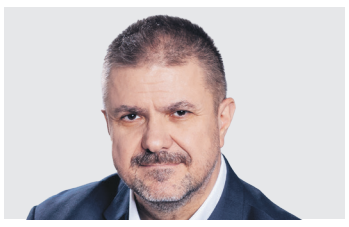
Ktoré oblasti sú najviac nedocenené?

ANKETA

Ešte žiadna iná otázka nezosypala takú smršť rýchlych odpovedí, ako téma, ktorá oblasť kybernetickej bezpečnosti na Slovensku je najviac nedocenená. Napriek širokému spektru účastníkov a rôznorodosti ich skúseností nad všetkým vyčnieva jedna téma.

Za ostatné roky urobilo Slovensko výrazný posun v tom, ako je na medzinárodnej scéne hodnotená jeho kybernetická bezpečnosť. Ale stále je čo zlepšovať. Odpovede profesionálov sa zosypali ako lavína. Ich vzácnou súčasťou sú však návrhy na zlepšenie.



Ivxkatura
generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti

Nad odpoveďou vôbec nemusím rozmýšľať: vzdelávanie a zvyšovanie bezpečnostného povedomia. Slovensko má akútny nedostatok kvalifikovaných ľudských zdrojov v kybernetickej bezpečnosti. Štát v tejto veci dlhodobo nekoná tak, aby čo najskôr vyplnil túto medzeru. A keďže vzdelávanie je na Slovensku najmä štátne, výčitky smerom ku politikom sú namieste. Situácia je doslova kritická. Nízka úroveň spôsobilostí je závažným zdrojom incidentov kybernetickej bezpečnosti.

Rastislav Janota
riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

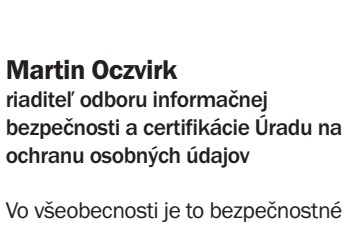
Na Slovensku je stále dôležitá každá oblasť kybernetickej bezpečnosti. Väčšina firiem a organizácii, vrátane a nielen v prípade verejnej správy, túto tému ignoruje. Rozhodne jej nevenuje ani minimálne nevyhnutnú pozornosť, nechápe ju ako dôležitú. Organizácie spravidla nerealizujú ochranné opatrenia, nevzdelávajú svojich ľudí a podobne. Ani školy neprodukujú absolventov, média sa téme stále venujú menej, ako by si zaslúžila, verejná diskusia sa sústredí najmä na spôsoby, ako sa povinnostiam vyhnúť a nie na to, ako to robiť dobre.

Jaroslav Oster
predseda Správnej rady preventista.sk

Stav kybernetickej bezpečnosti je dnes v takom žalostnom stave, že vytipovať, ktorá z problémových oblastí patrí k najviac nedoceneným oblasť je takmer nemožné. Ale ak sa na otázku pozrieme z nadhľadu a smerom do budúcnosti tak najpravdepodobnejšie je to dnes prevencia. Stačí urobiť rýchly prieskum, aký nízky objem finančných prostriedkov je vynakladaných na preventívne aktivity podporujúce znižovanie „ľudských“ rizík napríklad v školstve či samosprávach (ale nie len) a námety na riešenie sa ponúkajú samé.

Tomáš Hettych
viceprezident ISACA Slovakia, Asociácia Auditu a Kontroly Informačných Systémov

Podľa mňa je najviac nedocenenou oblasťou kybernetickej bezpečnosti riadenie kontinuity činností - Business Continuity Management (BCM). Aktuálna „koronakríza“ ukázala v plnej nahote (ne)pripravenosť drvivej väčšiny podnikov a organizácií na zmenu modelov podnikania, na nové typy hrozieb a incidentov. Doterajšie vnímanie BCM ako zbytočnej nákladovej položky, či len ako požiadavky regulácie, sa dramaticky a rýchlo mení. Organizácie potrebujú nové krízové plány, plány kontinuity činností, prehodnotiť nové hrozby a riadiť nové riziká. A paradoxne sa nejedná už len o stredné a veľké podniky. Kto sa neadaptuje, pravdepodobne môže mať problém s prežitím.



