového pomeru ale možno predpokladať existenciu malého počtu relatívne menších poisťovateľov kybernetických rizík, ktorí ale reportovali vysoké poistné udalosti z kybernetického poistenia, čo pripúšťa i samotná štúdia.

ocenenia rizík tak, aby poisťovne dokázali držať krok s dynamickým technologickým vývojom rizík, ktoré berú do krytia. V tejto súvislosti najväčší globálni poisťovatelia poukazujú na nedostatok IT expertov v radoch upisovateľov rizík. Na mieste sú i výzvy k celkovej opatrnosti, kedy vo svetle súčasného trendu škodového vývoja **zaisťovatelia upozorňujú na javiacu sa nedostatočnosť technických rezerv** tvorených poisťovňami práve na kybernetické riziká.

Tieto výzvy sú úzko spojené s nedostatkom údajov, na ktoré modelovanie a hodnotenie rizík kybernetického poistenia stále trpí. Z dostupných údajov o škodách získaných od poisťovní a zaisťovní, ktoré ale zachytávajú skôr udalosti menšieho rozsahu, už boli vytvorené prvé modely predpokladajúce škodový vývoj udalostí ako sú napr. cielené ransomwarove útoky, alebo izolované úniky dát.[2] Nedostatok údajov o udalostiach veľkého rozsahu ale stále obmedzuje modelovanie kybernetických škôd katastrofických rozmerov (Cyber CAT), ako napr. rozsiahly výpadok globálneho cloudu, alebo celosvetový, priamo necielený útok škodlivým softwarom.[3] V rámci diskusií zaznieva ale i názor, že v prípade globálnej kybernetickej udalosti dosahujúcej katastrofické rozmery by sa pravdepodobne jednalo o bezprecedentnú udalosť. Tento pohľad teda kladie viac do popredia potrebu predvídavého myslenia do budúcna ako nutnosť veľkého množstva historických údajov.

Zmierňovanie upísaného rizika a skryté poistenie kybernetických rizík

O vyššej opatrnosti poisťovní pri úpise kybernetických rizík svedčí aj to, že siahajú po využití rôznych foriem mitigácie, teda znižovania rizika, ktoré na seba preberajú.

Prirodzenou ochranou pre poisťovne je zaistenie[4], prípadne spolupoistenie rizík alebo pooling. Takmer všetky poisťovacie domy, ktoré sa zúčastnili štúdie IAIS, presúvali časť prijatého kybernetického rizika na zaisťovateľov. Vyššie percento postúpených rizík pritom nie je ničím neobvyklým v prípade relatívne nových druhov poistenia. Práve zaisťovacie domy disponujú najväčším množstvom dát, poznatkov a skúseností zozbieraných z celého trhu a sú tak katalyzátorom vývoja nových druhov poistenia.

Jasnejšie a prísnejšie formulované poistné podmienky a výluky z poistného krytia, redukcia poistných limitov, či vyššia spoluúčasť pramenia z rastúcich skúseností poisťovní s týmto druhom krytia. Skôr, ako poisťovne kybernetické riziko upíšu, vyžadujú väčšie množstvo dát a skúmajú, či spoločnosti spĺňajú napr. štandardy kybernetickej hygieny[5]. Požiadavky na IT bezpečnosť sa dostávajú do poistných podmienok a nezriedka môžu mať i konkrétnu podobu. Poisťovne tak vyžadujú, aby ich klienti aktívne pristupovali k vlastnej ochrane a minimalizovali pravdepodobnosť a rozsah možných škôd, pričom im zároveň do istej miery dávajú i návod na to, ako k budovaniu vlastnej kybernetickej odolnosti pristúpiť.

[2] V roku 2023 modeloval Lloyd´s globálny dopad hypotetických ale pravdepodobných kybernetických útokov na hlavný platobný systém finančných služieb a následného narušenia globálneho podnikania s potenciálnymi globálnymi stratami vo výške 3,5 bn. USD za obdobie piatich rokov. (6)

[3] I napriek menšiemu množstvu historických dát, analytická spoločnosť CyberCube modeluje 250-ročnú škodovú udalosť spôsobenú kybernetickými rizikami na úrovni 30 mld. USD s frekvenciou vzniku kybernetických katastrofických udalostí nižšou ako je tomu pri prírodných katastrofách. Celkové škody spôsobené prírodnými katastrofami, ako napr. hurikánmi či povodňami pritom dosahujú výšku stoviek mld. USD. (1)

[4] Podľa odhadov zaistného makléra Guy Carpenter až približne 40% globálne upísaného poistného z kybernetických rizík je postúpené na zaisťovateľov. Pre porovnanie, za celé odvetvie neživotného poistenia je to asi len 12%. (4)

