HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 16. – 18. DECEMBRA 2022

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Aby sme videli svetlo na konci tunela. A aby nešlo v protismere.

TÉMA

Bezpečnostní profesionáli pribúdajú v desiatkach, úlohy v stovkách, útoky v tisíckach. A čaká nás aj personálne upratovanie v kybernetickej bezpečnosti.

Potreby firiem a celej spoločnosti sa nemôžu spoliehať iba na klasický vzdelávací systém. ILUSTRAČNÁ FOTO: DREAMSTIME

Takmer tri štvrtiny firiem na Slovensku má problém nájsť kvalifikovaných IT odborníkov. Podľa septembrového prieskume nám chýba pätnásťtisíc IT profesionálov.

Čo sa však týka nedostatku bezpečnostných odborníkov, problém majú všetci. „Ak počítame iba nevyhnutné pozície, potrebujeme minimálne dvetisíc profesionálov," varuje Miroslav Havelka z Kompetenčného a certifikačného centra kybernetickej bezpečnosti.

Všetci sa zhodujú

Kybernetická bezpečnosť strháva na seba stále viacej pozornosti. Spúšťačom boli legislatívne povinnosti aj udalosti za ostatný rok. „Je to aj dôsledok zvýšených kybernetických hrozieb, ktorým čelia všetky firmy, bez ohľadu na ich veľkosť alebo oblasť podnikania," potvrdzuje rastúci záujem o služby kybernetickej bezpečnosti aj Lukáš Okál Security lead Microsoft Česká republika a Slovensko.

Organizácie všetkých typov a vo všetkých sektoroch sú konfrontované s otázkou, ako dokážu chrániť seba aj svojich zákazníkov. Povinnosti a kompetencie v kybernetickej bezpečnosti tak „pristali na stole" najmä íročkárom, právnikom a občas aj personalistom. Citovaný aktuálny prieskum spoločnosti Microsoft o nedostatku IT odborníkov nás však varuje, že ani tam nie sú nekonečné personálne zdroje.

Už nemáme odložený čas

Kritické sú najmä pozície manažéra kybernetickej bezpečnosti v organizáciách štátnej správy a v zdravotníctve a tesne nad priepasťou stojí samospráva. „Nemáme ani personálne, ani finančné zdroje," stručne charakterizuje stav Jana Červenáková viceprezidentka Únie miest Slovenska.

Primátori sú ako štatutári zodpovední za kybernetickú bezpečnosť, ale ak musia v súčasnosti riešiť esenciálne služby pre mesto, kybernetická ochrana sa často opiera o nádej, že „nás si nikto nevšimne". V tomto zazlieva Jana Červenáková štátnej správe, že mestám udeľuje iba úlohy a povinnosti a neposkytuje podporu, či už ide o rozpočet, vzdelávanie, alebo zdieľanie zdrojov.

> V kybernetickej bezpečnosti chýbajú aj dodávatelia, ktorí okrem základnej prevádzky a údržby vedia poskytnúť aj expertízu, analýzu, vedenie a strategickú podporu.
>
> **Rastislav Beňo,** manažér informačnej bezpečnosti

Aj tí najlepší hľadajú

Obrovský nedostatok kvalifikovaných špecialistov nie je žiadnym tajomstvom, ale obsadiť seniorné posty je samo osebe výzva. „Čo nás prekvapuje, nie je ani tak konkrétna oblasť, ktorá by dlhodobo v zručnostiach kandidátov absentovala, ale skôr vnímanie seniority verzus skutočne prezentované zručnosti," hovorí Michal Srnec, CISO Aliter Technologies. Veľa kandidátov vie zručnosti demonštrovať len na konkrétnom type výrobcu a nie vo všeobecnosti, teda koncepčne. Jeho kolegyňa, HR manažérka Zuzana Ištoková sa o to viac sústreďuje na prácu s talentmi: „Učí nás to viac a lepšie ich počúvať a názory, postoje a odporúčania citlivo zvážiť." Venuje informáciám z praxe zvýšenú pozornosť a vyberá tie, ktoré vie spoločnosť aplikovať a rozvíjať v súlade s technologickými trendmi.

Pohli sa ľady

„Intenzívne vnímame, že už aj zákazníci z iných odvetví ako IT začali venovať bezpečnosti zvýšenú pozornosť," pripája sa ku kolegom Jozef Bálint bezpečnostný špecialista Alison Slovakia.

Takže napríklad taký bezpečnostný architekt má na pracovnom trhu hodnotu futbalovej hviezdy. Aby bol schopný navrhnúť a implementovať kombináciu sieťovo a datacentrovo orientovaných opatrení na zabezpečenie prevencie, detekcie a reakcie na bezpečnostné incidenty, musí rozumieť mnohým oblastiam. A tieto opatrenia musia byť v súlade s bezpečnostnými politikami, ktoré vyplývajú z biznis a technických požiadaviek.

