NEXTECH

KYBERNETICKÁ BEZPEČNOSŤ PRE FIRMY

PREVENCIA
Ako sa pripraviť a priebežne kontrolovať stav ochrany

OCHRANA
Aké útoky hrozia firmám a ako sa pred nimi chrániť

REAKCIA
Čo robiť ak už k útoku došlo, ako reagovať

ESET.SK/FIRMY

PROTECT

BIZNIS RIEŠENIA NOVEJ GENERÁCIE

Spravujte IT bezpečnosť vašej firmy odkiaľkoľvek prostredníctvom cloudovej konzoly ESET PROTECT. Nové balíky bezpečnostných riešení prinášajú progresívnu ochranu pre firmy všetkých veľkostí.

NOVÉ BALÍKY FIREMNÝCH BEZPEČNOSTNÝCH RIEŠENÍ

ESET PROTECT Advanced

Viacvrstvové zabezpečenie koncových zariadení s ochranou pred ransomvérom a zero-day hrozbami, doplnené o riešenie na šifrovanie celých diskov.

ESET PROTECT Complete

Rozširuje balík bezpečnostných riešení Advanced o ochranu firemných cloudových aplikácií a e-mailovej komunikácie.

ESET PROTECT Enterprise

Komplexný bezpečnostný balík pre veľké firmy s proaktívnou ochranou pred neznámymi hrozbami a s riešením na detekciu a nápravu bezpečnostných hrozieb (EDR).

SLOVO NA ÚVOD

Pripravme sa na budúcnosť

O dôležitosti riešenia otázky kybernetickej bezpečnosti vo firmách vo všeobecnosti vládne už dostatočné povedomie, ale z hľadiska praktických krokov, konkrétnych opatrení, rozpočtu, ľudí, procesov, stavu technickej pripravenosti atď. je to stále poslabšie. Týka sa to pritom každej firmy či organizácie a otázkou nie je, či ju zasiahne nejaký kybernetický útok, ale kedy sa to udeje. Potom to je už len otázka času. Následná bezpečnostná udalosť preverí slabé miesta a pripravenosť danej organizácie reagovať, eliminovať škody a znovu rozbehnúť svoju prevádzku. Súvisiace škody pritom nemajú len ekonomický charakter ale aj reputačný, ktorý je dôležitý až do takej miery, že môže ohroziť budúcu (ne)existenciu danej organizácie. Preto je kriticky dôležité venovať pozornosť kybernetickej bezpečnosti ešte predtým, než sa niečo udeje, a nie až potom. Ako sa hovorí: „Budúcnosť patrí pripraveným."

Problematika kybernetickej bezpečnosti je však veľmi komplexná. Vektory útoku prebiehajú na viacerých perimetroch, cez rôzne kanály, médiá, zariadenia. Dôležitá nie je len technická stránka zabezpečenia, ale najmä pracovníci, ktorí vďaka sociálnemu inžinieringu bývajú často tým najslabším článkom. Dôležitá je príprava a prevencia a rovnako tak schopnosť rýchlo sa spamätať z útoku, odstrániť následky a znovu naštartovať biznis. Rovnako je dôležité riešiť otázku právnej zodpovednosti za škody a legislatívneho súladu. Našťastie všetky tieto aspekty sú už známe, podchytené a špecializovaní partneri sú pripravení pomôcť firmám v zvládnutí týchto úloh.

Pripravili sme pre vás komplexnú publikáciu, ktorá vám pomôže zorientovať sa v tejto problematike a pripraviť sa tak, aby vás budúcnosť nezastihla nepripravených.

Inšpiratívne čítanie vám praje

OBSAH:

TECHNOLÓGIE

Prečo je kybernetická bezpečnosť taká dôležitá 5
Aký je aktuálny stav 7
Motivácia 9
Svet optikou hackera 10
Ofenzívna bezpečnosť:
O hackeroch na vašej strane 12
Útoky DDoS 14
Ochrana pred útokmi ohrozením
firemného e-mailu 16
Druhy kybernetických útokov 18
Ransomvér je neutíchajúca hrozba. Ako sa brániť? 21
Zero trust 22
Bezpečnosť pri home office 24
Ako prežiť kyberútok 26
Ako sa zbaviť hrozby výpadkov 28
Zabezpečenie počítačov a ďalších zariadení 30
Využívanie vlastných zariadení
na pracovné účely (BYOD) 34
Zabezpečenie mobilných zariadení 36
Havarijný plán, reakcie na incidenty,
postup obnovenia fungovania IT 39
Zabezpečenie údajov 40
Zabezpečenie podnikovej siete 42
Prístup do Wi-Fi 46
Bezpečnosť v cloude 48

MANAŽMENT

Manažment informačnej bezpečnosti 52
Prvými krokmi k bezpečnosti sú audit a koncepcia 55
Bezpečnostný audit 56
Produkty a riešenia HP na bezpečnú
a efektívnu prácu 58
Bezpečnostná politika 61
Analýza hrozieb, potenciálnych rizík
a identifikácia zraniteľných miest 64
S hackermi treba bojovať ich
vlastnými zbraňami 66
Manažér kybernetickej bezpečnosti 68
Sken (testovanie) siete 69
Ako predísť pomste zamestnancov 70
Služba riadenia zraniteľností dáva zmysel
len v povolaných rukách 72
IT bezpečnosť sa presúva do oblakov,
ESET ponúka cloudové riešenie 74
Aké sú bezpečnostné riziká a aké opatrenia
by mali prijať zamestnávatelia 76
Zodpovednosť za legálny softvér 78
Poistenie kybernetických rizík 80
Vynútenie dodržiavania bezpečnostných politík 82

LEGISLATÍVA

Požiadavky na ochranu osobných údajov 84
Ochrana osobných údajov 86
Povinnosti a zodpovednosti v oblasti legislatívy
a manažmentu kybernetickej bezpečnosti 89
O rizikách úniku dát aj legislatíve 90

VZDELÁVANIE

Prečo je vzdelávanie v IT dôležité? 94
Školenie zamestnancov 96
Clashing: efektívne vzdelávanie
v kybernetickej a informačnej bezpečnosti 97
Vyžaduje vzdelávanie v IT slovenská legislatíva? 98
Aké možnosti vzdelávania môže firma využiť? 99
Zoznam partnerov 102

TECHNOLÓGIE

PREČO JE KYBERNETICKÁ BEZPEČNOSŤ TAKÁ DÔLEŽITÁ

Či sa nám to páči, alebo nie, žijeme v dvoch svetoch, v tom reálnom, fyzickom a vo virtuálnom. Obidva svety sú navzájom prepojené, čo sa stane v jednom, prejaví sa v tom druhom a naopak. Chcete príklad? Zoberme si typický virtuálny svet, sociálne siete. Informácie v nich sú digitálnymi stopami nášho reálneho sveta, dávame tam informácie o našich udalostiach, aktivitách, o našich záujmoch a zážitkoch, o našich dobrých aj zlých chvíľach. A naopak, práve informácie, ktoré nám ponúka virtuálny svet, na nás vplývajú fyzicky, pociťujeme radosť z úspechu našich známych, o ktorých nás informujú na sociálnych sieťach, prípadne smútok, občas možno hnev, ak sme svedkami negatívnych príspevkov. A možno nás to ovplyvní do takej miery, že to zmení náš postoj k reálnemu svetu a začneme v ňom fungovať inak.

V prípade virtuálneho sveta nehovoríme len o sociálnych sieťach. Ten virtuálny svet sa nás dotýka aj v rámci nášho pracovného života. Väčšina z nás pracuje s počítačom, prípadne s inými prostriedkami informačných technológií. Pracujeme s nimi v kanceláriách, pri home office, na cestách, využívame rôzne prostriedky na to, aby sme vedeli plniť svoje pracovné povinnosti.

Náš život vo fyzickom svete sa riadi podľa pravidiel, fyzikálnych, bezpečnostných, firemných a podobne. Tieto pravidlá nám hovoria o tom, ako sa správať tak, aby sa nám niečo nestalo, prípadne aby sme nespôsobili nehodu či škodu na majetku aj inej osobe. Zdá sa nám samozrejmé a logické, že je riskantné pohybovať sa po tmavých uličkách a prechádzať cez cestu bez toho, aby sme sa uistili, či môžeme bezpečne prejsť na druhú stranu ulice.

Rovnako ako sa riadime zásadami bezpečného správania sa v reálnom svete, platia zásady bezpečného správania sa aj v tom virtuálnom. Ale aké to sú? Čím sa riadiť a ako postupovať, aby sme dokázali ochrániť seba a takisto nášho zamestnávateľa? A naopak, ako zabezpečiť z pohľadu zamestnávateľa to, aby sa zamestnanci správali bezpečne? V reálnom svete je to jasnejšie, máme pravidelné školenia BOZP, požiarnej ochrany, v niektorých spoločnostiach aj s nácvikmi rizikových situácií. A pritom si možno ani neuvedomujeme, že aj v kybernetickej bezpečnosti platí, že človek je ten najkritickejší faktor. Môžem nakúpiť technické prostriedky, môžem mať interné smernice, ale ak to moji zamestnanci nebudú praktizovať vo svojom každodennom pracovnom živote, sú moje prostriedky vynaložené zbytočne. A ak nie sú pre mojich zamestnancov náplňou práce práve informačné technológie, je o to náročnejšie pre nich pochopiť riziká, ktoré práve tento virtuálny svet prináša. Je preto dôležité rovnako ako v prípade spomenutých školení BOZP a požiarnej ochrany poskytnúť zamestnanom takú formu vzdelávania, aby sa dokázali vyrovnať s touto problematikou a znížili tým kybernetické riziko a hrozbu kybernetického útoku u seba a aj u svojho zamestnávateľa.

Tu si možno poviete: „Veď my sme malá firma, pre kybernetických útočníkov nie sme zaujímaví, tieto útoky sa týkajú veľkých firiem." Omyl. Iste sa zhodneme na tom,

že nezáleží na veľkosti firmy, aby mala údaje a informácie, ktoré si cení a o ktoré by nechcela prísť. Alebo aby sa tieto informácie „stratili", prípadne aby ich získala konkurencia. To, že je firma malá, nehrá vo virtuálnom priestore žiadnu rolu. Vaši zamestnanci môžu dostať e-mail so škodlivým softvérom rovnako ako v korporáte. Môžu kliknúť na falošnú webovú stránku rovnako ako vo veľkej spoločnosti. Je preto dôležité, aby zamestnanci vedeli, že to nemajú robiť, že majú znalosti na to, aby dokázali takéto hrozby odhaliť a účinne sa proti nim brániť.

Ďalšia komplikácia je súčasná doba, keď sa presúvame z našich kancelárií do obývačiek, pracovní a keď čoraz častejšie pracujeme z domu. Kým vo firemných priestoroch sme mali tú výhodu, že naše informačné systémy boli zabezpečené firemnými prostriedkami, v našom domácom prostredí to tak vôbec nemusí byť. Je málo pravdepodobné, že si bežný používateľ doma zakúpi, nainštaluje a bude prevádzkovať bezpečnostné prvky v takom rozsahu, ako sú implementované vo firemnom prostredí. Takisto musíme brať do úvahy aj tú skutočnosť, že tieto bezpečnostné prvky treba prevádzkovať s využitím odborných znalostí, čo je v prípade bežných používateľov nereálne. A pritom riziko kybernetického útoku to vôbec nemení, či sme pripojení doma, v práci, alebo niekde na Wi-Fi. Vždy je to pripojenie do internetu so svojimi pozitívnymi, ale aj negatívnymi vlastnosťami a nástrahami. Je preto dôležité uvedomiť si práve tieto súvislosti a riziká, vedieť ich identifikovať, rozpoznať a podľa možností sa im úplne vyhnúť.

Ďalší problém, s ktorým sa môžeme stretnúť, je nedostatok odborníkov. Tu možno mnohí z vás spozornejú. Veď informatikov je určite dosť, aj susedov chalan je taký šikovný, aj program mi nainštaloval, aj zaseknutý papier vytiahol z tlačiarne... Tu si však musíme uvedomiť jeden zásadný rozdiel. Ako príklad môžeme použiť lekárov. Nie každý lekár je dentista, nie každý lekár má schopnosti a vedomosti na to, aby dokázal operovať mozog, prípadne zachraňovať životy na pohotovosti. Je preto opäť logické, že si napríklad problém s kolenom nedáme liečiť dentistovi a naopak, v prípade potreby zubného mostíka nepôjdeme k traumatológovi. Jednoducho každý lekár má svoju špecializáciu a práve táto špecializácia hovorí o tom, akú problematiku ovláda. Identický princíp platí aj v prípade odborníkov na informačné technológie. V praxi to znamená, že na každú oblasť IT existujú odborníci, ktorí sa danej oblasti venujú a ktorí nám vedia najlepšie pomôcť s prípadným problémom a jeho riešením. Ak hovoríme o kybernetickej bezpečnosti, aj na túto oblasť existujú odborníci. Logickým krokom preto bude, ak sa v prípade riešenia kybernetickej bezpečnosti obrátime práve na nich. Žiaľ, ako už bolo spomenuté, takýchto odborníkov je nedostatok. Uvažovať nad tým, že v prípade malej spoločnosti ho zamestnám ako interného zamestnanca, nie je vždy ekonomicky výhodné. A nehovoríme iba o pravidelnom mesačnom plate. Vývoj v oblasti kybernetickej bezpečnosti napreduje míľovými krokmi každým dňom, objavujú sa nové a nové hrozby, na ktoré treba reagovať. Pracovný život odborníka na kybernetickú bezpečnosť sa teda z veľkej časti skladá práve zo vzdelávania, ktoré sa nie vždy dá nájsť voľne na internete. A práve na to slúžia vysoko odborné školenia, ktoré však stoja nemálo peňazí, čo sú ďalšie náklady. Je preto rozumnejšie a ekonomicky výhodnejšie sa o takéhoto odborníka deliť s inými spoločnosťami a zdieľať tak finančné náklady. Výhodou okrem už spomenutej finančnej stránky je najmä skutočnosť, že v takomto prípade neplatím za konkrétneho človeka, ale platím za službu. Táto služba má zmluvne definované parametre, čiže mňa, ako prijímateľa tejto služby, nemusí zaujímať, aké sú náklady na strane dodávateľa služby.

Posledná, aj keď nemenej dôležitá oblasť pri téme kybernetickej bezpečnosti z pohľadu vzdelávania je práve chýbajúca potreba vzdelávať sa zo strany zamestnávateľov a zamestnancov. Ako sme spomínali v predošlej časti, je dôležité si uvedomiť riziká, ktoré nám v kybernetickom svete hrozia, a nemať postoj, s ktorým sa veľmi často stretávame: „Veď mne sa to nemôže stať." Žiaľ, v kybernetickej bezpečnosti platí, že nie je otázkou, či budeme cieľom a obeťou útoku, ale kedy. Ako sa s každým dňom objavujú nové a nové hrozby, je nevyhnutné sa kontinuálne vzdelávať, aby sme dokázali týmto hrozbám čeliť a úspešne sa im brániť. Našťastie na to nie sme sami, nie sme odkázaní na samoštúdium, internet, čo neprinesie požadovaný efekt, ale máme možnosť obrátiť sa na vzdelávacie inštitúcie a spoločnosti. Práve tie majú prostriedky, vedomosti a skúsených lektorov na to, aby nám vedeli problematiku kybernetickej bezpečnosti vhodne vysvetliť, a to pre rôzne úrovne našich znalostí. Dôležité je pritom zachovať kontinuitu a systematickosť vzdelávania, pretože práve toto je cesta a spôsob, ako sa pohybovať vo virtuálnom svete bezpečne.

QUBIT

AKÝ JE AKTUÁLNY STAV KYBERNETICKEJ BEZPEČNOSTI VO FIRMÁCH?

Zrejme by sa dalo jednoducho skonštatovať, že stav je – zaobalene povedané – neuspokojivý, a potom dodať, že by sme s tým mali niečo robiť. Môžeme donekonečna opakovať mantru, že kybernetická bezpečnosť sa týka každého a otázkou nie je, či sa kybernetický incident udeje, ale kedy sa udeje. Je to len otázka času. Môžeme rovnako poukazovať na štatistiky a čísla. Iba za posledných 12 mesiacov počet ransomvérových útokov vzrástol o viac ako 300 %. Útoky na kritickú infraštruktúru nabrali rozmery kybernetickej vojny. Len dva príklady z posledných týždňov: ransomvérový útok na prevádzkovateľa ropovodu Colonial Pipeline, ktorý na 5 dní ochromil dodávky pohonných hmôt na juhovýchode Spojených štátov, pričom posledný deň už viac ako 70 % čerpacích staníc v tejto oblasti bolo bez pohonných hmôt, alebo útok na írsky zdravotnícky systém, ktorý írsky premiér označil doslova za akt vojenského útoku. Máme platnú legislatívu v oblasti ochrany osobných údajov – zákon č. 18/2018 Z. z. o ochrane osobných údajov, zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti spolu s doplňujúcimi vyhláškami, zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe aj s vyhláškou č. 179/2020. Aj NBÚ vypracoval celkom solídny dokument s názvom Národná stratégia kybernetickej bezpečnosti na roky 2021 – 2025. Vznikli fungujúce útvary včasného varovania a pomoci organizáciám pri kybernetických útokoch ako SK-CERT a vládny CSIRT. Tak prečo potom odborníci ešte stále vyjadrujú znepokojnenie?
Dôvodov je viacero a sú navzájom prepojené.

1. Nedostatočné bezpečnostné povedomie u bežných ľudí

Ako vyplýva z prieskumu realizovaného začiatkom roka 2021 spoločnosťou Nielson, až polovica internetovej populácie na Slovensku nemá pojem kybernetická bezpečnosť zafixovaný ako osobné ohrozenie. Lenže tí ľudia sú alebo budú niekde zamestnaní a svoje zlozvyky a ľahostajnosť prenášajú do pracovného prostredia a napriek občasným školenia, ktoré sa (možno) v organizácii raz ročne uskutočnia, sú pre bezpečnosť svojho zamestnávateľa reálnou hrozbou.

2. Nedostatočný rozsah vzdelávania v oblasti kybernetickej bezpečnosti v školách

Spýtali ste sa svojich detí niekedy, čo o rizikách internetu v škole na hodinách informačných technológií preberajú? Pritom už školopovinné deti na prvom stupni ZŠ používajú mobilný telefón s pripojením do internetu. Požiadavky na dištančné vzdelávanie túto tému ešte viac vyhrotili. Stačí si pozrieť štátne vzdelávacie programy IT predmetov napríklad na stránkach ŠIOV a zistíme, že tam bezpečnosti veľa priestoru nevenujú, nehovoriac o skúsenostiach a schopnostiach učiteľov túto tému pútavo prezentovať. Ako huby po daždi nám rastú gymnáziá, ktoré nie sú technicky zamerané (a vlastne by ani nemali byť, veď na to máme odborné školy). Žiaci nemajú záujem ísť študovať „ťažké" predmety, nie sú motivovaní, a tak svoje rozhodnutie „odložia na potom", keď ukončia gymnázium. Odborné školy sa viac venujú programovaniu, prevádzke sietí, digitálnemu spracovaniu obrazu, ale len minimálne sociálnym a bezpečnostným dôsledkom digitálnej doby. Vysoké školy sa až teraz postupne spamätávajú a odbory zamerané vyložene na špecialistov v oblasti kybernetickej bezpečnosti sa len teraz budujú.

3. Nedostatok odborníkov v oblasti riadenia informačnej a kybernetickej bezpečnosti

Tento nedostatok je markantný teraz, keď sa končí obdobie, ktoré kritická infraštruktúra štátu mala na analýzu stavu bezpečnosti, vypracovanie a zavedenie bezpečnostných opatrení, či už v zmysle vyhlášky č. 362/2018 Z. z., alebo vyhlášky č. 179/2020 Z. z. „Zrazu" sa zistilo, že je potrebných rádovo v tisíckach viac profesionálov, ktorí sú odborne, technologicky, procesne a aj právne podkutí v oblasti kybernetickej bezpečnosti a boli by vhodní na post manažéra kybernetickej bezpečnosti, ktorý je pre organizácie kritickej infraštruktúry „povinný". Nehovoríme o administrátoroch, technikoch IKT, cloudových špecialistoch. Všetka česť im a ich práci. Chýbajú však ľudia, ktorí by dokázali kybernetickú bezpečnosť riadiť ako celok. Na to je potrebné odborné vzdelanie v oblasti riadenia procesov, riadenia rizík a niekoľkoročná prax. Keby sme neboli zanedbali akčný plán úloh (aspoň) v oblasti vzdelávania v kybernetickej bezpečnosti na roky 2015 – 2020, máme rádovo menšie problémy.

4. Nedostatok financií a „nekoordinovanosť" legislatívy

Áno, nič nejde bez peňazí. Väčšie organizácie, najmä tie, ktoré zároveň tvoria kritickú infraštruktúru štátu, operujú zvyčajne s väčším balíkom financií. Je to

potom hlavne o nastavení vedenia a jeho stotožnení sa s otázkou kontinuity procesov a o pochopení, že bez investícií do bezpečnostných opatrení v oblasti kybernetickej bezpečnosti ohrozia nielen seba, ale aj občanov štátu, prípadne aspoň oblasti (okres, kraj), kde pôsobia a kde ich služby majú dosah. Čo však s organizáciami verejnej správy a organizáciami v pôsobnosti orgánov verejnej správy? Peniaze do rozpočtu na zvýšenie kybernetickej bezpečnosti nedostali, majú si vytvoriť rezervu, ale z čoho? Peňazí mali samosprávy málo aj doteraz, posledný rok im navyše financie z rozpočtu odčerpávali opatrenia proti šíreniu COVID-19. Na jednej strane je zákon, na druhej realita. A to sme nespomenuli školstvo. Všetky školy v pôsobnosti zriaďovateľa orgánu verejnej moci tiež podliehajú plneniu bezpečnostných opatrení v zmysle vyhlášky č. 179/2020 Z. z. Len ich zatiaľ NBÚ nezaradil medzi prevádzkovateľov základnej služby tak, ako to urobil s mestami a obcami k 1. 3. 2020.

To, že rozsah bezpečnostných opatrení pre rôzne kategórie (podľa veľkosti dosahu a špecifika sektora či podsektora, kam organizácia patrí) je rozličný, je v poriadku, ale prečo sa autori zákonov nepokúsili zjednotiť na pojmoch a zadelení bezpečnostných opatrení do jednotlivých oblastí? Stačí si porovnať § 20 zákona č. 69/2018 Z. z. a bod A) prílohy č. 2 vyhlášky č. 179/2020 Z. z. pre kategóriu II a III a rozdiely (nielen v drobnostiach) sú evidentné. Aj to komplikuje orientáciu sa v povinnostiach pre bezpečnostné opatrenia.

5. Neexistencia legislatívneho tlaku v oblasti malých a stredných podnikov (MSP)

Malé a stredné podniky sú na tom vlastne najhoršie. Sú dôležitou súčasťou tvorby HDP, ale keďže neexistuje žiadny právny rámec (resp. existuje len tlak na ochranu osobných údajov, ale tú chápu skôr ako súbor dokumentácie s právnymi vyjadreniami než súbor technických a organizačných opatrení), MSP doslova tápajú v bezpečnostných opatreniach.

6. Nedostatok špecializovaných odborníkov v oblasti kybernetickej bezpečnosti

Chýbajú forenzní analytici, súdni znalci, vyšetrovatelia v oblasti kyberkriminality, manažéri kybernetickej bezpečnosti, ktorých úloha je dokonca vynútená zákonmi, ale legislatíva, ktorá by upravila spôsob, ako sa stať napr. manažérom KB a aké vedomosti, odborné znalosti a zručnosti treba mať, meška už takmer dva roky. Zatiaľ je len vyhláška č. 436/2020, ktorá upravuje pozíciu audítora. Vyhláška o znalostných štandardoch v oblasti kybernetickej bezpečnosti je podľa NBÚ „na spadnutie" a očakáva sa v najbližších mesiacoch.

Existuje riešenie?

Vyzerá to komplikovane a ako začarovaný kruh, ale riešenie existuje: treba „spojiť sily". Za posledných pár mesiacov sa formuje dosť silná skupina odborníkov v oblasti kybernetickej bezpečnosti. Ich výstupy vidieť v odborných vyjadreniach v rôznych novinách, odborných časopisoch, pribúdajú odborné konferencie a podcasty venované témam kybernetickej bezpečnosti. Príkladný počin je aj tento komplexný materiál o kybernetickej bezpečnosti, ktorý publikuje redakcia NEXTECH. To všetko je síce chvályhodné, ale nestačí to. Vláda SR a jej jednotlivé ministerstvá si musia osvojiť úlohy z akčného plánu a na plnení týchto úloh navzájom spolupracovať. A takisto úzko spolupracovať s odbornými združeniami, asociáciami či Alianciou sektorových rád. V opačnom prípade úlohy akčného plánu zostanú len na papieri. Pre autora by bolo veľkým sklamaním, keby peniaze, ktoré Európska únia „ponúka", neboli primárne využité aj na digitalizáciu spoločnosti a budovanie povedomia v kybernetickej bezpečnosti. ■

Autor je analytik v oblasti kybernetickej bezpečnosti a externý pedagóg IKT predmetov. V spolupráci s Digitálnou koalíciou sa aktívne podieľal na rozpracovaní národnej stratégie kybernetickej bezpečnosti na roky 2021 – 2025 do akčného plánu v oblasti vzdelávania. Pôsobí ako expert Sektorovej rady pre informatizáciu a telekomunikácie v oblasti tvorby nových štandardov zamestnaní v oblasti kybernetickej bezpečnosti.

Ing. PETER MATEJ,
CEO spoločnosti eMsec, s. r. o.,
šéfredaktor projektu incident.sk

MOTIVÁCIA

Napriek tomu, že účinné zabezpečenie všetkých úrovní infraštruktúry na IT podporu biznisu je investične veľmi náročná záležitosť, potenciálne dôsledky bezpečnostných incidentov sú pre firmu oveľa nákladnejšie, v mnohých prípadoch dokonca likvidačné. Dôsledky napadnutia IT, či už na úrovni koncových zariadení, serverov, alebo prieniku do siete, sú nielen priame, ale aj nepriame. Nepriame škody, teda strata reputácie postihnutej firmy a strata zákazníkov sú často ešte horšie ako priame dôsledky, medzi ktoré patrí strata údajov, v horšom prípade ich zneužitie, prípadne škody spôsobené nedostupnosťou IT podpory výrobných, logistických či obchodných procesov. Firma napadnutá škodlivým kódom, napríklad ransomvérom, stráca prístup k faktúram, údajom o zákazníkoch či údajom potrebným pre výrobné a logistické procesy. Môže dôjsť k čiastočnému alebo aj úplnému zastaveniu produkcie. Skôr či neskôr to postihne aj zákazníkov, ktorí potom môžu prejsť ku konkurencii.

Preto aj v tomto prípade platí osvedčená zásada, že prevencia, hoci je často nákladná, je v konečnom dôsledku oveľa lacnejšia ako terapia a zotavovanie sa po prípadnom incidente. Napríklad pravidelné a dobre nastavené zálohovanie si vyžaduje dodatočné úložné kapacity a s tým spojené investičné a/alebo prevádzkové náklady či už na interne prevádzkovaný hardvér, alebo na prenájom kapacity v cloude. No v prípade napadnutia ransomvérom je investícia do zálohovania doslova na nezaplatenie. Navyše zálohovanie údajov vás účinne ochráni aj v prípade fyzickej poruchy diskov.

MOTIVÁCIA SA TÝKA ĽUDÍ

Motivácia je vnútorný proces, ktorý dáva nášmu konaniu energiu, smer a cieľ. V kontexte bezpečnosti informačných systémov ju vnímame v dvoch rovinách. Predovšetkým treba presvedčiť vedenie firmy o strategických rozhodnutiach ohľadne zabezpečenia a vypracovania kvalitných bezpečnostných politík a takisto je potrebné motivovať zamestnancov, aby sa správali zodpovedne. Keby táto publikácia bola určená primárne pre veľké firmy, písali by sme o nezastupiteľnej úlohe CIO (Chief Information Officer), ktorý sa snaží presvedčiť manažment, aby podporil jeho víziu IT bezpečnosti. V menších firmách je situácia odlišná. Manažéri sú väčšinou zároveň aj majiteľmi či podielnikmi firiem, takže im logicky záleží na tom, aby firma prosperovala, a mali by sa snažiť ochrániť ju pred bezpečnostnými incidentmi, ktoré by mohli znamenať veľké straty.

Rovnako dôležitá je aj motivácia zamestnancov, aby sa správali zodpovedne a svojou nepozornosťou či ľahostajnosťou neumožnili prienik škodlivého kódu do firmy. Keď majiteľ alebo vrcholový manažér rozpráva o firme, používa prirodzene slovné spojenie „moja firma". Jedno z kritérií, ako sa rozpozná, že zamestnanec je motivovaný, by mohla byť skutočnosť, že zamestnanci nerozprávajú o firme ako o „tej firme", ale „mojej firme" a uvedomujú si, že keď firma bude prosperovať, budú z toho profitovať aj oni sami. Do hry vstupuje aj dôležitý faktor kolektívnej zainteresovanosti. Stačí, ak si zamestnanec predstaví situáciu, že to bol práve on, kto neuvážene otvoril podozrivú prílohu elektronickej pošty a umožnil tým prienik škodlivého kódu do firemnej siete. Inak povedané, že práve on je zodpovedný za to, že firma utrpela straty, v dôsledku ktorých zamestnanci napríklad nedostanú očakávané odmeny. Predpokladajme, že vedenie firmy si je vedomé dôležitosti zabezpečenia IT. Tým sa však ich úloha v tejto oblasti ani zďaleka nekončí. Určite si uvedomujú, že kvalifikovaná pracovná sila je jedno z najdôležitejších aktív firiem, a to nielen v IT sektore, a treba ju motivovať nielen na pracovné výkony, ale aj na zodpovedné správanie.

ĽUBOSLAV LACKO, NEXTECH

SVET OPTIKOU HACKERA

Kybernetická bezpečnosť sa týka nás všetkých. Pokúsme sa na chvíľu dostať do kože útočníka, aby sme lepšie pochopili, ako sa pripravuje, aké sú jeho motivácie a čo sa deje pri útoku.

Je zložité stať sa hackerom? V skutočnosti je to jednoduchšie, ako by sa mohlo zdať. Útočník v prvom rade potrebuje kreatívne a logické myslenie. Nevyhnutná je detailná znalosť technológií, na ktoré sa plánuje zamerať. Webové aplikácie, cloudové služby alebo sieťové zariadenia patria medzi tie najčastejšie. Všetko sa možno naučiť. Pre samoukov je nevyčerpateľným zdrojom internet s kopou kvalitného materiálu, na vysokých školách sú čoraz obľúbenejšie odbory, ktoré sa venujú etickému hackingu. Úlohou etického hackera je overovanie bezpečnostných mechanizmov aplikácií či infraštruktúry pomocou simulácie kybernetických útokov. Firmám tento proces pomáha identifikovať zraniteľnosti, ktoré opravia ešte pred prípadným ilegálnym útokom.

Môže sa však stať, že etický hacker prejde na druhú, temnú stranu a stane sa z neho Darth Vader. Aké sú jeho motivácie? Často je to vidina veľkého zárobku, ale môže to byť aj túžba zviditeľniť sa, niečo ovládať alebo sa jednoducho zabaviť.

Na zjednodušenie rozdeľme útočníkov na dve skupiny. Prvú motivuje vidina finančného zisku. Útočí viac-menej náhodne, chýba jej konkrétny objekt záujmu. Využíva techniky ako *phishing* a *ransomvér*, ktoré umožňujú plošný útok na veľké množstvo cieľov. Rastúce povedomie o kybernetickej bezpečnosti zdokonaľuje obranné mechanizmy firiem a poskytovateľov verejných služieb, takže hackeri musia byť kreatívnejší. V praxi to znamená, že sa zameriavajú na špecifické odvetvia, témy alebo regióny.

Druhá skupina má konkrétny cieľ: firmu, osobnosť, štátne alebo verejné inštitúcie. Býva organizovaná, zoskupuje expertov na rôzne technológie a koordinuje svoj postup. Má finančné zázemie a používa kombináciu pokročilých techník. Útok môže trvať mesiace až roky. Prečo? Snahou je byť neviditeľný. Na svoj prospech využíva technické zraniteľnosti v systémoch, ale aj metódy sociálneho inžinierstva, prípadne kompromitáciu dodávateľov a ich služieb.

A ako takýto útok vyzerá? V oblasti bezpečnosti je jeden zo základných pojmov skratka CIA – *Confidentiality* (Dôvernosť), *Integrity* (Integrita), *Availability* (Dostupnosť). Hacker sa pokúša aspoň jednu položku tejto triády kompromitovať. V prípade dôvernosti sa snaží získať prístup k dátam alebo operáciám, na ktoré za normálnych okolností nemá práva. Môže ísť o krádež citlivých dát, získanie administrátorského oprávnenia, odpočúvanie komunikácie a podobne. Slabiny v kóde sú pre útočníka vstupnou bránou do systému, do ktorého prenikne použitím techník ako *SQL Injection* či *Cross-Site scripting (XSS)*. V oblasti infraštruktúry a na úrovni operačného systému sa zneužívajú neaktualizované či zle nakonfigurované komponenty v kombinácii s *buffer overflow* útokmi.

Ako sa dá narušiť integrita systému? Útočník pozmení dáta, prepíše zdrojový kód alebo poškodí hardvér. Príkladom tejto formy útoku je *ransomvér*. Je to škodlivý softvér, ktorý v prípade oprávneného zápisu na disk zašifruje dáta v súčasnosti neprelomiteľným algoritmom. Jediná možnosť, ako sa k dátam zasa dostať, je dešifrovací kľúč.

Triádu uzatvára dostupnosť služieb. Určite ste už počuli o takzvaných útokoch *DoS* (Denial of Service) a *DDoS* (Distributed Denial of Service). Cieľom hackera je znemožniť prístup do služby, aplikácie či na server použitím škodlivého kódu. DDoS na to využíva armádu už nakazených počítačov, takzvaný botnet.

Faktom je, že tieto princípy sú aplikovateľné nielen na svet IT. Podobným spôsobom možno útočiť na systémy OT aj SCADA. Ako príklad uvediem prevzatie kontroly nad kamerou vo verejnom priestore (porušenie princípu *dôvernosti*), vzdialené ovládanie semaforov na križovatke (porušenie princípu *integrity*) alebo ochromenie výrobnej linky (porušenie princípu *dostupnosti*).

Každá spoločnosť by mala byť schopná rozpoznať, že sa deje niečo nekalé. V niektorých prípadoch dostáva podnet od tretích strán alebo dokonca od samotných hackerov. No nie vždy ide o kybernetický útok. Aj napriek tomu, že sa hacker môže oháňať internými dátami spoločnosti, nemusel ich získať vďaka úspešnému útoku. Kde ich potom vzal? Nie sú náhodou voľne dostupné na internete? Práve preto je nevyhnutné každé podozrenie dôkladne prešetriť. Konkrétny prípad prevezme tím expertov na forenznú analýzu. Skúmajú, čo sa naozaj stalo, aký to má na spoločnosť dosah, prípadne zbierajú dôkazy na ďalšie vyšetrovanie. Zameriavajú sa na hľadanie indícií útoku v sieťovej prevádzke, na pevných diskoch, ale aj v operačnej pamäti. Štandardne pracujú v skupinách na zabezpečených pracoviskách, aby nikto nemohol dôkazy zmeniť alebo odcudziť. Výsledkom vyšetrovania by mala byť jasná odpoveď na otázku, či došlo ku kybernetickému útoku alebo – v tom lepšom prípade – šlo o planý poplach.

MICHAL MERTA,
riaditeľ pražského Cyber Fusion Centra spoločnosti Accenture

OFENZÍVNA BEZPEČNOSŤ: O HACKEROCH NA VAŠEJ STRANE

Počuli ste už o prípade útočníka, ktorý zistil, že organizácia investovala do kybernetickej bezpečnosti a je certifikovaná podľa ISO 27001, a rozhodol sa s bezpečnostným prienikom prestať? Že nie? Ani my nie.

Bezpečnosť je komplexná téma. Profesionáli z oblasti kybernetickej bezpečnosti niekedy vravia, že je to nevďačná práca. Nie sú žiadne incidenty? Tak načo vás platíme, keď sa nič nedeje? Niekto nás hackol? Načo vás platíme, keď ste nás neubránili?

V organizácii ste nasadili bezpečnostné politiky, vyškolili zamestnancov, implementovali firewally, webové aplikačné firewally, máte bezpečnostný monitoring, ba aj SOC. Bezpečnostné technológie sú nasadené na pracovných staniciach aj serveroch, máte plán na nasadzovanie bezpečnostných aktualizácií. Napriek takémuto arzenálu bezpečnostných opatrení zažijete nepríjemný bezpečnostný prienik. Nepríjemná konfrontácia s krutou realitou. Ako to mohlo stať? Kde nastala chyba? Séria otázok, vnútorného nepokoja a často aj výčitiek je prirodzenou reakciou.

Práve na včasnú a bezbolestnú konfrontáciu s pohľadom útočníka slúžia techniky ofenzívnej bezpečnosti. Pomáhajú preveriť odolnosť celej množiny bezpečnostných opatrení vrátane toho, ako dobre do seba jednotlivé opatrenia zapadajú.

OFENZÍVNA BEZPEČNOSŤ:

- **Penetračné testy**
- **Sociálne inžinierstvo**
- **Red teaming**
- **Bug bounty**

Penetračné testy sú najznámejšia technika ofenzívnej bezpečnosti. Ide o kontrolovaný útok na špecifické ciele v rámci organizácie. Najčastejšie ciele sú webové a mobilné aplikácie, interná a externá infraštruktúra. V posledných rokoch rýchlo rastie dopyt po pentestoch cloudovej infraštruktúry a cloudových aplikácií, keďže sa pri nich ukazuje, že aj kvalitní odborníci s mnohými rokmi praxe majú čo robiť, aby dostatočne zabezpečili aj cloud. Samostatnú kategóriu predstavujú pentesty metódami **sociálneho inžinierstva**. Ide vlastne o prekonanie bezpečnosti formou obyčajnej ľudskej wmanipulácie. Zobrazila sa vám v mysli scéna z filmu, kde jeden človek vyvolá roztržku a upúta tak pozornosť strážnikov, zatiaľ čo druhý preskočí turniket? Prípadne

človek s rukami plnými škatúľ, ktorý vás prosí o to, aby ste mu podržali dvere, pretože si nevie „pípnuť" vlastnú prístupovú kartu? Presne to sú príklady sociálneho inžinierstva. Zoznam techník a cieľov penetračného testovania je dlhý. Priemyselné riadiace systémy, biometrické systémy a vlastne čokoľvek, čo je zaujímavé pre zločincov, je vhodné preveriť penetračným testom.

Občas sa môžete stretnúť s pojmom automatizovaný pentest. Tu ide typicky o inú službu, ktorá sa správne volá Vulnerability Assessment. Táto služba je hodnotná a potrebná, pretože pomáha odhaliť známe zraniteľnosti na základe prednastaveného zoznamu. Pomáha odhaliť prítomnosť starých a deravých verzií softvéru. Je však len taká dobrá, aká dobrá je predprogramovaná logika a databáza zraniteľností, ktorú softvér preveruje. Poctivý penetračný test je manuálny a jeho hodnota sa začína presne tam, kde sa hodnota automatizovaných nástrojov končí.

Red teaming je akýsi pentest na steroidoch. Nesústredí sa na konkrétne systémy či aplikácie, ale zameriava sa na konkrétne úlohy. *Pokúste sa získať prístup k dátam obchodného riaditeľa*. Tak môže znieť jedna z úloh. Cieľom je získať prístup k citlivým informáciám bez odhalenia a otestovať, ako organizácia reaguje. Tento prístup je čoraz viac vyhľadávaný, pretože lepšie odzrkadľuje celkovú bezpečnostnú úroveň organizácie. Jeho realizácia niekedy pripomína scenár z novej bondovky. O aktivite je informované iba najužšie vedenie spoločnosti. Členovia testovacieho tímu sa niekedy do firmy dostanú bežným HR procesom ako noví zamestnanci. Postup je v každej spoločnosti iný a ultimátnym cieľom je dostať sa dnu. Takmer za každú cenu. Totiž aj v prípade red teamingu je prvoradé dodržanie mantinelov, ktoré boli na začiatku zmluvne dohodnuté s najužším vedením.

