HN
obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
30. JÚNA 2023 – 2. JÚLA 2023

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Malé a stredné firmy to nemajú ľahké

TÉMA

Dali ste si niekedy otázku, prečo by ste sa mali zaoberať vo firme kyberbezpečnosťou? Obávate sa pokút, finančných škôd alebo straty dobrého mena? Alebo všetkého? Alebo ničoho?

Množstvo povinností, ale aj neznalosť, naivita a pohodlnosť. Kritický stav kyberodolnosti vo firmách má veľa dôvodov. FOTO: DREAMSTIME

Jedným z najčastejších útokov na malé a stredné firmy je v súčasnosti ransomvér. A aj reálnou hrozbou na Slovensku. Príbehy Telekomu, Nitrianskej nemocnice, Malaciek, košického VÚC, Datalanu, Mäspomy, Štátnych lesov, kúpeľov Dudince, výrobcu nábytku na strednom Slovensku či aktuálne Univerzity Mateja Bela poznáte? Už sú dostatočne známe, aby si ohrozenie uvedomili aj slovenské firmy. A primerane sa obávajú.

Cena za naivitu

Pri ransomvérových útokoch útočníci väčšinou prispôsobujú výšku výkupného primerane tržbám spoločnosti, ktoré sú verejne dostupné. „Výška je zvyčajne volená tak, aby si ju firma mohla dovoliť zaplatiť a nebola zároveň likvidačná," vysvetľuje Jozef Bálint z Alison Slovakia.

Vtedy firmy robia najväčšiu chybu, že sa k incidentu nepriznajú. Ak aj zaplatia, dáta im vrátia poškodené alebo si útočníci nechajú „zadné vrátka" v sieti. A navyše prispievajú k falošnému pocitu bezpečia.

Počítajme však ďalej. Cena za odstránenie bezpečnostného incidentu sa často stanovuje podľa jeho rozsahu a veľkosti napadnutej infraštruktúry. O sumách nechcú hovoriť napadnuté organizácie ani dodávatelia, ale už aj v prípade menšieho incidentu si treba priplatiť aspoň desaťtisíc eur.

Bojíte sa incidentu?

Dobre sa obávate, ale máme pre vás ešte horšiu správu. Kyberbezpečnosť sa najčastejšie zrúti na ľudských chybách. Ešte zrozumiteľnejšie? Zamestnanci kliknú na phishingový mail, posťahujú súbory kade-tade, používajú rovnaké heslá a nemenia si ich. Útoky zvonka sú postavené na neznalosti používateľov.

Ak necháme zvyšovanie bezpečnostného povedomia dlhodobo stagnovať, následkom je, že zostaneme jednými z najzraniteľnejších. Takže automaticky budeme atraktívnejším cieľom. Najmä ak ostatné okolie s touto témou účinne pracuje. „Pamätajte si, že útočníci vždy hľadajú najľahšiu cestu," varuje bezpečnostný konzultant Richard Kiškováč.

Bariéra je mega

Paradoxom je, že vieme, kde je problém. Malé a stredné podniky si uvedomujú, že najväčšou bariérou pri zvyšovaní úrovne kyberbezpečnosti je nedostatok digitálnych zručností zamestnancov. V aktuálnom prieskume agentúry AKO o tom hovorili štatutári či zodpovední zamestnanci.

Podľa odpovedí však školia zamestnancov v kyberbezpečnosti iba v štyroch prípadoch z desiatich. A aj to iba „podľa potreby a iba pre vybraných zamestnancov".

Nie sú ani tam, ani tam

Obdobnú skúsenosť má aj Kompetenčné a certifikačné centrum kybernetickej bezpečnosti. Čo sa týka vzdelávania zamestnancov, tak záujem „emespečiek" je opäť na bode mrazu.

Miroslav Havelka počíta, koľko manažérov kyberbezpečnosti vyškolili za tri roky pre malé a stredné firmy, a vychádza mu, že – dvoch. Do kurzov posielajú účastníkov veľké organizácie a štátna správa, alebo, naopak – mikropodniky, ktoré dodávajú kyberbezpečnostné služby.

Povedzme si pravdu

Bezpečnosť je pre firmy veľmi abstraktný a technicky pojem, preto sa často uspokoja so svojím „ajťákom", ktorý primárne opravuje tlačiarne a WiFi.

Karol Suchánek, vedúci oddelenia bezpečnosti a ochrany osobných údajov z Websupportu, má ďalší príklad: „Keď

> Ak sú ľudia súčasťou problému, musia byť aj súčasťou riešenia.
>
> **Richard Kiškováč,** kyberbezpečnostný lektor Elkan

ide o desaťtisíc eur, bojím sa, že marketing získa prednosť, lebo sa očakáva zvýšenie predaja či návštevnosti webových stránok. Investícia do bezpečnosti však nie je na prvý pohľad zrejmá."

Dodávateľská idyla

Chybou malých a stredných podnikov je spoliehať sa, že návrhy riešenia v prípade riadenia kybernetických rizík „prídu" z externého prostredia.

Ešte horšou správou je, že implementácii opatrení sa začnú venovať až po negatívnej skúsenosti s incidentom. Zanedbávajú výsledky analýzy rizík a odporúčania auditu kybernetickej bezpečnosti alebo sa na ne nedostatočne spoliehajú.

