

Hovoríte, že neťažíte kryptomenu? A ste si istí?

TÉMA

Bezpečnostné fakty, ktoré potešia aj šokujú.
Učíme sa žiť s kryptomenami.

Celkový objem transakcií kryptomien vzrástol v roku 2021 na 15,8 bilióna dolárov, čo je o 567 % viac ako v predchádzajúcom roku.

Najčastejšie citovaná správa Chainalysis preto zdôrazňuje, že so zločinom súviselo minulý rok iba 0,15 percenta kryptotransakcií. Rast legitímneho používania kryptomien ďaleko prevyšuje rast využívania v trestnej činnosti aj napriek obvyklému mediálnemu obrazu.

Závisí od ľudí

Prvá digitálna kryptomena bitcoin vznikla ako inštancia anonymných decentralizovaných peňazí a natívny prostriedok výmeny hodnoty v prostredí internetu, a to vďaka špecializovanej transparentnej technológii blockchain. Samozrejme, ako všetky nástroje, pôvodne neutrálne, sa môže využívať na nelegálne aktivity.

„Podvodníci často využívajú kryptomeny na vylákatie peňazí od ľudí, čo nerozumejú investovaniu, alebo na aktivity ako cryptojacking, keď využívajú výpočtový výkon, ktorý im nepatrí, na ťažbu kryptomien,“ dodáva David Stancel, investičný riaditeľ platformy Fumbi.

V roku 2021 bolo odcudzených približne 3,2 miliardy dolárov v kryptomene, čo je šesťnásobný medziročný nárast. V kryptomenovom priemysle sa totiž podniky rozbiehajú rýchlo, bezpečnostné riešenia sú často iba dodatočné a investori nedostatočne analyzujú riziko.

Ťažba je o lacných energiách

Predstavte si ťažbu kryptomien ako obrovskú farmu, kde špecializované ASIC zariadenia generujú svojím procesorovým a grafickým výkonom digitálnu menu.

Spoločnosť Digeconomists uvádza, že bitcoinová transakcia spotrebuje viac ako 1 500 kilowatthodín. Priemerná americká domácnosť by z tejto elektriny žila 50 dní.

„Preto je dôležité pri ťažbe kryptomien spotrebúvať energiu z obnoviteľných zdrojov,“ upozorňuje odborník na kybernetickú bezpečnosť Roman Čupka, „a energiu, ktorá pri ťažbe vzniká ako vedľajší produkt, recyklovať späť do infraštruktúry.“ Takto sa dá premeniť na kryptomenu sl-

nečná energia a teplo ako vedľajší produkt ťažby možno využiť na kúrenie či ohrev vody.

Počítače, routery, servery

Kryptomenu môže ťažiť ktokoľvek, kto má technológie, elektrickú energiu a prístup na internet. Nelegálna ťažba, keď hackeri využívajú infraštruktúru a energie bez vedomia majiteľov, sa preto stáva čoraz lákavejšou. A Slovensko nie je výnimkou.

Útoky spojené so snahou o kompromitáciu zariadení v infraštruktúre organizácií pripojených do podnikovej siete sú častým javom. Okrem počítačov a mobilných telefónov sa zneužívajú aj domáce routery telko operátorov a servery v dátových centrách.

Nemilá správa pre nás

Nelegálna ťažba kryptomien nie je to najhoršie, čo sa vám môže v kyberbezpečnosti stať, ale oberá vás o peniaze. Spoločnosť Progress Software preto vo februári uskutočnila meranie pomocou riešenia Flowmon v kybernetickom priestore jedného z najväčších telko operátorov na Slovensku, aby identifikovala anomálie.

„Takmer 18 percent identifikovaných udalostí je spojených s kompromitáciou infraštruktúry, využitím alebo so zneužitím zariadení na ťažbu a samotnou krádežou kryptomien,“ zhrňa Roman Čupka. V prípade kompromitácie je kľúčový detekčný mechanizmus, rýchla analýza stavu a odstránenie problému. Takto kompromitovaná infraštruktúra je často zdrojom ďalších udalostí spôsobujúcich závažné incidenty.