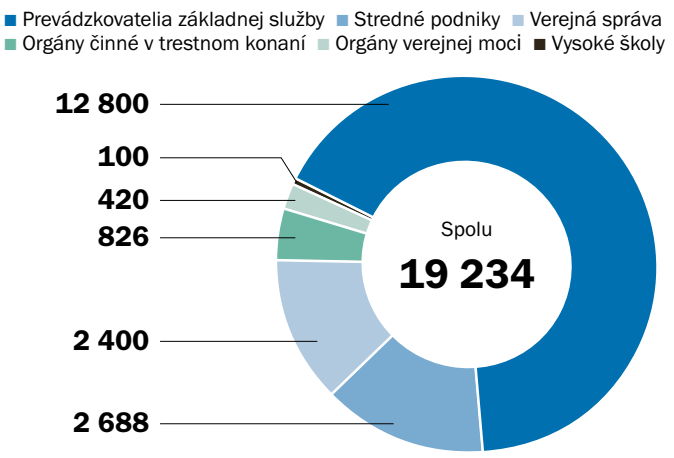
Aj by platili, ale niet komu

Rastislav Beňo manažér informačnej bezpečnosti Mitsubishi Chemical Advanced Materials pripomína situáciu, keď mnohí riaditelia bezpečnostných odborov nemohli kvôli obmedzeniam nákladov obstarať tú či onú technológiu. Dnes sa častejšie stretáva s problémom, že „napriek všetkým krízam dnešného sveta už pre mňa nie je takým problémom obstaranie technológie, ale skôr služby s pridanou hodnotou." Chýbajú aj dodávatelia, ktorí okrem základnej prevádzky a údržby vedia poskytnúť aj expertízu, analýzu, vedenie a strategickú podporu.

Aj snaha sa počíta

Kompetenčné centrum vypravilo do života už viac ako stovku manažérov kybernetickej bezpečnosti.

Požadovaný počet zamestnancov v kybernetickej bezpečnosti na Slovensku



Zdroj: Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

„Až na kurze som zistil, čo bude náplň mojej práce," je až príliš časté hodnotenie od účastníkov vzdelávacích kurzov. Miroslav Havelka sa tak stretáva s úprimnou snahou organizácií splniť zákonné požiadavky, ale najmä so zaskočenými adeptmi.

Do zodpovedajúcich pracovných pozícií sa často ustanovujú špecialisti z príbuzných oborov, ktoré sa zaoberajú ochranou údajov a je potrebné ich pripraviť na postupné zvládanie požiadaviek v kybernetickej bezpečnosti.

Do roka a do dňa

Problémom Slovenska tak stále zostáva nedostatok disponibilných profesionálov v kybernetickej bezpečnosti. Cieľom je preto v najkratšom možnom čase získať potrebný počet kvalifikovaného personálu a obsadiť aspoň roly, ktoré sú povinné zo zákona. Potrebujeme zároveň dobrú definícia úloh, kompetencií a vedomostí profesionálov kybernetickej bezpečnosti. Je to dobrý základ na vybudovanie bezpečnostných oddelení, platové tabuľky aj nastavenie vzdelávania.

Každý profesionál má svoju rolu

Od januára budúceho roku bude účinná vyhláška o znalostných štandardoch v kybernetickej bezpečnosti. Vyhláška zároveň stanovuje dvanásť rôl kybernetickej bezpečnosti na Slovensku.

Rola v kybernetickej bezpečnosti predstavuje konkrétne úlohy a činnosti. Zároveň sú s ňou spojené povinnosti aj oprávnenia pri návrhu, vývoji a prevádzke siete alebo informačného systému.

Tým, že vyhláška popisuje roly, stanovuje aj znalostné štandardy. Je to zároveň výborná navigácia pre personalistov, štatutárov, školy aj písanie životopisov. A dobrá správa pre menšie firmy? Pozícia môže zahŕňať aj viacero rôl.

Trend je upskilling

Ak zapĺňame prázdny priestor na trhu práce, najefektívnejšie je vydať sa cestou ďalšieho vzdelávania, či už odborného, rekvalifikačného alebo kontinuálneho. Aj vzdelaní profesionáli takto môžu napredovať v práci, alebo si nájsť ďalšie príležitosti v organizácii. Dlhodobým riešením pre personálne posilnenie kybernetickej bezpečnosti však zostáva vysokoškolské vzdelávanie.

Ivan Kotuliak, dekan FIIT STU je realistom a upozorňuje, že kvalitné vzdelávanie sa nedá urýchliť a počet študentov musí zodpovedať kapacitám univerzity. Takže ak sa školy zatiaľ pasujú s nulovým záujmom rezortu školstva aj nedostatkom pedagógov, stovky absolventov informačnej bezpečnosti môžeme očakávať tak o päť rokov.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · eset · Progress · MICRO FOCUS · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 16. – 18. DECEMBRA 2022

Čo ma pobavilo v roku 2022 v brandži

ANKETA

Čím je práca ťažšia, o to viac treba nadhľadu. Týka sa to aj bezpečnostných profesionálov. Táto kategória odpovedí by mala v športe názov voľná jazda. Oceňuje sa kreatívny prístup aj prekvapenia.

