HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 28. – 30. MARCA 2025

Odborná spolupráca

NBÚ

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Ofenzívna bezpečnosť? Nevyhnutnosť

TÉMA

Kybernetických útočníkov nezaujíma, či ste malá alebo veľká firma. Hľadajú vaše slabé stránky. Odpoveďou je – nájdite si ich skôr.

Digitálna transformácia podnikov a inštitúcií zvyšuje závislosť na technológiách a s tým súvisí aj rastúci počet kybernetických útokov či iných potenciálnych zlyhaní. SNÍMKA: DREAMSTIME

Banky, energetika a ďalšie organizácie kritickej infraštruktúry povinne a pravidelne testujú systémy na bezpečnostné riziká. Skratka OffSec – offensive security, je profesionálom známa už desiatky rokov a tí zvyknú hovoriť, že ten, kto chce dobre brániť, musí vedieť, ako sa útočí.

Nový kyberzákon však vyžaduje používanie praktík ofenzívnej bezpečnosti aj od ďalších, menej skúsených subjektov.

Šokujúce výsledky

„Pri teste stredne veľkej spoločnosti v sektore služieb sme nedávno odhalili kritické zraniteľnosti, ktoré mohli viesť k úplnému narušeniu bezpečnosti webového servera," hovorí Tomáš Ležovič zo spoločnosti ESET. Citlivé údaje zákazníkov, vrátane osobných informácií a histórie objednávok, boli voľne prístupné. „Je každodennou realitou, že pri testoch spoločností od najmenších až po medzinárodné korporácie odhalíme kritické zraniteľnosti," dodáva Ležovič.

Ak by sa tieto bezpečnostné chyby stali terčom útoku, neoprávnené osoby by mohli prevziať kontrolu nad zákaznícky-mi účtami. Spoločnosť by čelila nielen finančným stratám, možným sankciám zo strany regulátorov aj vážnemu poškodeniu reputácie a strate dôvery zákazníkov.

Piliere digitálneho sveta

Označenie etický hacker prvýkrát použila spoločnosť IBM pred tridsiatimi rokmi. Proces etického hackingu má rôzne podoby. Môže ísť o testovanie konkrétnej aplikácie, napríklad internetového bankovníctva či e-shopu. „Niekedy preverujeme serverovú infraštruktúru alebo dokonca celé interné systémy firiem," vysvetľuje Tomáš Zaťko zo spoločnosti Citadelo.

Na otázku, či sa im vždy podarí preniknúť do systémov, odpovedá Tomáš Zaťko jednoznačne: „V drvivej väčšine prípadov áno." Dĺžka testov závisí od veľkosti cieľa. Bežný penetračný test trvá jeden až tri týždne. Pri veľkých bankách, kde sú testy už povinné, môže ísť aj o niekoľkomesačný proces.

Zdravotníctvo v hľadáčiku

V Univerzitnej nemocnici v Martine testujú a skenujú infraštruktúru na prítomnosť zraniteľností už vyše päť rokov a viackrát už urobili aj phishingové testy. „Prvý test som inicioval hneď, ako som sa stal manažér kybernetickej bezpečnosti," hovorí Pavol Vrabec. „Presvedčiť vedenie nebolo ťažké. Detailne som im vysvetlil prínosy a nevyhnutnosť testu a, samozrejme, aj zákonnú povinnosť."

V nemocnici pribudlo aj penetračné testovanie, keďže z časového hľadiska výraznú zmenu zaznamenali práve v prístupe k službám a systémom dostupným z internetu. „Dnes platí zásada, že ak má byť nejaká služba vystavená do verejného prostredia, musí najprv prejsť dôkladnou analýzou a bezpečnostným testovaním," rezolútne uzatvára Pavol Vrabec.

Extra nároky

Telekomunikácie sú súčasťou kritickej infraštruktúry, ktorá má zásadný význam pre chod štátu a spoločnosti.

Tomáš Masný, riaditeľ informačnej bezpečnosti Slovak Telekom a T-Mobile CZ má desiatku rokov skúseností s offsec praktikami. Aj tu začínali základnými penetračnými testami a postupne pridávali sofistikovanejšie techniky ako simulácie útokov, red teaming a testovanie odolnosti voči sociálnemu inžinierstvu.

Skúsenosti treba zdieľať

Roky priniesli cennú skúsenosť, že téma ani konkrétne výsledky testov by sa nemali prezentovať manažmentu ako strašenie. Dôležité je kvantifikovať riziko a ukázať, ako pentesty môžu pomôcť k udržateľnosti biznisu a dôvery zákazníkov. Pomáha aj benchmark s konkurenciou a zdôraznenie regulačných požiadaviek.

„Testy ukážu, kde je slabý článok kyberbezpečnosti a najčastejšie je to človek a jeho chybovosť, zlé návyky z predchádzajúcej práce, či zlá architektúra," zhŕňa Tomáš Masný. Top príčina je nedostatočný manažment záplat a zastaralé systémy, kde sa už záplaty nedajú aplikovať.