So suverenitou súvisí zodpovednosť

„Kryptomeny nám dávajú naspäť suverenitu – možnosť sporiť, držať hodnotu a posilať ju komukoľvek na svete bez tretích strán,“ vysvetľuje Juraj Bednár, spoluzakladateľ platformy Hacktrophie. Ak sa však niekto stane obeťou podvodu, napríklad phishingu, podpíše transakciu a prevedie kryptomeny, nedá sa to vrátiť. V takomto prípade nepomôže polícia ani nikto iný.

Najčastejší bezpečnostný problém vzniká, keď investori kryptomeny neuchovávajú v hardvérovej peňaženke. Ak si niekto nainštaluje iba mobilnú aplikáciu ale-



Aby ste vyťažili hodnotu jeden dolár, potrebujete pri bitcoine dvojnásobok energie ako pri ťažbe medi, zlata, alebo platiny.

FOTO: DREAMSTIME

Podvodníci často
využívajú
kryptomeny
na vylákatie
peňazí od ľudí,
čo nerozumejú
investovaniu.

David Stancel,
investičný riaditeľ platformy
Fumbi

bo peňaženku do počítača, môže dôjsť k napadnutiu zariadenia a k nezvratnej krádeži.

A čo bežné appky?

Podľa prieskumu Národnej banky Slovenska má reálnu skúsenosť s kryptomenami už deväť percent Slovákov. V súvislosti s hrozbami upozorňuje David Stancel na smart kontrakt aplikácie. V posledných dvoch rokoch nastal obrovský boom v oblasti decentralizovaných financií a vznikli stovky až tisíce aplikácií.

Sú efektívne dostupné komukoľvek s dostatočnou technic-

kou gramotnosťou. Notoricky sú však tieto aplikácie známe vysokou chybovosťou kódu. Mnoho bežných používateľov sa tak stalo obeťou týchto chýb a nezaplatených zraniteľností, ktoré využívajú hackeri.

Dobré body

K lepšej povesti kryptomien prispel aj Andy Greenberg, keď opísal, ako tím federálnych vyšetrovateľov a analytikov blockchainu zlikvidoval najväčšie online úložisko materiálu o sexuálnom zneužívaní detí. Vypátrali stovky zneužívateľov tak, že sledovali anonymné platby v kryptomenách na podozrivej webovej stránke.

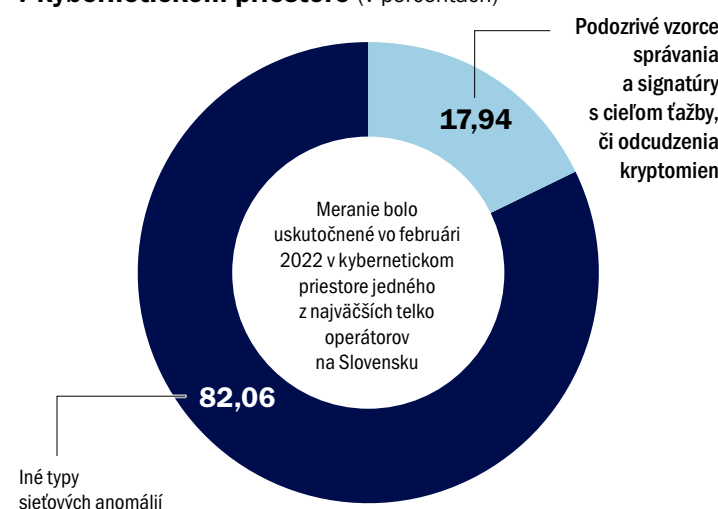
Jarek Jakubček pracuje ako riaditeľ vyšetrovacej sekcie v spoločnosti Binance a na otázku, či môže byť platba kryptomenami dokonalo anonymná, odpovedá stručne: „Nie.“ Transakcie zanechávajú stopy.