Minulý rok ste urobili penetračné testy a na ich základe ste implementovali lepšie bezpečnostné opatrenia. Minulý týždeň vás napriek tomu hackli. Päste udierajú na stôl. Čo sa zase stalo!? Dôvodov je viacero. Bezpečnostný tím organizácie môže byť kvalitný, stojí však proti kyberzločincom z celej planéty. V softvéri sa denne odhaľujú nové zraniteľnosti a tie umožňujú nové vektory útoku. Organizácie sú v pohybe a každá jedna zmena – technická aj netechnická – má dosah na bezpečnosť. Takýto boj je náročný a nie je ľahké ho vyhrať. Šance vie zásadne zlepšiť **bug bounty** program. Vďaka nemu dovolíte etickým hackerom odhaľovať diery vo vašich systémoch bez časového obmedzenia. Keď dieru nájdu, povedia vám o nej a vy im za jej zodpovedné nahlásenie vyplatíte odmenu. Pravidlá hry zároveň zakazujú zneužitie diery a zverejnenie informácií bez spoločnej dohody. Zrazu nestojíte proti planéte plnej útočníkov sami. Stoja na vašej strane etickí hackeri, ktorí medzi sebou súťažia o to, kto vám so zabezpečením pomôže skôr. Bug bounty programy sú využívané primárne v USA (Facebook, IBM, Oracle...), ale stále viac sa do nich zapájajú aj európske spoločnosti.

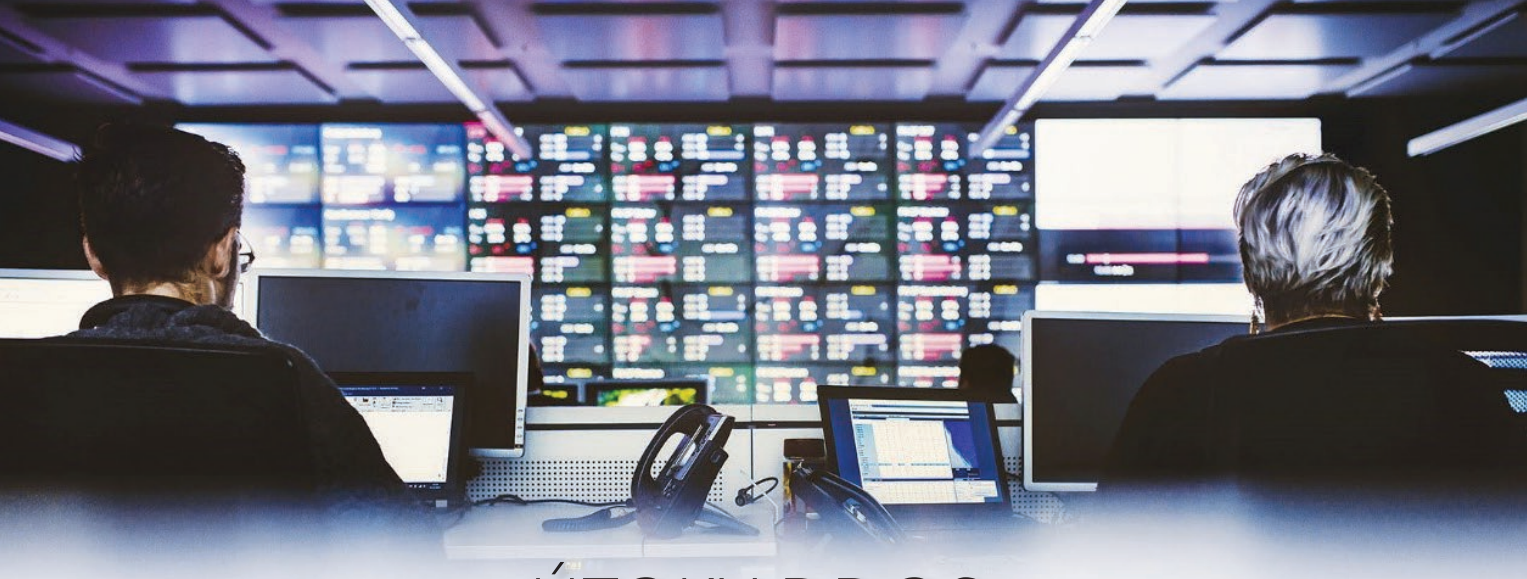
Spomínané kategórie testovania sa vzájomne nevylučujú. Organizácie s pokročilým stupňom bezpečnosti ich kombinujú do zmysluplného mixu, aby čo najlepšie pokryli rozmanité potreby ich IT infraštruktúry.

Zločincom stačí jediná bezpečnostná diera na to, aby ste si o prieniku do vašej organizácie prečítali na titulnej stránke novín. Urobte všetko pre to, aby ste im to prekazili a sebe umožnili pokojný spánok.

TOMÁŠ ZAŤKO, CITADELO

RED TEAMING – PRÍKLAD Z PRAXE:

Etický hacker prešiel štandardným výberovým procesom a zamestnal sa na pozícii junior programátora. Dostal firemný počítač a začal ním mapovať sieť. Následne sa pustil do prvých útokov. Po niekoľkých dňoch si IT oddelenie všimlo nezvyčajnú aktivitu, prišli ho konfrontovať a zobrali mu počítač. „Asi som dostal nejakú infekciu malvérom," to bolo dostatočne vierohodné vysvetlenie a ítečkár sa so zhabaným počítačom odobral preč. Hacker však do internej siete zapojil aj vlastné zariadenie, ktoré cez mobilnú sieť vytvorilo reverzný tunel. Vďaka nemu mali do siete prístup aj ostatní pentesteri a red team pokračoval v útoku. Kým boli ítečkári a bezpečnostní zaneprázdnení analýzou zhabaného počítača, pentesteri získali oprávnenia doménového administrátora, následne kontrolu nad celou sieťou a zákazníckymi zariadeniami vo viacerých krajinách.



ÚTOKY DDOS
MÔŽU OHROZIŤ VÁŠ BIZNIS AJ DOBRÉ MENO

Útoky DDoS (Distributed Denial of Service) predstavujú v súčasnom dynamickom svete ICT aktuálnu a nebezpečnú hrozbu so širokospektrálnymi následkami pre firmu či organizáciu, ktorá sa stala terčom tohto typu kybernetického útoku. Charakter týchto útokov je rôzny – od komerčnej cez politickú až po osobnú motiváciu.

Čo sú útoky DDoS?

Primárny a de facto jediný cieľ tohto typu útoku je dotknutú stranu zasiahnuť či už finančne, alebo poškodením dobrej povesti. V konečnom dôsledku tieto dosahy pre firmu, ktorá sa stala terčom útoku DDoS, môžu byť odlišné vzhľadom na charakter a oblasť jej pôsobenia. Útok DDoS je založený na nasadení väčšieho počtu internetových botov, ktoré útočia na jednu sieť, server, prípadne aplikáciu s vyšším počtom požiadaviek, čím zabraňujú v používaní služby reálnym používateľom.

Predstavte si, že máte e-shop, kde predávate interiérové doplnky. Na váš web sa dostanú všetci zákazníci a vám chodí jedna objednávka za druhou. Jedného dňa sa váš online obchod stane terčom útokov DDoS a ich množstvo nebude server stíhať. V takomto prípade vaša stránka „spadne" a nikto sa na ňu nebude môcť dostať. Útokom DDoS sme sa nevyhli ani na Slovensku. Stretnúť ste sa mohli s útokmi na politické, ale aj mediálne subjekty.

Útoky DDoS a technologická ochrana

Ochrana pred útokmi DDoS je náročná z technologickej a aj finančnej stránky. Tento fakt podčiarkuje aj to, že ak si útočiaca strana vytypuje konkrétny terč a disponuje dostatočnými finančnými prostriedkami a technickým zabezpečením, útok môže mať silné následky. Jeden z najjednoduchších spôsobov, ako sa môžu firmy či organizácie brániť pred útokmi DDoS, je využívať v rámci svojej konektivity bezpečnostnú službu. To v praxi znamená, že prípadný škodlivý dátový útok sa odfiltruje hneď pri vstupe do siete, čím sa predchádza úniku citlivých údajov, prípadne iným nepriaznivým následkom.

Obrana pred útokmi DDoS nemusí spočívať iba v nasadení technológie. Existuje veľké množstvo požiadaviek na daný terč útoku, o ktorých môžeme povedať, že sú škodlivé len s určitou pravdepodobnosťou. Inak povedané, tieto požiadavky sú označené za škodlivé napriek tomu, že sú legitímne. Automaticky škálujúce systémy vybavujú tento typ špecifických požiadaviek tak, aby nedošlo k odmietnutiu služby ani v situácii falošného pozitívneho nálezu.

Automaticky škálujúce systémy a infraštruktúra sa zabezpečujú súčasnými prostriedkami dátových centier a zabezpečiť sa dá napríklad aj automatické škálovanie do verejného cloudu. Služba je v tomto prípade prevádzkovaná v hybridnom prostredí cloudu, a teda

v privátnom a verejnom cloude súčasne. Výhodu tohto prístupu predstavuje prevažne úspora nákladov na rozširovanie systémov.

Zaujímavé však je, že medziročne počet útokov v roku 2018 oproti roku 2017 klesol o 13 %, napriek tomu zostáva znepokojujúcim faktom to, že miera sofistikovanosti útokov, naopak, výrazne rastie. Inak povedané, kvantitu útokov DDoS nahradila kvalita. Prispel k tomu fakt, že útočníci využívajú dostupnejšie sofistikované techniky na realizáciu svojho zámeru poškodiť danú organizáciu alebo spoločnosť.

Slovak Telekom má vo svojom portfóliu bezpečnostných riešení pre zákazníkov B2B manažovanú službu Network Protector, ktorej cieľom je ochrana pred útokmi DDoS. Kombinácia špičkovej technológie s balíkom funkcií ponúka zákazníkovi ochranu s odborným dohľadom špecialistov v režime 24/7/365. Nové, aktuálne riešenie prináša množstvo zlepšení, ktoré zákazníkovi garantujú bezpečnosť pred týmto typom kybernetických útokov.

SLOVAK TELEKOM

5 tipov, ako zlepšiť bezpečnosť IT infraštruktúry vo vašej firme

1. Zálohovanie

Každá firma disponuje dátami, ktoré sú z pohľadu jej pôsobenia a existencie mimoriadne citlivé. Ich strata a odcudzenie by znamenali značné finančné škody a poškodenie dobrej povesti v očiach verejnosti. Štandardom v dnešnej dobe sú cloudové riešenia, ktoré firmám ponúkajú bezpečné zálohovanie ich dát s vysoko efektívnym prístupom k týmto dátam.

2. Ochrana firemnej siete Wi-Fi

Tu platí zásada zašifrovania firemnej siete Wi-Fi silným šifrovacím algoritmom v kombinácii s odolným heslom. Všeobecne sa odporúča striktné oddelenie firemnej siete Wi-Fi od siete Wi-Fi, ktorá je dostupná pre zákazníkov alebo návštevy. S týmto úzko súvisí aj pravidlo nevyužívania verejných sietí Wi-Fi na prácu.

3. Zabezpečenie e-mailov

Pracovať s e-mailmi môžeme dvoma spôsobmi. Prostredníctvom klasického e-mailového klienta, ktorý je nainštalovaný na zariadení, alebo prostredníctvom webového rozhrania. Dôležité však je, aby sa pripájanie do konta uskutočnilo šifrovane a komunikácia bola chránená pred napadnutím. Existujú riešenia ako Office 365, kde si jednoducho vytvoríte e-mail s vlastnou firemnou doménou, ktorý zostane v bezpečí.

4. Správa hesiel

Či už pri zmene, alebo vymýšľaní nového hesla myslite na jeho dĺžku. Medzi základné odporúčania patrí používať aspoň 8 znakov (čím viac znakov, tým je heslo bezpečnejšie), striedať veľké a malé písmená a nezabudnúť ani na špeciálne znaky, prípadne čísla. Ak patríte medzi používateľov, ktorí v heslách radi využívajú osobné údaje, ako je dátum narodenia, zvýšte svoju pozornosť, pretože práve takéto heslá dokážu útočníci odhaliť najčastejšie. Vyhnite sa aj používaniu rovnakého hesla na viacerých prihlasovacích stránkach.

5. Firemná webová stránka pod ochranou

V oblasti webových stránok sa často stretávame s útokmi v podobe falošných stránok, keď web vyzerá ako oficiálna stránka obchodu alebo banky, ale v skutočnosti ide o falošné weby, ktorých úlohou je vylákať heslo alebo iné prihlasovacie údaje používateľa. Jednoduchý tip na zvýšenie bezpečnosti firemnej stránky je používanie bezpečnostného certifikátu. Stránky s HTTPS využívajú šifrovaný protokol. To znamená, že všetky dáta, ktoré sa posielajú či prijímajú, budú práve týmto certifikátom šifrované a chránené.

■

OCHRANA PRED ÚTOKMI OHROZENÍM FIREMNÉHO E-MAILU

Ohrozenie firemného e-mailu je rýchlo sa šíriaca hrozba kybernetického zabezpečenia, ktorej čelia všetky firmy, najmä malé a stredné podniky. **Internet Crime Complaint Center** (IC3) (Centrum pre nahlasovanie zločinov na internete) FBI vo svojej správe o internetovom zločine v roku 2020 uvádza, že za tento rok zaznamenali v Spojených štátoch 19 369 hlásení ohrozenia firemného e-mailu s upravenými stratami v hodnote 1,8 miliardy USD.

Útoky ohrozením firemného e-mailu primárne využívajú e-maily, možno ich však vykonať aj prostredníctvom SMS správ, hlasových správ či dokonca telefonátov. Tieto útoky sú zaujímavé, pretože sa vo veľkej miere spoliehajú na takzvané techniky sociálneho inžinierstva. Znamená to, že využívajú úskoky a klamstvá namierené voči ľuďom.

Útoky ohrozením firemného e-mailu dokážu byť veľmi účinné a ich obeťou sa môže stať každý bez ohľadu na veľkosť majetku či vedomosti. Vo februári 2020 Barbara Corcoran, americká podnikateľka, investorka a porotkyňa televíznej reality šou z podnikateľského prostredia Shark Tank, pri podvode tohto typu takmer prišla o 400 000 USD. Našťastie jej rýchle konanie umožnilo peniaze získať späť. Štatistiky FBI však ukazujú, že nie všetci majú toľko šťastia.

Keďže útoky ohrozením firemného e-mailu sa vo veľkej miere spoliehajú na sociálne inžinierstvo, tradičný bezpečnostný softvér pred nimi nie vždy chráni. Znamená to, že vy a vaši zamestnanci zohrávate pri ochrane pred týmito útokmi dôležitú úlohu. Preto je tiež dôležité porozumieť útokom ohrozením firemného e-mailu a tomu, ako fungujú.

AKO ÚTOKY OHROZENÍM FIREMNÉHO E-MAILU FUNGUJÚ

Existuje síce mnoho scenárov útokov ohrozením firemného e-mailu, všetky však majú jednoduchý princíp. Útočník sa pokúsi presvedčiť zamestnanca, aby mu poslal peniaze, tak, že sa bude vydávať za niekoho, komu zamestnanec dôveruje.

Útočníci sa často pokúsia zvýšiť si šance na úspech dvoma spôsobmi. Najskôr sa snažia navodiť dôveryhodný dojem vydávaním sa za konkrétnu osobu. Následne sa usilujú vytvoriť dojem naliehavosti, aby znížili šancu, že obeť spochybní transakciu a pri platbe využije riadne platobné kanály, ktoré by mohli podvod zachytiť.

Niektorí útočníci šikovne kombinujú tieto dve taktiky na čo najväčšiu účinnosť.

Jeden typ útoku ohrozením firemného e-mailu, ktorý sme zaznamenali, napríklad zahŕňa situáciu, keď zamestnanec dostane naliehavú správu od výkonného riaditeľa alebo iného vysokopostaveného výkonného pracovníka s informáciou, že zamestnanec má okamžite zaplatiť faktúru po dátume splatnosti alebo zabezpečiť darčekové karty na naliehavú firemnú udalosť. Môže ísť o e-mailové alebo textové správy, útočníci však už dokonca použili aj technológiu deepfake, pomocou ktorej imitovali hlasové

správy a hovory. Jeden vedúci pracovník v roku 2019 pri takomto útoku prišiel o 220 000 EUR (približne 243 000 USD), keď útočníci použili technológiu deepfake a vydávali sa za jeho výkonného riaditeľa.

V ďalšom type útoku ohrozením firemného e-mailu útočníci využívajú falošné a napadnuté e-mailové účty, pomocou ktorých presvedčia zamestnanca, že komunikuje s legitímnym dodávateľom. Útočníci si môžu so zacielenou obeťou vymeniť niekoľko e-mailov, aby ju presvedčili o tom, že sú skutočným dodávateľom, a následne jej poslú falošnú faktúru. Takto sa uskutočnil útok na Barbaru Corcoran.

Tretí typ útoku ohrozením firemného e-mailu sa zacieľuje na mzdové účtovníctvo firmy. Pri týchto útokoch sa útočníci vydávajú za zamestnancov a pokúšajú sa naviesť pracovníkov mzdového oddelenia firmy, aby zmenili údaje určené na priamy vklad zamestnanca na svoj vlastný bankový účet. Tieto útoky sú rafinovanejšie a vyžadujú viac času, môžu však byť veľmi účinné.

Takmer vo všetkých prípadoch je cieľom útočníkov získať peniaze jedným z dvoch spôsobov: elektronickým prevodom prostriedkov (vrátane kryptomien) alebo darčekových kariet. Aj keď môže byť použitie darčekových kariet na takýto útok prekvapivé, útočníci zistili, že predstavuje jednoduchý spôsob prevodu a prania špinavých peňazí.

AKO SA MÔŽETE CHRÁNIŤ PRED ÚTOKMI OHROZENÍM FIREMNÉHO E-MAILU?

Útoky ohrozením firemného e-mailu sú v skutočnosti klasické útoky založené na podvode, ktoré len využívajú súčasné technológie. Tento typ podvodov existoval dávno pred e-mailmi alebo hlasovými správami. Keďže nejde o útoky založené vyslovene na technológiách, znamená to, že technologické riešenia proti týmto útokom nebudú až také účinné ako napríklad proti ransomvéru. Dobre napísaný e-mail s cieľom ohroziť firemný účet, napríklad bezpečnostný softvér, len ťažko rozpoznáte od skutočného e-mailu, zvlášť ak pochádza od skutočného (no napadnutého) účtu alebo osoby, ktorej dôverujete.

Znamená to, že ochrana proti útokom ohrozením firemného e-mailu sa musí zameriavať na dve veci: vás a vašich zamestnancov. Najskôr oboznámte seba a svojich zamestnancov s útokmi ohrozením firemného e-mailu. Spolu so zamestnancami by ste sa mali naučiť, ako obozretne postupovať, keď dorazí neočakávaný e-mail od výkonného riaditeľa s textom: „Potrebujem, aby ste zabezpečili 5000 USD v darčekových kartách na dnešnú narodeninovú párty. Pošlite mi čísla a nikomu o tom nevravte." Obozretný prístup v takomto prípade môže byť z hľadiska prevencie takýchto útokov veľmi účinný.

Po druhé, zdôrazňujte dôležitosť overovania žiadostí o platbu a postupovania podľa zaužívaných pravidiel platenia účtov, zmeny údajov určených na priame vklady a nákupy a posielanie darčekových kariet. Požiadajte napríklad zamestnancov, aby v takom prípade zavolali zamestnancovi alebo dodávateľovi, ktorý túto žiadosť poslal. Uistite sa, že použijú číslo uvedené v záznamoch a pred ďalším postupom overia, že faktúra alebo žiadosť je legitímna.

Zdôraznite, že aj keď sa zdá, že žiadosti prichádzajú od vysokopostavených ľudí vo firme, zamestnanci majú povinnosť overiť si to. Útočníci sa pokúšajú presvedčiť zacielené obete, aby tieto útoky zostali utajené. Zvyšujú si tak šancu na úspech a využívajú to, že zamestnanci váhajú spochybňovať nadriadených. Dajte jasne najavo, že zamestnanci môžu a musia v takýchto situáciách klásť otázky.

Útoky ohrozením firemného účtu sú v konečnom dôsledku úspešné, pretože útočníci oklamú obete, ktoré uveria ich zavádzaniu. Aj keď útoky ohrozením firemného účtu využívajú technológie, v skutočnosti sú len modernou obmenou prastarých podvodov. Ak ich chceme zmariť, vyžaduje to, aby sme sa prispôsobili novým spôsobom, ako tieto staré podvody fungujú.

Dobrá správa je, že so správnym školením, vzdelaním a dodržiavaním riadnych pravidiel a postupov tieto útoky dokážete zmariť. Musíte si len nájsť čas na to, aby ste seba a svojich zamestnancov vzdelali v oblasti existencie takýchto podvodov, ich fungovania a správneho spôsobu, ako postupovať pri žiadostiach o platbu bez ohľadu na to, akým kanálom sa k vám dostanú.

CHRISTOPHER BUDD, AVAST

DRUHY KYBERNETICKÝCH ÚTOKOV

Klasické aj nové hrozby možno rozdeliť do niekoľkých kategórií:

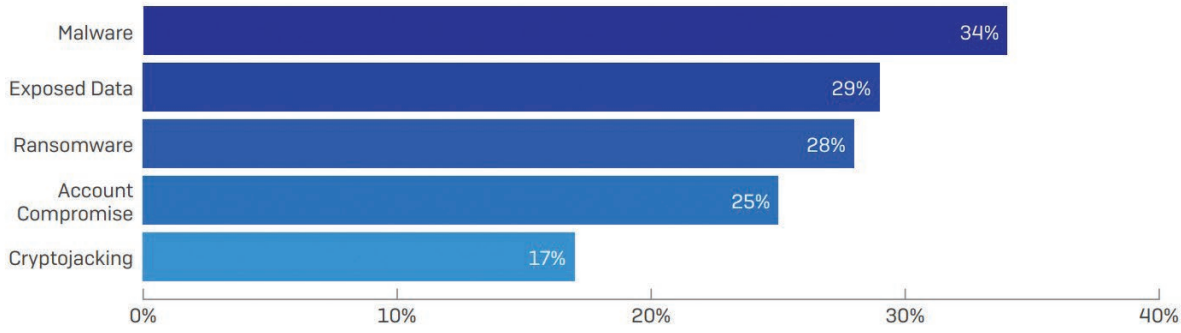
Klasické vírusy – počítačový vírus je program, ktorý dokáže rozmnožovať sám seba pridávaním svojho kódu do iných programov. Podobne ako biologický vírus potrebuje na svoje rozmnožovanie hostiteľa, v tomto prípade iný program, dokument, multimediálny súbor, e-mailovú správu a podobne. Vírus sa do počítača dostane po spustení infikovaného programu.

Makro vírusy napádajú dokumenty. Boli rozšírené najmä v prostredí kancelárskeho balíka MS Office. Týka sa to hlavne starších verzií, ktoré využívali binárny formát dokumentov. Od verzie 2007 aplikácie Word, Excel a PowerPoint využívajú komprimovaný formát XML, takže dokumenty sú na tento druh nákazy menej náchylné a navyše aplikácie na každé spustiteľné makro používateľa upozornia.

Internetové červy – počítačový vírus potrebuje na svoje zavedenie používateľovu asistenciu, aby spustil nakazený program. Vírus nakazí ďalšie aplikácie, no musí znovu čakať na nejakého spolupáchateľa, aby nakazený súbor niekomu poskytol, napríklad skopíroval na USB kľúč či poslal poštou, alebo uložil na nejaký „pirátsky" server na zdieľanie. Summa summarum, klasickým súborovým vírusom trvalo mesiace až roky, kým sa rozšírili v masovej miere. Internetové červy sú z hľadiska rýchlosti šírenia oveľa nebezpečnejšie a na hromadnú nákazu im stačí niekoľko hodín alebo dokonca minút, pretože sa dokážu šíriť „svojpomocne" pomocou počítačovej siete. Červ sa skúša pripojiť na každý dostupný počítač v počítačovej sieti a na svoj prenos využiť slabé miesto zle zabezpečeného počítača. Na tomto počítači sa červ aktivuje a znovu sa skúša šíriť do ďalších počítačov. Počet nakazených počítačov preto stúpa exponenciálne.

Trójske kone - Homérovu legendu o infiltrácii opevneného mesta pomocou bojovníkov ukrytých vnútri drevenej sochy koňa pozná azda každý. Ako to súvisí s počítačovými vírusmi? Počítačové siete sú dnes už dobre chránené proti napadnutiu z internetu. Podobne ako v prípade mestských hradieb za firewallom je sieť najzraniteľnejšia zvnútra. Trójsky kôň je škodlivý kód pribalený k zdanlivo neškodnému softvéru, ktorý používateľ často spúšťa. Na rozdiel od vírusov, ktoré škodlivé akcie vykonávajú priamo, trójske kone v pravidelných alebo náhodných intervaloch do systému vypúšťajú malvér, ktorý potom napadne sieť zvnútra, pričom je veľmi ťažké odhaliť zdroj nákazy. Aby sa trójske kone čo najviac priblížili legende, niektoré z nich slúžia doslova na otvorenie „zadných vrátok" (backdoor), cez ktoré sa potom hacker dokáže dostať do systému bez toho, aby

Percentuálny podiel jednotlivých typov incidentov vo firmách



ZDROJ: SOPHOS

poznal prístupové meno a heslo. Inými slovami, tento druh trójskeho koňa vytvorí v systéme bezpečnostnú dieru.

Spajvér – aplikácie z tejto kategórie zisťujú informácie o počítači a jeho používateľovi a bez súhlasu ich odosielajú tretej strane. Môže to byť zoznam kontaktov, zoznam navštevovaných stránok. Ešte nebezpečnejšie sú keyloggery, ktoré zaznamenávajú stlačenie klávesov, takže sa cez ne dajú získať prístupové heslá, čísla kreditných kariet a podobne.

Spamery a advér – úlohou spamerov je rozosielať nevyžiadanú poštu, najčastejšie s reklamným obsahom. Každý napadnutý počítač sa stáva odosielateľom nevyžiadanej pošty. Nepomôže ani zablokovanie adresy odosielateľa, pretože počet počítačov, z ktorých sa spam odosiela, sa zväčšuje lavínovito. Na koordinovanie takto napadnutých počítačov a zmenu obsahu odosielaných správ sa používajú botnety (venujeme im samostatnú stať). Názov advér vznikol zo slovného spojenia advertising-supported software. Bývajú súčasťou voľne šíriteľných programov, ktoré nie sú škodlivé, ale, naopak, užitočné a zobrazovanie reklamy je spôsob, ako sa ich tvorcovia snažia získať peniaze za svoj program. Žiaľ, často sa kombinujú so spajvérom.

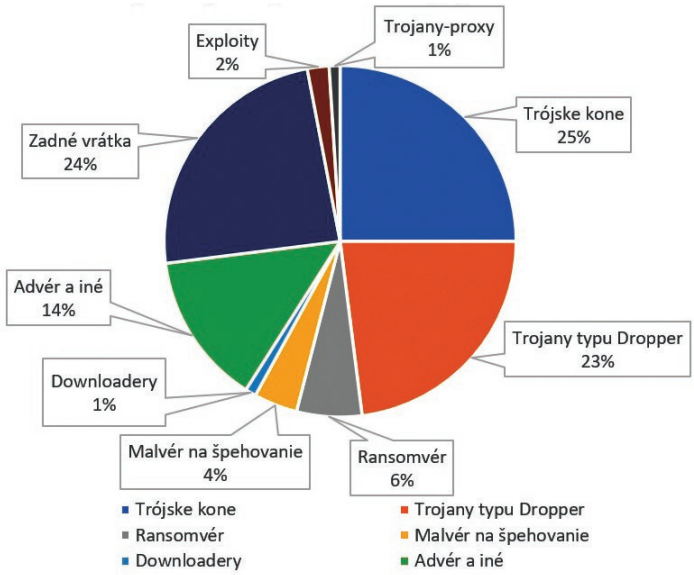
Hoax je falošná poplašná správa, ktorá vystríha používateľa pred počítačovými vírusmi, nebezpečenstvom zneužitia sietí a podobne.

Phishing (v preklade rybolov) na odvrátenie hrozby žiada od používateľa vykonať nejakú akciu, ktorá je nebezpečná, napríklad nainštalovanie a spustenie falošného antivírusového programu, zmenu hesla k bankovému účtu a podobne. V e-maile je umiestnený odkaz, na ktorom si máte heslo zmeniť. Odkaz smeruje na napodobeninu stránky banky a jej prevádzkovateľ takto „loví" prístupové kódy či osobné údaje.

Pharming (farmárčenie) presmerováva URL adresy stránok na falošné fyzické IP adresy. Ak takto napodobnia stránku internet bankingu vašej banky, získajú prístupové údaje k vášmu účtu priamo od vás a následne vás tentoraz cez pravú stránku banky „oholia".

Spoofing slúži na maskovanie totožnosti odosielateľa správ či maskovanie IP adresy. Zákernejšia metóda je tzv. man-in-the-middle. Doslovný preklad „muž

Najčastejsie identifikované typy malvéru



ZDROJ: KASPERSKY

v strede" je v tomto prípade veľmi výstižný. Narušiteľ sa pri tomto spôsobe votrie do komunikácie medzi klientom a serverom.

DDoS (Distributed Denial of Service), po našom distribuované odmietanie služby, sú útoky na dostupnosť. Server alebo infraštruktúra, ktorá je cieľom útoku, sa zahltí požiadavkami natoľko, že sa stane nefunkčnou a nedostupnou pre ostatných používateľov. Útočník musí mať k dispozícii veľké množstvo počítačov v rôznych geografických lokalitách. Na tento účel sa využívajú takzvané zombie. Sú to počítače (možno aj ten váš), ktoré sú infikované škodlivým kódom, napríklad vírusom alebo trójskym koňom. Na určitý podnet, napríklad vo vopred stanovenom čase, tieto zombie „ožijú" a začnú systematicky posielať pakety s požiadavkami na servery obete útoku. Obrana proti takémuto útoku je veľmi ťažká, až takmer nemožná. Útočí sa totiž pripája z reálnych IP adries infikovaných zombie, nič sa nepredstiera, takže softvér na odhaľovanie spoofingu je neúčinný. Firewall obete považuje pakety za korektné, veď nakoniec korektné aj sú, len je ich obrovské kvantum. Kľúčovou otázkou obrany je ich odlíšenie od skutočných požiadaviek a tu pomôže len analýza obsahu paketov. Keďže útok sa realizuje prostredníctvom tisícov až desiatok tisícov zombie počítačov, nakazených rovnakým škodlivým kódom, v nimi vygenerovaných požiadavkách sa dajú identifikovať určité vzory a následne sa požiadavky z týchto IP adries zablokujú.

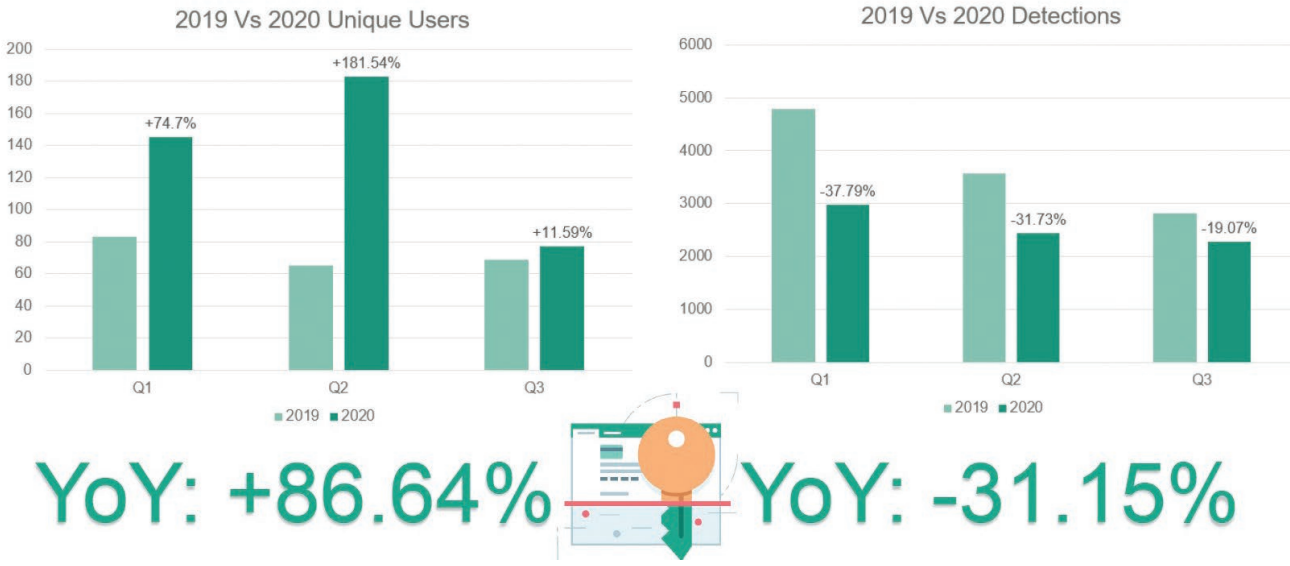
Ransomvér čiže novodobé výpalné. Pri novodobých metódach zločinnosti sa dá pozorovať kopírovanie metód klasickej kriminality, povýšených na novú technologickú úroveň. Typický príklad je internetové výpalné.

Kybernetický útok ako služba. Cloudovej ére, keď sa IT poskytuje ako služba, sa rýchlo prispôsobili aj kyberzločinci, ktorí ponúkajú kybernetický útok ako službu. Jednotlivci aj pokútne firmy zaoberajúce sa spamom ponúkajú možnosť zablokovať konkurenciu pomocou útoku DDoS, pričom cena za hodinu masívneho útoku sa začína na hodnote 20 USD. A aký by to bol marketing, keby neponúkal množstvové zľavy. Dvadsaťštyrihodinový útok stojí od 100 USD. To sú ceny za útoky smerované do komerčného prostredia. Ceny za ideologické útoky a útoky na politické weby sú podľa zákulisných informácií o dva až tri rády vyššie.

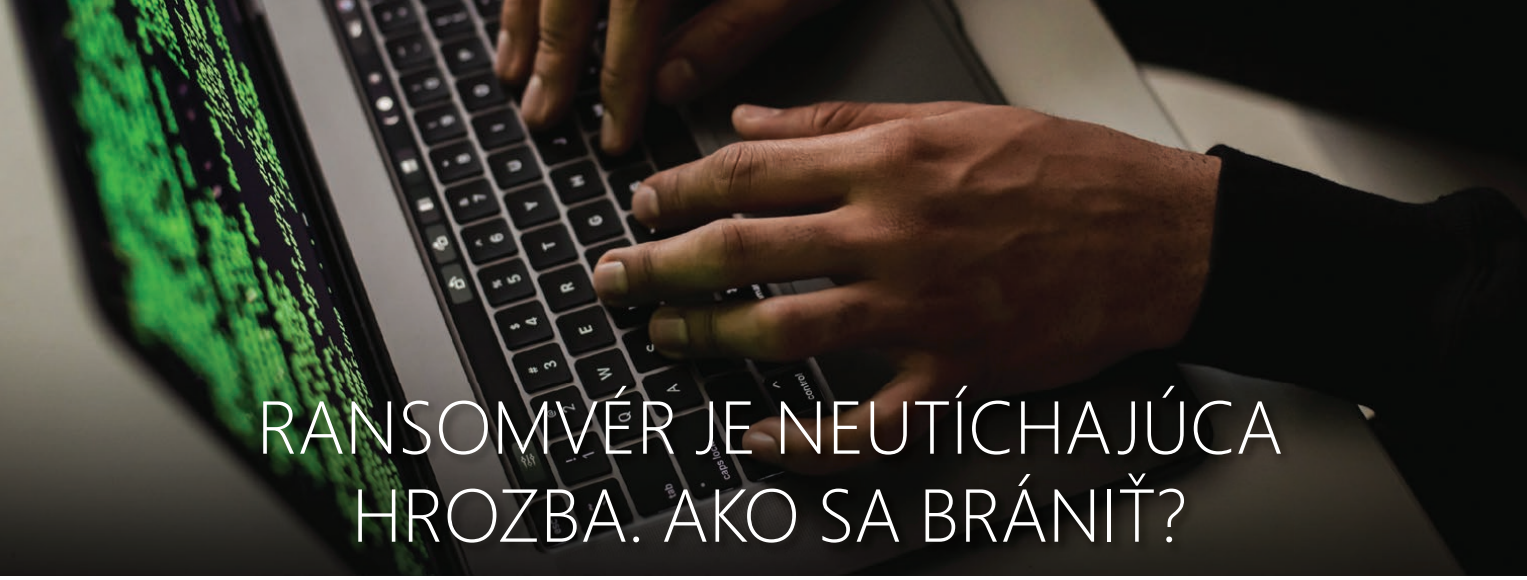
Ak pred takmer každú z vymenovaných hrozieb pripojíte predponu anti-, získate viac alebo menej presný prehľad modulov komplexných balíkov na zabezpečenie počítačov, serverov a mobilných zariadení.

ĽUBOSLAV LACKO, NEXTECH
ÚVODNÉ FOTO ZDROJ: rawpixel /freepik.com/

Ransomvér na Slovensku, porovnanie rokov 2019 a 2020



ZDROJ: KASPERSKY



RANSOMVÉR JE NEUTÍCHAJÚCA HROZBA. AKO SA BRÁNIŤ?

Ransomvér je typ škodlivého softvéru (malware – malicious software), ktorý po napadnutí počítačového systému zabráni používateľovi pristupovať k dátam tým, že ich zašifruje. Doterajšia prax útočníkov spočívala zväčša v požiadavke na zaplatenie finančnej sumy za navrátenie tohto prístupu. Takéto útoky môžu spôsobiť značné škody prerušením firemných procesov a viesť aj k trvalej strate dát.

Za posledné dva roky možno sledovať značný nárast počtu ransomvérových útokov. Podľa údajov Temple University* sa zvýšil počet nahlásených ransomvérových útokov na kritickú infraštruktúru medzi rokmi 2018 a 2019 takmer trojnásobne a medzi rokmi 2019 a 2020 skoro dvojnásobne. V roku 2021 bolo do polovice mája nahlásených 97 ransomvérových útokov na kritickú infraštruktúru.

Vo všeobecnosti sme doposiaľ vídali dve kategórie ransomvérových útokov:

1. kategória – útočník zašifruje pevné disky a žiada výkupné za sprístupnenie dát
2. kategória – útočník zašifruje súbory a žiada výkupné za poskytnutie dešifrovacieho kľúča

V poslednom čase sa začína viac a viac objavovať tretia kategória ransomvérových útokov, keď útočník ukradne veľké množstvo dát a potom hrozí ich zverejnením, ak mu nezaplatia výkupné. Jeden z dôvodov, prečo to tak je, tkvie v skutočnosti, že sa objavujú nové nástroje, ktoré sa zameriavajú na útoky prvej a druhej kategórie a vedia ich blokovať. Napríklad Microsoft má nástroje schopné monitorovať adresáre a detegovať a následne zablokovať neautorizované procesy (aplikácie), napríklad šifrovanie. Alebo môžeme použiť nástroj s názvom Raccine, ktorý vie úspešne zabrániť ransomvéru, ktorý zneužíva vssadmin.exe, aby zmazal „tieňové" kópie (shadow copies) uložené na napadnutom počítači, a potom zablokuje proces, ktorý túto požiadavku spustil. Takisto pravidelné zálohovanie s testovaním záloh a ich bezpečné uloženie dopomáha k zmenšovaniu dôsledkov na firemné procesy súvisiace s týmito kategóriami ransomvérových útokov.

Tretia kategória ransomvérových útokov sa postupne stáva dominantnou a je pravdepodobné, že to takto ešte nejaký čas aj zostane. Prečo to tak je? Ako sme už spomenuli, nové nástroje robia ransomvérové útoky prvej a druhej kategórie čoraz zložitejšími. Preto skupiny, ktoré sa zaoberajú takouto protiprávnou

** Rege, A. (2021). "Critical Infrastructure Ransomware Incident Dataset". Version 11. Temple University. Online at https://sites.temple.edu/care/resources/. Funded by National Science Foundation CAREER Award #1453040*

aktivitou, smerujú svoje úsilie do oblasti, kde z pohľadu ich „obchodného modelu" majú vyššiu šancu na zisk. Ak útočník použije taktiky a techniky, ktoré udržia jeho profil pod úrovňou detekcie v napadnutom systéme, možno predpokladať, že sa bude pohybovať v napadnutom systéme dlhodobo (podľa SANS 2019 Incident Response Survey je v prípade 42 % organizácií čas potrebný na odhalenie útočníka v napadnutom systéme v rozsahu dní až mesiacov; podľa špeciálnej správy M-Trends 2021 je globálny medián času potrebného na odhalenie útočníka v systéme 24 dní) a zhromažďovať veľké objemy firemných dát bez toho, aby sme o tom vedeli.

