HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
26. – 28. APRÍLA 2024

Odborná spolupráca
NBÚ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Poistíte sa, veríte si alebo to risknete?

Ochrana firmy, ľudí, majetku a duševného vlastníctva v treťom tisícročí nadobúda ďalší rozmer. FOTO: DREAMSTIME

TÉMA

Kyberbezpečnostný incident je niekoľkonásobná záťaž. Finančná, psychická, personálna. Možno by pomohla fajnová náplasť v podobe kyberpoistenia.

Firmám zasiahnutým kybernetickým útokom vznikajú straty v dôsledku prerušenia podnikania, náklady na reakciu na incidenty a neraz aj pokuty súvisiace s porušením ochrany údajov.

Poisťovne, korporácie aj malé firmy preto vášnivo diskutujú o tom, ako nás poistenie kybernetických rizík ochráni pred finančnými stratami.

Nehrnieme sa do toho

Marián Illovský robí audity v informačnej bezpečnosti už dvadsať rokov. Pracoval pre desiatky klientov zo zdravotníctva, technológií, softvérového vývoja, segmentu financií, ale aj z verejnej správy a často s nimi hovorí o ich očakávaniach.

Či už to boli klienti z medzinárodných spoločností alebo lokálnych malých firiem, žiadny z nich nechcel aktívne riešiť poistenie rizík kybernetickej bezpečnosti. „Je možné, že ani nevedia, že je taká možnosť, alebo poisťovne iba veľmi slabo, ak vôbec, ponúkajú taký produkt."

Sme nedôverčiví

„V praxi vidím, že firmy na Slovensku vnímajú kyberpoistenie rôzne, ak vôbec o ňom uvažujú," hovorí Michal Rampášek z advokátskej kancelárie Peterka Partners. Ovplyvňujú to faktory, ako náklady na poistné, ponúkané krytie a vlastné posúdenie firiem, ako sú vystavené rizikám a aké sú potenciálne straty z kyberincidentov.

Najčastejšie sa však aj táto kancelária stretáva s tým, že klienti považujú kyberpoistenie za drahé. Vysoké poistné a vnímané medzery v krytí môžu spochybniť efektívnosť kyberpoistenia ako súčasti celkovej stratégie riadenia rizík.

Kam to ide vo svete

Podľa vedúceho oddelenia komunikácie Národnej banky Slovenska Petra Majera sa však téma poistenia kybernetických rizík už dostáva do popredia.

Súvisí to s expanzívnou digitalizáciou, presunom ľudských činností do online prostredia, so zavádzaním prvkov umelej inteligencie a so silnejúcimi reguláciami, akým bolo aj Nariadenie o ochrane údajov GDPR.

Celosvetovo tak zaznamenáva trh s poistením kybernetických rizík rýchle tempo rastu. S rastúcim povedomím o kyberhrozbách sa očakáva ďalší exponenciálny rast trhu.

Naše míľniky

Počínajúc rokom 2018, čiže novelizáciou zákona o ochrane osobných údajov, je zvýšený záujem o poistenie kybernetických rizík aj na Slovensku. „S pripravovanou implementáciou nariadenia o digitálnej prevádzkovej bezpečnosti finančného sektora – DORA, predpokladáme ešte väčší záujem o túto problematiku," upozorňuje Peter Majer.

V roku 2023 preto uskutočnila Národná banka Slovenska dohľad na diaľku zameraný na oblasť kybernetických rizík vrátane ich poistenia.

Poistenie kybernetických rizík má v súčasnosti na slovenskom trhu relatívne slabé zastúpenie. Slovenskí klienti však majú možnosť poistiť sa proti kybernetickým rizikám v zahraničných poisťovniach.

Ostrovčeky istoty

Situáciu objasňuje Martin Kaňa, výkonný riaditeľ Slovenskej asociácie poisťovní: „Vzhľadom na rôznorodosť rozsahu a typu škôd, ktoré môžu kybernetické riziká v konkrétnej spoločnosti spôsobiť, je ponuka poistenia pre podnikateľov na Slovensku obmedzená na individuálne zmluvy a v niektorých poisťovniach úplne absentuje."

Aktuálne produkty poisťovní na Slovensku v oblasti poistenia kybernetických rizík sú zamerané skôr na fyzické osoby. Poskytujú ochranu v prípadoch útoku v rámci elektronických platieb, ohrozenia alebo zneužitia virtuálnej identity, poškodenia dobrého mena, kyberšikany či pri nákupoch na internete.

Ak chcete viac

Poistenie kybernetických rizík pre právnické osoby má zväčša kombinovaný charakter. Ide o poistenie zodpovednosti za škodu voči tretím osobám a majetkové poistenie.

> Poistenie kybernetických rizík má v súčasnosti na slovenskom trhu relatívne slabé zastúpenie.
>
> **Peter Majer,** Národná banka Slovenska

Krytými rizikami môžu byť napríklad straty v dôsledku prerušenia prevádzky, vydieranie, únik dát vrátane osobných údajov a s tým súvisiace pokuty, náklady na obnovu dát či náklady na IT špecialistov.