Spojené nádoby

Ofenzívna bezpečnosť testuje ľudí a technológie. Aj tu hrá významnú úlohu automatizácia. Produkty na správu útočnej plochy identifikujú potenciálne vektory útoku, ktoré by mohli využiť kyberzločinci. Nepretržite sa skenuje sieť organizácie vrátane domén, IP adries, webových stránok, e-mailových systémov, cloudových služieb, nástrojov SaaS, zariadení IoT a dátových úložísk.

> DÔLEŽITÉ JE KVANTIFIKOVAŤ RIZIKO A UKÁZAŤ, AKO PENTESTY MÔŽU POMÔCŤ K UDRŽATEĽNOSTI BIZNISU A DÔVERY ZÁKAZNÍKOV.
>
> **Tomáš Masný,** Slovak Telekom a T-Mobile CZ

Hneď v druhom kroku sa automatizovane aplikujú záplaty, následne sa preveruje ich účinnosť a opravujú sa chybné konfigurácie. K tomu odporúča Tomáš Vobruba zo spoločnosti Check Point aj integráciu spravodajstva o hrozbách v reálnom čase – Threat Intelligence.

Nároky na profesionálov

Vstup do elitnej spoločnosti etických hackerov umožňujú až náročné certifikácie. Na najnovší kurz a jeho nevyhnutnosť upozorňuje Jozef Bálint zo spoločnosti Alison Slovakia. Kľúčovou inováciou od minulého roku je tu integrácia umelej inteligencie do výučby aj praktických cvičení.

AI umožňuje automatizovanú identifikáciu zraniteľností a predikciu potenciálnych kybernetických hrozieb. Malvérová analýza v reálnom čase pomáha expertom rýchlejšie reagovať na nové hrozby. AI je aj súčasťou penetračných testov, kde automatizovane prehľadáva cloudové riešenia, IoT zariadenia či webové aplikácie. V interaktívnych útokoch zas umelá inteligencia napodobňuje reálne hackerské techniky.

Nástrahy boomu

Áno, od januára sa dramaticky zvýšil dopyt po praktikách ofenzívnej bezpečnosti. A trh reaguje.

Cena penetračných testov sa líši, no príliš lacné ponuky často znamenajú povrchné testovanie založené len na automatizovaných skenoch. Preto treba porovnať rozsah testu, metodológiu a kvalitu výstupov. Dôležité je venovať pozornosť odbornosti a skúsenostiam tímu. Kvalitný dodávateľ ponúkne aj konzultácie, pomoc pri opravách zistených chýb a možnosť re-testu, aby sa overila účinnosť opráv.

Nekvalitný test môže vytvoriť falošný pocit bezpečia, zatiaľ čo ten dobre vykonaný odhalí skutočné slabiny. V ideálnom prípade by malo byť testovanie pravidelné, pretože bezpečnostné hrozby sa neustále vyvíjajú.

ANKETA:

Zasiahol vás kybernetický útok, je chyba v systéme alebo iné zlyhanie? Rady od profesionálov. Čo robiť v prípade kyberincidentu vždy. Čo nerobiť nikdy.

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

Špeciálnu prílohu podporujú

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. MARCA 2025

Máte kyberincident? Toto urobte vždy!

ANKETA

Zasiahol vás kybernetický útok, je chyba v systéme alebo iné zlyhanie? Pamätajte radu od profesionálov. Čo robiť v prípade kyberincidentu vždy. Čo nerobiť nikdy.

Jaroslav Ďurovka riaditeľ,
Národné centrum kybernetickej bezpečnosti

V prípade kyberbezpečnostného incidentu je vždy doležité obrátiť sa na odborníkov z jednotiek CSIRT alebo špecializovaných firiem. Vo väčšej organizácii dodržujte vopred definované postupy v rámci riadenia incidentov. Prevádzkovatelia základných služieb sú povinní hlásiť závažný kyberbezpečnostný incident NBU. Určite nerobte paniku. Ako sa hovorí, najhoršia smrť je z oplašenia.

Veronika Paulinyová audítorka kyberbezpečnosti,
Skupina Cyllium

Neodporúčam zatajovať incident. Je potrebné úprimne ho priznať, zdokumentovať, postúpiť na relevantné miesta tak, ako každý ďalší útok na organizáciu. Mať bezpečnostný incident nie je hanba. Hanba je klamať, že žiaden nemáme.

Martin Fábry konzultant pre kyberbezpečnosť kritickej infraštruktúry,
Accura

Veď viete, čo robiť v prípade kyberincidentu. To, čo sme vždy poctivo a pravidelne trénovali pri table top cvičeniach, prípadne pri red a blue teamingoch, všakže. Že je tak? A určite viete, že nesmiete prepadať panike a chaosu. Útočník vždy profituje z paniky, lebo vie, že panika spôsobuje veľkú chybovosť.

