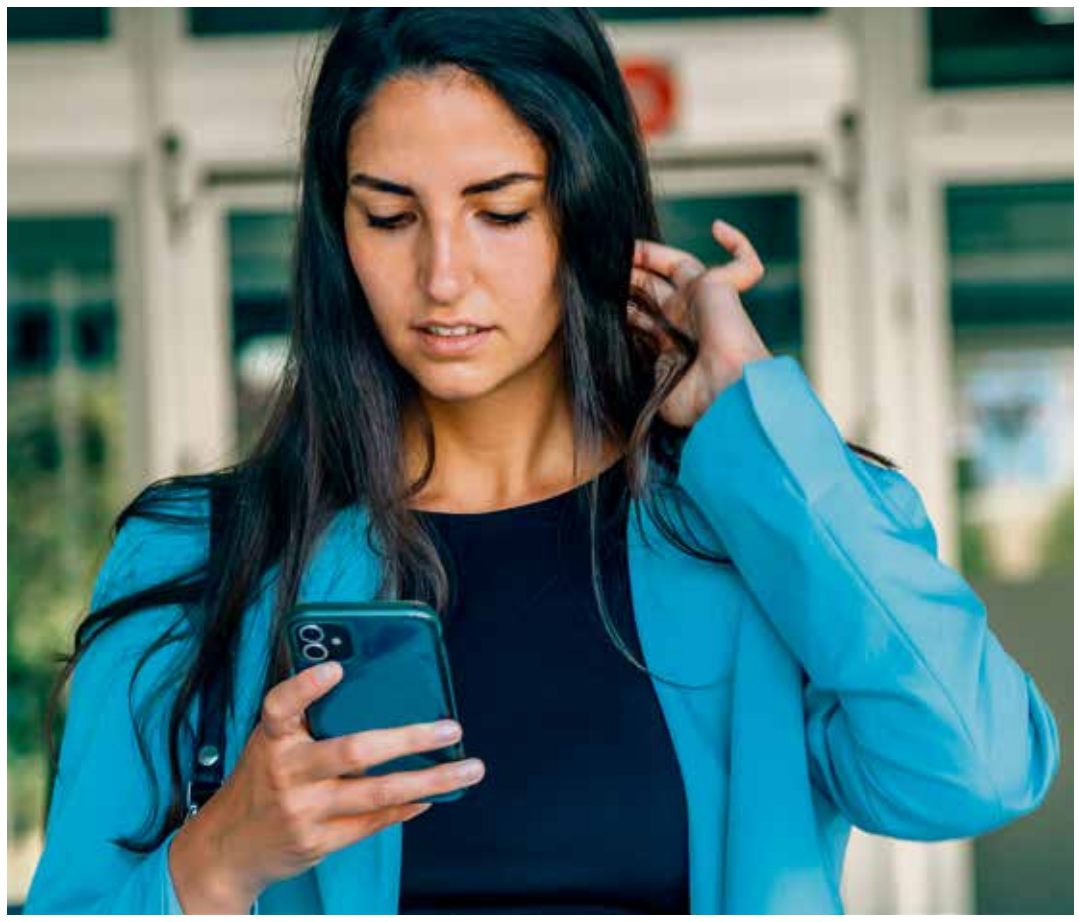
Čo sa stane, ak veríte aplikáciam a vývojárom

TREND

Väčšina súčasných porušení bezpečnosti je spôsobená zraniteľnosťami v aplikáciách.



Keď majú bezpečnostný problém aplikácie, máme problém všetci. SNÍMKA: DREAMSTIME

Trh požaduje čoraz viac aplikácií s častejšími aktualizáciami a IT sa musí požiadavkám prispôsobiť.

Tlak na rýchlosť vývoja a zároveň bezpečnosť aplikácii je enormný. V kombinácii s faktom, že na trhu práce je neustály nedostatok kvalifikovaných vývojárov, to predstavuje úzke hrdlo inovácií vo všetkých segmentoch.

