HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
28. – 30. OKTÓBRA 2022

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Že neveríte ničomu? A dobre robíte

TÉMA

V technológiách a v bezpečnosti sa dôvera hodnotí číslami. Najlepšie číslo je v tomto prípade nula.

V technológiách a bezpečnostných riešeniach platí: neveriť nikomu a ničomu. FOTO: DREAMSTIME

Útočníci to majú ľahké, ak sú firmy v strese alebo personálne poddimenzované.

Ako odznelo aj na nedávnej slovenskej konferencii o kyberbezpečnosti, aktéri hrozieb si hovoria: „Načo budem hackovať, keď si môžem zavolať a vypýtať si meno a heslo."

U nás doma

Bezpečnostný odborník Maroš Barabas prezentoval reálne incidenty, kde útočníci dokonca zotrvávali v sieti niekoľko týždňov. V jednom prípade „udreli" cez predĺžený víkend, keď mala drvivá väčšina firmy dovolenku, a zašifrovali všetky dáta. A ako sa dostali do siete? Ľahko. Na phishing reagoval administrátor.

V druhom prípade incident objavili náhodne, keď bezpečáci pri skenovaní darkwebu videli podozrivo zhodné firemné údaje na predaj. Keď videli, že údaje sú aj s fotkami zamestnancov, už ani nebolo o čom pochybovať.

Siete to majú ťažké

Skúsenosti z praxe podporujú aj tohoročné štatistiky a medziročné porovnania. Počet útočných kampaní zameraných na prienik do siete sa ku koncu polroka globálne zvýšil takmer o polovicu.

Čo je však pozoruhodné, stále klesá podiel škodlivého softvéru pri pokusoch o prienik do siete. Kyberbezpečnostná spoločnosť Crowdstrike deteguje vyše 70 percent útočných aktivít bez škodlivého softvéru. Súvisí to s tým, že útočníci zneužívajú platné prihlasovacie údaje do sietí.

Aj správcovia sietí to majú ťažké

Zabezpečenie siete je v súčasnosti kľúčovou úlohou firiem a inštitúcií všetkých veľkostí. Aj tej vašej.

Prístupy z vnútornej siete nie sú iba neškodné a prebieha odtiaľ čoraz viac útokov. Kompromitácia jedného dôveryhodného vnútorného zariadenia umožňuje získať útočníkovi prístup na ďalšie systémy. Aktéri hrozieb sú v sieti nepozorovaní, prehľadávajú a kopírujú údaje, vykonávajú špionáž, ransomvérové útoky, zapájajú zariadenia do botnetov alebo nelegálne ťažia kryptomenu.

Zmizla nám dôvera

V roku 2020 sa rozpadlo mnoho štruktúr aj v kybernetickej bezpečnosti. „Veľké množstvo služieb migrovalo do cloudu, zmenil sa spôsob práce, rastie počet zariadení v sieti a zamestnanci sa pripájajú z rôznych lokalít. Model perimetrovej bezpečnosti sa stal zastaraným," konštatuje Jozef Bálint, bezpečnostný špecialista Alison Slovakia.

Firewall, ako hlavný prvok ochrany na perimetri, odišiel do histórie. Rovnako prestalo platiť, že používatelia, zariadenia a aplikácie vo vnútornej sieti sú primárne považované za dôveryhodné a všetko vo vonkajšej sieti za nedôveryhodné.

Ak by sme to chceli povedať veľmi expresívne, dnes je nedôveryhodné všetko. Definitívne sa tak presadil koncept zero trust, čiže koncept nulovej dôvery.

Neveriť nikomu a overovať všetkých

Vonkajšia aj vnútorná sieť sú považované za nebezpečné, respektíve nepriateľské. Každý prístup, či už ide o používateľov, zariadenia alebo aplikácie, musí byť overený a autorizovaný. Všetko ostatné je zamietnuté.

Súčasťou konceptu nulovej dôvery je aj predpoklad prieniku, čiže očakávanie najhoršieho možného scenára a s tým súvisiacich reakcií na incident a plánov na zabezpečenie chodu organizácie. Používatelia a aplikácie majú pridelené len tie prístupy, ktoré potrebujú nevyhnutne na svoju činnosť.

Ako hovorí bezpečnostný profesionál Marek Zeman po nedávnych skúsenostiach s implementáciou, koncept nulovej dôvery spája bezpečnosť a prevádzku v jeden ucelený celok.

> Model perimetrovej bezpečnosti sa stal zastaraným.
>
> **Jozef Bálint,** bezpečnostný špecialista Alison Slovakia

Každý rok viac

V globálnom meradle takmer tri štvrtiny organizácií uviedli, že v tomto roku sú v procese prijímania zero trust stratégie alebo ju už prijali.

Implementáciu konceptu nulovej dôvery sa v Tatra banke rozhodli urobiť na základe odporúčaní materskej skupiny. „Pre kompletné nasadenie do banky našej veľkosti sme naplánovali štyroch expertov na celý čas projektu. V konečnom dôsledku implementáciu vnímam naozaj veľmi pozitívne," hodnotí Marek Zeman.

Po mesiacoch skúseností tu padol aj najväčší mýtus, že ide o neobratné a pomalé riešenie, ktoré nedovoľuje nikomu nikam pristupovať. Ukázalo sa, že koncept nulovej dôvery priniesol naozaj dobré a funkčné riešenie a má rovnaké muchy ako ktorékoľvek iné. Ale všetky muchy je možné „pochytať".