[5] Zásady kybernetickej hygieny hovoria napríklad o dostatočnom zabezpečení dát a prevádzky sietí ochranným softwarom, zálohovaní, alebo o prijatí a dodržiavaní rôznych praktík a procesov pri každodennej práci smerujúcich k ochrane a udržaniu odolnosti ich systémov, dát, zariadení i sietí. Vo svojich poistných podmienkach môžu poisťovne vyžadovať napríklad i minimálnu úroveň softwarového zabezpečenia proti kybernetickým útokom, vrátane pravidelných updatov, zálohovania, alebo požiadavku vykonávania pravidelných penetračných testov vrátane testovania zamestnancov simulovanými útokmi, či jednoduchú požiadavku na úroveň používaných hesiel.

Z pohľadu upisovacieho rizika je pre poisťovne rovnako dôležité priznať si i možnú existenciu krytia skrytých kybernetických rizík. Teda rizík upísaných v starších poistných zmluvách so znením poistných podmienok ešte z čias pred tým, ako sa kybernetické hrozby stali materiálnymi. Bez jasnej výluky kybernetických rizík môžu takéto zmluvy obsahovať formulácie, ktoré by v súčasných podmienkach mohli vyústiť do krytia kybernetických rizík a to nie len bez toho, aby bolo toto riziko ocenené v poistnom, ale hlavne bez toho, aby o ňom mala samotná poisťovňa vedomosť a prípadne si zvolila vhodné formy jeho zmierňovania. V tejto súvislosti hovoríme o širokom spektre poistných zmlúv, ktoré môže zahŕňať majetkové, zodpovednostné zmluvy, zmluvy poskytujúce ochranu v prípade prerušenia prevádzky, rôznych podvodov a podobne. Medzi možnosti ako predísť nepriaznivému dopadu neúmyselne krytých kybernetických rizík možno zahrnúť napríklad:

- **preskúmanie portfólia** poistných zmlúv a ich podmienok,
- **testovanie portfólia** so scenármi, ktoré napĺňajú podstatu kybernetických rizík, pričom je dôležité správne vyhodnotiť a otestovať akumulácie rizík, keďže kybernetické útoky môže byť cielené, ale i necielené a zasiahnuť veľkú časť poistných zmlúv a klientov poisťovne,
- **reálne zhodnotenie rizika**, vrátane odhadu veľkosti škôd, ktoré by mohli byť spôsobené kybernetickými útokmi a zároveň skryto kryté,
- **úprava poistných a zaistných podmienok**, ak je to možné, aby nožnice medzi potenciálnou udalosťou, poistným krytím a zaistným krytím portfólia zmlúv boli čo najmenej otvorené.

Poistenie kybernetických rizík a zavádzanie technologických inovácií z pohľadu dohľadu

Otázku poistenia kybernetických rizík a s ním spojeného upisovacieho rizika vnímajú citlivo i inštitúcie dohľadu nad poistným a zaistným trhom po celom svete. Väčšina z nich označuje riziko spojené s úpisom cyber poistenia za rastúce, z čoho pramení potreba jeho monitorovania a prevencie. Kľúčovým pre pochopenie a riadenie rizík je systematický zber dát a ich vyhodnocovanie z pohľadu dohľadu. I preto napríklad EIOPA od roku 2023 zahrnula do ročných reportov Solventnosti II samostatný hárok týkajúci sa práve poistenia kybernetických rizík.

Nemenej dôležitou je otázka operačnej bezpečnosti, ktorá v prostredí EÚ vyústila do prijatia nariadenia o digitálnej prevádzkovej bezpečnosti finančného sektora (DORA)[6].

Ďalším z rozmerov prenikania technologických inovácií do poisťovníctva je i zavádzanie umelej inteligencie a najmä generatívnej umelej inteligencie (genAI) do poisťovacích procesov, ktoré často priamo súvisia s činnosťami tvoriacimi podstatu poisťovníctva ako napríklad úpis rizika, jeho ocenenie alebo likvidácia poistných udalostí a pod. Otázky zodpovednosti za „rozhodnutia AI“ a schopnosť vysvetliť ich, otázky bezpečnosti, férovosti a nezaujatosti, technologické aspekty a mnohé ďalšie sú už teraz otázkami súčasnosti.

Poistenie kybernetických rizík na Slovensku

Zatiaľ, čo globálny trh s poistením kybernetických rizík rýchlo rastie, na Slovensku vidíme skôr útlm tohto druhu poistenia. Národná banka Slovenska uskutočnila v rokoch 2022, 2023 a na prelome rokov 2024/2025 prieskum zameraný na oblasť kybernetických rizík, vrátane poistenia kybernetických rizík. Z prieskumu vyplynulo, že v súčasnosti má poistenie kybernetických rizík na slovenskom poistnom trhu len slabé zastúpenie.