Tajomstvo vývojárov

Ako uvádza správa State of the Software Supply Chain, priemerne 80 percent kódu aplikácií pochádza z open source knižníc. Niektoré významné porušenia bezpečnosti sú spôsobené práve zraniteľnosťami v kódoch tretích strán. Priemerne každá aplikácia tak obsahuje 38 známych open source zraniteľností.

Ďalším slabým miestom je, ak sú aplikácie vytvorené softvérom tretích strán a ich vývoj riadia marketingové tímy. Aplikácie v malých firmách sú často mimo bežných obchodných procesov, a to s minimálnym alebo so žiadnym riadením.

Čísla nepustia

Stále hovoríme o aplikáciách, ktoré sa šíria prostredníctvom webových stránok, platforiem sociálnych médií, mobilnými zariadeniami a v cloude. Čiže nás dosiahnu prakticky všade.

Podľa správy 2019 Application Security Risk Report od Software Security Research 80 percent aplikácií obsahuje najmenej jednu kritickú alebo vysokú zraniteľnosť, 90 percent bezpečnostných incidentov je spôsobených zneužitím chýb v dizajne alebo kóde softvéru.

Problémy budú rásť

Ak sa bezpečnostný tím zapája až do posledných fáz vývoja, je vnímaný v tomto procese ako „brzda“. Výsledkom je, že keď sa zistia slabé miesta v neskorších fázach, firmy čelia časovému stresu. Ten vedie k interným nezhodám medzi tímami a často k oneskoreným termínom vydania.

> Ak sa bezpečnostný tím zapája až do posledných fáz vývoja, je vnímaný v tomto procese ako brzda.

A tak sa stáva, že do výroby sa posúvajú aj aplikácie so známymi bezpečnostnými chybami, aby splnili harmonogram. Výsledkom je stav, keď sú producent aj jeho zákazníci vystavení bezpečnostným hrozbám.

Veľa peňazí

Ako uvádza smernica NIST, náklady na nápravu bezpečnostných chýb sú tridsaťkrát drahšie vo výrobe a desaťkrát vyššie pri testovaní, ako keby boli zachytené v počiatočných fázach vývoja.

Jediný spôsob, ako zabezpečiť aplikácie bez ďalších nákladov, je prístup k bezpečnosti aplikácií riadený vývojármi. Napríklad Fortify Static Code Analyzer skenuje a zároveň opravuje kód, ktorý sa „práve píše“. Programátor tak okamžite vidí chybu, ktorú mu softvér vyhodnotí, a súbežne mu navrhne opravu. Šetria sa tým v obrovskom objeme financie aj čas vývojárov.

Niet o čom diskutovať

Bezpečnosť aplikácií vrátane mobilných sa stáva neoddeliteľnou súčasťou životného cyklu softvéru bez toho, aby vytvárala ďalšiu záťaž pre zainteresované strany.

Tento prístup je zažitý ako Development – Security – Operations, čiže vývoj – bezpečnosť – prevádzka. Na bezpečnosť je potrebné myslieť už od skorých fáz životného cyklu, keďže nájdenie a odstránenie chýb je rozhodne lacnejšie a časovo úspornejšie.

V ostatných pätnástich rokoch je lídrom v oblasti bezpečnosti aplikácií práve vývojársky nástroj Fortify, podľa spoločnosti Gartner ôsmy rok na najvyššej pozícii v Magic Quadrant for Application Security, ktorý definuje profesionálne štandardy a očakávania.

Posun doľava?

V bezpečnostnej brandži sa zažil Shift Left prístup. Znamená plnú integráciu do súčasného vývojového prostredia, automatické spúšťanie v rámci cyklu kontinuálnej integrácie, poskytovanie analýzy kvality a otvorenosť pre integráciu s bezpečnostnými riešeniami iných spoločností.

