HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
28. – 30. JANUÁRA 2022

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

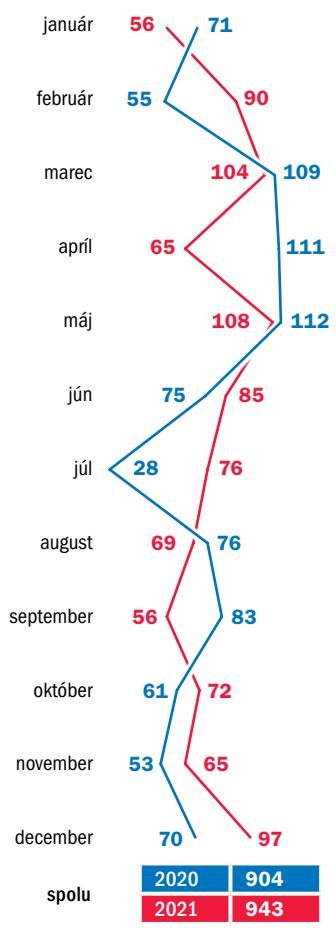
Stresu sa zbavíte, zodpovednosť zostáva

Niekedy naozaj ťažké odlíšiť kvalitných dodávateľov a preto sa pýtajte a žiadajte referencie.

SNÍMKA: DREAMSTIME

KYBER INCIDENTY NA SLOVENSKU

Hlásené incidenty na SK-CERT podľa zákona



Zdroj: NCKB SK-CERT

TÉMA

Ak má firma zabezpečiť kontinuitu podnikania či inštitúcia svoju prevádzku, súčasťou toho je aj povinnosť, že údaje sa nesmú stratiť ani byť zneužité a musia byť dostupné.

Slovenský podnikateľ, malý alebo veľký, to nemá ľahké. Má desiatky povinností, zamestnancov, k tomu záväzky voči štátu a je zodpovedný za rozvoj podnikania.

S digitalizáciou ekonomiky a verejnej správy sú tu ďalšie povinnosti. Pribúdajú právne predpisy, zostrujú sa zmluvné vzťahy a ešte aj zákazníci a občania sú na seba čoraz háklivejší.

Dáme to pod zámok

Keď ide o fyzickú bezpečnosť, skriňa sa dá zamknúť, na okno dáme mrežu a ešte aj alarm. No v treťom tisícročí, s postupujúcou digitalizáciou, nadobudol pojem bezpečnosti nový význam.

Miroslav Chlipala z advokátskej kancelárie Bukovinsky & Chlipala tento stav v slovenských firmách opisuje ako: „Všetko, čo nevieme uchopiť, odsúvame nabok. Ak máme veľa ďalších povinností, nevnímame akútnosť problému.“ Týka sa to cloudových služieb, ochrany osobných údajov aj kybernetickej bezpečnosti.

Ako šafranu

Spoločnosť Platon Technologies poskytuje hosting takmer sedemtisíc webov, špecializuje sa na prevádzku serverov a budovanie clusterov. Počet zákazníkov, ktorí sa zaujímajú aktívne o bezpečnosť, vyhodnotil Ondrej Jombik metaforou – je ich ako šafranu. „V drvivej väčšine prípadov dostaneme otázky na bezpečnosť, keď ide o povinnosť vyplniť informácie do nejakého dokumentu, ktorý potrebujú poslať ďalej.“

Zvýšený záujem zákazníkov o tému registrujú od roku 2018. Aj keď GDPR nie je priamo o zabezpečení serverov, mnohým ukázal, že je vhodné sa zaujímať o to, kde sú ich dáta uložené, kto má k nim prístup a ako sú zabezpečené.

Zodpovednosť ťažkého kalibru

Či už vyrábate súčiastky, liečite ľudí, máte e-shop, personálnu agentúru alebo vediete školu či úrad, údaje, ktoré spravujete, sú cenné. V prípade, ak príde ransomvérový útok a zašifruje ich, stanú sa nedostupné a hrozí ich zverejnenie a vydieranie.

Následok pri zanedbaní povinností kybernetickej bezpečnosti je takmer likvidačný. A pritom, ako opakuje Ondrej Jombík, záujem medzi zákazníkmi je stále dosť malý v porovnaní s tým, čo by si bezpečnostná problematika zasluhovala.

Aj štát má povinnosti

Pred štyrmi rokmi zákon definoval jedenásť strategických sektorov a vymedzil ich povinnosti v kybernetickej bezpečnosti. Patria sem súkromné spoločnosti, štátne podniky aj inštitúcie a organizácie verejnej správy. Vybrané subjekty sa tak stali povinnými osobami.

