HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 27. – 29. AUGUSTA 2021

Tí dobrí aj zlí, známi aj neznámi

ANKETA

Kto sú kladní hrdinovia alebo záporné postavy a tvorcovia informačnej bezpečnosti? Povedzte nám o svetových aj slovenských osobnostiach, ktoré vidno v médiách, aj o tých utajených. Čo vedia, čo urobili a prečo ich nominujete?

Tomáš Zaťko CEO
etický hacker
Citadelo

Ľudia majú radi hrdinov jednotlivcov. Hrdinstvá sú však väčšinou skupinové. Preto vyberiem skupinového hrdinu. Záporného. Ním sú tvorcovia a operátori ransomvéru. Ransomvér je najhrubší a najprimitívnejší druh kyberzločinu. Jeho autori preto vyhrávajú prvú priečku rebríčka antihrdina.

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

Dorothy E. Denning, ktorá medzi inými významnými míľnikmi v spolupráci s Petrom G. Neumannom vyvinula model systému detekcie prienikov používajúci štatistiky pre detekciu anomálií. Dodnes je práve toto základom systémov, ktoré vo veľkej miere napomáhajú v boji proti kybernetickým hrozbám.

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

Čiastočne aj pod vplyvom udalostí posledných dní u nás, sú práve etickí hackeri – white hat hackers, tí, ktorých považujem za výrazné osobnosti na poli informačnej bezpečnosti. To sú v mojich očiach kladní hrdinovia, respektíve takzvaní influenceri. Ľudia, ktorí odhaľujú chyby často v kritických bezpečnostných systémoch štátu a upozornia na ne príslušné orgány skôr, ako danú zraniteľnosť zverejnia.

Ivan Kopáčik
bezpečnostný expert
Gordias, s. r. o

Alan Turing. Filozof, matematik, kryptoanalytik, zakladateľ modernej informatiky. Dokázal, že informačná bezpečnosť môže ovplyvniť beh dejín. Počas druhej svetovej vojny úspešne dešifroval nemecké kódy šifrované zariadeniami Enigma. Odhaduje sa, že vďaka Turingovi sa skrátila vojna v Európe o dva roky a zachránilo vyše 14 miliónov životov.

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

Začal by som pri Kevinovi Mitnickovi a Kevinovi Poulsenovi alebo Robertovi Tappan Morrisovi, ktorému dávajú kredit za prvý počítačový vírus. Samozrejme, nemôžeme vynechať mená ako John McAfee alebo Eugene Kaspersky. V poslednej dobe sa často skloňuje aj meno Edwarda Snowdena. Na strane organizácií, určite NSA a portfólio spoločností, ktoré sa za zaoberajú vývojom produktov v oblasti kyberbezpečnosti.

Ivan Makatura
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Zakladateľ Microsoftu William Henry Gates. Nepôsobí síce v informačnej bezpečnosti, nakódoval však prvý operačný systém pre osobné počítače a neskôr bol architektom novších verzií, známych pod názvom MS Windows. Obrovské množstvo zraniteľností vo svete Windowsov bolo nepriamo jedným z dôvodov, prečo sa niektorí informatici začali profesionálne zaoberať informačnou bezpečnosťou.

Róbert Mramúch
manažér kybernetickej bezpečnosti
MH Teplárenský holding

Jedným z najznámejších hackerov je Kevin Mitnick – priekopník v sociálnom inžinierstve, teda v podvodnej technike, ktorá je dodnes stále jednou z najúspešnejších a najpoužívanejších. V špionáži, vo whistle-blowingu, v hacktivizme, rezonujú mená Julian Assange, Edward Snowden či Anonymous.

Vladimír Mlynarčík
riaditeľ pre región
Českej a Slovenskej republiky
Clico

Aby som nikoho nespravodlivo neopomenul, tak poviem, že pre mňa je osobnosťou momentálne každý CSO, ktorý to s kybernetickou bezpečnosťou myslí vážne, seriózne vníma výzvy v oblasti a manažuje ju s vedomím plnej zodpovednosti za dáta organizácie a osobné dáta ľudí.