Dôveruj, ale preveruj

Tento princíp je základným kameňom každej bezpečnostnej architektúry. Preto podľa názoru architekta kybernetickej bezpečnosti Mariána Trizuliaka marketingovo poňatý koncept zero zrust neprináša až také prevratné zmeny: „Buď pravidelne prehodnocujem riziká a aplikujem opatrenia, alebo jednoducho spím na vavrínoch. Toto nie je o technickej nulovej dôvere, ale predovšetkým o nás, o ľuďoch."

Zároveň však kriticky dodáva, že nech je bezpečnostný profesionál akokoľvek skúsený alebo ostrieľaný, po istom čase sa stane pohodlným a nemusí niektoré hrozby vnímať. Koncept nulovej dôvery dlhodobo udržiava v pozornosti aj profesionálov a nedovoľuje im spoliehať sa na zaužívané predpoklady pri budovaní bezpečnostných riešení.

Je to o rozmýšľaní

„Realizácia konceptu nulovej dôvery je podobná tomu, ako si budujeme vlastné bývanie – rozumne postaviť plot, zabezpečiť dvere, zakryť strechu," opisuje proces Marián Trizuliak. „Treba ísť pekne po vrstvách zvonku do vnútra ‚cibule', kde sa nachádza to najdôležitejšie."

Tento koncept má pomôcť profesionálom udržovať pozornosť, neustále zvažovať a vyhodnocovať hrozby aj tam, kde doteraz nevnímali priestor na zlyhania či narušenia. Nulová dôvera môže zároveň predstavovať princípy bezpečnostnej architektúry IT prostredia alebo prevádzkových technológií.

Bezpečnosť nemá konečnú

Architektúra nulovej dôvery je nevyhnutná všade, kde zamestnanci pracujú z rôznych lokalít, využívajú cloudové riešenia a internet nahradil ich firemnú sieť.

V dobe globálnej komunikácie a konektivity sa táto architektúra uplatňuje v každom segmente, ktorý potrebuje byť efektívny a konkurencieschopný a minimalizovať riziká spojené s kybernetickými hrozbami.

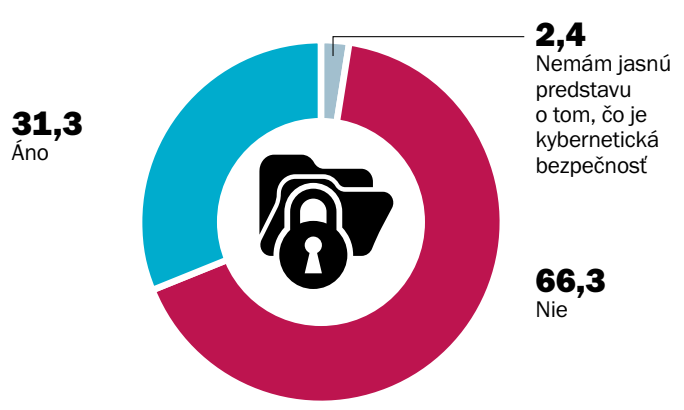
Posilnenie konceptu nulovej dôvery predstavuje kombináciu s hĺbkovou ochranou (defence-in-depth). „Pridávajú sa tu nástroje na riadenie a monitorovanie privilegovaných účtov, ktoré umožňujú zvýšiť úroveň bezpečnosti pomocou vytvárania auditových logov a záznamov," vysvetľuje Jozef Bálint.

Už to bude iba viac

Spoločnosť Gartner odhaduje, že globálne výdavky na riešenia nulovej dôvery budú v tomto roku 820 miliónov amerických dolárov. Nejde ani o sumu samotnú, ale o predpokladaný dramatický rast. Ročné výdavky na riešenia nulovej dôvery sa do troch rokov viac ako zdvojnásobia.

Na porovnanie – ročné výdavky na informačnú bezpečnosť a riadenie rizík vo svete narastú v roku 2025 „iba" o necelých štyridsať percent.

Zaoberáte sa kybernetickou bezpečnosťou vo firme, aj keď vám to legislatíva neprikazuje? (v percentách)