Účel zákona, vykonávacích vyhlášok a certifikačných schém je jednoznačný – zabezpečiť kontinuitu. Ak by sme to mohli voľne povedať, zákon o kybernetickej bezpečnosti je pre povinné osoby záväzný, pre súkromný sektor inšpiratívny.

Pán riaditeľ to vie?

Ak v dôsledku kybernetického útoku nefunguje firma, inštitúcia či obec, je zodpovedný štatutárny orgán. Miroslav Chlipala to formuluje jasne – povinnosťou štatutára je zabezpečiť službu kybernetickej bezpečnosti. „Neustálym opakovaním katastrofických správ o incidentoch nie je vystrašiť riaditeľov k smrti, ale upozorniť na riziká,“ dodáva.

Lebo kým všetko funguje, nikoho nič nebolí. Pritom v organizáciách sa považuje za štandard kybernetická bezpečnosť na úrovni IT riešenia, doplnená organizačnými opatreniami, vzdelávanie zamestnancov a zmluvné vzťahy.

Základ už existuje

Lenka Gondová prezidentka ISACA Slovensko dáva do pozornosti, že pri implementácii opatrení kybernetickej bezpečnosti je stále veľmi užitočné využívať základné normy ISO z oblasti informačnej bezpečnosti.

> Ak máme veľa ďalších povinností, nevnímame akútnosť problému.
>
> **Miroslav Chlipala,** z advokátskej kancelárie Bukovinsky & Chlipala

Keďže v praxi sa informačná a kybernetická bezpečnosť čoraz viac prekrývajú, odráža sa to aj v aktualizácii ďalších noriem. Patria sem napríklad normy pre riadenie rizík či bezpečnosti dodávateľov a v oblasti riadenia ochrany súkromia.

Situácia je riešiteľná

Ak si organizácia uvedomí svoju povinnosť, je to prejavom zodpovednosti. A prvým krokom. Či už sa rozhodne plniť povinnosti tak, že nájde kvalifikovaných zamestnancov, poverí dodávateľa, alebo si objedná kybernetickú bezpečnosť ako službu.

Špecialista Jozef Bálint zo spoločnosti ALISON rozhodne súhlasí s tým, že problematika kybernetickej bezpečnosti je aktuálne natoľko rozsiahla, že spoločnosť ktorá sa nevenuje výhradne IT, má problém pokryť celú oblasť pomocou vlastných personálnych a technologických zdrojov.

Úlohy, ktoré si vyžadujú odborné spôsobilosti, je možné realizovať aj využitím dodávateľských služieb. Na Slovensku sa tak v súčasnosti profiluje trh bezpečnostných služieb a jeho rast sa spája aj s nástupom cloudových technológií a nedostatkom IT špecialistov.

V cloude je to jasné

Dve dekády riešení priniesli množstvo skúseností, a preto ide táto oblasť príkladom. „Zákazník, teda používateľ cloudovej služby, je vždy zodpovedný za riadenie prístupu, kontrolu dát a, samozrejme, aj za bezpečnosť zariadenia, z ktorého sa ku cloudovej službe pripája,“ vysvetľuje Daniel Suchý zo spoločnosti Aliter Technologies.

Riaditeľ malého podniku však nemusí mať dostatočné znalosti o kybernetickej bezpečnosti a téma ho môže zaujímať len okrajovo, ak vôbec. Skôr bude riešiť, koľko to bude stáť. Pokiaľ nemá skúsenosti a znalosti, stratégiu migrácie IT do cloudu by mal zveriť do rúk profesionálov.

Pýtajte sa

Ak spadá organizácia pod reguláciu, prvá otázka pri presune do cloudu by mala byť na tému GDPR. Ďalšie otázky budúceho zákazníka súvisia s tým, akú službu si objednáva od cloud providera a čo tam plánuje prevádzkovať. Ak chce zapojiť vlastné IT oddelenie, musí ho zaškoliť a zvážiť, či má kompetencie.

V prípade nadnárodných cloudov nie je veľký priestor zasahovať alebo upravovať zmluvné podmienky, ktoré definujú kybernetickú bezpečnosť. „Tu by som vo vzťahu k službe dal urobiť kompletnú rizikovú a právnu analýzu, aby som vedel, na čom som a ako takéto rizika pokryť,“ radí Henrich Šnajder manažér IT bezpečnosti Orange Slovensko, a. s.