Pri tvorbe týchto produktov si musí poisťovňa vymedziť cieľový trh a s ohľadom naň zabezpečiť posúdenie všetkých relevantných rizík. Zároveň pravidelne preveruje a prihliada na udalosti, ktoré by mohli významne ovplyvniť možné riziká pre tento trh.

Hlavná výzva

Tu však podľa Michala Rampáška narazíme: „Ako navrhnúť spoločný, ale pragmatický prístup k riadeniu kybernetických rizík?" Problém je nedostatok dostupných údajov a aj fakt, že modely v dynamickom prostredí kyberhrozieb rýchlo zastarajú.

Ďalším návrhom je hodnotiť kybernetické riziko prostredníctvom ratingu či indexu. Ten objektívne posudzuje stav kybernetickej bezpečnosti organizácie na základe rôznych faktorov. Patria sem napríklad zabezpečenia siete, ochrany údajov a schopnosti reagovať na incidenty.

Rating kybernetického rizika sa môže používať aj na vyhodnotenie rizika kybernetického útoku a určenie ceny poistného alebo krytia.

Fakty nepustia

S tým, že poistenie rizík kybernetickej bezpečnosti pre firmy je špecifikovaný produkt, súhlasí aj Marián Illovský. Upozorňuje preto aj na možnú vysokú cenu takéhoto poistenia. „Organizácie majú problém akceptovať rádovo nižšie ceny za bezpečnostné opatrenia, keďže nemajú ocenené možné riziká."

Podľa Martina Kaňu by rozšíreniu ponuky poisťovní určite napomohlo, keby sa výrazne zlepšila úroveň kybernetického auditu u podnikateľov. Čím lepšie vie klient identifikovať, ale aj správne zabezpečiť kritické situácie a odhadnúť možné škody, tým s väčšou pravdepodobnosťou poisťovňa dokáže poskytnúť na tieto prípady poistnú ochranu.

Chráňte sa

Spoliehať sa iba na poistenie kybernetických rizík nie je dobrá cesta. Organizácie musia už dnes investovať do proaktívnych opatrení, ako sú pokročilé bezpečnostné technológie, školenia zamestnancov o kybernetických hrozbách a robustné postupy ochrany údajov.

Tento prístup zahŕňa implementáciu bezpečnostných štandardov, pravidelné hodnotenia zraniteľnosti a plány reakcie na incidenty na zmiernenie rizika kybernetických incidentov.

EXKLUZÍVNY OBSAH

10 najväčších kybernetických hrozieb pre Európu

Vaša príručná mapa. Čo všetko ovplyvňuje cenu kyberpoistenia

Anketa: Kedy sa rozhoduje top manažment pre opatrenia v kyberbezpečnosti?

ALISON
ALITER TECHNOLOGIES
cyllium LEAD YOUR BUSINESS PROTECTED
ESET
EVIDEN
Progress
CHECK POINT
SOITRON

Špeciálnu prílohu podporujú

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 26. – 28. APRÍLA 2024

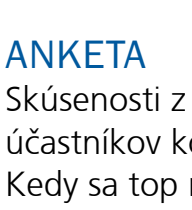
Pomáha osveta, pokuty aj paranoja

ANKETA

Skúsenosti z praxe, úprimné zážitky aj názory účastníkov konferencie SecTec Security Day: Kedy sa top manažment či štatutári rozhodujú pre opatrenia v kybernetickej bezpečnosti?

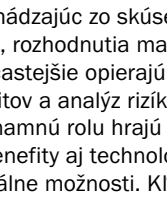
Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Vychádzajúc zo skúseností na trhu, rozhodnutia manažmentu sa najčastejšie opierajú o výsledky auditov a analýz rizík, pričom významnú rolu hrajú náklady a benefity aj technologické a personálne možnosti. Kľúčovými faktormi sú zavádzanie nových technológií alebo systémov, identifikácia zraniteľností alebo situácia po bezpečnostnom incidente, potom zmeny legislatívy a požiadavky noriem, ak chce byť spoločnosť certifikovaná.



Alexander Varga,
informačný architekt,
U. S. Steel

Prioritou je efektívne riadenie rizík, keď sa top manažment opiera o viaceré vstupy. Základný rámec na implementáciu bezpečnostných opatrení určuje legislatíva. Kľúčovým zdrojom sú však pravidelné nezávislé bezpečnostné audity poskytujúce prehľad o aktuálnom stave zabezpečenia a potenciálnych slabinách.



Tomáš Zaťko,
CEO etický hacker,
Citadelo

Osvietení systematicky investujú do bezpečnosti podľa zvážených rizík vo svojom segmente. Samozrejme – ak majú budget. Firmu bez budgetu na bezpečnosť jedného dňa zastihne bezpečnostná katastrofa a potom sa peniaze nájdu. Lebo sa musia. Lenže vtedy je všetko drahšie a náročnejšie.

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies

Rozhodnutia by mali byť súčasťou stratégie a založené na posúdení rizík a technologických potrieb. Vo väčšine prípadov však stále prevláda faktor zistených hrozieb, zraniteľností či nálezy auditov. Čiže akési „donútenie zvonka“. A potom to je často len o vyriešení problémov, nie o stratégii.