Ivan Makatura predseda,
Asociácia kybernetickej bezpečnosti

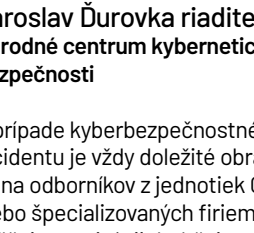
Okamžite dajte preč ruky z klávesnice! Nepokúšajte sa riešiť problém svojpomocne. Ak ste v korporácii, zavolajte špecialistov kybernetickej bezpečnosti a informujte vedenie. Ak pracujete v malom alebo strednom podniku, volajte technickú podporu, alebo známeho bezpečáka. Pri rozsiahlejšom incidente by som odporúčal objednať znalca. A nezabudnite na povinné hlásenia, inak riskujete pokutu.

Marek Madžo technický riaditeľ,
Centrum kybernetickej bezpečnosti void SOC

V prípade incidentu je dôležité mať Incident Response Plan a riešiť podľa neho – to znamená zaoberať sa oblasťou riešenia bezpečnostného incidentu proaktívne a byť pripravený. A čo nikdy nerobiť? Nikdy by ste nemali nechať incident bez reakcie, alebo naň reagovať neodborne.

Tomáš Zaťko CEO,
Citadelo

Zavolajte firmu, pre ktorú je odpoveď na incidenty jednou z hlavných služieb. Prvé hodiny rozhodujú o všetkom. Uchovajte stopy. Fyzické počítače nechajte zapnuté. Všetky odrežte od internetu. Veď ani zápal slepého čreva si neoperujete sami.



Ján Adamovský riaditeľ bezpečnosti,
Slovenská sporiteľňa

Zachovám chladnú hlavu. Postupujem podľa spísaných a natrénovaných postupov reakcie na kybernetický incident. Hasiči, záchranári tak isto svoje kroky trénujú.

Jakub Berthoty advokát,
Dagital Legal

Vždy je potrebné incident zdokumentovať a posúdiť jeho závažnosť. Podľa závažnosti je potrebné ho oznámiť Úradu na ochranu osobných údajov a NBU, ak ide o prevádzkovateľa základnej služby. Rôzne povinnosti, rôzne lehoty. Často sa zabúda na oznámenie najzávažnejších incidentov aj dotknutým osobám respektíve verejnosti podľa GDPR.

Lenka Gondová prezidentka,
ISACA

Vždy aktivujte incident response plán. Rýchla a koordinovaná reakcia šetrí čas, dáta aj reputáciu. Nikdy nemanipulujte s dôkazmi. Neodstraňujte logy ani nevypínajte systémy bez konzultácie s expertmi.

Michal Srnec CISO,
Aliter Technologies

Ak existuje, tak jednoznačne vždy postupujte podľa plánu reakcie na incidenty. Určite bol premyslený a obsahuje minimálne kľúčové osoby a postupy. A ak žiaden plán nie je? Dajte okamžite dokopy kvalitný tím špecialistov, interných alebo externých, vytvorte im čas a priestor na riešenie, dôverujte im a hlavne komunikujte transparentne. Inak sa môže stať, že to dopadne katastrofálne.

Peter Kočík manažér Systémových Inžinierov,
Fortinet

Poučte sa z tejto situácie! Ak ste sa stali obeťou kyberútoku, znamená to, že niečo vo vašej bezpečnosti zlyhalo. Analyzujte, čo to bolo, posilnite ochranu a zabráňte opakovaniu. Každý incident je drahá lekcia, využite ju, aby ste boli o krok vpred. Zvážte nasadenie technológie na nalákanie a oklamanie útočníkov, aby ste ďalší útok vedeli identifikovať čo najskôr.

Roman Čupka riaditeľ pre stratégiu,
Istrosec

Kontaktujte profesionálov, čo vedia vyjednávať na medzinárodnej úrovni a majú aj skúsenosti s psychológiou tímov. A to najneskôr v piatok na konci týždňa. Najväčšou chybou je odložiť to na pondelok.

Peter Bukovinsky šéf IT bezpečnosti,
Eviden Slovensko

Ihneď odstavte, podľa možnosti vypnite a určite izolujte napadnuté zariadenie od siete, odpojte sieťový kábel, obaľte aspoň dvojmo alobalom alebo inou rádio-odrazivou fóliou, ak zariadenie má aj wifi, aby sa zabránilo šíreniu respektíve rozvoju útoku. Neskúšajte utajiť. Určite neklamte a neodstraňujte dôkazy, aby bolo možné incident analyzovať, čo najskôr ho odstrániť a vyťažiť z neho účinné poučenie.

Július Selecký senior technický špecialista,
ESET

Pri kyberincidente je izolácia napadnutých systémov absolútna priorita. Inak sa škodlivý kód šíri rýchlejšie ako klebety v open space. Skontrolujte či XDR systém odpojil zasiahnuté zariadenia od siete, deaktivujte vzdialený prístup a zablokujte napadnuté účty. Nepanikárte a hlavne nevypínajte všetko bez rozmyslu, IT tím potrebuje analyzovať situáciu. Čím skôr izolujete hrozbu, tým menšie škody.