Rastislav Janota,
riaditeľ, Národné centrum kybernetickej bezpečnosti SK-CERT

Pracujeme v oblasti, kde sú vtipné historky často súčasťou veľkých problémov. Zažil som viacero niekedy až komických situácií, je to však zábava cez slzy. Ale z roka si chcem pamätať dobré skúsenosti a tie sa spájajú s ľuďmi. Vidím zväčšujúcu sa skupinu odborníkov a manažérov, ktorí rozumejú, chcú, vedia a veľa pre to v organizáciách robia. Pribúdajú aj ľudia, ktorí nezištne pomáhajú iným aj komunite. A to nás posúva všetkých dopredu.

Michal Ďorda,
audítor kybernetickej bezpečnosti Auditori.it

Tohtoročná informácia o využívaní nezašifrovaných komunikačných nástrojov medzi rôznymi významnými osobami na Slovensku, ktorým chýba povedomie o zabezpečení citlivých informácií. Predstavte si, že sedíte večer v reštaurácii, prihlásite sa na verejnú WiFi sieť reštaurácie a pomedzi jednotlivé chody si píšete s ostatnými ministrami a poslancami ohľadom citlivých štátnych záležitostí. Želám všetkým viac obozretnosti v roku 2023.

Peter Dufek,
manažér kybernetickej bezpečnosti Procare a Svet zdravia

Ani po dvoch dňoch som si nedokázal spomenúť na veselú príhodu súvisiacu s našou misiou. Nie je jednoduché zažiť v našej brandži niečo úsmevné alebo vtipné. Spravidla sa až neskôr zabávame na veciach, ktoré keby sa nám stali, by nám neprišli až také vtipné. Ako napríklad, keď sa dvojica adminov po prehýrenom večierku rozhodla zmeniť heslá, alebo iní zasa pokračovať vo vianočnom večierku v serverovni, keďže blikajúce svetielka routerov a serverov im prišli viac cool.

Ján Grujbár,
generálny riaditeľ Aliter Technologies

S kolegami sme si povedali, že skúsime s touto otázkou osloviť umelú inteligenciu a musím povedať, že nás nesmierne pobavilo ako AI dnes dokáže porozumieť otázke aj v našom jazyku a v odpovedi vytvoriť vtipný inšpiratívny a vskutku verný príbeh. Skúste si to. A to znamená len jedno, že umelá inteligencia bude ešte výraznejším driverom v informačnej bezpečnosti a jej význam bude rásť tak na strane red teams, čiže útočníkov, kde budú napríklad sofistikovanejšie phishingové kampane, ako aj na strane blue teams – obrancov, kde rastú možnosti behaviorálnej analýzy.

Roman Varga,
manažér kybernetickej bezpečnosti Dôvera zdravotná poisťovňa

„Vycibrená“ komunikácia s kyberpodvodníkmi, ktorí útočia proti Dôvere pri phishingových útokoch, prináša veľakrát úsmevné situácie. No nie pre nich. Po dosiahnutí môjho cieľa začínam s trestnými oznámeniami „v štádiu pokusu“ alebo nahlasovaním incidentov s dostatočnými dôkazmi na csirt.sk.

Tomáš Zaťko,
CEO, etický hacker, Citadelo

Obrovské pokroky v oblasti strojového učenia. Prebiehajúci ošiaľ s ChatGPT zabáva a šokuje ľudí, pretože dáva veľmi zmysluplné odpovede. Dokáže napísať kusy programov, dokonca nájsť v programoch zraniteľnosti. A vývoj pokračuje ďalej. Budúcnosť je teraz!

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

Pravdupovediac, pobavilo ma veľa vecí, ale skôr to bolo niečo na hranici údivu, keď neveriacky pozerám. Hodnotili sme bezpečnostný incident a pýtali sme sa subjektu, či robia aj testy zraniteľností. Odpoveď bola – nie. Ale pri predložení dokumentácie som zrazu narazil na niekoľko reportov, ktoré opisovali, aké zraniteľnosti sú v systéme. Teda testy dodávateľ urobil, ale akosi si ich veľmi nevšímal, že existujú.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti, Void SOC Soitron

Žarty bokom, kybernetické riziká a hrozby nie sú žiadna „sranda“. To si uvedomujú všetci ľudia z odvetvia, a napriek tomu nás môže práca baviť aj pri vážnych témach či situáciách. Teda, ak práve náhodou nenájdete u klienta bezpečnosť ako cibuľu – že „ošúpete“ pár vrstiev a je vám do plaču.

Igor Práznovský,
riaditeľ odboru bezpečnosti informačných systémov Sociálna poisťovňa

Nezriedka sa zabavíme kreativitou „content writerov“ phishingových emailov. Za všetky spomeniem napríklad text výhražného emailu, ktorý uvádzal, že odosielateľ má kompromitujúce nahrávky na VHS kazete, iný zase ponúkal reálnu štúdiu o plodnosti mužov, ktorí nosia kilt (škótsku sukňu), priloženú v spamovom emaile, aby prešiel automatickou analýzou textu.

Matej Síleš,
manažér IT bezpečnosti UPC BROADBAND SLOVAKIA

Oblasť kybernetickej bezpečnosti vôbec nie je nudná. Práveže ide o veľmi dynamický a zaujímavý odbor. Popri našej práci sa vždy nájdu aj vtipné momenty, ktoré nám spríjemňujú dni. Veď ako sa hovorí, s humorom ide všetko lepšie. Mňa vždy pobavia odpovede typu „To sa asi samo...“ alebo „Ja s tým neviem robiť.“ Samozrejme, aj pre nás sú najvtipnejšie situácie, ktoré sú bohužiaľ nepublikovateľné.

