HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
25. – 27. JÚNA 2021

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Veľa strát prinieslo účinné riešenia

V roku 2021 sa priemerné globálne náklady na nápravu škôd spôsobených ransomvérovým útokom zvýšili na 1,5 milióna amerických dolárov, čo je viac ako dvojnásobok priemeru v predchádzajúcom roku. SNÍMKA: DREAMSTIME

TÉMA

Aj za výkonnými systémami stoja ľudia. A ako ľudia sme omylní. Preto musia na bezpečnosť myslieť vývojári a dizajnéri skôr, než čokoľvek zapoja a spustia. Security by design.

Štúdie opakovane a stále skúmajú príčiny toho, prečo dochádza k incidentom v kybernetickej bezpečnosti, následne finančným stratám, ohrozeniu činnosti organizácií a únikom dát.

Za rok 2020 reportuje spoločnosť IBM, že ľudská chyba je hlavnou príčinou až 95 percent bezpečnostných incidentov. Inými slovami, ak by došlo k úplnému odstráneniu ľudských chýb, 19 z 20 incidentov by sa nemuselo stať vôbec.

Bolestivé prebudenie

Uplynulá dekáda priniesla fascinujúci rozvoj digitalizácie. Finančný, priemyselný sektor, služby, školstvo, verejná správa, cloudové riešenia a aplikácie sa dostali do hviezdnych čísel.

Následok? Digitalizáciou stúpal a s množstvom automatizovaných činností rástol aj počet incidentov. Prvý bolestivý následok pocítili banky. Falošné transakcie, skopírované platobné karty, pokuty, súdne spory, vybielené účty. Stálo to peniaze.

Bankové straty zo začiatku minulej dekády v Európe, ktoré spôsobili neoprávnené kartové transakcie, sa odhadujú až na štyri miliardy eur.

Ako spojiť nespojiteľné

Profesionáli vychádzali z premisy „ak znížime počet zraniteľností, predídeme škodám“. Čiže čím menej zraniteľností, tým odolnejší systém. Pochopiteľné.

Rovnaké pochopenie si však vyžaduje fakt, že zručnosti a schopnosti používateľov výpočtovej techniky zaostávali za jej rozširovaním. Počínajúc manažérmi, zamestnancami a končiac zákazníkmi a klientmi.

Priestor hrozieb sa s digitalizáciou jednoducho zväčšoval a bolo nutné na to reagovať. Chrániť systémy, dáta a tak zákazníkov či klientov.

Niekde tu vznikol pojem privacy by design, ktorý vyžadoval špecificky zabudovať ochranu súkromia už do návrhu aplikácie, procesu alebo činnosti systému či obchodného procesu. Údaje tak majú byť chránené štandardne a trvalo udržateľným spôsobom vo všetkých procesoch.

Ako to ešte lepšie spojiť

Pôvodcom iniciatívy privacy by design sa tak stal súkromný sektor, ktorý vytvoril tlak na bezpečnostné štandardy. Základná bezpečnosť postúpila na úroveň regulácie, čo znamená, že bola „vynútená“ zákonom.

Požiadavka na prijatie legislatívy bola formulovaná v roku 2014 a štyri roky nato uzákonená ako nezabudnuteľné Nariadenie GDPR.

Trh, ktorý nemôže čakať na zákon, ale musí dbať o svoju dôveryhodnosť a bezpečnosť, však sformuloval vlastnú mantru – mysli na bezpečnosť, už keď niečo navrhuješ. Princíp security by design začali programátori a vývojári používať bez toho, aby ho niekde videli napísaný alebo určený.

A ako uviesť do praxe

Zraniteľnosť systémov vychádza z princípu ľudskej podstaty. Všetky zraniteľnosti vznikajú pri návrhu, všetky incidenty sú výsledkom zraniteľnosti.

Omylní sú inžinieri, programátori aj architekti systému, a keďže sme si toho vedomí, dokážeme sa na to pripraviť a sme povinní urobiť maximum opatrení. Softvér aj hardvér musia byť navrhnuté s cieľom myslieť na bezpečnosť.

Prístup security by design nie je všeliek, ale veľmi účinný liek. Týka sa to jednoduchej používateľskej aplikácie aj jadrovej elektrárne. Súčasťou každého procesu je testovanie, tisíce a tisíce testov, až je pravdepodobnosť zraniteľnosti zanedbateľná.