Dôrazne však dodáva, že ultimatívna zodpovednosť a dosahy na firmu sa nedajú preniesť na nikoho a už vôbec nie na cloud providera.

Určite máte web

Medzi povinnosti prevádzkovateľa webu patrí jeho bezpečnosť. Ondrej Jombík vidí ako najväčšiu nástrahu zmlúv nejasnú špecifikáciu okruhov zodpovednosti zákazníka a dodávateľa.

„Nie je nič horšie, ako keď sa nejaká dôležitá činnosť ocitne v sivej zóne a nikto za ňu nenesie zodpovednosť. Vtedy je to len otázka času, kedy nastane problém, je to časovaná bomba,“ upozorňuje Jombík ako skúsený prevádzkovateľ, ktorý už odolal nejednému DDoS útoku.

Ako príklad uvádza jasné definovanie v prípade webhostingu, kto je zodpovedný za pravidelné aktualizácie CMS systému. Obvykle to býva sám zákazník, ale v určitých zmluvných prípadoch môže byť činnosť presunutá na dodávateľa.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Cloud toho rieši veľa, ale pozor na bezpečnosť

Budúcnosť je hybridná. Čím skôr akceptujeme tento fakt, tým rýchlejšie napredujeme. SNÍMKA: DREAMSTIME

> Je nevyhnutné vedieť, kde všade sa budú vaše dáta nachádzať počas svojho životného cyklu.
>
> **Daniel Suchý,**
> bezpečnostný špecialista
> Aliter Technologies

TRENDY

Či si to uvedomujeme, alebo nie, takmer každý človek už získal nejakým spôsobom skúsenosť s cloudom. A zodpovednosť zaň máme vo vlastných rukách.

Určite používate niektorú e-mailovú službu, máte predplatený kancelársky balík alebo si zálohujete fotky z telefónu do úložiska, ktoré ste na tento účel dostali od výrobcu telefónu.

Čo je vlastne cloud? Zjednodušene, je to datacentrum či počítač niekoho iného. Vy mu platíte za to, že môžete používať jeho úložisko, výpočtovú kapacitu alebo iné služby, ktoré poskytuje.

Nejde teda o imaginárny obláčik, ale o reálnu infraštruktúru, ktorú je potrebné spravovať a udržiavať v prevádzke. O toto sa vždy stará poskytovateľ cloudovej služby.

Základná trojka

Niektorí používatelia majú predstavu, že prechodom do cloudu sa vyriešia všetky ich problémy nielen s infraštruktúrou, ale aj s bezpečnosťou. Myslia si, že poskytovateľ cloudovej služby je zodpovedný za všetko. Nie je to však celkom tak.

V súčasnosti sú tri najpoužívanejšie modely cloudových služieb – infraštruktúra ako služba, platforma ako služba a softvér ako služba.

Keď sa pozrieme bližšie na ktorúkoľvek z nich, tak vo všetkých prípadoch je zákazník, teda používateľ cloudovej služby, zodpovedný za riadenie prístupu, kontrolu dát a, samozrejme, aj za bezpečnosť zariadenia, z ktorého sa ku cloudovej službe pripája.

Túto delegáciu zodpovedností je potrebné mať vždy na pamäti a dostatočne vyhodnotiť riziká spojené s implementáciou cloudových riešení v rámci organizácie.

Kľúčové oblasti

Bezpečnosť klasickej infraštruktúry, ale aj tej cloudovej či hybridnej vieme podchytiť v spoločných oblastiach.

V prvom rade je potrebné držať neustály prehľad o všetkých aktívach. Nie je totiž možné chrániť niečo, o čom nevieme. Táto požiadavka je v cloude omnoho zásadnejšia, keďže ten umožňuje vytvárať nové aktíva takpovediac jedným klikom. Dôležitým prvkom je riadenie zmien a rozdelenie zodpovedností, ktoré zabezpečujú viacúrovňovú kontrolu aktív.

Druhou kľúčovou oblasťou je riadenie prístupu a identít. V prípade cloudu sa stráca význam klasického perimetra a ten sa presúva na úroveň identity.

V rámci životného cyklu je potrebné riadiť nielen používateľov, ale aj jednotlivé služby a aplikačné rozhrania. Je podstatné určiť, kto má kam prístup, ale taktiež to, aké má kto oprávnenia z hľadiska akcií. Ide napríklad o vytváranie nových inštancií, ako sú počítače v cloude, dátové úložiská či databázové úložiská.