Jaroslav Oster,
predseda Správnej rady Preventista.sk

Úprimné pobavenie nepodfarbené sarkazmom asi aktuálny vývoj cybersec neposkytuje. Preto skôr pohľad na to, čo mňa osobne potešilo, inšpirovalo. Boli to drobné poznania, ako napríklad, že učebnice pre základné a stredné školy vydané naším občianskym združením našli reálne uplatnenie, že sa nám podarilo dokončiť ďalšie učebnice pre slovenské školstvo a že sme našli nadšenie i energiu pokračovať v tvorbe ďalších.

Roman Čupka,
hlavný konzultant Progress Software a CEO Synapsa Networks

Pravidlo obuvníkov syn chodí bosý platí aj v kybernetickej bezpečnosti. A aj u nás v domácnosti. Po smishingu bol kompromitovaný menej významný bankový účet člena rodiny. Potvrdilo sa, že nepozornosť a tlak na urgenciu sú základom úspešného kybernetického útoku. Našťastie však striktne oddeľujem rozloženie a úschovu aktív, a tie významné mám osobne pod niekoľkostupňovou ochranou.

Ivan Makatura,
generálny riaditeľ Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

V európskych inštitúciách zrejme definitívne prevládlo heslo „čím viac kyber – tým viac odborník“. Pomaly každý úradník EÚ má tento rok tendenciu k nadužívaniu výrazu kyber. Najlepšie vo forme nových právnych predpisov. Kto ešte nemá vlastné kybernariadenie či kybersmernicu, nech sa hlási u súdruha Müllera na vrátnici Európskeho parlamentu. Vlastne to už ani nie je smiešne.

Ján Lichvár,
konateľ, Axenta

Nič ma v tomto roku nepobavilo a nenašiel som naozaj nič. Dobrá správa však je, že sa objavujú prvé lastovičky na strane prevádzkovateľov základnej služby, ktorí chápu, že informačná a kybernetická bezpečnosť je proces a nie dodávka krabice. Uvedomujú si, že bezpečnosť je o ľuďoch, procesoch a technológiách, s ktorými je potrebné pracovať na dennej báze.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov Tatra banka

Vtip v informačnej bezpečnosti má vždy smutný podtón. Napríklad naše banky boli zaradené pod pôsobnosť zákona o kritickej infraštruktúre. Dostali príslľub: „Štát vám v čase krízy pomôže.“ Smutné a vtipné zároveň je, že keď boli splnené všetky požiadavky štátu na zaradenie, tak bolo oznámené, že v čase krízy podpora nebude. Pretože banky nie sú prvkom hospodárskej mobilizácie.

Daniel Chromek,
riaditeľ informačnej bezpečnosti ESET

Práca CISO je ťažká a nie je v nej miesto na zábavu. Mojím jediným potešením je ignorovanie každodennej várky emailov od rôznych spoločností, ktorých zástupcovia sa ma pýtajú, či mám 15 minút na telefonát tento týždeň.

Marián Klačo,
vedúci oddelenia bezpečnosti informácií Volkswagen Slovakia

Keď vám kamarát povie, že má najbezpečnejšie heslo na svete. A potom zistíte, že ho má napísané pod klávesnicou, lebo si ho nezapamätá. Alebo si prečítate v „serióznom“ preklade, že firewall je protipožiarna stena. Hovorí sa, že humor lieči. Možno raz bude stačiť len sa veľa smiať a vyliečite aj ransomvérom zavírený počítač. Šťastný a bezpečný rok 2023 všetkým.

Diana Legdanová,
vedúca úseku bezpečnosti Východoslovenská energetika Holding

Pred pár dňami ma pobavil pokus o získanie môjho telefónneho čísla. Teda skôr tá kombinácia faktov ako samotný pokus. Akože pán XY z pôdohospodárstva volal mojej kolegyni z iného oddelenia, či mu môže dať moje číslo, lebo sme sa stretli na jednej medickej konferencii, kde som hovorila o phishingu, ale ja som mu ušla a nestihol si na mňa vypýtať kontakt. Našťastie má kolegyňa zdravý rozum.

Ján Adamovský,
riaditeľ bezpečnosti Slovenská sporiteľňa

Rýchlosť doby, v ktorej žijeme, a bezpečnostné hrozby, ktorým čelíme, prinášajú rôzne príbehy. Klientku banky podvodník telefonicky presvedčil, aby urgentne poslala niekoľko tisíc bratovi jej manžela, ktorý peniaze súrne potrebuje. Pri následnom volaní do banky klientka oznámila, že chce nahlásiť podvod, lebo si uvedomila, že jej manžel brata nemá.

Napriek technológiám a ich rýchlemu rozvoju zostáva kybernetická bezpečnosť stále oblasťou, kde sú najdôležitejší ľudia. Každý z nás. Nech sú vaše dni bezpečné v osobnom aj pracovnom živote.