[6] Nariadenie DORA zavádza komplexný rámec a harmonizuje štandardy a prístupy k operačnej digitálnej odolnosti spoločností pôsobiacich vo finančnom sektore, vrátane pravidiel pre riadenie rizík informačných a komunikačných technológií (IKT), podávania správ o incidentoch, zdieľania informácií, testovania prevádzkovej odolnosti, ale i riadenia rizík IKT tretích strán – kritických poskytovateľov služieb.

Predmetné poistenie rôznych typov a rozsahu poskytuje na našom trhu len obmedzený počet poisťovní a pobočiek poisťovní z iného členského štátu, pričom v niektorých prípadoch došlo k pozastaveniu ponuky produktov poistnej ochrany voči kybernetickým rizikám z dôvodov slabého záujmu zo strany klientov o tento produkt. I napriek tomu ale slovenské poisťovne, nad ktorými NBS vykonáva dohľad a ktoré ponúkajú najmä produkty s možnosťou pripoistenia kybernetických rizík, vykázali mierne nárasty poistných zmlúv obsahujúcich krytie tohto rizika. Slovenskí klienti majú zároveň možnosť poistiť sa i proti kybernetickým rizikám aj v zahraničných poisťovniach a to na základe slobodného poskytovania služieb v rámci Európskeho hospodárskeho priestoru. Práve s rozvojom technológií a on-line priestoru sa poskytovanie poisťovacích služieb naprieč EÚ stáva ešte prístupnejším.

Cyber pripoistenie môže v zmysle dojednaných poistných podmienok zahŕňať situácie, kedy sa klient poisťovne stane obeťou podvodných stránok a pochybných internetových obchodov a dôjde k zneužitiu údajov z jeho platobnej karty, alebo internetového či mobilného bankovníctva. Poisťovňa môže napríklad uhrádzať náklady na súdne konanie, alebo zastupovala klienta voči banke. Stáva sa, že tovar, ktorý si klient zakúpil on-line, mu nie je nikdy doručený. V takýchto prípadoch by poisťovňa mohla byť nápomocná pri vymáhaní tovaru, alebo by vyplatila náhradu za nedoručený tovar. Poisťovne však môžu vymedziť skupinu tovarov, ktorých sa takéto krytie netýka, prípadne podmieniť náhradu škody zo zneužitej platobnej karty policajných záznamom, či stanoviť si iné podmienky krytia.

Zneužitie osobných údajov a dokladov na internete napríklad tým, že si podvodník vezme pôžičku na meno poškodeného, je ošemetná situácia, v rámci ktorej môže poisťovňa zabezpečiť právne zastúpenie, uhradiť náklady na súdne konanie, nahradiť samotnú škodu alebo i náklady na vydanie nových dokladov, ktoré boli zneužité.

Ešte citlivejšie sú prípady zneužitia dobrého mena a kyberšikany na internete. V týchto prípadoch vedia poisťovne zabezpečiť odborníkov, ktorí dokážu odstrániť, prípadne vytlačiť nepravdivé informácie poškodzujúce dobré meno klienta z popredných miest internetových vyhľadávačov. V mene klienta kontaktujú a komunikujú s vyhľadávačom alebo správcami rôznych internetových služieb, či sociálnych sietí a žiadajú vymazanie klamlivého a zavádzajúceho obsahu.

Poisťovne a hlavne pobočky poisťovní pôsobiace na Slovensku i v EÚ ponúkajú poistné krytie kybernetických rizík vo forme samostatných produktov i vo forme pripoistení. Slovenské poisťovne pri tvorbe týchto produktov pritom vo veľkej miere využili skúsenosti svojich zahraničných materských spoločností alebo tento produkt outsourcujú. Možnosti poisteného krytia sú pomerne široké a jednotlivé poisťovacie subjekty v EÚ i na Slovensku sa v tejto oblasti zameriavajú na rozličných klientov, ktorými môžu byť právnické i fyzické osoby.

Poistenie kybernetických rizík ponúkané klientom **fyzickým osobám** je zväčša vo forme pripoistenia k iným produktom, ktoré poisťovňa ponúka (napr. poistenie domácnosti) či pripoistenia k platobným kartám pri on-line nakupovaní, asistenčné služby zahrňujúce pomoc IT špecialistov, právnu pomoc pri odcudzení identity, kyberšikane alebo vytlačenie nepravdivých informácií poškodzujúcich dobré meno klienta z popredných miest vyhľadávačov.