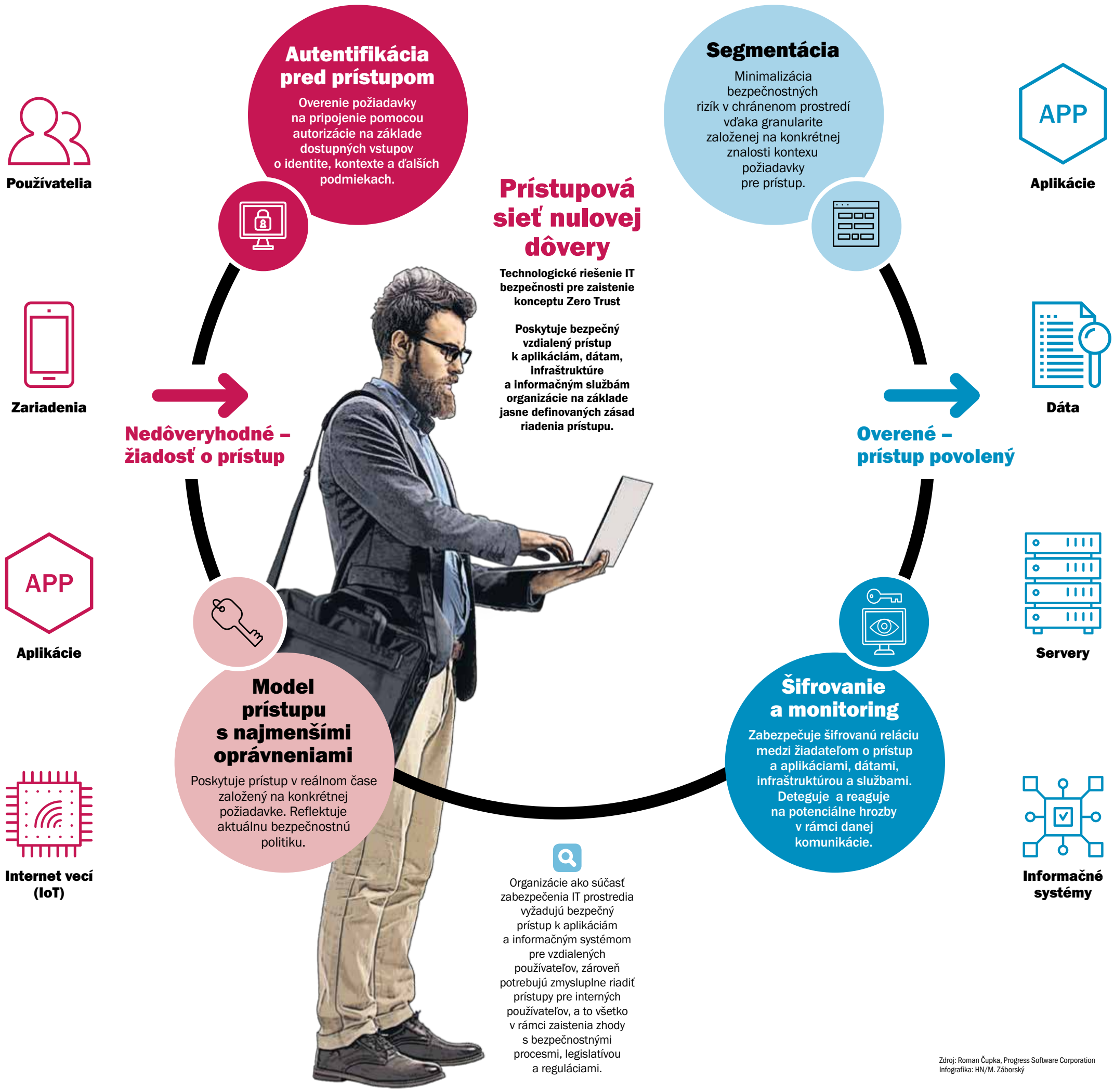
Prieskum stavu kybernetickej bezpečnosti v malých a stredných podnikoch
Zdroj: Slovak Business Agency, Bratislava, 2022

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

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

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. OKTÓBRA 2022

Všetci o tom hovoria, každý to chce. Pozrite sa, ako funguje Zero Trust



Zdroj: Roman Čupka, Progress Software Corporation
Infografika: HN/M. Záborský

KOMENTÁR

Ak robíme verejné politiky, mali by sme vedieť ako a pre koho

Ambícia robiť verejné politiky ešte efektívnejšie a adresnejšie opäť rezonuje na európskej regulačnej scéne. Žije tu s nami už druhú dekádu, no nie vždy úspešne.

Cieľ takzvanej lepšej tvorby predpisov je rozhodne šľachetný, avšak nikdy sa nebude dať dobre realizovať bez kvalitných vstupných údajov, alebo, ako sa často stáva – aj bez akýchkoľvek údajov. A to druhé píšem s úplnou vážnosťou.

Sám som bol v minulosti svedkom prípravy nejedného opatrenia, ktoré malo mať dosahy na podniky či občanov a ktoré nebolo podkuté dostatočnou údajovou bázou či komunikované s cieľovými skupinami. O transparentnosti už ani nehovoriac.

Jedným z kľúčových dokumentov, ktoré sa v najbližších mesiacoch dostanú medzi odbornú verejnosť a ktorý má zároveň ambíciu prispieť k príprave lepších verejných politík, je Národný index kybernetickej bezpečnosti.

Úlohou indexov či porovnávacích alebo výkonnostných rebríčkov vo všeobecnosti, s ktorými sa stretávame dnes na medzinárodnej scéne, je cez jednotnú metodiku vyhodnotiť súčasný stav v sledovaných oblastiach. V digitálnej sfére je u nás známy napríklad index DESI (EÚ) a v oblasti kybernetických záležitostí zase Global Cybersecurity Index (OSN).

Tieto rebríčky porovnávajú jednotlivé krajiny ako celok. S čím sa však stretávame menej často, ak vôbec, sú výsostne vnútroštátne porovnávania, ktoré sledujú a posudzujú vývoj v určených oblastiach, takzvaných dimenziách.

Národný index kybernetickej bezpečnosti prinesie možnosť pravidelne vyhodnocovať súčasný vnútorný stav kybernetickej bezpečnosti a umožní zachytávať trendy. Podrobnejšie preskúmanie aktuálneho stavu pomôže nielen upriamiť pozornosť na pretrvávajúce nedostatky, ale taktiež sa pripraviť na budúce výzvy a postupne zvyšovať pripravenosť a odolnosť krajiny.

Index by sa mal orientovať na štyri skúmané dimenzie, ktoré predstavujú regulované subjekty v zmysle zákona o kybernetickej bezpečnosti, neregulované subjekty, ďalej sa zameria na spoločnosť a vzdelávanie.

Po zavedení indexu ako podporného nástroja pre lepšie riadenie štátu a verejných politík sa Slovensko môže zaradiť medzi tie krajiny, ktoré prichádzajú s inovatívnymi riešeniami.