Ochrana dát a logy

Je nevyhnutné vedieť, kde všade sa budú vaše dáta nachádzať počas svojho životného cyklu. S týmto je neodmysliteľne spojené šifrovanie a správa kľúčov, ako aj porozumenie tomu, akým spôsobom sú dáta zmazané.

Existuje tu totiž možnosť náhodného úniku zvyškov dát, keďže cloudové prostredie sa riadi filozofiou zdieľania zdrojov. To je jeho veľká výhoda, ale zároveň aj bezpečnostné riziko, ktoré je potrebné identifikovať a ošetriť.

Na záver, tak ako aj pri klasickej infraštruktúre, je veľmi dôležité mať prehľad o tom, čo sa v cloude deje. Zabezpečenie dostatočného prehľadu o stave a potenciálnych škodlivých aktivitách si vyžaduje zber a analýzu záznamov – logov – a monitorovanie toku komunikácie.

Budúcnosť je hybrid

Cloud sa neustále vyvíja, prispôsobuje požiadavkám trhu, ale aj meniacim sa hrozbám. Dôkazom môže byť čoraz častejšie využívanie cloudových riešení na úrovni vlád, respektíve armád.

Toto rozšírenie umožňujú rôzne modely nasadenia cloudových služieb. Preto ako najpravdepodobnejšia sa do budúcnosti javí implementácia hybridného modelu nasadenia pozostávajúceho z kombinácie verejného a súkromného cloudu.

Ten by umožnil organizáciám využívať všetky výhody vyplývajúce zo základných charakteristík cloudových služieb a taktiež vyhovieť požiadavkám štandardov a legislatívy.

ANALÝZA

Záujem o služby rastie vo všetkých segmentoch

Odborníci očakávajú, že trh bezpečnostných služieb vo svete sa v nasledujúcich piatich rokoch takmer zdvojnásobí.

Hnacou silou rastu je nevyhnutnosť dodržiavať regulačné zákony a nariadenia na ochranu údajov a zároveň zvýšený dopyt po cloudových bezpečnostných riešeniach medzi malými a strednými firmami.

VÝHODY

Prístup k najnovšej bezpečnostnej technológii

Prístup k odborníkom, ktorí sa venujú výlučne bezpečnosti

Flexibilita rýchleho zvýšenia alebo zníženia zabezpečenia

VÝZVY

Chýbajúca plná kontrola nad bezpečnostnými operáciami

Hrozba zdieľaných technologických zraniteľností

Možný **únik dát**

Bezpečnosť ako služba podľa ponuky

Ponuku na tomto trhu tvoria softvér, riešenia a služby. Doteraz dominujú najmä bezpečnostné riešenia (41 percent) a odhaduje sa, že hlavný podiel si udržia až do roku 2026. Najrýchlejší rast sa očakáva pre softvérové riešenia na predchádzanie zraniteľností.

Bezpečnosť ako služba podľa odvetvia

Trh pokrýva automobilový priemysel, letectvo a obranu, IT a telekomunikácie, bankovníctvo, finančné služby a poistenie, maloobchod a e-obchod, zdravotníctvo, vládu aj sektor energetiky.

Najvyšší podiel na trhu – 18 percent – patril v roku 2020 bankovníctvu, finančným službám a poisťovníctvu. Rovnako tu sa predpokladá dominancia aj nasledujúcich päť rokov. Okrem toho, že sú to najvyhľadávanejšie ciele kybernetických zločincov, masívne sem prenikajú cloudové technológie.

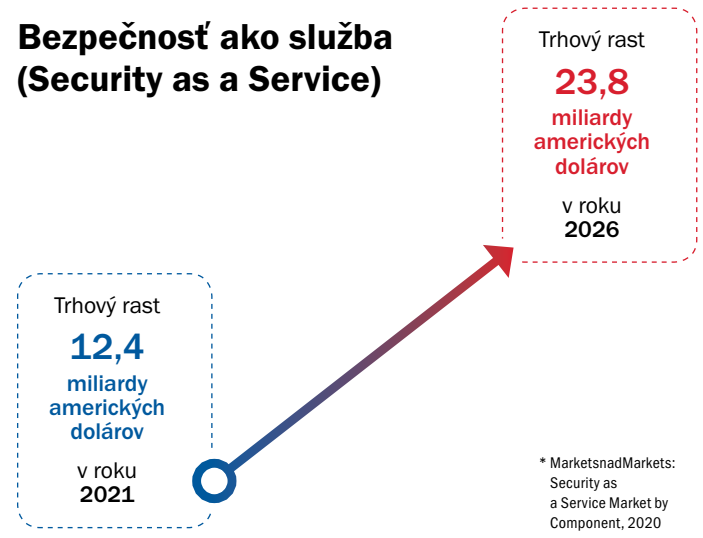
Bezpečnosť ako služba podľa regiónu

Z geografického hľadiska je SaaS trh rozdelený na regióny Severnej a Južnej Ameriky, Európy, Ázijsko-pacifický región a zvyšok sveta. Tretinový podiel na trhu mal na začiatku desaťročia severoamerický región, čo je dôsledkom vysokých investícií do IT infraštruktúry a alarmujúceho rastu kybernetických útokov.