Únik dát, vrátane osobných, dôverných a citlivých údajov a neoprávnené nakladanie s nimi, je ďalším typickým rizikom, ktoré pokrývajú cyber poistné zmluvy. Nemusí sa jednať len o dáta danej firmy ale i o dáta tretích osôb. Poisťovne v týchto prípadoch väčšinou uhrádzajú za poisteného škody a náklady právneho zastúpenia voči vzneseným požiadavkám tretej strany, súvisiace hlavne s chybným konaním pri spracovaním týchto údajov, ktoré mohlo viesť k ich zničeniu, skresleniu či znehodnoteniu, k inštalácií škodlivého softwaru či kódu do dát tretej strany, odmietnutiu prístupu tretej strany k údajom, alebo naopak ich neoprávnenému zverejneniu. Pokuty spojené s únikom či zneužitím dát sú taktiež často kryté. Nemalou položkou po kybernetických útokoch bývajú náklady na obnovu dát, ktorá si často vyžaduje pomoc externých špecialistov, náklady na forenzných IT špecialistov, ktorí zisťujú nie len ako k útoku došlo, ale aj ako a či boli ukradnuté dáta zneužité, a následne náklady na ďalšie zabezpečenie, vrátane poradenstva. V prípade úniku dát sú to i náklady na oznámenie dotknutej osobe.

Poistenie kybernetických rizík určené pre **právnické osoby** má zväčša kombinovaný charakter poistenia zodpovednosti za škodu voči tretím osobám a majetkového poistenia. Krytými rizikami môžu byť napr. straty v dôsledku prerušenia prevádzky (prerušenie vlastnej prevádzky, ale i následné prerušenie prevádzky, kedy v dôsledku napadnutia hackermi musí zastaviť činnosť nie len firma, na ktorú bol kybernetický útok spáchaný, ale aj jej odberateľské spoločnosti), vydieranie pri ramsomwerových útokoch a zablokovaní prístupu do systémov, únik dát vrátane dôverných a citlivých informácií či osobných údajov a s tým súvisiace pokuty, náklady na obnovu dát, náklady na IT špecialistov, na zabezpečenie, či PR špecialistov a ďalšie.

Útoky vydieračským ransomware softvérom sú v súčasnosti označované za jedno z hlavných kybernetických rizík. Jedná sa o útoky, ktorými hackeri zablokujú systémy, siete, či dáta spoločností a za ich sprístupnenie požadujú výkupné. V prípade, že by spoločnosť výkupné neuhradila, hackeri spoločnosť vydierajú, či už zverejnením citlivých informácií a osobných dát, alebo sa vyhrážajú zničením samotných dát, celej siete, systémov a podobne. Vyplatenie finančných prostriedkov súvisiace s takýmto vydieraním, teda vlastne zaplatenie výkupného, je taktiež možné kryť poistnou zmluvou. V takomto prípade by výkupné, alebo jeho časť, po odčítaní spoluúčasti, uhradila za poisteného poisťovňa. Častou podmienkou poisťovní pri uzatváraní krytia rizika ransomwarových útokov je utajenie takéhoto krytia zo straty poisteného.

Firmy, ktoré „prežili“ najmä mediálne publikovanú kybernetickú udalosť musia často zápasiť aj s obnovou ich dobrej povesti. Prinavrátenie dobrého mena sa pritom často netýka len spoločnosti samotnej, ale aj fyzických osôb, jednotlivcov, ktorí ju reprezentujú. Náklady môžu v týchto prípadoch zahŕňať marketingové výdavky, náklady na PR poradenstvo, mediálnu a komunikačnú stratégiu a podobne. Ich cieľom by malo byť zamedzenie alebo zmiernenie nepriaznivých dopadov mediálne známeho kybernetického útoku na ďalšiu činnosti firmy, alebo na osobnú i profesionálnu integritu jej zamestnancov a vedúcich pracovníkov.

Dôležitou súčasťou akéhokoľvek poistenia, poistenie kybernetických rizík nevynímajúc, sú i výluky z poistného krytia. V dnešnej dobe sú kybernetickým hrozbám vystavení všetci, jednotlivci, i spoločnosti z akéhokoľvek odvetvia. Rozsah poistného krytia kybernetických rizík prakticky nemá hranice a preto práve výluky dotvárajú finálny obraz toho, čo vlastne poistná zmluva kryje a dodávajú jej obrysy. Pretože nie všetky riziká sú z pohľadu poisťovne poistiteľné. Úplné vymenovanie výluk z poistenia, podobne ako i vymenovanie toho, čo všetko môže poistenie proti kybernetickým rizikám zahŕňať, je prakticky nemožné. Rozsah poistného krytia vždy záleží od konkrétnych podmienok dojednaných danou poistnou zmluvou.