Andrej Žucha
generálny riaditeľ
ALISON Slovakia

Mnohým európskym štátom ušiel vlak a s ním ochrana dát občanov Únie, vývoj technológií či umelej inteligencie. Vysoko hodnotím prácu viceprezidentky Európskej komisie Margrethe Vestagerovej, dvojnásobnej dánskej ministerky. Podporuje spoluprácu štátneho a verejného sektora, konkurencieschopnosť Únie v kybernetickej bezpečnosti, vzdelávanie a upozorňuje na etický rozmer rozvoja technológií.

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

Pre mňa je osobnosť, ktorá sa významne zapísala do povedomia, Edward Snowden. Poukázal, aký rozsah informácií je možné získať pre spravodajské účely pomocou technológií. A to doslova „od stola“. Po jeho čine si mnohí uvedomili, ako sme naviazaní na technológie a ako sú technológie naviazané na nás. To, či je kladný alebo záporný hrdina, nechám na posúdení čitateľa.

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

Alan Turing – anglický matematik, ktorý počas druhej svetovej vojny rozlúštil tajnú nemeckú šifru Enigma. Ukázal, že neexistuje absolútne zabezpečená informácia, pokiaľ na druhej strane stojí odhodlanie a sila geniálneho ľudského myslenia. V dnešnej dobe by človek s jeho schopnosťami bol zaiste hviezdou prvej veľkosti na jednej alebo druhej strane barikády rozdeľujúcej svet kybernetickej bezpečnosti.

Richard Kiškováč
bezpečnostný konzultant
Digital Systems, a. s.

Kevin Mitnick bol prvý známy, aspoň nám, prípad hackera, ktorý sedel za kybernetické zločiny a potom začal pracovať na druhej strane. Publikoval viacero kníh, prvá bola The Art of Deception: Controlling the Human Element of Security. Na tú si všetci pamätáme, bolo to také kvázi odhalenie. Druhou, možno kontroverznou osobnosťou, je Edward Snowden, ktorý tiež poriadne rozvíril verejnú mienku svojimi odhaleniami.

Rastislav Janota
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Informačná bezpečnosť je veľmi anonymná téma. Útočníci sa snažia o maximálnu anonymitu, obrancovia sú anonymní a aj (aspoň na Slovensku,) obete sa snažia byť anonymné, aby nemuseli priznať, že často sú obete najmä svojím pochybením. Napriek tomu by som vybral Mareka Zemana, ktorý pre povedomie a vzdelávanie v informačnej bezpečnosti na Slovensku spravil určite najviac. Je preto najväčšou (a možno jedinou) osobnosťou v tejto oblasti.

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

Výraznou osobnosťou informačnej bezpečnosti bol nedávno zosnulý programátor, biznismen, politik, zakladateľ a podporovateľ mnohých IT startupov John McAfee. Už v roku 1987 uviedol na komerčný trh prvý antivírusový softvér VirusScan s funkciami automatickej detekcie a odstránenia škodlivého kódu. VirusScan bol zároveň jeden z mála softvérových produktov, ktorý ste si mohli zakúpiť online cez internet.

Roman Varga
manažér kyber bezpečnosti
Dôvera, zdravotná poisťovňa, a. s.

Zostanem na domácej pôde. Jednoznačne sú to slovenskí nezávislí etickí hackeri. Opakovane nedeštruktívne otestovali nové štátne verejné produkčné informačné systémy v sektore zdravotníctva a oblasti ochrany osobných údajov. Reálny únik dát by zasiahol nás všetkých. Upozornili štát opakovane na závažné kybernetické zraniteľnosti. Prečo sa štát namiesto poďakovania zachoval alibisticky, je nepochopiteľné.