Aj tu sa sleduje primárny cieľ, ako posilniť nielen národnú, ale aj európsku kybernetickú bezpečnosť v kontexte rozvíjajúcej sa transformácie digitálneho prostredia vrátane súvisiacich hrozieb. Kvalitné a adresné opatrenia je totiž možné uskutočňovať len vtedy, ak budeme poznať aktuálny východiskový stav.

Takto budeme vedieť písať lepšie zákony, stratégie či akčné plány. Index striktne založený na dátach a s kvalitnou metodikou by sa tak mal stať východiskom pre budúce predpisy a pravidlá. Také, ktoré budú transparentné, ich súčasťou bude vyhodnotenie dosahov a zároveň sa k nim budú môcť vyjadrovať tí, ktorých sa týkajú.

Som rád, že Národný bezpečnostný úrad, ktorý z povahy svojho pôsobenia často nemôže zdieľať s verejnosťou detaily všetkých aktivít, dáva potrebný impulz aj na vznik dokumentov, ako je práve index.

Radoslav Repa,
Národný bezpečnostný úrad

IT projektom roka 2022 sa stala CyberGame

SÚŤAŽ

Na začiatku bola úloha, s ktorou sa Slovensku borí už roky – nedostatok špecialistov kybernetickej bezpečnosti, náročná problematika a uzavretá komunita. Na konci to bolo uznanie v podobe hráčskeho nadšenia a komunitného ocenenia.

Ocenenie na IT Gala prebral Matej Šalmík, riaditeľ odboru vzdelávania, podpory a medzinárodnej spolupráce NCKB SK-CERT.

FOTO: PRODUKCIA S.R.O

Podľa hodnotenia zástupcov IT segmentu a odborných novinárov sa CyberGame stala IT projektom roka 2022. „Kľúčovými kritériami pre hodnotenie bol prínos pre cieľovú skupinu, originálnosť a unikátnosť riešenia a využívanosť výsledkov projektu," vysvetľuje predseda poroty Martin Drobný.

Dvadsiaty ročník IT Gala tak zároveň ocenil aj spojenie a spoluprácu rôznych sektorov. Až nechceným aktualizačným momentom sa stala napätá bezpečnostná situácia v kybernetickom priestore.

Ivan Kopáčik, ktorý zastupoval v porote ISACA hovorí: „Názov je síce hravý, ale všetko ostatné zodpovedá podmienkam krutej reality. CyberGame bola reálna simulácia skutočného stavu a reálne sa môže používať ako skúška schopnosti a pripravenosti."

Účastníci od dvanásť do šesťdesiat rokov

CyberGame má parametre kybernetického cvičenia a je koncipovaná tak, že obsahuje úlohy rôznej náročnosti. Odborným garantom súťaže bolo Národné centrum kybernetickej bezpečnosti SK-CERT a všetky úlohy vytvoril tím jeho profesionálov.

Súťaž bola rozdelená do štyroch tematických vetiev, účastníkom stačil na hru vlastný počítač a voľne dostupné analytické nástroje. Obsah tvorilo vyše päťdesiat jedinečných úloh a odborný garant prevádzkoval aj komunikačný kanál, poradenstvo a priebežne aktualizoval výsledky.

Hra trvala desať týždňov a pritiahla viac ako tisíc účastníkov. Hrali primárne programátori, študenti, odborníci kybernetickej bezpečnosti, pridali sa gameri, ale aj učitelia. Trojica víťazov – najlepší hráč s celkovým hodnotením, najlepšia hráčka a najlepší hráč študent leteli na exkurziu do malvérového laboratória do Toronta.

Priamo, komunitným šírením, cez média a sociálne siete oslovila téma kyber bezpečnosti odborníkov, akademický sektor aj širokú verejnosť.

Môžu sa „hrať" aj firmy

Vzhľadom na mimoriadny záujem bude v novembri CyberGame prístupná v upravenej forme pre firmy, inštitúcie aj školy, čiže organizácie každého typu a veľkosti. Zo súťažnej hry sa tak stane tréningová platforma kybernetickej bezpečnosti s rôznymi úrovňami náročnosti.

> Kľúčovými kritériami pre hodnotenie bol prínos pre cieľovú skupinu, originálnosť a unikátnosť riešenia a využívanosť výsledkov projektu.
>
> **Martin Drobný,** predseda poroty

Odborný garant súťaže pripravil na november desiatky úloh v štyroch hracích vetvách a sprístupní aj komunikačný kanál.

Každá organizácia, ktorá o to požiada písomne, dostane prístup do hráčskeho rozhrania. Následne sa tam môžu prihlásiť zamestnanci a vyskúšať si úlohy kyberbezpečnostných odborníkov. CyberGame sa dá poňať ako súťaž profesionálov, ale aj exkurzia záujemcov.

Ako ukázal prvý ročník, medzi hráčmi sa našli výnimočné talenty a to dokonca bez predchádzajúcich skúseností v kybernetickej bezpečnosti.

„Plánujeme aktívne vyžívať CyberGame ako tréningovú platformu pre firmy a inštitúcie, priebežne ju aktualizovať a trikrát do roka ju otvoriť pre záujemcov," uviedol Rastislav Janota, riaditeľ SK-CERT. Tím CyberGame pripravuje už ďalší ročník s hlbokým presvedčením, že talenty si zaslúžia príležitosť.

ANALÝZA

Zero Trust: marketing alebo skutočná zmena?