Tu sa do popredia dostáva aktívne vyhľadávanie hrozieb v počítačovej infraštruktúre. Perspektívna a vysoko účinná technika je vytváranie falošných nastražených dokumentov – honeydocs, ktoré sú zaujímavé z hľadiska potenciálneho útočníka. Napríklad môže ísť o súbor .xlsx s podstrčeným zoznamom hesiel. Rovnako zaujímavé z pohľadu útočníka sú aj nastražené administrátorské účty, tzv. honeyaccounts. Obe metódy sú v prípade neoprávnenej manipulácie alebo použitia schopné poslať hlásenie v reálnom čase a upriamiť tak pozornosť SOC (Security Operation Center) operátora a vzápätí iniciovať reakciu na danú udalosť. Túto stratégiu možno implementovať za veľmi krátke obdobie a takisto s rozumným rozpočtom.

Ďalšia perspektívna stratégia aktívneho odhaľovania útočníka v sieti je inšpekcia/monitoring komunikácie so vzdialeným riadiacim počítačom (command and control alebo C2) – v angličtine sa tento druh komunikácie označuje beacon. Samozrejme, tento druh komunikácie používajú aj legitímne a autorizované aplikácie, preto je dôležité vedieť, na čo sa zamerať. Tento prístup vyžaduje, aby sme sa nepozerali na individuálne relácie TCP, ale na komunikáciu ako celok z pohľadu väčšieho časového úseku. Toto nám pomôže identifikovať anomálie, ktoré vedú k odhaleniu neautorizovanej komunikácie. Na podporu tejto stratégie existuje bezplatný nastroj RITA (Real Intelligence Threat Analytics), ktorý v súčasnosti okrem detekcie C2 komunikácie využíva aj ďalšie možnosti kontroly.

Do budúcnosti sa dá predpokladať jednoznačne stúpajúci trend ransomvérových útokov tretej kategórie a tomuto trendu treba prispôsobiť aj obranné stratégie počítačovej infraštruktúry.

DANIEL SUCHÝ, špecialista na kybernetickú bezpečnosť,
Aliter Technologies, a. s.

ZERO TRUST

Zero trust nie je nič nové. Tento koncept bol predstavený už v roku 2010 a jeho hlavné zameranie je ochrana dát. Odvtedy uplynulo už viac ako 10 rokov, ale rozsiahlejšie implementácie bolo možné zaznamenať až minulý rok, keď museli malé firmy aj veľké korporácie prejsť z práce v kanceláriách (konvenčný model) na prácu z domu pri veľkej väčšine zamestnancov. Ten, kto by si myslel, že ide o niečo jednoduché, sa mýli. Rovnako ako ten, kto by si myslel, že zaobstaraním a implementáciou novej technológie, ktorá je hrdo označená zero trust, je úloha splnená. Štandardne sa takýto proces plánuje na dva a viac rokov. No minulý rok priniesol aj naozajstné výnimky, keď niektoré spoločnosti implementovali architektúru zero trust takpovediac cez noc. Čo je teda zero trust?

V skratke možno zero trust vyjadriť ako „ničomu nedôveruj a všetko preveruj". Neexistuje jednotná definícia, no vo všeobecnosti sa dá povedať, že zero trust je neustále sa vyvíjajúca stratégia kybernetickej bezpečnosti s cieľom opustiť zastaraný konvenčný statický model, založený na ochrane perimetra, a zamerať sa na dynamickejší prístup cez používateľov, zariadenia a zdroje.

Konvenčný model má viac-menej dve kritériá. Všetko, čo je mimo firemnej siete (internet), pokladá za nedôveryhodné a všetko v rámci firemnej siete (LAN) za dôveryhodné. Rovnaký prístup je aj na základe vlastníctva zariadenia – firemné je dôveryhodné, súkromné zariadenie je nedôveryhodné. Toto však už dávno neplatí.

Architektúra zero trust je iba odpoveď na trendy v rámci firemnej (korporátnej) infraštruktúry vrátane vzdialeného prístupu (napr. práca z domu), používania súkromných zariadení na pracovné účely (BYOD) a, samozrejme, firemných aktív umiestnených v cloude. Môžeme povedať, že ani v jednom z týchto prípadov nemáme kontrolu nad tým, kde sa takéto aktívum nachádza. S určitosťou však vieme, že nie je v uzavretej firemnej sieti (v konvenčnom ponímaní) s pevne definovanými hranicami. Preto sa stratégia zero trust zameriava

na ochranu zdrojov (firemné aktíva, služby, sieťové účty, workflow atď.), a nie na sieťové segmenty, pretože lokalita v sieti už nie je primárnym komponentom bezpečnostného statusu zdroja. Stratégia zero trust sa líši od konvenčného prístupu tým, že automaticky nepovažuje používateľov a zariadenia za dôveryhodné iba na základe fyzickej polohy alebo „polohy" v sieti, resp. vlastníctva zariadenia.

Zhrňme si teda základné princípy architektúry zero trust:

1. Vždy pristupujte k vašej internej/externej sieti, akoby bola napadnutá
2. To, že je sieť interná, nie je dostatočný argument na to, aby sme jej dôverovali
3. Každé zariadenie, používateľ a komunikácia v sieti musia byť preukázateľné
4. Nepretržitý hĺbkový monitoring siete

Nepretržitý monitoring siete je základný prvok, ktorý umožňuje identifikáciu a klasifikáciu dát, mapovanie pohybu citlivých dát, porozumenie vlastnej sieti, zariadeniam a aplikáciám. Je potrebné, aby riešenie na monitorovanie siete bolo nepretržité a jeho nastavenie umožňovalo aj monitorovanie komunikácie v rámci internej siete, medzi internými zariadeniami. Následne je ideálne prepojenie na SIEM (nástroj na monitorovanie a odhaľovanie kybernetických hrozieb). Ten zhromažďuje záznamy, ktoré nás zaujímajú, a pomáha zachytiť potenciálnu prítomnosť útočníka/hrozby v sieti. Takisto vie vykonať preddefinovanú akciu na základe nastavených algoritmov.

A ako začať? Ak používate hlavne prostredie Windows, na to, aby ste začali uplatňovať stratégiu zero trust, pravdepodobne nepotrebujete nič extra okrem toho, čo už máte vo svojej infraštruktúre. Napríklad namiesto jednostrannej autentifikácie zo strany servera začnite uplatňovať vzájomnú autentifikáciu na komunikáciu medzi serverom a klientom s využitím internej PKI (Public Key Infrastructure – systém na tvorbu a distribúciu digitálnych certifikátov). Druhým príkladom môže byť izolácia domén a vynútenie IPsec (Internet Protocol security – autentifikačný a šifrovací protokol) atď.

Pre tých, ktorí by sa chceli dozvedieť viac o koncepte zero trust, odporúčam knihu *Zero Trust Networks: Building Secure Systems in Untrusted Networks* od Evana Gilmana a Douga Bartha.

DANIEL SUCHÝ,
špecialista na kybernetickú bezpečnosť, Aliter Technologies, a. s.

BEZPEČNOSŤ PRI HOME OFFICE

Úplne presný názov tejto state by bol Bezpečnosť NIELEN pri home office. Inak povedané, ak v súvislosti s prechodom menšieho či väčšieho počtu zamestnancov na prácu z domu sprísnite pravidlá a bezpečnostné politiky a budete striktnejšie vyžadovať ich dodržiavanie, znížite tým riziko napadnutia škodlivým kódom či inou formou kyberkriminality a v dlhodobom horizonte posilníte stabilitu a konkurencieschopnosť svojej firmy. V dlhodobom preto, lebo momentálne s tým síce budete mať určite vyššie náklady a možno ste v pokušení, či by tieto prostriedky nebolo výhodnejšie investovať do modernizácie technologického vybavenia, ale v prípade bezpečnostného incidentu v dôsledku nedostatočného zabezpečenia by sa vám to určite nevyplatilo.

Začneme dvoma kľúčovými zásadami na zabezpečenie počítača, ktorý používate na prácu z domu.

- Uistite sa, že váš počítač používa aktualizovaný operačný systém. Rovnaké pravidlo platí aj pre váš prehliadač a všetky ďalšie aplikácie, ktoré plánujete použiť.
- Ešte pred pripojením k internetu by ste mali mať nainštalované spoľahlivé antivírusové riešenie s aktualizovanou databázou, ktoré dokáže hrozby či prípadné útoky zachytiť včas a zabráni tak škodám.

OCHRANA ZARIADENIA V DOMÁCEJ, PRÍPADNE NEZNÁMEJ SIETI WI-FI

Ak sieť, do ktorej sa pripájate, nie je dostatočne zabezpečená, aktivity v takejto sieti môže sledovať tretia strana pomocou nástrojov, ktoré sú v súčasnosti voľne dostupné na internete. Neoprávnený prístup do zabezpečenej siete využívajúcej spoľahlivé štandardy šifrovania je oveľa náročnejší závisí to však od nastavení, medzi ktorými významnú úlohu zohráva sila hesla.

Jedno z najväčších rizík takéhoto pripojenia je tzv. útok man-in-the-middle, pri ktorom útočník vstupuje do komunikácie medzi vami ako používateľom a cieľovou stránkou či službou, na ktorú sa snažíte pripojiť. Týmto spôsobom ju môže nielen sledovať, ale aj meniť a upravovať tak, aby ste mu poskytli citlivé údaje. Pri prístupe do firemných sietí treba využívať ďalšie dodatočné opatrenia na ochranu dát, napr. technológiu VPN (Virtual Private Network).

PRÁCA S DOKUMENTMI

V malých firmách stále prevládajú dokumenty vytvorené v aplikáciách kancelárskych balíkov a uložené na lokálnych diskoch. Väčšina z nich absolvuje svoj životný cyklus vrátane schvaľovania a revízií posielaním dokumentov ako príloh elektronickej pošty. Dokumenty vznikajúce priamo v podnikových informačných systémoch sú v segmente SMB v menšine a v menšine sú aj dokumenty, ktoré síce v kancelárskych balíkoch vzniknú, no vstupujú do informačných systémov, aby tam pokračovali v ďalších fázach životného cyklu.

Lokálne ukladanie dokumentov, ktoré je stále realitou v mnohých malých a stredných firmách, je úplne najhorší scenár, aký môže z hľadiska bezpečnosti existovať, a dovolíme si tvrdiť, že v porovnaní s érou pred PC, keď sa dokumenty vytvárali na písacích strojoch, je to veľký krok späť. Nechával vtedy niekto dokument po ukončení práce v písacom stroji? Nie. Uložil ho na bezpečné miesto do zberača alebo citlivé a dôverné dokumenty uložil do trezoru, prípadne dokument odoslal a založil si na bezpečné miesto jeho kópiu. Ak sa v noci nepovolaná osoba vlámala do kancelárie a písací stroj ukradla, dokumenty boli pri správne organizovanom systéme ukladania v bezpečí. Rovnako to fungovalo aj v personálnej sfére. Ak si študent zabudol kufríkový písací stroj vo vlaku, diplomová práca mu zostala v aktovke. Inak povedané, v mnohých prípadoch počítače len zjednodušili a nahradili klasické metódy pred érou PC, ale lokálne ukladanie dokumentov žiadny precedens nemá.

Riešením je ukladanie dokumentov v cloude alebo na firemnom serveri. S takto uloženými dokumentmi môžu zamestnanci pracovať odkiaľkoľvek a z akéhokoľvek zariadenia. Notebook či tablet sú len nástroje. V prípade ich poruchy, straty alebo krádeže neprídete o svoje dokumenty ani údaje a pri správnom zabezpečení sa k nim nikto neoprávnený nedostane.

Vo veľkých firmách môže byť vlastná serverová a úložná infraštruktúra aj cenovo výhodnejšia, pretože objem „konzumácie" týchto komodít sa dá predvídať a podľa toho plánovať investície do hardvéru a softvéru. Pri startupoch a menších firmách je spravidla výhodnejšia cloudová služba vďaka flexibilite a modelu „platiť len za to, čo používaš". No ak z rôznych dôvodov nechcete alebo nemôžete presunúť svoje dokumenty alebo ich časť do cloudu, treba vytvoriť na svojich serveroch, či už fyzických, alebo čoraz častejšie virtuálnych, vhodné prostredie na správu dokumentov a tímovú spoluprácu.

„SKÚSTE SI TROCHU SPYTOVAŤ SVEDOMIE A POLOŽIŤ SI OTÁZKU, ČO BY SA STALO, KEBY NIEKTORÉMU Z DESIATICH NAJDÔLEŽITEJŠÍCH ĽUDÍ VO VAŠEJ FIRME UKRADLI POČÍTAČ. AKÉ INFORMÁCIE SA NÁJDU NA JEHO DISKOCH A SÚ NEJAKÝM SPÔSOBOM CHRÁNENÉ, NAPRÍKLAD ŠIFROVANÍM?"

V IT platí, že čím viac autonómie firma vyžaduje, tým viac infraštruktúry musí spravovať. Ak firma nemá dostatok IT personálu, ktorý sa na plný úväzok venuje správe systémov, môže zastrešiť túto oblasť iným spôsobom. Jedno z riešení je outsourcing. Vo všeobecnosti ide o odčlenenie čiastočnej alebo aj kompletnej IT infraštruktúry a jej prevádzkovanie špecializovanou firmou. Hlavnou výhodou outsourcingu je to, že jeho poskytovateľ spravidla vykoná určitú konsolidáciu a zavedie moderné nástroje diaľkovej správy a monitoringu, dôsledkom čoho sa spravidla zefektívnia aj súvisiace procesy.

ĽUBOSLAV LACKO, NEXTECH

AKO PREŽIŤ KYBERÚTOK

Treba zachovať chladnú hlavu, nepodliehať panike a zhromaždiť dôkazy. A byť pripravený...

Zabezpečiť kontinuitu svojho podnikania bez vkladu do kyberbezpečnosti je v dnešnom online svete nemožné. Napriek tomu ju firmy radia na chvost investičných priorít. Len málo manažérov si uvedomuje, že reputačné a finančné následky po útokoch môžu naprávať roky. Hovorili sme s expertom na kybernetickú bezpečnosť **Ľubomírom Kopáčkom**.

Ako pristupujú slovenské firmy k otázke kyberbezpečnosti?

Ľubomír Kopáček: Väčšina sa touto témou zaoberá, až keď je neskoro. Najčastejšie vtedy, ak už organizácia čelila útoku, ak je predmetom zákonnej regulácie a ak má materskú firmu v zahraničí alebo potrebuje splniť požiadavku na kyberbezpečnosť od svojich obchodných partnerov. Treba povedať, že výrazne lepšia situácia je práve v spoločnostiach so zahraničnou účasťou, kde sa kyberbezpečnosť berie vážne. Predovšetkým to platí vo firmách pochádzajúcich z Nemecka a Francúzska.

Podobná situácia je aj v štátnych inštitúciách?

Ľubomír Kopáček: Tie sa v drvivej väčšine iba snažia formálne splniť požiadavky zákona o kybernetickej bezpečnosti. Od jeho účinnosti žijú v omyle, že po audite je pre nich téma uzatvorená. Neuvedomujú si, že audit sa bude pravidelne opakovať, a teda kybernetická bezpečnosť musí byť systematicky riadená.

Aký je motív útočníkov pri cielení na firmy a organizácie?

Ľubomír Kopáček: Neexistuje jednotný motív, ale najbežnejšie motívy sú peniaze a poškodenie organizácie.

Dá sa konkretizovať, koľkým útokom čelia slovenské firmy a štátne inštitúcie v ročnom priemere?

Ľubomír Kopáček: Nedá. Zasiahnuté subjekty sa k útokom nerady priznávajú, vnímajú to ako reputačné riziko a obávajú sa poškodenia dobrého mena. Štátne inštitúcie a organizácie, ktoré sú regulované zákonom o kyberbezpečnosti, majú zákonnú povinnosť hlásiť závažné incidenty autorite, v tomto prípade Národnému bezpečnostnému úradu. Takáto informácia je však predmetom utajenia, a teda sa o nej okrem dotknutej inštitúcie a NBÚ nik nedozvie.

Existujú aj subjekty, ktoré kyberútokom nečelia?

Ľubomír Kopáček: Ak si to nejaká spoločnosť myslí, je to utópia a jednoznačný dôkaz, že majú nulový rozhľad. V skutočnosti o žiadnych incidentoch nevedia preto, lebo nie sú schopné ich identifikovať. Incidentom čelí každá jedna firma alebo štátna inštitúcia bez výnimky.

Z toho vyznieva, že slovenské subjekty nevenujú kyberbezpečnosti dostatočnú pozornosť, hoci je v dnešnom online svete nevyhnutná na zabezpečenie kontinuity ich biznisu.

Ľubomír Kopáček: Prevažne ju pokladajú za zbytočnú investíciu. Nedochádza im, že môžu prísť o cenné dáta, citlivé informácie, ohrozený môže byť výrobný proces a v hre je aj strata dôveryhodnosti pred klientmi či dodávateľmi, ktorú si budovali roky. Schopní manažéri dobre vedia, aké ťažké je firmu budovať, a určite si dokážu predstaviť, že ešte ťažšie by bolo napraviť si reputáciu po takomto incidente. Mnoho firiem používa dokonca stratégiu, keď si spočítajú škody pri najhoršom možnom scenári, toto číslo si porovnajú s výškou investícií do kyberbezpečnosti a rozhodnú, že potenciálne škody sú jednorazovo akceptovateľné.

To môže z čisto ekonomického pohľadu dávať zmysel.

Ľubomír Kopáček: Áno, ale má to chybičky krásy. Ten najhorší možný scenár sa môže zopakovať, a to nie raz. Bude sa opakovať dovtedy, kým organizácia nezačne kyberbezpečnosť aktívne riadiť tak, aby mohla útokom predchádzať. Tu už ekonomický pohľad až taký zmysel nedáva. Incidenty môžu byť pre firmy aj likvidačné.

Čo treba zmeniť, aby moderní manažéri dokázali incidentom predísť?

Ľubomír Kopáček: Ideálne by bolo, keby mali organizácie úprimnú snahu a záujem riešiť kyberbezpečnosť bez toho,

aby im to niekto prikazoval. Toto sa však nedeje. Potrebná je zmena myslenia a edukácia manažérov, pretože žiadneho manažéra len tak neosvieti a nepovie: Poďme minúť 5 percent zo zisku na kyberbezpečnosť. Potrebuje vedieť o hrozbách aj možnostiach ochrany, aby vedenie nemuselo aktivovať plán obnovy po katastrofe (Disaster Recovery – DR), ktorým sa potom činnosť organizácie dostáva do normálneho stavu. V skratke možno povedať, že sa treba dostať z reaktívneho prístupu na proaktívny.

Hovorili ste o pláne obnovy po katastrofe. Ten je nevyhnutnou súčasťou plánu na udržanie kontinuity biznisu (Business Continuity Plan – BCP). Čo to však znamená v súvislosti s kyberbezpečnosťou?

Ľubomír Kopáček: Treba mať pripravené a najmä pravidelne testované rôzne scenáre, ktoré majú vplyv na chod a prežitie organizácie v súvislosti s rôznymi „katastrofami". Aktuálny príklad je povinná práca z domu. Tak ako bol home office štátom nariadený, dá sa hovoriť o katastrofe z pohľadu biznisu. Ak má organizácia plán na zvládnutie napríklad totálneho a dlhodobého výpadku dodávky elektrickej energie, tento istý plán môže aktivovať aj pri povinnej práci z domu. Je to totiž presne to isté. Keď príde organizácia o napájanie elektrickou energiou na dlhší čas, takisto môže väčšinu zamestnancov iba poslať domov. Ak chce tento výpadok organizácia prežiť, musí mať pripravený a otestovaný scenár, ako prácu organizovať na diaľku. Dobrá správa je, že v oblasti kyberbezpečnosti netreba nič vymýšľať na kolene, keďže existujú normy a medzinárodné štandardy, ktoré nám pri tvorbe BCP krok za krokom dokážu poradiť, ako takéto plány zostavovať.

Čo je teda potrebné riešiť v rámci plánu kontinuity biznisu?

Ľubomír Kopáček: Na detailnú odpoveď by nám nestačilo ani niekoľko desiatok strán. Stručné zhrnutie: je nevyhnutné mať plány pripravené tak, aby sa neriadená kyberbezpečnosť nestala prostriedkom, ktorý bude zosilňovať dôsledky katastrofy. Konkrétny príklad je, že spoločnosti by sa mali vyvarovať toho, aby v prípade nútenej práce z domu pracovali zamestnanci na svojich domácich počítačoch. Dôvod je jednoduchý. Organizácia nemá tieto počítače pod kontrolou a mohli by sa stať prostriedkom pre kybernetický útok na ňu.

Líšia sa plány a úroveň zabezpečenia proti kyberútokom podľa veľkosti, druhu či zamerania firiem?

Ľubomír Kopáček: Samozrejme. Zabezpečenie potrebujú mať vytvorené na mieru podľa toho, či ide o finančnú inštitúciu, online podnikanie, alebo je firma orientovaná na priemysel a výrobu. Líšia sa nielen podľa sektora, ale úroveň zabezpečenia je rôzna v každej jednotlivej spoločnosti. Mala by byť primeraná účelu a ekonomickým možnostiam organizácie. Toto sa dá jednoznačne nastaviť. Umením je nájsť primeranosť výšky investícií vzhľadom na potenciálne škody. Vo všetkých však platí, že najcennejšie sú dáta, v tom prípade je nepodstatné, o aký sektor ide.

Ako by teda mala vyzerať príprava na kybernetický útok?

Ľubomír Kopáček: Na útok musíme vedieť hlavne reagovať a ideálne mu predchádzať. Dá sa dostať do súladu s niečím, čo je vyskúšané, a keď sa toho budeme držať, s veľkou pravdepodobnosťou budeme vedieť na útok reagovať. Hovorím napríklad o norme ISO 27001 alebo o vyhláške 362/2018, prípadne iných vhodných štandardoch.

Možno nakoniec útok zastaviť?

Ľubomír Kopáček: Len vtedy, keď máme schopnosť ho identifikovať a disponujeme ľuďmi a prostriedkami na jeho zastavenie alebo aspoň zmiernenie dôsledkov. V praxi by som manažérom poradil, aby si v takejto situácii zachovali chladnú hlavu, nepodliehali panike a zhromaždili čo najviac dôkazov. Ak si nevedia poradiť sami, mali by požiadať špecializovanú firmu o riadenie celej udalosti. Rozhodne nie je namieste riešiť to svojpomocne.

ĽUBOMÍR KOPÁČEK,
expert na kybernetickú bezpečnosť GAMO a.s.

AKO SA ZBAVIŤ HROZBY VÝPADKOV

A ZABEZPEČIŤ FIRME MENEJ ADMINISTRÁCIE, VIAC KOMFORTU A VYŠŠIU BEZPEČNOSŤ S RIEŠENÍM OD FORTINETU?

ŠPECIÁLNY PROJEKT

Zamestnanci sa presunuli z kancelárie na home office a všetky interné porady do virtuálneho prostredia. Veľa spoločností nebolo pripravených na prácu zo vzdialeného prostredia a utrpel tým hlavne manažment, ktorého riadenie zrazu nabralo ťažší priebeh. Druhým pálčivým problémom bolo a naďalej je, že IT tímy v spoločnostiach dostatočne neprispôsobili danej situácii svoju kybernetickú bezpečnosť. Ako dokáže v tomto smere pomôcť technológia od Fortinetu a koncept Zero Downtime? Na danú tému sme sa rozprávali s **Rudolfom Bohušom**, výkonným riaditeľom spoločnosti eGroup Solutions, a. s.

Ako ste pociťovali u vás vo firme koronakrízu? Čo všetko sa u vás v rámci práce zmenilo?

Rudolf Bohuš: Na krízu sme reagovali okamžite a vyhlásili sme povinný home office, maximálne jeden človek v kancelárii. Našťastie pracovne sme neutrpeli, skôr bol problém dohodnúť sa so zákazníkmi na stretnutiach a návštevách. Home office je pre IT firmy štandardom dlhé roky, takže korona nemala reálny dosah na firmu okrem väčšieho dôrazu na organizáciu práce a zadávanie úloh. Uvidíme, ako sa toto všetko bude vyvíjať ďalej.

Spolupracujete s lídrom v oblasti kybernetickej bezpečnosti Fortinetom. Aké sú kľúčové výhody, pre ktoré ho odporúčate svojim klientom?

Rudolf Bohuš: Čo sa týka firewallov, spolupracujeme len s Fortinetom, s ktorým máme dlhoročné skúsenosti. Jeho portfólio hardvérových a softvérových produktov pokrýva celú oblasť kybernetickej bezpečnosti. Zákazníci hľadajú komplexné riešenia s čo najväčším komfortom a v tom je Fortinet viac ako vyhovujúci. Naši klienti si chvália rýchle reakcie na zmeny, dostupnosť a update softvéru v prípade problémov, podporu pri poruche a okamžitú výmenu zariadenia. Pri tom všetkom vieme poskytnúť silnú podporu z našej strany a postarať sa o nulový výpadok siete.

Ktoré konkrétne technológie od Fortinetu nasadzujete u svojich klientov?

Rudolf Bohuš: Používame **FortiGate Next-Generation Firewall (NGFW)**, a to nielen u klientov, ale aj na svoje interné účely. Využívame aj **FortiMail** na úrovni virtuálnych strojov, dokonca ho využíva aj jeden z našich najväčších klientov, ktorý má vyše 1000 používateľov. Ďalej využívame **FortiGate Cloud**, čo je cloudová služba SaaS (Software as a Service), ktorá ponúka množstvo správ a služieb pre firewallové brány od Fortinetu. Čo sa týka reportov, tie posiela potom Fortinet priamo zákazníkom.

Pokiaľ ide o firewallové riešenia FortiGate NGFW, vedeli by ste opísať u niektorého vášho klienta, ako vyzerala situácia v rámci IT pred nasadením a ako vyzerá teraz, po nasadení tohto riešenia?

Rudolf Bohuš: Väčšina inštalácií je u našich dlhoročných klientov, kde sme začínali pred 8 až 10 rokmi. Práve stabilita a účinnosť pri zachytávaní škodlivého kódu firewallu od Fortinetu je to, prečo je Fortinet dobrá voľba v tejto oblasti. U väčšiny zákazníkov boli používané SW a firewally, ktoré okrem funkčného softvéru na bezpečnosť potrebovali aj ďalší hardvér a podporný softvér. Zo strany administrátora to napríklad znamenalo, že sa musel starať o viac vecí. Pri NGFW sme použili jedno až dve zariadenia a o nič iné sa už nebolo treba starať. Zákazníkom to prinieslo nižšiu poruchovosť, vyššiu ochranu a spomínaný komfort.

Aké technické, ale aj obchodné výsledky im to prinieslo?

Rudolf Bohuš: O úspešnosti vypovedajú reporty, v ktorých je zaznamenané, koľko škodlivého kódu sa zachytilo. Môžu vidieť, že nemajú žiadny incident, to je v podstate najväčší úspech. Snom každého manažéra alebo CEO je mať vo firme IT, o ktorom nevie, a Fortinet spolu s konceptom Zero Downtime môže tento sen preniesť skutočne do reality. Prináša to menej administrácie, viac pokoja, vyššiu bezpečnosť aplikácií a dát a lepšie riadenie prístupov používateľov podľa požiadaviek.

A čo samotná inštalácia? Ako prebieha? Zabezpečujete ju z vašej strany?

Rudolf Bohuš: Inštalácie produktov Fortinet sú veľmi intuitívne a jednoduché na konfiguráciu a správu. Na druhej strane to však neznižuje ich účinnosť pri odchytávaní škodlivého kódu. Pri inštalácii dochádza v prvom kroku k analýze existujúceho prostredia, či už sieťového, ale aj toho, ktoré sa týka prístupu používateľov k informáciám, či už k interným aplikáciám, alebo s prístupom na internet. Na základe toho vypracujeme návrh riešenia a navrhneme zariadenie z takého radu, aby okrem funkcionality vyhovovalo aj výkonnostne. Takisto sa snažíme navrhovať riešenia vysokej dostupnosti (HA – high availability). Zjednodušuje to servisovanie a podporu bez dosahu na prevádzku. A to všetko pri dodržiavaní konceptu Zero Downtime, ktorý znamená, že IT infraštruktúra bude navrhnutá, vybudovaná a prevádzkovaná tak, aby nedochádzalo k výpadkom. IT zákazníka je pod stálou kontrolou, vďaka čomu môžu špecialisti okamžite reagovať na všetky udalosti a zmeny, ktoré nastanú v danom prostredí, prípadne na všetky žiadosti o poskytnutie služby podľa požiadaviek klienta. Hlavnou úlohou je zabezpečiť funkčnosť a bezpečnosť všetkých IT systémov.

Aké výzvy vidíte v budúcnosti pre spoločnosti v oblasti IT bezpečnosti? Akú úlohu v tom bude hrať Fortinet?

Rudolf Bohuš: Kybernetická bezpečnosť sa stáva jednou z najdôležitejších vecí, ktoré sa týkajú prevádzky IT. Musím však povedať, že nestačí mať iba dobré zariadenia, ale treba tomu prispôsobiť aj interné procesy, dodržiavať ich a vedieť reagovať na vzniknuté situácie. Načo budete mať super zariadenie, keď nebude nikto vyhodnocovať, čo zachytilo a ako reagovalo? Ako nastaviť procesy, keď dôjde k útoku? Tu je, myslím si, veľký priestor na zlepšovanie sa v každej firme. A Fortinet patrí medzi silnú trojku spoločností, ktoré sa venujú výhradne bezpečnosti. Ak budú pokračovať v tom, čo robia a ako to robia, budú patriť do okruhu firiem, s ktorými je skutočne radosť spolupracovať. ■

ZABEZPEČENIE POČÍTAČOV A ĎALŠÍCH ZARIADENÍ

Zatiaľ čo servery, či už vlastné, alebo virtuálne v cloude, sú väčšinou rozmaznávané starostlivou pozornosťou kvalifikovaných špecialistov, klientske zariadenia „v prvej línii" sú nezriedka ponechané na svojvôľu používateľov. Správa a zabezpečenie klientskych zariadení je preto spravidla najnáročnejšia úloha.

V mnohých firmách je, žiaľ, stále hlavným správcom klientskych zariadení entropia. Inými slovami, veci ponechané samy na seba majú tendenciu spieť „od desiatich k piatim". Podľa rovnakých pravidiel z bezpečnostného hľadiska pokojne chátrajú aj počítače, smartfóny a tablety, o ktoré sa nikto pravidelne a organizovane nestará.

Navyše ak túto záležitosť nerieši manažment firmy, vznikajú medzi pracovníkmi a správcami rozpory, pretože niektorí pracovníci majú pocit (a dosť často oprávnený), že ich striktné pravidla ohľadne používania počítačov a mobilných zariadení obmedzujú v práci. Trecie plochy medzi správcami a používateľmi pracovných staníc vznikajú najmä preto, lebo správca má na zreteli iné kritériá, než je používateľský komfort.

Ak má pracovník možnosť sám si konfigurovať a spravovať svoj firemný počítač, spravidla pri tom sleduje viac svoje osobné ciele než strategické záujmy firmy. Laicky povedané, snaží sa čo najviac opevniť vo svojej pozícii. Týka sa to hlavne pracovníkov na stredných manažérskych postoch a niektorých špecifických povolaní, napríklad účtovníkov. V menšej miere to platí aj pri budovaní izolovaných infraštruktúr jednotlivých oddelení firiem, prípadne organizačných zložiek rôznych úradov. Hoci na prvý pohľad by sa mohlo zdať, že ak si pracovník organizuje prostredie na svojom desktope sám, zvyšuje to jeho produktivitu, zvyčajne je pravdou pravý opak. Moderné systémy poskytujú také pokročilé možnosti personalizácie aplikácií, že tento argument patrí už jednoznačne do histórie.

Mnohé oddelenia firmy spravujú dôverné informácie nielen v centralizovaných databázach, ale v podobe rôznych dokumentov dosť často aj na diskoch počítačov. Tu vzniká zdanlivo oprávnená paranoja zo zverenia takýchto počítačov do správy pracovníkov iného oddelenia. Málokedy si však manažéri oddelení uvedomujú, že IT oddelenie spravuje vo firemných databázach spravidla oveľa väčšie portfólio dôverných informácií a výsledkov analýz, než sa nachádza v dokumentoch na diskoch počítačov.

Problémy vznikajú aj pri nedostatočnom kapacitnom dimenzovaní poskytovateľov správy systémov. Používatelia sú niekedy nútení po niekoľkých avízach problému, ktoré zostanú bez adekvátneho ohlasu, riešiť problém

so softvérom vlastnými silami. Pritom na druhej strane preťažené a zahltené IT oddelenia čelia rozpočtovým obmedzeniam a zároveň neustále náročnejším požiadavkám a očakávaniam používateľov.

TIEŇOVÉ IT

Dynamický biznis kladie stále náročnejšie požiadavky na IT podporu a v mnohých prípadoch manažéri nie sú ochotní akceptovať termíny, ktoré im navrhne IT oddelenie, a obstarávajú si softvér, prípadne cloudové služby sami. Tento nekoncepčný postup sa zvykne nazývať „tieňové IT". Až potom sa manažéri alebo príslušné oddelenie či pobočka znova obrátia na IT oddelenie, od ktorého očakávajú, že prevezme na seba nákladové, bezpečnostné a ďalšie atribúty riešenia, ktoré nakúpila iná organizačná zložka firmy. Nie vždy sa nakúpené riešenie ukáže v konečnom dôsledku ako najlepšie, najspoľahlivejšie a ekonomicky výhodné. Navyše vo firme vzniká čoraz zložitejšia heterogénna infraštruktúra, ktorú spravovať je veľmi drahé. Pojem vo firme navyše nie je úplne presný. Väčšinou sa nakupujú cloudové služby, takže tieňové IT má prevažne podobu niekoľkých izolovaných ostrovčekov vo verejných cloudoch rôznych poskytovateľov. IT oddelenia prestávajú mať prehľad nad používanými cloudovými službami a infraštruktúrami. Nemajú dokonca ani informácie, či táto služba vyhovuje bezpečnostnej politike firmy.

Na jednej strane manažéri tvrdia, že decentralizácia IT má pozitívny dosah na podnikanie, urýchľuje schopnosť prinášať na trh nové produkty a služby, zjednodušuje inovácie a zvyšuje konkurencieschopnosť, pretože firma dokáže lepšie reagovať na vývoj trhov. Tí istí manažéri si však paradoxne zároveň uvedomujú aj nutnosť kontroly a aspoň čiastočnej integrácie. Viac než 40 % manažérov sa domnieva, že decentralizácia v praxi znamená zdvojenie nákladov, nejednoznačnosť, čo sa týka vlastníctva a zodpovednosti za IT subsystémy, a nedostatočnú bezpečnosť. Viac než 60 % oslovených manažérov sa nazdáva, že IT by malo umožňovať inovačné snahy, ale musí stanoviť strategický smer a niesť zodpovednosť za bezpečnosť. Spomínané percento naznačuje, aká je zhruba požadovaná rovnováha medzi funkciou centrálneho IT jednak z hľadiska zachovania kontroly, jednak z hľadiska podpory inovácií v niektorých organizačných zložkách firmy.

CENTRÁLNA SPRÁVA

Centrálna správa klientskych zariadení do značnej miery eliminuje nevýhody autonómnej správy. IT oddelenie alebo externý poskytovateľ služieb môže oveľa efektívnejšie spravovať a udržiavať softvér na týchto zariadeniach vrátane centrálnej aplikácie bezpečnostných záplat a opravných balíčkov. Jednotné a konzistentné prostredie vo firme môže takisto zvýšiť produktivitu práce zamestnancov, pretože všetci zdieľajú všeobecné pracovné prostredie. Normalizácia prevádzkových systémov a aplikácií znižuje aj výdavky na ich správu. Špecialisti z IT oddelenia môžu jednoducho nainštalovať nové programy a bezpečnostné aktualizácie centrálne namiesto toho, aby museli nahrávať potrebné systémy a aplikácie na každú pracovnú stanicu samostatne. To podstatne zrýchľuje aktualizáciu softvéru a zabraňuje výpadkom a prestojom IT kapacít. Jednotné nastavenie a dodržiavanie politiky konfigurácie je zárukou, že centrálne spravované počítače či mobilné zariadenia sú oveľa menej vystavené bezpečnostným hrozbám.

Ak externý poskytovateľ preberie kontrolu nad pracovnými stanicami vo firme, preberá tým automaticky aj zodpovednosť za zabezpečenie ich spoľahlivej prevádzky, a to z hľadiska zaistenia informačnej bezpečnosti, počítačových sietí, technického aj softvérového servisu a, samozrejme, aj technickej podpory.

ONLINE MONITORING A SPRÁVA

Servisná správa na diaľku (online cez internet) dokáže pokryť prevažnú väčšinu servisných zásahov, ako aj riešenie požiadaviek zákazníkov. Komunikácia cez internet sa uskutočňuje s použitím silného šifrovania, čo zaručuje spoľahlivú ochranu prenášaných údajov. Tento spôsob servisu výrazne šetrí celkové náklady na servis a skracuje čas potrebný na vykonanie servisného úkonu. Pravidelne sa kontroluje stav a aktuálnosť operačného systému vrátane záplat a servisných balíčkov. Kontrolujú sa aj zmenené alebo pridané programy, dokumenty a ostatné súbory, stav a aktuálnosť antivírusového softvéru. Pravidelná kontrola týchto parametrov pomôže zabrániť vzniku problémov.

SPRÁVA SYSTÉMOV V CLOUDE

Zdalo by sa, že ak firma presunie svoju infraštruktúru do cloudu, zbaví sa starostí s jej správou. Úplne to platí len v prípade modelu SaaS (softvér ako služba) a len pre serverovú infraštruktúru. Najproblematickejšia časť z hľadiska správy čiže klientske zariadenia stále zostávajú u zákazníka v jeho správe, prípadne môže ich správu outsourcovať.

Vo všeobecnosti pre cloudové modely poskytovania služieb platí, že čím viac autonómie firma, ktorá je v tomto kontexte zákazník poskytovateľa cloudových služieb, požaduje, tým viac infraštruktúry musí spravovať. V prípade modelu PaaS (platforma ako služba) zákazník spravuje len aplikácie. Ak sa rozhodne pre model IaaS (infraštruktúra ako služba), teda prenájom virtuálnych serverov, tento model mu poskytne vysoký stupeň autonómie. Nemusí spravovať dátové centrá, zariadenia, hardvér ani virtualizáciu, to je úloha poskytovateľa služby. Všetky architektonické vrstvy nad virtualizáciou si však spravuje zákazník sám alebo ním poverený subjekt. Zákazníci sa zbavia starostí a investičných nákladov súvisiacich s nákupom a prevádzkou serverov, úložísk alebo sieťovej infraštruktúry. To všetko si kupujú vo forme služby. Model IaaS je výhodný napríklad pre firmy, ktoré majú nakúpené softvérové licencie, ale nechcú viazať kapacity na hardvér.

Pri modeli IaaS je zákazník úplne zbavený starosti o IP, hardvérovú aj fyzickú bezpečnosť, ktorú rieši poskytovateľ služby IaaS. Vy si len objednáte potrebnú kapacitu, teda počet virtuálnych strojov, ktoré plánujete využívať. Aj v prípade, ak si vyberiete renomovaného poskytovateľa cloudovej služby, odporúčame šifrovať obsah virtuálnych diskov obsahujúcich citlivé údaje. Vyhnete sa tak potenciálnemu riziku, že zamestnanec poskytovateľa získa prístup k vašim údajom.

ANTIVÍRUSOVÉ RIEŠENIA VO VIRTUALIZOVANOM PROSTREDÍ

Aj napriek tomu, že moderné EPP (Endpoint Protection Platforms) sa snažia počítač, ktorý chránia, zaťažovať čo najmenej, na základe naplánovaných harmonogramov sa vykonávajú kontroly operačného systému a súborov a takisto pravidelné každodenné aktualizácie, ktoré si pre seba ukroja niekoľko málo percent výpočtovej a prenosovej kapacity, čo sotva postrehnete. A teraz si predstavte, že takéto riešenie je nasadené na desiatkach či stovkách virtuálnych počítačov bežiacich na jednom výkonnom serveri. Ak riešenie EPP nebolo koncipované na beh vo virtualizovanom prostredí, inak povedané, že ide o samostatné, nezávislé, a teda nekoordinované riešenie, spomínané akcie (kontrola súborov či aktualizácia) sa začnú na všetkých virtuálnych strojoch súčasne. Pre tento stav sa zaužívalo označenie „antivírusová búrka". Paralelné skenovanie na viacerých virtuálnych strojoch vygeneruje dlhodobú záťaž, počas ktorej dochádza k súpereniu virtuálnych strojov o prostriedky. Aj nekoordinovaná paralelná distribúcia aktualizácií antimalvérových databáz môže v danom, relatívne krátkom okamihu vygenerovať veľkú záťaž.