Lahko ukradnúť, ťažko prať

V Európe spravoval Jarek Jakubček komunitu viac ako dva a pol tisíce policajných vyšetrovateľov zameraných na kryptomeny. O podrobnostiach nemôže hovoriť, ale – ak by neboli výsledky, neboli by na vyšetrovanie vynakladané podobné prostriedky.

„Úspech vyšetrovania závisí od komplexnosti prípadu, sofis-

Takmer 90-tisíc identifikovaných anomálií v kybernetickom priestore (v percentách)



tikovosti páchatela, schopností vyšetrovateľa a času, ktorý môže prípadu venovať, sledovacích nástrojov, ktoré má k dispozícii, a od efektívnej spolupráce s kryptozmenárňami.“

Takto sa podarilo vypátrať množstvo páchatelov zodpovedných za šírenie ransomvéru či detskej pornografie, aktivity na dark webe, kybernetické útoky, krádeže kryptomien a investičné podvody.

Svetlo aj tma

Čo sa týka pracovného trhu, v celej IT sfére existujú špecia-

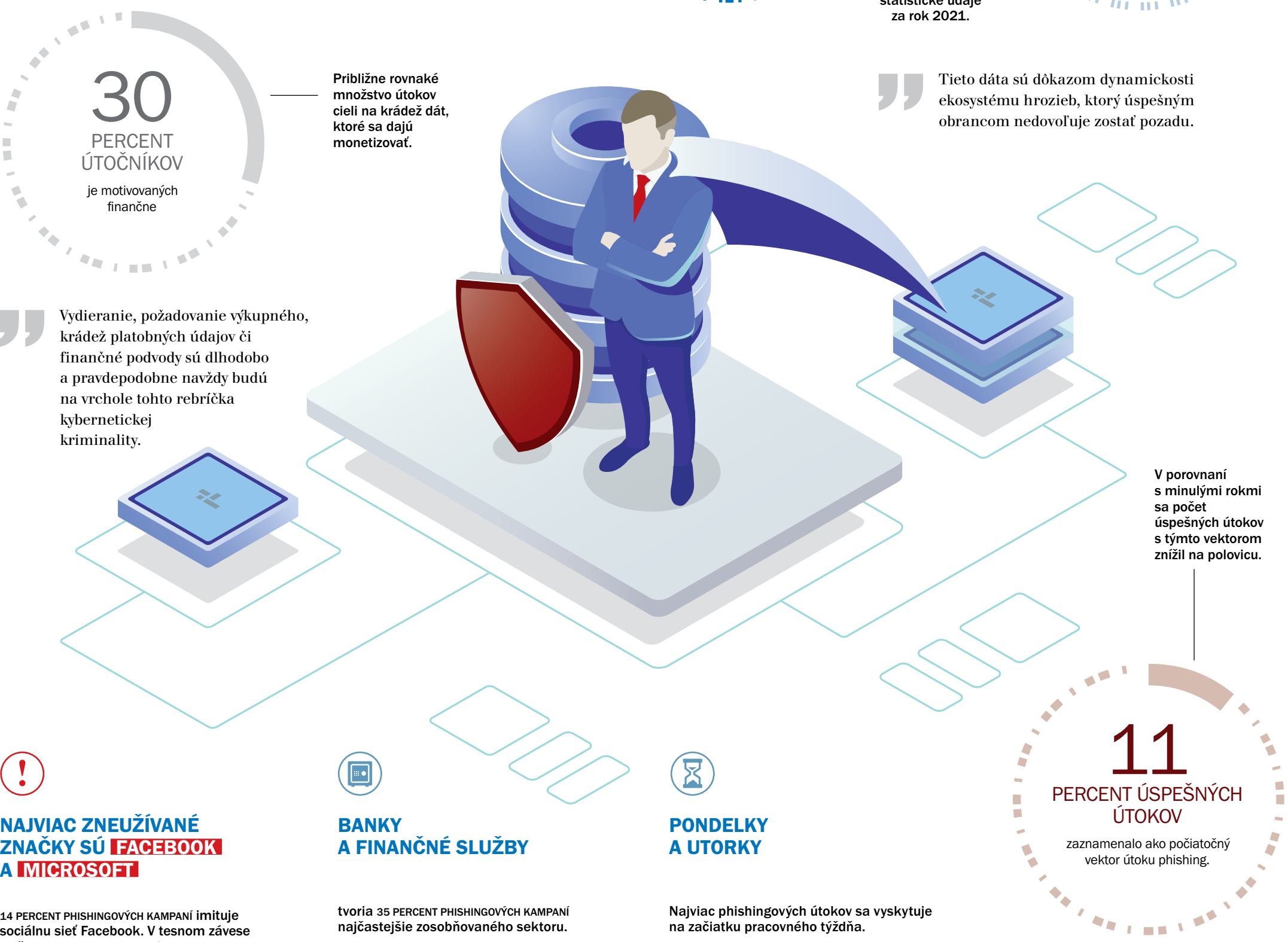
lizácie na kryptomeny a blockchain, napríklad administrátor platobnej brány, správca kľúčov, kryptograf alebo obchodník vo finančnom manažmente. Zároveň kryptomeny prinášajú aj nové príležitosti – právnici, účtovníci, správcovia, vývojári a najmä bezpečnostní analytici.