A prečo sú bezpečáci takí posadnutí? Vedia totiž, že aj keď sa niečo spustí, aj tak ešte niekde môže byť chyba.

Dekáda potom

„Či je to softvér pre energetické spoločnosti, alebo pre banky a ďalších európskych klientov, už pri dizajne riešení premýšľame nad tým, ako ich vyrobiť efektívne a zároveň čo najbezpečnejšie,“ potvrdzuje Richard Schwartz, obchodný riaditeľ Unicorn Systems SK.

V praxi to znamená už pri návrhu zvažovať viacero vrstiev ochrany, ktoré zaisťujú dôvernosť, dostupnosť a integritu aplikácií či informácií v nich. „Keďže to robíme už vo fáze dizajnu riešenia, nevyčísľujeme rozdiel prácnosti pre vývoj a testovanie, snažíme sa skrátka dodať čo najbezpečnejšie riešenie.“

> Security by design chápeme ako prístup k návrhu a tvorbe informačných systémov.
>
> **Ľuboš Kováčik,** solution architekt spoločnosti Softec

Je totiž oveľa jednoduchšie zabezpečiť splnenie bezpečnostných požiadaviek počas návrhu. Ak sa opomenú, ich realizácia neskôr je výrazne prácnejšia alebo sa bez zásahu do architektúry nedajú realizovať.

Nový vek bezpečnosti

Nástupom cloudových platforiem a internetu vecí nastal zásadný posun vo vnímaní zodpovednosti za nasadzovanie a prevádzku informačných systémov. Najvýraznejšie sa to prejavuje pri systémoch dodávaných formou softvér ako služba.

Dodávatelia sa tu stávajú spoluzodpovední až plne zodpovední za bezpečnosť informačných systémov aj za ďalšie požiadavky, akými sú vysoká dostupnosť, výkonnosť a s nimi súvisiaci monitoring. Zároveň sa táto téma stáva už aj súčasťou zmlúv.

„Bezpečnosť je integrálnou súčasťou každej etapy životného cyklu tvorby informačného systému. Security by design chápeme ako prístup k návrhu a tvorbe informačných systémov,“ potvrdzuje Ľuboš Kováčik, solution architekt spoločnosti Softec. Dôsledná aplikácia takého prístupu zahŕňa zníženie rizika samotného útoku, schopnosť jeho detekcie a redukciu prípadných negatívnych následkov. Zároveň sa táto téma stáva už aj súčasťou zmlúv.

Keď to zažijete

Ukážkovou oblasťou pre pojem security by design je vývoj nových áut, ktoré sú pripojené do internetu. „Ransomvérový útok v rýchlosti 135 kilometrov za hodinu môže mať negatívny dosah na bezpečnostné systémy vozidla, a teda aj jeho posádku,“ vysvetľuje Martin Fabry, audítor kybernetickej bezpečnosti.

Svet prevádzkových technológií je však konzervatívne impérium – vyžaduje si dostupnosť, spoľahlivosť, stabilitu a teraz musí v krátkom čase akceptovať extrémne dynamické požiadavky kybernetickej bezpečnosti. Pre priemysel je security by design ďalší kvalitatívny parameter, ktorý sa stáva nevyhnutným.

Už nebudete chcieť inak

„Legislatíva a požiadavky zákazníkov vytvárajú tlak na výrobcov riadiacich systémov na integráciu bezpečnostných opatrení do produktu. V prípade predchádzajúcich generácií sa dodatočné opatrenia musia dopracovať,“ vysvetľuje Martin Fabry.

V budúcnosti si všetky produkty budú vyžadovať bezpečnostnú certifikáciu, či už ide o ochranu spotrebiteľov pred zbieraním dát z ich domácich spotrebičov, alebo priemyselnú linku s využitím umelej inteligencie.

Nech majú produkty akékoľvek určenie, používatelia novej generácie budú požadovať, aby boli funkčné, pekné a bezpečné v digitálnom svete.

DEŇ NA INTERNETE?