Hoci sa pojem Zero Trust môže javiť ako nový trend v kybernetickej bezpečnosti, samotná myšlienka „odstraňovania implicitnej dôvery" bola prvýkrát predstavená tak pred 15 rokmi.

Aby sme lepšie pochopili princípy

Pripomeňme si v skratke, ako funguje bezpečnostný model postavený na princípe definovania perimetra.

Takýto model vychádza z premisy, že služby zákazníka sú prevádzkované v jeho datacentrách, takzvaných on premise. V tomto prípade vieme veľmi presne definovať perimeter, ktorý oddeľuje externé siete – internet od lokálnej siete, ktorá je prevádzkovaná organizáciou.

Na perimetri potom môžeme zabezpečiť veľmi robustnú ochranu proti kybernetickým hrozbám, pričom bezpečnostné pravidlá v rámci lokálnej infraštruktúry môžu byť voľnejšie definované, keďže samotná lokálna sieť je pod správou organizácie a je teda dôveryhodná.

Zero Trust koncept stavia model perimetrovej bezpečnosti takpovediac „na hlavu". V jednoduchosti by sme mohli povedať, že tento koncept hovorí, že žiadny perimeter neexistuje a implicitná dôvera lokálnej infraštruktúry už nie je viac relevantná.

Ak by sme však chceli formálnu definíciu, museli by sme sa pozrieť do článkov Národného Inštitútu pre Štandardy a Technológie (NIST) konkrétne NIST 800-207.

Koncept Zero Trust teda nemôžeme vnímať ako jedinú architektúru, zariadenie či postup. Je to súbor princípov, systémových dizajnov či procesov. Hlavné myšlienky však možno zoskupiť do troch oblastí.

Nikomu nedôveruj, vždy preveruj

V architektúre nulovej dôvery neexistujú žiadne dôveryhodné zariadenia, zdroje či zóny. Navyše toto preverovanie musí byť vykonávané kontinuálne.

Tento bod predstavuje podľa môjho názoru najväčšiu zmenu oproti „klasickým" modelom informačnej bezpečnosti postavenej na perimetrovej bezpečnosti, keď po zaradení do dôveryhodnej siete či segmentu je už tento prístup udelený a používa sa až do zmeny politiky.

V architektúre Zero Trust takáto implicitná dôvera neexistuje. Používateľ, zariadenie, server či vo všeobecnosti zdroj sú posudzované pri každej požiadavke. Navyše, toto posudzovanie sa deje na základe kontextuálnych dát získaných z prostredia.

Minimalizovanie dosahu

Tento bod vychádza z paradigmy o predpoklade, že sieť je kompromitovaná. V takom prípade sa snažíme o minimalizovanie dosahu samotného prieniku. Minimalizovať dosah môžeme primárne správnou segmentáciou siete a použitím princípu minimálnych oprávnení.

Pri segmentácii siete však Zero Trust koncept dáva do popredia nielen klasickú L3/L4 segmentáciu, no pridáva aj rozmer identity používateľa.

Zber kontextuálnych informácií a rýchla odpoveď

Pre správne rozhodovanie v čase je nutné z prostredia zberať a spracovávať veľké množstvo dát, ktoré sa využívajú pri vyhodnocovaní politík v rámci konceptu nulovej dôvery.

Skutočná zmena paradigmy, ako pre koho

Princípy nulovej dôvery kombinujú nové postupy a koncepty so „starým známym". Pre organizácie, ktoré sú pravidelne auditované a majú vybudovaný systém riadenia informačnej bezpečnosti, prináša tento koncept len minimálny počet radikálnych zmien či nutnosti veľkých investícií.

Tieto organizácie využívajú koncepty ako segmentácia siete, princíp minimálnych oprávnení a overovaní používateľov a zariadení aj v internej sieti.

Na druhej strane spektra je však nespočetne veľa organizácií, ktoré stále používajú perimetrovú bezpečnosť a spoliehajú sa na „dvojicu firewallov" pred vstupom do ich siete.

Pre takéto organizácie bude koncept Zero Trust skutočne predstavovať radikálnu zmenu a nutnosť nemalých investícií do zabezpečenia organizácie. Táto zmena bude o to intenzívnejšia, o čo viacej sa bude organizácia otvárať cloudovým príležitostiam a vzdialenej práci.

Michal Srnec, odborník na kyberbezpečnosť Aliter Technologies

TREND

Umelá inteligencia sa stále pozerá, ako sa správa používateľ

Nákup technológií rieši iba časť kybernetickej odolnosti. Kľúčovou je však naša schopnosť rozmýšľať dynamicky. Ste pripravení?

Najznámejším a najstarším kľúčom na ochranu digitálnych informácií sú používateľské meno a heslo, ktoré sa zadávajú v prvom kroku na začiatku prihlasovania. Ak je potrebná vyššia úroveň, vytvorí sa zabezpečenie aj formou tokenov a dvojfaktorovej autentifikácie.

Tieto konfigurácie sú zvyčajne statické, čiže pôvodná úroveň rizika sa posudzuje a upravuje iba v čase žiadosti o prístup.

Stratégia nulovej dôvery prináša zmenu v tom, ako sa zabezpečuje ochrana. Autentifikácii používateľov je nepretržitá a opakovane sa prehodnocuje hodnotenie systému, či môže pokračovať prístup k službe. Metriky prístupu sa neustále zhromažďujú a riziko sa často prepočítava.

Adaptívna inteligencia

Tradičná obrana ako napríklad brány firewall nie je proti pokročilým aktérom hrozieb veľmi účinná, keďže ich vedia obísť. Vylepšenie je možné nepretržitou autentifikáciou, ktorá používa typy hodnotenia rizík ako základná autentifikácia a je aktívna počas celej relácie. Adaptuje sa.