Július Selecký,
senior technický špecialista,
ESET

Vrcholoví manažéri sa často rozhodnú pre seriózne opatrenia v kybernetickej bezpečnosti, keď sa spoja tri faktory. Majú osobnú alebo blízku skúsenosť s bezpečnostným incidentom. Do tohto rozhodnutia ich nútia regulácie či zákony. Tretí dôvod zvykne byť paranoja, respektíve strach z narušenia chodu spoločnosti.

Milan Haliena,
vedúci odboru informatiky,
FNsP J. A. Reimana Prešov

Keď si štatutári uvedomia, že v prípade kybernetického incidentu je to vo finále ich zodpovednosť, rozhodujú sa až prekvapivo rázne. Ich rozhodnutie je umenie možného. Vyberú sa opatrenia, ktoré s minimom nákladov riešia čo najväčšie pokrytie hrozieb. A ak už je potrebné investovať finančné zdroje, tak nech je z nich úžitok aj do iných oblastí – napríklad v prevádzke.

Ján Grujbár,
generálny riaditeľ,
Aliter Technologies

Je kategória firiem, ktoré si uvedomujú finančné hrozby a reputačné riziká. Manažment v nich popri budovaní hlavného biznisu priebežne investuje do kybernetickej bezpečnosti. Uvedomujú si, že o rokmi ťažko budovaný úspech je možné prísť nedbanlivosťou zo dňa na deň. V druhej skupine sú firmy, ktoré sa začnú zaoberať kybernetickou bezpečnosťou až vo chvíli, keď sa stanú obeťou reálneho útoku. Vy viete, do ktorej skupiny patríte.

Roman Čupka,
hlavný konzultant,
Progress a CSO Istrosec

Sú len tri príklady štatutárov. Tí, ktorí si spočítajú, koľko stojí prevencia, tí, ktorí platia za kybernetický bezpečnostný incident, a tí, ktorí majú povinnosť plniť regulatívne či legislatívne požiadavky. V konečnom dôsledku nie je medzi nimi rozdiel. Každý jeden v dnešnej dobe investuje nemalé prostriedky do kybernetickej bezpečnosti. A to len preto, aby ochránili svoje podnikanie v čase digitálnej transformácie.

Henrich Šnajder,
manažér IT bezpečnosti,
Orange Slovensko

Po rokoch skúseností a stovkách porád je moja skúsenosť takmer exaktná. Top manažment a štatutári sa rozhodujú pre opatrenia v kybernetickej bezpečnosti z dôvodov rizika straty dát, legislatívnych požiadaviek, spoločenskej zodpovednosti a ochrany biznisu. Ich rozhodnutia sú ovplyvnené aj úrovňou hrozieb, možnými finančnými následkami, reputačnými rizikami a potenciálnymi stratami klientov.

Ivo Kovačič,
obchodný riaditeľ pre komerčný sektor,
Eviden Slovensko

V praxi často vidíme, že sa manažment pre kybernetickú bezpečnosť rozhoduje, až keď nastane problém alebo ho núti zákon. Preto je naším cieľom aj budovanie povedomia a osveta, aby sa manažéri vedeli kompetentne a včas rozhodovať na základe analýzy rizík, hodnoty chránených aktív, bezpečnostného projektu a poznania súčasného stavu. Zároveň je dôležité, aby manažéri sami boli príkladom dodržiavania pravidiel kybernetickej bezpečnosti.

Jaroslav Ďurovka,
riaditeľ,
Národné centrum kybernetickej bezpečnosti

Kedysi sme vymysleli vtipnú tézu, že úlohou manažéra kybernetickej bezpečnosti je udržiavať v hlavách top manažérov primeranú mieru paranoje. V tom prípade je manažment spoločnosti náchylný ľahšie schvaľovať investície do bezpečnostných opatrení. Ak to formalizujeme, ide v podstate o rozhodovanie založené na riadení rizík. Pri presviedčaní pomáha poučenie z incidentov, ale, samozrejme, aj tlak regulácie.

Andrej Mišura,
partner,
Cyllium

Pevne verím, že na základe pravidelného a detailného riadenia rizík, ktoré je vykonávané vyškolenými odborníkmi. Dúfam, že rozhodnutia nie sú na základe odporúčaní predajcu akýchkoľvek blikajúcich technologických škatuliek zapojených v serverovni s nálepkou najbezpečnejšie zariadenie alebo vlastného presvedčenia, že „kto by na nás už len útočil“.

Ivan Makatura,
generálny riaditeľ,
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Podľa prieskumov, ktoré vykonávame už tretí rok, sú na popredných miestach dve motivácie: 1. poučenie z incidentu a 2. odporúčanie dodávateľov. Interpretujem to takto: top manažment sa začne serióznejšie venovať kyberbezpečnosti až vtedy, keď už je neskoro. A potom je náchylný na šikovnosť obchodníkov a riešenia, ktoré sa v korporáciách nazývajú „quick-wins“. Slovač je skrátka nepoučiteľná.