Ďalší priestor pre virtuálne meny v našom svete vytvorili aj pandémie či vojnový konflikt. Juraj Bednár vystihuje ich svetlé aj tienisté strany: „Pri kryptomenách sa vás nikto na nič nepýta. To je výhoda aj nevýhoda.“

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Hovorí sa tomu helikoptérový pohľad

Alebo aktuálne fakty kyberbezpečnosti



Tieto služby sú z hľadiska počtu používateľov lídrami vo svojom odvetví. Útočníci majú istotu, že kampaniou zasiahnu vysoký počet potenciálnych obetí.

Urgentne znejúce správy od finančných inštitúcií v ľuďoch vzbudzujú strach o vlastné úspory. Krádež platobných údajov pre útočníkov zároveň predstavuje najpriamejšiu cestu k profitu.

Ľudia sú po víkende zavalení e-mailami a phishingový pokus im tak ľahšie preklízne „pomedzi prsty“. Navyše, žiadosť o opätovné prihlásenie do služby môže po pracovnej odmlke pôsobiť legitímne.

Základom je efektívne nastavenie pravidiel detekcie a blokovania škodlivých e-mailov v kombinácii s uvedomelými a vyškolenými používateľmi

Zdroj: Mandiant M-Trends 2022, Vader Phisher's Favorites: Year 2021 in Review
Komentár: Daniel Suchý, bezpečnostný špecialista, Aliter Technologies

KOMENTÁR

Digitálne platformy: kde nám pomáhajú a kde nás ohrozujú?

Digitálne platformy sú už desiatky rokov neoddeliteľnou, ba až prirodzenou súčasťou našich životov. Niektoré sú jednoznačne pozitívne, ako napríklad online navigačné systémy, a iné služby zamerané na zvyšovanie kvality života. Iné sa stali predmetom odborných debát, kde miera ich negatívnych externalít predstavuje pre jednotlivcov a spoločnosť čoraz väčšie riziká.

Asi najznámejšou negatívne vnímanou službou je produkt Facebook od spoločnosti Meta. Čoraz viac odborníkov upozorňuje, že Facebook roky realizuje dizajnové rozhodnutia, pre ktoré je miestom, kde sa spoločnosť skôr oslabuje. Používatelia siete sú vystavení čoraz silnejšiemu vplyvu rôznych toxických javov, ako sú nenávistné prejavy alebo dezinformácie.