Čo na to zákon

Kyberbezpečnostný profesionál Roman Čupka hovorí o tom, že väčšina firiem nevníma ešte kybernetickú tému ako ťažiskovú pre budúce fungovanie či stabilitu podnikania. A regulácie a legislatívne požiadavky? „Tie berú podniky len ako zaťaženie svojej agendy s už aj tak poddimenzovanými zdrojmi."

Úprava zákona o kyberbezpečnosti sa však blíži a mnohé podniky čaká zmena. Budú musieť reflektovať požiadavky na zvýšenie bezpečnosti, aby predišli aj potenciálnym sankciám.

Ukážte pochopenie

Iba máloktorý štatutár si dostatočne uvedomuje životne dôležité prepojenie technológií s biznisom. Niet sa však čomu čudovať, pretože ich primárnym cieľom je vytvárať zisk v silne konkurenčnom prostredí.

„Myslím, že to nie je primárne nezáujem, ale skôr nevedomosť," hovorí Richard Kiškováč. A nevedomosť čiastočne vyplýva aj z nedostatku odborníkov, ktorí dokážu efektívne túto tému tlmočiť či riešiť. Preto aj Roman Čupka uznáva, že aj bezpečáci musia v prvom rade pochopiť, ako táto ťažisková a chrbticová časť národnej ekonomiky funguje a ako im problematiku prezentovať. Zodpovednosť v digitálnom priestore by mala byť na rovnakej úrovni ako klasické BOZP. To poznáme všetci.

Urobte krok vpred

Keď je podpora manažmentu, ktorý berie bezpečnosť ako prioritu, je aj ochota do nej investovať. Potom to ide už naozaj ľahko a dá sa začať aj s menším rozpočtom. Väčšie firmy zvyčajne majú pozície, kde sa následne riadi bezpečnosť, menšie si to môžu outsourcovať.

Vo Websupporte hovoria, že ak je niekto lídrom na trhu, musí byť príkladom. Svoju bezpečnosť majú poskladanú z viacerých vrstiev, podobne ako cibuľa. Pomyselnými vrstvami sú rôzne technické prostriedky, neustále vzdelávanie zamestnancov a klientov, ako aj nezávislé bezpečnostné testy a audity.

„Čím viac vrstiev je medzi nami a útočníkmi, tým viac sme v bezpečí my, naše systémy aj naši klienti," prízvukuje Karol Suchánek.

Ako z toho von

Ak sú ľudia súčasťou problému, musia byť aj súčasťou riešenia. Technológie sú aj napriek skvelému marketingu dobré, ale nie sú všemocné.

Po rokoch skúseností vo vzdelávaní už Richard Kiškováč vie, že z každého používateľa nemôže byť špecialista na kyberbezpečnosť. „Na začiatok však úplne postačuje, keď dokážeme vyvolať takú zmenu v správaní, že sa človek zamyslí pred tým, ako vykoná nejakú akciu."

Príčiny incidentov podľa zdroja

Zdroj: Ponemon Institute LLC: The Cost of a Data Breach Report

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
auditori.it
CHECK POINT
eset
Progress
SOITRON
SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 30. JÚNA – 2. JÚLA 2023

Záblesky eufórie i trpké sklamania

ANKETA

Kyberbezpečnostná komunita hodnotí prvý polrok 2023 na Slovensku. Hovoria o tom, čo považujú za pozoruhodnú udalosť alebo jav v kyberbezpečnosti, čo ich potešilo alebo sklamalo. A, samozrejme, o tom, ako to ovplyvní život nás všetkých.

Tomáš Valenta
riaditeľ
Check Point Software Technologies na Slovensku

CyberGame. Raz sa o tom bude hovoriť ako o míľniku pre slovenskú kyberbezpečnosť. Ak udržia autori a organizátori úroveň, vznikne na Slovensku vzácny precedens.

Ivan Makatura
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Malý krok pre legislatívu, veľký krok pre kyberbezpečnosť. Celý polrok sa pripravovala vyhláška, ktorou sa vykonáva zákon o znalcoch, tlmočníkoch a prekladateľoch. Novelou vzniká znalecké odvetvie kybernetická bezpečnosť. Pomôže to zvýšiť kapacity znaleckých činností, rozšíri možnosti orgánov činných v trestnom konaní vo vyšetrovaní počítačovej kriminality, umožní efektívnejšie vykonávať znalecké posudky v ochrane údajov, posudzovaní bezpečnostných opatrení alebo hodnotení zraniteľností.

Andrej Aleksiev
partner a CTO
Kreston

Teší ma, že povedomie o bezpečnosti neustále rastie. Vďaka dobre napísanému zákonu o kybernetickej bezpečnosti a aktívnej práci nielen NBÚ sa „cybersecurity“ dostáva čoraz viac do popredia priorít každej organizácie. Na strane druhej ma udivuje pokračujúci nezáujem riadiacich orgánov štátu. Ich nevôľa investovať do digitálnej ochrany bude mať v budúcnosti zásadný vplyv na rozvoj našej krajiny.

Jakub Berthoty
advokát
Dagital Legal

Facebook (Meta) dostal v Írsku pokutu 1,2 miliardy eur za porušenie GDPR z dôvodu nedostatočného šifrovania prenosov dát do USA. Pozitívne na tom je, že musí dôjsť k zmene k lepšiemu a musíme brať cezhraničné prenosy a preverenia dodávateľov vážne.