Tento prístup má ešte jeden strategický a neprehliadnuteľný dôvod – priebežná možnosť auditovať proces vývoja aplikácií. Práve vďaka auditom majú IT manažéri jasný prehľad o štruktúre vývoja, sú schopní lepšie plánovať ďalšie kroky a organizácie spĺňajú nároky bezpečnostných politík a štandardov.

Anna Stehlíková, manažérka pre bezpečnostné licencie pre región Česka a Slovenska Micro Focus

V Únii využíva cloudové služby len štvrtina podnikov

Pre implementáciu cludového riešenia odporúča Cloud Security Alliance postupovať v siedmich krokoch.

1 IDENTIFIKOVANIE POŽIADAVIEK

Prečo sa potrebujeme presunúť do cloudu. Pomenovať výhody a príležitosti a zároveň inherentné riziká, ktoré do cloudu prinášame.

2 VÝBER POSKYTOVATEĽA, SLUŽBY A MODELU NASADENIA

Keď už vieme prečo, musíme si vybrať s kým. Je potrebné identifikovať poskytovateľa cloudových služieb aj model služieb a nasadenia.

3 DEFINOVANIE ARCHITEKTÚRY

DEFINOVANIE ARCHITEKTÚRY Definuje sa rozsah implementácií v cloude – typy a počty serverov, aplikácií, služieb a ďalšie požiadavky, napríklad ako sa budú navzájom autentifikovať. Bezpečné prepojenie prostredí, ochrana dát, roly a zodpovednosti.

4 HODNOTENIE BEZPEČNOSTNÝCH OPATRENÍ

Sumarizujeme požiadavky zákazníkov aj partnerov, profesijné štandardy a povinnosti v zákonnej rovine.

5 IDENTIFIKÁCIA MEDZIER V BEZPEČNOSTNÝCH OPATRENIACH

Analýza ukáže, aké opatrenia máme a čo nové treba implementovať. Už tu treba nastaviť efektívnu komunikáciu s poskytovateľom služieb, pochopiť jeho aplikované bezpečnostné opatrenia a definovať očakávania v servisnej zmluve.

6 NÁVRH A ZAVEDENIE BEZPEČNOSTNÝCH OPATRENÍ

Nasleduje prispôsobovanie a nasadzovanie bezpečnostných opatrení, aby naplnili obchodné ciele, boli v súlade s cieľmi riadenia rizík a zodpovedali bezpečnostným požiadavkám.

7 RIADENIE ZMIEN

Riadenie zmien je potrebne nastaviť tak, aby podporovalo dynamiku cloudového prostredia a zároveň zaručovalo udržateľnú bezpečnosť z dlhodobého hľadiska.

Daniel Suchý, bezpečnostný špecialista Aliter Technologies

BEZPEČNOSŤ

Tri ľahké kroky pre zvýšenie bezpečnosti v malých firmách

Vďačným terčom kybernetických útokov sa stávajú firmy s niekoľkými desiatkami alebo menej ako desiatkou zamestnancov, keďže nemajú tímy bezpečnostných špecialistov a zvyčajne ani interné IT oddelenia.

Technológie, inštalačné a konfiguračné služby či iný servis malým podnikateľom poskytujú obvykle menší miestni dodávatelia IT. Väčšina z nich však zabezpečenie pred kybernetickými rizikami vybaví inštaláciou antivírusov a nastavením firewallu. Takéto opatrenia dnes rozhodne nestačia. Zvýšiť ochranu v malých firmách však nemusí byť nevyhnutne drahé ani mimoriadne prácne. Tu sú tri jednoduché kroky s veľkým efektom, ktoré sa dajú urobiť s minimálnymi nákladmi a úsilím.