Henrich Šnajder manažér IT bezpečnosti,
Orange Slovensko

Ihneď izolujte postihnuté systémy od siete, ale nevypínajte ich a informujte bezpečnostný tím. Zaznamenajte podrobnosti a postupujte podľa interného plánu reakcie, aby ste minimalizovali škody. Nepanikárte, nereštartujte ani nevypínajte zariadenia, aby ste nezničili dôkazy. Neodkladajte nahlásenie, rýchla reakcia je kľúčová. Nezdieľajte detaily incidentu mimo oprávnených osôb, aby ste predišli šíreniu nepravdivých alebo úniku citlivých informácií.

Tomáš Valenta riaditeľ,
Check Point

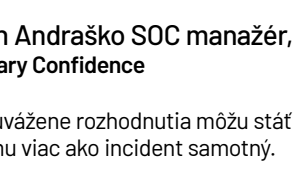
Ak k tomu dôjde, je dobré mať plán a nerobiť náhodné kroky. Analyzujte a dokumentujte. Všetko. Čo sa stalo, prečo sa to stalo, čo bolo ohrozené a zneužité. Komunikujte.

Andrej Žucha generálny riaditeľ,
ALISON Slovakia

Po zvládnutí incidentov u zákazníkov vždy robíme vyhodnotenie. Zákazníci vždy najviac hodnotia profesionálny ľudský prístup, schopnosť robiť za hranicou povinností a pochopenie. Technológie a postupy kúpite. Vyberte si na riešenie incidentu ľudí, s ktorými budete zdieľať najťažšie chvíle.

Tomáš Hettych člen predstavenstva,
KCCKB

Urobte poriadnu analýzu rizík, aby ste identifikovali prípadné najväčšie straty. Následne informujte o incidente a prípadných scenároch vedenie organizácie, nech majú objektívne informácie pre prípadné rozhodnutia.



Ján Andraško SOC manažér,
Binary Confidence

Neuvážene rozhodnutia môžu stáť firmu viac ako incident samotný.

INZERCIA

MS216029/25

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. MARCA 2025

Ako vyzerá Slovensko na perimetri?

REPORT

V ostatných šiestich mesiacoch zasiahlo jednu organizáciu na Slovensku priemerne 1 664 kybernetických útokov týždenne.

Čo sa týka typu, najvyšší počet detegovaných útokov predstavovali botnetové útoky zamerané na nedostupnosť systémov, čo presahuje globálny priemer.

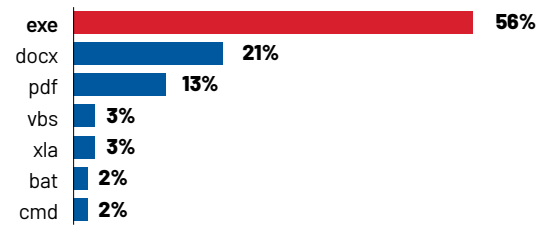
Viac ako polovica škodlivých súborov bola na Slovensku za posledných tridsať dní doručená prostredníctvom webových stránok. V porovnaní so štatistikami koncom minulého roka tak prišlo k významnej zmene, keďže dlhodobo najčastejším vektorom útoku bol e-mail. Kyberzločinci používajú webové stránky ako nástroj na skryté šírenie škodlivého kódu. Od zabezpečenia webových stránok pred kybernetickými hrozbami závisí ochrana kódu aj bezpečnosť používateľov v online priestore.