Martin Oczvirk
riaditeľ odboru informačnej bezpečnosti a certifikácie Úradu na ochranu osobných údajov

Vo všeobecnosti je to bezpečnostné povedomie a vzdelávanie v tejto oblasti. Pozornosť by som primárne upriamil na všade prítomné mobilné zariadenia. Dnes má skoro každý smartfón, kde má uložené hory dát a osobných údajov. A často si neuvedomujeme, že veľa týchto dát dobrovoľne a aj nedobrovoľne zdieľame napríklad zlým zabezpečením. V dnešnej dobe je nevyhnutnosťou začať rozprávať o kybernetickej bezpečnosti už na prvom stupni základnej školy. Samozrejme prijateľnou formou. To isté platí aj pre seniorov. Tiež je potrebné zaviesť plošné vzdelávacie programy vo verejnej a štátnej správe ako pre technický tak aj netechnický personál.

Lukáš Neduchal
podpredseda Správnej rady Asociácie kybernetickej bezpečnosti

Vzdelávanie. A to na všetkých úrovniach, či už z pohľadu koncového používateľa, alebo IT profesionála. Z hľadiska IT hrozieb je tu veľká skupina, ktorá zneužíva rôznymi spôsobmi základné neznalosti používateľov, alebo základné zraniteľnosti neošetrených systémov. Kolegovia z brandže preto pripravili aj metodické materiály pre výuku IT bezpečnosti a bezpečného správania sa už na základných školách. Kontinuálne vzdelávanie a zdieľanie užitočných informácií je jednou z hlavných výhod profesijných združení a asociácií.

Andrej Žucha
generálny riaditeľ Alison Slovakia

Slovensko je poznačené chýbajúcou kontinuitou bezpečnostných projektov v štátnej správe aj samospráve. Mám za to, že silná vízia a zároveň profesionálna revízia míľnikov by zabezpečili nielen vysoký štandard projektov, ale aj cenovú efektívnosť riešení. Bezpečnosť by nemala byť mýtizovaná oblasť, ani hracia karta politických kampaní a agenda na sociálne siete. Je to vážny atribút budúcnosti krajiny a súčasť medzinárodných záväzkov. A často chýba k tejto téme práve takýto pragmatický prístup a reálny výkon v teréne.

Peter Dostál
generálny riaditeľ a predseda Predstavenstva Aliter Technologies, a. s.

Najviac nedocenené oblasti kybernetickej bezpečnosti v administratíve a štátnej správe sú popri vzdelávaní zamestnancov, kontinuálny monitoring a kontrola bezpečnosti samotných aplikácií. Bežne sa stáva, že aj napriek ochrane infraštruktúry a stavaniu silného perimetra, sa útočníci dostávajú dnu cez otvorené dvere a okná v aplikáciách. Pri priemyselných podnikoch a v domácnostiach je to stále sa rozširujúca sieť IoT. Dnes je väčšina elektrických zariadení riadená vstavaným počítačom pripojeným do siete. Z výroby sú tieto zariadenia nastavené tak, aby sa vedeli čo najjednoduchšie pripojiť do Internetu. Žiaľ bez ohľadu na bezpečnosť.