Ján Andraško,
SOC manažér,
Binary Confidence

Z našej skúsenosti sú to tri dôvody. Najčastejšie je to nejaká regulácia, no vtedy je motiváciou väčšinou si bezpečnosť len „odškrtnúť“ s čo najmenšou námahou. Druhým je, že ich do splnenia bezpečnostných požiadaviek tlačí ich klient. No a tým tretím, najmenej častým, ale z nášho pohľadu najlepším, keď má manažment reálny záujem bezpečnosť riešiť.

Igor Urban,
regionálny manažér,
Forcepoint

Rád by som odpovedal, že skôr ako zažijú na vlastnej koži dôsledky bezpečnostného incidentu. Treba povedať, že to je prevažná väčšina prípadov. Iná otázka je samotná motivácia ich rozhodnutí. V ideálnom prípade by to nemali byť len obavy z prípadných postihov. Žiaľ, mám pocit, že najmä v štátnej správe je hlavným motivátorom stále iba splnenie legislatívnych požiadaviek či riešenie zistení auditných nálezov.

Peter Roth,
manažér kybernetickej bezpečnosti,
ANASOFT

Zavádzanie opatrení kybernetickej bezpečnosti pravidelne plánujeme pri aktualizácii analýzy rizík a auditoch kybernetickej bezpečnosti. Prioritami v tomto procese sú kritickosť eliminovaného rizika, jeho dosah a náklady. Ďalším významným dôvodom je bezpečnostný incident. Ak nastane, snažíme sa z neho poučiť a zaviesť opatrenia, ktoré ho v budúcnosti eliminujú.

Tomaš Masný,
riaditeľ informačnej bezpečnosti,
Slovak Telekom & T-Mobile Česká republika

Téma manažment firmy a múdre riadenie pre zisk a bezpečnosť by mohla byť predmetom dizertačnej práce. Manažment má za úlohu dosahovať ciele firmy, budovať jej konkurencieschopnosť a dôveru zákazníkov. To si vyžaduje múdre riadenie zdrojov, procesov a bezpečnostných rizík. Investície do bezpečnosti sa oplatia, ak chránia firmu pred škodami a znižujú riziko. Neznalosť rizík vedie k hazardu a skaze. Šalamúnova múdrosť platí aj pre firmy: múdre riadenie vedie k prosperite, hlúpe k pádu. (Príslovia 14, 1)

Tomáš Daniška,
Soitron

Stručne: neskoro :). V ideálnom svete by kybernetická bezpečnosť bola vždy riešená preventívne a prirodzene. V praxi sa však stretávam skôr s reaktívnym prístupom, až keď sa niečo udeje. V lepšom prípade niekomu v okolí, v tom smutnejšom prípade na základe vlastnej skúsenosti. No a potom tu máme ešte národný fenomén riešiť ju najmä preto, aby bola naplnená litera predpisu, bohužiaľ často naoko. Nuž, „rozmohl se nám tady takový nešvar“.

INZERCIA

MS213040/23

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 26. – 28. APRÍLA 2024

Európu ohrozuje aj rastúca závislosť

VAROVANIE

Európska agentúra pre kybernetickú bezpečnosť ENISA zostavila pravidelnú predpoveď TOP 10 kybernetických hrozieb s ohľadom na ich pravdepodobnosť do roku 2030.

Najväčšie kybernetické hrozby

1. Kompromitácia softvérových závislostí v dodávateľskom reťazci

Najvyššie hodnotenou hrozbou ostáva kompromitácia v dodávateľskom reťazci. Vysoké hodnotenie je dôsledkom neustále sa rozširujúcich dodávateľských reťazcov, čo prináša nové potenciálne zraniteľnosti a útoky.

Čoraz viac komponentov a služieb od tretích strán a partnerov by mohlo viesť ku kompromitácii u dodávateľa aj zákazníka.

2. Nedostatok zručností v kyberbezpečnosti

Nedostatok zručností v kybernetickej bezpečnosti sa posunul v rebríčku ENISA z konca zoznamu rovno na druhé miesto najväčších hrozieb. Chýbajú odborníci v celom spektre pozícií vo firmách aj vládnych inštitúciách a stále chýba aj vzdelávanie a osveta zamestnancov v kybernetickej bezpečnosti.

Podľa správy spoločnosti Cybersecurity Ventures bude do roku 2025 pravdepodobne vo svete chýbať v kybernetickej bezpečnosti približne 3,5 milióna ľudí.

3. Ľudské chyby a zneužívanie zastaraných systémov v kyberfyzikálnych ekosystémoch

Masívna a unáhlená akceptácia IoT zariadení, potreba modernizovať staré systémy a súčasne pretrvávajúci nedostatok odborných zručností či poznatkov, školení a porozumenia kyberneticko-fyzického ekosystému by mohli viesť k patovej situácii.

Manuály pre staršie zariadenie prevádzkových technológií sú dostupné online. Keď nájdu kyberzločinecké skupiny zraniteľnosť, dokážu sa zamerať na konkrétne zariadenia alebo iné IoT produkty v priemyselných segmentoch. Dokážu tak odstaviť dôležitú infraštruktúru či celé prevádzky.