Vojtech Gáborík
riaditeľ úseku informačných technológií
Prvá stavebná sporiteľňa

Nie je jednoduché sa rozhodnúť pre jednu osobnosť. Preto som zúžil priestor na osobnosti, s ktorými som mal česť spolupracovať u nás na Slovensku. Dovolím si poukázať na Doc. RNDr. Karola Macáka, CSc. Stál pri zrode NBÚ a jeho meno je úzko spojené s výskumom národných kryptografických prostriedkov. Zapísal sa aj v prostredí NATO v oblasti infraštruktúry verejného kľúča a aktivitami v akademickom prostredí.

Marek Zeman
vedúci oddelenia bezpečnosti informačných systémov
Tatra banka

Dnes som sa rozhodol načrieť do existujúcej studnice živých ľudí zo Slovenska. Informačná bezpečnosť je súčasťou trhu informačných technológií. Trh sa vyznačuje dravosťou, cieľavedomosťou a často aj bezohľadnosťou. Zriedkavo vidieť človeka, ktorý je múdry, rozhľadený, nápomocný a prirodzený. Z môjho pohľadu do tejto skupiny patrí Tomáš Zaťko z firmy Citadelo. Tomášov odborný nadhľad a prístup je pre mňa inšpirujúci a povzbudivý, spoločné projekty sú odsúdené na úspech.

Roman Čupka
hlavný konzultant
Flowmon a CEO Synapsa Networks

Slovenskou osobnosťou je bezpochyby Pavol Lupták. Ten okrem iných, pre mňa inšpiratívnych vecí, stelesňuje aj bezpečnostnú spoločnosť Nethemba. Neustále nastavuje zrkadlo stavu zabezpečenia základných služieb verejnej správy napriek tomu, že neposkytuje platené služby pre štát. Tému kybernetickej bezpečnosti dokázal povzniesť nad úroveň klasického IT ponímania a jeho prístup k problematike si zaslúži pozornosť.

Pavol Adamec
výkonný riaditeľ oddelenia Riadenie rizík
KPMG Slovensko

Zoznam kladných aj záporných hrdinov informačnej bezpečnosti by bol veľmi dlhý. Za lokálnu slovenskú úroveň by som rád vyzdvihol troch vysokoškolských učiteľov – profesorov a docentov, ktorí skutočne desaťročia ovplyvňovali našu vysokoškolskú, ale aj všeobecnú odbornú diskusiu o informačnej bezpečnosti. Páni, uvedení v abecednom poradí, Otokar Grošek, Ladislav Hudec, Daniel Olejár. Za mňa veľké ďakujem!

Jaroslav Oster
predseda Správnej rady
Preventista.sk

Miroslav Trnka, zakladateľ spoločnosti ESET. Prečo nominujem práve zakladateľa jedného z lídrov bezpečnostných firiem na Slovensku a nepochybne aj vo svete, je zrejmé asi každému na Slovensku nezávisle od toho, či je bezpečnostný profesionál alebo laik. Jeho prínos pre vývoj bezpečnostných produktov a rovnako aj pre popularizáciu informačnej bezpečnosti v dlhodobom horizonte je nespochybniteľný a neoceniteľný.

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

Možno kontroverzné, no kľúčovými postavami sú aj hackeri. Oni sú väčšinou tí, ktorí nakoniec ľudí prinútia zmeniť prístup. Sú ako lekári, ktorí diagnostikujú skryté vážne choroby. Často až vtedy zmeníme životný štýl. Začneme chodiť na preventívky, v našej brandži sú to security nástroje, zdravo sa stravovať – security systém a športovať – testovanie. Paradoxne, hackeri prispievajú k systémovému zvyšovaniu kyberbezpečnosti.