Roman Čupka
hlavný konzultant Flowmon pre strednú a východnú Európu

Výskum, vývoj a podpora inovácií. V porovnaní napríklad s Českom či Poľskom zaostávame a pomyselný vlak nám každým dňom uniká. Chýba ucelený program duálneho vzdelávania na stredných aj vysokých školách, rovnako ako jednoduchá podpora inovatívnych projektov a začínajúcich technologických firiem zo strany štátu. Aj preto na Slovensku vzniklo doteraz iba málo “start-upov" s vlastným vývojom a produktmi, ktoré dokázali preraziť na zahraničných trhoch. A to napriek tomu, že podpora v tejto oblasti by bola prínosom pre ekonomiku a zabránila odlivu študentov aj vzdelaných odborníkov do zahraničia.

Andrej Aleksiev
riaditeľ pobočky Check Point Software Technologies na Slovensku

Kybernetická bezpečnosť na Slovensku je všeobecne zaznávaná téma obzvlášť vo sfére mobilných a smart zariadení. Už v roku 2016 sme zaznamenali, že viac browsujeme na internete cez mobilné telefóny ako cez počítače – 51,3 percent v porovnaní so 48,7. Ak pridáme k tomuto fenoménu fakt, že každé mobilné zariadenie má dve kamery, mikrofón, zväčša zapnutú geolokáciu, prístup k citlivým aplikáciám ako internet banking a množstvo osobných údajov, mobilné zariadenie sa stáva atraktívnym terčom útokov pre hackerov. Priznajme sa, kto má dnes chránený mobil tak dobre ako počítač?

Igor Urban
regionálny manažér Forcepoint pre východnú Európu

Fenoménom, ktorému sa v našich končinách venuje pramálo pozornosti, je behaviorálna analýza. Máme sanačné nástroje v prípade úniku dát, ale chýba nám predvídavosť, kedy môže prísť k úniku, alebo dokonca útoku, forenzný prístup a následné dokazovanie. Toto je nočná mora asi každého bezpečáka a právnikov. A pritom sa dá niektorým hrozbám predchádzať, keďže sa dajú softvérovo predvídať. Za každým útokom aj únikom dát je totiž človek a konkrétna motivácia. Na prvý pohľad nesúvisiace aktivity predznamenávajú, že časom môže dôjsť k bezpečnostnému incidentu.

Marek Král
generálny riaditeľ SecTec

Určite treba zapracovať na zvýšení všeobecnej gramotnosti v oblasti kybernetickej bezpečnosti. Najjednoduchšie pre hackerov je „nachytať“ interných zamestnancov spoločnosti a spôsobiť škody zvnútra organizácie. Treba sa viac venovať zvýšeniu bezpečného správania cez špecializované školenia a cielenú evanjelizáciu. A to nehovorím o školení bezpečnostných špecialistov, to je iná dôležitá téma. Zároveň veľmi chýba dlhodobejšia stratégia a koncepcia kybernetickej bezpečnosti vo veľkej väčšine organizácií, kde sa poväčšine implementujú iba riešenia, ktoré plátajú aktuálne diery.

Jana Puškáčová
manažérka útvaru Informačná bezpečnosť MOL IT & Digital Slovensko

Veľké rezervy vidím v doťahovaní kybernetických projektov do úplného konca, čiže aby výstupy projektu pokrývali technologické, procesné a ľudské požiadavky. Ak sa projekt končí stavom „technology ready“, samotné dychberúce technológie bez zavedenia nových alebo úpravy existujúcich procesov a bez dostatku ľudských zdrojov zvyčajne nepostačujú na ochranu prostredia zákazníka. Tie isté technológie dnes môžu zabezpečiť viacerí dodávatelia – práve preto pridaná hodnota v podobe návrhu či ladenia procesov na podporu technológií, ako aj identifikácie ľudských zdrojov potrebných na jej prevádzku, môže byť konkurenčnou výhodou ponuky na projekt v oblasti kybernetickej bezpečnosti. Zákazník očakáva kompletné riešenie, nie len implementovanú technológiu ako takú, ale aj odborné znalosti a skúsenosti dodávateľa pri stanovení a následnom naplnení rôznych potrieb a požiadaviek nevyhnutných pre jej spoľahlivé fungovanie.