4. Využívanie nezaplátaných systémov a systémov po záruke v preťaženom technologickom ekosystéme naprieč sektormi (nový faktor)

Koncept „všetko ako služba“ prináša so sebou množstvo nástrojov a služieb, ktoré vyžadujú časté a synchronizované aktualizácie a koordinovanú údržbu. Táto skutočnosť v kombinácii s nedostatkom odborných zručností predstavuje stále sa rozširujúcu a ťažko zvládnuteľnú plochu zraniteľností, ktorú zneužívajú aktéri hrozieb.

Často ide o komponenty v infraštruktúre, ktoré sú po záruke alebo u dodávateľa, kde nie sú zdroje či kapacity na to, aby zareagoval na útok. Ohrozené sú aj zastarané nemocničné systémy, ktoré sa nedajú aktualizovať, pretože výrobca už neposkytuje podporu.

5. Nárast digitálneho dohľadu, strata súkromia

Verejné či súkromné systémy na rozpoznávanie tváre, digitálny dohľad na internetových platformách alebo úložiská digitálnych identít sa môžu stať cieľom zločineckých skupín.

Umelá inteligencia, kryptomeny a veľké jazykové modely v kombinácii s phishingom a ransomvérom ako službou vedú k čoraz sofistikovanejším podvodným kampaniam. Zločinci už nepotrebujú pokročilé technické zručnosti a stačia im na to aj relatívne nízke náklady.

Predikcia agentúry ENISA opakovane zdôrazňuje rýchlu evolúciu prostredia hrozieb a dynamické vektory útokov. Upozorňuje na skupiny pokročilých trvalých hrozieb a aktérov štátnych subjektov či sofistikovaných organizácií kyberzločincov, ktorí neustále prispôsobujú a zdokonaľujú taktiky.

6. Cezhraniční poskytovatelia IKT služieb ako bod zlyhania

Kybernetická bezpečnosť čoraz častejšie zlyháva v dôsledku globalizácie a prepojenia infokomunikačných služieb. Táto hrozba medziročne postúpila až na pozíciu šesť.

Sektor IKT služieb, ktorý spája kritické služby ako dopravu, elektrické siete a priemysel, bude pravdepodobne čoraz častejšie cieľom hrozieb ako nasadenie malvéru cez „zadné vrátka“, fyzickej manipulácie či DDoS útokov.

7. Pokročilé dezinformačné kampane

Deep fake útoky slúžia na manipuláciu s komunitami z geopolitických dôvodov či kvôli finančnému zisku.

Veľké jazykové modely dokážu v rekordne krátkom čase produkovať autentické texty a odpovede, ktoré môžu byť následne zneužité. Rovnako sa výstupy používajú na šírenie dezinformácií a manipuláciu s verejnou mienkou.

8. Nárast pokročilých hybridných hrozieb

V dôsledku zvýšenia počtu inteligentných zariadení, využívania cloudu, online identít a sociálnych platforiem sa rozvíjajú fyzické alebo offline útoky a často sa kombinujú s kybernetickými útokmi.

9. Zneužitie umelej inteligencie

Manipulácia s algoritmami umelej inteligencie a tréningovými dátami môže byť zneužitá na zvýšenie škodlivých a protizákonných aktivít. Sem patria hrozby ako tvorba dezinformácií a falošného obsahu, využívanie predsudkov, zbieranie biometrických údajov a ďalších citlivých dát, vojenské roboty a „data poisoning“, čiže niečo ako otrava či infekcia zdrojových dát.

10. Dosah fyzikálnych a prírodných vplyvov na kritickú infraštruktúru (nový faktor)

Zvýšená závažnosť a frekvencia environmentálnych katastrof v dôsledku klimatických zmien môže spôsobiť nečakané regionálne výpadky a poruchy. Redundantné záložné miesta, ktoré zabezpečujú dostupnosť kritickej infraštruktúry, sú rovnako masívne ovplyvňované extrémnymi poveternostnými javmi.

Zdroj: ENISA, Foresight Cybersecurity Threats for 2030

KOMENTÁR

Pekné grafy už máme, dôležité je však ich uplatnenie v praxi

Agentúra ENISA v jednej zo svojich strategických priorít už minulý rok publikovala výstup z analýzy budúcich hrozieb a výziev v kybernetickej bezpečnosti do roku 2030.

Závery analýzy sú výsledkom dlhodobej práce a pripomienkovania viacerých skupín odborníkov na základe vopred vypracovanej metodiky. Oblasť kybernetickej bezpečnosti sa však pomerne dynamicky vyvíja, a preto sa správa dočkala aj svojej aktualizácie.

Výsledok analýzy nie je až takým prekvapením. Ak by sme sa pokúšali vypracovať podobnú predikciu na Slovensku, s veľkou pravdepodobnosťou by bol výsledok rovnaký, prípadne by sa zásadne neodlišoval.