Andrej Žucha
generálny riaditeľ
ALISON Slovakia

Potešilo aj zarmútilo súčasne. Dosah ransomvéru na Slovensku. Potešenie vyplýva z nečakanej osvety a prináša nádej, že sa poučia tí, ktorých to ešte netrafilo, a začnú sa konečne venovať kyberbezpečnosti. Je mi ľúto tých, ktorí sa teraz trápia s tým, ako ochrániť nevinné obete útoku pred únikom údajov. Každý kyberincident predstavuje veľké finančné aj personálne náklady a naštrbenie dôvery.

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

Smutným konštatovaním je stále rastúci počet kybernetických incidentov, čo sa týka ochrany osobných údajov. Som sklamaný, že štát stále nevenuje dostatočnú pozornosť vyškoľovaniu v oblasti kyberbezpečnosti zamestnancov verejnej správy ani osvete formou kampaní v plošných médiách pre menej zručnejších používateľov.

Tomáš Zaťko
CEO, etický hacker
Citadelo

Rapídny vývoj v oblasti umelej inteligencie. Jedných potešil, druhých sklamal, tretí sa ho hrozia. Väčšina ho v praxi ignoruje. A pritom ide o jednu z najzásadnejších zmien – technologických a spoločenských zároveň, aké vo svojich životoch zažijeme.

Pavol Sokol
vedúci CSIRT-UPJS
Univerzita Pavla Jozefa Šafárika v Košiciach

Kybernetickú komunitu potešila úspešnosť inštitúcií zo Slovenska vo výzve Digitálna Európa. Evidujeme až osem úspešných projektov zameraných na informačnú a kybernetickú bezpečnosť so slovenskou stopou. To jednoznačne pomôže v odbornom raste našej kybernetickej komunity, ako aj v rozvoji európskej spolupráce v tejto oblasti.

Marek Zeman
vedúci oddelenia bezpečnosti informačných systémov
Tatra banka

Potešilo ma, že sa Európska únia zaoberá bezpečnosťou umelej inteligencie a kryptomien. Špeciálne ma prekvapilo zameranie na etiku a vysvetľovanie funkcionalít technológií. Sklamalo ma, že z reakcie to vyzerá, že sa veľmi bojíme oboch nových typov technológií. A neprekáža nám zaškrtiť časť trhu, aj za cenu fiktívneho pocitu bezpečnosti, keďže iné krajiny takéto škrupule nemajú.

Tomáš Hettych
viceprezident
ISACA

Slovenskú kybernetickú komunitu určite potešilo, že v jarnej výzve EÚ programu Digitálna Európa uspelo až osem slovenských projektov. Čo len potvrdzuje, že Slovensko je jedným z najúspešnejších hráčov v EÚ v tejto oblasti. K tejto pozitívnej bilancii určite prispeli aj aktivity KCCKB, ktoré výzvy aktívne promovalo a ponúkalo potenciálnym žiadateľom pomoc s prípravou dokumentov na podanie projektov.

Peter Dufek
manažér kybernetickej bezpečnosti
ProCare a Svet zdravia

Bezpečnosť sa stáva celoeurópskou spoločenskou zodpovednosťou, preto aspoň za seba by som uviedol potešujúcu informáciu, že eurokomisia navrhla Akt o kybernetickej solidarite, ktorého cieľom bude posilniť solidaritu v spoločnom krízovom riadení vo všetkých členských štátoch, a zároveň predstavila Akadémiu kybernetických zručností na zaručenie koordinovanejšej koncepcie pokrytia nedostatku talentov v kybernetickej oblasti.

Ivan Kopáčik
bezpečnostný expert
Gordias

Veľmi ma potešilo, že po mnohých rokoch kyberbezpečnostná komunita dostáva pozornosť a podporu, akú si zaslúži. V Európskej únii sa vytvára spoločná európska komunita pre kompetencie v kybernetickej bezpečnosti, ktorej členmi sa môžu stať entity zo všetkých členských štátov. Národné koordinačné centrum SR sa úlohy koordinátora v SR zhostilo s veľkým entuziazmom a kyberkomunita sa určite má na čo tešiť!

Diana Legdanová
vedúca úseku bezpečnosti
Východoslovenská energetika Holding

Úprimne ma potešilo, že sa opäť našli dobrí ľudia, ktorí priniesli na svet druhý ročník CyberGame – od partnerov cez „výrobný štáb“, odborných garantov až po promotérov. Lebo to nie je „len hra“, je to investícia do našej kyberbezpečnostnej komunity – ďakujeme. Vyše 2 300 účastníkov prejavilo vášeň, nadšenie, vytrvalosť, záujem vzdelávať sa v tejto zložitej téme – to je viac ako 2 300 unikátnych zážitkov, ktoré prispejú k rozvoju kultúry kyberbezpečnosti na Slovensku.

Roman Čupka
hlavný konzultant
Progress a CEO Synapsa Networks

Počas Qubit konferencie v Prahe v máji som mal možnosť spoznať sa a pohovoriť si s veľkým množstvom mladých ľudí, ktorí rozširujú kyberbezpečnostnú komunitu na Slovensku. A som úprimne rád, pretože problematikou začína žiť širšie spektrum mladších ročníkov a nie je to len o nás, digitálnych dinosauroch. Pokiaľ sa budeme všetci vzájomne inšpirovať a pomáhať si, myslím si, že sa dá využiť potenciál tejto komunity správnym smerom.