K tradičným výlukám patria akékoľvek úmyselné, podvodné, či dokonca trestné činy. V súvislosti s kybernetickým poistením ale môžeme mať pred sebou zmluvu, ktorá kryje škody na majetku poisteného, ale aj takú, ktorá poškodenie alebo zničenie hmotného majetku klienta z krytia vylučuje. Podobne to môže byť aj s ujmou na živote a zdraví, kam patria i psychické ujmy spôsobené napríklad kyberšikanou, alebo i nevhodnou mediálnou publikáciou. Výluka porušenia duševného vlastníctva, licenčných či patentových práv napríklad neoprávneným zverejnením (čo v prípade úniku dát môže byť reálna hrozba). Alebo v prípade európskych poistných zmlúv výluka nárokov plynúcich z USA, Kanady či Austrálie, teda krajín, ktorých právny systém je založený na inom právnom princípe ako sme zvyknutí v našich zemepisných šírkach.

Z prieskumu NBS taktiež vyplynulo, že len malý počet slovenských poisťovní vykonal posúdenie svojich existujúcich produktových portfólií z pohľadu skrytého krytia kybernetických rizík. Pritom najmä pre poisťovne so širokým kmeňom rôzne starých majetkových a zodpovednostných zmlúv, v prípade ktorých je pravdepodobnosť skrytého kybernetického krytia najvyššia, by takéto posúdenie bolo prínosné z pohľadu riadenia rizík. Naše poisťovne sa pri testovaní rôznych stresových scenárov v súvislosti s kybernetickými rizikami ale sústredia skôr na operačné riziká ako na upisovacie riziko spojené s kybernetickým poistením, vrátane skrytého rizika, či prípadne jeho akumulácie. Pri riadení upisovacieho rizika siahajú poisťovne najmä po výlukách

z poistného krytia. Všeobecné výluky kybernetických rizík sú už bežnou súčasťou dnes upisovaných štandardných poistných zmlúv.

Poistenie kybernetických rizík sa stáva, a v niektorých častiach sveta sa už stalo, etablovaným poistným produktom, ktorý nevyužívajú len veľké firmy a nadnárodné korporácie, ale v čoraz väčšej miere i menšie podniky a jednotlivci. A to hlavne tí, ktorí si uvedomujú potrebu chrániť sa aj pred rizikami, ktoré možno nezachytí ochranný softvér či opatrenia operačnej a IT bezpečnosti. Slovenský trh ale len veľmi pomaly zvažuje toto riziko ako „hodné poistenia", teda výmeny platby poistného za poistnú ochranu v rozsahu poistných podmienok. Faktom ostáva, že kybernetické riziká a útoky rôzneho rozsahu a dopadu sú a ostatnú prítomné i v našej spoločnosti.

Daniela Kašovská

Referencie

1. Cyber Cube (2023). *Cyber Predictions Report 2023*.

   www.cybercube.com

2. EIOPA (2019). *Cyber risk for insurers – challenges and opportunities*.

   https://www.eiopa.europa.eu/publications/cyber-risk-insurers-challenges-and-opportunities_en

3. EIOPA (2020). *EIOPA strategy on cyber underwriting*.

   https://www.eiopa.europa.eu/publications/cyber-underwriting-strategy_en

4. IAIS (2023). *Global Insurance Market Report (GIMAR). Special topic edition – Cyber*.

   https://www.iaisweb.org/activities-topics/cyber-risk/

5. IAIS (2020). *Cyber risks underwriting. Identified Challenges and Supervisory Considerations for Sustainable Market Development.*

   https://www.iaisweb.org/activities-topics/cyber-risk/

6. Lloyd´s (2023). *Lloyd´s systemic risk scenario*

   https://www.lloyds.com/about-lloyds/media-centre/press-releases/lloyds-systemic-risk-scenario-reveals-global-economy-exposed-to-3.5trn-from-major-cyber-attack

7. Munich Re (2024). *Cyber risks. Cyber Insurance. Risks and Trends 2024*.
   https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

8. Swiss Re (2024). *Reality check on the future of the cyber insurance.*

   https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/about-cyber-insurance-market.html

9. poistné podmienky poisťovní a pobočiek poisťovní z iných členských štátov pôsobiacich na Slovensku a poskytujúcich poistenie kybernetických rizík

10. prieskum NBS zameraný na poisťovne, nad ktorými NBS vykonáva dohľad, v oblasti kybernetických rizík