Možno nemusíme úplne rovnako vnímať ranking jednotlivých hrozieb. To však nie je až také dôležité. Podstatné je, aby sme tieto hrozby a dynamiku ich pôsobenia vnímali a postupne prijímali kroky na ich elimináciu. Pozastavme sa nad niektorými z nich.

Začnime hrozbou s najvyšším rizikom, teda kombináciou dôsledku a pravdepodobnosti jeho pôsobenia. Je predpoklad, že práve hrozba kompromitácie systémov a služieb založená na závislostiach softvérových komponentov dodávaných a integrovaných tretími stranami sa do roku 2030 stane najvýznamnejšou.

Tvorba softvéru sa dnes totiž rýchlo transformuje do agilnej formy kontinuálneho vývoja a nasadzovania. Interní či externí vývojári využívajú rôzne open-source komponenty a knižnice a tie vzájomne kombinujú a integrujú do jedného funkčného celku.

Práve uvedené komponenty a postupy môžu využívať hekeri a hekerské skupiny na infiltráciu škodlivého kódu a ten následne využijú pri útokoch.

Zaujímavé je umiestnenie hrozby nedostatku zručností v aktualizovanom rankingu na druhom mieste. Ako uvádza ENISA, táto hrozba spočíva v získavaní informácií z pracovného trhu.

Je totiž predpoklad, že ak istá organizácia hľadá na trhu veľké množstvo zamestnancov na voľné pozície v IT oblasti alebo v oblasti informačnej bezpečnosti, zrejme trpí ich nedostatkom. Ergo spôsobilosť takejto organizácie odolávať kybernetickým útokom môže byť nižšia.

Vzhľadom na výskyt témy na konferenciách a v médiách je prekvapením, že hrozba zneužívania umelej inteligencie sa umiestnila až na ôsmom mieste. Hoci téma je veľmi populárna, výsledok analýzy vychádza zrejme z triezveho zhodnotenia možností umelej inteligencie na úrovni dnešných znalostí.

Dynamika vývoja umelej inteligencie a jej využívanie aktérmi kybernetických útokov budú však hodné zreteľa.

V každom prípade bude veľmi dôležité okrem sledovania vývoja hrozieb primerane na ne reagovať. Prevencia musí spočívať nielen v postupnom nasadzovaní moderných bezpečnostných technológií, ale aj vo vzdelávaní expertov v oblasti kybernetickej bezpečnosti. Jednoznačne potrebujeme zvýšiť úsilie v oblasti kvality systému vzdelávania.

V neposlednom rade musí Slovensko prijať takú politiku, aby mladých odborníkov u nás nielen vychovávalo, ale motivovalo zostať – pracovať alebo podnikať. Práve kvalitných a zručných ľudí v oblasti kybernetickej bezpečnosti potrebujeme ako soľ.

Jaroslav Ďurovka, riaditeľ Národné centrum kybernetickej bezpečnosti

Mohol by to byť biznis snov

ANALÝZA

Trh s poistením kybernetickej bezpečnosti je vnímaný ako dynamický a s najväčším potenciálom na rast a rozvoj v poistnom priemysle. A napriek tomu ho sprevádzajú rozpaky.

Kyberpoistenie si trúfajú zatiaľ ponúkať predovšetkým silné globálne finančné domy. FOTO: DREAMSTIME

Ukážme si to na príklade

Zatiaľ čo globálny trh s poistením vozidiel v súčasnosti predstavuje hodnotu viac ako 600 miliárd dolárov, trh s poistením kybernetickej bezpečnosti bol ohodnotený na 16,6 miliardy. Dramatický rozdiel je však v predpoklade, ako budú trhy rásť nasledujúcu dekádu. Poistenie vozidiel očakáva medziročne rast niečo vyše päť percent, kyberpoistenie takmer 25 percent.

Celosvetovo tak badáme zdravé formovanie tohto trhu.

Dokonca v roku 2022 sme mohli pozorovať pokles v počte nahlásených a riešených poistných plnení. A hoci tento trend opätovne mnohí pripisujú vojne na Ukrajine, keď hackerské skupiny zmenili svoje zameranie, obrovský dopyt zo strany organizácií, ako aj zvýšený záujem z poisťovní naznačujú, že predpoklad rastu je opodstatnený.

Čo sa dá a nedá poistiť

V jednoduchosti? Základný princíp je rovnaký ako pri poistení vozidiel, keď sa snažíme vykryť straty spôsobené následkami dopravných nehôd.

Kyberpoistenie kryje straty spôsobené kybernetickými incidentmi. Sem patria napríklad straty pri prerušení činnosti spoločnosti, odškodnenie klientov či náklady spojené s obnovou systému.

Vzhľadom na komplexnosť problematiky má však aj tento typ poistenia výnimky, pričom záleží aj na obchodnom modeli poisťovne. Tými najčastejšími výnimkami sú prieniky cez tretie strany, sociálne inžinierstvo, vnútorné hrozby, štátom sponzorované útoky, zneužitie známej zraniteľnosti a výpadky, ktoré nie sú zapríčinené kyberincidentom.