Roman Varga
manažér kyberbezpečnosti
Dôvera, zdravotná poisťovňa

V ostatnom období pribúda obetí kyberpodvodov. A to aj napriek mierne rastúcemu povedomiu o hrozbách a novým technológiám na ochranu používateľov. Kde robíme chybu my odborníci? Sú fakt útočníci takí dobrí, alebo sú používatelia proste naivní, nepoučiteľní či nepozorní? Mal by poskytnúť štát kapacity a technické vybavenie na ochranu pred útočníkmi v štádiu pokusu? Na túto otázku hľadám partnerov na riešenie už celý polrok.

Július Selecký
senior technický špecialista
ESET

Som prekvapený, že aj keď je smernica NIS2 témou každej IT konferencie posledného polroka, stále nie je u nás k dispozícii na nahliadnutie aspoň prvotný návrh legislatívnych zmien. Ide o dôležitú legislatívu, ktorá má priamy dosah na bezpečnosť krajiny či občanov. Na porovnanie s ČR, NÚKIB už odoslal návrh nového zákona o kybernetickej bezpečnosti do medzirezortného pripomienkového konania.

Ján Grujbár
generálny riaditeľ
Aliter Technologies

Naše skúsenosti v prvej polovici roku 2023 sú, bohužiaľ, prevažne negatívne. Z posledných konferencií a workshopov nám vyplýva, že kým vládne organizácie – niektoré – vedia, že majú nedostatočnú ochranu proti kybernetickým útokom a snažia sa túto situáciu riešiť – rýchlosť a úspešnosť teraz bokom, tak napríklad prevádzkové technológie či malé a stredné podniky ešte ani len netušia, ako zle sú na tom z hľadiska kybernetickej bezpečnosti.

Filip Pásztor
bezpečnostný konzultant
auditori.it

Sprístupnenie nástrojov umelej inteligencie zjednodušilo podvodníkom a hackerom prácu. Zároveň široká ani odborná verejnosť si často nie sú vedomé možností umelej inteligencie, a dokonca desať percent našich spoluobčanov ani netuší, že existuje. Namiesto toho, aby sme reagovali na nové trendy a vývoj, kyberkomunita u nás bojuje s veternými mlynmi a snaží sa vysvetliť, že kybernetická bezpečnosť je vôbec potrebná.

Matej Síleš
manažér IT bezpečnosti
UPC BROADBAND SLOVAKIA

Mňa osobne teší, že sa kyberbezpečnosti začala venovať zvýšená pozornosť, a to najmä v mediálnom priestore, a zároveň vznikajú aktivity na školách všetkých stupňov, ktorých cieľom je výchova k bezpečnému používaniu digitálnych technológií. Tento jav je veľmi nápomocný pri budovaní bezpečnostného povedomia širokej verejnosti, čo je v časoch, keď veľa citlivých procesov a transakcií prebieha v online priestore, kľúčové.

Miroslav Chlipala
partner
Advokátska kancelária Bukovinský & Chlipala

Pozoruhodnou udalosťou je revolučný vstup systémov umelej inteligencie do každodenného života. Snahu o právnu reguláciu systémov umelej inteligencie, ako aj reguláciu zodpovednosti za škodu, ktorú spôsobia, hodnotím ako pozitívny a potrebný krok. Otázkou ostáva, ako tieto systémy ovplyvnia nazeranie na rozsah a kvalitu opatrení, ktoré je potrebné implementovať na zachovanie dostatočnej miery kyberbezpečnosti a kyberodolnosti.

Rastislav Janota
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Pretrvávajúca neochota pristupovať ku kybernetickým incidentom otvorene a komunikovať ich existenciu férovo je pre mňa dlhotrvajúcim sklamaním. A to tak zo strany štátnych organizácií, ako aj súkromných firiem. Také to slovenské „keď to zatlčiem, tak sa to nestalo“ je pri kybernetických incidentoch veľmi nebezpečný prístup. A to dokonca aj od organizácií, kde je táto povinnosť priamo zakotvená v zákone. Tento prístup okrem iných problémov priamo ohrozuje zákazníkov a partnerov a spôsobuje škody aj u nich.

Stanislav Smolár
manažér oddelenia bezpečnosti
Soitron

Najpozitívnejšie vnímam aktivity Kompetenčného a certifikačného centra kybernetickej bezpečnosti, ktoré veľmi ovplyvňujú tvorbu a rast kyberbezpečnostnej komunity na Slovensku. Dokázali bez prehnanej byrokracie alokovať priame EÚ dotácie na kyberbezpečnosť pre slovenské subjekty, čo považujem za obrovský úspech a dobrý základ pre ďalší rast slovenskej expertízy v tejto oblasti.