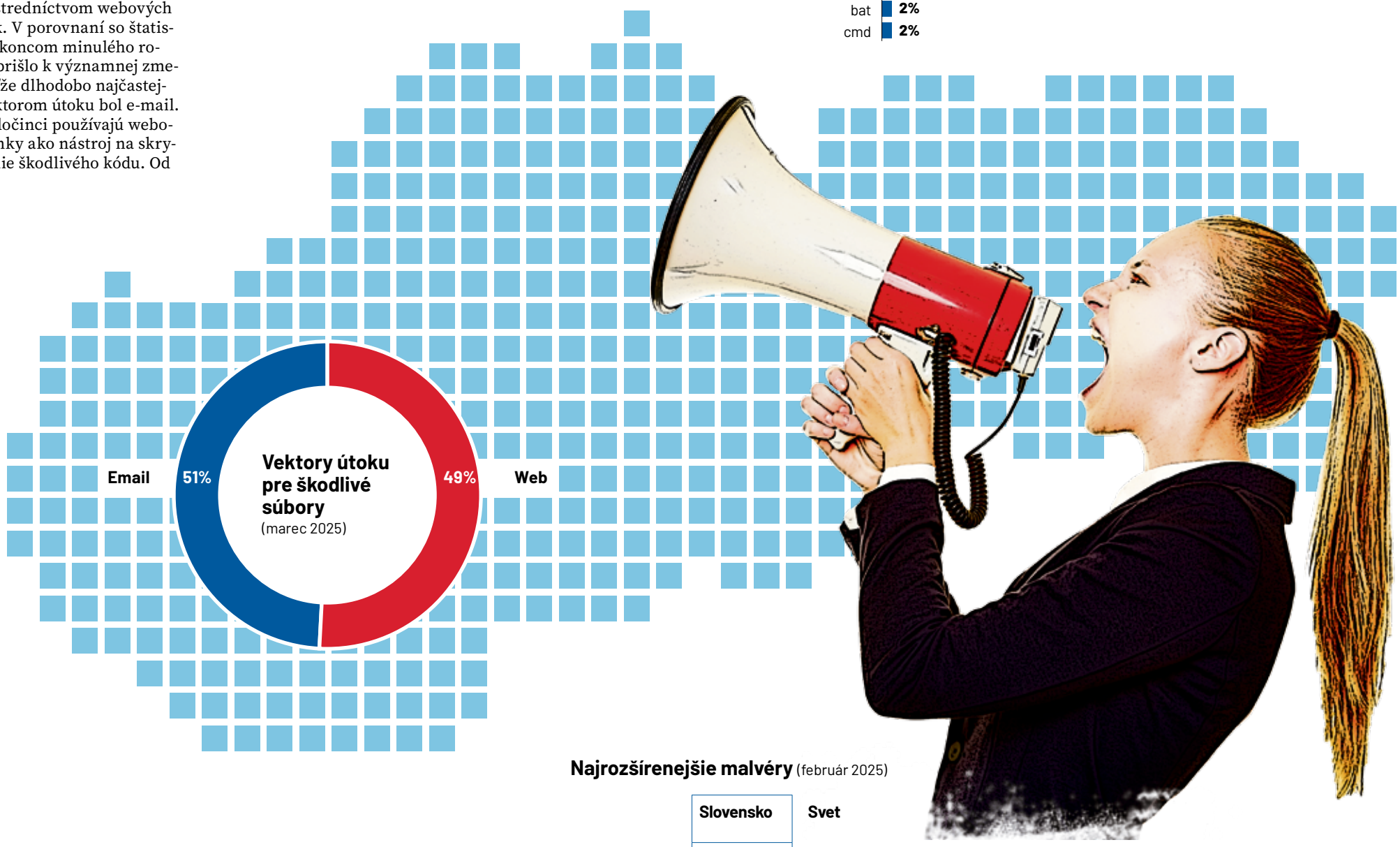
Zdroj: Threat Intelligence Report spoločnosti Check Point Research, Slovensko 23. 9. 2024 – 24. 3. 2025

Typy malvéru zasahujúce organizácie (percentuálny podiel na týždennej báze)

	Ransomvér	Mobilný malvér	InfoStealer	Bankový malvér	Útoky vedené cez botnet
Slovensko	3,5%	0,1%	2,7%	3,3%	11,4%
Svet	4,0%	0,8%	3,0%	2,7%	8,7%

Najčastejšie typy škodlivých súborov
(marec 2025)





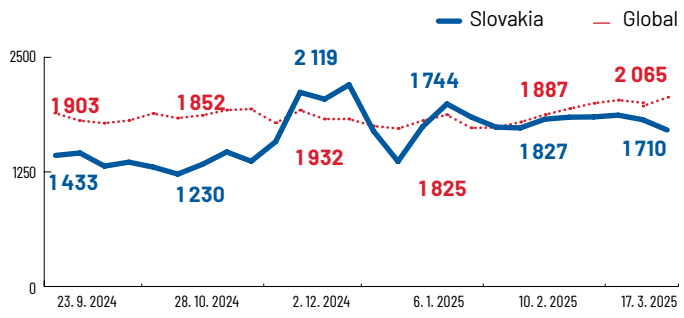
Najviac zasiahnutý sektor (september 2024 – marec 2025)

Priemerný počet kyberútokov na organizáciu týždenne

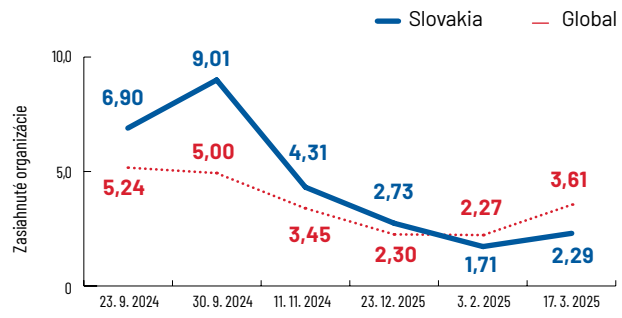
Najrozšírenejšie malvéry (február 2025)

	Slovensko	Svet	
Androxgh0st	**5,9%**	2,8%	Botnet, ktorý sa zameriava na platformy Windows, Mac a Linux. Na počiatočnú infekciu využíva viacero zraniteľností. Malvér kradne citlivé informácie, ako sú informácie o účte Twilio, prihlasovacie údaje SMTP, kľúč AWS. Na zhromažďovanie požadovaných informácií používa súbory Laravel. Rôzne varianty vyhľadávajú rôzne informácie.
AsyncRat	2,9%	2,2%	Pokročilý trojan so vzdialeným prístupom, ktorý zasahuje Windows systems
Aquabot	2,2%	0,2%	Súčasť botnetu Mirai, prvýkrát identifikovaný v novembri 2023. Útokmi typu DDoS kompromituje IoT zariadenia