Najrýchlejšie rastúcim trhom by mal byť Ázijsko-pacifický región, keďže tu rastie dopyt po digitálnej biznisovej stratégii a masívne a rýchlo sa zavádzajú cloudové aplikácie.

Výhody a výzvy

Bezpečnosť ako služba je komplexné riešenie a pomáha organizácii riešiť akýkoľvek bezpečnostný problém bez potreby vlastných vysoko špecializovaných odborníkov. Outsourcingom špecializovaných služieb sa organizácia môže sústrediť na objemy či inovácie. Ako každá služba má však SaaS nesporné výhody aj nástrahy.



ZRANITEĽNOSŤ

Keď ide o bezpečnosť firemného areálu, aký plot si vyberáte?

Predstavte si návštevu nového výrobného areálu u (imaginárneho) slovenského výrobcu mobilných telefónov.

Vo firme panuje čulý pracovný ruch, no už pri príchode vás zarazí, že vstup do celého areálu je úplne voľný. Autom bez problémov vojdete až ku skladom, žiadna rampa, kontrola, žiadni strážnici.

Uvedomíte si, že celý pozemok je oplotený iba záhradníckym pletivom, ktoré je navyše miestami roztrhané alebo úplne chýba. Výrobné haly aj expedičné sklady majú brány pootvárané a vyzerá to, akoby fungovali „samoobslužne“ – ktokoľvek príde, naloží si tovar a odíde.

Administratívna budova je taktiež bez recepcie, alarmu či kamier. V otvorených vchodových dverách má len retiazku vo výške kolien s tabuľkou „Cudzím vstup zakázaný“.

Absurdná predstava? Áno, ale ak si fyzickú ochranu zameníme s kybernetickou, ide o bežný stav firiem či inštitúcií na Slovensku.

Ako je to možné? Myslím si, že kľúčový problém je, že mnohé organizácie ešte nezačali kybernetickú bezpečnosť brať vážne.

Nevenujú jej dostatočnú pozornosť, a teda ani ľudské a finančné zdroje. V prieskume spoločnosti PwC medzi slovenskými generálnymi riaditeľmi sa obavy z kybernetických hrozieb objavujú na spodných priečkach rebríčka desiatich problémov, ktoré ich znepokojujú.

Pritom v rovnakom prieskume uvádzajú manažéri v USA a západnej Európe kybernetické hrozby na prvom mieste, ako najviac znepokojujúce.

Je to paradoxné, keďže kybernetický priestor geografické hranice nemá. A hrozby medzi krajinami nerozlišujú – s výnimkou tých politicky motivovaných.

> Myslím si, že kľúčový problém je, že mnohé organizácie ešte nezačali kybernetickú bezpečnosť brať vážne.
>
> **Martin Lohnert,**
> **riaditeľ centra kybernetickej bezpečnosti Void**
> **SOC a IT odborník Soitron**

Aj keď počas pandémie pribudlo viac zraniteľných miest či aplikácií vďaka práci z domu, videli sme sofistikovanejšie vydieračské útoky, častejší a lepšie jazykovo lokalizovaný phishing, išlo o globálne „trendy“, s ktorými sa stretávajú štátne inštitúcie aj firmy kdekoľvek.

Je tu ešte možnosť, že slovenské spoločnosti nevnímajú kybernetické hrozby ako podstatné preto, že majú bezpečnosť na mimoriadne vysokej úrovni.

Skúste sa na to spýtať niekoho z odbornej komunity a zrejme ho takouto hypotézou dobre pobavíte.

Realita má často podobu deravého pletiva a je len otázkou šťastia, že sme na Slovensku ešte nezažili kybernetickú „katastrofu“ s mnohomiliónovými škodami, o akých stále čítame zo zahraničia.

Kybernetický zločin aj obrana sú vysoko organizovaný priemysel. SNÍMKA: DREAMSTIME

Dajte im rozpočet a pozerajte sa!