Dominik Procházka
riaditeľ odboru bezpečnosti
AGEL SK

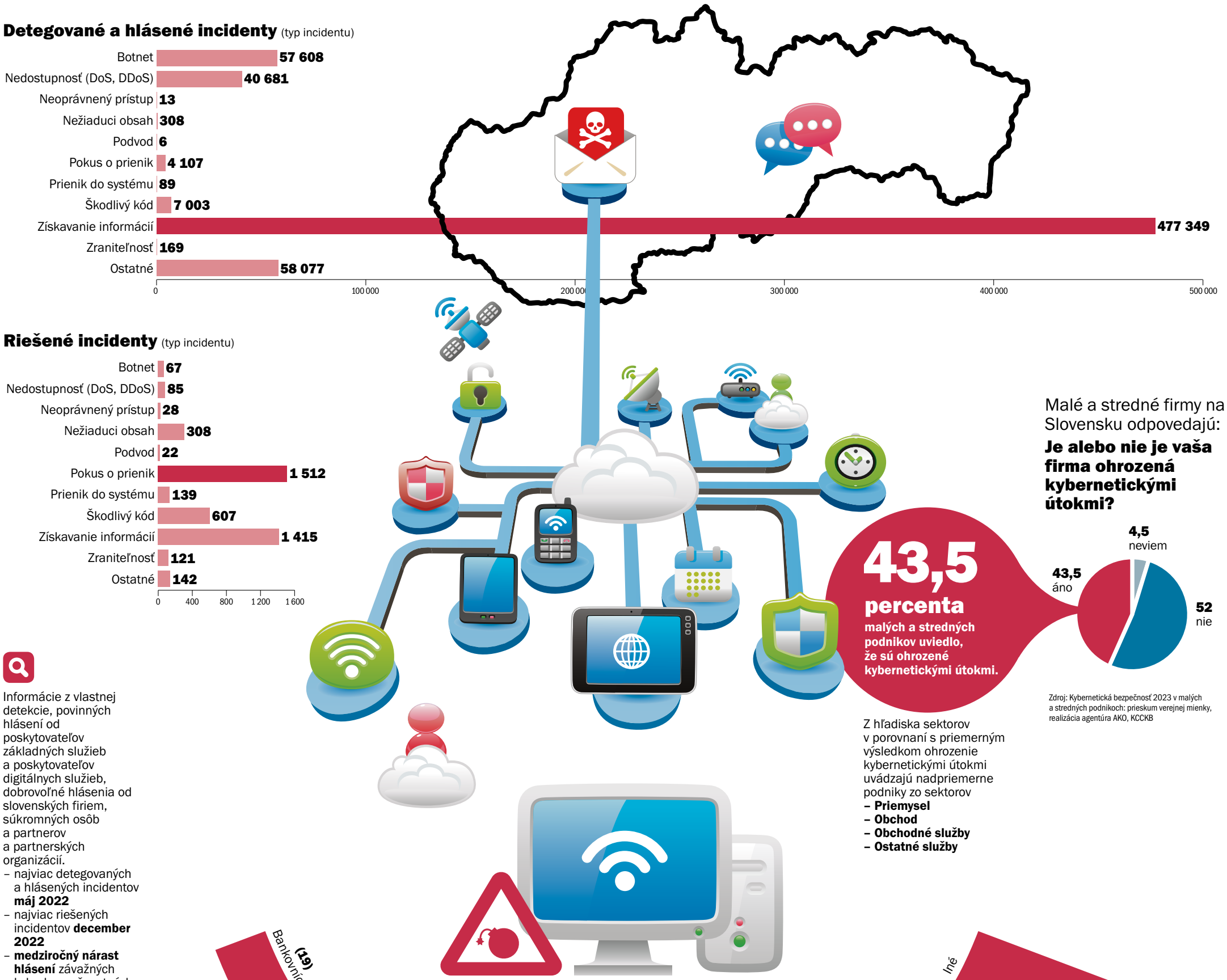
Rastúci trend využívania AI chatbotov. Na jednej strane ponúka možnosť pomôcť v najrôznejšej forme, napríklad pri úpravách skriptov a hľadaní chýb v softvéroch, pri automatizácii a podpore pre rôzne profesie, čo prispieva k zefektívneniu práce. Na druhej strane je to alarmujúci potenciál zneužitia týchto technológií pre kybernetickú kriminalitu, čo predstavuje obrovské riziko.

Timea Tomčová
manažérka informačnej bezpečnosti
Poisťovňa Union

Keď som koncom mája listovala v Správe o kybernetickej bezpečnosti v Slovenskej republike za rok 2022, ostala som veľmi nemilo prekvapená. Správa poukazuje na to, že v niektorých významných sektoroch kyberbezpečnosť stále nie je pochopená a aplikuje sa povrchne. Čo mňa ako zákazníčku daných inštitúcií znepokojuje asi najviac, je to, že tento stav pretrváva dlhodobo a nenastáva zlepšenie.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 30. JÚNA 2023 – 2. JÚLA 2023

Exkluzívne štatistiky: čo sa tu deje?



Zdroj: Kybernetická bezpečnosť 2023 v malých a stredných podnikoch: prieskum verejnej mienky, realizácia agentúra AKO, KCCKB

Zdroj: Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2022, Národný bezpečnostný úrad. V zátvorke je uvedený počet povinných subjektov v danom sektore.

KOMENTÁR

Správy o kyberbezpečnosti v malých a stredných podnikoch

Malé a stredné podniky podľa oficiálnych údajov predstavujú 99,9 percenta firiem na Slovensku.