Práve pre ne je dnes Meta vnímaná ako disruptívna technologická firma, ktorá značne narušila vývoj spoločnosti a negatívne zasahuje rôzne oblasti od politiky cez bezpečnosť až po psychické zdravie.

Facebook totiž v snahe maximalizovať zisk potrebuje, aby na jeho platforme trávilo čo najviac osôb čo najviac času. Táto metrika je dosahovaná tým, že publiku sú zobrazované obsahy, ktoré majú schopnosť vyvolať rôzne negatívne emócie. Tento biznis model má v sebe negatívne externality, ktoré postupne zaťažujú a menia spoločnosť po celom svete vrátane Slovenska.

Facebook je na Slovensku najpoužívanejšou informačnou technológiou, keďže má takmer tri milióny používateľov. Viac ako polovica z nich tvrdí, že informácie o svete získava primárne z tejto platformy. Facebook sa tak stáva na Slovensku zároveň najsilnejším médiom.

Preto je pre jednotlivcov a spoločnosť mimoriadne nebezpečné, že v nastavení algoritmov umožňuje Facebook násobne posilňovať manipulatívne zdroje na úkor tých, ktoré si ctia základné parametre slušnej a faktickej diskusie.

Pre mnohých sa tak realita prekrútila na nepoznanie. Ako to pomenoval Tristan Harris - mnohých zviadli algoritmy duopolov po krivej ploche priamo do „mestečka šialenstva“. Teda ku krivému obrazu reality, ktorý ľuďom servíruje nepravdy, dezinformácie, nepokoj, nedôveru, strach a chaos.

Výsledkom je iný svet. Demoralizovaná, vystrašená a nahnevaná spoločnosť.

To všetko hlučne, za bieleho dňa, v plnej sile najviac exponovaných digitálnych účtov malej skupiny mimoriadne angažovaných politických síl. Osemdesiat percent interakcií proruskej propagandy na Slovensku totiž produkujú štyri skupiny aktérov.

Nedeje sa to pritom prvýkrát. Presne tak, len za pomoci iných nástrojov, postupovali extrémisti naprieč 20. storočím. Vplyv propagandy a hybridných hrozieb pociťujeme na Slovensku aj v kontexte vojenskej agresie Ruska proti Ukrajine. Všetci sledujeme, ako rôzni extrémisti realizujú novú ofenzívu proti demokracii a jej hodnotám.

A ak mnohí zľahčovali varovania bezpečnostných komunití doteraz, vojna u nášho východného suseda je možno posledným buditelom k budovaniu odolnosti proti informačným hrozbám. Nabudúce môže byť na prebudenie už naozaj neskoro.

Tomáš Kriššák
odborník na informačnú bezpečnosť
Gerulata Technologies

Prémiová liga sa začína touto otázkou

ANKETA

Akú otázku dávate potenciálnym kolegom, keď sa uchádzajú o prácu v kybernetickej bezpečnosti?



Tomáš Zaťko, CEO, etický hacker
Citadelo

Hľadáme hackera. Životopis nahrajte na naše interné firemné úložisko. Tento starý vtip sme sa u nás rozhodli realizovať. Kandidáti na pozíciu etického hackera sa preto musia najskôr prehacovať cez niekoľko úrovní systémů, ktorý sme pre nich pripravili. Otázky im kladieme až potom, keď sa im to podarí.



Daniel Chromek, riaditeľ informačnej bezpečnosti
ESET

Čo zaujímavé ste čítali alebo ste sa naučili v oblasti kybernetickej bezpečnosti? Snažíme sa totiž vyhľadávať skôr kandidátov, ktorí sa zaujímajú o oblasť bezpečnosti a chcú sa vzdelávať a rásť. Je ťažké nájsť na trhu kandidáta, ktorý presne sadne na naše požiadavky. Avšak hard skills sa dajú získať, ak má človek chuť rásť. Naopak, ak sa vzdelávať nechce, tak skôr či neskôr stratí prehľad.