ANKETA

Ak by ste mali veľmi veľký rozpočet a mohli urobiť iba jednu investíciu u vás vo firme alebo v úrade, čo by ste urobili v oblasti kybernetickej bezpečnosti?

Tomáš Hettych
viceprezident
ISACA

Nasadiť bezpečnostný a prevádzkový monitoring a pripojiť doň všetky relevantné informačné aktíva. Bez monitoringu je organizácia slepá a hluchá a spolieha sa len na klasické (väčšinou pasívne) bezpečnostné mechanizmy. Nasadenie centrálneho monitoringu je veľký a náročný projekt, ktorý organizáciu zabaví na niekoľko mesiacov, ale výsledok a výstupy sú väčšinou dosť dramatické a zaujímavé.

Ján Grujbár
generálny riaditeľ
Aliter Technologies

Sme technologická firma a tak by sa očakávalo, že investícia bude smerovať do najnovšej technológie. Avšak najcennejším aktívom každej organizácie sú ľudia. Ak im dáte adekvátny tréning a priestor, prinesú vám úžasné riešenia. Investícia v našom podaní by smerovala predovšetkým do rozšírenia vzdelávacích možností pre zamestnancov a vytvorení priestoru pre podporu inovatívnych projektov.

Marián Trizuliak
architekt kybernetickej bezpečnosti
Západoslovenská distribučná

Najať schopných útočníkov (whiteheťákov) – red, purple, blue team – a celú spoločnosť riadne otestovať, ako odolá rôznym formám útokov. A hlavne, ako by reagovala na veľmi kreatívne formy útokov a či vôbec dokáže vhodne reagovať alebo útok odhaliť. Kreativita útočníkov nepozná hraníc. V rozpočte by som pravdepodobne počítal aj s malou rezervou na lieky na upokojenie a vitamíny. Budeme ich potrebovať.

Ivan Makatura
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Výraz „investícia“ evokuje technické opatrenie. Avšak neexistuje technológia, ktorá by bola bezpečnostným všeliekom. Správnejšie je presadzovať koncept hĺbkovej ochrany, v ktorom sú informácie chránené niekoľkými bezpečnostnými vrstvami. Ak mám dať len jediné odporúčanie, potom nasadenie robustného procesu riadenia rizík. Na ten ani veľký rozpočet netreba. A z neho vyplynú čiastkové opatrenia.

David Dvořák
audítor kybernetickej bezpečnosti
Auditori.it

Inšpiroval by som riaditeľov a zodpovedných manažérov a nadchol ich pre tému. Urobil by som kyber bezpečnostnú hru s reálnymi úlohami, adrenalínovým dobrodružstvom a odmenami. Ak používateľ nepostrehne útok, celá organizácie je v ohrození. Cvičili by sme zručnosti zážitkami. Hovoriť v treťom tisícročí iba o školeniach je „old school“. Ak by zvýšilo, obsadil by som do hlavnej úlohy Daniela Craiga.

Andrej Žucha
generálny riaditeľ
ALISON Slovakia

Keďže má ísť o jedinú investíciu, tak by to bolo vybudovanie centra bezpečnostných operácií. To je ten moment mať „fungujúci orchester bez disonantných tónov“, ku ktorému sa snaží dopracovať každý, čo rieši bezpečnosť v organizácii. Ak by pod pojmom investícia, mala byť jedna technológia, tak by to bol bezpečnostný monitoring. Dôležité je vedieť, čo sa mi deje a podľa toho vedieť reagovať.

Roman Čupka
hlavný konzultant
Flowmon a CEO Synapsa Networks

Vybudoval by som profesionálne stredisko bezpečnostných operácií (SOC) vybavené viacerými vrstvami technológií a vyškolenými internými odborníkmi, ktoré by fungovalo s podporou externých tímov zameraných na overovanie pripravenosti organizácie na hrozby, reakcie na incidenty a forenzné vyšetrovanie.

Ivan Kopáčik
bezpečnostný expert Gordias

Vypočul by som si predstavy bezpečnostného manažéra o internom vzdelávaní v kyberbezpečnosti. Nechal ho systematicky vyhodnotiť zručnosti a vedomosti zamestnancov, vypracovať štruktúrovaný plán vzdelávacích aktivít podľa potrieb a cieľových skupín a potom ho s profesionálnymi lektormi realizovať. Tak, aby kurzy zohľadňovali špecifiká organizácie a potreby vedenia, IT špecialistov a používateľov.