Zároveň však stále platí, aj pred novelizáciou zákona o kybernetickej bezpečnosti, že zvyčajne nie sú zo zákona povinnými osobami. Inými slovami: že zákonom o kybernetickej bezpečnosti sa malé a stredné podniky nemusia riadiť. Neexistuje žiadna páka, ktorou by ich štátna moc mohla prinútiť k ochrane vlastných dát. V tejto súvislosti mám pre vás niekoľko správ z prieskumu o stave kyberbezpečnosti v týchto podnikoch.

Pozitívnou správou je, že väčšina podnikov chráni svoje údaje úplne dobrovoľne. Aj bez povinnosti vyplývajúcej zo zákona. Tiež sa príjemne číta, že firmy už vnímajú niektoré riziká a začínajú zavádzať procesy riadenia rizík.

Zlá správa vyplývajúca z interpretácie údajov je tá, že v podnikoch kybernetickú bezpečnosť robia zamestnanci bez podpory vedenia. Takpovediac z vlastnej iniciatívy. A ak sa štatutárne vedenie angažuje, tak sa spolieha najmä na odporúčania dodávateľov. Zdá sa, že obchodníci dodávateľských firiem odviedli výbornú prácu – tým niet čo vyčítať. Ale u konateľov malých a stredných podnikov mi chýba štipka pragmatizmu. Pretože ďalším z najčastejšie označovaných faktorov v prieskume bolo „poučenie z predchádzajúceho incidentu“.

To v kombinácii s predchádzajúcou odpoveďou znamená nielen to, že štatutári sa spoliehajú, že kybernetickú bezpečnosť vyrieši niekto za nich, ale aj to, že venovať sa jej začnú, až keď sa popália na incidente. Nerád to hovorím, ale vtedy je už väčšinou neskoro.

Na to, aby vás vedenie podporovalo v práci, nepotrebujete zákon. Členovia štatutárneho orgánu spoločnosti sú povinní vykonávať svoju pôsobnosť s náležitou odbornou starostlivosťou, pričom starostlivosť o majetok spoločnosti má byť podľa rôznych judikatúr vykonávaná v rovnakom rozsahu, akoby išlo o vlastný majetok štatutára. Nemajú štatutári záujem chrániť vlastný majetok?

Dúfal som, že v oblasti informačnej bezpečnosti notoricky známa technická norma ISO/IEC 27001 už za tie roky priniesla svoje ovocie. Zjavne však nepriniesla. Pretože aj podľa nej by mal zámery a smerovanie organizácie formálne vyjadrovať jej vrcholový manažment. A mal by preukázať podporu politiky informačnej bezpečnosti, postupov a implementácie opatrení.

Normy sú dobrovoľné a hovorí sa im tiež kodifikovaná dobrá prax. Ignorujú azda konatelia malých a stredných podnikov dobrú prax?

Kdekto tu ponúka, že pomôže firmám s implementáciou novej smernice NIS2. Zakaždým sa na tom zabávam, pretože výraz smernica EÚ na rozdiel od nariadenia EÚ znamená, že musí byť transponovaná do slovenského právneho systému národnou legislatívou. Konkrétne požiadavky budú uvedené až v novelizovanom zákone o kybernetickej bezpečnosti.

O to vtipnejšie je, že NIS2 z niekoľkých tisícov malých a stredných podnikov urobí povinné osoby. Potom už kyberbezpečnosť týchto podnikov nebude o dobrovoľnom rozhodnutí ich štatutárov. Hádam sa z ich strany zmení aspoň tá podpora vlastných kvalifikovaných zamestnancov.

Ivan Makatura,
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Našli v sebe nevídaný talent

REPORTÁŽ

Chýbajú nám tisícky profesionálov. Ak však ľudí nadchnete, dokážu v sebe objaviť nečakaný talent. Preto kyberbezpečnosť ukazuje, že je aj kreatívna a inšpiratívna.

Tomáš Szmrecsányi ©hn
tomas.szmrecsanyi@mafraslovakia.sk

Rastislav Janota, riaditeľ NCKB SK-CERT, ocenení hráči Martin Jantošovič, Mikuláš Hugec a Peter Švec, Tomáš Valenta, Check Point Software Technologies FOTO: PRODUKCIA

Druhý ročník národnej kyberbezpečnostnej súťaže CyberGame evidoval spolu viacej ako 2 300 registrovaných účastníkov na slovenskej aj anglickej platforme.

Náročná súťaž

Napriek hráčskemu názvu je však CyberGame predovšetkým náročná súťaž. V tej najťažšej úrovni slúži ako tréningová platforma profesionálov. Nájdete tu študentov, zamestnancov verejnej správy aj súkromného sektora a špeciálne niekoľko desiatok učiteľov. Viac ako sedemsto účastníkov malo menej ako 25 a najmladší mal 13 rokov.

Hracia platforma bola otvorená pre všetkých záujemcov a na účasť stačil počítač a voľne dostupné analytické nástroje.

Očakávanú zostavu tvorili tri analytické vetvy – malvérová, forenzná a OSINT analýza a kryptografia. Pribudli hracia vetva na zvýšenie úrovne bezpečnosti, takzvaný hardening, a netechnická vetva procesy a riadenie bezpečnosti.

Umelá inteligencia

Tohoročná CyberGame už mala v sebe zapracovaný aktuálny fenomén – využívanie generatívnych jazykových modelov na báze umelej inteligencie v kyberbezpečnosti. Tím SK-CERT pri tvorbe úloh a testov pracoval s modelom ChatGPT tak, aby jeho používanie nedávalo počas súťaže hráčom výhodu.