1. Zabráňte phishingovým útokom

Phishing vo forme podvodných e-mailov, telefonátov či webových stránok, ktorými sa útočníci a podvodníci snažia od obetí vylákať heslo, číslo kreditnej karty či inú dôvernú informáciu, býva spúšťačom väčšiny kybernetických útokov. Na základe získanej informácie následne dokážu napríklad infikovať systém škodlivým kódom, zablokovať dáta a následne obeť vydierať, alebo sa pokúsiť realizovať podvodnú transakciu.

Pripravte pre zamestnancov jednoduché školenie, ktoré im vysvetlí, ako takéto útoky vyzerajú a ako im predchádzať. Dôležité je najmä neklikať na linky v podozrivých e-mailoch a četoch, aj keď zdanlivo prichádzajú od známych odosielateľov, nezadávať

Bezpečnosť vo firme je na pleciach štatutára. SNÍMKA: DREAMSTIME

citlivé údaje na nezabezpečených weboch a používať filtre proti podozrivým e-mailom a webom.

2. Zaveďte používanie VPN

V čase pandémie ľudia viac pracujú mimo kancelárie, ale využívanie notebookov s internetovým pripojením z domova, z kaviarne alebo cez iné verejné WiFi siete môže byť nebezpečné. Bez zašifrovania je totiž pomerne ľahké sledovať aktivitu používateľa a odchytiť jeho komunikáciu vrátane hesiel napríklad na prístup do firemnej siete.

Začnite používať virtuálne privátne siete (VPN) pre bezpečné a šifrované pripojenie cez domáce či iné slabšie zabezpečené siete. Takýmto spôsobom sa dajú bezpečne prepojiť aj viaceré počítače z rozličných, fyzicky vzdialených WiFi, a takisto prepojiť počítače do firemného intranetu. K dispozícii sú aj bezplatné VPN-ky ako ProtonVPN či Windscribe VPN, hoci verzie zadarmo majú isté obmedzenia.

3. Dbajte na aktualizácie

Štatistiky vravia, že viac ako polovici kybernetických útokov mohli obete predísť včasným zaplátaním zraniteľností operačného systému, aplikácií či firmwaru. Vyše tretina obetí pritom priznáva, že o bezpečnostnej diere v čase jej zneužitia vedela.

Nastavte a zaveďte formálny proces s pravidlami pre vykonávanie aktualizácií a poskytnite zamestnancom školenia o základoch a význame kybernetickej hygieny. Nesmie sa stávať, že používatelia pri upozorneniach na potrebu aktualizácií opakovane volia možnosť „Pripomenúť neskôr“ alebo ponuku úplne zrušia.

Roman Čupka, hlavný konzultant Flowmon Networks a CEO Synapsa Networks

Otázka prekvapila, odpovede ešte viac

ANKETA

Pracovnou náplňou profesionála v kyberbezpečnosti je nečakať nič dobré. Tam masívny útok, tam nová zraniteľnosť, tam chýba rozpočet a ešte aj ľudia. To všetko ste už počuli. Tak sa pre zmenu pýtame: Čo dobré sa stalo v roku 2021?

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Viacej sa o téme hovorí, či už na úrovni verejnej správy alebo firiem. A našli sa aj svetlé výnimky, ktoré nevedú iba plamenné prejavy, ale pracujú na reálnych projektoch kyberbezpečnosti. Krok za krokom, dôsledne, každý deň. Možno to nie je úplne sexi téma, ale na schopnosti a dennom výkone týchto ľudí stojí naša bezpečnosť.

Henrich Šnajder,
manažér IT bezpečnosti
Orange Slovensko, a. s.

Určite ste stokrát počuli, že digitalizácia a automatizácia prinášajú kybernetické riziká. Niektorí si to plne uvedomia až vtedy, keď sa im prihodí vážnejší incident a počítajú straty. Iní sa posúvajú ďalej vďaka reguláciám, zákonným povinnostiam či spoločenskej zodpovednosti. Verím, že tento rok už každý, čo aspoň začal riešiť kybernetickú bezpečnosť, chápe, že téma bude čoraz aktuálnejšia a bolestivejšia.