24 000
škodlivých mobilných aplikácií je blokovaných na internete

30 000
webových stránok je hacknutých

94 percent
malvéru sa šíri mailom

64 percent
organizácií má skúsenosť s kybernetickým útokom

Zdroj: bezpečnostné analýzy a štatistiky 2021, techjury.net

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti
CYBERARK
Flowmon A Kemp Company
MICRO FOCUS
SYNAPSA
paloalto NETWORKS
SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Čo nás učí rok 2021 a ako ďalej

Správcovia sietí a manažéri kybernetickej bezpečnosti revidujú škody aj prínosy pandemického roku. SNÍMKA: DREAMSTIME

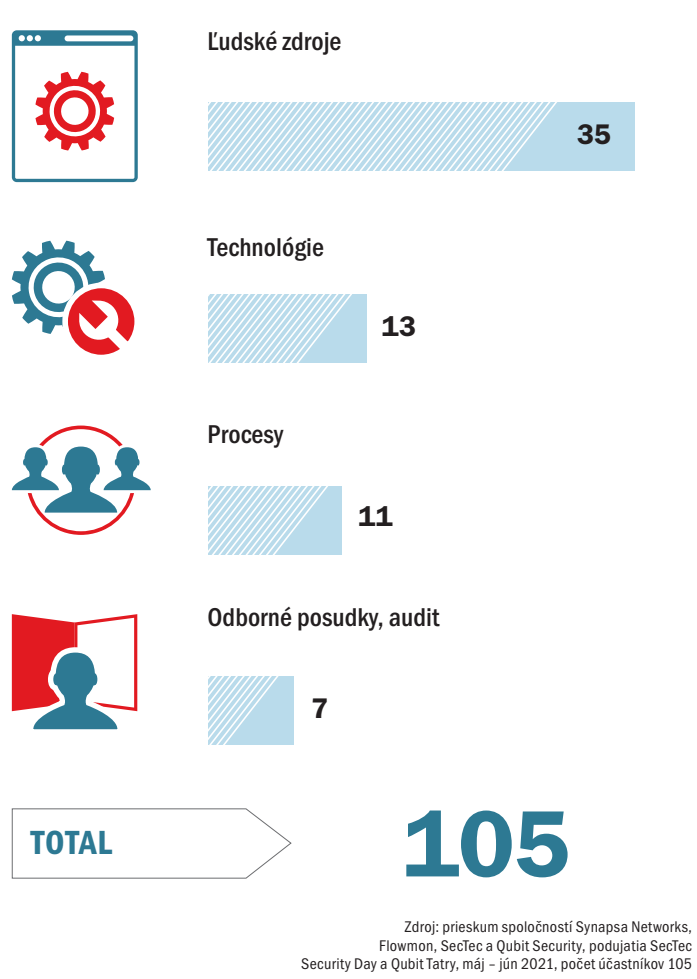
Prieskum sa realizuje medzi špecialistami a manažérmi v oblasti informačnej a kybernetickej bezpečnosti na Slovensku už druhý rok.

Výsledky prezentujú ucelený prehľad o tom, ako je odborná problematika vnímaná a aké majú účastníci reálne skúsenosti či očakávania. Interpretácia odpovedí nás inšpiruje vo vzdelávaní a budovaní povedomia o kybernetickej bezpečnosti.

Prieskum je anonymizovaný a súbežne sa realizuje na Slovensku a v Českej republike. Tohtoročný prieskum je ešte otvorený a zároveň po prvýkrát porovnáme výsledky s minulým rokom, čím budeme vedieť mapovať posun stavu aj očakávaní.

Roman Čupka, hlavný konzultant Flowmon a Kemp company a CEO Synapsa Networks

Ktorú z týchto potrieb vnímate v súčasnosti ako najdôležitejšiu na zabezpečenie prevádzky a posilnenie IT bezpečnosti vo vašej organizácii?



Zdroj: prieskum spoločností Synapsa Networks, Flowmon, SecTec a Qubit Security, podujatia SecTec Security Day a Qubit Tatry, máj – jún 2021, počet účastníkov 105

Vposlednom období sme sa naučili, že digitalizáciu je možné osvojiť si rýchlejšie, ako sa predpokladalo.

Spoločnosti sa od prvej vlny pandémie postupne začínajú zotavovať a obnovovať prevádzky. Nie vždy je však prioritou kybernetická bezpečnosť. Aj tu platí, že ju netreba podceňovať, keďže by mala byť bežnou súčasťou digitálneho spôsobu života. Pri zmierňovaní nových hrozieb musíme byť ostražití a pripravení na vznikajúce situácie.