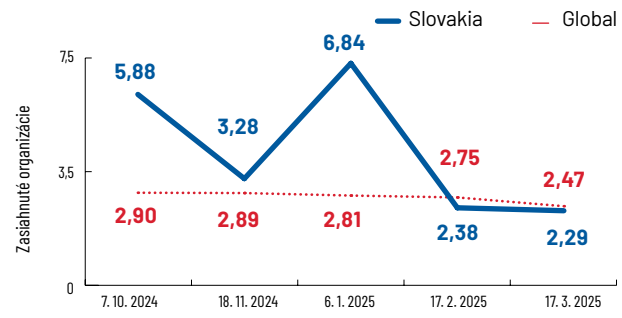
Priemerný počet kyberútokov na organizáciu týždenne
(september 2024 – marec 2025)



Útoky infostealerom
(v %)



Útoky na banky
(v %)



Útoky vedené cez botnet
(v %)

Ransomvérové útoky
(v %)

Dá sa predvídať incident?

Kybernetická odolnosť je kombinácia technologického výkonu a ľudských skúseností s využitím umelej inteligencie. SNÍMKA: DREAMSTIME

RIEŠENIA

Je užitočné odhaliť slabé miesta skôr, než to urobia útočníci a regulátor.

Hackeri najlepšie vedia, akí sme zraniteľní. Ak ich máte na svojej strane, vaša šanca prežiť v kyberpriestore bez vážnej ujmy sa zvyšuje.

Zatiaľ čo kedysi stačilo preveriť vo firemnej sieti niekoľko základných slabín v softvéri, dnes sa už firmy musia brániť sofistikovaným útokom, ktoré kombinujú technické zraniteľnosti so sociálnym inžinierstvom.

Od základky po univerzitu

Organizácie si v súčasnosti objednávajú penetračné testy podľa náročnosti a toho, čo si chcú overiť. Základné testy preverujú konkrétne systémy, aplikácie či infraštruktúru. Sofistikovanejší scenár, ako je red teaming, simuluje komplexný hackerský útok zo všetkých smerov. Špeciálna kategória penetračných testov overuje aj splnenie zákonných smerníc a noriem.

Najnáročnejšou kategóriou sú TLPT testy (Threat-Led Penetration Testing), nazývané ako ultimátny test bezpečnosti. Vykonávajú sa najmä vo finančných inštitúciách a v segmentoch kritickej infraštruktúry. Trvajú aj niekoľko mesiacov a simulujú útoky, ako ich robia vysoko organizované APT skupiny. Testovací tím sa tu snaží preniknúť do systému akýmkoľvek spôsobom vrátane sofistikovaných kombinovaných útokov, sociálneho inžinierstva a dlhodobej infiltračnej činnosti.

Je to jasné

Cieľ etického hackingu však zostáva stále rovnaký – nájsť zraniteľnosti skôr, ako ich objavia útočníci. A tak testujú aplikácie, riešenia alebo systémy v extrémnych podmienkach. Etickí hackeri skúšajú, ako sa systém správa pri neočakávaných situáciách, či obsahuje nezdokumentované chyby a ako by sa dal zmanipulovať.

Tento proces je hľadanie niečoho, čo ešte nebolo objavené. Hackeri sa snažia donútiť systém, aby sa správal inak, než bol naprogramovaný. Ak sa im to podarí, majú v rukách prienikový bod.

Nástroje sú výborné, ale

Na trhu už existujú nástroje, ktoré dokážu automaticky identifikovať známe zraniteľnosti. Sú naprogramované na vykonávanie konkrétnych útokov, takzvaných exploitov. Čiže v podstate majú v sebe predpripravené zraniteľnosti, ktoré sa dajú využiť. Každý, kto si kúpi nástroj, môže vykonať útok.

Pridaná hodnota kvalitného testovacieho tímu sa však začína tam, kde sa končí výkon týchto nástrojov. Rozdiel medzi automatizovaným útokom a prácou etických hackerov je v kreativite a schopnosti objavovať nové slabiny.

Jadro toho, čo robia kvalifikovaní profesionáli, je vytváranie nových techník a exploitov pre systémy, kde ešte existujú zraniteľnosti, ktoré doposiaľ neboli odhalené a zdokumentované.

Správa z odvrátenej strany

Ak sa dnes niekto rozhodne, že chce byť kybernetický zločinec, nemusí mať hĺbkové znalosti. Kriminálne gangy už fungujú ako organizované podniky, kde si delia prácu. Niektorí programujú malvér, iní ho šíria, ďalší kradnú databázy kreditných kariet a niekto iný ich dokáže speňažiť.

Umelá inteligencia posúva tento model ešte ďalej. Znižuje bariéru vstupu do kybernetickej kriminality a umožňuje menej skúseným útočníkom vykonávať činnosti, ktoré si kedysi vyžadovali roky skúseností. S rozvojom AI bude bezpečnosť ešte komplikovanejšia a obrancovia sa musia, pochopiteľne, prispôsobiť.