„V druhom ročníku sme urobili ťažšie úlohy, a napriek tomu sme videli skvelé hráčske výkony. Hráči museli viacej študovať, zlepšovali sa takpovediac v priamom prenose a tam sme objavili aj nové talenty," hovorí Rastislav Janota, riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT.

Študent Martin vyhral nielen študentskú kategóriu, ale stal sa aj absolútnym víťazom CyberGame 2023. „Motivácia spočívala v tréningu, v zlepšovaní a objavovaní nových oblastí, v tom, čo mám rád, čomu sa venujem a čo študujem," hovorí.

> Získal som množstvo nových poznatkov a naučil sa vidieť niektoré veci inak.
>
> **Peter Švec,**
> Fakulta prírodných vied a informatiky UKF v Nitre

Detektívne pátranie

Víťazi v súťaži aj jednotlivých kategóriách hovoria o neodolateľnej kombinácii detektívneho pátrania a vedomostných nárokoch. Programátor Martin Jantošovič hovorí, že má rád logické hádanky. Mikuláš Hugec patrí tiež do programátorskej brandže, skúsil to minulý rok, a keďže je fanúšik rébusov, zdalo sa mu, že „to je pravé orechové".

Najlepší hráč v kategórii učiteľ nahral body na celkové ôsme miesto. Do CyberGame sa zapojil preto, aby sebe aj študentom ukázal, že neplatí „kto to nevie, ten to učí". Peter Švec učí na Fakulte prírodných vied a informatiky UKF v Nitre a hovorí, že získal množstvo nových poznatkov a naučil sa vidieť niektoré veci inak. „Tento širší pohľad tak môžem posunúť študentom. Zadania v hre boli spracované na vysokej odbornej úrovni, za čo patrí tvorcom veľká pochvala."

Táto trojica sa zároveň na jeseň pobalí na cestu do kyberbezpečnostného výskumného a vývojové centra Check Point Software Technologies v Izraeli.

Ocenený hráč z verejnej správy Rastislav Kavecký hovorí, že jeho motiváciou zapojiť sa bola výborná príležitosť naučiť sa a vyskúšať si niečo nové v kyberbezpečnosti a „taktiež to bola aj skvelá zábava".

Výnimočné talenty

Súťaž oceňuje aj hráčov vo vetvách a tam sa často ukážu výnimočné talenty. Vo forenznej analýze hral skvelo Andrej Šimko, doteraz väčšinou systémový administrátor. Ako hovorí, proste bol zvedavý a má záujem o kyberbezpečnosť. Juraj Bôrik bol taký nespokojný s minuloročným 57. miestom, že výsledkom jeho prípravy v tomto ročníku bolo prémiové miesto vo vetve malvérová analýza.

Marek Vavrečan dostal ocenenie za výkon vo vetve OSINT.

Ervín Haramia, predseda Predstavenstva Aliter Technologies, a Martin, najlepší hráč CyberGame 2023 FOTO: PRODUKCIA

Rád hovorí, že práca developera je preňho vášeň, a popri nej si chcel vyskúšať iné úlohy a odhaliť nové zručnosti v sfére za hranicami svojej typickej práce. „Úlohy ma veľmi bavili a zamestnali na niekoľko dní a hodín."

Tím vybraných hráčov do 25 rokov bude reprezentovať Slovensko ako Team Slovakia v prestížnej súťaži European Cyber Security Challenge 2023 na jeseň v Nórsku.

Odborným garantom súťaže bol Národný bezpečnostný úrad.

PORADŇA

Dá sa preniesť zodpovednosť?

Je možné outsourcovať zodpovednosť za kybernetickú bezpečnosť? Vo firme nemáme zamestnanca, ktorý by mal vzdelanie alebo kurz v kyberbezpečnosti, a keďže sme menšia firma, outsourcing by bol pre nás výhodný.

V tejto otázke je potrebné rozlišovať medzi štatutárnou, čiže zákonnou zodpovednosťou za riadenie bezpečnosti, a vykonnou zodpovednosťou za riadenie bezpečnosti.

Zákonnú zodpovednosť štatutárneho orgánu nie je možné outsourcovať.

Podľa Obchodného zákonníka je štatutárny orgán spoločnosti povinný konať s odbornou starostlivosťou, v súlade so záujmami spoločnosti, pričom zodpovedá za porušenie týchto povinností.

Táto povinnosť si vyžaduje, aby si štatutár pri konkrétnom rozhodovaní zaobstaral a vyhodnotil všetky objektívne dostupné informácie. Následne sa má náležite rozhodnúť v kontexte týchto informácií a vlastnej profesionality. Výkonnú zodpovednosť za riadenie bezpečnosti je však možné obstarať ako službu dodávateľským spôsobom. Má merateľné parametre a je možné uzatvoriť na ňu zmluvu prostredníctvom dohody o úrovni služieb (SLA). Zmluva s dodávateľom služieb kybernetickej bezpečnosti však nepredstavuje nahradenie zákonných zodpovednostných vzťahov a ich prenos na tretiu osobu.

Ak by som teda mal všetkým firmám malej či strednej veľkosti odpovedať jednoznačne, riadenie kybernetickej bezpečnosti je vždy potrebné vnímať v dvoch samostatných kontextoch. Až potom si dávať konkrétne otázky a úlohy.