Tento holistický postoj k správe prístupov bráni vonkajším aktérom kradnúť prihlasovacie údaje cez phishing a blokuje aj útoky typu man-in-the-middle. Súčasne dokáže odhaliť útočníkov z vnútra siete, ktorí zneužívajú pridelené práva alebo využívajú zdieľané poverenia na získanie neoprávneného prístupu.

Aby bola adaptívna bezpečnostná infraštruktúra efektívna, musí sa opierať o hlbší pohľad na používateľa a analýzu jeho správania.

Analýza správania

Organizácie menia správu prístupu tak, aby dosiahli zero-trust zabezpečenie pre všetky svoje aktíva. Potrebujú detekciu rizík, ktorá presahuje rámec definovaných zásad a zahŕňa analýzu správania.

Jediným spôsobom ako to dosiahnuť je hromadiť kontextové informácie a aplikovať na ne strojové učenie. Takéto zhromažďovanie pri každom prístupe k chráneným údajom vytvára ucelený profil bežného správania používateľa. Následné využitie analytických technológií a pravidelné vyhodnocovanie informácií poskytuje presnejší obraz očakávaného správania a zlepšuje schopnosť identifikovať rizikové situácie.

Monitoring zároveň detekuje zmenu úrovne rizika aj potrebu, kedy spustiť požiadavku na autentifikáciu. Vytvára to priestor na znižovanie alebo zvyšovanie úrovne autorizácie na základe identifikovaného rizika a dostupného overenia identity.

Ako blokovať správne

Jednou z najťažších úloh ako rozšíriť prístup používateľov s nepretržitou autentifikáciou, sú situácie, keď dochádza k blokovaniu aj legitímneho používateľa. Najbežnejším prístupom k odstráneniu alebo minimalizácii týchto incidentov je overenie identity používateľa pasívnou autentifikáciou.

Populárnymi metódami sú biometria využívaná pre prihlasovanie do systému Windows či na smartfón, rozpoznanie používateľa prostredníctvom spôsobu jeho písania, využívanie čítačky na odtlačky prstov, verifikácia hlasu alebo overenie FIDO autentifikáciou bez hesla. Čím väčšia knižnica metód pasívnej autentifikácie je k dispozícii, tým flexibilnejšie sa prispôsobuje správna metóda danej situácii.

Sila integrovanej NetIQ platformy spočíva v tom, že využíva adaptívnu inteligenciu, ktorá prispôsobuje silu overenia a úroveň autorizácie nameranému riziku a podriaďuje ju stratégii nulovej dôvery.

Anna Stehlíková, manažérka pre bezpečnostné licencie Micro Focus

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. OKTÓBRA 2022

Tento rok nám to zrátal. A výsledok?

ANKETA

Náročná ekonomická a politická situácia ukázala v plnej nahote naše podlžnosti a zanedbané oblasti. Profesionáli hodnotia, aká je urgentná úloha kyberbezpečnosti.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti
Void SOC Soitron

Vo firemnom prostredí je už dnes celkom bežné zhromažďovať veľké množstvá dát a používať napríklad behaviorálnu analýzu a strojové učenie, aby sme dokázali bezpečnostné incidenty včas identifikovať. Je však správne aplikovať podobné princípy vo verejnom priestore? Sme pripravení tolerovať sledovanie správania, ak nám to pomôže predísť teroristickým činom? Ak áno, ako zabránime zneužitiu zbieraných dát? Možno je niekedy úlohou bezpečnosti chrániť nás aj pred sebou samými.

Tomáš Hettych,
viceprezident
ISACA

Podľa mňa je terorizmus ideológia alebo aspoň posledné riešenie nejakého problému. A odborníci v kybernetickej bezpečnosti možno môžu pomôcť predvídať útoky alebo zmierniť následky. Samotnému terorizmu však asi nemôžeme zabrániť.

Ivan Kopáčik,
bezpečnostný expert Gordias

Na kyberbezpečnosť sme sa roky pozerali ako na niečo exotické, čo sa bežného človeka či firmy netýka. Dianie nás však čoraz dôraznejšie presviedča o opaku. Kyberbezpečnosť je už súčasťou nášho života. Zaoberať sa ňou musí každé hospodárske odvetvie. A čím menej budeme rozumieť zásadám kyberbezpečnosti, tým viac na to budeme doplácať – ako štát, firmy i občania.

Jaroslav Oster,
predseda Správnej rady
Preventista.sk

Dlhodobo sme zanedbali potrebu vzdelávania a prevencie v školskom sektore. Smutná a dlhá polemika ďaleko nad rámec pár viet. K tvorbe koncepcií a rôznych projektov sa často vyjadrovali jednotlivci bez reálnych skúseností, v mnohých prípadoch boli projekty tvorené s politickým a ekonomickým podtextom, čo má, samozrejme, pramálo spoločné s kvalitou a dosahom. Ako vraví klasik – kto seje vietor, žne búrku.

Július Selecký,
senior technický špecialista
ESET

Pocit bezpečia a bezpečnosť samotná sú jedným z pilierov rozvoja každého štátu. Život okolo nás je úzko naviazaný na informačné a komunikačné technológie a kybernetické incidenty oslabujú štát, firmy, respektíve celú ekonomiku a aj dôveru ľudí v tieto inštitúty. V súčasnosti nie je možné bez posilnenia kyberbezpečnosti napredovať.