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

Ono to nie je nikdy jedna otázka. Pracovať v štátnej sfére nie je pre každého, aj keď kybernetická bezpečnosť je veľmi zaujímavá a fascinujúca. Preto by som sa pýtal zloženou otázkou. Prečo vôbec chcete robiť v štátnej správe kybernetickú bezpečnosť a kam to chcete v oblasti kyberbezpečnosti dotiahnuť?



Marián Klačo, vedúci oddelenia bezpečnosti informácií
Volkswagen Slovakia

Ako v každom odbore, aj pre prácu v kybernetickej bezpečnosti je dôležitý zápal pre vec. Ak chce človek niečo robiť poriadne, mal by mať na to vnútornú motiváciu. Preto sa vždy pýtam: Čo vás na kybernetickej bezpečnosti priťahuje? Kde sa v rôznych témach vidíte? Čo vás motivuje „ponoriť

sa“ hlbšie do jednej z najdynamickejších oblastí IT/OT sveta?



Ján Grujbár, generálny riaditeľ
Aliter Technologies

Budem najradšej, keď sa to potenciálni kolegovia dozvedia na pohovore u nás na vlastnej koži. Keďže každá oblasť má svoje špecifiká, neexistuje žiadna „zlatá“ otázka. Môžem však prezradiť, že určite budeme zvedaví, čo považujú za cieľ programu informačnej bezpečnosti v organizácii a akú majú motiváciu pracovať u nás. Považujeme totiž za dôležité, aby naši bezpečiaci vnímali svoju úlohu aktívne a kontextuálne.



Kateřina Turzová, vedúca oddelenia informačnej bezpečnosti a riadenia rizík
TIPOS

Stabilnou súčasťou každého pohovoru je otázka, ako využiť outsourcing na plnenie úloh informačnej bezpečnosti. Zaujima ma subjektívny pohľad uchádzača na moderný trend outsourcingu v kybernetickej bezpečnosti. Som zvedavá, aký má názor na úkony, ktoré môžu vykonávať tretie strany bez obmedzenia alebo ohrozenia prevádzky a ktoré, naopak, je potrebné ponechať v jednoznačnej zodpovednosti vlastníka procesu.



Tibor Paulen, manažér informačnej bezpečnosti
Stredoslovenská distribučná

Pravdupovediac, nič výnimočne zaujímavé sa ich nepýtam, len také bežné veci. Ako trávite voľný čas? Dokážete oddychovať a vyčistiť si hlavu?



Juraj Koník, bezpečnostný manažér
Allianz – Slovenská poisťovňa

Ak by ste mali neobmedzené možnosti, čo by ste zabezpečili ako prvé v oblasti kybernetickej bezpečnosti v našej spoločnosti? Kam/Do akej oblasti by ste investovali svoj pracovný čas a finančné prostriedky našej spoločnosti, aby mali čo naje-

pektívnejšie využitie a zaistili maximalizáciu ochrany našich dát a IT aktív?



Ivan Kopáčik, bezpečnostný expert
Gordias

Najčastejšia otázka je: Kedy sa vieme stretnúť a porozprávať sa oca hodinku? Kybernetická bezpečnosť z pozície konzultanta je nesmierne široká a komplexná problematika. Dlhší úvodný rozhovor pokladám za dôležitý z pohľadu zamestnávateľa i potenciálneho zamestnanca. Bez neho nie je možné identifikovať očakávania strán ani reálnu kvalifikáciu zamestnanca.



Andrej Žucha, generálny riaditeľ
ALISON Slovakia

Pýtam sa budúcich kolegov, čo najhoršie sa im v profesijnom živote stalo. V kybernetickej bezpečnosti sú úspechy a výkon vynikajúco odmeňované, ale musíte si ich zaslúžiť. Nesmieme sa vzdávať a bojovať treba každý deň a o každú minútu.