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

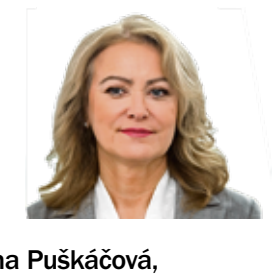
Úprimne a nefalšovane ma pobavil počet a kvalifikácia odborníkov, ktorí sa vyrojili pri kybernetickom „útoku“ na Národnú radu. Aký útok, takí odborníci.

Ivan Kopáčik,
bezpečnostný expert, Gordias

Odchytili mi heslo. A teraz musím premenovať môjho psa. Alebo povestné – čo sa stane vo Vegas, ... skončí na YouTube. Áno, máme svoje vtipy. Ale zasmeje sa len ten, kto problematike ako-tak rozumie. Čo môže byť tiež motivácia začať sa bezpečnosťou zaoberať.

Tomáš Hettych,
viceprezident, ISACA

Po dvoch náročných rokoch s covidom ma baví prehnaný zápal niektorých organizácií riešiť požiadavky kybernetickej bezpečnosti. Niektoré aktivity, dokumenty a riešenia sú naozaj neortodoxné a originálne. Iba čas, prax a hlavne audit kybernetickej bezpečnosti ukážu, či sú aj také účinné, ako sú zábavné.



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

Asi najväčšie pobavenie a vytriezvenie prišlo s uvedomením, že napriek všetkej osvete, ktorú sa snažíme sprostredkovať našim používateľom, a vlastným dlhoročným skúsenostiam v kybernetickej bezpečnosti, som sa sama osobne takmer stala obeťou podvodu v kybernetickom svete.

Timea Tomčová,
manažérka kybernetickej bezpečnosti, Poisťovňa Union

Dokáže ma vždy pobaviť, keď napriek stupňujúcej sa medializácii kybernetických útokov diskutujúci znalý IT problematiky položí otázku „Kto by už len na nás útočil?“ Alebo argumentuje „Veď u nás sa nikdy nič také nestalo.“ A pritom väčšinu dňa trávi aktívne v kybernetickom priestore, no riziká s tým spojené spochybňuje.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 16. – 18. DECEMBRA 2022

Sú vyzbrojené vedomosťami, silou aj rozpočtom. Sú veľmi nebezpečné

APT skupiny

APT skupiny sú zoskupenia útočníkov zvyčajne z radov štátnych organizácií alebo formácie, ktoré pracujú na štátne objednávky.

V útočných operáciách využívajú pokročilé pretrvávajúce hrozby – Advanced Persistent Threats (APT). Disponujú širokou škálou poznatkov, pokročilými nástrojmi, technikami, ktoré zneužívajú zero-day zraniteľnosti a často aj značnými zdrojmi.

APT skupiny realizujú cielené a sofistikované kybernetické operácie, prenikajú do systémov vysokopostavených cieľov a nepozorovane v nich zotrvávajú. Účelom je väčšinou dlhodobá kybernetická špionáž vládnych organizácií či korporácií.

Čoho sa vyvarovať na Slovensku v roku 2023?

Aj napriek tomu, že sme malá krajina, sme cieľom pre APT skupiny.

- Slovensko je členskou krajinou NATO a Európskej únie, má prístup k rôznym informáciám a takisto aj vplyv na vývoj situácie.
- Terčom môžu byť dodávatelia pre firmy v krajinách v hľadáčiku cudzích vlád.
- Útoky zaznamenajú aj firmy, ktoré vyjadrujú podporu Ukrajine.

Na kyberpriestor bude naďalej s vysokou pravdepodobnosťou vplývať geopolitické napätie.

- Predpokladajú sa štátmi sponzorované kybernetické útoky typu DDoS či pokusy o šírenie deštruktívnych malvérov.
- Očakáva sa pokračovanie útokov na zdravotnícky sektor, čo je obzvlášť závažné.

Ako sa treba pripraviť na rok 2023?

- Základným pilierom je dodržiavanie základných bezpečnostných pravidiel zamestnancami.
- Na úspešnú obranu je potrebný monitoring koncových bodov v reálnom čase pomocou XDR riešení, ktoré prinášajú prehľad o dianí v celej sieti.
- Odporúčam nasadiť nástroje cloudového sandboxu, ktoré dokážu odhaliť doposiaľ nezverejnené zraniteľnosti bez toho, aby vznikla škoda v sieti.

Július Selecký,
senior technický špecialista ESET, spol. s r. o., odborný asistent, Fakulta managementu UK

Ktoré štáty sú spájané s APT skupinami?

Rusko
Primárnym cieľom APT skupín je Ukrajina. Ukrajinské vojnové ciele sú špeciálne v hľadáčiku skupín Sandworm, Callisto a Turla.

■ Na zozname agresívnych aktérov hrozieb s politickým kontextom je dlhodobo Gamaredon. InvisiMole je spájaná s útokmi na ukrajinské zastupiteľstvá a organizácie vo východnej Európe. The Duke sa presadzuje ako útočná skupina proti vládnym organizáciám v západných krajinách.

Severná Kórea
Na letecký a obranný priemysel sa sústreďujú útočníci skupiny Lazarus. Napadli organizácie v tomto segmente v rôznych častiach sveta a ich prácu našli výskumníci aj vo firmách, ktoré sa zaoberajú kryptomenami.