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

Kybernetický priestor je podobný fyzickému a okrem bezpečnostných bariér a ochranných prvkov si oba vyžadujú aj monitoring. Z hľadiska kybernetickej bezpečnosti je preto kvalitný monitoring základom prevencie. Bezpečnostný monitoring však často ide na úkor súkromia. Preto treba nájsť balans, keď bezpečnosť, a teda monitoring aktivít, prevažuja nad potrebou súkromia.

Diana Legdanová,
vedúca úseku bezpečnosti
Východoslovenská energetika Holding

Úlohy kyberbezpečnosti a nás profesionálov sú podstatne väčšie, ako si používatelia myslia a uvedomujú. V globálno-digitálnom svete, v čase až nepochopiteľnej potreby zverejňovania osobných informácií, je anonymita irelevantným pojmom. Pamätajte však, že všetko, čo je na nete, je zneužiteľné. Tu platí menej je viac. Čím menej zverejnených informácií, tým väčšia bezpečnosť. Či ide o firmy, verejné inštitúcie alebo súkromné osoby.

Róbert Mramúch,
manažér kybernetickej bezpečnosti
MH Teplárenský holding

Prikladať väčší dôraz na ľudí a financie. Témy kyberbezpečnosti dostať viac do povedomia a pochopiteľnou formou dostávať bližšie k laickému obyvateľstvu. Investovať do súčasných technológií a rozvoja špecialistov.

Roman Čupka,
hlavný konzultant
Progress | Flowmon a CEO
Synapsa Networks

Mali by sme nahliadať na kybernetický priestor vrátane sociálnych sietí ako na významnú súčasť spoločenského celku a bezpečnosť vnímať holisticky. Základy bezpečnej a morálnej spoločnosti sa majú formovať individuálne v každej domácnosti a nespoliehať sa na tretie strany. Následne sa môžeme domáhať väčšej kontroly kybernetického priestoru a spoliehať sa na expertízu v oblasti kybernetickej bezpečnosti.

Dominik Procházka,
riaditeľ odboru bezpečnosti
AGEL SK

Kybernetická bezpečnosť dnes zohráva veľmi dôležitú úlohu na celkovej bezpečnosti spoločnosti. Kamkoľvek sa človek pozrie, je na pozadí IT systém a bez funkčných ovládacích zariadení môže nastať veľký chaos. Následky kybernetických útokov môžu byť fatálne. Ochrana dát, zabezpečenie spoločností, školenie ľudí a nárast investícií v oblasti kybernetickej bezpečnosti by mali byť pre spoločnosť prioritné.

Ján Golais,
poradca bezpečnosti
Slovak Telekom

Najväčšou výzvou kyberbezpečnosti je zabezpečenie dostatočného informovania a edukácie osôb participujúcich na procesoch u prevádzkovateľov základných služieb. Najzraniteľnejším ohnivkom v reťazci opatrení je a vždy bude človek. Platí to na všetkých od manažmentu až po posledného používateľa. Podceňovanie edukácie vyžaduje niekoľkonásobne zvýšené náklady a úsilie na odstránenie dosahu. Akceptácia tohto rizika iba posúva problém.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Zanedbali sme kvalifikáciu ľudí. Na všetkých úrovniach. Vzdelávacie programy nereflektovali nárast objemu dát a mieru informatizácie – akokoľvek aj tá je pozadu. Ministerstvo školstva zrejme dodnes nezaznamenalo existenciu nového odboru. Bezpečnostné povedomie je mizerné a vzdelávanie je v plienkach. Stratili sme najmenej 15 rokov. Nie som si istý, či do dôchodku dokážem zmierniť tento stav.

Ján Grujbár,
generálny riaditeľ
Aliter Technologies

V posledných rokoch sme svedkami raketového rastu online podnikania, a to až do takej miery, že mnohé služby už nemajú ani svoju fyzickú reprezentáciu. S týmto trendom rastie na jednej strane komplexnosť systémov, čo na druhej strane prináša aj množstvo nových bezpečnostných rizík. Ako hlavnú úlohu preto vnímam zaradenie informačnej bezpečnosti už do štandardných procesov vývoja IT a dôkladné zabezpečenie používateľských dát.

Miroslav Chlipala,
advokát
Advokátska kancelária Bukovinský & Chlipala

Pravidelne sa pýtam sám seba, či má kybernetická bezpečnosť bližšie k informačným technológiám alebo k bezpečnosti ako takej. Som presvedčený, že čím bude bezpečnostné povedomie v spoločnosti vyššie, tým bude vyššia aj úroveň kybernetickej bezpečnosti. Informačné technológie nie sú najdôležitejšie. Sústreďme sa na vzdelávanie, budovanie povedomia o bezpečnosti. Budeme lepší!

Roman Varga,
manažér kyberbezpečnosti
Dôvera, zdravotná poisťovňa

Kyberpriestor nepozná pojem mier a aj my sme pod paľbou záujmových skupín či jednotlivcov. Eliminovať terorizmus v tomto priestore je takmer nemožné. Vieme správne, rýchlo a objektívne reagovať na nové hrozby? Áno, aktívnejšou obranou. Je nutné dobudovať a v spolupráci využívať kapacity na reakcie na kybernetické útoky a iné bezprostredné hrozby. Platí však, že aj my používatelia vieme rozpoznať a zmierniť niektoré riziká.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií
Volkswagen Slovakia

Zlyhávala osveta – často sa podceňovali riziká a nástrahy v online priestore. Súčasnosť nám nastavuje zrkadlo. Ukazuje, že ochrana informácií na súkromnej, komerčnej aj štátnej úrovni musí mať vyššiu prioritu. Pozornosť, akú si zaslúži. Zvyšujme povedomie o nástrahách v kyberpriestore, implementujme efektívne opatrenia na prevenciu a reakciu proti bezpečnostným hrozbám. Testujme ich. Ešte nie je neskoro.