Rozsah potenciálnej antivírusovej búrky si najlepšie uvedomíte na praktickom príklade. Podľa skúseností s virtualizáciou desktopov možno optimálne zaťažiť server približne šiestimi virtuálnymi desktopmi na jeden logický procesor. Na serveri so 64 jadrami by sme teda mohli teoreticky vytvoriť 384 virtuálnych desktopov. To v prípade, keby išlo o tzv. heavy workers, teda používateľov, ktorí by napríklad na svojom desktope robili lokálne analýzy v Exceli. Bežných používateľov by server zvládol dvoj- až štvornásobok, teda 500 až 1000 priemerne zaťažených virtuálnych desktopov, pričom občasné zvýšené požiadavky na výpočtovú kapacitu niektorého z nich by vďaka rozdeľovaniu záťaže na úrovni virtualizačnej platformy nebol žiadny problém. Ak sa však na 500 virtuálnych počítačoch rozbehne súčasne antivírusová kontrola náročná aj na kapacitu procesora, ale hlavne zaťažujúca diskový systém, môže to byť veľký problém.

Masovému nasadzovaniu virtualizačných riešení, či už v oblasti virtualizácie serverov, alebo desktopov, sa začínajú prispôsobovať aj riešenia EPP. Využívajú sofistikované metódy, ktorých cieľom je dosiahnuť rovnomernejšie rozdelenie záťaže. Využíva sa náhodné, prípadne rozložené skenovanie, skenovanie virtuálnych strojov, ktoré sú v režime offline, náhodná aktualizácia databáz, skenovanie do vyrovnávacej pamäte či tzv. gold image whitelisting, keď sa vytvorí zoznam kmeňových súborov, spoločných pre všetky klonované virtuálne stroje. Tieto súbory potom nie sú skenované pri periodických kontrolách, ale osobitne. Explicitná podpora a optimalizácia pre vir-

tualizované prostredia by sa mala stať povinnou súčasťou každého moderného riešenia EPP. Presadzuje sa aj nová filozofia tzv. bezagentových antivírusových nástrojov (agentless antivirus).

Napriek problémom s paralelným skenovaním či aktualizáciou, ktoré sú vhodnou koordináciou ľahko riešiteľné, virtualizované prostredie umožňuje dosiahnuť oveľa väčší výkon, hlavne pri virtualizácii desktopov či aplikácií. Veľa virtuálnych strojov je vytvorených klonovaním zo spoločnej šablóny virtuálneho obrazu. Potom predsa nemá zmysel skenovať pri plánovaných kontrolách rovnakú súpravu súborov pre všetky virtuálne desktopy znova a znova, stovky až tisícky krát, podľa toho, koľko desktopov je hostovaných na jednom fyzickom serveri. Preto moderné riešenia EPP využívajú koordinačných agentov v základnom obraze (obraze, z ktorého vznikli klony) a vyrovnávacie pamäte. Ešte sofistikovanejšie riešenie je vytvorenie tzv. zlatého obrazu (gold image whitelisting) čiže zoznamu súborov, ktoré nemajú byť následne testované. Pretože predsa len existuje malé riziko, že aj súbory patriace do tohto „zlatého obrazu" by mohli byť napadnuté, vykonávajú sa aj pravidelné kontroly týchto šablón. Rozdiel v nárokoch na fyzické zdroje je zrejmý na prvý pohľad. Súbory patriace do „zlatého obrazu" sa skontrolujú iba raz, a nie pri kontrole každého virtuálneho stroja naklonovaného z nich. Obraz kompletného virtualizovaného stroja je fyzicky jeden súbor, ktorý sa dá jednoducho presúvať medzi fyzickými servermi dokonca aj počas behu VM a rovnako jednoducho zálohovať. Preto firmy čoraz viac využívajú riešenia na virtualizáciu aj na „zabalenie" a vnútornú distribúciu zložitejších konfigurácií. Takto možno napríklad distribuovať vo virtuálnych obrazoch celé predkonfigurované serverové prostredie pre pobočky a podobne. Preto bezpečnostné riešenia musia byť schopné pristupovať aj dovnútra týchto kontajnerov a vykonávať v nich v reálnom čase antimalvérové skenovanie a ďalšie funkcie EPP, napríklad kontrolu aplikácií. Nie je žiadny technický dôvod, prečo by sa skenovanie VM muselo vykonať na rovnakom fyzickom serveri, kde sa predpokladá jeho spustenie. Pravdepodobne najlepšie riešenie je spúšťať takéto „zakonzervované" virtuálne stroje v karanténe a skenovať ich v „živom" stave.

ZABEZPEČENIE TLAČIARNÍ

Aj napriek masívnej digitalizácii papierové dokumenty, a teda aj tlačiarne na ich tlač tu budú stále. Tlačiarne majú sieťovú konektivitu, možnosti softvérových aktualizácií a môžu slúžiť ako vstupná brána do podnikovej siete. Až 56 percent firiem ignoruje bezpečnostné riziká spojené s tlačiarňami a ďalšími periférnymi zariadeniami. Iba 30 percent respondentov tvrdí, že ich organizácia má metódu na identifikáciu vysoko rizikových tlačiarní. Obchod (označený 93 percentami respondentov) a ľudské zdroje (76 percent) sú považované za oddelenia s najslabšími bezpečnostnými opatreniami v súvislosti s tlačiarňami a laxným prístupom k ich kontrole. Iba 44 percent respondentov uviedlo, že bezpečnostná politika ich spoločností zahŕňa zabezpečenie tlačiarní pripojených do siete. Až 64 percent potvrdilo, že ich spoločnosti vnímajú vyššie riziko skôr v súvislosti so stolovými počítačmi a notebookmi. Väčšina respondentov je pesimistická ohľadom svojej schopnosti zabrániť úniku dát obsiahnutých v pamäti tlačiarne alebo priamo na výtlačkoch. Tlačiarne, hlavne v menších firmách, navyše nie sú chránené proti neoprávnenému prístupu cez Wi-Fi či otvorené porty.

ĽUBOSLAV LACKO, NEXTECH

VYUŽÍVANIE VLASTNÝCH ZARIADENÍ NA PRACOVNÉ ÚČELY (BYOD)

Trend nazývaný BYOD (Bring Your Own Device), teda prineste si vlastné zariadenie, sa postupom času vyprofiloval predovšetkým na využívanie vlastných smartfónov, pretože pri týchto zariadeniach sa najviac prelínajú pracovné aktivity s osobným životom. V súvislosti s masívnym prechodom na home office však veľa zamestnancov, ktorí využívajú tento spôsob práce, začalo používať aj svoje súkromné notebooky či domáce počítače.

Vo všeobecnosti BYOD je alternatívna stratégia, ktorá umožňuje zamestnancom, obchodným partnerom a externým spolupracovníkom používať súkromné klientske zariadenia úplne alebo čiastočne podľa vlastného výberu, spúšťať na nich firemné aplikácie a pristupovať k firemným údajom. BYOD však zároveň vyvoláva veľa polemík, predovšetkým čo sa týka bezpečnosti. Na druhej strane aj bezpečnostní analytici kvitujú, že de facto ide o formalizáciu existujúceho stavu prenikania smartfónov do všetkých sfér osobného aj pracovného života a takisto mobilného štýlu práce kedykoľvek a odkiaľkoľvek.

AKO TO FUNGUJE V PRAXI

Prístroj si vyberie a zakúpi používateľ, pričom firma alebo organizácia mu môže dať zoznam zariadení, ktoré sú prijateľné z hľadiska podpory a zabezpečenia. IT oddelenie poskytuje čiastočnú alebo úplnú podporu pre zariadenia, sieťový prístup, aplikácie a údaje. Firma takisto môže, no nemusí poskytnúť čiastočnú alebo aj úplnú refundáciu ceny zariadenia. Zamestnanci dostanú prístupové práva k podnikovým aplikáciám primerané svojmu zaradeniu a na druhej strane musia dodržiavať bezpečnostné pravidlá a politiky. BYOD sa môže týkať len vybraného okruhu manažérov, odborných pracovníkov či externých zamestnancov a pracovníkov na čiastočný úväzok, dodávateľov, stážistov, konzultantov a ďalších pracovníkov, ktorí nie sú vo firme priamo zamestnaní. Politiky vypracúva spravidla IT oddelenie v spolupráci s právnym a HR oddelením. Týkajú sa rizika a zodpovednosti, úrovne služieb podpory, školenia a financovania.

Na ilustráciu rizík, dôsledkov a možných riešení uvedieme dva scenáre.

1. Notebooky

Pochopiteľne, zamestnanci nechcú, aby im firmy plne spravovali ich súkromné zariadenia. Chcú na nich pracovať z domu, ale zároveň si na ne chcú inštalovať hry a aplikácie, a to aj z iných zdrojov, než je oficiálny aplikačný obchod pre príslušnú platformu.

Dôsledky: Vzhľadom na relatívne vysokú pravdepodobnosť straty alebo krádeže zariadenia, ak firma dôsledne nepresadzuje politiky ochrany údajov a ich šifrovania, sú súkromné zariadenia doslova bránou na únik údajov a prienik malvéru dovnútra firmy prostredníctvom pripojenia LAN a VPN.

Odporúčanie: Súkromným zariadeniam by nemalo byť povolené pripájanie do firemnej siete inak než cez zabezpečený prístup VPN. Každé zariadenie musí mať najnovšiu aktualizáciu operačného systému a hlavne musí mať nainštalovaný antimalvérový softvér. Prípadne používateľ môže pristupovať k podnikovým aplikáciám a údajom len prostredníctvom online portálu pripojeného cez zabezpečené pripojenie. V nevyhnutných prípadoch, ak treba mať možnosť pracovať aj offline, je riešením dobre zabezpečený virtualizovaný počítač.

2. Smartfóny

Rizikom sú neregistrované súkromné smartfóny, prípadne tablety s aplikáciami pripojenými do firemných systémov a databáz.

Dôsledky: Do firemnej IT infraštruktúry prenikajú zariadenia, ktoré môžu byť pripojené k podnikovým systémom. Zdôrazňujeme slovo môžu. Pri neregistrovaných zariadeniach to totiž nikto presne nevie. Pri smartfónoch používatelia oceňujú operatívnosť, teda schopnosť okamžitého nábehu a vypnutia. Z toho však vyplýva veľké riziko. Používatelia môžu odísť od zariadenia bez ukončenia aplikácie a odhlásenia sa od siete. Pri práci doma sa k aplikáciám prihláseným k podnikovým sieťam dostanú napríklad deti a ich kamaráti. Dá sa v takejto situácii vôbec hovoriť o nejakom zabezpečení?

Odporúčanie: Nijaké zariadenie by nemalo získať prístup k akýmkoľvek firemným IT službám bez spoľahlivého overenia zahŕňajúceho príslušné certifikáty. Musí byť definovaná a predovšetkým vynútená politika ich bezpečného používania a postup pri prípadných incidentoch typu straty či krádeže, ktoré by mal zamestnanec okamžite oznámiť firme.

ZODPOVEDNOSŤ ZA ZABEZPEČENIE

IT si udržuje kontrolu na úrovni zariadení definovaním politík a obmedzením zmien nastavenia zabezpečenia alebo sťahovania aplikácií, ktoré nie sú priamo spojené s obchodným využitím, ale môžu byť dôležité pre nepriamu podporu firemných aktivít. Typický príklad sú aplikácie napojené na sociálne siete. V konečnom dôsledku IT preberá všetku zodpovednosť za bezpečnosť, preto musí obmedziť správanie koncových používateľov napríklad vynucovaním dodržiavania politík. Skúsenosti ukázali, že pokusy presadiť zákaz všetkých „nebiznisových" aplikácií vedú k nespokojnosti, ba až k otvoreným vzburám koncových používateľov. To v lepšom prípade. V horšom prípade zamestnanci nevynútené pravidlá v tichosti obchádzajú.

METODIKY A ODPORÚČANIA

Bezpečnostní konzultanti odporúčajú štruktúrovaný prístup k zamestnancom, ktorí používajú vlastné zariadenia, s rôznym stupňom voľnosti a podpory a akceptovateľnými kompromismi pre obidve strany. Ten, kto vyberá typ zariadenia a zariadenie vlastní, je úplne alebo z veľkej časti zodpovedný za softvérovú podporu a riešenie bezpečnostných hrozieb. Možnosti IT oddelenia firmy, čo sa týka správy heterogénnych súkromných zariadení, sú limitované hlavne kapacitami. Možnosti používateľov zas limitujú hlavne odborné znalosti a ochota niesť osobnú zodpovednosť za dôsledky prípadných incidentov.

Väčšina hierarchických modelov využíva tri základné kategórie služieb na podporu a zabezpečenie. V každej kategórii definuje typy koncových zariadení a rozdelenie kompetencií a povinností.

Plne spravované: IT oddelenie je stopercentne zodpovedné za podporu a zabezpečenie zariadení v ich vlastníctve. Táto kategória je vhodná pre používateľov, ktorí nemajú záujem participovať na správe a zabezpečení svojich zariadení a uspokoja sa s výberom zariadení poskytovaných IT oddelením.

Čiastočne spravované: V tejto kategórii sú povinnosti rozdelené medzi IT oddelením a používateľom. IT poskytuje zoznam typov zariadení, pre ktoré možno poskytnúť podporu. Model zabezpečenia je založený na izolácii cez zabezpečený prístup (tenký klient, sandbox, kontajnery...). Táto kategória sa hodí pre technicky fundovaných koncových používateľov, ochotných investovať svoj osobný čas do úkonov spojených s podporou a zabezpečením. IT by malo vzdelávať koncových používateľov o rozsahu týchto povinností.

Výnimky: Táto kategória by mala byť dostupná len za špecifických okolností, prípadne pre kľúčových výkonných zamestnancov, pretože náklady na poskytnutie pomoci sú v takomto prípade veľmi vysoké.

Tento model zároveň predpokladá možnosť zmeny úrovne podpory. Napríklad koncový používateľ si zvolil plán, v ktorom si môže vybrať zariadenie a prevziať na seba bremeno podpory. No po niekoľkých mesiacoch zistí, že si to vyžaduje priveľa času. V ďalšej perióde má takýto používateľ možnosť prejsť na plán, ktorý ponúka väčšiu podporu zariadení, ale menšiu flexibilitu pri ich výbere. Niektorí zamestnanci budú, naopak, chcieť prejsť od plne podporovaného plánu na flexibilné plány. Tento prístup umožňuje koncovým používateľom prakticky vyskúšať možnosti, práva a povinnosti svojho výberu a v prípade potreby plán zmeniť.

ĽUBOSLAV LACKO, NEXTECH

ZABEZPEČENIE MOBILNÝCH ZARIADENÍ

Mobilné zariadenia, teda smartfóny a do určitej miery aj tablety majú obrovský potenciál zvyšovať produktivitu pracovníkov, ktorých činnosť závisí od operatívneho prístupu k informáciám. Týka sa to tak manažérov, ako i radových zamestnancov. Smartfóny a tablety už majú nezastupiteľnú úlohu prakticky vo všetkých sférach biznisu. Priekopníkmi boli klientske aplikácie systémov ERP a CRM.

Vyššia mobilita vedie spravidla k lepšej organizácii času, pretože pracovník má prístup k svojej agende a dokumentom kedykoľvek, kdekoľvek a naprieč širokým spektrom zariadení. Mobilita, variabilita a sloboda vedú v konečnom dôsledku k vyššej spokojnosti pracovníkov. Aby sme to spresnili, pracovníkov využívajúcich mobilné zariadenia. Bezpečnostných expertov či pracovníkov IT oddelení zodpovedných za bezpečnosť však pojmy variabilita a sloboda doslova desia. Preto treba definovať politiky a pravidlá využívania mobilných zariadení vo firme či organizácii.

„NAJVÄČŠIA VÝZVA V OBLASTI FIREMNÝCH MOBILNÝCH ZARIADENÍ JE ZABEZPEČENIE A OCHRANA INFORMÁCIÍ."

O neslávne prvenstvo medzi hrozbami súperia škodlivé aplikácie, predovšetkým na platforme Android, kde je benevolentnejšia kontrola aplikácií pred ich zaradením do aplikačného obchodu, so stratami a krádežami mobilných zariadení a v neposlednom rade s nízkym uvedomením manažérov a zamestnancov.

Najčastejšími hrozbami v oblasti mobilnej bezpečnosti sú:

- strata alebo krádež mobilného zariadenia,
- inštalácia škodlivej aplikácie,
- pripojenie na nezabezpečenú bezdrôtovú sieť,
- infekcia po kliknutí na škodlivý hyperlink.

Výsledky prieskumov medzi manažérmi IT firiem ukázali, že takmer polovica respondentov netušila, či ich firma má zavedené bezpečnostné politiky ohľadne používania mobilných zariadení. Uvedomenie medzi zamestnancami bude ešte nižšie. Z toho logicky vyplýva, že kto nepozná pravidlá, nemôže ich ani dodržiavať.

ZÁSADY ZABEZPEČENIA MOBILNÉHO PRÍSTUPU

Základom je stanovenie firemných pravidiel a dôsledná kontrola ich dodržiavania. Minimálny „balíček" ochranných opatrení tvorí povinné heslo pri odomykaní telefónu alebo tabletu, povinný time-out s automatickým odpojením pri nečinnosti, vyžadovanie použitia VPN pri pripojení na firemné servery a šifrovanie všetkých dát na zariadení. Dôležitou zásadou

pri prevádzkovaní sietí Wi-Fi je používať rovnakú bezpečnostnú politiku ako pri klasických notebookoch. Ideálne je, keď môže IT oddelenie spravovať konfiguráciu a aktualizáciu bezpečnostného softvéru centrálne a bezdrôtovo pre všetky registrované zariadenia.

Ak má firma vytvorené bezpečnostné politiky, je veľmi dôležité aj vynútenie ich dodržiavania. Dôležité je vykonávať periodický audit, pri ktorom pracovník systémového zabezpečenia overí dodržiavanie bezpečnostných pravidiel na náhodne vybraných prístrojoch. Vzhľadom na splývanie pracovného a osobného života sa však dostávame na hranicu medzi osobným a firemným. Dá sa predpokladať, že zamestnanci nebudú len tak bez reptania prijímať prehliadku citlivého súkromného obsahu. Aj z tohto dôvodu je dôležitá osveta – pravidelné organizovanie školení na tému zabezpečenia mobilov a tabletov, pretože pozitívny prístup k opatreniam môže mať len ten pracovník, ktorý rozumie ich zmyslu.

OPRÁVNENIA PRE MOBILNÉ APLIKÁCIE

Škodlivý kód sa môže skrývať aj v aplikáciách, ktoré si používatelia stiahnu do svojich smartfónov, a to dokonca aj v prípade, ak si aplikácie stiahnu z oficiálnych aplikačných obchodov. Moderné mobilné platformy sú však koncipované tak, že aplikácia bez ohľadu na platformu môže robiť len to, čo jej používateľ povolí.

Aplikácie, hlavne také, ktoré si nainštalujete mimo aplikačného obchodu z nedôveryhodných zdrojov, vás môžu poškodiť nielen tak, že bez vášho vedomia budú posielať SMS správy na spoplatnené SMS služby. Napríklad ak aplikácia získa prístup k vašim kontaktom, môže ich rôznym spôsobom zneužiť. V niektorých prípadoch sa dajú zneužiť aj fotografie či dokumenty uložené v smartfóne.

Preto aplikácie využívajúce funkcie, ktoré by mohli narušiť používateľovo súkromie alebo ho nejakým spôsobom poškodiť, musia mať od používateľa povolenie, aby mohli tieto funkcie využívať.

Skúste si najskôr trochu spytovať svedomie a spomeňte si, aké povolenia ste udelili pre tri posledné aplikácie, ktoré ste do svojho smartfónu nainštalovali. V starších verziách Androidu sa pred inštalovaním aplikácie z Google Play zobrazil zoznam povolení, ktoré aplikácia bude vyžadovať, a museli ste s nimi vyjadriť súhlas. Niektoré aplikácie mali takto deklarovaných povolení veľa, takže záujemcovia o aplikáciu, dychtiví vyskúšať jej možnosti, zoznam mechanicky odsúhlasili a aplikáciu si nainštalovali. S odstupom času nemali šancu spomenúť si, ktorá aplikácia aké povolenia využíva. Iní používatelia si aplikáciu vyžadujúcu udelenie povolení nainštalovali a prvýkrát ju spustili neskôr, keď už zabudli, aké potenciálne nebezpečné funkcie aplikácia využíva. Od verzie Android 6.0 bol tento mechanizmus prepracovaný. Aplikácia nevyžaduje udelenie povolení, ktoré na svoje fungovanie potrebuje, ihneď po inštalácii, ale až pri prvom použití príslušnej funkcionality, napríklad pri prvom prístupe ku kontaktom.

ŠIFROVANIE DÁT

Pri použití šifrovania sa dáta ukladajú vo forme, ktorú možno prečítať iba vtedy, keď je váš telefón alebo tablet odomknutý. Odomknutím šifrovaného zariadenia dešifrujete dáta. Šifrovanie poskytuje dodatočnú úroveň ochrany pre prípad, že dôjde k odcudzeniu zariadenia. V šifrovanom zariadení sa šifrujú všetky osobné údaje. To zahŕňa napríklad váš e-mail, správy SMS, kontakty, dáta účtu Google či iCloud, dáta aplikácií, fotky, médiá a stiahnuté súbory. Na zariadeniach s Androidom nie je šifrovanie aktivované implicitne, ale treba túto funkciu zapnúť. Na väčšine zariadení stačí klepnúť na položky Nastavenia, potom Zabezpečenie a potom Šifrovať telefón. Šifrovanie trvá niekedy aj hodinu či viac a vyžaduje pripojenie k nabíjačke počas celého procesu, ale robíte tak iba raz.

BEZPEČNOSTNÉ PLATFORMY

Príkladom riešenia na bezpečné používanie smartfónu vo firmách, prípadne v rámci BYOD aj v bežnom živote je bezpečnostná platforma Samsung Knox. Táto platforma sa využíva nielen na zabezpečenie smartfónov, ale je súčasťou všetkých podnikových riešení a služieb spoločnosti Samsung. Rieši zabezpečenie počnúc SoC čiže čipmi a prechádza cez každú

jednotlivú vrstvu vrátane operačného systému a aplikačných vrstiev. Tvorcovia tejto bezpečnostnej platformy správne predpokladali využívanie smartfónu na firemné aj súkromné účely. Samsung Knox preto napomáha moderný mobilný životný štýl aj tým, že umožňuje oddelenie profesionálnych informácií od osobných na tom istom zariadení cez Secure Folder. Secure Folder využíva kontajnerovú technológiu Knox na poskytnutie bezpečného priestoru oddelene od ostatných aplikácií, správ a informácií, ktoré vytvárajú dodatočnú vrstvu zabezpečenia. To je ideálne pri spravovaní firemných zariadení, ktoré zamestnanci často využívajú aj na súkromné účely.

Keďže bezpečnostné riešenie Samsung Knox je založené na virtualizácii, umožňuje vytvoriť dve zariadenia v jednom – jedno súkromné a jedno firemné. Okrem toho umožňuje vďaka API nastaviť používateľské profily a spravovať cez konzolu Mobile Device Management (MDM) viac zariadení naraz. Platforma Samsung Knox poskytuje viacvrstvovú ochranu, ktorá izoluje a šifruje firemné dáta prostredníctvom šifrovania na zariadení a neustále monitoruje integritu zariadenia. S Knox Configure môžu firmy úplne prispôsobiť a ušiť na mieru zariadenie, ktoré vyhovuje prostrediu, pre ktoré je určené. IT manažérom poskytuje konfiguráciu, nasadenie aplikácií a možnosti personalizácie UI/UX, ako aj služby vzdialenej hromadnej registrácie a poskytovania služieb, čím úplne ovládajú svoje mobilné riešenie od začiatku do konca.

Ak firma zaraďuje do správy väčšie množstvo zariadení, možno využiť produkt Knox Mobile Enrollment, ktorý na základe vytvorenia profilu na Mobile Enrollment serveri umožní aktivovať zariadenie bez vlastného zásahu IT, čo šetrí čas a náklady na IT. Pri hromadnej dodávke niekoľkých desiatok či dokonca stoviek smartfónov do organizácie sa tým dá ušetriť veľa času a ďalšie dodatočné náklady na IT odborníkov.

SPRÁVA MOBILNÝCH ZARIADENÍ - MDM

Z povestných trojpísmenových skratiek pre subsystémy podnikovej informatiky sa pre systémy na správu mobilných zariadení zaužívalo označenie MDM (Mobile Device Management). Požiadavky kladené na MDM môžeme zhrnúť takto:

- Inventarizácia zariadení (Inventory Assets) – zoznam spravovaných zariadení, ich HW a SW konfigurácia, aktuálne nastavenia a pod.
- Automatizované nasadenie zariadení (Device Enrollment) – automatizovaná a vzdialená distribúcia nastavení do spravovaných zariadení
- Bezpečnosť (Security) – Remote Lock, Remote Wipe, Device Track, Encryption
- Automatizovaná distribúcia a správa politík (Policy Enforcement and Compliance)
- Kontajnerizácia (Containerization) – „obalenie" dát alebo aplikácií a ich oddelenie od ostatného okolia (OS, iné aplikácie)
- Správa aplikácií (MAM)
- Správa obsahu (MCM)
- Reporting
- Podpora BYOD (Bring Your Own Device)

Moderné systémy MDM (Mobile Device Management) poskytované formou SaaS sú vďaka flexibilite, škálovateľnosti a efektívnosti nákladov v porovnaní s on-premise riešeniami prijímané firmami a organizáciami veľmi pozitívne. Umožňujú aj distribúciu súborov a ich zdieľanie prostredníctvom zabezpečených spravovaných zložiek na súkromných zariadeniach či verejných cloudových službách.

Komplexné riešenie MDM by podľa odporúčaní analytikov malo byť vybudované na štyroch hlavných pilieroch:

- Správa softvéru – schopnosť riadiť a podporovať mobilné aplikácie, obsah a operačné systémy
- Správa sieťových služieb – schopnosť získať informácie zo zariadení ohľadne ich lokalizácie a používania vrátane informácií o miestnych mobilných a bezdrôtových sieťach (WLAN)
- Správa hardvéru – správa majetku, podpora
- Správa zabezpečenia – zabezpečenie, overovanie a šifrovanie

Aby produkty a služby, ktoré pomáhajú podnikom zvládnuť nasadenie mobilných zariadení, zodpovedali definícii MDM, musia spĺňať minimálne tri z týchto kritérií.

ĽUBOSLAV LACKO, NEXTECH

HAVARIJNÝ PLÁN, REAKCIE NA INCIDENTY, POSTUP OBNOVENIA FUNGOVANIA IT

Táto stať by mohla mať aj názov Manažment bezpečnostných incidentov. Cieľom je vypracovanie a aktualizácia účinných postupov na konzistentné a účinné riešenie bezpečnostných incidentov vrátane určenia zodpovednosti manažérov a zamestnancov.

V prvom rade treba mať postupy na oznamovanie bezpečnostných incidentov. Ak za zistí, že došlo k akémukoľvek druhu bezpečnostného incidentu, prípadne existuje odôvodnené podozrenie, že takýto incident nastal, je potrebné vedieť, komu a akou formou ho neodkladne nahlásiť. V mnohých prípadoch, napríklad pri úniku osobných údajov, sa musí tento incident oznámiť príslušnej inštitúcii.

V TEJTO PUBLIKÁCII VEĽAKRÁT ZDÔRAZŇUJEME VÝZNAM PREVENCIE, ČIŽE BEZPEČNOSTNÝM INCIDENTOM TREBA PREDCHÁDZAŤ, PRETO JE NEVYHNUTNÉ OZNAMOVAŤ NIELEN INCIDENTY, ALE AJ ODHALENÉ ČI POTENCIÁLNE ZRANITEĽNÉ MIESTA.

Po nahlásení bezpečnostného incidentu treba analyzovať situáciu a jej potenciálne dôsledky a rozhodnúť o čo najúčinnejšej reakcii, ktorá by minimalizovala prípadné škody. Keďže hlavne v prípade odcudzenia a následného zneužitia údajov, ich zašifrovania či úmyselného vyradenia niektorých systémov ide o veľké škody a z legislatívneho hľadiska je to trestný čin, je potrebné zaistiť forenzné dôkazy.

Súčasťou havarijného plánu by mali byť aj postupy, ako čo najrýchlejšie obnoviť funkčnosť systémov, inak povedané, ako sa po incidente čo najrýchlejšie zotaviť. Spravidla to zahrnuje obnovu údajov zo zálohy, v prípade virtualizovanej infraštruktúry možno obnoviť virtuálne servery zo záloh ich obrazov a podobne. Postupy na obnovu normálneho fungovania IT podpory biznisu v čo najkratšom možnom čase s minimálnymi stratami – či už priamymi finančnými, alebo nepriamymi, ako sú napríklad strata reputácie a následne zákazníkov – sú súčasťou DRP (Disaster Recovery Plan) a BCP (Business Continuity Plan). DRP je plán, ktorý definuje, ako sa firma zotaví po bezpečnostnom incidente, a BCP je súbor postupov, ktoré zabezpečia, že firma bude aj v prípade prebiehajúceho bezpečnostného incidentu naďalej fungovať.

Z predchádzajúcej state vymedzujúcej, čo majú DRP čiže plán obnovy po havárii a BCP čiže plán kontinuity fungovania firmy zabezpečiť, je zrejmé, že ide o sofistikované postupy, na ktoré menšia firma s predmetom podnikania mimo IT nemá kapacity. Riešením je využiť služby firmy, ktorá sa na takúto činnosť špecializuje, takže má v tejto oblasti dlhoročné skúsenosti a tím kvalifikovaných odborníkov.

Plán, nech je akýkoľvek kvalitný, nie je príliš užitočný, ak si ho kompetentní zamestnanci neosvoja. Preto by sa mali realizovať aj pravidelné školenia, nielen čo sa týka znalostí postupov, ale aj ich praktickej realizácie. Súčasťou školení by preto mali byť aj praktické cvičenia, kde si pracovníci na cvičných incidentoch tieto postupy vyskúšajú.

Hovorí sa, že najlepšie sa učí na cudzích chybách, ale ak už vo firme nejaký bezpečnostný incident nastal, treba sa z neho poučiť a snažiť sa zabrániť, aby k rovnakej alebo podobnej situácii už nedošlo.

ĽUBOSLAV LACKO, NEXTECH

ÚVODNÉ FOTO ZDROJ: Luis Villasmil / unsplash.com/

ZABEZPEČENIE ÚDAJOV

Údaje sú pre väčšinu firiem jedno z najcennejších aktív (ak nie vôbec najcennejšie). Často sa konštatuje, že údaje sú ropou tretieho tisícročia a všetci vieme, že o ropu sa viedlo niekoľko vojen. Analogicky sa podnikajú kybernetické útoky na firmy s cieľom získania údajov. Preto treba údaje, ako významný atribút konkurencieschopnosti, čo najlepšie ochrániť.

ŠIFROVANIE

Šifrovanie je proces kódovania informácií tak, aby ich neoprávnené osoby nedokázali prečítať. Na rozdiel od iných spôsobov ochrany je šifrovanie aj veľmi účinné. Možno si poviete, že ak majú vaši zamestnanci notebooky chránené silným prístupovým heslom, zlodejovi alebo nepoctivému nálezcovi budú nanič. Ďalší veľký omyl! Stačí z „ukoristeného" počítača vybrať disk a pripojiť ho k inému počítaču ako externý. Pokiaľ disk nie je zašifrovaný, dajú sa z neho skopírovať úplne všetky údaje.

Sila šifrovania zvyčajne zodpovedá dĺžke kľúča (v bitoch) a použitému šifrovaciemu algoritmu. Najjednoduchší spôsob, ako prelomiť šifrovanie, je vyskúšať všetky možné kľúče. Tento postup sa nazýva útok hrubou silou (brute force attack), používaním dlhších kľúčov sa však stal neúčinným. Na ilustráciu, keby ste chceli hrubou silou prelomiť 128-bitový kľúč AES, každý z približne 7 miliárd ľudí na Zemi by musel skúšať 1 miliardu kľúčov za sekundu po dobu 1,5 trilióna rokov, aby sa vyskúšali všetky kľúče. Preto sa útočníci zvyčajne nepokúšajú spätne rekonštruovať algoritmus alebo prelomiť kľúč hrubou silou. Namiesto toho hľadajú zraniteľnosti šifrovacieho softvéru, prípadne sa pokúšajú infikovať systém škodlivým kódom, ktorý dokáže odchytávať heslá alebo kľúče v čase ich použitia.

„FIRMY ZAVÁDZAJÚ NOVÉ TECHNOLÓGIE, V POSLEDNOM ČASE HLAVNE CLOUDOVÉ, NA ANALÝZU VEĽKÝCH DÁT V REÁLNOM ČASE, TAKŽE OCHRANE INFORMÁCIÍ, KTORÉ VZNIKNÚ AKO VÝSLEDOK ANALÝZ, JE POTREBNÉ VENOVAŤ OBZVLÁŠŤ VEĽKÚ POZORNOSŤ. "

Pri výbere vhodného riešenia na šifrovanie treba prihliadať na niekoľko veľmi dôležitých kritérií. Predovšetkým jednoduchosť používania pre bežných zamestnancov. Musíme si uvedomiť, že zašifrované počítače a externé disky nebudú používať experti z IT oddelení, ale bežní zamestnanci. Ak bude riešenie zložité a neustále bude vyžadovať zadávanie dlhých hesiel, používateľ si ich napíše pod displej na nálepku a ochrana stráca zmysel. Prípadne sa budú snažiť šifrovaniu vyhnúť aj za cenu porušovania firemných bezpečnostných politík či interných smerníc. Jednoduchá by mala byť aj správa bezpečnostného riešenia, a to napriek tomu, že ju budú robiť ľudia z IT oddelenia

alebo externá firma spravujúca počítače. Najčastejším úkonom správcov bude pravdepodobne obnovovanie zabudnutých prístupových kľúčov, preto by tento úkon mal byť čo najjednoduchší, no jednoduchosť nesmie byť na úkor bezpečnosti. Pri výbere riešenia treba zohľadniť použité šifrovacie algoritmy a priemyselné štandardy, hlavne FIPS-140-2. Je dôležité, aby riešenie bolo overené, certifikované, prípadne schválené autoritami, napríklad americkým Národným inštitútom štandardov a technológií (NIST), bolo certifikované kľúčovým hráčom na trhu (napríklad OPSWAT) a darilo sa mu v nezávislých testoch.

SÚ VEĽKÉ DÁTA AJ VEĽKOU HROZBOU?

Na takúto jednoznačne položenú otázku sa paradoxne dá odpovedať, že ani nie, aspoň nie priamo. Terabajty údajov zhromaždené každý deň priemerne veľkou firmou síce obsahujú cenné informácie, ale tie treba z nich najskôr sofistikovanými postupmi vydolovať. Dobrá analógia je, keby niekto ukradol fúrik, nákladné auto alebo hoc aj plný vagón rudy, v ktorej je malé promile zlata alebo platiny. No keby ukradol čo i len malé množstvo finálneho produktu (v tomto prípade drahého kovu), ktoré sa vojde do vrecka, spôsobil by veľkú škodu. Čiže keby narušiteľ ukradol nie terabajty „surových" údajov, ale z nich vydolované informácie, ktoré sa vojdú na jednu obrazovku manažérovho iPadu, škoda by mohla byť obrovská. Veľké dáta často majú na zabezpečenie dokonca pozitívny vplyv. Výsledkom ich analýzy sú aj informácie umožňujúce odhaliť a zastaviť bezpečnostné incidenty oveľa rýchlejšie, než firmy boli schopné predtým.

PRAVIDLÁ NA ZDIEĽANIE ÚDAJOV S PARTNERMI

Neodmysliteľnou súčasťou takmer všetkých priemyselných odvetví sú dodávateľsko-odberateľské vzťahy. Do ich rámca patrí aj zdieľanie informácií a využívanie spoločných aplikácií a databáz, takže aj subdodávatelia a obchodní partneri môžu byť pre firmy bezpečnostným rizikom. Preto treba mať nastavené pravidlá na narábanie s dátami. Jedna z hlavných výhod implementácie pravidiel na spoluprácu s tretími stranami je v tom, že definuje oblasti zodpovednosti pre obe zúčastnené strany. Vďaka tomuto nastaveniu sa zvyšuje pravdepodobnosť, že podnik dostane kompenzáciu od dodávateľa, ak sa on stane vstupným bodom pre útok.

„PODĽA VÝSLEDKOV PRIESKUMOV VÄČŠINA VEĽKÝCH FIRIEM MÁ DEFINOVANÉ PRAVIDLÁ, KTORÉ VYSVETĽUJÚ PARTNEROM A DODÁVATEĽOM, AKO PRACOVAŤ SO ZDIEĽANÝMI ZDROJMI A DÁTAMI, PRIČOM JE TU ZAHRNUTÁ AJ INFORMÁCIA O MOŽNÝCH POKUTÁCH, KTORÉ MÔŽU BYŤ V PRÍPADE INCIDENTOV APLIKOVANÉ."

ĽUBOSLAV LACKO, NEXTECH

ZDROJ: MACROVECTOR / FREEPIK

ZABEZPEČENIE PODNIKOVEJ SIETE

Pre väčšinu firiem bez ohľadu na veľkosť je internet jeden z hlavných pracovných nástrojov, takže prípadné výpadky pripojenia sú neakceptovateľné. Navyše všadeprítomný cloud podčiarkuje dôležitosť sieťovej infraštruktúry, predovšetkým spoľahlivosť, bezpečnosť a, samozrejme, rýchlosť pripojenia, či už v kancelárii, alebo mobilného pripojenia. Aj v tomto prípade platí, že kvalitu určuje najslabší článok, takže infraštruktúra poskytovateľa cloudových služieb môže byť akákoľvek výkonná a na maximum zabezpečená, pri nespoľahlivej a nedostatočne zabezpečenej sieti vám to nebude nič platné.

KÁBLE ALEBO WI-FI?

Na prvý pohľad by sa mohlo zdať, že vzhľadom na výhody Wi-Fi, ako je predovšetkým operatívnosť a nezávislosť od polohy v objekte pokrytom signálom, nie je vlastne čo riešiť. Navyše už nielen smartfóny a tablety, ale ani moderné ultratenké notebooky neumožňujú pripojiť eternetový kábel, aspoň nie priamo, takže Wi-Fi je jednoznačná voľba. Máte pravdu, hlavne ak vaša firma sídli v samostatnom objekte. Vo veľkých obchodných centrách, kde v jednom priestore koexistuje množstvo sietí Wi-Fi, logicky vznikajú interferencie a znižuje sa úroveň kvality prenosu. Takisto z hľadiska zabezpečenia treba prihliadať na to, že signál siete je dostupný v dosahu antén routerov či opakovačov aj mimo priestorov firmy.

Moderné siete Wi-Fi využívajúce pásmo 5 GHz sú vzhľadom na viaceré kanály schopné ponúknuť kvalitnejšie pripojenie a vďaka väčšej frekvencii umožňujú dosiahnuť vyššie prenosové rýchlosti. Majú však aj nevýhody vyplývajúce z fyzikálneho princípu šírenia rádiových vĺn. Vyššia frekvencia z tohto pohľadu v porovnaní s 2,4 GHz v praxi znamená horšiu priechodnosť signálu prekážkami. Teoretická maximálna prenosová rýchlosť pre najmodernejší štandard IEEE 802.11ac je 1,3 Gb/s, nový duálny štandard Wave 2 3×3 MU-MIMO teoreticky umožňuje dosiahnuť kombinovanú prenosovú rýchlosť až 1,6 Gb/s, ale v praxi dosahované rýchlosti v reálnom prostredí sú oveľa nižšie, pri veľmi kvalitných routeroch priemerne 350 Mb/s, takže 10 či 100-gigabitovému eternetu konkurovať nemôžu.

„MODERNÁ BEZDRÔTOVÁ SIEŤ MUSÍ UMOŽNIŤ ODDELIŤ FIREMNÚ SIEŤ OD ZÁKAZNÍCKEJ, A TO AJ V MALÝCH FIRMÁCH, AK K VÁM CHODIA ZÁKAZNÍCI ČI OBCHODNÍ PARTNERI."

Káblové pripojenie je výhodnejšie hlavne pre firmy, ktorých pracovníci často prenášajú veľké objemy údajov. Typický príklad sú reklamné agentúry, dizajnové štúdiá a podobné firmy, ktoré pracujú s veľkým objemom multimediálnych údajov, napríklad pri editovaní fotografií, videa, návrhoch CAD a podobne. Samozrejme, aj pri káblovom pripojení je reálna prenosová rýchlosť minimálne o 5 – 10 % nižšia ako maximálna deklarovaná rýchlosť.

PROJEKT SIEŤOVEJ INFRAŠTRUKTÚRY

Možno sa vám pojem projekt pre sieť malej firmy s niekoľkými zamestnancami bude zdať trochu prehnaný, je to však najdôležitejšia fáza návrhu sietí. Pri projektovaní káblového prepojenia v prenajatých priestoroch treba zmapovať existujúce vedenia, určite je niekde u správcu budovy plán kabeláže. Ak nevyhovuje, nie je problém nainštalovať káble do líšt na povrchovú montáž, prípadne ich umiestniť za krycie lišty podlahy a podobne v závislosti od konkrétnych podmienok. Vo vlastných priestoroch máte väčšie možnosti. Pokiaľ sa rekonštruuje budova, je to vynikajúca príležitosť na inštaláciu potrebnej kabeláže.