■ Skupina Kimsuky pri útokoch na finančné inštitúcie a firmy využila zraniteľnosti Microsoftu. Konni pokračuje v útokoch na diplomatickú vertikálu.

Čína
Skupina SparklingGoblin nasadila proti univerzite v Hongkongu nový variant backdooru SideWalk pre Linux. Confluence zraniteľnosť zas zneužila pri útoku na potravinársku spoločnosť v Nemecku a strojársku spoločnosť v USA.

■ Jedna z kampaní skupiny MirrorFace sa zamerala na voľby do hornej komory japonského parlamentu. Mustang Panda aktívne cieli na vládne, vzdelávacie a telekomunikačné organizácie v Európe a Ázii.

Irán
Čoraz väčší počet skupín sa zameriava najmä na izraelské ciele. Skupina POLONIUM cielila na desiatku organizácií v Izraeli, pričom zneužila na komunikáciu s riadiacim strediskom cloudové služby ako Dropbox, Mega či OneDrive.

■ Agrius v útoku na dodávateľský reťazec cielila na spoločnosti v diamantovom priemysle v Južnej Afrike, Hongkongu a Izraeli. Skupina APT35 sa zamerala na maloobchodný predaj kozmetiky, spoločnosti kybernetickej bezpečnosti, výrobu elektroniky a právne služby.

Zdroj: ESET APT Activity Report. Prvé vydanie, máj – august 2022. Škodlivé aktivity opísané v správe sú detegované produktmi ESET. Monitoring hrozieb je založený väčšinou na vlastnej telemetrii a overený výskumom ESET.
Infografika: HN/M. Rybanský

Aplikácie vedia všetko o tom, čo a kedy robíme

TECHNOLÓGIE

Platba cez telefón? Tri kliky. Kontrola zabezpečenia firmy na displeji? Dva kliky. Prenos dát z idúceho auta do centrály? Pilierom je aplikačná bezpečnosť.

Ku koncu roka 2022 je k dispozícii viac ako sedem miliónov aplikácií na dvoch hlavných, hráčskych aj minoritých platformách.

ILUSTRAČNÉ FOTO: DREAMSTIME

Údaje v „appkách“ sú tým najcennejším aj pre ich tvorcov a prevádzkovateľov, či už ide o prácu, alebo zábavu.

Spracovanie informácií v aplikáciách, ich prenos a uchovávanie v systémoch prevádzkovateľa sa stáva jednou z najdôležitejších úloh bezpečnostného sektora.

Optikou konkurencie

Aplikácie sú neoddeliteľnou súčasťou komunikácie, riadenia, výroby aj služieb. Organizácie okrem používania štandardných biznis aplikácií majú často aj vlastný vývoj. „Údaje môžu urobiť zásadný rozdiel medzi výhrou a prehrou,“ hovorí Julian A. Garcia-Grajales, zodpovedný za výkon tímu Jaguar TCS Racing. Firemný tím používa päťdesiat aplikácií zabudovaných v pretekárskom aute, ktoré predstavujú štvrť milióna riadkov kódu.

Treba dobre začať

Aplikácie sa používajú na načítanie a analýzu aktuálnych údajov aj údajov z predchádzajúcich pretekov a testovacích jázd. Takže rozhodnutia, ako nastaviť stratégiu na okruhu a dosiahnuť čo najlepší výkon, sú plne založené na dátach. Bezpečnosť aplikácií a ich prevádzky v komplexnom prostredí sú pre tím Jaguaru životne dôležité. Pri vývoji nových funkcií alebo optimalizácii aplikácií je kľúčové analyzovať už zdrojový kód, aby bol bezpečný. Tu sa využíva statická analýza. Softvérový nástroj Fortify kategorizuje a prioritizuje zistenia, aby ich vývojári mohli okamžite riešiť.

Čo všetko appky zvládnu

Samotná korporácia prevádzkuje cloudové prostredie, ktoré uľahčuje spoluprácu medzi všetkými pretekmi Jaguar tímu. Väčšina prístupu k aplikáciám je cez webové alebo aplikačné rozhrania a práve tu sa uplatňuje dynamické skenovanie. Táto funkcia zabezpečuje, aby bol kód robustný a zostal plne bezpečný. Súčasné statické a dynamické skenovanie identifikuje potenciálne zraniteľnosti v kóde aplikácie. Všetky zraniteľnosti sú tak vyriešené skôr, ako by mohli spôsobiť problémy v produkčnom prostredí. Pravidelné skenovanie kódu zas pomáha vývojárom dizajnovať lepšiu štruktúru a ochranu aplikačného rozhrania, čo vedie k vyššej kvalite aplikácií.

Jednoducho a intuitívne

Vývojári aplikácií a zadávatelia často vinili bezpečnostné požiadavky za to, že ich zdržujú a brzdia vo vývoji. Preto hľadajú jednoduchý a flexibilný spôsob, ako testovať aplikácie rýchlo, presne a bez toho, aby museli vyčleniť ďalšie zdroje alebo inštalovať a spravovať ďalšie riešenia. Riešenie Fortify On Demand umožňuje vývojárom využívať bezpečnostný softvér ako službu (Software-as-a-Service) a nevyžaduje zmenu nástrojov. Vplyv na prevádzku je iba minimálny.