Pred rokom veľa spoločností prekvapila povinnosť pracovať z domu a kvôli nedostatočnej príprave a neflexibilnej infraštruktúre museli situáciu riešiť „dočasnými“ záplatami. Často nákupom rôznych VPN riešení a cloud služieb, ktoré boli aktuálne na trhu dostupné za prijateľné ceny a spĺňali ako-tak požadovaný štandard.

Odohrávalo sa to rýchlo, spravidla bez detailnej analýzy, keďže primárnym cieľom bolo obnoviť prevádzku a znížiť straty na minimum. Až čas preukázal vhodnosť zvoleného riešenia a vyzdvihol problémy vznikajúce s integráciou, so správou a prípadne škálovateľnosťou novej technológie.

Zmeny v „zabehnutej“ architektúre sa robia ťažko a pravidelne prinášajú mnohé negatívne vstupy, ktoré bránia ráznej zmene. Teraz po miernom upokojení pandémie nastal ideálny čas na IT hygienu a optimalizáciu.

Odstránením zbytočných technológií a procesov taktiež eliminujeme množstvo vektorov, ktoré môžu útočníci zneužiť. Nemá zmysel prevádzkovať technológiu, ktorá len zamestnáva správcov, a tak im uberá čas venovať sa dôležitejším úlohám. Ako zvyknú ironicky hovoriť: „Neexistuje krajší pocit, ako keď

> Odstránením zbytočných technológií a procesov taktiež eliminujeme množstvo vektorov, ktoré môžu útočníci zneužiť.

mám na starosti desiatky technológií.“

Svet, ako sme ho poznali, sa už do „normálu“ nevráti.

Okrem výberu správnej bezpečnostnej platformy, ktorá vám pomôže v procese optimalizácie bezpečnostných riešení, nesmieme zabúdať ani na disciplínu, vhodne nastavené procesy a pravidelné vzdelávanie zamestnancov.

Veľa ľudí pracujúcich na diaľku nikdy predtým takto nepracovalo. Možno si ani neuvedomujú veci, ktoré bežne robia a ktoré môžu zbytočne spôsobiť neúmyselné riziká. Ako príklad možno uviesť používanie silných hesiel a ich pravidelná zmena, používanie viacfaktorového overenia, správu a zabezpečenie zariadení, oddelené osobné a firemné účty a iné.

Martin Vivodik, bezpečnostný konzultant Clico, s. r. o.

SLOVENSKO

Či už ide o verejnú správu, zdravotníctvo alebo malé a stredné firmy a inštitúcie, reálna implementácia zákona o kybernetickej bezpečnosti je pre 90 percent organizácií úlohou, ktorá dramaticky presahuje ich možnosti a kapacity.

Dosahovaný súlad s požiadavkami zákona o kybernetickej bezpečnosti vo väčšine týchto organizácii je päť percent.

Miera úspešnosti phishingových kampaní – simulácia podvodného emailu – je 85 percent. V dvadsiatich percentách prípadov je manažér kybernetickej bezpečnosti priamo podriadený manažmentu, a nie IT oddeleniu.

Manažér kybernetickej bezpečnosti pri budovaní systému kybernetickej bezpečnosti spracúva a riadi desiatky rôznych dokumentov a úloh, akými sú stratégia, politiky, smernice, registre, pracovné postupy a implementácia opatrení. Každý dokument musí byť zároveň preskúmaný, vytvorený, pripomienkovaný, schválený, implementovaný a kontrolovaný.

Väčšina organizácií používa na riadenie projektov základné nástroje, akými sú Word, Excel a Outlook. Ak však nimi v praxi chceme riadiť kybernetickú bezpečnosť, spôsobujú nasledujúce problémy:

- zložitosť aktualizácie jednotlivých častí
- chýbajúci kontext a súvislosti, vzťahy
- nízka úroveň kolaborácie
- nejasné riadenie jednotlivých aktivít
- chýbajúce dodržiavanie postupov
- chýbajúca integrácia procesného a technického sveta
- nízka kontrola efektívnosti

Riadenie dokumentov a úloh tak v praxi môže trvať viac ako 12 mesiacov.