Richard Kiškováč
Security Consultant Digital Systems, a. s.

Bude to možno znieť ako klišé, ale budem to opakovať znovu a znovu. Za najviac nedocenenú oblasť kybernetickej bezpečnosti považujem budovanie a udržiavanie bezpečnostného povedomia používateľov, alebo zákazníkov. Napriek všeobecnej zhode v odbornej verejnosti o dôležitosti bezpečnostného povedomia sa do tejto oblasti trvale investuje najmenej v porovnaní s inými. Druhou najmenej docenenou oblasťou je vzdelávanie špecialistov kybernetickej bezpečnosti, kde naše školstvo zatiaľ nevie adekvátne zareagovať na potreby trhu.

Tomáš Zaťko
CEO Citadelo, etický hacker

Crowdsourcing bezpečnosti. Bug bounty programy, ako napríklad slovenské HackTrophy, kedy etickým hackerom dovolíte, aby hľadali diery vo vašich systémoch a hlásili vám ich. Mnoho manažérov sa tohoto systému bojí. “Prečo by som mal dovoliť hackerom útočiť na mňa?”, čudujú sa. Bug bounty programy pozývajú práve tých, ktorí vám chcú pomôcť. Zločinci na pozvanie nečakajú. Kriminálnici vás hackujú aj teraz, keď čítate tieto riadky. A čo tí dobrí? Dovolili ste im pomáhať vám? Alebo to majú zakázané?

Pavol Adamec
výkonný riaditeľ oddelenia Riadenie rizík KPMG Slovensko

Zatiaľ nevieme vytvárať v ľuďoch od ranného veku návyky bezpečného správania sa v digitálnom priestore. Deti už v škôlke učíme, že na červenú na ceste majú zastať. Že nemajú v počítači na všetko „klikať“, ich často naučíme, až keď prvý raz zavíria počítač alebo mobil. Dva roky sa snažíme pracovať s deťmi základných a stredných škôl a vidíme obrovskú existujúcu dieru vo vzdelávaní. Kybernetická bezpečnosť je o ľuďoch - tvorcoch a prevádzkovateľoch systémov, používateľoch aj útočníkoch. Mať ľudí schopných tvoriť a prevádzkovať systémy bezpečne nie je jednoduché, ale je to zvládnuteľné.

Marián Trizuliak
architekt kybernetickej bezpečnosti, Západoslovenská distribučná, a. s.

Kybernetickú bezpečnosť nevidíte, až kým sa niečo nestane. A to je viac či menej dobre. Dobré ale nie je, že na trhu chýbajú kvalifikovaní pracovníci, ktorí majú chuť pracovať, nemajú neadekvátne požiadavky a sú angažovaní. Nedocenených oblastí je viac – ja však vnímam ako nedocenenú oblasť najmä zdravý ľudský rozum. Bezpečnostným pracovníkom sa totiž nestanete vyštudovaním jednej alebo viacerých univerzít, ale tvrdou prácou, silnou vôľou a rokmi praxe v rôznych oblastiach IT resp. OT prostredí..

Ján Adamovský
Chief Security Officer Slovenská sporiteľňa

Vzdelávanie a budovanie povedomia v oblasti kybernetickej bezpečnosti u nás patrí medzi dlhodobo zanedbávané oblasti. Od malička nás učia ako správne prejsť cez cestu, no nevieme, ako sa bezpečne pohybovať po digitálnych diaľniciach, hoci ich už ako deti využívame. Myslím, že tu by sa mal svojej úlohy chopiť štát a zaviesť komplexnú stratégiu rozvoja vzdelávania. Zároveň tu vidím aj priestor pre spoluprácu so súkromným sektorom, ktorá by spoločne posunula túto oblasť vpred.

V záverečnej piatkovej ankete budú účastníci o týždeň odpovedať na otázku

- Koho a čoho sa treba vyvarovať v kybernetickej bezpečnosti?