> Pri vývoji nových funkcií alebo optimalizácii aplikácií je kľúčové analyzovať už zdrojový kód, aby bol bezpečný.
>
> **Anna Stehlíková,** manažérka pre bezpečnostné licencie Micro Focus

Kde sú slabé stránky

Na rastúce hrozby reaguje komunita Open Web Application Security Project, ktorá ponúka voľne dostupné metodiky, dokumentáciu a nástroje pre bezpečnosť webových aplikácií. V minulom roku klasifikovala ako najväčšie riziko narušenie či prelomenie kontroly prístupu. Až 94 percent testovaných aplikácií malo v tejto oblasti slabé stránky. Následkami sú neoprávnené zverejnenia informácií, modifikácie či zničenie údajov alebo aktivity bez povolenia používateľa.

Niečo o silných stránkach

Prácou kybernetických zločincov je stále odhaľovať a vyhľadávať nové zraniteľnosti v softvéri. Čoraz častejšie to robia nástroje na báze umelej inteligencie.

Ochrana aplikácií si vyžaduje rovnako sofistikované nástroje a ešte vyššiu rýchlosť. Súčasťou testov je preto aj kontinuálna analýza bezpečnostných rizík, ktoré vznikajú v čase.

Nástroje na testovanie bezpečnosti využívajú informácie priamo z monitorovania nových hrozieb. Bezpečnostný tím Fortify Software Security Research deteguje viac ako tisíc kategórií zraniteľnosti v dvadsiatich siedmich programovacích jazykoch a pokrýva viac ako jeden milión aplikačných rozhraní.

„Skrátene povedané, najlepší kód je bezpečný kód. Či už ide o aplikácie pre pretekárske tímy, logistické firmy, zdravotníctvo, finančné služby, alebo využitie v malých vývojárskych firmách,“ uzatvára Anna Stehlíková.

TREND

Chcel by som vám niečo priať aj pod stromček

V desiatkach organizácií som urobil desiatky auditov a rok končím s hlbokým presvedčením, že kľúčovým pilierom kybernetickej bezpečnosti sú aj naďalej ľudia.

Kto sa teda podieľa na tom, aby mala firma šancu sa ubrániť útoku? Sú to top manažéri, ktorých úloha je najmä nastaviť firemné DNA tak, aby sa kybernetická bezpečnosť v organizácii vôbec riešila. Niekedy je veľmi ťažké presvedčiť ich o tom, aby na túto úlohu nerezignovali. Mal som však šťastie a zopár som ich pri svojej práci za posledné obdobie stretol. Prajem si, aby ich bolo čoraz viac. Ústredným pilierom je však manažér kybernetickej bezpečnosti. Tých je stále akútny nedostatok a podľa aktuálnej štúdie spoločnosti ICS2 z tohto roku ich celosvetovo chýba 3,4 milióna, čo je najviac za celé obdobie, odkedy štúdiu pripravujú. Aj napriek snahe univerzít, ktoré sa snažia pripraviť nové posily, a ďalších vzdelávacích inštitúcií je prírastok nových síl nižší, ako rastie dopyt. A preto je mojím druhým prianím, aby sa viac kolegov osmelilo a vydalo sa na dráhu manažéra kybernetickej bezpečnosti.

Dôležitými sú aj administrátori a bezpečnostní špecialisti, ktorí zabezpečujú, aby všetky prvky, ktorými sa vie firma brániť, zostali v najlepšej kondícii. Veľakrát pracujú aj v situácii, keď vedenie nedáva tejto téme žiadnu prioritu. Bez nich by aj manažéri kybernetickej bezpečnosti boli len kapitáni bez lode. Mojím tretím prianím je, aby im v novom roku neubudlo síl, zanietenosti a trpezlivosti. Nech sú inšpiráciou pre ďalších kolegov, ktorí sa k nim pridajú.

A napokon bežní používatelia – tí, pre ktorých sú všetky tie vymoženosti pripravené. Musíme ich oslovovať čoraz viac. Je nevyhnutné, aby prispeli obozretnosťou k tomu, aby ani v ťažkých časoch, keď čelíme bezprecedentnému tlaku, nepodľahnú a zachovajú si kritický úsudok a zdravú podozrievavosť. Ak im bude nabudúce ich banka písať, že im zablokovala kartu a musia sa prihlásiť cez pripravený link, spozornejú a zavolajú do banky, aby si to preverili. Naučia sa, že internet je nebezpečné miesto, voči ktorému sa musia správať s rešpektom a primeranou obozretnosťou. Mojím štvrtým prianím je, aby každý z nás používateľov bol pozornejší a ani pod umelo vytvoreným nátlakom nerezignoval na zdravú mieru podozrievavosti.

Nakoniec, čo vieme urobiť my „sekuriťáci“? Vieme pomôcť tým, že o kybernetickej bezpečnosti hovoríme na konferenciách, v médiách a v celej našej každodennej práci. Našou úlohou je podnecovať záujem o túto oblasť. Snažiť sa odovzdať svoje znalosti a posmeliť ďalších k tomu, nech sa k nám pridajú.

Tento rok a aj ten ďalší zostávajú aj naďalej najcennejším aktívom vo firmách ľudia.