S kvalitným nástrojom na riadenie kybernetickej bezpečnosti sa znižujú náklady na dosiahnutie súladu s legislatívou a eliminujú sa chyby a nejasné výstupy, čím sa vyvarujete predražených konzultácií.

A ako skontrolovať, či je takýto systém riadenia profesionálny? Je škálovateľný, priebežne vyhodnocuje stav bezpečnosti a používateľa sprevádza celým procesom.

Peter Tyko, riaditeľ divízie IT bezpečnosti ALISON Slovakia

SVET

Zmeny v tom, ako žijeme, pracujeme a vzdelávame sa, vytvorili deliacu čiaru, ktorá aj v kybernetickej bezpečnosti definitívne oddelí fungovanie vecí pred pandémiou a po nej.

Koncept práce z domu aj exponenciálny nárast rýchlosti prechodu do cloudu priniesli nižšiu transparentnosť ekosystému kybernetickej bezpečnosti, zníženie možnosti kontroly koncových zariadení a s tým spojené rôznorodejšie možnosti útokov pre potenciálnych útočníkov.

Počet úspešných útokov voči organizáciám v roku 2020 sa zvýšil o 5,5 percenta a prekonal svetový rekord za posledných šesť rokov.

Následok útoku so zneužitím vedie k väčším obavám spojeným s rizikom, ktoré predstavuje dodávateľský reťazec pre jednotlivé organizácie.

Táto situácia a výzvy sa, samozrejme, preniesli aj do roku 2021.

78 percent spoločností očakáva ďalší útok na dodávateľský reťazec v rozsahu podobnom útoku na SolarWinds.

88 percent organizácií zvyšuje rozpočet na bezpečnosť. Ako najčastejší dôvod uvádza zvýšenie využívania cloudových služieb.

84 percent organizácií sa stalo za posledné dva roky cieľom úspešného kybernetického útoku s kompromitáciou emailu ako najčastejším spôsobom útoku.

Daniel Suchý, špecialista pre kybernetickú bezpečnosť, Aliter Technologies, a. s.

Príležitosti aj hrozby sú u nás všade

ANKETA

Najväčšie IT podujatie na Slovensku. Takou bola jarná ITAPA 2021, kde sa stretávajú stovky expertov, manažérov, politikov a vlastne celá IT komunita. Aj na tomto odbornom podujatí sa s mimoriadnou naliehavosťou stáva dominantnou témou kybernetická bezpečnosť. V špeciálnom vydaní tradičnej ankety sa rečníkov a účastníkov pýtame: Akú výzvu predstavuje kybernetická bezpečnosť pre vašu kompetenciu?

Vladimír Lengvarský,
minister zdravotníctva Slovenskej republiky

Otázka je ťažká a bezpečnosť je extrémne dôležitá. Ale ako všetci dobre vieme, investičný dlh v nemocniciach je obrovský. Treba toho veľa doháňať, a tak, samozrejme, keď si nemocnice mali vybrať, či investujú do nového prístroja alebo do kybernetickej bezpečnosti, tak väčšinou zvolili to prvé. Preto tento dlh budem musieť nejakým komplexným spôsobom riešiť.

Našou úlohou je nájsť komplexné riešenie, ktoré budeme aplikovať vo všetkých nemocniciach a u poskytovateľov zdravotnej starostlivosti, aby sme dáta precízne chránili. Pracujeme na tom spolu aj s Národným centrom zdravotníckych informácií. Verím, že sa to podarí.

Marek Antal,
štátny tajomník Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

Prioritou je vzdelávanie v kybernetickej bezpečnosti a uvedomenie si rizík, ktoré vyplývajú z toho, ako používame informačnú techniku. Má to dve zásadné oblasti – potrebujeme veľa odborníkov na kybernetickú bezpečnosť a zároveň informovať o tejto oblasti všetkých používateľov. Aby sa nestávali obeťou kybernetických útokov a aby rozumeli, že to, čo robia za počítačom, zanecháva stopy. V širšom kontexte je to riziko používania informačných technológií a s tým súvisia hybridné hrozby, akými sú napríklad hoaxy.