V prípade siete Wi-Fi treba nakresliť plán pokrytia a rozmiestnenia prístupových bodov s grafickým znázornením predpokladaných oblastí ich dosahu. Musíte brať do úvahy problémy s prekonávaním prekážok v prípade pásma 5 GHz. V rozsiahlejších priestoroch je potrebné zaistiť plynulý prechod od jedného prístupového bodu k inému. Veľmi významné parametre sú predpokladaný počet používateľov, ich zariadení a nároky na prenosovú rýchlosť. Dôležitý je aj princíp prideľovania IP adries a najdôležitejší je bezpečnostný projekt siete.

Pri konfigurácii siete pre hostí treba zvážiť, či povolíte, alebo zakážete komunikáciu hostí medzi sebou. Ak máte vo firme pevný pracovný čas, aspoň čo sa týka rokovaní so zákazníkmi a partnermi, môžete na vyššiu bezpečnosť nastaviť aj časy, keď bude táto hosťovská sieť dostupná.

ZABEZPEČENIE FIREMNEJ SIETE

Zabezpečenie odporúčame riešiť ako prioritnú tému, najmä čo sa týka sietí Wi-Fi. Dôkladným zabezpečením firemnej či v prípade drobného podnikateľa podnikajúceho v rodinnej firme aj domácej siete zamedzíte útočníkovi prístup do tejto siete. V mnohých firmách si povedia, že údaje v ich sieti nie sú natoľko citlivé, aby ich bolo treba obzvlášť chrániť. Skutočne? Aj vzhľadom na nové pravidlá spracovávania osobných údajov deklarovaných v nariadení GDPR? Dokonca aj v zriedkavom prípade, keby ste mali pravdu a únik vašich údajov by predstavoval prijateľné riziko, je tu iný potenciálny problém. Útočníci totiž nemusia potrebovať vaše údaje (hoci sú cenné pre vás, útočník ich možno nedokáže zneužiť), ale vašu identitu. Po prieniku do vašej siete totiž kyberkriminálnici využívajú vašu sieť, budú de facto páchať nelegálnu činnosť vo vašom mene, napríklad posielať spam, šíriť škodlivý kód či uskutočňovať iné, ešte nebezpečnejšie aktivity. Keď tieto aktivity začnú vyšetrovať kompetentné orgány, zistia, že ich pôvodcom je vaša IP adresa. A vy máte postarané o veľký problém. Kým sa všetko vysvetlí, môžu vám zabaviť servery či spôsobiť iné nepríjemnosti, ktoré ochromia chod vašej firmy.

VYUŽÍVAJTE SILNÉ ŠIFROVANIE SIETE WI-FI

Aktivujte jeden zo šifrovacích štandardov: WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise. Dôrazne varujeme pred používaním šifrovania technológiou WEP, tá je značne zastaraná a je ľahšie ju prelomiť. Protokol WEP obsahuje niekoľko slabých miest, ktoré umožňujú jeho napadnutie a vo všeobecnosti sa nepovažuje za bezpečný. Využíva symetrický spôsob šifrovania, teda na šifrovanie a dešifrovanie sa používa rovnaký algoritmus a rovnaký kľúč. Autentizácia v rámci WEP je považovaná za veľmi slabú až nulovú. Štyridsaťbitový používateľský kľúč na autentizáciu je statický a rovnaký pre všetkých používateľov danej siete (zdieľaný kľúč). Klienti ju používajú spolu so svojou MAC adresou na autentizáciu k prístupovému bodu. Autentizácia sa uskutočňuje iba jednostranne, prístupový bod sa neautentizuje.

Odporúčame používať pripojenie WPA2 s PSK, ktorý umožňuje autentifikáciu a výmenu kľúčov na hotovom štandarde 802.11i a určuje nevyhnutnosť používať CCMP – Counter-Mode/CBC-MAC protokolu (AES). WPA (Wi-Fi Protected Access) používa

rovnako ako WEP šifrovací mechanizmus RC4, ktorý bol zvolený hlavne na zaistenie kompatibility s existujúcimi zariadeniami. Vďaka tomu bola modernizácia možná prostredníctvom softvérových zmien. WPA používa protokol TKIP na riešenie nedostatkov pri WEP, implementuje použitie dynamických kľúčov, ale takisto umožňuje použitie statických zdieľaných kľúčov na jednoduchšiu implementáciu. Medzi tri hlavné zložky WPA patrí TKIP, MIC a EAP. Takisto rieši problém s prakticky neexistujúcou autentizáciou pri WEP a ponúka rôzne režimy na jej zabezpečenie. Umožňuje využitie centralizovaného autentizačného servera, napríklad RADIUS servera, táto metóda je vhodná na podnikové použitie. Na domáce použitie a pre malé rodinné firmy je bežnejšie využitie jednoduchšieho mechanizmu prednastavených kľúčov (PSK, Pre-Shared Key). WPA2 úplne nahrádza zabezpečenie pomocou WEP. Poskytuje kompletnú bezpečnosť za pomoci implementácie nového protokolu CCMP s využitím šifrovania AES.

Autentizácia je možná dvoma spôsobmi, a to pomocou PSK alebo normy 802.1x. Použitie PSK je dostačujúce pre väčšinu domácich sietí, pre firemné siete sa však neodporúča. Treba totiž vopred nadstaviť heslo na routeri a prístupových bodoch, ktoré potom používatelia využijú pri prihlasovaní sa do siete. Toto heslo je rovnaké pre všetkých používateľov. V prípade väčšej siete alebo väčšieho počtu používateľov je takéto riešenie nepraktické, lebo pri nutnosti zmeny hesla to treba vykonať na všetkých zariadeniach. Naproti tomu autentizácia prostredníctvom 802.1x umožňuje využitie protokolu EAP alebo servera Radius. Tento variant je o niečo zložitejší na implementáciu, pre firemné prostredie je však vhodnejší. Následná správa systému je už jednoduchšia.

Vyplňte tzv. PSK (Pre-Shared key) t. j. heslo k vašej sieti Wi-Fi. Heslo by nemalo byť totožné s heslom do administrácie routera. Uskutočnite upgrade routera. Zapnite zabudovaný firewall v routeri.

Ak nepoužívate prístupy typu Web Access from WAN či FTP, vypnite ich. Zapnite WAN & LAN filter a MAC filter, kde zadefinujete presné adresy zariadení, ktoré budú mať prístup k vašej firemnej sieti. Zariadenia s inými MAC adresami ignoruje, resp. odpovie záporne. Každá sieťová karta má svoju unikátnu MAC adresu, niečo ako výrobné číslo. Na svete by nemali existovať dve sieťové rozhrania IEEE 802.11 s rovnakými MAC adresami.

POKRYTIE SIGNÁLOM

Paradoxne nebudeme riešiť rozšírenie pokrytia, ale jeho obmedzenie. Obmedzte dosah signálu len na úroveň, ktorú potrebujete. Vo firmách, kde sa pracuje s citlivým obsahom, cennými údajmi a podobne, odporúčame použiť sieťové zariadenie WIPS (Wireless intrusion prevention system), ktoré monitoruje rádiové spektrum na prítomnosť nepovolených prístupových bodov. Používajte Wireless IDS (Intrusion Detection System) – systém na detekciu prienikov, ktorý by nemal chýbať na žiadnej sieti, ktorej bezpečnosť nie je ľahostajná. IDS určené špeciálne pre WLAN sa nazývajú WIDS (Wireless IDS). IDS dokážu spozorovať konkrétne druhy útokov, nezvyčajnú prevádzku na sieti, spotvorené rámce a aj útoky DoS a urobiť na základe toho nasledujúce opatrenia:

- odfiltrovanie komunikácie prichádzajúcej od identifikovaného útočníka,
- vypnutie citlivých služieb,
- odpojenie napadnutej stanice od citlivých služieb,
- odpojenie napadnutého segmentu od zvyšku siete.

A napokon tip, ako zistíte, či je niekto cudzí pripojený na vašu sieť Wi-Fi. V konfiguračnom programe routera v sekcii Status & Log si zobrazíte DHCP Leases. V tomto logu sa zobrazia pripájané IP a MAC adresy na vašu sieť.

AUDIT FIREMNEJ SIETE

V súvislosti s pripájaním čoraz väčšieho počtu prístrojov do podnikových sietí, nielen počítačov, tabletov a smartfónov, ale aj inteligentných spotrebičov (veď inteligentné chladničky, kávovary a iné zariadenia sa nevyužívajú len v domácnostiach, ale aj vo firmách) sa kladú vysoké požiadavky aj na zabezpečenie siete. Aby bolo možné sieť chrániť, najskôr treba spoznať jej konfiguráciu. Dodávatelia antivírusového softvéru ponúkajú účinné nástroje na audit siete, či už lokálne, alebo formou cloudovej služby, ktorá umožňuje otes-

tovať firemný router na rôzne zraniteľnosti, ako je napríklad slabé alebo dokonca implicitné heslo, prípadne neaktuálny firmvér. Poskytuje zoznam aktuálne pripojených zariadení, používateľ ich môže na lepšiu prehľadnosť zaradiť do rôznych kategórií. Všetky spomínané informácie sa dajú zistiť aj z konfiguračných stránok routera, ale ruku na srdce: koľko domácich používateľov to dokáže? Pripomíname, že táto funkcia len deteguje a zobrazuje informácie o potenciálnych problémoch, router nekonfiguruje. To môže urobiť používateľ často v súčinnosti s technickou podporou, ktorej umožní diaľkový prístup do svojho počítača.

VYBUDOVANIE A SPRÁVA SIETE OD EXTERNEJ FIRMY

Ak je podnikanie vašej firmy mimo oblasti informačných technológií a vo firme nemáte žiadneho dostatočne kvalifikovaného IT špecialistu, stať o projekte firemnej siete vám oprávnene bude pripadať trochu nezrozumiteľná. Ak vo firme používate sieť, ktorú vám „vybudoval" študent alebo miestny „IT špecialista" tak, že iba prepojil nakúpené routery a neobťažoval sa s nastavením ich zabezpečenia, mali by ste si znovu prečítať stať o zabezpečení siete a možných rizikách nedostatočného zabezpečenia. Alebo naopak, ak vo vašej firme máte dosť vysokokvalifikovaných a veľmi dobrých IT špecialistov, ktorí pracujú na projektoch súvisiacich s predmetom podnikania vašej firmy a zamestnávať ich rutinnými úlohami správy siete by bolo neefektívne.

Tak alebo onak, ak nezvládnete alebo nemáte kapacitu na správu IT, kde je kľúčová správa siete, riešením pre vás je vybudovanie a následná správa siete formou služby od špecializovanej externej firmy.

Okrem skúseností je výhodou externej správy aj transparentnosť. Namiesto odpovede typu „do konca týždňa si možno nájdem čas pozrieť sa na to" od vlastného správcu priebeh riešenia každej vašej požiadavky môžete sledovať na ich zákazníckom portáli. Ale nepredbiehajme. Po predbežnej objednávke vám firma najskôr vypracuje audit, v ktorom zosumarizuje používaný hardvér, softvér, prípadne aj zmapuje potenciálne hrozby. Výsledky auditu budú podkladom pre finálnu objednávku, ako aj pre projekt siete a jej zabezpečenia. Pri realizácii projektu externá firma prihliada aj na to, aby súvisiace úkony čo najmenej zasahovali do chodu vašej firmy.

„DÔLEŽITÝ ARGUMENT PRE TÚTO FORMU JE SKUTOČNOSŤ, ŽE VÄČŠINU ÚKONOV SÚVISIACICH SO SPRÁVOU ČI KONFIGURÁCIOU SIETE NAPRÍKLAD PRI PRIPOJOVANÍ POČÍTAČA A MOBILNÝCH ZARIADENÍ NOVÉHO ZAMESTNANCA MOŽNO RIEŠIŤ NA DIAĽKU."

Súčasťou objednávky je aj spôsob platby – buď formou paušálu, alebo na báze hodinovej sadzby. Na prvý pohľad sa zdá výhodnejšia paušálna platba. Vtedy nemusíte mať podozrenie, že sa riešenie problémov preťahuje, aby sa dalo zákazníkovi naúčtovať viac hodín. Takisto máte istotu, že firma zabezpečila vašu sieť maximálne, ako je schopná, nie preto, že by jej extrémne záležalo na úspechu vášho podnikania, ale jednoducho preto, aby s vašou infraštruktúrou mala čo najmenej starostí. Inak povedané, správca IT, či už interný, alebo externý, platený podľa hodín nie je motivovaný riešiť problémy rýchlo a vyriešiť ich tak, aby sa už neopakovali. Garantovaná reakčná doba je pri tejto forme externej správy sietí 3 – 5 hodín, podľa praktických skúseností sa väčšina problémov vyrieši do 30 minút. Navyše vo väčšine prípadov sa dá problém vyriešiť na diaľku bez toho, aby technik musel prísť do vašej firmy.

ĽUBOSLAV LACKO, NEXTECH

PRÍSTUP DO WI-FI

Bezdrôtové siete tvoria dôležitú súčasť firemnej infraštruktúry. Nielen smartfóny a notebooky, ale aj tlačiarne či rôzne zariadenia IoT kladú na bezdrôtové siete čoraz väčšie nároky, nielen pokiaľ ide o prenosovú kapacitu, ale aj zabezpečenie. Predovšetkým zabezpečenie prepojenia siete Wi-Fi s existujúcou infraštruktúrou a dôsledné oddelenie prístupu pre klientov či návštevy.

Nároky na zabezpečenie sa odvíjajú od určenia siete a celkovej IT architektúry. Pri budovaní siete s vysokým zabezpečením sa treba prioritne zamerať na štyri kľúčové aspekty:

- šifrovanie údajov,
- model AAA (Authentication, Authorization Accounting),
- segmentácia,
- monitoring.

Na zabezpečenie prenášaných dát vo firemnom prostredí je štandardom šifrovanie WPA2-enterprise, ktoré využíva blokovú šifru AES a dynamicky generované kľúče WPA2-enterprise a počíta s overovaním jednotlivých používateľov, a teda s nasadením AAA.

Koncept AAA zaisťuje autentizáciu čiže overenie identity, autorizáciu (pridelenie sieťových prostriedkov) a účtovanie v zmysle sledovania využívania sieťových služieb používateľmi. Na autorizáciu sa využívajú služby protokolu 802.1X a autentizáciu zaisťuje EAP.

Segmentácia čiže oddelenie bezdrôtovej siete od infraštruktúry je veľmi dôležitý bod, pretože v určitých ohľadoch stále možno považovať bezdrôtovú časť siete za nedôveryhodnú. Problémy v tejto oblasti umocňuje trend BYOD (Bring Your Own Device), v rámci ktorého si používatelia nosia do firemnej siete vlastné zariadenia (notebooky, inteligentné telefóny a tablety), ktoré nie sú pod kontrolou firmy. Môžu tak potenciálne obsahovať rôzne formy škodlivého kódu.

Dôležitá súčasť vybudovanej siete je aj jej monitoring, vďaka ktorému môžete odhaliť prípadných problémových používateľov a ďalšie hrozby. Výrobcovia zariadení WLAN väčšinou dodávajú aj špecializovaný softvér, ktorý si rozumie s ich zariadeniami a dokáže celú sieť monitorovať.

KONFIGURÁCIA A ZABEZPEČENIE

Prinášame rámcový návod, pomocou ktorého môžete nastaviť, prípadne auditovať, teda skontrolovať zabezpečenie vašej podnikovej siete. Ihneď po prihlásení do Wi-Fi routera **zabezpečte administráciu** (System Setup - Change Password) minimálne 8 – 64-znakovým heslom. Heslo by malo pozostávať zo znakov veľkej abecedy, malej abecedy, číslic a špeciálnych znakov (+-*/#&@{}<>$ß¤×÷~`;). V tomto prípade odporúčame voliť silnejšie heslo, pretože počítače a iné zariadenia zamestnancov sa prihlasujú len raz a následne si parametre prihlásenia pamätajú. **Pre návštevy, napríklad zákazníkov, dôrazne odporúčame vytvoriť samostatnú sieť, dôsledne oddelenú od firemnej siete.** Na novom routeri zvyklo byť prednastavené meno a heslo, spravidla user/user, admin/admin, administrator/administrator, a prednastavená IP adresa je zvyčajne 192.168.0.1, 192.168.1.1, 10.0.0.1, prípadne 10.10.10.1. Najnovšie routery majú už od výrobcu nastavené pomerne silné heslá, ktoré sú uvedené na vloženom papieri alebo na nálepke na zariadení. Napriek tomu odporúčame tieto heslá zmeniť. Nie preto, že by sme nedôverovali výrobcovi, ale niekto, napríklad predajca, človek z firmy, ktorá router inštalovala, prípadne niekto z vašich zamestnancov, mohol ešte pred vami router vybaliť a odfotenie štítka s implicitným heslom je otázka sekundy. Aj neskôr ktokoľvek môže v nepozorovanej chvíli nadvihnúť router a odfotiť mobilom údaje na nálepke.

SSID predstavuje označenie siete. Pri pridružení klientskeho zariadenia k stanici sa požaduje znalosť SSID siete, ku ktorej sa chcú pripojiť. Implicitne sú prístupové body nastavené, aby tento názov vysielali každých niekoľko sekúnd v administratívnej správe beacon. Týmto dáva zariadenie o sebe vedieť, aby o sieti okolité zariadenia vedeli a mohli sa k nej pripojiť. SSID sa vysiela v otvorenej forme v rade riadiacich správ, ako správa beacon, probe request, probe response, association request. Väčšinu prístupových bodov možno nastaviť tak, aby správu beacon s SSID pravidelne nevysielali, čím umožňujú skrytie siete pred bežnými používateľmi. Takéto bezpečnostné opatrenie môže byť účinné voči neskúseným používateľom, potenciálny útočník však SSID dokáže pomerne jednoducho zistiť. Stačí mu na to odpočúvať sieťovú prevádzku a odchytiť komunikáciu, keď sa niektorá zo staníc pokúša o pripojenie. Ďalší spôsob je aktívny útok, keď útočník pošle falošnú požiadavku na odpojenie inej aktívnej stanice. Tá sa následne opäť pripojí, čím prezradí SSID siete.

Ak vytvoríte silné heslo, prihlásite naň všetky zariadenia vo firme a po pol roku zistíte, že ste heslo zabudli, prípadne neuložili do vhodného správcu hesiel, je to menší problém. Vyriešite to hardvérovým resetom routera a jeho opätovným nastavením. Réžia spojená s opätovným pripájaním zariadení zamestnancov je neporovnateľne menší problém než hacknutie firemnej siete. **Odporúčame skryť názov siete**, aby nebola pri vyhľadávaní pre okolie viditeľná, pomocou funkcie Hide SSID v nastaveniach routera.

Nasledujúce odporúčanie o zmene hesla na správu routera sa vám bude zdať samozrejmé, ale čudovali by ste sa, v koľkých malých firmách používajú Wi-Fi router tak, ako ho vybalili zo škatule. O nutnosti zmeny hesla na pripojenie sa k sieti sme sa už zmienili. Zmeniť treba aj heslo v aplikácii na správu routera. Presvedčíme vás jednoduchým experimentom. Do firmy príde návšteva, napríklad obchodný partner, školiteľ alebo zákazník, a vy mu poskytnete heslo do firemnej siete, aby sa mohol pripojiť. No a teraz si na chvíľu predstavte, že vy ste tá návšteva. Skúste do webového prehliadača zadať adresu http://192.168.0.1. Je to univerzálna adresa na prístup k väčšine routerov. Zobrazí sa vám webová stránka na správu príslušného zariadenia, ktorá od vás pýta heslo. Zatiaľ je všetko v poriadku. No a teraz zadajte ako heslo „admin", čo je implicitné heslo na úvodnú konfiguráciu takmer všetkých routerov. Heslo bude akceptované a vy sa dostanete do aplikácie na správu routera a môžete si ako návšteva s firemnou sieťou robiť, čo sa vám zachce. A to už určite v poriadku nie je. Takže ako prvý konfiguračný krok zmeňte heslo do aplikácie na správu zariadenia.

ĽUBOSLAV LACKO, NEXTECH

BEZPEČNOSŤ V CLOUDE

Atraktívnosť cloud computingu, vlajkového trendu v IT, neustále rastie a z jeho výhod, hlavne čo sa týka znižovania investičných aj prevádzkových nákladov, spoľahlivosti a dostupnosti, profitujú firmy od SMB až po najväčšie korporácie. Cloud však nesprevádzajú len výhody, ale aj obavy z potenciálnych bezpečnostných rizík. Zodpovední záujemcovia o cloudové služby by si v prípravnej fáze projektu mali nielen zvoliť najvýhodnejší model ich poskytovania, ale aj analyzovať riziká. Čo by sa stalo, keby bola narušená dôvernosť, integrita alebo dostupnosť vašich údajov alebo aplikácií v cloude?

„AŽ 40 % FIRIEM UVIEDLO BEZPEČNOSŤ AKO NAJVÄČŠIU PREKÁŽKU ĎALŠIEHO ROZŠÍRENIA CLOUDU. "

Rozdelenie zodpovednosti za zabezpečenie cloudových služieb závisí od modelu ich poskytovania. Najviac zodpovednosti na seba zákazník preberá pri modeli IaaS, keď musí spravovať, a teda aj chrániť všetko, čo je z hľadiska IT architektúry situované nad vrstvou virtualizácie. Tento všeobecný výklad rozdelenia zodpovednosti je adekvátny pre všetky oblasti s výnimkou zabezpečenia. Tu sa zákazníkova zodpovednosť týka navyše aj súborov s obrazmi virtuálnych diskov. IT odborníkom netreba vysvetľovať riziká spojené s virtuálnymi servermi, preto by ich „image" súbory mali byť spoľahlivo zabezpečené šifrovaním. Ako môže zákazník ovplyvniť zabezpečenie na tejto úrovni? Predsa výberom dostatočne zabezpečenej služby od poskytovateľa, ktorý má v tejto oblasti dostatok skúseností.

RIZIKOVÉ FAKTORY

Používanie cloudu prináša aj nové riziká. Tieto riziká treba analyzovať a podľa požiadaviek na bezpečnosť dát zvoliť vhodný typ (verejný, privátny alebo hybridný) a servisný model (IaaS, PaaS alebo SaaS) cloudu. Pre všetky oblasti bezpečnosti – dátovú, sieťovú, prevádzkovú aj fyzickú – existujú riešenia, pomocou ktorých vieme dosiahnuť rovnakú bezpečnosť ako pri tradičnom budovaní vlastnej IT infraštruktúry. Podľa štatistík najväčšou bezpečnostnou hrozbou zostávajú vlastní zamestnanci, ktorí nedodržujú bezpečnostné predpisy alebo sa úmyselne pokúšajú zneužiť firemné dáta bez ohľadu na to, či sú v cloude, alebo vo vlastnom dátovom centre. Teda šesť z desiatich ľudí, ktorí od vás odídu, vás ešte aj okradne. Naproti tomu okráda vás o dáta váš mobilný operátor? Predáva ich potom konkurencii? Pravdepodobne mu v tomto ohľade dôverujete. Rovnako môžete dôverovať aj vášmu poskytovateľovi cloudových služieb. V zmluve, ktorú podpíšete, je zakotvená sankcia, ktorá by vášho poskytovateľa postihla v prípade, že by vás okradol. No nie je to jediná motivácia. Ďalšou je napríklad to, že v tomto segmente chce poskytovateľ cloudu podnikať dlhodobo a krádež by nebola ideálna referencia.

Pri verejnom cloude je ochrana reputácie poskytovateľa hlavný faktor, ktorý znižuje riziká (v prípade poškodenia reputácie poskytovateľ stratí väčšinu zákazníkov). Zo skupiny faktorov na zvýšenie rizík možno spomenúť riziko spoločnej havárie (útok DDoS na jedného zákazníka môže ovplyvniť aj ostatných).

Komunitný cloud je na tom lepšie z pohľadu faktorov na znižovanie rizík: zdroje cloudu využíva spoločná komunita a prístup je povolený iba jej členom (ku cloudu majú prístup iba autorizovaní používatelia). Riziká zvyšuje používanie spoločných zdrojov organizáciami s rôznymi požiadavkami na bezpečnosť. Hlavná výhoda privátneho cloudu je možnosť znižovať riziká postavením cloudu vo firemnej infraštruktúre (on-site nasadenie). Ako faktor na zvýšenie rizík sa pridáva personál so špecifickými znalosťami cloudu (pri on-site nasadení).

„AŽ 59 % ZAMESTNANCOV, KTORÍ OPUSTIA VAŠU FIRMU, SI SO SEBOU ODNESIE AJ VAŠE FIREMNÉ DÁTA."

Hybridný cloud zdedí výhody a nevýhody cloudov, z ktorých sa skladá, a pridá ďalší možný zdroj problémov: komunikáciu medzi prostrediami, ktoré sú v rôznych bezpečnostných zónach.

AKÉ INFORMÁCIE ULOŽIŤ DO CLOUDU?

Takmer všetko, čo má firma uložené vo vlastnom dátovom centre, môže presunúť do cloudu. Najčastejšie sú to aplikácie a dáta typu ERP, CRM, mailový systém a zdieľanie súborov. Cloud umožňuje zdieľať informácie nielen v rámci firmy, ale aj celého firemného ekosystému, t. j. vrátane zákazníkov a dodávateľov, ktorí môžu dostať prístup do určitých modulov systému ERP alebo CRM a aktívne ho využívať na vzájomnú spoluprácu.

FIREMNÝ VERZUS OSOBNÝ CLOUD

Hlavný rozdiel medzi profesionálnym cloudom a voľne dostupnými riešeniami, ako sú napríklad iCloud, OneDrive, Disk Google, je v úrovni poskytovanej služby (SLA) a v bezpečnosti takéhoto riešenia. Zamestnanci používajú voľne dostupné riešenia na zdieľanie citlivých firemných informácií so zákazníkmi a dodávateľmi. Všetko toto sa často deje bez vedomia IT oddelenia. Dôverné firemné dáta sa ukladajú mimo firmy, pravdepodobne aj mimo EÚ, čo môže byť v rozpore s podnikovými predpismi alebo regulačnými nariadeniami. Je to potenciálny zdroj úniku týchto citlivých informácií, ktorý môže poškodiť firmu v jej konkurenčnom boji.

Na druhej strane profesionálne riešenie umožňuje mať všetko pod kontrolou IT oddelenia. Dosiahnuť požadovanú úroveň poskytovanej služby (SLA) a nastaviť také bezpečnostné pravidlá, aby citlivé firemné informácie nemohli byť zneužité, ale aby sa zároveň nestratila žiadna výhoda, ktorú umiestnenie dát do cloudu prináša.

CLOUD A MOBILITA

Cloud umožňuje mobilným pracovníkom bezpečný prístup k podnikovým dátam a aplikáciám odkiaľkoľvek a kedykoľvek, umožní im zdieľať dáta s ostatnými spolupracovníkmi, synchronizovať dáta medzi rôznymi zariadeniami a bezpečne používať aj rôzne vlastné zariadenia (BYOD).

BEZPEČNOSTNÉ RIEŠENIE AKO CLOUDOVÁ SLUŽBA

Na riešenie bezpečnostných problémov možno zvoliť jeden z dvoch spôsobov:

premise-based – bezpečnostné riešenia, ktoré sú fyzicky nainštalované v zákazníckej sieti,

cloudové riešenie – bezpečnostné zariadenia sú fyzicky inštalované v dátových centrách a sú poskytované pre viacero zákazníkov.

Pri rozhodovaní sa, akým spôsobom sa bude pristupovať k zabezpečeniu siete, treba zvážiť nasledujúce otázky:

- Má firma dostatok IT zamestnancov a odborníkov na bezpečnosť?
- Má firma dosť financií na zakúpenie všetkých potrebných bezpečnostných zariadení?
- Má firma špeciálne bezpečnostné požiadavky, ktoré vyžadujú extra zariadenia?
- Má firma miesto na inštalovanie všetkých zariadení s príslušným napájaním a zálohovaním v prípade výpadku?
- Má firma prostriedky a zdroje na manažovanie všetkých bezpečnostných zariadení?

Ak ste odpovedali „áno" na všetky tieto otázky, bude pre vás výhodné premise based riešenie. Ak máte jednu alebo viac odpovedí „nie", mali by ste sa zamerať na cloud based. Výhodou cloudových bezpečnostných riešení je ich škálovateľnosť a dostupnosť. Pri expanzii firmy sa bezpečnostné politiky rozšíria do nových pobočiek bez toho, aby sa museli nakupovať zariadenia. Stačí dokúpiť licencie pre ďalších používateľov. Platí sa za to, čo zákazník aktuálne využíva, teda podľa počtu používateľov spravidla na mesačnej báze.

ZA KVALITU A DOSTUPNOSŤ CLOUDOVEJ SLUŽBY JE ZODPOVEDNÝ JEJ PREVÁDZKOVATEĽ

Cloudové bezpečnostné riešenia možno nasadiť bez nutnosti investícií, netreba kupovať hardvér ani licencie a inštalovať softvér, netreba sa starať o jeho aktualizáciu a ani o aktualizáciu antivírusových databáz. To výrazne skracuje čas nasadenia riešení. Bezpečnostné funkcie sú aplikované na dáta ešte prv, ako sa vôbec dostanú do zákazníkovej siete. Pri nasadení cloudového riešenia na filtrovanie škodlivého obsahu vo firme či organizácii so sieťou pobočiek možno aplikovať globálne politiky na webovú prevádzku vrátane šifrovanej komunikácie cez SSL. Tak sa dá zabezpečiť, aby citlivé informácie a dokumenty neopustili sieť. Centrálne politiky sú distribuované do všetkých pobočiek, takže sa dosiahne rovnaká úroveň zabezpečenia v celej sieti. Webové aktivity vzdialených zamestnancov sú presmerované cez najbližšie dátové centrum prevádzkovateľa cloudového riešenia, takže aj v prípade týchto zamestnancov možno zaistiť požadovanú úroveň bezpečnosti. Veľká výhoda cloudových riešení je synergia. Na odhalenie škodlivého obsahu a útokov sa používa široké spektrum detekčných technológií. Denne sa analyzujú desiatky až stovky miliónov webových požiadaviek v reálnom čase a získané informácie sú zdieľané pre všetkých zákazníkov.

Výhodná je aj vysoká dostupnosť cloudových riešení. Sú spravidla prevádzkované redundantne vo viacerých dátových centrách, medzi ktorými prebieha paralelné spracúvanie informácií. To umožňuje dosiahnuť až 99,999-percentnú dostupnosť.

ĽUBOSLAV LACKO, NEXTECH

MANAŽMENT

MANAŽMENT INFORMAČNEJ BEZPEČNOSTI

Pod pojmom manažment informačnej bezpečnosti rozumieme systematický prístup k zabezpečeniu firemnej IT infraštruktúry. Zaistenie potrebnej úrovne zabezpečenia je komplexný a nepretržitý proces, ktorý sa prelína s inými procesmi vo firme. Dosiahnutie primeraného stupňa zabezpečenia si vyžaduje nielen súčinnosť manažmentu a aj všetkých zainteresovaných zamestnancov, ale v mnohých prípadoch aj súčinnosť takzvaných tretích strán, teda dodávateľov, obchodných partnerov, logistických firiem a podobne.

Zabezpečenie IT je komplexná záležitosť a má určité špecifiká. Je to na jednej strane nákladovo náročný proces, pričom náklady na informačnú bezpečnosť (IB) sa ťažko zdôvodňujú, no len dovtedy, kým nedôjde k závažnejšiemu bezpečnostnému incidentu. Vtedy sa ukáže, že prevencia by bola mnohonásobne lacnejšia než dôsledky zanedbania IB a náklady na nápravu. Ďalší problém je, že hlavne vo vzťahu k ľudskému faktoru čiže zamestnancom sa nedá uplatniť uniformný prístup, pretože každá skupina zamestnancov (a v mnohých prípadoch aj jednotliví zamestnanci) má rôzny rozsah oprávnení prístupu k údajom a aplikáciám v súvislosti so svojimi pracovnými povinnosťami a rozsahom kompetencií.

Hlavne v malých firmách, no, žiaľ, nielen v nich, sa často uplatňuje takzvaný ad hoc prístup k IB. Je to prístup typu problém – riešenie, čiže problémy sa riešia až vtedy, keď sa vyskytnú. V mnohých prípadoch, napríklad pri útokoch ransomvéru, je však už neskoro.

ISO 27000

Väčšinu hardvéru aj softvéru používaného vo firmách tvoria štandardné produkty, používané na celom svete. To uľahčuje fungovanie nielen firmám, ale, žiaľ, aj kriminálnikom v kybernetickom priestore. Inými slovami, so štandardným hardvérom a softvérom súvisia aj „štandardné" bezpečnostné problémy a našťastie aj ochrana proti útokom. Preto snaha, aby firma tieto problémy riešila samostatne a vyvíjala si na to vlastné nástroje, je okrem odôvodnených výnimiek plytvaním finančných prostriedkov a kapacít špecialistov. Preto sa vytváraním a aktualizáciou osvedčených praktík zaoberajú medzinárodné organizácie. Individuálny

prístup má zmysel napríklad vtedy, ak firma či organizácia má vyššie požiadavky bezpečnosť, ako sa požaduje v štandarde.

Medzinárodná organizácia pre štandardizáciu (ISO) v spolupráci s Medzinárodnou elektrotechnickou komisiou (IEC) vydáva štandardy radu 27000 (ISMS – Information security management system), ktoré sú zamerané na systém riadenia informačnej bezpečnosti. Štandard ISO 27001 definuje požiadavky, ktoré sú kladené na organizácie usilujúce sa o certifikáciu podľa tohto štandardu. Integrálna súčasť tohto štandardu je normatívna príloha A, ktorá definuje bezpečnostné ciele a opatrenia. Odporúčania ohľadne implementácie sú definované v štandarde ISO 27002.

K bezpečnostným incidentom spravidla nedochádza z dôvodu zlyhania hardvéru či softvéru, ale vplyvom ich nesprávneho používania. Nie vždy sa správne používanie informačných a komunikačných prostriedkov dá „vynútiť" pomocou technických opatrení. Preto treba definovať a hlavne dodržiavať súbor pravidiel, politík a pracovných postupov. A takisto je potrebné mať vo firme zavedený systém pravidelných školení na zvyšovanie bezpečnostného povedomia zamestnancov.

Informačnú bezpečnosť rieši množstvo noriem ISO. Nebudeme ich preberať detailne, zameriame sa na všeobecné princípy. Základný dokument je politika informačnej bezpečnosti, ktorá pre každého zamestnanca určuje, čo môže, čo nesmie, čo musí a za čo je zodpovedný. Tejto téme sa venujeme v samostatnej kapitole.

Manažment informačnej bezpečnosti rieši aj organizáciu IB, správu aktív, personálnu a fyzickú bezpečnosť, prevádzku informačných a komunikačných systémov, manažment aplikačných a cloudových služieb, riadenie prístupu či riešenie bezpečnostných incidentov.

Cieľom **organizácie informačnej bezpečnosti** je vytvorenie organizačných podmienok na zavedenie a riadenie informačnej bezpečnosti vo firme či organizácii. Vedenie firmy schvaľuje politiku IB, posudzuje a reviduje implementáciu IB, zaraďuje zamestnancov do bezpečnostných rolí, dbá na zohľadnenie bezpečnostných aspektov v projektovom manažmente a takisto iniciuje spoluprácu s partnerskými firmami.

Cieľom **správy aktív** je inventarizácia a adekvátna ochrana aktív firmy, pričom každé dôležité aktívum musí mať vlastníka, ktorý je zodpovedný za jeho správu a ochranu. V kontexte informačnej bezpečnosti sa pod pojmom aktívum chápu predovšetkým informácie, ktoré treba klasifikovať a následne adekvátne chrániť.

Úlohou **personálnej bezpečnosti** je, aby nielen zamestnanci, ale aj externí spolupracovníci a zamestnanci tretích strán rozumeli svojim povinnostiam, vedeli, za čo nesú zodpovednosť, a mali dostatočné kvalifikačné predpoklady na rolu, do ktorej sú zaradení. Povinnosti ohľadne IB by mali byť špecifikované už v pracovnej zmluve. Dôležité je nielen úvodné školenie, ale aj adekvátne priebežné vzdelávanie. Je potrebné definovať spoluprácu HR a IT oddelenia nielen pri prijímaní zamestnanca a počas pracovného pomeru, ale aj v prípade jeho ukončenia alebo zmeny zaradenia. Týka sa to nielen vrátenia zariadení, ale aj odobratia prístupových práv. Nespokojný zamestnanec je jedna z najčastejších príčin bezpečnostných incidentov.

Úlohou **fyzickej bezpečnosti** je zabrániť neoprávnenému fyzickému prístupu k aktívam organizácie, ako aj ochrana aktív pred poruchami, prípadne inými predvídateľnými aj nepredvídateľnými udalosťami.

Informačnej bezpečnosti sa týka aj **manažment vzťahov** s dodávateľmi a poskytovateľmi služieb, pretože tieto subjekty majú prístup do informačných systémov firmy. Vzťahy s externými subjektmi definuje bezpečnostná politika a bezpečnostné požiadavky by mali byť zakotvené aj v zmluvách.

Na zabezpečenie bezproblémovej **prevádzky systémov IKT** by mali byť definované kompetencie a zodpovednosti aj ohľadne ochrany proti škodlivému softvéru, zálohovania údajov, manipulácie s pamäťovými médiami či správy zabezpečenia sietí. V súčasnosti k tomu pribudla správa a zabezpečenie mobilných zariadení a IT bezpečnosť súvisiaca s prácou z domu.

Manažment aplikačných a cloudových služieb na sieti je rozdelený medzi firmu a poskytovateľa cloudových služieb. Platí jednoduché pravidlo, že každý je zodpovedný za tú časť IT architektúry, ktorú spravuje.

Pri modeloch poskytovania SaaS sa povinnosti firmy koncentrujú na správu prístupových práv používateľov a zabránenie neoprávnenému prístupu k aplikáciám a informačným zdrojom v cloude.

BEZPEČNOSTNÝ PLÁN

Bezpečnostný plán obsahuje opis možných spôsobov narušenia jednotlivých komponentov IT infraštruktúry, opis zraniteľných miest týchto komponentov a subsystémov a takisto bezpečnostné opatrenia ich jeho ochranu, či už technické, alebo organizačné. Súčasťou bezpečnostného plánu sú aj plány kontroly a vzájomná kombinácia fyzických, technických a organizačných opatrení. Rozsah bezpečnostných opatrení na ochranu komponentu alebo subsystému sa určuje na základe posúdenia jeho dôležitosti, prípadnej zastupiteľnosti a takisto predpokladaných spôsobov narušenia alebo zničenia.

Pri tvorbe bezpečnostného plánu sa najskôr identifikujú kľúčové komponenty, ktoré treba ochrániť aj za vynaloženia vyšších nákladov. Následne sa vyhodnocuje riziko narušenia alebo zničenia týchto prvkov, ich zraniteľné miesta, ako aj predpokladané dôsledky ich narušenia. Práve tie môžu byť argumentom voči manažmentu a motiváciou na vynaloženie adekvátnych prostriedkov a úsilia na zabezpečenie. Následne sa definujú bezpečnostné opatrenia na ochranu týchto komponentov. Tieto opatrenia sú jednak jednorazové, napríklad nákup bezpečnostného softvéru či hardvérového komponentu, a jednak trvalé, ktoré si tiež vyžadujú časové kapacity a náklady.

Opatrenia sa členia na

- Technické zabezpečovacie prostriedky
- Bezpečnostné prvky informačných systémov
- Organizačné opatrenia
- Odbornú prípravu zamestnancov, ktorí zabezpečujú ochranu prvku
- Kontrolné opatrenia na dodržiavanie bezpečnostných opatrení
- Spôsob varovania pri zistení hrozby narušenia, prípadne incidentu
- Operatívne a mimoriadne bezpečnostné opatrenia, ktoré sa uplatňujú v prípade hrozby narušenia komponentu alebo subsystému

Rozdiel medzi bezpečnostnou politikou a bezpečnostným plánom, ktorý je rozpracovaním implementácie bezpečnostnej politiky, je zrejmý z nasledujúcich príkladov.

Bezpečnostná politika: správa prístupových práv používateľov a zabránenie neoprávnenému prístupu.

Bezpečnostný plán: implementácia systému jednotného prihlasovania, definovanie biometrického prístupu, minimálnej dĺžky a požadovanej zložitosti hesla, nastavenie času exspirácie hesiel, odmietnutie nastavenia predtým požadovaného hesla, trvalé zamknutie zariadenia a vymazanie údajov po mnohonásobnom zadaní nesprávneho hesla a upovedomenie administrátora, že k takejto situácii došlo, automatické uzamknutie zariadenia po zadefinovanom čase, keď sa nepoužíva...