Stanislav Smolár
manažér oddelenia bezpečnosti
Soitron

V Soitrone máme kybernetickú bezpečnosť už dnes na relatívne vysokej úrovni. Preto by som zvolil nástroj, ktorý dokáže posilniť detailné poznanie všetkých IT aktív, zanalyzovať ich bežné či anomálne správanie a priraďovať k týmto aktívam relevantné risk skóre. Nástroj by ma vždy upozorňoval na rizikové aktivity zariadení a potenciálne incidenty, a preto by som zintegroval detekciu incidentov s interným SOC.

Július Selecký
senior technický špecialista

Z hľadiska bezpečnosti by som odporučil investovať zákazníkom do EDR riešenia na ochranu koncových zariadení s prislúchajúcimi službami vyšetrovania incidentov. Stačí iba trochu vyšší rozpočet. Prevencia je vždy lepšia ako liečba, ale nie vždy je to možné. Najlepší spôsob, ako minimalizovať následky útokov, je ich včasné odhalenie. Nástroje, akými sú EDR riešenia, tento proces urýchľujú a zabraňujú tak šíreniu hrozieb.

Tibor Paulen
manažér informačnej bezpečnosti
Stredoslovenská distribučná

Investoval by som do systému budúcnosti, riadeného umelou inteligenciou, ktorý by zbieral a analyzoval dáta z našich systémov a učil sa tak predvídať a rozpoznať „stav mieru“ od „stavu vojny“. Postupne by sa naučil aktívne meniť parametre systémov a radiť ich správcom pri predchádzaní a reakcii na bezpečnostné incidenty. A mne by radil, do akých bezpečnostných technológií je potrebné investovať :-)

Peter Dufek
manažér kybernetickej bezpečnosti
Procare a Svet zdravia

Pokiaľ by som si mal vybrať, rozhodne by som odporúčal investovať do sofistikovaného nástroja Endpoint Detection and Response (EDR) na cielenú detekciu a reakciu na útoky na koncové zariadenia zamestnancov, pretože medzi súčasné najväčšie hrozby patria ransomvér, malvér, ako aj emailové útoky cielené na krádež hesiel alebo údajov smerované na koncového používateľa.

Matej Síleš
manažér IT bezpečnosti
UPC BROADBAND SLOVAKIA

Určite by som zvažoval investíciu do viacerých projektov, ale ak by som mal možnosť výberu výlučne jedného, tak by to bol projekt zameraný na mapovanie všetkých procesov v spoločnosti a aktív, ktoré sú s nimi viazané. To je totiž kľúčové pre správne riadenie rizík a ich následnú minimalizáciu. Lebo iba v prípade dobrej znalosti prostredia je možné efektívne smerovanie investícií do bezpečnosti.

Zuzana Ďuračinská
projektová manažérka
LIFARS LLC

Investovala by som do kvalitných ľudí so skúsenosťami. Dobrých ľudí by som nasadila tak do manažérskych, ako aj do technických úrovní. Až po dôslednom audite by som sa rozhodla, ako ďalej investovať a určite by som rozdelila investície do menších častí a na rôzne riešenia.

Martin Fischer
manažér oddelenia bezpečnosti
Všeobecná zdravotná poisťovňa

Nanešťastie, ani v prípade neobmedzeného rozpočtu sa oblasť kybernetickej bezpečnosti nedá pokryť jednou zázračnou škatuľkou. Investícia by však určite smerovala do technologického vybavenia, ktoré musí držať krok s dobou, aby sme vedeli efektívne čeliť najaktuálnejším hrozbám. Oblasť IT a predovšetkým kyber bezpečnosť sa vyvíjajú veľmi rýchlo, preto si nemôžeme dovoliť zaostávať.

Marek Zeman
vedúci oddelenia bezpečnosti informačných systémov
Tatra banka

Informačná bezpečnosť stojí na súhre veľkého počtu navzájom zapadajúcich koliesok. Každá firma si musí nájsť miesto v rozpočte na ochranu, monitoring systémov, mať nástroje na prevenciu, zastavenie útoku a dobrý incident manažment. Určite by som odporúčal, aby sa CISO venoval každému koliesku samostatne a zameral sa na najmodernejšie technológie. Neobmedzený rozpočet sa často nevidí.