Stále je aktívna generácia, ktorá bola vychovaná tak, aby dôverovala inštitúciám a médiám a rovnako sa správa aj na internete. Nechápu, aké hrozby v súvislosti s používaním výpočtovej techniky hrozia. Ak chceme, aby populácia používala informačné systémy a spoločnosť bola oveľa viac digitalizovaná, musíme upozorňovať na to, že hrozby budú niekoľkonásobne väčšie. V blízkej budúcnosti musíme tejto téme priradiť dôležitosť, sústrediť sa na ňu a musíme začať so vzdelávaním.

„Na pomyselnej stupnici o 1 po 10 vnímam úroveň povedomia o kybernetickej bezpečnosti na Slovensku tak na hodnote 3.“

Ladislav Miko,
vedúci Zastúpenia Európskej komisie v SR

Kybernetická bezpečnosť je kľúčová. Sme si toho vedomí nielen na európskej úrovni, ale aj na národných úrovniach a máme už aj prvé skúsenosti, čo sa stane, ak nie je dostatočne zabezpečená. V súčasnom globalizovanom svete je evidentná snaha získavať výhody práve tým, že nejakým spôsobom ohrozím súpera práve v oblasti kybernetickej bezpečnosti.

Pokiaľ sa tomu nebudeme efektívne brániť a od samého počiatku to nebudeme veľmi intenzívne riešiť, tak nás to dostáva do strategickej nevýhody. Prístup ku kybernetickej bezpečnosti je zásadná vec, a preto ju treba systematicky budovať nielen na úrovni národných štátov, ale aj v prepojenej Európe.

Ján Kyselovič,
generálny riaditeľ Centrum vedecko-technických informácií SR

Dnes treba kybernetickej bezpečnosti venovať omnoho väčšiu pozornosť. Potrebujeme systém, ktorý by zabezpečoval niekoľkonásobnú ochranu a nebol ohrozený nevedomosťou koncového používateľa. Poznám to prostredníctvom projektov, ktoré prinášajú nové patentové riešenia, alebo prostredníctvom patentov na lieky, ktorých hodnota môže presiahnuť 10 až 12 rádov. Práve v tejto oblasti chceme ponúkať úložiská pre tieto centrá alebo zdravotnícke startupy. Musíme vytvoriť chránenú databázu informácií našich pacientov, ktoré budú chránené nielen podľa nariadenia GDPR, ale aj vzhľadom na povahu a unikátnosť informácií.

Pre naplnenie spoločných cieľov v oblasti ochrany informácií a databáz je nutné vytvoriť optimálne podmienky hardvérové, softvérové, bezpečnostné, školenie pracovníkov a zároveň pozitívne poznatky a zistenia transformovať do nových projektov a výziev. Cieľom musí byť vytvorenie komplexnej ochrany každého pracoviska. Ak sa snažíme prichádzať s novými nápadmi a kreujeme príležitosti pre budúce a inovatívne formy spolupráce, tak takýto cieľ je úplne prirodzený.

Matej Šalmík,
riaditeľ odboru vzdelávania, podpory a medzinárodnej spolupráce Národné centrum kybernetickej bezpečnosti SK-CERT

Podliehame enormnej informačnej záťaži a nikto z nás nedokáže efektívne spracúvať informácie v reálnom čase. Kvalitná analýza si vyžaduje hlbokú expertízu, technologické zázemie a dobre nastavené procesy. Potrebujeme preto vytvoriť mechanizmus zdieľania informácií, vedomostí a skúseností na báze vzájomnej dôvery a rešpektu.

Keď neviete, že niečo existuje, alebo ani o tom, že to máte vedieť, stávate sa extrémne zraniteľným. V kybernetickej bezpečnosti nadobúda toto tvrdenie až bytostný význam. Ak neviete o hrozbách, nechávate otvorené dvere útočníkom. Spolupráca nás posúva od pasívnych obetí k zodpovedným používateľom.

Martin Florian,
riaditeľ sekcie kybernetickej bezpečnosti Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

Hlavnou výzvou kybernetickej informačnej bezpečnosti vo verejnej správe, a týka sa to aj sektorov, ktoré nie sú primárne v našej gescii, je na prvom mieste nedostatok odborne zdatných, motivovaných spôsobilých ľudí. Chýbajú bezpečnostní architekti, ktorí vedia poňať veci v kontexte, v technickej, logickej a biznis architektúre, a chápu celý životný cyklus vyvíjania nových riešení.