AI aj tu

Umelá inteligencia už dnes dokáže analyzovať kód, hľadať zraniteľnosti, generovať phishingové útoky, dokonca vykonávať autonómne útočné operácie. No zároveň pomáha pri obrane – zlepšuje detekciu útokov, opravuje chyby v systémoch a chráni dáta.

Či sa dostaneme do bodu, kde umelá inteligencia bude hackerom aj obrancom zároveň, je otázka času. No jedno je isté – kybernetická bezpečnosť sa už nikdy nebude riadiť len pravidlami ľudí. Rozmachom umelej inteligencie vstupuje do tejto hry niečo oveľa rýchlejšie a nepredvídateľnejšie.

Zraniteľnosť najvyššej priority

Kybernetická bezpečnosť sa posúva od útokov na zariadenia k útokom na dáta. A tam už čoraz menej záleží na tom, kde sa nachádza samotný používateľ. Útočníci sa už nepotrebujú „vlámať“ do konkrétneho počítača. Potrebujú sa dostať k vašim súborom. A pokiaľ sú tieto súbory niekde v cloude, cesta môže byť napríklad cez phishingové útoky.

Sociálne inžinierstvo tak zostáva jednou z najefektívnejších zbraní útočníkov. Riziká na bežných používateľov číhajú na webových stránkach, v e-mailoch, na sieťach aj v neznámych médiách.

Tomáš Horváth
kyberbezpečnostný konzultant Citadelo

Poradňa manažéra kybernetickej bezpečnosti 3/12

PORADŇA

Aj aktíva treba upratať

Po audite bezpečnosti už vieme, že naša fiktívna firma Chrum & Chrum má pred sebou poriadnu dávku práce. Objavili sa zraniteľnosti, slabé miesta v procesoch aj technické nedostatky.

Pred tým, než sa pustíme do opatrení, potrebujeme poznať odpoveď na jednoduchú otázku: Čo vlastne chránime? Marec som preto zasvätil inventarizácii aktív – teda všetkému, čo má pre firmu hodnotu a čo môže byť cieľom útoku, výpadku alebo chyby. Bez toho sa bezpečnostná stratégia postaviť nedá.

Čo sú to aktíva

Aktívum je všetko, čo má pre firmu hodnotu, čiže informácia, proces, systém, know-how, služba, ľudia, hardvér, celkovo päť kategórií.

Informačné aktíva sú dokumenty, databázy, zmluvy, reporty, zákaznícke údaje a v prípade našej firmy aj receptúry.

Fyzické aktíva si ľahko vieme predstaviť. Sú to servery, pracovné stanice, sieťové zariadenia, výrobné linky, záložné zdroje, lokality.

Nasledujú softvérové aktíva ako ERP systém, skladový softvér, dochádzka a bezpečnostné nástroje.

Aktíva predstavujú aj služby, čiže internet, IT podpora a aj služby externých partnerov.

Ľudské zdroje, zamestnanci, ich odborné znalosti a k tomu ich prístupové oprávnenia sú aktívum, ktoré získava čoraz viac na hodnote.

Ku každému aktívu sme priradili vlastníka – človeka. Toho, ktorý vie, na čo dané aktívum slúži, čo sa stane, ak prestane fungovať, a kto by mal reagovať, ak sa niečo pokazí.

Klasifikácia

Nie všetky informácie majú rovnakú hodnotu. Preto sme s vlastníkmi každé aktívum posúdili z pohľadu troch vlastností: integrita, dostupnosť a dôvernosť.

Integrita znamená, že informácia je presná a nezmenená. Pri nízkej úrovni, akú majú napríklad interné oznamy, zmena neprekáža. Keď sa však zmenia parametre výroby, zmena môže mať vážne následky, čiže tu je nevyhnutná vysoká úroveň integrity.

Dostupnosť hodnotí, aký veľký je problém, keď systém vypadne. Archív zvládne výpadok, ale výpadok výrobného systému už firmu zastaví.

Dôvernosť rieši, kto má k informáciám prístup. Firemný web je verejný, no receptúry či osobné údaje patria medzi prísne chránené.

Mapa

Hodnotenie nám pomáha určiť, čo je kritické, čo potrebujeme chrániť viac a čo menej. Nezabúdajme na zásadný fakt – aktíva nie sú izolované, a preto sme si zaznačili aj väzby a nadväznosti medzi aktívami, kto sa na koho „spolieha“. Naše najkritickejšie aktíva, označené ako červené zóny, zaraďujeme medzi najvyššie priority na ďalšie zabezpečenie.

Inventarizácia je dôkladná príprava na ďalší krok. V apríli sa budeme venovať analýze dosahov, ktorá nám pomôže zistiť, čo sa stane, keď niektoré aktívum zlyhá.