Poisťovne to vedia

Podľa odhadov pracuje v kybernetickej bezpečnosti celosvetovo 5,5 milióna pracovníkov. Ich počet rastie, ale zároveň s tým rastie aj rozdiel v ponuke a dopyte po špecialistoch. V kyberbezpečnosti stále absentujú takmer štyri milióny pracovníkov.

Kombinácia ekonomickej neistoty, rapídneho vývoja technológií, fragmentovanej legislatívy a chýbajúcich špecialistov tak môže predstavovať nebezpečnú kombináciu pre celý kybernetický priestor. Poistenie kybernetickej bezpečnosti by mohlo prispieť k zmierneniu tejto neprívetivej prognózy.

Poistenie nie je všeliek

Tak ako pri opotrebovaných pneumatikách či tečúcom motorovom oleji nám nenapadne riešiť poistenie, nemalo by kyberpoistenie predstavovať prvotný zámer pri ošetrovaní rizík.

> Poisťovne majú len limitované historické dáta o kybernetických incidentoch a ich dosahoch.
>
> **Michal Srnec,**
> vedúci oddelenia informačnej bezpečnosti Aliter Technologies

Samozrejme, presun rizika je legitímna stratégia, ako ošetriť identifikované riziko. Netreba však zabúdať na to, že sa používa najmä vtedy, ak je ošetrenie samotného rizika neefektívne pre organizáciu alebo ide o extrémne nepravdepodobný scenár.

V niektorých prípadoch môže byť kyberpoistenie dokonca kontraproduktívne. Niektoré skupiny hackerov si totiž pri úspešnom ransomvérovom útoku priamo pýtajú detaily poistenia kybernetickej bezpečnosti.

Najdrahšie poistky

Pochopiteľne, že čím vyššie je ohrozenie, tým je vyššia cena poistky. Preto neprekvapí, že medzi premiantov patria finančný a technologický sektor a zdravotníctvo. Tieto sektory vyžadujú vysoké úrovne ochrany a poistenie musí byť špecificky prispôsobené na zvládanie ich jedinečných rizík.

Najťažšou úlohou pre poisťovne sú však malé a stredné firmy. Často im chýbajú finančné a personálne kapacity na kyberbezpečnosť a potenciálny finančný dosah incidentov je pre ne devastujúci, čo zvyšuje cenu poistenia.

Ako u nás doma

Hoci sa rozprávame o globálnom trhu s miliardovou hodnotou, stále je to relatívne nový druh poistenia a samotné poisťovne majú problém s odhadovaním rizika.

Tento fakt je jasne badateľný aj na slovenskom trhu s kyberpoistením. Poisťovne majú len limitované historické dáta o kybernetických incidentoch a ich dosahoch. Tento samotný fakt, samozrejme, značne sťažuje odhadnúť a správne nastaviť rizikový model pre danú spoločnosť a správne nastaviť aj cenu poistenia.

Niektoré poisťovne tak limitujú rozsah samotného poistenia či sú nútené dvíhať jeho cenu. Tento fakt akcentuje aj Národná banka Slovenska, ktorá v štúdii uvádza, že pravdepodobnosť výskytu kybernetického útoku je vyššia ako pravdepodobnosť výskytu poistnej udalosti.

PORADŇA

V akom štádiu je novela kyberzákona?

Národný bezpečnostný úrad zverejnil predbežnú informáciu o príprave očakávanej novely zákona o kybernetickej bezpečnosti.

Nepôjde o zásadnú revolúciu, avšak novela by v praxi mala znížiť riziká súvisiace s rýchlym technologickým vývojom, digitalizáciou a zvýšiť celkovú úroveň kybernetickej bezpečnosti našej krajiny.

Novela identifikuje prevádzkovateľov základnej služby podľa konkrétnych kritérií napríklad na základe veľkosti, čo zmení spôsob identifikácie týchto povinných osôb. Pôsobnosť zákona sa rozšíri o nové sektory a regulované služby.

Ako novú hodnotu pre posúdenie rizikovosti a kritickosti subjektu definuje aj kritickú základnú službu. Od toho sa budú odvíjať povinnosti, bezpečnostné opatrenia, audity aj kontrola.

Nové bezpečnostné opatrenia budú kopírovať európsky štandard a smernicu NIS2.

Novelizáciou sa zavedie minimálna kybernetická hygiena. Zároveň sa zruší kategorizácia a klasifikácia informácií a informačných systémov a nahradí ich analýza rizík ako univerzálny nástroj pre aplikáciu opatrení.

Zavedie sa aj zodpovednosť za plnenia bezpečnostných opatrení pre subjekty v dodávateľskom reťazci.

Zabezpečí sa zvýšenie úrovne a kvality zdieľaných informácií, keďže sa zefektívni hlásenie hrozieb, zraniteľností, udalostí odvrátených na poslednú chvíľu a kybernetických bezpečnostných incidentov.

Prispeje to k zvýšenej informovanosti o kybernetických hrozbách, čo zase zvyšuje schopnosť subjektov predchádzať tomu, aby sa takéto hrozby stali incidentmi.