Na trhu práce nie sú odborníci pre dátovú analytiku a bezpečnosť, ľudia, ktorí vedia chrániť dáta, dešifrovať ich a včas detegovať hrozby a riešiť ich vo včasnom zárodku skôr, ako „spôsobia požiar“. Z legislatívneho hľadiska nám chýbajú aj odborníci, ktorí vedia napísať zákon a vyhlášku tak, aby boli prepojené s technickou realizáciou a uskutočniteľné.

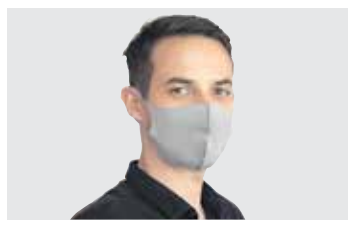
V súčasnosti nám chýba minimálne 1 200 pracovníkov pre kybernetickú a informačnú bezpečnosť v týchto profiloch. Keby tu boli hneď, teraz a dnes, tak nemajú šancu byť nezamestnaní, a v priebehu niekoľkých kvartálov narastie tento nedostatok na dve tisícky.

Radoslav Danilák,
spoluzakladateľ a CEO Tachyum

Kybernetická bezpečnosť je čoraz kritickejšia a viac sa na ňu sústreďuje aj pozornosť médií. Verejnosťou nedávno „pohli“ aj informácie o odpočúvaní európskych predstaviteľov. Európa potrebuje digitálnu suverenitu a kybernetická bezpečnosť je jedným z jej základných pilierov.

Umelá inteligencia sa stáva hlavným nástrojom aj v kybernetickej vojne, pretože vie rýchlejšie reagovať. Napríklad umiestnenie jadrových zbraní skracuje čas na obrannú reakciu na taký krátky čas, že v niektorých prípadoch už nie je možné, aby ľudia rozhodli dostatočne rýchlo.

V smerovaní našej spoločnosti predstavuje kybernetická bezpečnosť vysokú prioritu. V datacentrách sa na jednom našom čipe budú spracúvať údaje rôznych firiem, ktoré môžu byť medzi sebou konkurentmi. Náš procesor má vstavané mnohé funkcie na zvýšenie bezpečnosti aplikácií.



Robert Lipovský,
špecialista na kybernetické hrozby Eset

Hranice hrozieb sa začínajú rozplývať. Predpokladáme, že budú pribúdať hybridné útoky, ktoré využívajú techniky pokročilých pretrvávajúcich hrozieb a zároveň sú finančne motivované. Už v súčasnosti monitorujeme niekoľko takých skupín a útočia už nielen na korporácie, ale v podstate na akúkoľvek spoločnosť.

Treba si priznať, že útočníci majú výhodu, pretože si vedia otestovať, či nejaké antimalvérové riešenie deteguje ich škodlivý softvér skôr, ako ho vypustia. A až potom podniknú útok. Takže im stačí nájsť jeden spôsob, ako preniknúť do siete, zatiaľ čo my v pozícii ochrany musíme zablokovať všetky možné kanály. Je to možné iba viacvrstvovou úrovňou ochrany, takže stále vyvíjame nové technológie a nové vrstvy ochrany, aby sme sa vedeli brániť vylepšeným technikám útočníkov.

To je jedna časť, tá technická, a to druhou je vzdelávanie. Naša práca je neustále vysvetľovať a argumentovať aj profesionálom vo firmách, že tieto hrozby sa týkajú aj ich. Myslím si, že za ostatné roky sme už v tomto smere spravili pokrok, ale nepoľavujeme a pokračujeme.

„Za našu najväčšiu výzvu považujem stále vysvetľovať, aby si všetci uvedomili, že neexistujú hrozby, ktoré by sa nás netýkali.“

Ján Grujbár,
výkonný riaditeľ Aliter Technologies, a. s.

Za posledné obdobie sledujeme nárast počtu úspešných kybernetických útokov proti rôznym organizáciám. Súvisí to s externými vplyvmi aj s postojom organizácií. Často neprikladajú kybernetickej bezpečnosti adekvátnu dôležitosť, keďže sa obávajú vysokých nákladov s dlhou dobou návratnosti alebo potreby budovať špecializovaný tím. Nemali by to však vzdávať. Mali by mať spoľahlivého partnera, ktorý poskytuje kybernetickú bezpečnosť ako službu, pýtať sa a verifikovať referencie. Tento prístup umožní aj tej najmenšej firme venovať sa prioritne podnikaniu v bezpečnom prostredí.