Diana Legdanová, vedúca úseku bezpečnosti
Východoslovenská energetika Holding

Na aký svoj úspech ste hrdý a prečo? Čo bola pre vás najväčšia osobná výzva a prečo? Akú najbližšiu metú máte v pláne dosiahnuť a prečo? Touto magickou trojkou sa dozviem všetko, aby som vedela, či to bude fungovať. V čom je človek dobrý, ako ďaleko za svoju komfortnú zónu je ochotný ísť a či vie, čo chce. A jednu orientačnú na záver: O akej kybernetike ste čítali naposledy?



Vladimír Jančok, vedúci oddelenia informačná bezpečnosť
VÚB

Okrem technických otázok, ktoré sú viac profilované pre konkrétnu pozíciu, sa často pýtame na incident manažment. Preferujeme interaktívnu formu, kde predstavíme určitý typ útoku a kandidát sa snaží načrtnúť, ako by danú situáciu riešil. Podľa odpovede môžeme pokračovať v simulovanom priebehu incidentu a pýtať sa viac detailov. S tým trochu súvisia aj otázky ohľadom samostatného riešenia problémov.



Alexandra Dorčáková, vedúca prevádzky bezpečnosti sietí
DT IT Solutions Slovakia

Na pohovor prizývam aj kolegov z tímu, ktorí overujú veľmi dôležité technické predispozície. Okrem toho preverujeme aj analytické uvažovanie, pochopenie abstraktu aj komunikáciu s klientom na úrovni. Je dôležité, aby klienti mali pocit bezpečia a profesionality, keďže nám zverujú dáta. Na úvod sa niekedy pýtame aj otázku, koľko pingpongových loptičiek sa vojde do autobusu.



Pavel Nechala, partner
Advokátska kancelária WISE3

Mám obľúbenú otázku: Čo vnímate ako opačnú stranu digitalizácie? Oblasť, bez ktorej nie je možné rozvíjať elektronické služby, navrhovať inovatívne riešenia a zlepšovať napríklad aj zdravotníctvo alebo školstvo. Lebo ako znie notoricky známy výrok Ursuly von der Leyenovej, predsedníčky Európskej komisie, kybernetická bezpečnosť je odvrátenou stranou digitalizácie.



Roman Varga, manažér kyberbezpečnosti
Dôvera, zdravotná poisťovňa

V týchto dňoch sme úspešne ukončili výber security architektov. Zapadne do IT orchestra, ktorý u nás budujeme? Bude úspešný kybernetický dirigent? Bude jeho hlava tvrdohlavá a presadí tie najlepšie bezpečnostné riešenia? Nestratí sa jeho nadšenie v spleti náročných úloh? Keď sa ma niekto o pár rokov opýta, prečo sme sa preňho rozhodli, tak azda neskromne ukážem na dielo, pod ktorým budeme hrdo podpísaní.



Ján Andraško, manažér strediska bezpečnostných operácií
Binary Confidence

Aby obrancovia vedeli dobre brániť, musia rozmyšľať ako útočníci a vedieť, ako útoky prebiehajú. Preto sa na pohovoroch budúcich SOC analytikov pýtam, ako by postupovali oni, ak by mali za úlohu hacknúť mňa ako osobu alebo našu firmu. A, samozrejme, hneď sa aj pýtam, ako by sa ich aktivity dali detegovať a aké preventívne opatrenia prijať.



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

Odhladnuc od technických znalostí, medzi zručnosťami, ktoré sa snažíme nájsť u potenciálnych kolegov, patria schopnosť stručne, jasne a zrozumiteľne komunikovať komplikované témy, umenie spolupracovať s rôznymi tímami mimo IT, zhostiť sa roly diablovho advokáta a predvídať, čo môže zle „vypáliť“, dokázať nájsť ihlu v kope sena a sústreďiť sa na udalosti s potenciálne najväčším dosahom. A k tomu ochota neustále sa prispôbovať a celý život sa vzdelávať.