Zmeny zasiahnu aj sankčný mechanizmus. Cieľom je zavedenie novej formy správneho sankcionovania a zefektívnenie vynucovania pokút.

Do 25. apríla bola sekcia regulácie a dohľadu NBÚ otvorená návrhom verejnosti a začiatok pripomienkového konania sa predpokladá na máj 2024.

Zdroj: aktualita NBÚ

RIEŠENIA

Vaša príručná mapa. Čo všetko ovplyvňuje cenu kyberpoistenia

V princípe je proces poistenia obchodné rokovanie s poisťovňou. A na to sa dá predsa pripraviť.

Svet kyberzločinu neskrotíme, ale poistná matematika si už poradila so všeličím.

Obvykle je najľahšie riešiť kyberpoistenie zariadení, prípadne výkupné, lebo sa dajú dobre vyčísliť. Poistenie dát je problematické z hľadiska stanovenia hodnoty.

Atraktívne ciele kyberútokov totiž predstavujú technické, konštrukčné či výskumné dáta z hľadiska priemyselnej špionáže.

Najčastejším cieľom sú osobné údaje, ktoré sa následne využívajú na krádež peňazí či odcudzenie identity. Hneď v tesnom závese sú zdravotnícke údaje, ktoré umožňujú vydieranie kvôli reputácii alebo vyhrážanie sa poškodením zdravia.

Cena je vždy dôležitá

Samotnú cenu kyberpoistenia ovplyvňujú štyri základné faktory. Základný kontext sa vytvára v kombinácii vstupov poistenca, rizík reálneho sveta a poistnej štatistiky, takže to nechám v kompetencii poisťovne.

Do ceny poistky vstupuje hodnota hmotných a nehmotných aktív. Principiálne si treba povedať, čo chceme poistiť a akú hodnotu to má. Možným škodám, samozrejme, najlepšie rozumie manažment firmy.

Cena poistky zohľadňuje vstupy podľa rizík, kam patria externé útoky, útoky zvnútra a prevádzkové chyby.

Štvrtým faktorom, ktorý ovplyvňuje cenu poistky, sú opatrenia, ktoré môžete urobiť interne alebo ich obstarať ako službu.

Analýza a projekt

Pozrime sa na škálu IT služieb, ktoré koncept bezpečnosti pokrývajú. Mnohé z nich sú nevyhnutným predpokladom na uzavretie výhodného poistenia.

Dobrá stratégia sa začína bezpečnostnou a rizikovou analýzou. Na jej základe je postavený bezpečnostný projekt, ktorý obsahuje plán ochrany a opatrení na základe konkrétnej situácie. Ak ste niekde počuli výraz „papierová bezpečnosť“, presne to je tá etapa, kde má kvalitná dokumentácia svoje opodstatnenie.

Testy a vzdelávanie

Penetračné testovanie pomôže odhaliť možné slabé stránky. Ďalšie testy by vám mali odhaliť reakciu systémov na útok aj na výpadok či schopnosť obnovenia systémov a dát. Šance odolať kyberútoku zvyšuje pravidelné vzdelávanie všetkých používateľov, a ani top manažment nie je výnimkou. Aj vďaka tréningom dokáže napríklad pani účtovníčka odhaliť falošný e-mail predtým, ako na urgovanie „riaditeľa“ presunie peniaze na neznámy účet.

Dnešný svet je komplikovaný a previazaný právnymi zodpovednosťami. FOTO: DREAMSTIME

Vyladené nástroje

Medzi nevyhnutné opatrenia pri kyberpoistení patrí správa identít a prístupov a monitorovanie, pričom práve v tomto trhovom segmente je v súčasnosti široká ponuka riešení. Rovnako ako aj v prípade ponuky nástrojov na správu dát a ochranu proti úniku.

V tejto kapitole opatrení sa pripravte na to, že poisťovňa sa vás bude pýtať na oprávnenosť zbierania, ochranu a mazanie dát podľa GDPR.

Vyššia liga

Máte hardvér, softvérové vybavenie a často prevádzkové technológie. A s nimi všetky zraniteľnosti, či chcete, alebo nie. Preto je tu dôležitá detekcia a správa zraniteľností.

Bezpečnostnú architektúru dopĺňajú systémy na správu udalostí a incidentov, riadenie odpovedí a opatrení. Služby ako stredisko bezpečnostných operácií (SOC) či orchestráciu bezpečnosti, automatizáciu a reakciu (SOAR) si firmy z dôvodu personálnej i odbornej náročnosti väčšinou outsourceujú.

Spoločná úloha

Globalizácia prináša IT dodávateľom a službám mnoho príležitostí, ale aj výziev. Postaviť sa im znamená prepájať stratégie zamerané na inovácie, adaptabilitu a kontinuálne vylepšovanie kybernetickej bezpečnosti.

Uvedomujeme si, že prináša čoraz vyššie nároky na bezpečnosť dodávateľov. A zároveň IT služby, ktoré poskytujeme, musia byť v súlade so zvyšovaním kyberodolnosti zákazníkov.

Ivo Kovačič,
obchodný riaditeľ
pre komerčný sektor
Eviden Slovensko