Bezpečnostná politika: ochrana zariadení pri strate a krádeži.

Bezpečnostný plán: implementácia vyhľadávania strateného zariadenia, informácia o polohe zariadenia, možnosť diaľkového aktivovania vymazania údajov, postup v prípade straty či krádeže.

ŽIVOTNÝ CYKLUS BEZPEČNOSTI IT

Celý postup riadenia informačnej bezpečnosti, ktorý sa začína analýzou rizík, definovaním bezpečnostnej politiky, bezpečnostným plánom obsahujúcim súbor bezpečnostných opatrení a pokračuje bezpečnostným auditom a kontrolou dodržiavania politík, nie je jednorazový proces, ale cyklický, presnejšie povedané, proces s cyklickým životným cyklom, vynúteným novými technológiami, na ktoré sa kriminálnici v kybernetickom priestore rýchlo adaptujú. V životnom cykle IT bezpečnosti je preto dôležitá fáza periodickej kontroly a zmenového riadenia, v ktorom sa aktualizujú nevyhovujúce postupy, prípadne softvérové či hardvérové prostriedky.

ĽUBOSLAV LACKO, NEXTECH

PRVÝMI KROKMI K BEZPEČNOSTI SÚ AUDIT A KONCEPCIA

Vedeli ste, že cieľom až 90 percent stránok, ktoré vlani vznikli v súvislosti s koronavírusom, bolo podviesť návštevníka? *„Nástup digitalizácie, presun do cloudu, viac pripojených objektov i rozmach práce na diaľku menia spôsob, ako firmy fungujú, no zároveň lákajú tých s nečestnými úmyslami,"* hovorí **Michal Sekula**, bezpečnostný odborník spoločnosti Atos. *„Dbať na kybernetickú bezpečnosť je preto dnes dôležitejšie ako kedykoľvek predtým,"* hovorí.

PREHĽAD O DÁTACH

Neznamená to však hneď sa vrhnúť do investícií. Bezpečnostných riešení je veľmi veľa a nie všetky vyhovujú potrebám konkrétnej organizácie, podniku či firmy.

„Základom pri rozmýšľaní o kyberbezpečnostnej stratégii je bezpečnostný audit. Ten sa na celú problematiku pozrie z nadhľadu a preverí nielen zabezpečenie jednotlivých zariadení, ale preskúma i bezpečnosť firemných procesov či bezpečnostné povedomie zamestnancov," vysvetľuje odborník spoločnosti Atos. Kybernetickú bezpečnosť treba riešiť koncepčne. Každá organizácia by mala mať prehľad o dátach, ktoré chce chrániť – kde sa nachádzajú, kto k nim má prístup, do akej miery sú dôležité, ale napríklad i to, či chce predísť ich krádeži alebo ju ochromí aj dočasná nedostupnosť.

ZAČNITE PREVENCIOU

Základné riešenie sú nástroje typu Data Leakage Prevention, ktorých cieľom nie je riešiť bezpečnostné incidenty, ale zabrániť, aby k nim vôbec došlo. Pomocou upozornení či priamo zablokovaním predídu tomu, aby citlivé dáta úmyselne alebo nechtiac opustili firmu, či už na USB kľúči, mailom, alebo iným kanálmi. Vhodným prevenčným doplnkom je napríklad databázový firewall.

ÚPLNÝ PREHĽAD

Ucelený prehľad o okamžitej bezpečnostnej situácii poskytujú nástroje typu SIEM – Security Information and Event Management. *„Zbierajú všetky prevádzkové a bezpečnostné záznamy, triedia ich, analyzujú, spájajú, porovnávajú a vyhodnocujú, čo by manuálne bolo nad ľudské sily. Okrem toho však medzi nimi hľadajú aj súvislosti a získaným dátam tak dávajú zmysel,"* hovorí odborník spoločnosti Atos.

Moderné nástroje tohto typu využívajú umelú inteligenciu, takže okrem včasného upozornenia bezpečnostného tímu už vedia aj napovedať, ako problém rýchlo riešiť.

PREPOJENIE TECHNOLÓGIE A ĽUDÍ

Najvyššia forma pri riešení bezpečnosti je prepojenie technológie a ľudí. Bezpečnostné nástroje sú silnou zbraňou, o najvhodnejšom postupe však často dokážu rozhodnúť len roky skúseností. Tie môže organizáciám ponúknuť napríklad služba centra bezpečnostných operácií, takzvané SOC. Firmy sa pri nej nemusia spoliehať na vlastné zdroje, majú k dispozícii najlepších odborníkov v čase a miere, v akej potrebujú. *„Rozhodnutie, akým smerom by sa mala bezpečnosť uberať, by však mali spraviť organizácie ešte skôr, ako sa pustia do nákupov. Nie vždy je totiž najlepším kritériom cena, do úvahy treba brať kompatibilitu riešení aj ich vhodnosť pre potreby firmy. Akémukoľvek nákupu by tak malo predchádzať zistenie stavu, vyhodnotenie situácie a premyslený návrh celkovej bezpečnostnej architektúry bez slabých článkov,"* uzatvára bezpečnostný odborník spoločnosti Atos. ■

BEZPEČNOSTNÝ AUDIT

Audit bezpečnosti informačného systému je odborné posúdenie a ohodnotenie koncepcie, návrhu riešenia, prevádzky, prípadne inovácie celého informačného systému z hľadiska ochrany a schopnosti plniť povinnosti ukladané zákonnými normami, internými predpismi a požiadavkami organizácie. Z toho vyplýva, že audítor pri uskutočňovaní auditu bezpečnosti IS musí vychádzať z určitého predpokladaného alebo vopred definovaného požadovaného stavu bezpečnosti systému, ktorý by mu mala poskytnúť predovšetkým schválená bezpečnostná politika, riziková analýzy, bezpečnostná dokumentácia, prípadne závery a poznatky predchádzajúceho auditu.

„BEZPEČNOSTNÝ AUDIT JE OHODNOTENIE ZABEZPEČENIA INFORMAČNÉHO SYSTÉMU, PROCEDÚR, PRAKTÍK A OHODNOTENIE ÚROVNE RIZÍK, KTORÝM INFORMAČNÝ SYSTÉM A INFORMAČNÉ AKTÍVA ČELIA. "

Bezpečnostný audit IT umožní odhaliť bezpečnostné problémy s IT systémami vrátane softvéru, hardvéru, infraštruktúry, procedúr, obchodných procesov a ľudí. Audit je zameraný najmä na riziká a na ohodnotenie rizík straty, kompromitovania alebo zničenia informácií.

Audit bezpečnosti informačného systému je systematický proces získavania a vyhodnocovania poznatkov o bezpečnosti systému a v ňom obsiahnutých údajov s cieľom:

- zistiť mieru súladu medzi bezpečnostnou politikou a skutočnou situáciou,
- poskytnúť primeranú istotu o tom, že bezpečnosť systému je na požadovanej úrovni a že bezpečnostný systém organizácie neobsahuje významné medzery,
- odhaliť slabé miesta v bezpečnosti systému,
- oznámiť zistené výsledky, prípadne navrhnúť možné riešenia zistených nedostatkov.

Audítor posudzuje úroveň kontrolných prvkov na úrovni aplikácie informačného systému a takisto hodnotí kvalitu riadenia relevantných prvkov a aspektov systému, t. j. posudzuje:

- prvky regulujúce prístup k aplikácii a manipuláciu s ňou,
- kontroly na vstup a verifikáciu vstupných dát do systému,
- kontroly na zabezpečenie správnosti prenosu a spracovania údajov,
- kontroly databázy,
- kontroly výstupných údajov.

Audítor hodnotí úroveň manažmentu informačného systému z hľadiska jeho plánovacej, organizačnej, personálnej, riadiacej a kontrolnej funkcie vo vzťahu k bezpečnosti systému, ďalej systém riadenia vývoja IS a riadenia samotnej rutinnej prevádzky. Hodnotí celkový stav a úroveň ochrany organizácie, bezpečnosť IS ako celku, ako aj jeho jednotlivých častí a realizáciu opatrení a protiopatrení na minimalizáciu alebo elimináciu možných hrozieb.

Z teórie aj praxe vyplýva, že nemožno vybudovať absolútne bezpečný systém, a teda ani audítor nemôže jednoznačne potvrdiť jeho bezpečnosť, pretože:

- absolútna bezpečnosť sa vzhľadom na neustály vývoj v príslušnej oblasti nedá dosiahnuť,
- na systém bezpečnosti významne vplýva ľudský faktor
- každý systém sa dá chrániť proti náhodnému omylu, ale nie pred úmyselným zneužitím alebo poškodením.

Audítor a klient sa musia dohodnúť na podmienkach zákazky auditu. Forma a obsah záväzného listu u rôznych klientov sa môžu líšiť, v zásade by však mal obsahovať:

- ciele auditu,
- rozsah auditu,
- formu správ alebo inú prezentáciu výsledkov zákazky,
- skutočnosť, že v dôsledku charakteru auditu existuje riziko, že niektoré významné nesprávnosti môžu ostať neodhalené,
- neobmedzený prístup k akýmkoľvek správam, dokladom a ostatným všetkým potrebným informáciám.

Zodpovednosťou audítora je vyjadriť objektívny a nezávislý názor na bezpečnosť systému. Nezávislosť a objektivita sú základné kritériá pre profesionálnu zdatnosť audítora alebo člena audítorského tímu. Vzhľadom na rozsah a charakter práce sa na audítora bezpečnosti IS kladú pomerne vysoké nároky. Predovšetkým musí ísť o čestnú, bezúhonnú a dôveryhodnú osobu, pretože organizácia mu poskytuje veľmi dôverné informácie.

TYPY AUDITOV

Firmy, ktoré vykonávajú bezpečnostné audity, ponúkajú niekoľko typov auditu:

Audit systému riadenia informačnej bezpečnosti – audit sa vykonáva podľa medzinárodného štandardu ISO/IEC 27001:2005 (BS ISO/IEC 17799). Výsledkom auditu je záverečná správa hodnotiaca súlad úrovne informačnej bezpečnosti v organizácii práve vzhľadom na tieto medzinárodne uznávané štandardy, určené na budovanie a riadenie informačnej bezpečnosti.

Audit konfigurácie zariadení – cieľom auditu je preverenie bezpečnosti nastavenia a služieb poskytovaných daným zariadením. Môže ísť o konfiguračný audit aktívnych sieťových prvkov infraštruktúry (ako sú firewally, smerovače, prepínače, prístupové servery, VPN tunely) alebo o audit zabezpečenia serverov a operačných systémov. Pri takomto audite sa zariadenie audituje podľa vlastných auditných metodológií zohľadňujúcich odporúčania výrobcu zariadenia, ako aj všeobecne platné „best practices" v danom profesijnom segmente. Je vhodné, ak je audit doplnený aj o audit procesov používania a administrácie daných zariadení z pohľadu bezpečnosti (napr. audit procesov správy smerovača, zálohovania firewallu, kontrolu integrity konfiguračného auditu...)

Penetračné testovanie – formou penetračných testov má zákazník možnosť získať prehľad o reálnych, ale aj potenciálnych slabinách, ktoré môžu predstavovať reálne riziká pre chránené aktíva. Zákazník má takisto počas testovania príležitosť overiť si funkčnosť a efektívnosť všetkých implementovaných obranných mechanizmov, či už ide o firewally, riešenia IDS/IPS, alebo ochranné mechanizmy na úrovni aplikácií. Počas testovania skupina špecialistov systematicky prehľadáva všetkými dostupnými prostriedkami cielené aktíva, pričom sa snaží simulovať reálneho útočníka, ktorý buď nemá žiadne informácie o cieľových systémoch, alebo disponuje základnými informáciami o nich. Rozdiel medzi reálnym útočníkom a audítorom je v tom, že cieľom penetračných testov je identifikácia všetkých slabín systému, zatiaľ čo reálny útočník by hľadal iba jednu, ktorú by následne aj zneužil.

Procesný audit – cieľom auditu je posúdenie existencie, funkčnosti a opodstatnenosti vykonávania procesov z vybranej oblasti riadenia informačnej bezpečnosti (napr. riadenie prístupov).

Bezpečnostný audit bezdrôtovej siete – audit je vhodný pre všetky spoločnosti, ktoré využívajú bezdrôtové siete na kritické operácie, prípadne ich siete Wi-Fi nie sú striktne oddelené od dôveryhodných vnútorných sietí.

Audit zabezpečenia aplikácií – audit skúma segregáciu aplikácií, ako aj celých operačných systémov pomocou sandboxov či virtualizačných techník.

Cieľom auditu v oblasti **fyzickej bezpečnosti** sú budovy a ich okolie, možnosť vniknutia cudzej osoby, spôsob stráženia vrátane skúmania vzťahu medzi strážnou službou a prevádzkovateľom systému. Do tejto oblasti patrí aj skúmanie možnosti ohrozenia pri živelnej pohrome, existencia a úroveň elektrického zabezpečovacieho systému, umiestenie kľúčov jednotlivých častí auditovaného systému a súvisiacich priestorov, spôsob likvidácie dokumentov po lehote platnosti, skartačný poriadok, skartačné zariadenie, prístup upratovacej služby do kľúčových priestorov auditovaného systému.

Audit v oblasti **personálnej bezpečnosti** skúma zainteresovanosť zamestnancov na celkovej bezpečnosti organizácie, úroveň zaškolenia zamestnancov na prácu s dôvernými a citlivými údajmi. Zisťuje nielen podmienky, v ktorých používatelia systému pracujú a ktoré môžu vplývať na chybovosť ich práce, ale dokonca aj motiváciu pracovníkov na kľúčových miestach z hľadiska ochrany údajov a spoľahlivosti chodu informačného systému. Dôležitý je aj mechanizmus pri rozväzovaní pracovného pomeru z hľadiska utajenia informácií, smernice pre zastupovanie a podobne.

Audit **bezpečnosti technických prostriedkov** skúma druh, kvalitu a certifikáciu technických prostriedkov, plombovanie pracovných staníc, ochranu pred neautorizovaným zásahom, zabezpečenie servisu, periodicitu prevencie, spoľahlivosť zálohovania, náhradný zdroj energie, vypínanie obrazoviek terminálov, použitie hesla, špeciálne antireflexné filtre a pod.

Audit bezpečnosti údajov skúma kompetencie a smernice pre zadávanie dát, mechanizmy autorizácie a rozlíšenie prístupu k údajom, zálohovanie, archiváciu a likvidáciu údajov, šifrovanie dát a pod.

ĽUBOSLAV LACKO, NEXTECH

ROZHOVOR: **ERIKA LINDAUEROVÁ**, HP INC.

PRODUKTY A RIEŠENIA HP NA BEZPEČNÚ A EFEKTÍVNU PRÁCU

O zabezpečení počítačov, tlačiarní, bezpečnosti a efektivite pri home office a ďalších zaujímavých novinkách sme sa porozprávali s Erikou Lindauerovou, generálnou riaditeľkou HP pre Českú republiku, Slovenskú republiku a Maďarsko.

Ako reagovala spoločnosť HP, ako výrobca notebookov, na pandemickú situáciu?

Erika Lindauerová: Prioritou spoločnosti HP je zdravie a bezpečnosť zamestnancov, zákazníkov, partnerov a ich rodín. Naše kancelárie sme zavreli 13. marca 2020 a stále sme sa do nich nevrátili. Všetci sa museli prispôsobiť novej situácii, ale pracovná flexibilita tu bola už pred pandémiou. Ešte pred akýmikoľvek oficiálnymi opatreniami sme boli veľmi proaktívni v zaistení bezpečnosti zamestnancov a v zaistení toho, aby naši zamestnanci mali správne vybavenie na prácu z domu.

Odkedy sa pandémia pred viac ako rokom začala, väčšina zamestnancov pracuje na diaľku, existuje tak dopyt po ďalších IT zariadeniach, riešeniach domácej tlače a podobne. Preto sa zameriavame na inovácie a vývoj produktov.

Poskytla spoločnosť HP firemným zákazníkom riešenia na bezpečnú prácu z domu?

Erika Lindauerová: Hybridné modely práce a učenia sa stanú novým normálom, ľudia budú chcieť, aby spoločnosti ponúkali flexibilitu v spôsoboch ich práce. Pozornosť sa začala sústreďovať na výberové

kritériá pre zariadenia – dopyt po nich je vyšší a PC segment sa vyvíja z jedného počítača na domácnosť na jeden počítač na osobu – toto nebolo nikdy dôležitejšie. Vzhľadom na to, že ľudia pracujú z domu, zaznamenali sme takisto zvýšený dopyt po vybavení domácej kancelárie, napríklad po tlačiarňach do domácností na podporu práce z domu, ale aj domáceho vzdelávania a tzv. nového normálu.

Od zavedenia práce z domu sa jednou z dôležitých tém stala bezpečnosť – kybernetické útoky sú na vrchole a spoločnosti reagujú na nové scenáre útokov a na situáciu, že v strednodobom až dlhodobom horizonte musia zabezpečiť veľkú časť IT pracoviska mimo priestorov spoločnosti. Práca v domácom prostredí sa líši z hľadiska bezpečnosti. Zamestnanci podstupujú väčšie riziko ako v kancelárii, napríklad používaním nezabezpečených zariadení, zdieľaním zariadení s rodinou a priateľmi a používaním pracovných prostriedkov aj na osobné účely. HP Wolf Security je nový druh zabezpečenia koncových zariadení s portfóliom vynúteného zabezpečenia hardvéru a bezpečnostných služieb zameraných na koncové zariadenia, ktoré sú navrhnuté tak, aby pomáhali organizáciám chrániť počítače, tlačiarne a ľudí pred číhajúcimi kybernetickými predátormi. HP Wolf Security poskytuje komplexnú ochranu a odolnosť koncových zariadení, ktorá sa začína na hardvérovej úrovni a rozširuje sa na softvér a služby.

Home office zrejme aj sama využívate. Aké sú vaše odporúčania pre ľudí, ktorí používajú firemný notebook na prácu z domu?

Erika Lindauerová: Povedala by som, že mám šťastie, že môžem mať samostatný priestor, kde môžem pracovať, čo je pre mňa dôležité. Mám takisto vynikajúcu zostavu, ktorá obsahuje aj monitor, aby som mohla používať dvojitú obrazovku, bezdrôtovú klávesnicu a myš. V prípade potreby na videohovory používam headset na potlačenie hluku, čo je užitočné pre väčšie súkromie pri práci z domu, a moja stolička HP Omen ju robí ešte pohodlnejšou. Posun k hybridnej práci bude určite výraznejší, preto by som odporúčala vybaviť si domácu kanceláriu zariadeniami, vďaka ktorým bude práca z domu čo najjednoduchšia a najpohodlnejšia.

Pri týchto rozhodnutiach treba pamätať na bezpečnosť, pretože svet okolo nás sa neustále transformuje a vyvíja rýchlym tempom, rovnako musí držať krok aj kybernetická bezpečnosť. Musíme byť neustále flexibilní, proaktívni a reaktívni, aby sme dosiahli odolnosť, a to je to, čo prináša HP Wolf Security. Bude sa neustále vyvíjať a našim zákazníkom pomôže udržať si náskok pred modernými hrozbami.

Táto nová bezpečnostná platforma predstavuje zjednotenie všetkých ponúk zabezpečenia spoločnosti HP v oblasti osobných systémov, tlače, softvéru a služieb do jedného portfólia hardvérovo vynútených bezpečnostných služieb a bezpečnostných služieb zameraných na koncové zariadenia.

Zabezpečenie je dôležité nielen pre počítače, ale aj pre tlačiarne a ďalšie zariadenia. Na čo by firma či domáci používateľ mali dbať, aby ich tlačiarne boli bezpečné?

Erika Lindauerová: Používatelia si čoraz viac uvedomujú bezpečnosť, a to najmä pri práci z domu. Práca mimo bezpečia kancelárie zvyšuje pravdepodobnosť kybernetických útokov na rôzne zariadenia. Správa Blurred Lines & Blindspots pre HP Wolf Security zdôrazňuje, že globálny objem kybernetických útokov sa počas covidu zvýšil o 238 %, pričom hackeri cielili najmä na vzdialených pracovníkov.

Ešte raz spomeniem Wolf Security – patria sem najbezpečnejšie počítače a tlačiarne na svete s rozsiahlou súpravou softvéru a služieb na zvýšenie ochrany a odolnosti koncových bodov. Je to novinka na trhu, preto by som to odporučila podnikovým aj domácim používateľom. Používateľ sa môže cítiť viac v pohode, pretože firma mu umožní ľahko a bezpečne tlačiť, či už je v kancelárii, alebo doma. Až 76 % kancelárskych pracovníkov tvrdí, že práca z domu počas COVID-19 stierala hranice medzi ich osobným a profesionálnym životom. Polovica z nich uviedla, že teraz vidí svoje pracovné zariadenie ako vlastné osobné zariadenie, a 46 % priznáva, že svoj pracovný notebook používa aj na súkromné účely.

Moderné tlačiarne HP využívajú pripojenie ku cloudovým službám. Aké sú bezpečnostné výhody takéhoto pripojenia?

Erika Lindauerová: Digitalizácia sa zrýchlila vo všetkých oblastiach, vo výrobe aj v kanceláriách. Nedávno sme uviedli službu Instant Ink a HP+ na 35 trhoch vrátane Slovenska. Ide o inteligentné, pohodlné a udržateľné predplatné atramentu a tonera, ktoré modernizuje používateľskú skúsenosť s domácou aj hybridnou tlačou a šetrí až 70 % nákladov na atrament a 50 % na toner. Originálne atramentové kazety HP sa predplatiteľom služby odosielajú automaticky skôr, ako sa minie existujúca kazeta, a predplatné môžete jednoducho spravovať pomocou aplikácie HP Smart.

Vďaka novému cloudovému ekosystému HP+ môžu zákazníci a malé podniky zostať v spojení a zabezpečené pomocou exkluzívnych nových funkcií, ako je napríklad odolnosť nového cloudu, ktorá automaticky odhaľuje a opravuje problémy s pripojením, a nový monitoring Smart Security, ktorý pomáha detegovať malvérové útoky a predchádzať im. HP+ je významný posun v tlači, každé z našich zlepšení s HP+ bolo

navrhnuté tak, aby vyhovovalo potrebám tých, ktorí najviac závisia od svojich tlačiarní, pričom v popredí nášho úsilia je bezpečnosť.

Máme takisto dlhú históriu v oblasti zabezpečenia s viac ako 20-ročným výskumom a inováciami v oblasti bezpečnosti zo Security Lab v laboratóriách HP, čo nám pomáha zaistiť, že máme najbezpečnejšie počítače a tlačiarne na svete. HP Wolf Security bude platformou pre všetky bezpečnostné inovácie spoločnosti HP, ktoré sú rozdelené na HP Wolf Security for Home, HP Wolf Security for Business, HP Wolf Pro Security a HP Wolf Enterprise Security.

Medzi výhody pripojenia moderných tlačiarní HP ku cloudovým službám patrí, že spoločnosť HP môže monitorovať konfiguračné nastavenia tlačiarne, aby zabezpečila súlad s odporúčanými nastaveniami – túto funkciu dnes poskytuje HP SmartSecurity. Môžeme tiež poskytnúť bezpečné riešenie na tlač z cloudu, ktoré umožňuje tlač po overení pri tlačiarni. Takto je zaistené, že citlivé dokumenty sa vytlačia, iba ak sa fyzicky nachádzate pri tlačiarni. Bezpečnosť je pre nás skutočne dôležitá, a to najmä pri práci na diaľku, a budeme naďalej poskytovať zlepšené riešenia.

V čom vnímate výhody produktov a služieb HP v porovnaní s konkurenciou?

Erika Lindauerová: Spoločnosť HP je známa ako spoločnosť inžinierov – inovácie, prístupnosť a kreativita sú pre nás veľmi dôležité. Sme jednou z popredných svetových technologických spoločností v oblasti tlače a osobných systémov (PS) a vytvárame technológie, ktoré zlepšujú život ľudí na celom svete. Ako spoločnosť pretvárame kultúru pracovných síl, spoluprácu a kreativitu a zároveň inovujeme svoje technológie a služby pre hybridné spôsoby práce a vedieme silný pokrok v oblasti VR, AI a cloud computingu.

Inovujeme prostredníctvom našich produktov, ako je uvedenie na trh prvého notebooku, monitora, mobilnej pracovnej stanice a podnikových Chromebookov vyrobených z plastov, ktoré by ináč skončili v oceáne. Posledný prírastok do tohto udržateľného portfólia je HP Elite Dragonfly G2.

Trvalo udržateľný rozvoj je pre nás veľmi dôležitý. Aj keď sme lídrom na trhu v oblasti našich výrobkov a služieb, zaviazali sme sa k vízii budúcnosti pozitívnej k lesom. Práve sme oznámili ambiciózne ciele v oblasti zmeny podnebia, medzi ktoré patrí zníženie emisií skleníkových plynov v reťazci HP o 50 % do roku 2030, dosiahnutie uhlíkovej neutrality a nulového odpadu v prevádzkach spoločnosti HP do roku 2025, a do roku 2030 chceme dosiahnuť 75 % podiel recyklácie v produktoch a ich obaloch.

A nakoniec spoločnosť HP je lídrom v oblasti zabezpečenia koncových zariadení. Detailne sa zaoberáme všetkými bezpečnostnými aspektmi v operačnom systéme, pod i nad ním. Na túto oblasť sme sa zameriavali už dlhšie, ale až pandémia skutočne zvýšila potrebu a túžbu po prvotriednom zabezpečení. Máme množstvo nástrojov, ako napríklad HP SureStart, ktorý deteguje a opravuje škodlivé kódy v systéme BIOS, HP SureClick umožňuje bezpečné prehliadanie internetu, HP SureSense je umelá inteligencia, ktorá hľadá škodlivé kódy, HP SureRun chráni kľúčové aplikácie. Toto všetko sú jedinečné nástroje, ktoré pomáhajú každému používateľovi počítača alebo tlačiarne HP pracovať, učiť sa a hrať sa bezpečnejšie.

Čo má HP nové vo svojich produktoch?

Erika Lindauerová: Aj naďalej budeme stáť na čele s inováciami. Rozprestretejší digitálny svet nemusí znamenať zraniteľnejší svet. Ako sa kybernetický svet neustále vyvíja, musí sa meniť aj kybernetická bezpečnosť. V nadväznosti na naše oznámenie o Wolf Security zostáva bezpečnosť prioritou, zlepšili sme množstvo funkcií na integrovanú ochranu, aby sme zaistili, že máme najbezpečnejšie tlačiarne na svete. Až 71 % zamestnancov pristupuje z domova častejšie a k väčšiemu množstvu firemných údajov, ako to bolo pred pandémiou, a my budeme naďalej zavádzať nové bezpečnostné funkcie, ktoré používateľom pomôžu udržať si náskok pred vyvíjajúcimi sa hrozbami.

V októbri 2020 sme rozšírili náš program odmeny za chyby (bug bounty), aby sme ho konkrétne zamerali na chyby zabezpečenia tlačových kaziet pre kancelárie. Cieľom je identifikovať potenciálne riziká v tlačových kazetách pre kancelárie – ponúkame etickým hackerom odmenu za odhalené chyby zabezpečenia.

Uviedli sme takisto HP+ a Instant Ink, čo je prelomový cloudový ekosystém, ktorý je bezpečný, produktívny a jedinečne udržateľný. Veríme, že toto je budúcnosť tlače navrhnutá pre nové hybridné modely toho, ako žijeme a pracujeme.

Nedávno sme ohlásili naše rozsiahle portfólio Spring Gaming. V roku 2020 sme zaznamenali oživenie v hraní, obrovský nárast počtu ľudí hrajúcich online, ako aj mnoho hráčov, ktorí ešte len začali. Medzi najdôležitejšie položky patrí najnovší herný hardvér a softvér určený pre súčasných hráčov s výkonnými počítačmi OMEN 16 a OMEN 17, jasný a prispôsobiteľný herný monitor OMEN 25i a komunitné hranie s funkciou OMEN OASIS4 Beta v hernom rozhraní OMEN Gaming Hub5. Veľký úspech mal aj rad Victus by HP s jeho portfóliom mainstreamových herných počítačov novej generácie so 16-palcovým notebookom.

HP

BEZPEČNOSTNÁ POLITIKA

Bezpečnosť je vo všeobecnosti definovaná ako komplex procesov a činností zameraných na odvrátenie alebo zmenšenie identifikovaných rizík, resp. prejavov hrozieb, ktoré pôsobia na príslušné aktíva, v tomto prípade na IT infraštruktúru a údaje.

Bezpečnosť je kontinuálny proces na udržiavanie akceptovateľnej miery zisteného rizika.

Kľúčová je tá časť definície, že zabezpečenie nie je produkt ani konečný stav, ktorý chceme dosiahnuť, ale nepretržitý kontinuálny proces. Metódy kriminálnikov v kybernetickom priestore sú stále sofistikovanejšie, a preto sa musí neustále zdokonaľovať aj zabezpečenie.

Bezpečnosť IT je komplexná problematika. Nejde len o zabezpečenie serverov, sietí, počítačov či mobilných zariadení, ale celej infraštruktúry. Tu si môžeme vziať príklad od profesionálov, ktorí sa starajú o zabezpečenie dátových centier. Riešia aj objektovú bezpečnosť čiže zabezpečenie miestností, budov a ich vonkajšieho perimetra, kontrolu vstupu autorizovaných osôb a zabránenie prístupu nepovolaným osobám. Keď už spomíname zamestnancov, samozrejmosť sú pravidelné školenia. A takisto ochrana serverovej a komunikačnej infraštruktúry, či už fyzickej, alebo virtualizovanej.

Bezpečnosť IT je postavená na troch základných pilieroch: dostupnosti, integrite a dôvernosti. Služby, funkcie a údaje systémov na IT podporu biznisu musia byť k dispozícii 24 hodín a sedem dní v týždni. Údaje musia byť úplné a nezmenené. Strata integrity z bezpečnostného pohľadu znamená zmenu údajov bez autorizácie, falšovanie samotnej informácie či falšovanie času jej vytvorenia. Takisto treba zabrániť neoprávnenému prístupu k údajom a aplikáciám.

Bezpečnostná politika informačného systému je súhrn politík na zabezpečenie jeho prevádzky. Obsahuje súhrn bezpečnostných požiadaviek na riešenie

informačnej bezpečnosti na úrovni fyzickej, personálnej, administratívnej, počítačovej a komunikačnej bezpečnosti. Bezpečnostná politika musí byť ako dokument schválený vedením spoločnosti ako záväzná vnútropodniková smernica.

Dobre definovaná bezpečnostná politika rieši hlavne prevenciu proti útokom na ktorýkoľvek podsystém alebo komponent informačného systému, či už ide o útoky z externého, alebo interného prostredia, vedomé alebo nevedomé ohrozenie bezpečnosti IS firmy či organizácie.

Sú to práve bezpečnostné politiky, ktoré odporúčajú, lepšie povedané, predpisujú administrátorom systémov a sietí, ako sa zachovať v špecifických situáciách. Bez jasne definovaných postupov môžu administrátori pri riešení rovnakých incidentov postupovať rôzne podľa svojich domnienok, čo často vedie k nesprávnym, niekedy až kontraproduktívnym rozhodnutiam. Dôležitý faktor je aj migrácia pracovnej sily. Administrátori sa môžu meniť, no bezpečnostné politiky zostávajú a v prípade nutnosti sa inovujú a dopĺňajú. Typický príklad je zavádzanie nových IT architektúr, napríklad cloud computingu či virtualizácie.

„DEFINOVANIE BEZPEČNOSTNÝCH POLITÍK PRE INFORMAČNÉ SYSTÉMY JE VO VLASTNOM ZÁUJME KAŽDEJ FIRMY A ORGANIZÁCIE. SPRÁVNE DEFINOVANÉ PROAKTÍVNE PRAVIDLÁ UMOŽŇUJÚ ĽAHŠIE A EFEKTÍVNEJŠIE ZVLÁDAŤ BEZPEČNOSTNÉ INCIDENTY."

Firmy bez správne definovaných politík alebo firmy, ktorých bezpečnostné politiky zlyhajú, strácajú dôveru zákazníkov, obchodných partnerov a v prípade nezvládnutia bezpečnostných incidentov väčšími firmami či korporáciami na túto skutočnosť reagujú aj akciové trhy. Typický príklad sú nedávne krádeže údajov o používateľských účtoch v niektorých významných globálnych spoločnostiach.

SMERNICA O BEZPEČNOSTNEJ POLITIKE

Je to písomný dokument schválený vedením spoločnosti ako záväzná vnútropodniková smernica, ideálne v podobe komplexného projektu na ochranu informačnej infraštruktúry spoločnosti, v ktorom budú definované jednotlivé hrozby špecifické pre danú spoločnosť. Smernica by mala obsahovať súhrn bezpečnostných požiadaviek a opatrení na riešenie IT bezpečnosti na fyzickej, serverovej, komunikačnej, personálnej a administratívnej úrovni. Takisto by mala obsahovať komplexné riešenie bezpečnosti informačného systému v rámci celej firmy či organizácie. Smernica by mala poskytnúť odpovede na základné okruhy otázok:

„SMERNICA O BEZPEČNOSTNEJ POLITIKE JE KĽÚČOVÝ PÍSOMNÝ DOKUMENT FIRMY ALEBO ORGANIZÁCIE, KTORÝ DEKLARUJE PREDSTAVU MANAŽMENTU O KOMPLEXNOM RIEŠENÍ BEZPEČNOSTI IS."

- Čo je predmetom ochrany a prečo to treba chrániť
- Spôsob proaktívnej ochrany
- Reaktívna ochrana, ak dôjde k zlyhaniu proaktívnych opatrení

Z vymenovaných bodov je zrejmá orientácia na proaktívnu ochranu, no smernica či projekt by mali obsahovať aj protiopatrenia a definíciu postupov v prípade kybernetického incidentu. Bezpečnostný projekt musí obsahovať aj zoznam hrozieb, ktoré neboli z určitých dôvodov ošetrené. Najčastejší dôvod sú vysoké náklady, prípadne malá dôležitosť niektorých údajov, napríklad diagnostických či prevádzkových, ktoré nie sú citlivé.

TYPY BEZPEČNOSTNÝCH POLITÍK

Rozpoznávame tri typy základného filozofického prístupu k bezpečnostnej politike využívania IS:

Paranoja – zakázané je všetko vrátane tých aktivít, ktoré by mali byť povolené. V psychiatrii paranoja znamená, že sa neverí nikomu a ničomu – nebezpečenstvo môže prísť odkiaľkoľvek. Paranoja má oprávnenie v odvetviach s tajnými alebo pre firmu veľmi cennými informáciami. V bežnej firemnej praxi sa aplikovať nedá. To by firma veľmi rýchlo prišla o talentovaných ľudí, schopných samostatne premýšľať.

Opatrná politika – zlatá stredná cesta. Všetko je zakázané okrem tých aktivít, ktoré sú explicitne povolené.

Liberálna politika je opak paranoje, teda čo nie je zakázané, je povolené. Ľudia by sa mali riadiť rozumnými pravidlami, ktoré ich neobmedzujú pri práci, ALE každý má iba oprávnenia, ktoré nevyhnutne potrebuje pri svojej práci.

Anarchia – absolútny chaos, keď si vo firme každý robí, čo chce. Anarchia môže vládnuť buď v celej firme, alebo len od určitej úrovne (napríklad stredný technický manažment, prípadne paradoxne IT oddelenie, hlavne programátori). Administrátor nezvláda správu siete a manažmentu nezáleží na používaní informačných technológií.

ODPORÚČANIA Z PRAXE

V tejto stati heslovite opíšeme kroky, ktoré sa osvedčili pri definovaní bezpečnostnej politiky v podnikovej praxi.

Inventarizácia aktív – zmapovanie prostriedkov a definovanie ich priorít. Od toho sa odvíja stupeň požadovanej ochrany.

Analýza potenciálnych hrozieb a rizík – ktoré hrozby sú aktuálne a ktoré najnebezpečnejšie. Pri každej hrozbe musíme definovať predpokladaný dôsledok pre našu firmu alebo organizáciu.

Spôsob ochrany – z predchádzajúcich krokov vieme, aké prostriedky pred akými hrozbami treba chrániť. V tomto kroku je potrebné definovať najvhodnejší spôsob ochrany a postup pri disaster recovery. Najvhodnejší znamená kompromis medzi účinnosťou a nákladmi. Takisto treba pre každý obranný mechanizmus vymedziť kompetencie, určiť zodpovedné osoby.

Prevencia – aby ste sa vyhli strate najcennejšieho aktíva čiže údajov, je nevyhnutné zálohovanie. Odporúča sa vypracovať projekt počnúc určením dôležitosti údajov cez výber vhodných záložných médií (čoraz populárnejšie je zálohovanie v cloude, ak to charakter údajov dovoľuje) až po určenie intenzity zálohovania. Dôležitú úlohu hrajú náklady – tie nemôžu prevýšiť hodnotu údajov. Aj v tomto kroku je potrebné určiť zodpovedné osoby.

Definovanie pravidiel a zodpovednosti – súčasťou bezpečnostnej politiky je definovanie kompetencie jednotlivých zamestnancov a pravidlá, ktoré musia dodržiavať. Kompetencie stanovujú, kto a za akých okolností má prístup ku ktorým zariadeniam a ku ktorým zariadeniam pristupovať nesmie. Súčasťou pravidiel je nielen stanovenie postihov za porušenie predpisov, ale aj to, ako má zamestnanec postupovať v situácii, keď bezpečnostné mechanizmy zlyhajú (napr. jeho počítač je napadnutý vírusom). Dôležité je, aby zamestnanci podpísali, že sa s týmito pravidlami oboznámili.

Plány pre stav ohrozenia – postupy reagovania na kybernetický útok či stratu, prípadne odcudzenie údajov alebo iné škody. Ak sú jasne definované kompetencie a postupy, škoda spôsobená útokom sa zminimalizuje. Zamestnanci nespanikária a kompetentní správne vyhodnotia danú situáciu.

BEZPEČNOSTNÝ PROJEKT

Bezpečnostný projekt musí obsahovať všetky náležitosti, ktoré mu ukladá legislatívna. Mal by byť vybudovaný na troch základných pilieroch:

Bezpečnostný zámer – definícia základných bezpečnostných cieľov a špecifikovanie minimálne požadovaných bezpečnostných, technických, organizačných a personálnych opatrení na jeho dosiahnutie. Bezpečnostný zámer spravidla definuje aj zabezpečenie ochrany osobných údajov v informačnom systéme a spôsob ich využitia.

Analýza bezpečnosti IS: analýza rizík, kde sú identifikované hrozby pôsobiace na jednotlivé aktíva informačného systému spôsobilé narušiť jeho bezpečnosť alebo funkčnosť. Analýza by mala obsahovať aj návrhy opatrení, ktoré eliminujú alebo minimalizujú vplyv rizík.

Bezpečnostné smernice: opis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach. Smernice by mali obsahovať nielen rozsah oprávnení a opis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému, ale aj rozsah zodpovednosti oprávnených osôb a predovšetkým osoby zodpovednej za dohľad nad ochranou osobných údajov. Súčasťou smerníc by mala byť aj špecifikácia spôsobu, formy a periodicity kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému. Okrem proaktívnych opatrení musia bezpečnostné smernice obsahovať aj definície postupov pri haváriách, poruchách a iných mimoriadnych situáciách vrátane možností efektívnej obnovy stavu pred haváriou.

ĽUBOSLAV LACKO, NEXTECH

ANALÝZA HROZIEB, POTENCIÁLNYCH RIZÍK A IDENTIFIKÁCIA ZRANITEĽNÝCH MIEST

Riziko opisuje pravdepodobnosť výskytu a praktický následok negatívnej udalosti. Spôsobené škody sa môžu líšiť svojimi následkami, či už priamymi, alebo nepriamymi. Podľa toho môže byť predmetná udalosť viac či menej tolerovateľná. Na to, aby firma či organizácia vedela posúdiť, ktoré udalosti sú vzhľadom na pomer následkov a nákladov na odvrátenie príslušnej udalosti prijateľné a ktoré udalosti sú vzhľadom na závažnosť dôsledkov neprijateľné, musí čo najlepšie poznať potenciálne hrozby a mieru vlastnej zraniteľnosti.