Andrej Mišura, manažér kybernetickej bezpečnosti

Seriál Takto to robím ja nájdete v hnonline.sk v sekcii Kybernetická bezpečnosť

Inventarizáciu aktív si môžete predstaviť ako jarné upratovanie vo firme. SNÍMKA: DREAMSTIME

MANAŽMENT

Ofenzívna bezpečnosť – ťažko na cvičisku, ľah... ľahšie na bojisku

Ofenzívna bezpečnosť je dnes už štandardom pri niektorých vysoko regulovaných odvetviach či špecializovaných útvaroch jednotlivých zložiek bezpečnostných agentúr. A rozhodne nejde iba o dobre známe názvy z filmov, ako sú CIA alebo FBI.

Trend používania techník ofenzívnej bezpečnosti však pomaly preniká do širšieho povedomia firiem. A je to len dobre. Týmto prístupom zvyšujú svoju bezpečnostnú odolnosť a minimalizujú riziká.

Niečo z vojenského žargónu

Dobre známe porekadlo „ťažko na cvičisku, ľahko na bojisku“ sa dá v prenesenom význame použiť aj pri využívaní prvkov ofenzívnej bezpečnosti. Reálnou simuláciou útokov získame komplexný obraz o danom systéme a nespoliehame sa len na nastavené politiky či správne napísaný softvér, ale jednotlivé komponenty podrobíme reálnej skúške.

Samozrejme, táto skúška musí byť dostatočne reálna, no na druhej strane nemôže ohroziť našu prevádzku či spôsobiť firemné straty. Dôležité je však simulované útoky správne vyhodnotiť a potom spätne reflektovať výsledky do procesov a do bezpečnostných nastavení. Vždy sa oplatí mať tieto znalosti skôr ako útočník.

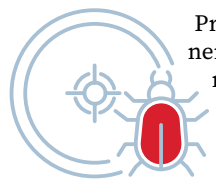
Skúste pentest

Prvky ofenzívnej bezpečnosti sa dajú použiť na takmer akúkoľvek súčasť bezpečnostných nastavení, či už ide o zabezpečenie siete, aplikácií, procesov, či dokonca na obozretnosť používateľov. Výber jednotlivých prvkov sa bude líšiť podľa profilu spoločnosti, no takmer každá spoločnosť môže využiť najmä penetračné testovanie a interné phishingové kampane.

Penetračné testovanie môže odhaliť dôležité slabiny v kľúčových systémoch spoločnosti, a tým predchádzať zneužitím týchto zraniteľností útočníkmi. Penetračné testovanie sa však nelimituje len na softvér či webové aplikácie. Pentesty vieme využiť aj na testovanie dodávateľských reťazcov.

Hlavne začať

Dáta a poznatky, ktoré získame takýmito cvičeniami, sú nesmierne relevantné a poskytujú reálny obraz o bezpečnosti v danej spoločnosti. Takéto dáta nevieme nijako inak dostať, a preto by hlavnou otázkou nemalo byť, či s prvkami ofenzívnej bezpečnosti začať, ale kedy a ako ich správne integrovať do procesov riadenia informačnej bezpečnosti.



Stáva sa, že techniky ofenzívnej bezpečnosti vníma manažment spoločnosti s odstupom alebo nedôverou. Výsledky však majú zásadný vplyv na celú oblasť informačnej bezpečnosti.

Strategická úroveň

Ofenzívne techniky poskytujú pre vrcholový manažment dôkazy o reálnych rizikách a slabinách jednotlivých systémov a procesov. Dáta sú základom pre strategické rozhodnutia a alokáciu zdrojov, čiže vedia priorizovať investície do bezpečnosti na základe reálnych, de facto potvrdených hrozieb.

Pre finančných alebo generálnych manažérov prinesú testy porozumenia rizikám na úrovni ich povinností a zodpovednosti. Dokážu tak účinnejšie začleniť bezpečnostnú kultúru a súlad s reguláciami do stratégie firmy.

Taktická úroveň

Stredný manažment, často bezpečnostní a IT manažéri využívajú výsledky testov na zlepšenie interných procesov, politík a bezpečnostných architektúr.

Výstupom sú pre nich informácie o reálne zneužiteľných zraniteľnostiach z hľadiska závažnosti aj dosahu na biznis operácie. Následne tak navrhujú bezpečnostné kontroly a opatrenia. Výsledky im pomáhajú pri tvorbe plánov reakcie na incidenty, v zlepšení SOC operácií a v zladení technických a biznis cieľov v bezpečnostných projektoch.

Operatívna úroveň

Kyberbezpečnostní špecialisti, admini, analytici samotné ofenzívne techniky často realizujú alebo reagujú okamžite na ich výstupy.

K dispozícii tak majú reálne prípady pre ladenie detekcie v monitoringu alebo bezpečnosti koncových zariadení. Riešia konkrétne zraniteľnosti a nasadzujú bezpečnostné záplaty, optimalizujú pravidlá firewallov, manažment prístupov a oprávnení. Ak bolo cvičenie realizované interným red tímom, tak, samozrejme, aj pre nich prináša takéto cvičenie personálny prínos v podobe osvojovania si taktík, techník a procedúr v „skoro reálnom“ cvičení.

Michal Srnec
vedúci oddelenia informačnej bezpečnosti
Aliter Technologies