Peter Dostál,
generálny riaditeľ
a predseda Dozornej rady
Aliter Technologies, a. s.

V oblasti kyberbezpečnosti sa toho udialo v tomto roku veľa. Mňa osobne prekvapil záujem o túto prílohu Hospodárskych novín. Je vzrušujúce sledovať rastúce povedomie o dôležitosti kyberbezpečnosti aj v širokej verejnosti. Spolupráca odborníkov a rastúce investície do vzdelania, budovania odolnosti infraštruktúry a vývoja nových technológií prinášajú reálne výsledky a predpokladám rovnaký trend aj budúci rok.

Tomáš Hettych,
viceprezident
ISACA

Z úvodných auditov kybernetickej bezpečnosti je zrejmé, že sa téme konečne dostáva v organizáciách zaslúžená pozornosť. Niekde je to síce stále len legislatívna požiadavka vnímaná rozporuplne, ale vo väčšine organizácií vládne pozitívny prístup, aj pri nižších hodnotách súladu. Organizácie už na to vyhradili zdroje a začína sa s implementáciou opatrení. A určite tomu pomohla aj novela zákona o kybernetickej bezpečnosti.

Rastislav Janota,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Veľa. Z hľadiska výkonu sú to hlavne úspechy našich odborníkov na medzinárodnom poli. Či už mimoriadne úspešná účasť SK-CERT expertov v rámci NATO tímu na cvičení LockedShield 2021 a ich šieste miesto, alebo veľmi oceňovaná účasť Slovenskej republiky na NATO cvičení Cyber Coalition 2021, kde náš kolega viedol tím štyroch inštitúcií NBÚ SK-CERT, CKO – VS, MIRRI SR a NASES.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Nariadením EÚ 2021/887 vzniklo Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier. Túto rolu v Slovenskej republike plní Kompetenčné a certifikačné centrum kybernetickej bezpečnosti. Jednou z jeho úloh bude poskytovanie finančnej podpory komunite z grantov udeľovaných Európskym kompetenčným centrom.

Roman Varga,
manažér kyberbezpečnosti
Dôvera, zdravotná poisťovňa, a. s.

Prostredie okolo nás je čoraz viac závislé od IT technológií a elektronických služieb. Sme senzitívnejší na kybernetické útoky. Hlavne na tie, ktoré sa týkajú nás a našich osobných a zdravotných údajov. Uvedomujeme si ich hodnotu a sme ostražitejší pri ich zverejňovaní.

Jana Puškáčová,
manažérka útvaru
Informačná bezpečnosť
MOL IT
& Digital Slovensko

Podstatne sa zmenilo vnímanie kybernetickej bezpečnosti na Slovensku. Aj vďaka tejto zaujímavej ankete a jej pravidelnému prínosu názorov a informácií.

Tibor Paulen,
manažér informačnej bezpečnosti
Stredoslovenská distribučná, a. s.

Ako pozitívnu udalosť vnímam júnové stretnutie prezidentov Bidena a Putina v Ženeve, ktorí tému agresie v kybernetickom priestore otvorili ako oblasť hodnú diskusie na najvyššej úrovni predstaviteľov svetových mocností. V konvenčnom svete existujú medzi krajinami dohody, ktorých cieľom je zamedziť konfliktom, alebo aspoň minimalizovať ich následky. Tak prečo by to tak nemohlo byť aj v kyberpriestore?

Tomáš Zaťko,
CEO, etický hacker
Citadelo

Cítiť postupný posun, že stakeholderi začínajú brať informačnú a kybernetickú bezpečnosť vážne. A to je dobré.

Diana Legdanová,
vedúca úseku bezpečnosti
Východoslovenská energetika Holding, a. s.

Som hrdá, že sa nám podarilo dosiahnuť výborné výsledky kybernetického auditu. V praxi to znamená, že musí spolu ladiť mnoho činiteľov – od povedomia ľudí až po systémové nástroje a niekde medzi tým je ešte silná podpora topmanažmentu. Ale týmto sa to nekončí, práve naopak, začína sa „next level“.