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

Osobností, ktoré prispeli k rozvoju kybernetickej bezpečnosti, či už pozitívne alebo negatívne, je mnoho. Ťažko vybrať jednu konkrétnu. Osobnosťou je pre mňa každý človek, ktorý sa venuje zodpovedne ochrane informácií v kybernetickom priestore. Každý, kto pomáha hrozby a zraniteľnosti odhaľovať, kto ich berie vážne a nasadzuje opatrenia a každý, kto pomáha zlepšovať povedomie o kybernetickej bezpečnosti.

Ján Adamovský
riaditeľ bezpečnosti
Slovenská sporiteľňa

Mali sme v banke kolegu, ktorý si rád vystrelil z tých, ktorí si pri odchode z miesta nezamkli počítač. Ak ste sa stali jeho obeťou, mohlo sa vám napríklad stať, že z vášho počítača odišiel šteklivý návrh kolegyni či iná lotrovina. Stačilo si takto vystreliť dva- či trikrát, a odvtedy sa na celom poschodí nenašiel nikto, kto by si nezamkol počítač, aj keď išiel iba ku kopírke či kávovaru. Aj kybernetická bezpečnosť by mala mať štipku humoru a recesie.

Jana Puškáčová
manažérka útvaru Informačná bezpečnosť
MOL IT & Digital Slovensko

Ak by sme mali vyskladať ideálnu osobnosť kybernetickej bezpečnosti, potrebovali by sme za hrsť altruizmu, lebo hlavným poslaním by malo byť pomáhať druhým. Treba veľkú mieru nadšenia pre technológiu, odhodlanie neustále sa vzdelávať a držať krok s novými prístupmi, štipku perzistencie hraničiacej s otravnosťou, primeranú dávku zvedavosti a dostatočnú dávku pozornosti detailom.

HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

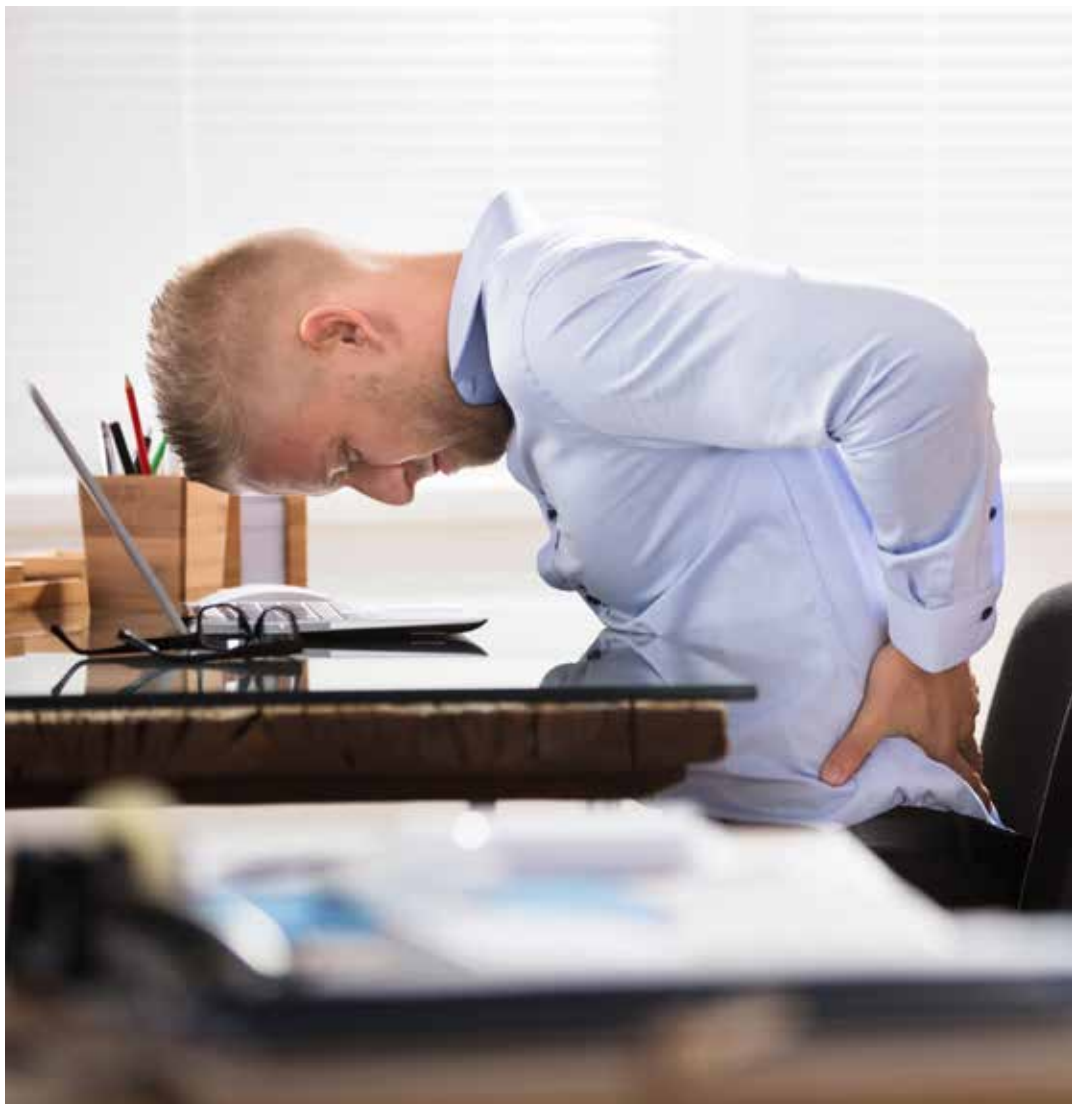
PIATOK – NEDEĽA
27. – 29. AUGUSTA 2021

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Vieme, kde nám tečie do topánok?

TÉMA

Blíži sa november a vyše tisícšesťsto organizácií by malo predložiť národnej autorite záverečnú správu auditu kybernetickej bezpečnosti. Doteraz tak urobili tri percentá subjektov.



Ľudia, procesy, technológie. Mantra kybernetickej bezpečnosti platí aj pre audit. SNÍMKA: DREAMSTIME

CENA INCIDENTU KYBERNETICKEJ BEZPEČNOSTI SPOJENÉHO S ÚNIKOM DÁT ROK 2021 (V MIL. USD)

Svetový priemer	4,24*	+ 9,8 %**
Výskum	3,60	+ 135,0 %
Média	3,17	+ 92,1 %
Verejný sektor	1,93	+ 78,7 %
Hotely a reštaurácie	3,03	+ 76,2%
Retail	3,37	+ 62,7 %
Zákaznícky servis	3,70	+ 42,9 %
Zdravotníctvo	9,23	+ 29,5 %
Komunikácie	3,62	+ 20,3 %
Služby	4,65	+ 7,8 %
Finančníctvo	5,72	–
Farmaceutický priemysel	5,04	–
Technológie	4,88	–
Výroba	4,24	–
Zábava	3,80	–
Vzdelávanie	3,79	–
Doprava	3,79	–
Energetika	4,65	– 27,2 %

*Priemerné náklady (milióny USD), **Medziročná zmena
Zdroj: IBM Cost of Data Breach 2020 a 2021 report, spracoval Aliter Technologies

Koho trápi základná služba

Zjednodušene povedané – základná služba je podstatná služba pre chod spoločnosti, či už je komerčná alebo poskytovaná štátom. My, všetci občania, sme jej používateľmi.

Správa z auditu je jedna vec, ale úroveň kybernetickej bezpečnosti sa týka všetkých. Či už priamo cez elektronické služby, ktoré používame, alebo cez štandardy, ktoré musia firmy, inštitúcie a úrady dodržiavať pri ochrane našich údajov.