Ján Bodnár
konateľ
Unique People Košice

Najcennejší, ale aj najviac zraniteľný článok sú samotní zamestnanci. Investoval by som preto do ich neustáleho vzdelávania tak, aby sa zžili s pravidlami kybernetickej bezpečnosti, boli schopní minimalizovať riziká napadnutia, rýchlo reagovali na prípadne hrozby a v krajnom prípade okamžite zasiahli. Pretože ani najlepší hardvér a softvér nás nedokáže ochrániť bez správne angažovaného zamestnanca.

Pavel Nechala
partner
Advokátska kancelária WISE3

Budovanie kultúry odolnosti voči kybernetickým hrozbám je zložitejší proces ako vzdelávanie o problematike. Cieľom je nielen odovzdať najnovšie poznatky, ale súčasne vysvetliť pracovníkom, ako konať a presvedčiť ich, že ich postoj je dôležitý. Ako je zrejmé, nebude na to postačovať jedna prednáška či smernica, ani jeden elearning, vyžaduje to kontinuálny proces budovania pozornosti.

Richard Kiškováč
generálny riaditeľ
IstroSec

Rozhodnutie o investícii by pravdepodobne smerovalo k nájdeniu odborne zdatného partnera, ktorý je schopný pokryť široké portfólio služieb kybernetickej bezpečnosti od prevencie až po riešenie bezpečnostných incidentov. Kľúčovým faktorom pri výbere by bol v prvom rade dostatočný počet kvalifikovaných expertov pre špecifické oblasti a ich reálne skúsenosti z praxe.

Igor Práznovský
riaditeľ odboru bezpečnosti informačných systémov
Sociálna poisťovňa

Nasadenie L7 firewallu a mikrosegmentácia siete so zapnutými threat profilmi aj pre vnútorné toky s cieľom implementovať princípy Zero Trust architektúry.

Robert Mramúch
manažér kybernetickej bezpečnosti
MH Teplárenský holding

S veľkou pravdepodobnosťou by som začal sieťovou infraštruktúrou. Kvalitný a (pre dané prostredie) správny návrh architektúry, zároveň i kvalitné nasadenie do prostredia, sú tie najlepšie predpoklady na budovanie bezpečnosti v každej organizácii.

Petra Zorvanová
špecialistka informačnej bezpečnosti
Lidl Slovenská republika

V skratke pár slovami: investovali by sme do awareness programu. Aby sme sa ešte viac venovali kolegyniam a kolegom. Pretože jedným z najslabších článkov je vo veľa prípadoch práve človek. A vzbudiť povedomie o informačnej bezpečnosti im pomôže nielen v pracovnom, ale aj súkromnom živote.

Ján Golais
konateľ
JUDICIUM

Kúpiť len jedinú vec by bola veľmi ťažká voľba. Kybernetický priestor je obrovský a taký bezpečný ako jeho najslabší prvok, preto je potrebné investovať do všetkých prvkov, ktorými sú technológie, personál. Súčasným trendom je zavedenie tzv. zero trust konceptu a určite sa oplatí investovať aj do viditeľnosti do siete.

Juraj Koník
bezpečnostný manažér
Allianz-Slovenská poisťovňa

Zabezpečiť kontinuálne a obsahovo rôznorodé vzdelávanie a nadobúdanie vedomosti všetkých našich zamestnancov za účasti nasadenia automatizovaných nástrojov pre zaznamenávanie bezpečnostných udalostí, ich flexibilnú a rýchlu analýzu prepojenia na biznis model spoločnosti až po celkovú eradikáciu.

Jaroslav Oster
predseda správnej rady
Preventista.sk

Investoval by som do vybudovania cyklického, systematického a cieleného zvyšovania bezpečnostného povedomia zamestnancov podľa reálnych potrieb. Realizácii by však muselo predchádzať zisťovanie aktuálneho stavu znalostí. Zvýšenú pozornosť by som venoval obsahu, aby reflektoval prostredie a zohľadňoval zavedené technické a organizačné opatrenia a skúsenosti z predchádzajúcich incidentov.

Pavol Draxler
výkonný riaditeľ
Binary Confidence

Objednal by som si Managed Security Service Provider (MSP) spoločnosť, ktorá sa bude starať o celú bezpečnosť v našej firme.

Marián Klačo
vedúci oddelenia bezpečnosť informácií
Volkswagen Slovakia

Vo všeobecnosti považujem za potrebné priebežne investovať do obnovy IT/OT technológií. Veľa organizácií totiž ešte stále používa zastarané a v praxi často už nepodporované technológie, ktoré býva problém vhodne zabezpečiť alebo patchovať. Rizikové sú najmä komponenty v priemyselných sieťach, často aj v kritickej infraštruktúre.