Richard Kiškováč,
generálny riaditeľ
IstroSec, s. r. o.

Za pozitívum považujem postupné spúšťanie projektov po dlhšej stagnácii, pravdepodobne najmä kvôli požiadavkám regulácie. Dôležité však bude reálne zvýšenie úrovne kybernetickej bezpečnosti v organizáciách. Úspešné ransomvérové útoky na Slovensku naznačujú, že aj napriek úsiliu sme stále len na začiatku. Pravda je taká, že väčšina organizácií si s kybernetickými útokmi poradiť nevie.

Roman Čupka,
hlavný konzultant
Flowmon a CEO Synapsa Networks

Je to síce paradoxné, ale je to medziročný nárast počtu kybernetických bezpečnostných incidentov a veľké množstvo rôznych útokov a kritických zraniteľností. Vďaka tomu sa téma informačnej a kybernetickej bezpečnosti dostáva do povedomia širšej verejnosti, budujú sa zaujímavé komunity, zvyšujú sa investície do ochrany kybernetického priestoru a vzniká množstvo inovatívnych technologických firiem.

Andrej Aleksiev,
riaditeľ slovenskej pobočky
Check Point Software Technologies

Potešilo ma, že v roku 2021 sme oslávili už 18. ročník Cyber Security Awareness Month. Inými slovami, napriek narastajúcemu počtu útokov sa spoločnosť snaží čoraz efektívnejšie informovať o potenciálnych hrozbách. To až do tej miery, že v oxfordskom slovníku vznikol nový pojem breach fatigue. Definuje veľkosť útoku, ktorý musí byť aplikovaný, aby sa dostal do titulkov správ. Inak, viete, ktorá krajina je najbezpečnejšia v kybernetickom priestore? oksnáD.

Július Selecký,
senior technický špecialista
ESET, spol. s r. o.

Už aj v domácnostiach sa kybernetická bezpečnosť stáva dôležitejším faktorom pri výbere zariadení napojených do siete. V ostatných segmentoch čoraz viac platí, že náklady na kvalitné zabezpečenie tvoria len zlomok sumy v prípade úspešného kybernetického útoku. A pozitívom boli audity kybernetickej bezpečnosti na Slovensku, ktoré výrazne pomohli väčšine organizácií zvýšiť bezpečnosť na novú úroveň.

Robert Mramúch,
manažér kybernetickej bezpečnosti
MH Teplárenský holding

Zákony a vyhlášky prestali byť pre firmy a podnikateľov strašiakom so zhlukom paragrafov a takmer nepochopiteľných zdôvodnení. Postupne sa prenášajú do praxe v podobe konkrétnych návrhov a opatrení. Kybernetická bezpečnosť sa stáva neoddeliteľnou súčasťou každodenného biznisu. Aj ankety ako táto prispievajú k zvyšovaniu povedomia o kybernetickej bezpečnosti.

Pavol Adamec,
výkonný riaditeľ oddelenia
Riadenie rizík
KPMG Slovensko

Nemám rád, ak je dôvod na aktivitu „lebo zákon“, ale tento rok prižmúrim oko. Povinnosť vykonať prvý audit kybernetickej bezpečnosti v zmysle zákona bola do novembra 2021. Mnohé firmy tak síce neurobili, zrazu však vidno zvýšenú aktivitu, rozmýšľanie, plánovanie... Aha, nás sa to týka – čo s tým? Ako budeme reagovať na nedostatky, ak to musí audítor o dva roky skontrolovať? Aktivita je život.