Na čo je audit

Na Slovensku je v súčasnosti päťdesiatka certifikovaných audítorov kybernetickej bezpečnosti a viacej ako polovica z nich aktívne vykonáva audity.

„Prínos každého auditu by mal byť nezávislý pohľad a neskreslená informácia pre štatutára o stave kybernetickej bezpečnosti v ich organizácii“, hovorí Marián Illovský zo spoločnosti auditori.it.

Pri audite sa totiž vyhodnocuje u objednávateľa súlad s požiadavkami zákona a príslušných vyhlášok. Nikde nie je požadovaný počet „správnych odpovedí“, aby subjekt auditom prešiel.

Takže audit slúži primárne pre jeho objednávateľa, aby mu nezávislý expert povedal, „kde mu tečie do topánok a kde ho tlačí kamienok“.

Milióny klientov

Audit kybernetickej bezpečnosti v Národnej agentúre pre sieťové a elektronické služby trval vyše dvoch mesiacov.

V súčasnosti úrad reguluje celkovo 1 659 subjektov ako prevádzkovateľov základnej služby,“ spresňuje Peter Habara, hovorca Národného bezpečnostného úradu.

Patria sem výrobcovia a dodávatelia energií, doprava, telekomunikační operátori aj správcovia sietí, obchodné reťazce, bankovníctvo a finančné služby, pošta, priemysel, zdravotníctvo a samozrejme štátna správa aj samospráva.

Na splnenie povinnosti mali prevádzkovatelia dva roky. „K 19. augustu 2021 je na úrad doručených celkovo 56 auditových správ,“ pokračuje Peter Habara. A nepomôže ani fakt, že dve sú tam už od minulého roka.

Samotný objednávateľ priznáva, že proces si vyžiadal jeho značné kapacity, keďže audítori pomerne dôsledne verifikovali aktuálnosť bezpečnostnej dokumentácie a aj súlad jej aplikovania v dennodennej prevádzke.

„Musím konštatovať, že to bola citeľná záťaž najmä na úrovni stredného manažmentu, ale dobre identifikované a zdokumentované nálezy určite stáli za všetko úsilie,“ hodnotí proces Pavel Karel, generálny riaditeľ NASES.

Pozor: citlivé

Pavel Karel otvorene hovorí o tom, ako ho audit krátko po jeho nástupe postavil pred organizačné a technické nedostatky: „Kybernetickú bezpečnosť pri poskytovaní elektronických služieb štátu občanom a podnikateľom predchádzajúce manažmenty a riadiace a kontrolné orgány agentúry systematicky zanedbávali.“

„Aktívne už pracujeme na zvyšovaní úrovne kybernetickej bezpečnosti. Opierame sa práve o akčný plán riešenia nálezov auditov základných služieb aj o implementáciu projektu Národný systém riadenia incidentov kybernetickej bezpečnosti vo verejnej správe,“ vyratúva Pavel Karel.

Zámerom agentúry je vybudovať kvalitné a procesne zrelé bezpečnostné operačné centrum s cieľom vysokej úrovne detekcie kybernetických hrozieb. V prvej fáze sa NASES zameriava hlavne na infraštruktúru a postupne prejde na aplikačnú úroveň zabezpečenia koncových služieb pre fyzické a právnické osoby.

Kde to bolí

V skupine Svet zdravia išlo v prípade kybernetickej bezpečnosti o špecifický výkon, keďže sa auditovalo jedenásť samostatných subjektov.

Audit trval takmer tri mesiace a vyžadoval si súčinnosť IT odborníkov, personalistov, špecialistov kvality, prevádzkových zamestnancov a, samozrejme, manažéra kybernetickej bezpečnosti.