Michal Ďorda, certifikovaný audítor kybernetickej bezpečnosti
auditori.it

Akú super schopnosť by si chcel mať ako konzultant bezpečnosti? Ide o psychologicky položenú otázku, pri ktorej sa kandidátovi otvorí okno do sveta fantázie. Odpoveď môže byť od bláznivej až po racionálnu. Vy si však vytvoríte obraz o vnímaní problematiky a skúsenostiach získaných z bežného života kandidáta sediaceho na stoličke oproti vám. Každý z nás mal v detstve sen stať sa superhrdinom.



Miroslav Ilavský, data manažér kybernetickej bezpečnosti
i-Secure

Základná je motivácia uchádzača chcieť sa vzdelávať a prijímať nové poznatky, spoznávať nové technológie, nové hrozby, stále rásť v tejto oblasti. Otázka teda znie: Chcete sa seriózne venovať kybernetickej bezpečnosti? Ak áno, urobte si kurz, získajte certifikáty, sledujte aktuálne hrozby a skúšajte nové technológie a postupy na ochranu proti nim.



Richard Kiškováč, generálny riaditeľ
IstroSec

Vybrať správneho kolegu nie je jednoduchá záležitosť. Z manažérskeho hľadiska je dôležité poznať svoj tím, expertízu, ktorá je k dispozícii, ale hlavne tú, ktorá chýba. Podľa toho je možné zvoliť správne otázky. Moje prvé otázky smerujú väčšinou k motivácii. Od nej sa potom odvíjajú ďalšie, zamerané na odbornú úroveň alebo osobnostné

črty. Komunikáciu považujem aj v bezpečnosti za kľúčovú z hľadiska vedenia ľudí, aj napriek tomu, že u technických špecialistov to nebýva ich najsilnejšia stránka.



Tomáš Hettych, viceprezident
ISACA

Nových budúcich kolegov si väčšinou vytypujem vopred, alebo sú k nám odporučení a dávam im väčšinou viacero otázok: Viete si predstaviť prácu v štátnej odbornej organizácii? Bude vám vyhovovať flexibilný pracovný čas a home office? Preferujete projektový prístup založený na výsledkoch alebo na strávenom čase? Ako často sa vzdelávate a v akej oblasti?



Stanislav Smolár, manažér oddelenia bezpečnosti
Soitron

Snažíme sa zistiť, s akými technológiami má kandidát skúsenosti, ale vždy sa pýtame potenciálnych kolegov aj na to, ako majú zabezpečenú svoju domácu sieť a osobné účty. Bezpečnosť sa nekončí v práci a to, ako rozmyšľajú o svojej osobnej bezpečnosti, dáva dobrý náhľad na celkové povedomie problematiky.



Ján Adamovský, riaditeľ bezpečnosti
Slovenská sporiteľňa

Kybernetická bezpečnosť je tímová hra. Obdobne ako v kolektívnom športe vyžaduje obsadiť rôzne posty tými správnymi hráčmi. Otázky preto smerujú k tomu, aká časť kybernetickej bezpečnosti daného kandidáta naplňa a ako vie hrať za tím. Nehľadáme superhrdinov, ktorí vedia všetko. Hľadáme tímových hráčov, ktorí vynikajúco zastanú svoje miesto, prihrávajú kolegov, a keď si to situácia vyžaduje, neboja sa zahrať aj na inom poste.



Marián Trizuliak, architekt kybernetickej bezpečnosti
Západoslovenská distribučná

V mojej pozícii nerobím pohovory. Ale ak by som niekoho vyberal, určite by som vynechal klasické otázky - kde sa vidíte o päť rokov, prečo práve naša spoločnosť. Chcel by som vedieť odpoveď na základnú otázku vesmíru a života. Podľa presnosti odpovede by som sa rozhodol ako pokračovať v rozhovore.