Michal Ďorda,
audítor kybernetickej bezpečnosti
Auditori.it

Špecialisti kybernetickej bezpečnosti sa už dlhodobo podieľajú na vzdelávaní a vysvetľovaní bežným používateľom a laikom, akým spôsobom čítať informácie na internete od anonymných používateľov. Celková bezpečnosť spoločnosti je aktuálne ohrozená radikálnymi myšlienkami a umelo vytvorenými hoaxmi. Avšak len trénovaným kritickým myslením budeme premýšľať, čo je správne a čo už je za čiarou v boji proti hybridným hrozbám. A táto úloha s nami ostane už navždy.

František Boda,
manažér kybernetickej bezpečnosti EMM

Žijeme v období, v ktorom sa prelína realita s kybernetickým priestorom. Ľudia sú ovplyvňovaní v online, často z neoverených zdrojov. Skrývajú sa za anonymitu avatarov. Za najurgentnejšie považujem vzdelávanie spoločnosti, od malých detí až po dôchodcov. Aby sa vedeli zorientovať v tomto svete. Aby okrem výhod poznali aj hrozby, vedeli sa s nimi vyrovnať a tiež niesť zodpovednosť za svoje výroky.

Tomáš Zaťko,
CEO, etický hacker
Citadelo

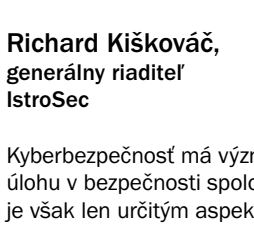
Podľa mňa je bezpečnosť oveľa viac o dlhodobej konzistencii ako o urgencii. Vo firme to máme definované víziou. Chceme tvoriť svet, v ktorom kriminálni hackeri nikdy neuspejú. To je, samozrejme, vysnený ideál, ku ktorému sa úplne nedostaneme. Žijeme totiž v obyčajnej realite. Víziu ideálu však potrebujeme. Je to jasný maják, ku ktorému vždy smerujeme, a je tiež skúškou správnosti. Keď idem niečo robiť, vždy sa pýtam – ako ma to posúva k vízii bezpečného sveta?

Martin Fischer,
manažér oddelenia bezpečnosti
Všeobecná zdravotná poisťovňa

Potrebujeme dostať zásady a pravidlá, ktoré platia pre kybernetický priestor, do povedomia a bežného zvyku širšej verejnosti – každý z nás považuje za samozrejmosť zamykať, keď odchádza z domu, a rovnako potrebujeme uplatňovať aj tieto „digitálne“ pravidlá. Uvedomme si tiež, že do kyberpriestoru môže prispievať dnes už ktokoľvek, a preto je nutné informácie o to viac overovať a chrániť tak seba aj blízkych.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Najhoršie, čo sa nám mohlo stať, je práve táto otázka. Nemali by sme dospieť do štádia, že v bezpečnosti riešime niečo urgentne. Určite príde mnoho odpovedí kolegov, ktorých si vážim. Želal by som si však, aby si urgentne aspoň jednu z odpovedí zobrali k srdcu čitatelia a tí, ktorí rozhodujú.



Richard Kiškováč**,**
generálny riaditeľ
IstroSec

Kyberbezpečnosť má významnú úlohu v bezpečnosti spoločnosti, je však len určitým aspektom. V ostatnom čase sa rozširuje pojem do oblastí, ktoré s jej základným účelom – ochrana dôvernosti, dostupnosti a integrity informácií, nemajú veľa spoločného. Tieto oblasti si vyžadujú iné odborné znalosti, skúsenosti a postupy ako ochrana pred kyberútokom. Odpoveďou na aktuálnu situáciu je zamyslieť sa nad schopnosťami orgánov činnými v trestnom konaní, orientovať sa a efektívne kontrolovať kriminalitu v kybernetickom prostredí. Kedy, ak nie teraz?

Matej Síleš
manažér IT bezpečnosti
UPC Broadband Slovakia

Jednou z úloh kybernetickej bezpečnosti je viesť spoločnosť k tomu, aby kybernetický priestor bol vnímaný ako súčasť reálneho sveta, v ktorom každý jednotlivec nesie zodpovednosť za svoje konanie a podľa toho sa aj musí správať. Je dôležité zamerať naše aktivity na zvyšovanie tohto povedomia u používateľov vo všetkých vekových skupinách. Táto aktivita si vyžaduje čas, ale je nesmierne dôležitá.

Rastislav Janota,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Kybernetická bezpečnosť je striktne apolitická téma. Napriek tomu (vďaka tomu) sa týka naozaj nás všetkých rovnako. Zvyšovanie odolnosti každého z nás pred hrozbami v kybernetickom priestore je nevyhnutným predpokladom na zvyšovanie odolnosti celej spoločnosti. Na naozajstný pokrok v tejto situácii nám najviac chýba vzdelanie, čo je zároveň najviac a dlhodobo zanedbaná oblasť. Od vytvárania dobrého povedomia a znalosti kyberhygieny u všetkých obyvateľov Slovenska každého veku až po naozaj expertné vzdelávanie odborníkov v oblasti.