Ivan Kopáčik,
bezpečnostný expert
Gordias, s. r. o

Všetko zlé je na niečo dobré, obzvlášť v kybernetickej bezpečnosti. Z tohto uhla pohľadu vlny ransomvérových útokov síce spôsobili množstvo škôd, ale zapríčinili aj dôslednejší prístup k ochrane systémov a dát. Je však mrzuté, že to muselo zájsť tak ďaleko.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií/IT manažment kvality
Volkswagen Slovakia

Podarilo sa viaceré závažné zraniteľnosti nakoniec úspešne zaplátať. Viacej sa o kybernetickej bezpečnosti rozprávalo aj na Slovensku vďaka upravenému zákonu a prebiehajúcim auditom. Marek Zeman s ďalšími kolegami vydali knihu pre školy o kybernetickej bezpečnosti. Používatelia sú zasa o kus obozretnejší v tom, ako chrániť svoje citlivé údaje.

Anna Stehlíková,
manažérka pre bezpečnostné licencie pre región Česka a Slovenska
Microfocus

Ak porovnávam podobné štáty, akými sú Česko a Slovensko, smerom na západ vidím výrazne viacej konkrétnych aktivít, odvahy a realizovaných projektov. Súkromný aj verejný sektor podchytili dynamiku prostredia.

Jaroslav Oster,
predseda Správnej rady
Preventista.sk

Podarilo sa vydať prvú časť Učebnice informačnej bezpečnosti pre stredné odborné školy a gymnáziá a uviesť ju do reálneho života slovenského školstva. Prvé dve stovky slovenských škôl ju v súčasnosti majú v rukách a začínajú s ňou pracovať v rámci vzdelávacích aktivít.

Blanka Vargová,
manažérka tímu kybernetickej bezpečnosti
U. S. Steel Košice, s. r. o.

V smere vzdelávania v kybernetickej bezpečnosti rok 2021 priniesol veľa nového. Školenia, ktoré budú prínosom pre budúcnosť profesionálov v tejto oblasti, učebnicu pre stredoškolákov a memorandá o spolupráci s vysokými školami. Všetko toto pomôže v budovaní povedomia a vo výchove nových kolegov, ktorých je nedostatok. Týmto by som sa chcela veľmi pekne poďakovať všetkým, ktorí „v tom majú prsty“.

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

Hovorí sa, že všetko zlé je na niečo dobré. Medializovanými únikmi údajov sa ukázalo, v akom stave sa nachádza bezpečnosť informačných systémov na Slovensku, ale aj ako rýchlo sa šíri informácia o zverejnených osobných údajoch na internete. U kompetentných azda vznikne snaha to zlepšiť. Veľmi dobré je aj prezentovanie názorov o stave bezpečnosti prostredníctvom ľudí, ktorí sa tejto problematike venujú.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov
Tatrabanka

Veľmi si cením, že firmy sa viac zaujímajú o informačnú bezpečnosť. Rozbehli sa aktivity, ako sú vydávanie podcastov, okrúhle stoly, vzdelávanie na školách. Zatiaľ vzácne sú komplexné programy vzdelávania. Príkladom novej, ucelenej aktivity, ktorá zasiahla veľkú časť obyvateľstva a podporuje komunitné vzdelávanie, je program www.predigitalnubezpecnost.sk. Verím, že takýchto činov bude oveľa viac.

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

Som rád, že sme rok prežili bez kritického incidentu a vďaka tomu nikto nezomrel. V kybernetickej vojne viac pozitív nevidím.

Ján Lichvár,
konateľ
Axenta s.r.o.

Jednoznačne je to Akčný plán realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 – 2025. Odhodlanie kompetentných ma napĺňa nádejou, že tentoraz napísané slová neostanú len na papieri, ale akčný plán sa skutočne podarí realizovať. Potešilo ma aj keď len malé, ale začínajúce zvyšovanie povedomia ochrany dátových aktív zo strany povinných subjektov. Poslednou je vydanie učebnice Informačná bezpečnosť pre stredné školy. Ďakujeme pánom Blšákovi, Chromiakovi, Osterovi a Zemanovi.