Nové príležitosti a s nimi spojené ohrozenia sa budú objavovať tak, ako sa bude ďalej vyvíjať spoločnosť, technológie a s tým spojené požiadavky na trhu. Úlohou kybernetickej bezpečnosti vždy bolo a bude prinášať riešenia na znižovanie identifikovaných rizík a tak umožňovať rozvoj a rast organizácií.

Peter Matej,
šéfredaktor incident.sk

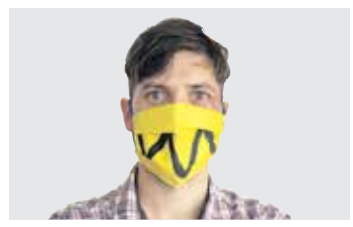
Najväčšia výzva v oblasti kybernetickej bezpečnosti je vzdelávanie. Je tu obrovská priepasť medzi odborníkmi špecialistami a bežnými občanmi, ktorí používajú technológie dennodenne. Keď nedostaneme vzdelávanie medzi deti do škôl a postupne až na vysoké školy, tak priepasť sa bude len zväčšovať.

V súčasnosti ešte nemáme postačujúci počet učiteľov s touto odbornosťou a celá spoločnosť by ocenila IT odborníkov, ktorí by momentálne mohli pomôcť školám. Nie je to ich úlohou, ale ich ochota rýchlo dovzdelávať učiteľov by nám pomohla pri rozbehu vzdelávania. Nedá sa tak kontinuálne suplovať úloha školstva, ale teraz, v tejto chvíli by to pomohlo.

Vojtech Németh,
technologický riaditeľ Vnet

Chýba nám uvedomenie. Ransomvérový útok na Colonial Pipeline v Spojených štátoch sa dotkol aj bežných občanov, ktorí zrazu nemohli natankovať, lebo sieť bola odstavená. Možno by sme na Slovensku pochopili význam kybernetickej bezpečnosti až vtedy, keby sme sa ocitli v podobnej situácii. Kybernetická bezpečnosť je pre väčšinu populácie iba abstraktný pojem. O útokoch síce počujeme z médií, ale ak ich nezažijeme „na vlastnej koži“, neuvedomujeme si ich dôsledky.

Až keď si firmy a ľudia uvedomia dôležitosť kybernetickej bezpečnosti, potom už nebude problémom presvedčiť ich, že vzdelávanie je nevyhnutným krokom, a začať s ním na všetkých úrovniach.



Peter Kulich,
výkonný riaditeľ Slovensko.Digital

Považujeme za našu povinnosť dávať vláde otázky k tomu, aká je celková stratégia Slovenska v kybernetickej bezpečnosti a ako ju efektívne uchopiť. Počínajúc celkovou stratégiou, cez otázky, aké technológie používať, aké prístupy uplatniť, až po vzdelávanie ľudí. Lebo nestačí byť dobrý iba v tom, že sa nakúpia moderné nástroje a technológie, ale dôležitejšie je mať ľudí, ktorí s nimi vedia aj pracovať. Takže sa pýtame na strategické aktivity, zaujíma nás denná operatíva, nástroje, ľudia.

Jedna z dôležitých pripomienok k plánu obnovy, ktorú sme dávali, bola práve v oblasti kybernetickej bezpečnosti. Chýba nám tu kontinuálny plán vzdelávania, spolupráca s vysokými školami, spolupráca so súkromným sektorom a zavedenie napríklad nových študijných odborov, rekvalifikačných kurzov. Navrhujeme zaviesť procesy alebo reformy, ktoré budú dlhodobejšieho charakteru a dosahu. Napríklad zaviesť možnosť vzdelávania, a to aj pre ľudí, ktorí už sú po strednej alebo vysokej škole a chceli by sa v kybernetickej bezpečnosti vzdelávať alebo absolvovať kurzy.

„Reagovali sme na to, že každý hovorí, že na Slovensku je nedostatok odborníkov v kybernetickej bezpečnosti, ale v pláne obnovy sme vôbec nezachytili, aké aktivity budú tento nedostatok systémovo riešiť.“