David Dvořák, audítor kybernetickej bezpečnosti auditori.sk

Aj v tradične technologickej oblasti rastie hodnota ľudských skúseností.

ILUSTRAČNÉ FOTO: DREAMSTIME

RIEŠENIA

Najzaujímavejšie odpovede, ak riešite kybernetický incident

Počas významnej konferencie kybernetickej bezpečnosti na jeseň v Tatrách dostali účastníci panelových diskusií mnoho otázok. Zaznamenali sme tie najdôležitejšie z oblasti incident response.

Čo je dôležité pre udržanie kontinuálnej schopnosti reakcie na bezpečnostný incident? Prakticky, prosím.

Aby ste na vzniknutý bezpečnostný incident dokázali efektívne reagovať, je potrebné zabezpečiť niekoľko vecí. Treba mať dobre premyslený, naplánovaný a odsúhlasený proces riadenia bezpečnostných incidentov, „ušitý“ na mieru. Kritické je, aby proces nebol iba formalitou, ale aby bol zavedený a používaný v praxi, pravidelne testovaný a revidovaný. Ak máte správne zostavený, kvalifikovaný a dobre pripravený tím, bude schopný pri reakcii na incident rýchlo a efektívne spolupracovať. Súbor nástrojov a technických prostriedkov budete počas incidentu potrebovať na jeho identifikáciu, analýzu, riešenie a zdokumentovanie. Nezabudnite na vzťahy a spoluprácu s tretími stranami, ako sú poskytovatelia IT či služieb kyberbezpečnosti, telekomunikační operátori, právnici, regulátori, a podobne vašu schopnosť reakcie na incident veľmi pravdepodobne otestujú skôr či neskôr priamo reálni útočníci. Nemusí to byť hneď kybernetická katastrofa s odstavením celej organizácie, ale ak máte pocit, že vo vašej infraštruktúre sa nič podozrivého nedeje, odporúčame zlepšiť detekčné schopnosti.

Je metodika ITIL vhodná ako základ pri nastavení Security Incident Management procesu?

ITIL obsahuje zbierku best practices a rámcových návodov z oblasti IT služieb, a preto môže byť aj vhodným základom pre nastavenie procesu riadenia bezpečnostných incidentov. Ďalšou inšpiráciou môžu byť voľne dostupné publikácie Computer Security Incident Handling Guide od NIST a Good Practice Guide for Incident Management od ENISA. Je však veľmi dôležité si uvedomiť, že každá organizácia má vlastné špecifiká v oblasti bezpečnosti, a preto by aj proces riadenia bezpečnostných incidentov mal byť „ušitý“ na mieru.

Kto by mal podľa vášho názoru či skúsenosti tvoriť Incident Response tím, napríklad v spoločnosti spadajúcej pod zákon o kybernetickej bezpečnosti?

Základ incident response tímu budú určite tvoriť profesionáli z oddelenia IT a špecialisti na kybernetickú bezpečnosť. Aby však tím dokázal efektívne reagovať na rôzne typy situácií, mali by jeho členovia predstavovať širšiu paletu schopností a skúseností aj mimo IT. Nemali by tam chýbať zástupcovia z najvyššieho vedenia, právneho oddelenia,

ILUSTRAČNÉ FOTO: DREAMSTIME

HR a špecialisti na externú aj internú komunikáciu. Výber rol a ich obsadenia bude veľmi závisieť od povahy a veľkosti organizácie, jej služieb, činností, geografického záberu a ďalších faktorov. Vôbec nie je nevyhnutné, aby bola každá expertná rola v tíme obsadená interným zamestnancom. Je celkom bežné, že niektoré činnosti, napríklad krízová komunikácia, forenzné analýzy a podobne sa dopĺňajú vopred kontrahovanými externými dodávateľmi.

Ako si pri poskytovateľoch služby SOC as a service vie zákazník spoľahlivo overiť ich kompetentnosť ešte pred výberom?

Schopnosti a skúsenosti každého tímu Strediska bezpečnostných operácií odporúčame overiť z niekoľkých hľadísk. Prvým je vyspelosť poskytovania a riadenia služieb kybernetickej bezpečnosti, ktorú reprezentujú relevantné certifikácie, napríklad ISO 20000 a 27000 a členstvá v renomovaných organizáciách, ako sú TF-CSIRT Trusted Introducer a FIRST. Druhým faktorom môžu byť doterajšie skúsenosti SOC tímu a spokojnosť klientov s jeho službami. Tie si môžete overiť tak, že si vyžiadate referencie od súčasných či minulých zákazníkov SOC poskytovateľa. Tretím aspektom je odbornosť, ktorá sa tradične overuje technickými certifikátmi členov SOC tímu. Odporúčame ju však doplniť aspoň o jednu osobnú návštevu v poskytovateľovom SOC-u, spojenú s technickou diskusiou napríklad o riešení modelových incidentov s jeho špecialistami. Pomôže vám to doplniť formálne kvalifikácie o ľudský rozmer a aspoň čiastočne získať predstavu, ako by spolupráca v realite vyzerala.

Martin Lohnert, riaditeľ centra kybernetickej bezpečnosti Void SOC Soitron