V prvom rade ide o zodpovednosť štatutárneho orgánu, ktorá vyplýva priamo zo všeobecne záväzných právnych predpisov. Až následne ide o zodpovednosť zmluvnú, založenú napríklad voči manažérovi kybernetickej bezpečnosti alebo dodávateľovi kyberbezpečnostných služieb.

Uvedené zodpovednosti si nie je možné zamieňať.

Štefan Pilár,
advokátska kancelária
Bukovinsky & Chlipala, s. r. o.

Každá vaša otázka je v kybernetickej bezpečnosti dôležitá. Či už ste mikropodnik, alebo veľká firma, v tejto oblasti stojíte pred mnohými výzvami.

Otázky posielajte na adresu: **kyberporadna@mafraslovakia.sk**

TREND

Váš IT tím potrebuje nástroje. Stále totiž opravuje zraniteľnosti

Bratislava – Rastúci záujem o prácu na diaľku a čoraz častejšie využívanie cloudových služieb prispeli k nevídanému rozmachu hrozieb, ktoré zneužívajú zraniteľnosti.

Každý IT správca vám pritom potvrdí, že oprava zraniteľností je jednou z časovo najnáročnejších úloh a celý proces je navyše čoraz zložitejší. Problém pomôže vyriešiť Vulnerability and Patch Management, čiže nástroj na správu zraniteľností a záplat.

Cez zraniteľnosť do celej siete

Firmy a ich zamestnanci používajú na zariadeniach množstvo rôznych softvérov. Je viac ako pravdepodobné, že pri takom kvante aplikácií bude v istom čase nejaká z nich obsahovať zraniteľnosť.

Ide o bezpečnostnú chybu, ktorú útočníci dokážu zneužiť na preniknutie do firemných systémov. Jediný spôsob, ako zraniteľnosť opraviť, je aktualizácia, ktorá chybu zapláta.

Keď sú IT zdroje preťažené, nasadzovanie záplat sa, nanešťastie, odsúva na druhú koľaj. Je však nevyhnutné, aby tímy nepoľavovali. Včasné nasadenie bezpečnostných záplat v aplikáciách a operačných systémoch je kľúčové pri predchádzaní potenciálnym narušeniam bezpečnosti.

Aktualizácie bez zdržaní

Preťažené IT tímy bojujúce so správou záplat môžu najnovšie využiť plne automatizovanú funkciu Vulnerability and Patch Management. Tento pokročilý nástroj na vyhľadávanie a opravu zraniteľností pridal do svojich riešení pre firmy slovenský ESET.

Nástroj aktivuje aktualizácie kľúčového softvéru, a to bez oneskorenia. Takéto včasné nasadenie záplat predstavuje efektívny nástroj na opravu aj najnovších zero-day zraniteľností, čo významne prispieva k posilneniu celkovej bezpečnosti organizácie.

Používanie nástroja na správu zraniteľností a záplat dostáva do firiem sofistikované techniky určovania priorít a automatizácie. Takto sa dá nastaviť aj optimálna frekvencia kontrol a ich synchronizácia s nastaveniami nasadzovania záplat. Relevantné a zneužiteľné zraniteľnosti sa „riešia" bez preťažovania IT tímov.

Odstránenie slepých miest

Vďaka nástroju na správu zraniteľností a záplat dokážu IT tímy centralizovať a automatizovať aj viaceré úlohy súvisiace s IT bezpečnosťou a jej správou. Udržiavajú si tak aktuálny inventár a môžu odstrániť všetky dosiaľ existujúce slepé miesta v infraštruktúre.

Samotným firmám to uľahčuje ochranu a zjednodušuje dodržiavanie súladu s nariadeniami a normami ako GDPR, HIPAA a PCI DSS.

Hviezdny nováčik

Správa zraniteľností a záplat ESET, čiže Vulnerability and Patch Management, je ako nový superčlen vášho IT tímu. Kontroluje tisíce obľúbených aplikácií, napríklad Adobe Acrobat, Mozilla Firefox a Zoom Client, na prítomnosť viac ako 35-tisíc bežných zraniteľností a rizík (CVE).

Zraniteľnosti je možné filtrovať a priorizovať podľa ich závažnosti. Firmy môžu uprednostniť opravu kritických chýb a zaplátanie zvyšných opráv naplánovať na čas mimo špičky, aby sa vyhli prerušeniam.

Správa z jednotnej cloudovej konzoly

Funkcia ESET Vulnerability and Patch Management sa ovláda jednoducho prostredníctvom jednotnej cloudovej konzoly na správu bezpečnosti ESET PROTECT. Ide o prispôsobiteľné riešenie vytvorené s ohľadom na zákazníkov, ktoré ESET neustále aktualizuje.

Prostredníctvom cloudovej konzoly môžu firmy získať reporty o najzraniteľnejšom softvéri a dotknutých zariadeniach. Pridanou hodnotou platformy je tiež podpora viacerých jazykov a nízke nároky na IT infraštruktúru. Riešenie ESET PROTECT je zahrnuté v piatich úrovniach ochrany. Nová funkcia Vulnerability and Patch Management je súčasťou balíka ESET PROTECT Complete aj nového balíka ESET PROTECT Elite.

Igor Kmiť,
Bezpečne vo firme (ESET)