Peter Dufek, manažér kybernetickej bezpečnosti u prevádzkovateľa nemocníc a polikliník, si však naliehavosť riešenia uvedomuje: „V aktuálnej, pretrvávajúcej pandemickej situácii si zaslúžia najväčšiu pozornosť služby súvisiace s ochranou života a zdravia ľudí. Aj vzhľadom na obrovské množstvo zhromaždovaných údajov o obyvateľoch a ich zdravotnom stave.“

Znova a znova

Audit kybernetickej bezpečnosti v organizácii by sa nemal končiť odovzdaním auditnej správy. Ide o systematický proces, ako budovať a udržiavať celý ekosystém opatrení a procesov.

Po získaní výsledkov si v skupine stanovili záväzné opatrenia a harmonogram odstránenia nedostatkov. „Významným krokom bolo aj posilnenie tímu IT bezpečnosti a v spolupráci s manažmentom kvality pracujeme na zavedení procesov internej kontroly a auditu,“ dodáva Peter Dufek.

> Prínos auditu by mal byť nezávislý pohľad a neskreslená informácia o stave kybernetickej bezpečnosti.
>
> **Marián Illovský**
> certifikovaný audítor kybernetickej bezpečnosti

Bezpečáci si uvedomujú, že každá organizácia bude len taká bezpečná, aký význam a dôležitosť kybernetickej bezpečnosti pripisuje manažment organizácie. A zároveň jeden z faktorov, ktorý predstavuje najväčšiu potenciálnu zraniteľnosť, je ľudský faktor, teda veľké množstvo používateľov s nepostačujúcimi IT zručnosťami.

Čísla až neuveriteľné

Počet uskutočnených auditov v súčasnosti odhadujú profesionáli tak na vyše stovky. Časť prevádzkovateľov audit kybernetickej bezpečnosti povinnosti zanedbala, časť sa vyrovnáva s covid rokom, v prípade miest a obcí sa čakalo na novelizáciu zákona.

Nízky počet uskutočnených auditov vysvetľuje aj Tomáš Hettych z Kompetenčného a certifikačného centra kybernetickej bezpečnosti: „Tento nepomer je daný hlavne zdĺhavými procesmi obstarávania vo verejnej správe, kde objednanie auditu trvá aj niekoľko mesiacov.“

Prvé výsledky

Skúsenosti audítorov z terénu sú obdobné ako všetkých oblastiach. „Všade nájdete šikovných ľudí, skôr vidno rozdiely pri porovnaní sektorov,“ sumarizuje Marián Illovský.

Najlepšie hodnotenia sú pre sektory, ktoré mali reguláciu informačnej bezpečnosti skôr, ako bol platný zákon o kybernetickej bezpečnosti, čiže financie alebo telekomunikácie. Najväčšie rezervy sú vo verejnej správe a v zdravotníctve.

Najčastejším nesúladom pri audite sú neformálne, ale fungujúce procesy, prevádzkovateľom chýba dokumentácia, neexistuje riadenie aktív a rizík a chýba riadenie kontinuity. „Opätovne sa však stretávame so zarážajúco nízkym povedomím o bezpečnosti,“ neveriacky hovorí Tomáš Hettych.

A pokuta bude?

Ak teda šťastný objednávateľ už drží v ruke záverečnú správu z auditu, mal by ju do začiatku novembra poslať Národnému bezpečnostnému úradu. A zároveň vykonať opatrenia na základe auditu.

Úrad ako národná autorita by tak mal dostať porovnateľné informácie o stave kybernetickej bezpečnosti v jednotlivých sektoroch. Zároveň má právo kontroly u prevádzkovateľa základnej služby a aj pokuty.

A tu je hranica medzi auditom a kontrolou, ktorú Tomáš Hettych vysvetľuje obrazne: „Pokuta nie je za zistenie audítora, ale za to, že prevádzkovateľ napriek výsledkom auditu nekonal.“

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · ESET · Flowmon A Kemp Company · MICRO FOCUS · SYNAPSA · paloalto NETWORKS · SK CERT Národné centrum kybernetickej bezpečnosti