Rast rizika ešte viac podmieňuje čoraz menšia tolerancia k akémukoľvek zlyhaniu, čo má nepriamo na svedomí rozmach a globalizácia masovokomunikačných prostriedkov. Každé zlyhanie firiem, napríklad krádež údajov o klientoch, vyjde takmer okamžite najavo a dôsledkom je prakticky bezprostredný pokles ratingu príslušnej firmy. Preto je nevyhnutné, aby každá firma mala implementovaný taký systém riadenia, ktorý zvládne aj krízové situácie. Preto je riadenie rizík – Enterprise Risk Management – dôležitá súčasť podnikových informačných systémov. Často sa používa aj pojem EWRM, čo znamená Enterprise-Wide Risk Management a označuje celopodnikový manažment rizika. Manažérstvo rizika je termín používaný na označenie logickej a systematickej metódy určovania súvislostí, identifikovania, analýzy, vyhodnotenia, zaobchádzania, monitorovania a oznamovania rizík súvisiacich s akoukoľvek činnosťou, funkciou alebo procesom spôsobom, ktorý organizáciám umožní minimalizovať straty a maximalizovať príležitosti a možnosti. Manažérstvo rizika sa zaoberá aj identifikáciou príležitosti, ako aj vylučovaním alebo znižovaním strát. Riadenie rizík súvisiace s bezpečnosťou IT je súčasťou ERM.

Systematický prístup k posudzovaniu hrozieb a odhaľovaniu zraniteľností vyžaduje pravidelné vykonávanie analýzy rizík. Je to základný nástroj systému riadenia informačnej bezpečnosti, ktorý poskytuje organizácii efektívny prostriedok na kvalifikované určovanie priorít v oblasti informačnej bezpečnosti na strategickej aj operatívnej úrovni. To, či dané riziko bude odstránené, eliminované, prípadne akceptované, závisí od stupňa závažnosti a nákladov potrebných na jeho riešenie.

Analýza rizík je základný nástroj systému riadenia informačnej bezpečnosti, ktorý slúži na kvalifikované určovanie priorít v oblasti informačnej bezpečnosti

na strategickej, taktickej aj operatívnej úrovni. Analýza rizík môže byť realizovaná interne aj externe. Ak analýzu vykonáva špecializovaná firma, dôsledkom sú objektívne výsledky získané nezávislou stranou.

Súčasťou analýzy rizík je aj vytvorenie metriky nepredvídateľných faktorov, vyplývajúcich z nedokonalosti systémov a postupov, prípadne z konania človeka alebo zásahu vyššej moci. Vysvetliť predchádzajúcu vetu by si do roku 2019 vyžadovalo dosť veľké úsilie. Koronakríza v roku 2020 názorne ukázala dôležitosť zahrnutia nepredvídateľných faktorov.

Výsledky analýzy rizík poskytujú podklady na rozhodovanie manažmentu IT oddelenia a, samozrejme, aj exekutívy, aby mohli prijímať správne rozhodnutia a aplikovať efektívne opatrenia v oblasti informačnej bezpečnosti.

Analýza rizík prebieha v dvoch krokoch. V prvom kroku sa identifikujú a klasifikujú aktíva. Parametrami klasifikácie dát sú dostupnosť, dôvernosť a integrita.

Výsledkom je súpis aktív. Každému aktívu sú v spolupráci s vlastníkom stanovené požiadavky na jeho ochranu a zabezpečenie.

V druhom kroku sa identifikujú zraniteľnosti a posudzujú hrozby pôsobiace na aktíva. Na základe týchto informácií sa určí hodnota závažnosti jednotlivých rizík. Výsledkom druhého kroku je zoznam identifikovaných rizík s opisom, určenou závažnosťou a návrhom na odstránenie alebo minimalizáciu rizika.

Skúmajú sa scenáre a ich dosah najmä z hľadiska straty integrity, dostupnosti a dôvernosti informácií. Medzi negatívne dôsledky patria hlavne čas na vyšetrovanie a opravu, prestoje, náklady na odborníkov schopných obnoviť zasiahnutý systém, strata reputácie, príležitostí, a teda aj konkurencieschopnosti.

Výsledkom analýzy informačných rizík by mal byť spôsob dosiahnutia rovnováhy medzi požadovanou úrovňou zabezpečenia na jednej strane a nákladmi potrebnými na jej dosiahnutie na druhej strane. Rozlišujú sa prijateľné a neprijateľné riziká. Pri prijateľnom riziku je pravdepodobnosť výskytu nežiaduceho efektu veľmi malá, prípadne jeho následky sú akceptovateľné, takže firma alebo organizácia je s ohľadom na potenciálne náklady spojené s jeho prípadnou elimináciou ochotná toto riziko podstúpiť. Neprijateľná úroveň rizika znamená ohrozenie či dokonca zánik firmy, a preto nevyhnutne vyžaduje prijatie preventívnych opatrení na jeho zníženie. Výstupom analytickej fázy by mal byť katalóg rizík, ktorý obsahuje všetky významné riziká vrátane ohodnotenia ich možného dosahu na podnikanie spoločnosti a pravdepodobnosti vzniku kritickej udalosti. Tieto informácie sa použijú v rozhodovacom procese, v ktorom sa definujú opatrenia na pokrytie rizík a stanovujú sa priority pri ich nasadzovaní. Ak riziko nie je akceptovateľné, treba sa mu vyhnúť, čiže je potrebné prijatie iného riešenia, ako je to, ktoré viedlo k riziku. Ďalšie riešenie je zdieľanie rizika čiže poistenie.

Riadenie rizík informačnej bezpečnosti usmerňuje medzinárodná norma ISO/IEC 27001. Norma ISO/IEC 31000 rieši manažérstvo rizika. Opisuje 31 metód na ohodnotenie rizík.

ĽUBOSLAV LACKO, NEXTECH

DECEPTION TOKEN TECHNOLOGY

S HACKERMI TREBA BOJOVAŤ ICH VLASTNÝMI ZBRAŇAMI

Aby ste sa bránili počítačovým zločincom, musíte sa zamyslieť nad tým, ako uvažujú. Pokročilé hrozby vyžadujú pokročilé riešenia. Patria medzi ne technológie podvádzania a vytvárania návnad, tzv. tokenov na zachytenie škodlivých činiteľov, ktoré umožnia rýchlejšiu detekciu útokov. Tieto technológie vedia nalákať zločincov, aby sa chytili do pasce, a výrazne zlepšujú možnosti bezpečnostných tímov na rýchle a presné odhalenie útokov.

ČO ZNAMENÁ TECHNOLÓGIA DECEPTION

Technológia deception – alebo technológia pascí – predstavuje efektívny prístup k vytváraniu bezpečnostných obranných systémov, ktoré včas detegujú hrozby minimalizovaním falošných poplachov s minimálnym dosahom na výkon v sieti.

Táto technológia vytvára návnady – realisticky pôsobiace falošné aktíva (domény, prístupy k databázam, serverom, aplikáciám, súborom, používateľské poverenia a ďalšie), ktoré sú v sieti umiestnené spolu s legitímnymi aktívami. Pre útočníka, ktorý narušil sieť, neexistuje spôsob, ako odlíšiť falošné od skutočného. V okamihu, keď interaguje s návnadou, spustí sa tichý alarm, zatiaľ čo ostatné bezpečnostné systémy zhromažďujú informácie o vniknutí a zámeroch útočníka.

VYTVÁRANIE NÁVNAD

Základom fungovania technológie deception je vytváranie „virtuálneho mínového poľa", tisícky atraktívnych návnad a klamných cieľov. Sú to tzv. tokeny, na ktoré lákame útočníka a bránime tak útokom na kritické systémy.

Návnady musia spĺňať nasledujúce charakteristiky:

- Atraktívne pre hackera, aby ich použil v prieskumnej fáze útoku
- Kompletne pasívne
- Autenticky vyzerajúce
- Bežný používateľ by k nim nemal mať jednoduchý prístup
- Nie sú to aplikácie bežiace v RAM ani nainštalované na počítač
- Na počítači nie je záznam o inštalovaní tokenu

Sociálny inžiniering proti hackerom. Je dôležité, aby firma okrem klasických návnad vytvorila vlastné

návnady a klamné ciele, ktoré dokážu hackera v sieti zmiasť.

IT spoločnosti, ktoré poskytujú služby technológií deception, majú vlastné know-how, ako pristupovať k útočníkom. Na to sa často proti hackerom využíva ich vlastná zbraň – sociálne inžinierstvo. Presne tak sa vytvárajú aj návnady, na ktoré sa má chytiť sám útočník.

ODHALIŤ / UPOZORNIŤ / POSKYTNÚŤ DÁTA

Technológie deception po nasadení návnad okamžite detegujú podozrivé aktivity hackera v kritických systémoch. V priemere trvá vyše pol roka, kým spoločnosť objaví, že má v sieti útočníka. Dobre nastavené technológie deception dokážu dramaticky zrýchliť odhalenie neželaného návštevníka.

Technológia deception dokáže informovať o prebiehajúcich bezpečnostných útokoch pomocou štandardných monitorovacích nástrojov. V súčasnosti nie je otázkou, či firma bude cieľom kybernetického útoku, ale kedy.

Technológie deception poskytujú dáta na ďalšie vyšetrovanie vektorov útokov.

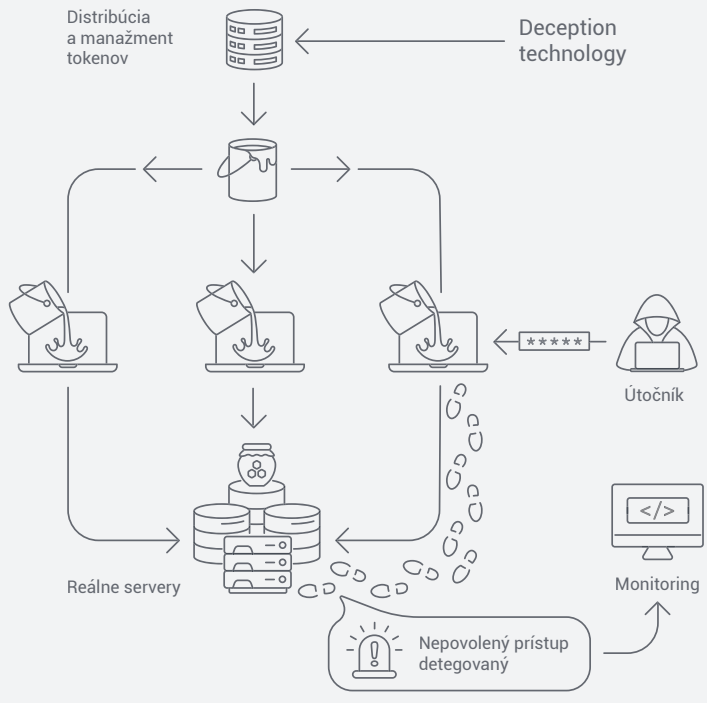
PRE KOHO JE TECHNOLÓGIA DECEPTION

Je známe, že každým rokom rastie počet kybernetických útokov, pričom väčšina spoločností nedokáže útok odhaliť. Technológie deception využívajú hlavne veľké a bezpečnostne vyspelé organizácie. Čoraz viac si však riziko útokov uvedomujú aj menšie spoločnosti a považujú túto technológiu za mimoriadne atraktívnu.

BENEFITY VYUŽÍVANIA

Zlepšená detekcia hrozieb jasne naznačuje, že útočník je v sieti. Technológia deception je pre útočníka neviditeľná a návnady sú v podstate útočníkmi nedetegovateľné. Použité výstrahy sú založené na skutočnej aktivite, takže minimalizujú počet falošných poplachov. Dobre rozmiestnené návnady okamžite upozorňujú na podozrivú aktivitu, čím sa výrazne znižujú škody spôsobené útokom. Takto generované výstrahy o útoku majú vysokú mieru dôveryhodnosti a v reálnom čase poskytujú bezpečnostným tímom príležitosti na prípravu obranných scenárov.

PETER ROTH, CIO SPOLOČNOSTI ANASOFT



TECHNOLOGICKÉ RIEŠENIE

1. **Umiestnenie tokenov:** umiestnenie návnad, ktoré sú pre útočníka atraktívne. Obsahuje preddefinované návnady s možnosťou vytvárania vlastných. Ideálne je, keď pre útočníka pripravíte vlastné návnady, ktoré sa čo najvernejšie približujú zodpovedajúcim aktívam vašej spoločnosti.

2. **Distribúcia tokenov:** návnady sú automaticky distribuované na počítače v sieti pomocou štandardných nástrojov (napr. MS SCCM, Tivoli, MS GPO).

3. **Servery:** Informácie z tokenov smerujú na falošné (honeypot) alebo existujúce servery a služby.

4. **Monitoring:** technológia deception monitoruje zneužitie tokenov pomocou štandardných nástrojov, ako sú MS SCOM, Zabbix, Nagios, OpenNMS, prípadne SIEM.

MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI

V poslednom čase môžeme pozorovať zvýšený záujem hackerov o slovenské organizácie a narastajúci počet prípadov ich napadnutia rôznymi kybernetickými útokmi. Preto sa dostáva do popredia otázka kybernetickej bezpečnosti. V rámci nej je potrebné vybudovať tím, ktorý bude aktívne predchádzať takýmto útokom, a jednou z rolí v tomto tíme je funkcia manažéra kybernetickej bezpečnosti. Organizácie, ktoré spadajú pod zákon o kybernetickej bezpečnosti, musia túto funkciu zabezpečiť zo zákona. Pre ostatných je to na ich zvážení, ale treba si povedať, že tieto veci sa neoplatí podceňovať. Napriek tomu mnohé organizácie berú kybernetickú a informačnú bezpečnosť na ľahkú váhu.

ČO JE ÚLOHOU MANAŽÉRA KYBERNETICKEJ BEZPEČNOSTI?

Je to zodpovednosť za organizovanie systému riadenia kybernetickej bezpečnosti. Cieľom jeho fungovania je obmedziť škody, ktoré by mohli vzniknúť v dôsledku chýb, omylov alebo neoprávneného použitia sietí a informačných systémov. Táto úloha je úplne kľúčová na správne nastavenie fungovania systému riadenia kybernetickej bezpečnosti.

Manažér kybernetickej bezpečnosti má povinnosť informovať priamo štatutárny orgán prevádzkovateľa základnej služby o činnostiach vyplývajúcich z výkonu jeho úlohy. Najmä o stave systému riadenia kybernetickej bezpečnosti. Manažér kybernetickej bezpečnosti je jeden zo základných nástrojov tvorby bezpečnostných opatrení prevádzkovateľa základnej služby a ich aplikácie do praxe. Manažér kybernetickej bezpečnosti by mal detailne poznať zavedené procesy a mal by disponovať dostatočnou znalosťou vnútorných IT procesov. Mal by kontrolovať fungovanie zavedených procesov informačnej bezpečnosti a ich dodržiavanie, hlavne zamestnancov informatiky, ale aj ostatných zamestnancov.

Manažér informačnej bezpečnosti je predovšetkým výkonná funkcia, ale niektoré výstupy jeho práce (koncepčné materiály informačnej bezpečnosti, prehľady stavu informačnej bezpečnosti v organizácii a najmä navrhované opatrenia) sa musia prerokovať vo vedení organizácie a po prípadných úpravách a schválení presadzovať z úrovne vedenia organizácie.

KTO BY MAL BYŤ MANAŽÉROM KYBERNETICKEJ BEZPEČNOSTI?

Asi by to nemal byť informatik, ktorý si procesy navrhne, zavedie a nakoniec si ich aj sám skontroluje, či fungujú tak ako majú. Mal by to byť človek, ktorý rozumie aj informatike, len takých je okrem informatikov už pomenej. Jedno zo schodných riešení je zabezpečiť si túto funkciu externým odborníkom alebo firmou, ktorá má s touto problematikou dlhoročné skúsenosti a vie sa oprieť o silné referencie.

DANIEL SCHIKOR,
vedúci auditor informačnej bezpečnosti, SOMI Systems a.s.

SKEN (TESTOVANIE) SIETE

Skenovanie siete predstavuje posúdenie zraniteľností siete a informačných systémov organizácie. Pri riadení testovania sa kladie dôraz na zhromažďovanie informácií o technickej zraniteľnosti siete a informačných systémov organizácie. Takisto je veľmi dôležité zhodnocovať mieru vystavenia sa zraniteľnosti, aby organizácia mohla pristúpiť k zavedeniu príslušných opatrení na potlačenie rizík. Pri skenovaní siete sa používa špecializovaný softvér, ktorý na základe vstupných parametrov na konci skenovania pridelí každému zariadeniu na konkrétnej adrese v sieti hodnotenie, tzv. CVSS - Common Vulnerability Scoring System. Tento systém v doslovnom preklade znamená „systém hodnotenia známych zraniteľností" a predstavuje verejný industriálny štandard na hodnotenie závažností zraniteľností počítačových systémov a sietí.

Výsledkom testovania siete je prehľadný manažérsky report pre vedenie organizácie a podrobný technický report pre IT oddelenie. Na základe týchto správ získa organizácia podrobný prehľad o slabých a rizikových miestach vo svojej sieti, na ktoré sa následne treba zamerať a vhodnými nástrojmi a postupmi ich čo najskôr eliminovať.

Testovanie siete zahŕňa:

- zistenie zariadení zapojených v sieti (aktívne sieťové prvky, PC, servery)
- zistenie zraniteľností na zariadeniach v sieti podľa databázy CVSS
- klasifikáciu nájdených zraniteľností podľa ich závažnosti
- testovanie na prítomnosť základných (predvolených) hesiel

Ing. ZUZANA REJKOVÁ,
analytik informačnej bezpečnosti, SOMI Systems a.s.

AKO PREDÍSŤ POMSTE ZAMESTNANCOV

Jeden z atribútov súčasného dynamického trhu práce je migrácia. Pracovníci odchádzajú, prípadne sú prepustení z rôznych dôvodov a s priebehom tohto procesu nepanuje vždy obojstranná spokojnosť. Niektorí prepustení zamestnanci pociťujú voči bývalému zamestnávateľovi nevraživosť a budú sa snažiť ho rôznym spôsobom poškodzovať. Najčastejšie ide o krádež údajov s úmyslom ich zneužitia alebo pokus o útok na podnikové informačné systémy. Podľa výsledkov viacerých nezávislých prieskumov analytických a konzultačných spoločností sa potenciálnej odvety od bývalých zamestnancov obáva až 75 % manažérov a zároveň si kladú otázku, čo treba urobiť, aby sa vyhli problémom, ktoré im nespokojní prepustení zamestnanci môžu spôsobiť. Prieskum sa, samozrejme, robil aj u zamestnancov. Viac než 40 % respondentov, s ktorými bol počas uplynulých 12 mesiacov rozviazaný pracovný pomer, priznalo, že si z firmy odniesli dôležité dáta. Najčastejšie uvádzané dôvody boli vízia ich využitia v novom zamestnaní, využitie obchodných kontaktov, využitie informácií pri vlastnom podnikaní. Najatraktívnejšie informácie sú podľa vyjadrenia respondentov databázy obchodných kontaktov, zmluvy a iné dôležité dokumenty. Na ilustráciu načrtneme situáciu, ktorá je hlavne v malých firmách viac než bežná. Pracovník má na svojom prenosnom počítači, ktorý používa v práci a často si ho berie aj domov, nielen aplikácie, ale aj dokumenty a neraz dokonca komplexné údaje v lokálnych databázach, prípadne v súboroch dokumentov tabuľkových procesorov. V lepšom prípade má zamestnanec len dokumenty a údaje, ktoré potrebuje na svoju prácu, v horšom prípade postupne zhromaždil väčšinu IT agendy svojej firmy. Pri ne-

správne nastavených bezpečnostných politikách si pracovník prv, než odovzdá firemný notebook, môže skopírovať údaje na súkromné pamäťové médiá.

Čo môže zamestnávateľ urobiť, aby pracovníkovi zabránil tieto údaje zneužiť? Odpoveď je, žiaľ, alarmujúca: Nemôže urobiť takmer nič. Pomsta bývalých zamestnancov je popri ransomvéri azda najmarkantnejší príklad toto, že prevencia je oveľa účinnejšia než riešenie následkov. Jediné, čo môže pracovníka od zneužitia údajov odradiť, je legislatívny postih. Ak pracovník údaje svojho bývalého zamestnanca zneužije a poskytne ich konkurencii alebo médiám, vystavuje sa riziku trestného stíhania. Postih za porušenie legislatívy nemusí byť aplikovateľný vo všetkých prípadoch. Dokonca môže vzniknúť opačná situácia, keď nespokojný zamestnanec poskytne niektoré údaje od svojho bývalého zamestnávateľa vyšetrovateľovi, prokurátorovi, daňovému či finančnému úradu. Tento scenár je natoľko kontroverzný, že ho nebudeme ďalej rozvíjať.

Vážny problém pre firmu, v ktorej si každý spravuje svoj počítač sám, môže byť aj odchod pracovníka, ktorý je spokojný a nemá ani v najmenšom úmysel bývalému zamestnávateľovi škodiť. Na ťažkosti môže narážať prevzatie agendy. Aj v prípade, že bol migrujúci pracovník svedomitý a poriadkumilovný a má snahu svoju agendu zodpovedne odovzdať, bude pre jeho nástupcu pomerne problematické vyznať sa v organizácii jeho dokumentov a priečinkov.

Ak zamestnávateľ podcení prevenciu, v okamihu prepustenia zamestnanca je prakticky bezmocný. No ak firma realizuje dôslednú analýzu rizík a prijme dôsledné opatrenia ohľadne správy klientskych zariadení, nielenže signifikantne zníži riziko odplaty bývalých zamestnancov a umožní bezproblémové prevzatie agendy, ale vo väčšine prípadov podstatne zvýši produktivitu. Dôležitý je hlavne audit zabezpečenia údajov, predovšetkým tých citlivých, ktorých únik by znamenal oslabenie firmy v konkurenčnom boji. Formy útokov sú stále sofistikovanejšie, takže firmy musia na ochranu vynakladať veľa úsilia a nákladov.

VŠETKO NA SERVERI ALEBO V CLOUDE

Momentálne najúčinnejšie riešenie, ako sa vyhnúť potenciálnej pomste bývalého zamestnanca, je umiestniť všetky dokumenty a údaje na server, prípadne do cloudu, či už privátneho, alebo verejného od spoľahlivého poskytovateľa. Každý pracovník by mal mať prístup k údajom a aplikáciám iba v rozsahu, ktorý potrebuje na výkon svojej práce. Aj v takomto prípade možno (napríklad príkazom Save as v aplikácii kancelárskeho balíka) vytvoriť lokálnu kópiu dokumentu.

Ešte sofistikovanejšie riešenie je využiť virtuálne desktopy VDI (Virtual Desktop Infrastructure), teda model architektúry, v ktorom sú klientske operačné systémy prevádzkované vo virtuálnych počítačoch na serveri v dátovom centre a pracovníci k nim pristupujú pomocou rozhrania s definovanými privilégiami. Jedinou úlohou klientskeho zariadenia je sprostredkovať prezentačné rozhranie, teda prenášať od servera ku klientovi obsah obrazovky a od klienta povely zadávané používateľom prostredníctvom klávesnice a myši. VDI tak poskytuje plnofunkčné a individuálne prispôsobené pracovné prostredie, pričom správca si zachováva úplnú kontrolu nad virtuálnymi počítačmi a aplikáciami. Výhodná je centralizácia údajov – údaje sú bezpečne uložené na centrálnom serveri namiesto počítačov zamestnancov.

Najvyššiu úroveň ochrany predstavujú zariadenia typu zero client, po našom nulový klient. Takéto zariadenie neobsahuje nič z klasickej architektúry počítača, tabletu ani smartfónu. Nenájdete tu procesor v klasickom ponímaní, operačnú pamäť či disky. Malá a lacná škatuľka obsahuje len zákaznícky čip schopný sprostredkovať prezentačnú vrstvu. Všetko s výnimkou zobrazovania a snímania reakcie používateľa cez klávesnicu a myš sa odohráva na serveri, kde sa klientsky počítač virtualizuje. Zariadenia typu zero client sa postupne presadzujú hlavne v oblastiach, kde je kritickým faktorom bezpečnosť. Zdôrazňujeme, že na klientskom zariadení sa NIKDY fyzicky nenachádzajú žiadne údaje, takže ani jeho prípadné fyzické odcudzenie v žiadnom prípade nespôsobí únik údajov.

ĽUBOSLAV LACKO, NEXTECH

SLUŽBA RIADENIA ZRANITEĽNOSTÍ DÁVA ZMYSEL LEN V POVOLANÝCH RUKÁCH

Len za uplynulé dva roky bolo zverejnených viac než 46-tisíc unikátnych zraniteľností systémov. A každé také „nedopatrenie" prináša zvýšené riziko napadnutia. Pokiaľ sa útočníkovi podarí zneužiť zraniteľnosť systému, je chyba na strane organizácie, pretože nedokázala správne a včas odhaliť a odstrániť problém. A to napriek tomu, že dnes už sú k dispozícii kvalitné nástroje a služby, ktoré to bežne umožňujú. Hlavným riešením je Vulnerability Management, teda riadenie zraniteľností.

Prečo by firma, ktorá už má bezpečnosť zaistenú antivírusovým programom či firewallom, mala vôbec premýšľať o nasadení Vulnerability Managementu (VM)? Napríklad preto, že tak v antivíruse, ako aj vo firewalle môžu byť zraniteľnosti, a ak firma nemá zavedený aspoň nástroj na detekciu zraniteľností, nikdy sa to nedozvie. Pokiaľ organizácia o zraniteľnostiach vo svojom systéme nevie, nepomôže jej ani ten najdokonalejší antivírus, ani ten najlepší bezpečnostný expert.

Z pohľadu odborníkov na kybernetickú bezpečnosť sa VM radí k základným nástrojom a službám na prevenciu útokov. Je to niečo, čo by mal mať k dispozícii každý, kto prevádzkuje sieť, o ktorú sa treba starať a ktorej bezpečnosť je nevyhnutné zaisťovať. Podobne ako by každý, kto má počítač, mal používať antivírusový program, aj organizácia, ktorá spravuje systém zhromažďujúci nejaké dáta, resp. generuje zisk, by mala využívať nástroje a služby Vulnerability Managementu.

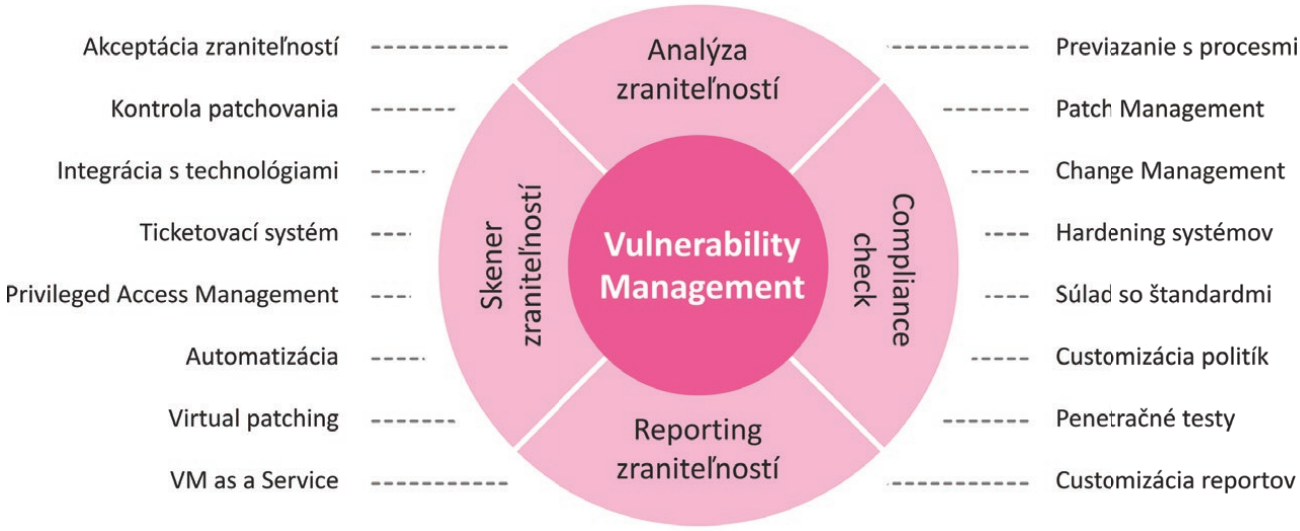
Riadenie zraniteľností je proces zahŕňajúci detekciu, analýzu a vyhodnotenie zraniteľností systému vrátane ich odstránenia. Základný nástroj na detekciu je zariadenie používané na skenovanie zraniteľností. Ide o produkt, ktorý si firma môže kúpiť a nechať nainštalovať s tým, že práve vďaka nemu bude mať dokonalý prehľad o zraniteľnostiach vo svojom systéme. Iná, vlastne tá zásadná vec však je, čo si následne s prívalom odhalených zraniteľností počne.

Čisto teoreticky možno všetky procesy súvisiace s riadením zraniteľností nastaviť tak, aby sa vykonávali automatizovane. Vždy je však vhodné mať v celom procese ľudský dohľad. Tie najkritickejšie zraniteľnosti by mal analyzovať odborník, ktorý dokáže porozumieť nielen tomu, ako ich môže útočník zneužiť, ale pozná aj danú sieť a systémy v nej. Tento prístup je najefektívnejší z hľadiska prioritizácie zraniteľností aj ich následného odstránenia.

EXPERTI AEC PRACUJÚ SO ŠPIČKOVÝMI NÁSTROJMI OD TENABLE

Spoločnosť AEC patrí k popredným poskytovateľom kybernetickej bezpečnosti. V roku 2010 rozšírila svoje portfólio o nástroje od svetového lídra v oblasti Vulnerability Managementu. Pri detailnom porovnávaní ponúk firiem ponúkajúcich produkty z oblasti riadenia zraniteľností (náhodne Rapid7, Qualys, Tripwire, Tenable, Greenbone alebo Kenna Security) sa rozhodla uprednostniť spoluprácu s americkou spoločnosťou Tenable.

Aj vďaka spolupráci s firmou Tenable sa pre nás stal Vulnerability Management strategickým produktom. Postupne sme vybudovali tím expertov, ktorí dokážu pomocou špičkových nástrojov, postupov a techník obsiahnuť celý proces riadenia zraniteľností v kto-



rejkoľvek firme či inštitúcii, počínajúc identifikáciou zraniteľností cez ich analýzu, prioritizáciu, patch management až po monitoring či reporting.

Prioritizácia zraniteľností je jeden z dôležitých procesov, ktorý má veľký vplyv na úspech celého riešenia. Dôležité je správne a včas vybrať tie aktuálne najkritickejšie zraniteľnosti, čo však býva kameňom úrazu v prípade väčšiny zákazníkov. Vďaka nástrojom a skúsenostiam dokážu naši odborníci pravidelne a systematicky vyhodnocovať získané informácie a vykonávať prioritizáciu tak, aby nimi nebola dotyčná spoločnosť zahltená.

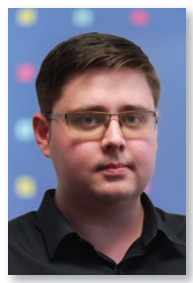
VÝBER NÁSTROJA JE DÔLEŽITÝ, ALE NA RIEŠENIE ZĎALEKA NESTAČÍ

Komplexný nástroj na riadenie zraniteľností poskytuje aj možnosť kontroly súladu, teda zaistenie tzv. compliance. Zraniteľnosti nie sú jediný problém, ktorému firmy čelia. Často môže útočník zneužiť aj nesprávne nakonfigurovaný systém, ktorý nespĺňa určité bezpečnostné štandardy. Práve zaistenie bezpečnej konfigurácie, tzv. hardening, je oblasť, ktorú dokáže tím AEC pomocou nástrojov Tenable efektívne riešiť.

Prostredie každého klienta je vysoko individuálne. Pokiaľ má VM správne plniť svoju funkciu, nemožno túto službu redukovať iba na implementáciu nástrojov, vyhodnotenie získaných dát a opravu kritických zraniteľností. Z našich skúseností vyplýva, že predovšetkým pre bezpečnostných manažérov firiem je absolútne zásadné riadenie celého procesu.

Ide o otázku, ako bude proces riadenia zraniteľností uchopený, ako sa celý tento systém podarí integrovať do súčasných procesov v spoločnosti. Súčasťou riešenia AEC je preto aj využívanie testovacieho prostredia tak, aby pri patchovaní zraniteľností nebolo priamo ohrozené produkčné prostredie zákazníka. A v neposlednom rade treba o každom kroku podrobne reportovať a doložiť úspešnosť toho, ako riadenie zraniteľností prebieha.

A to je vlastne najväčší rozdiel medzi tým, keď si zákazník zadováži samotný skener zraniteľností, a tým, keď si zaistí expertné služby odborníkov z AEC. Nástroje síce vedia na základe výpočtov a odhadov identifikovať zraniteľnosti, ale ich možnosti, ako s týmito zraniteľnosťami ďalej pracovať v prospech klienta, sú limitované. Naši ľudia vedia, čo zákazník používa, rozumejú tomu, ako funguje jeho prostredie, a preto vždy urobia všetky potrebné postupy a techniky lepšie, než to dokáže akékoľvek zariadenie.



TOMÁŠ HLIBOKÝ
Senior Security Specialist
AEC, s. r. o. | Security Technologies Division,
www.aec.sk

IT BEZPEČNOSŤ SA PRESÚVA DO OBLAKOV, ESET PONÚKA CLOUDOVÉ RIEŠENIE

ŠPECIÁLNY PROJEKT

Presunom zamestnancov na home office sa firemné siete rozšírili do stoviek domácností. Na ochranu pred kybernetickými hrozbami potrebujú mať organizácie pod kontrolou všetky koncové zariadenia. Spoločnosť ESET ponúka dokonalý prehľad cez cloud s novým produktovým balíkom ESET PROTECT.

Čoraz viac firiem presúva správu IT infraštruktúry do cloudu. Na chod firemnej siete tak možno dohliadať prakticky z akéhokoľvek miesta. Takzvaná „cloudifikácia" naberá na obrátkach už pomerne dlho. Pandémia je však pre tento proces doslova katalyzátorom. Koronavírus zmenil svet okolo nás a firmy sa museli prispôsobiť novému spôsobu práce z domu.

Na situáciu sa však adaptovali aj kybernetickí zločinci, ktorí nezaháľajú ani počas globálnej zdravotníckej krízy. Nedávno rezonoval napríklad mohutný ransomvérový útok, ktorý ochromil ropovod rozvádzajúci najviac ropy v USA. Spoločnosť Colonial Pipeline nakoniec vyplatila hackerom výkupné vo výške okolo 5 miliónov dolárov. Oblasť digitálnych hrozieb sa neustále vyvíja a okrem tradičných hrozieb využívajú útočníci aj pokročilé techniky. Zamestnanci, ktorí pracujú na diaľku, sú pritom novými hrozbami ešte zraniteľnejší. Dokonalý prehľad o zabezpečení celej siete v reálnom čase je preto pre firmy dôležitejší ako kedykoľvek predtým.

ODPOVEĎ NA DYNAMICKÉ ZMENY

Na dynamické zmeny v oblasti kybernetickej bezpečnosti reaguje spoločnosť ESET uvedením produktových balíkov **ESET PROTECT**. Cloudové riešenie **ESET PROTECT Cloud** ochráni pomocou konzoly digitálne zariadenia zamestnancov bez ohľadu na to, kde sa nachádzajú. Tento nástroj umožňuje organizáciám spravovať všetky koncové zariadenia z jedného miesta, čo ponúka dokonalý prehľad o zabezpečení celej firemnej siete vrátane zariadení v priestoroch firmy aj mimo nej. Okrem riešenia bezpečnostných incidentov si IT správcovia môžu na diaľku zobrazovať informácie o konkrétnych zariadeniach.

Toto riešenie prináša aj množstvo nových zaujímavých funkcií, ako je napríklad cloudová správa mobilných zariadení. V spojení s aplikáciou **ESET Endpoint Security** pre Android umožňuje správu mobilných zariadení a poskytuje ďalšiu vrstvu zabezpečenia. Chráni používateľov zariadení so systémom Android pred najbežnejšími hrozbami typickými pre túto platformu a zároveň zabraňuje šíreniu malvéru, ktorý môže do firemnej siete preniknúť práve prostredníctvom mobilných zariadení.

S RIEŠENÍM ESET PROTECT CLOUD UŠETRÍTE

Mnohé firmy začali v dôsledku pandémie škrtať výdavky a optimalizovať vynakladané prostriedky. Bez toho, aby odsúvali bezpečnosť na druhú koľaj, dokážu spoločnosti dosiahnuť želané úspory prechodom na cloudové riešenia. Pri správe na diaľku odpadávajú náklady na zabezpečenie servera, ktoré sú bežné pri lokálnych riešeniach v priestoroch firmy. Cloudové zabezpečenie umožňuje, aby sa spoločnosti zbavili fyzických serverov, záložných serverov či klastrov pre prípad zlyhania. IT správcovia sa navyše viac nemusia zaoberať aktualizáciami serverového softvéru či komponentov. Túto úlohu za nich vybaví ESET.

ESET PROTECT Cloud v skutočnosti vyžaduje iba jedného IT správcu. Balík pokročilých bezpečnostných riešení na ochranu firmy pred útokmi nasadí jednoducho a rýchlo prostredníctvom cloudovej konzoly. Firmy, ktoré sa rozhodnú zabezpečiť novým produktom, tak nebudú potrebovať tím špecialistov na nastavenie a údržbu serverov, databáz, softvéru a inej lokálnej infraštruktúry. Správcovia zostanú odbremenení aj od starostlivosti o aplikácie, pri ktorých sa často vyskytujú chyby zabezpečenia. Namiesto ich dôslednej opravy sa môžu venovať urgentnejším problémom.

EFEKTIVITA, POHODLIE AJ FLEXIBILITA

Vďaka jednoduchému a rýchlemu nastaveniu sa dokáže IT správca prihlásiť do konzoly a začať s ochranou zariadení už do niekoľkých minút. ESET PROTECT ponúka rozličné spôsoby nasadenia s využitím pomoci live inštalátorov. Bezproblémové zavedenie bezpečnostných riešení na všetky koncové zariadenia je tak jednoduché aj v tej najväčšej firemnej sieti.

Riešenie je zároveň škálovateľné, aby vyhovelo potrebám všetkých zákazníkov. Firmám umožňuje rozšíriť alebo znížiť pokrytie podľa ich veľkosti z pohľadu počtu pracovníkov. Prispôsobiť dynamicky sa meniacim potrebám veľkých organizácií či malých firiem sa dokážu aj praktické reporty. Tie prinášajú správcom lepší prehľad. Na ovládanie nie je potrebný špecializovaný tím IT pracovníkov, rozsiahle školenia ani dodatočný hardvér. Špecialisti zo spoločnosti ESET sú navyše v prípade potreby pripravení kedykoľvek pomôcť.

Všetky produktové balíky zahŕňajú cloudovú alebo lokálnu konzolu na správu zabezpečenia a takisto bezpečnostné riešenia na ochranu koncových zariadení. Ak vaša firma hľadá najmä spoľahlivú ochranu e-mailovej komunikácie, môže siahnuť po balíku **ESET PROTECT Mail Plus**.

BALÍKY PRODUKTOV ESET PRE FIRMY A ORGANIZÁCIE

ESET PROTECT Advanced zahŕňa ochranu koncových zariadení pred ransomvérom a novými (tzv. zero day) hrozbami spolu so zabezpečením údajov pomocou úplného šifrovania disku. Riešenie je ideálna voľba pre malé a stredné firmy a poskytovateľov spravovaných služieb (MSP). Umožňuje aj analýzu s využitím strojového učenia na vysokovýkonných počítačoch v cloude, čo prispieva k rýchlejšiemu odhaleniu nových druhov malvéru, ktoré sa snažia vyhnúť detekcii bezpečnostných produktov na koncových zariadeniach.

Pre veľké organizácie je vhodný balík **ESET PROTECT Enterprise**, ktorý poskytuje komplexný prehľad o bezpečnosti a zachytí dokonca techniky skupín, ktoré používajú pokročilé pretrvávajúce hrozby. Tento balík totiž ponúka sofistikované **EDR riešenie** na detekciu a reakciu na útoky na koncové zariadenia s detekciou na základe pravidiel, vyhľadávaním hrozieb a možnosťou nápravy zistených bezpečnostných problémov. Zvolením predplatného ESET PROTECT Enterprise tak firemní zákazníci získajú všetky benefity balíka ESET PROTECT Advanced, doplnené o výhody riešenia EDR.

NÁSTUPCA ESET CLOUD ADMINISTRATOR

ESET PROTECT Cloud je nástupcom a rozšírením produktu ESET Cloud Administrator. V rámci nového riešenia sa zvýšila horná hranica spravovaných zariadení, čo ocenia najmä väčšie firmy. ESET PROTECT Cloud kladie dôraz na riešenie výziev a problémov, s ktorými sa reálne stretávajú firmy a organizácie všetkých veľkostí, a snaží sa plniť ich potreby súvisiace so správou zabezpečenia koncových zariadení.

ESET

AKÉ SÚ BEZPEČNOSTNÉ RIZIKÁ A AKÉ OPATRENIA BY MALI PRIJAŤ ZAMESTNÁVATELIA

ŠPECIÁLNY PROJEKT

O rizikách, ktoré číhajú na zamestnancov pracujúcich z domu, a o preventívnych opatreniach sme sa rozprávali s **Jánom Vaľom**, bezpečnostným špecialistom spoločnosti LYNX.

Aké sú riziká práce z domu? Sú počítače pripojené cez domácu sieť ľahkým cieľom kyberzločincov?

Ján Vaľo: Domáci používatelia sú iba zriedka kvalitne chránení pred kybernetickými útočníkmi, často nevyužívajú ani základné možnosti ochrany pred útokmi, nie sú aktualizované zariadenia a počítače a často nie sú zmenené štandardné nastavenia vrátane hesiel. Potom sa stávajú ľahkým cieľom útočníkov. Typickým následkom sú zašifrované dáta po ransomvérovom útoku, uniknuté osobné údaje alebo počítače zaradené v botnetoch využívaných na kriminálnu činnosť.
Firemné počítače pripojené k takejto sieti sa potom stávajú ľahkým cieľom. Napadnuté môžu byť, pokiaľ napríklad na prístup na internet využívajú nechránené domáce pripojenie, prípadne po lokálnej sieti z kompromitovaného domáceho počítača.

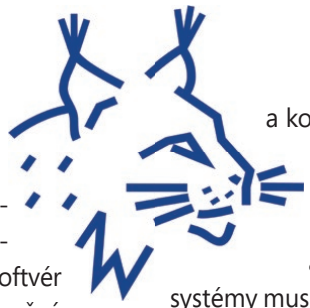
Aké opatrenia by mal urobiť zamestnávateľ pri presune pracovníka na home office?

Ján Vaľo: Firemný počítač musí byť aj v domácej sieti chránený minimálne podľa rovnakých firemných bezpečnostných politík ako vo firemnej sieti. Napríklad využitie súkromných počítačov na prácu z domu je vhodné iba v niektorých, veľmi špecifických prípadoch. Pracovné prostredie zamestnávateľa na to musí byť dopredu pripravené. V žiadnom prípade by súkromný počítač nemal slúžiť ako náhrada pracovného počítača pri home office.

Treba si uvedomiť, že v domácej sieti pracovný počítač nie je chránený firemným perimetrom ani fyzickými bezpečnostnými opatreniami. Takto pripojený firemný počítač musí využívať niektoré centrálne firemné bezpečnostné technológie na komunikáciu s externým prostredím buď pripojením do firemnej siete cez VPN, alebo pomocou využitia cloudových služieb bezpečnostných spoločností (technológie typu secure access service edge – SASE).

Prečo je potrebné používať pripojenie VPN a ako čo najlepšie zabezpečiť domácu sieť?

Ján Vaľo: Interné systémy firmy predstavujú často jej najcennejšie aktíva v rámci IT. Ich ochrana by preto mala byť na najvyššom stupni bezpečnosti. Prístup k nim by mal byť striktne kontrolovaný a zabezpečený. Na tieto účely slúži vzdialený prístup pomocou VPN. Umožňuje jednak utajenie komunikácie pomocou šifrovania, na druhej strane umožňuje aj silno autentizovať používateľa, zaručiť, že daný počítač spĺňa bezpečnostné požiadavky na vstup do internej siete, a prípadne aj obmedziť tento prístup na nevyhnutné minimum.



Bez zvýšenia nákladov možno realizovať aspoň základné zabezpečenie:

- zmeniť konfiguráciu domácich smerovačov tak, aby sme zmenili základné nastavenie siete, štandardné heslá, aktualizovať softvér na poslednú verziu, na Wi-Fi použiť bezpečné protokoly (personal WPA2), nezverejňovať svoju sieť (hide SSID), aktivovať sieťový firewall na smerovači a zakázať akúkoľvek komunikáciu zvonku dovnútra domácej siete
- všetky počítače a mobilné zariadenia by mali byť legálne, aktualizované, najlepšie automaticky, a mali by mať inštalovaný bezpečnostný softvér
- používatelia by vo verejných cloudových službách nemali využívať jednoduché heslá, opakovane používať rovnaké heslo alebo využívať heslá, ktoré používajú vo firemnej infraštruktúre – ideálne je používať softvér na generovanie a ukladanie hesiel

Porovnajte výhody a nevýhody pripájania sa počas home office ku cloudovej službe a na podnikový server. Aké nové hrozby prináša využívanie cloudových služieb?

Ján Vaľo: V čase intenzívneho home office je veľmi výhodné využitie cloudových služieb na prácu zamestnancov. Či už videokonferencií, kolaboračných nástrojov, alebo zdieľania súborov a podobne. Používateľom umožňujú jednoduché použitie z rôznych lokalít, využitie rýchleho lokálneho pripojenia bez zdĺhavého pripájania sa do firemnej VPN. Z pohľadu firmy umožňujú zbaviť sa centrálnej správy a dohľadu nad aplikáciami.

Využívanie cloudových služieb však prináša nové hrozby. Treba si uvedomiť, že cloud je v princípe iba „počítač niekoho iného". CSP (Cloud Service Provider) zvyčajne využíva takzvaný shared responsibility model. To v preklade znamená, že zodpovednosť za bezpečnosť celého riešenia si CSP a používateľ delia v závislosti od typu služby (IaaS, PaaS, SaaS...). Bezpečnosť dát je vždy na zodpovednosti zákazníka, preto je nevyhnutné zabezpečiť ich zálohovanie a obnovu, aj pokiaľ sa ukladajú v cloude.

Aké produkty a služby odporúčate firmám na zaistenie bezpečnej práce z domu (na cestách, v hoteli...)?

Ján Vaľo: Samozrejmosť je použitie moderného antimalvérového riešenia vrátane detekcie anomálií v správaní a komunikácie botov, ochrany pri sťahovaní súborov z internetu pomocou ich kontroly v cloudovom bezpečnostnom systéme (sandbox), obmedzenie spúšťania aplikácií či šifrovanie diskov. Všetky tieto systémy musia byť centrálne spravované a používateľsky čo najviac transparentné.

Bezpečnosť komunikácie počítača by mala byť zaistená lokálnym firewallom, spadajúcim pod centrálnu firemnú správu, ktorý obmedzí prevádzku na nevyhnutne potrebnú – ideálne iba na komunikáciu pomocou VPN do firmy. Ďalej treba prevádzku šifrovať, a to buď pomocou VPN pri prístupe do firemnej siete, alebo pomocou protokolu HTTPS pri prístupe k webovým službám. Ľahko realizovateľná a relatívne lacná možnosť je aj využitie bezpečnostných riešení vo forme filtrovania prevádzky DNS. V tomto prípade sa komunikácii počítača so známym nebezpečným cieľom na internete zabráni už pri nadväzovaní spojenia a komunikácia sa vôbec neuskutoční.

Aké opatrenia by mal presadiť a zrealizovať CIO v rámci firemnej infraštruktúry na maximálnu bezpečnosť home office?

Ján Vaľo: CIO/CISO by mal mimoriadne dbať hlavne na úpravu aktuálnej bezpečnostnej politiky vzhľadom na nové hrozby, ktoré prináša masívny home office, a jej implementáciu vo firemnom prostredí. Keďže každá spoločnosť je jedinečná, aj hrozby, ktoré na ňu vplývajú, sú do veľkej miery individuálne. Preto treba vykonať rizikovú analýzu, vychádzajúcu z reálnych podmienok. Aj napriek všetkej snahe o bezpečnosť sa využívaním home office rozširuje vektor potenciálnych útokov. Preto je potrebné pripraviť sa aj na možnosť bezpečnostného incidentu. Pre prípad straty dát (napr. pri útoku ransomvéru) treba mať funkčnú a kvalitnú zálohovaciu stratégiu. Samozrejmosťou by malo byť pravidelné, ideálne automatizované testovanie obnoviteľnosti zálohy.

Pre prípad výpadku infraštruktúry je takisto nevyhnutné mať vytvorený a pravidelne testovaný plán obnovy pri katastrofe (disaster recovery) a plán na pokračovanie spoločnosti v prevádzke (business continuity). Zároveň je vhodné, aby sa spoločnosť pokúsila pomôcť svojim zamestnancom so zabezpečením ich domácich sietí.

LYNX

ZODPOVEDNOSŤ ZA LEGÁLNY SOFTVÉR

Softvér je dnes kľúčový komponent digitálnej transformácie a jeho používanie v súlade s licenčnými podmienkami nadobúda čoraz väčší význam. Právny základ **komerčného** softvéru tvorí smernica EÚ 2009/24/ES o právnej ochrane počítačových programov, ktorá sa v slovenskej legislatíve transponovala do autorského zákona č. 185/2015 Z. z. Pri **nekomerčnom**, tzv. open source softvéri je rozšírená mylná predstava, že je automaticky zadarmo, čo však nemusí byť vždy pravda. Preto je dôležité, aby firmy rozumeli podmienkam správneho používania softvéru, spôsobu licencovania a právnym dôsledkom v prípade porušenia licenčných zmlúv. Softvérové firmy si čoraz prísnejšie chránia svoje duševné vlastníctvo a spravidla každá licenčná zmluva obsahuje klauzulu o možnosti vykonať tzv. softvérový audit s cieľom preveriť súlad nasadenia a používania softvéru s licenčnými podmienkami. Nelegálnym používaním softvéru dochádza k porušovaniu nielen autorského zákona, ale aj k splneniu skutkovej podstaty trestného zákona.

S nesprávnym alebo neoprávneným používaním softvéru sú spojené rôzne **riziká**, napr. finančné, právne, reputačné, daňové, regulačné a ďalšie. Je na zamestnávateľovi, ktorý vlastní počítače a servery, aby zabezpečil legálny softvér a informoval a vzdelával svojich zamestnancov v tejto oblasti. Za činnosť organizácie nesie zodpovednosť jej štatutárny zástupca. Hoci formálne je zodpovedná za činnosť organizácie jedna osoba, legálne používanie softvéru je vec všetkých zamestnancov – od koncového používateľa až po vrcholový manažment firmy.

Legálny softvér, zodpovednosť za používanie a ďalšie okruhy sú súčasťou širšej oblasti nazvanej **riadenie životného cyklu softvérových aktív** (Software Asset Management – SAM), ktorá je už dnes dobre opísaná a štandardizovaná, napr. ISO Working Group for SAM Standards (ISO/IEC JTC1 SC7 WG21) (**www.iso.org**), Overview of the Development Process for ISO/IEC Standards for SAM (**www.iaitam.org**), ITIL v4 SAM Guide, SAM and ITAM Standards: Benefits for Organizations and Individuals BSA SAM Advantage Program (**www.bsa.org**). Oblasť SAM obsahuje množstvo overených praktík a postupov, aby nedochádzalo k nelegálnemu používaniu softvéru. Z doterajších skúseností je zrejmé, že požadovaný stav sa nedá dosiahnuť len správnym používaním IT technológií, ale treba definovať celkovú stratégiu riadenia IT aktív, **pravidlá** a **procesy**, spôsob **zberu dát** a neustále **vzdelávať** zamestnancov firmy. Na celkovej „compliance" sa podieľajú všetci radoví zamestnanci a stredný manažment s podporou vrcholového riadenia firmy. Legálny softvér nie je len vec IT oddelenia, svoj diel zodpovednosti nesú alebo k nemu prispievajú aj ďalšie oddelenia, ktoré by mali poznať najlepšie postupy a štandardy v danej oblasti:

1. **IT oddelenie** – je to primárne oddelenie, keďže riadi všetky IT aktíva. Pre softvér definuje zoznam povolených (whitelist) alebo zakázaných aplikácií (blacklist), plánuje a riadi požiadavky na nákup, inštaláciu, prípadne odinštalovanie softvéru, sleduje využívanie softvéru a výskyt nelicencovaných aplikácií. Optimalizuje aplikačné portfólio s cieľom jeho maximálnej štandardizácie. Vedie centrálnu databázu o stave a používaní všetkých IT aktív nielen v on-premise prostredí, ale aj v cloude (SaaS). Prevádzkuje nástroje na automatickú hardvérovú a softvérovú inventarizáciu v IT infraštruktúre firmy a v cloude s prípadným stanovením stavu: podlicencovaný (riziko penalizácie) alebo nadlicencovaný (možnosť úspor).
2. **Nákupné oddelenie** – riadi centrálnu databázu nákupov licencií a údržby pre každý softvér a vedie históriu nákupov. Je zodpovedné za optimálne obstarávanie softvéru a za minimalizáciu tzv. shadow IT, teda softvéru, ktorý bol nadobudnutý legálne, ale mimo štandardných procesov a postupov. Tento softvér je síce legálne nadobudnutý, ale mimo vedomia IT oddelenia a nie je centrálne riadený a monitorovaný podľa odporúčaných postupov.
3. **Právne oddelenie** – rieši obsah licenčných a servisných zmlúv z právneho hľadiska a chápe význam IT pojmov a prípadné sankcie.

4. **Finančné oddelenie** – sleduje celkové finančné náklady na softvér a jeho údržbu, náklady na penále a na opätovnú obnovu údržby. Venuje pozornosť nákladom na cloud, SaaS atď. Rieši problém shelfware, t. j. softvéru, ktorý sa už vo firme nevyužíva a predstavuje viazaný kapitál.
5. **Oddelenie rizík** – definuje riziká softvérových auditov v oblasti IT a navrhuje spôsoby ich minimalizácie. Spolu s IT vykonáva aspoň raz ročne celkový interný softvérový audit.
6. **Oddelenie kybernetickej bezpečnosti** – pre CISO manažéra predstavuje nelegálny softvér vysoké riziko, preto by mal všemožne podporovať výhradné používanie legálneho softvéru a mať presne stanovené pravidlá BYOD pre súkromné licencie používané vo firme. SAM je zdroj neoceniteľných informácií pre oddelenie počítačovej bezpečnosti (v zátvorke je uvedené príslušné kritérium fázy IDENTIFY podľa kybernetického rámca NIST www.nist.gov):

a) Zisťuje, koľko, kde a aké hardvérové/cloudové zariadenia sa používajú (**NIST ID.AM-1**).

b) Informuje, aké platformy a aplikácie sú vo firme nainštalované (**NIST ID.AM-2**).

c) V prípade incidentu definuje **procesy** a dátové toky IT aktív (**NIST ID.AM-3**).

d) Poskytuje **kategorizáciu** softvérových aplikácií (**NIST ID.AM-4**).

e) Poskytuje **klasifikáciu** softvéru podľa jeho kritickosti a hodnoty (**NIST ID.AM-5**).

f) Definuje oblasti **zodpovednosti** pre zamestnancov, manažérov a externých dodávateľov (**NIST ID.AM-6**), ako aj mnoho ďalších, napr. poskytuje prehľad, aké zálohy boli nainštalované a na ktorých serveroch, informuje o oficiálnych zraniteľnostiach, sleduje, ktoré verzie softvéru/firmvéru sa používajú a či sú ešte oficiálne podporované výrobcom, atď.

V stredných a veľkých firmách je overená prax mať vlastný **program SAM**, ktorého cieľom je minimalizovať riziká v súvislosti s nelegálnym softvérom a s „non-compliance" a optimalizovať využívanie existujúceho softvéru vo firme tak, aby ste platili za to, čo reálne používate. Program SAM vo firme presne stanoví osoby a oblasti zodpovednosti, procesy, spôsob zberu potrebných údajov a ich požadovanú kvalitu, kľúčové technológie na automatizáciu a indikátory úspešnosti programu SAM. IT oddeleniu môže výrazne pomôcť pri automatizácii nasadenia niektorého zo zahraničných alebo domácich nástrojov SAM (Gartner: Magic Quadrant for SAM Tools https://www.gartner.com/en/documents/3987747/magic-quadrant-for-software-asset-management-tools).

V menších firmách môžu byť prvým krokom licenčné školenia a konzultácie, určenie IT špecialistu a prípadne využívanie licenčných nástrojov, ktoré poskytuje výrobca softvéru zadarmo.

Používanie výhradne legálneho softvéru je vo vyspelom svete samozrejmosť. Hoci klasické softvérové pirátstvo je na Slovensku na ústupe, v oblasti riadenia softvérových aktív je ešte čo zlepšovať. Problém nezmizne ani pri prechode do cloudového prostredia, kde sa odhaduje, že 30 % až 35 % investícií je vynaložených neefektívne, zatiaľ čo nové IT softvérové technológie prinášajú nové výzvy.

RUDOLF KLEIN,
Senior konzultant, Risk Advisory, Deloitte

POISTENIE KYBERNETICKÝCH RIZÍK

Srastúcim povedomím o cloud computingu, sociálnych sieťach, firemnej politike Bring Your Own Device (BYOD), internete vecí (IoT) a veľkých dátach (big data) sa kybernetické riziká stávajú jednou z hlavných tém pre všetky organizácie.

Napadnuté zariadenia, odstavené webové stránky, prelomené siete, nedostupné služby, skopírované e-maily, ukradnuté dáta z kreditných kariet alebo iné kybernetické útoky sa pre mnohé firmy stávajú dennou realitou.

A tu treba prijať fakt, že žiadna firma nie je proti nim úplne imúnna a na 100 % chránená.

Väčšina firiem preto pracuje na tom, aby si zvyšovala svoju schopnosť efektívne zareagovať na kybernetické útoky. Pretože práve táto schopnosť – zareagovať správne a včas – rozhoduje o tom, aké veľké škody takéto útoky zanechajú na fungovaní firiem.

V čoraz prísnejšom právnom a regulačnom prostredí (napr. GDPR) a vzhľadom na častejšie celosvetové kybernetické útoky uskutočňujú spoločnosti proaktívne kroky na preskúmanie, obranu a prípadné prenesenie kybernetických rizík.

Chrániť vaše príjmy a budúcnosť vášho podnikania pomôže poistenie kybernetických rizík. Toto poistenie je určené pre všetky podnikateľské subjekty bez ohľadu na predmet činnosti.

Poistenie kybernetických rizík je dôležité na zabezpečenie podnikania, pretože dnes sa väčšina činností spolieha na počítačové systémy alebo softvér. Každý podnikateľ zhromažďuje a uchováva dáta o zákazníkoch, dodávateľoch alebo zamestnancoch. Frekvencia kybernetických útokov stúpa a už to nie je problém iba veľkých spoločností. Obzvlášť zraniteľné sú malé a stredné podniky, ktoré majú menej zdrojov na zabezpečenie systémov a údajov.

PREČO NESTAČÍ „TRADIČNÉ" POISTENIE?

Hoci existujúce tradičné formy poistenia môžu zahŕňať určitý stupeň krytia (tzv. silent cyber), nie sú koncipované tak, aby pokrývali množstvo rizík spojených s čoraz viac digitálnym svetom. Tradičné formy poistenia reagujú takto:

- **Všeobecná zodpovednosť** – pokrýva fyzické zranenia a majetkovú škodu, nie hospodárske straty
- **Zodpovednosť za škody spôsobené výkonom povolania** – pokrýva iba hospodárske škody, ktoré vzniknú v dôsledku zlyhania definovaných služieb, a môže obsahovať výluku zodpovednosti za porušenie ochrany dát a osobných údajov

- **Poistenie majetku** – pokrýva hmotný majetok a dáta ním NIE sú. Stratu musí spôsobiť fyzická udalosť, kým udalosti poškodzujúce dáta sú pravdepodobne vírusy alebo hackerské útoky
- **Poistenie pred trestnými činmi (crime)** – pokrýva zamestnancov a zvyčajne iba peniaze, cenné papiere a hmotný majetok, nepokrýva majetok tretích strán, napr. dáta zákazníkov/klientov

Chrániť vaše príjmy a budúcnosť vášho podnikania môže **poistenie kybernetických rizík**.

HLAVNÉ DÔVODY NA ZVÁŽENIE POISTENIA KYBERNETICKÝCH RIZÍK:

- Odborná pomoc 24 hodín denne a 7 dní v týždni – reakcia na krízové situácie v oblasti IT, PR a právneho poradenstva na:
  - rýchle obnovenie údajov alebo počítačových programov
  - plnenie záväzkov voči zákazníkom, splnenie ich očakávaní a v konečnom dôsledku zachovanie vašej dobrej povesti
  - udržiavanie prevádzky vášho podniku
- Poistná náhrada vašich nákladov vrátane:
  - nákladov na uvedenú pomoc
  - vášho ušlého zisku/strateného príjmu a dodatočných výdavkov
  - nákladov na obnovenie dát alebo systémov po vydieraní
  - nákladov na ochranu a vyrovnanie pohľadávok tretích strán a regulátorov ochrany osobných údajov

POISTNÉ RIEŠENIE KYBERNETICKÝCH RIZÍK UŠITÉ NA MIERU SA VZŤAHUJE NA:

- **náklady na odborné služby** na účel zabránenia či zmiernenia nepriaznivého dosahu, ako PR služby, komunikačné služby, IT služby, náklady na obnovu dát
- **prerušenie prevádzky (výpadok siete)** – úhrada ušlého zisku súvisiaceho s neoprávneným vniknutím do počítačového systému
- **povinnosti voči dozorným orgánom** – sankcie uložené dozorným orgánom za neoprávnené a nesprávne nakladanie s údajmi vrátane nákladov na právne zastupovanie
- **zodpovednosť za neoprávnené nakladanie s údajmi** – dôverné osobné a obchodné informácie vrátane dát uložených u subdodávateľov
- škody a náklady na právne zastúpenie v prípade **porušenia práv duševného vlastníctva tretej osoby** alebo nedbalosti pri správe elektronického obsahu médií
- **škody spôsobené vydieraním** – vlastné škody spôsobené vydieraním hackera vrátane úhrady výkupného

SLAVOMÍR CYPRICH,
obchodný riaditeľ, Aon Central and Eastern Europe, organizačná zložka

VYNÚTENIE DODRŽIAVANIA BEZPEČNOSTNÝCH POLITÍK

Pod pojmom bezpečnostná politika chápeme dokument alebo súbor viacerých dokumentov, ktorými organizácia definuje celkový prístup k bezpečnosti. Vedenie prostredníctvom nej vyjadruje svoj záväzok a odhodlanie implementovať informačnú bezpečnosť, prezentuje bezpečnostné ciele a stanovuje rámec pre opatrenia, ktorými sa informačná bezpečnosť v organizácii dosahuje.

Každé nariadenie je natoľko účinné, nakoľko dokážeme vynútiť jeho dodržiavanie. Pojem vynútiť môžeme chápať v rôznych kontextoch. Vynútiť dodržiavanie nariadení z oblasti bezpečnosti IT možno, samozrejme, sankciami pri zistení porušenia alebo technickými prostriedkami. Väčšina z nás pozná z vlastnej praxe, že k účtom v dôležitých službách si musia zvoliť dostatočne silné heslo, prípadne ich systém prinúti po uplynutí určitého času heslo zmeniť. Ťažko povedať, ktorý spôsob je účinnejší. Na prvý pohľad by sa mohlo zdať, že jednoznačne vynútenie dodržiavania pravidiel technickými prostriedkami. No nie je to celkom tak, pretože takto nedokážeme obsiahnuť všetky potenciálne rizikové situácie. V tomto ohľade je účinnejšia hrozba sankciami, prípadne kombinácia. Technické obmedzenia môžu vzbudiť pocit falošného bezpečia, že ak zamestnanec dodržal všetko, čo sa od neho požaduje, urobil maximum na zabránenie bezpečnostným incidentom.

Naproti tomu, ak si zamestnanec uvedomuje, aký postih ho čaká (či už priamy v podobe sankcií voči nemu, alebo nepriamy postih vyplývajúci z toho, že firma, v ktorej pracuje, utrpí pri bezpečnostnom incidente veľké škody a stratu reputácie), bude sa snažiť, aby k takejto situácii nedošlo. Inak povedané, ak je zamestnanec zodpovedný a iniciatívny, nebude dodržiavať len priame nariadenia, ale bude sa zaujímať aj o osvedčené metódy, ako postupovať v rôznych situáciách.

Vynútenie dodržiavania bezpečnostných politík je zakomponované aj do medzinárodného štandardu ISO/IEC CD 29146 Information technology - Security techniques, kde sa predpokladá, že architektúra informačných systémov bude obsahovať nielen takzvané body rozhodnutia o politike (v originálnej terminológii Policy decision point), ale aj body zabezpečujúce vynútenie politiky (Policy enforcement point). Týka sa to hlavne prístupu k údajom a službám.

Bez ohľadu na veľkosť firmy by mal byť určený manažér, prípadne zamestnanec, ktorý je zodpovedný za zabezpečenie IT. Aby svoje poverenie mohol efektívne a zodpovedne vykonávať, musí mať aj príslušné právomoci, aby dokázal u ostatných zamestnancov firmy presadiť dodržiavanie pravidiel. V tomto ohľade, samozrejme, potrebuje podporu od manažmentu firmy. Aj pri nasadzovaní bezpečnostných prostriedkov, či už softvérových, alebo hardvérových, je dôležité, či a ako dokážu nielen zabezpečiť, ale keďže ide o ochranu kritickej infraštruktúry, aj vynútiť dodržiavanie bezpečnostných politík.

„IT SYSTÉMY MUSIA MAŤ IMPLEMENTOVANÚ BEZPEČNOSTNÚ POLITIKU A MUSIA BYŤ SCHOPNÉ VYNÚTIŤ JEJ DODRŽIAVANIE ZO STRANY ZAMESTNANCOV."

Dobrý príklad, keď je nevyhnutné vynútiť využívanie bezpečnostného mechanizmu, je šifrovanie údajov v mobilných zariadeniach, pretože tie sú spojené so zvýšeným rizikom zneužitia, či už neúmyselného pri strate alebo krádeži, alebo úmyselného zneužitia zo strany zamestnanca, ktorý takéto zariadenie, presnejšie jeho možnosť prístupu k podnikovým údajom využije na vynášanie citlivých informácií z firmy. Preto systém MDM (Mobile Device Management) musí vynútiť implementáciu a dodržiavanie bezpečnostných zásad. Predovšetkým ochranu údajov, ktoré sa v zariadení nachádzajú, a takisto používanie bezpečného prístupu do firemnej siete prostredníctvom technológie VPN, teda virtuálnych privátnych sietí. Rovnako treba kontrolovať aktuálnosť bezpečnostných záplat a zabrániť inštalovaniu nepovolených aplikácií. Ani jedno zo spomínaných opatrení však nezabráni už spomenutému úmyselnému zneužitiu mobilného zariadenia na vynášanie citlivých informácií z firmy. Na minimalizáciu tohto rizika treba zamestnancovi poskytnúť prístup len k údajom a aplikáciám, ktoré na svoju prácu potrebuje, a vytvárať protokoly o tom, k akým údajom a systémom zamestnanci pristupujú.

■


LEGISLATÍVA

POŽIADAVKY NA OCHRANU OSOBNÝCH ÚDAJOV

V súčasnosti má v podstate každá spoločnosť zraniteľnosti, ktoré môžu byť zneužité na bezpečnostný incident. Bezpečnostné incidenty vo väčšine prípadov nie sú cielené útoky hackerov, ale často prichádzajú aj od vlastných zamestnancov (či už úmyselne, alebo neúmyselne). Ochrana osobných údajov a informačná bezpečnosť tak tvoria dôležité oblasti, pri ktorých spolupráca odborníkov v oblasti IT a práva umožní predísť rôznym rizikám (alebo ich aspoň znížiť). Hoci posúdenie vhodnosti bezpečnostných opatrení je hlavne úlohou expertov na informačnú bezpečnosť, právnici sú nevyhnutní pri posúdení dôsledkov z hľadiska platnej legislatívy.

PRIMERANÉ BEZPEČNOSTNÉ OPATRENIA

Zákonné požiadavky na informačnú bezpečnosť sú stanovené najmä v zákone o ochrane osobných údajov[1], GDPR[2], zákone o kybernetickej bezpečnosti (ďalej len „KybZ")[3], prípadne ďalších sektorových právnych predpisoch, najmä pri elektronických komunikáciách[4], platobných službách[5], poskytovateľoch zdravotnej starostlivosti alebo pri verejnej správe[6].

Článok 32 GDPR vyžaduje, aby boli prijaté primerané technické a organizačné opatrenia, no ponecháva na každého prevádzkovateľa, aby posúdil, aké sú primerané opatrenia vo vzťahu k spracúvaniu *„so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb"*.[7] Na tomto mieste treba uviesť, že GDPR ponecháva uváženie o primeranosti opatrení na samotnú spoločnosť.

KybZ stanovuje rôzne povinnosti v oblasti informačnej bezpečnosti pre prevádzkovateľov základných služieb[8] alebo poskytovateľov digitálnych služieb.[9] Poskytuje aj detailnejšiu definíciu a bezpečnostné opatrenia definuje v § 20 ods. 1 nasledovne takto:

"Bezpečnostnými opatreniami na účely tohto zákona sú úlohy, procesy, roly a technológie v organizačnej, personálnej a technickej oblasti, ktorých cieľom je zabezpečenie kybernetickej bezpečnosti počas životného cyklu sietí a informačných systémov. Bezpečnostné opatrenia realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardmi v oblasti kyber-

---

[1] § 39 zákona č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

[2] Čl. 32 nariadenia č. Európskeho parlamentu a rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov

[3] § 20 zákona 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

[4] § 64 zákona č. 351/2011 Z. z. o elektronických komunikáciách

[5] Napr. § 28c zákona č. 492/2009 Z. z. o platobných službách

[6] zákon č. 95/2019 Z. z o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov

[7] Článok 32 ods. 1 GDPR ďalej pokračuje: "...pričom uvedené opatrenia prípadne zahŕňajú aj: a) pseudonymizáciu a šifrovanie osobných údajov; b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb; c) schopnosť včas obnoviť dostupnosť osobných údajov a prístup k nim v prípade fyzického alebo technického incidentu; d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania."

netickej bezpečnosti sa prijímajú s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služby." [10]

Konkrétne bezpečnostné opatrenia závisia od rizík danej spoločnosti. Úrad na ochranu osobných údajov SR prijal katalóg opatrení vo vyhláške k zákonu o ochrane osobných údajov s názvom *Opatrenia na elimináciu rizík pre práva fyzických osôb*. Tento katalóg poskytuje príklady opatrení vhodných na zníženie rizika (napriek použitiu termínu eliminácia prijatie opatrení často neeliminuje, ale iba zníži riziko pre fyzické osoby a v rámci transakcie, samozrejme, aj riziko pre právnické osoby).[11] Národný bezpečnostný úrad ďalej vo svojej vyhláške ku KybZ konkretizuje opatrenia a ustanovuje obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.[12] Pre informačné technológie verejnej správy je relevantná takisto Vyhláška č. 179/2020 Z. z. [13]

POSTUPY RIEŠENIA BEZPEČNOSTNÝCH INCIDENTOV

Bezpečnostné incidenty sú významným rizikom pre zasiahnuté spoločnosti, ale aj pre ich zákazníkov alebo dodávateľov. Dôsledkom môžu byť pokuty od dozorných orgánov, nároky dotknutých osôb na náhradu vzniknutých škôd alebo nároky zmluvných partnerov z porušenia zmlúv. Je preto dôležité jednak zabezpečiť detekciu incidentov, ako aj identifikovanie tých incidentov, ktoré majú právny dosah.

Pokuty od dozorných orgánov udelené za porušenie ochrany osobných údajov sú síce menej časté, no patria medzi najvyššie v porovnaní so sankciami za iné porušenia GDPR. Napríklad podľa správy o stave ochrany osobných údajov za obdobie 25. máj 2019 až 31. december 2019 bola najvyššia pokuta udelená slovenským Úradom v danom období vo výške 50 000 EUR práve za porušenie bezpečnosti spracúvania osobných údajov. [14] No pokuty udelené v súvislosti s nedostatočnou bezpečnosťou môžu byť aj oveľa vyššie[15] a môže dôjsť takisto k súbehu sankcií za porušenie ochrany osobných údajov a KybZ v rámci toho istého bezpečnostného incidentu.

Hoci bezpečnostné incidenty môžu viesť k vysokým škodám, nie každý incident treba považovať za významné riziko. Zo štatistík možno vyčítať, že dozorné orgány udeľujú pokutu len v malej časti notifikovaných bezpečnostných incidentov. Navyše iba menšina incidentov, ktoré spoločnosti identifikujú, musí byť notifikované podľa GDPR.

Článok 33 GDPR vyžaduje notifikáciu dozorných orgánov do 72 hodín po tom, čo sa prevádzkovateľ dozvedel o porušení, s výnimkou prípadov, keď nie je pravdepodobné, že incident povedie k riziku pre práva a slobody fyzických osôb. Oznámiť incident dotknutým osobám je potrebné bez zbytočného odkladu v prípade porušenia ochrany osobných údajov, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb. Z uvedeného vyplýva, že pokiaľ nie je pravdepodobné, že incident povedie k riziku pre fyzické osoby, netreba ho oznamovať. V praxi možno vidieť, že skutočne nie každé porušenie má uvedené právne dôsledky.

LUKÁŠ AUGUSTÍN MRÁZIK, Kinstellar, s.r.o.

---

[8] Zoznam prevádzkovateľov základnej služby je dostupný na: *https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/prevadzkovatelia-ZS.htm*

[9] Register poskytovateľov digitálnych služieb je dostupný na: *https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/poskytovatelia-DS.htm*

[10] § 20 ods. 1 KybZ ďalej pokračuje: Bezpečnostné opatrenia sú všeobecné, realizované v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti pre všetky siete a informačné systémy a sektorové, ktoré sa realizujú na základe špecifík kategorizácie sietí a informačných systémov ústredného orgánu v rozsahu svojej pôsobnosti podľa prílohy č. 1 a v súlade s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti."

[11] Príloha k vyhláške Úradu na ochranu osobných údajov Slovenskej republiky č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov

[12] Vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení

[13] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

[14] Úrad na ochranu osobných údajov Slovenskej republiky. Správa o stave ochrany osobných údajov za obdobie 25. máj 2019 až 31. december 2019, 2021, s. 37, dostupné na: *https://dataprotection.gov.sk/uoou/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2019_az_31.decembra_2019.pdf*

[15] Pozri napríklad pokutu GBP 20,000,000 pre British Airways, dostupné na: *https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/*

OCHRANA OSOBNÝCH ÚDAJOV

Odpoveď na otázku, či firma spracúva osobné údaje, zjednodušuje fakt, že ak má vaša firma zákazníkov alebo zamestnancov, osobné údaje určite spracováva. Ak dôjde k incidentu, pri ktorom uniknú z firmy údaje, napríklad databáza zákazníkov, ktorá obsahuje osobné údaje, hrozí firme finančný aj nefinančný postih, pričom nefinančné dôsledky, napríklad strata reputácie a dobrého mena firmy, môžu byť pre firmu ešte nepríjemnejšie než vysoká pokuta.

GDPR

Od mája 2018 v rámci celej Európskej únie platí nové nariadenie o ochrane osobných údajov GDPR (General Data Protection Regulation – všeobecné nariadenie o ochrane údajov). Cieľom nariadenia je zjednotiť právnu úroveň ochrany osobných údajov vo všetkých členských štátoch.

GDPR je založené na princípe „protection by design". V praxi to znamená, že správcovia osobných údajov sú povinní prijať primerané technické opatrenia na ochranu nimi spravovaných osobných údajov. Nie je to však len o dostatočne zabezpečených projektoch informačných systémov, ale pojem spravovanie sa v GDPR chápe ako priebežný, to znamená, že správcovia majú povinnosť dokladovať, že účinnosť prijatých opatrení na ochranu osobných údajov bola priebežne preverovaná a že tieto opatrenia boli v prípade potreby priebežne aktualizované.

Ochrana údajov fyzických osôb sa vzťahuje na spracúvanie osobných údajov automatizovanými prostriedkami, ako aj na manuálne spracúvanie, ak sú osobné údaje uložené v informačnom systéme alebo do neho majú byť uložené. Ochrana by mala byť technologicky neutrálna, inak povedané, nemala by závisieť od použitých technologických riešení.

PRÁVNE ZÁKLADY NA SPRACÚVANIE OSOBNÝCH ÚDAJOV

Jedna z hlavných zásad týkajúcich sa spracúvania osobných údajov je zákonnosť, čiže spracúvanie musí mať určitý právny základ a nie vždy je nevyhnutný súhlas

dotknutej osoby. Napríklad zamestnávateľ spracúva väčšinu osobných údajov, aby mohol plniť svoje zákonné povinnosti, napríklad odvádzať za zamestnanca dane a odvody. Ak vyžaduje údaje, ktoré sú nad rámec zákonných povinností, vtedy si už musí vyžiadať súhlas zamestnanca. Druhý právny základ je teda súhlas dotknutej osoby. Tretí právny základ je plnenie zmluvy. Ak teda firma alebo organizácia uzatvorí zmluvu s fyzickou osobou, ktorá na účely tejto zmluvy poskytne niektoré osobné údaje, prevádzkovateľ, v tomto prípade firma, ich spracúva preto, aby bola schopná plniť si povinnosti dohodnuté v zmluve. V tomto prípade je právnym základom na spracúvanie osobných údajov samotná zmluva a firma či živnostník, ktorí zmluvu s fyzickou osobou uzatvárajú, už nepotrebujú súhlas, aby mohli osobné údaje spracúvať. Takýchto právnych základov je šesť:

- dotknutá osoba vyjadrila súhlas so spracúvaním OÚ na jeden alebo viaceré konkrétne účely
- spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba
- spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa
- spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby
- spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi
- spracovanie je nevyhnutné na účel oprávneného záujmu prevádzkovateľa

Ak niekto potrebuje spracúvať osobné údaje, mal by si ozrejmiť, na základe ktorého dôvodu to môže robiť, a ak nenájde iný dôvod mimo súhlasu, bude musieť spracovávať osobné údaje na základe súhlasu dotknutej osoby. Praktická realizácia súhlasu môže byť napríklad zaškrtávacie políčko vo formulári na webovej stránke s informáciou o účele spracovania.

PRÁVA FYZICKÝCH OSÔB

Firmy na svoje obchodné aktivity potrebujú spracúvať a ukladať osobné údaje o svojich zamestnancoch a mnohé aj o zákazníkoch. S tým súvisí aj nutnosť dodržiavania ich práv, čo sa týka osobných údajov. Pripomenieme kľúčové zásady:

- Možno spracovávať len tie osobné údaje fyzickej osoby, ktoré sú nevyhnutné na konkrétny účel.
- Fyzická osoba má právo na prenos jej osobných údajov od jedného správcu osobných údajov k druhému. Preto je pôvodný správca povinný bezplatne poskytnúť fyzickej osobe jej osobné údaje, ktoré od nej získal, a to v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte.
- Fyzická osoba má právo „byť zabudnutá", čiže môže požiadať správcu osobných údajov o vymazanie osobných údajov, ktoré mu v minulosti poskytla.
- Súhlas fyzických osôb so spracovaním ich osobných údajov bude musieť byť formulovaný jednoznačne a zrozumiteľne. V prípade online služieb budú môcť dať súhlas so spracovaním osobných údajov dieťaťa mladšieho než 16 rokov len jeho zákonní zástupcovia.

Právo na vymazanie, samozrejme, nie je absolútne právo fyzickej osoby. Nevzťahuje sa napríklad na situácie, keď spracovanie a zálohovanie dát požaduje legislatívny predpis. Typický príklad sú osobné údaje o zamestnancoch. V rámci implementácie politík na manipuláciu s osobnými údajmi a ich uschovávanie sa odporúča rozdeliť osobné údaje na tie, ktoré je firma povinná spracovávať a uchovávať, od ostatných – voliteľných. Napríklad zoznam poskytnutého náradia určite nie je vhodné uchovávať v databáze, kde je adresa, prípadne číslo účtu pre potreby mzdovej učtárne.

POVINNOSŤ OHLÁSENIA INCIDENTU

Prevádzkovateľ by mal preto ihneď, ako sa dozvie, že došlo k porušeniu ochrany osobných údajov, bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín od okamihu, ako sa dozvedel, že došlo k porušeniu ochrany osobných údajov, toto porušenie oznámiť dozornému orgánu s výnimkou prípadov, keď vie prevádzkovateľ v súlade so zásadou zodpovednosti preukázať, že nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb.

OHLASOVACIA POVINNOSŤ V RÁMCI GDPR

Citujeme z nariadenia GDPR. Článok 33, ktorý sa týka oznámenia porušenia ochrany osobných údajov dozornému orgánu, presne definuje, čo ste povinní urobiť: „V prípade porušenia ochrany osobných údajov prevádzkovateľ bez zbytočného odkladu a podľa možnosti najneskôr do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel, oznámi porušenie ochrany osobných údajov dozornému orgánu príslušnému podľa článku 55...“ a príslušný orgán to bude v rámci legislatívnych rámcov riešiť, najčastejšie pokutou, ktorej výška bude závisieť od závažnosti incidentu.

Asi ste si všimli, že sme citáciu článku 33 nariadenia GDPR prerušili tromi bodkami. Znenie článku ďalej pokračuje takto: „...s výnimkou prípadov, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva a slobody fyzických osôb“.

V praxi to znamená, že ak máte údaje na diskoch chránené šifrovaním, pričom ste na šifrovanie použili renomované riešenie, ktoré využíva silné algoritmy a šifrovacie kľúče, je takmer isté, že sa k zašifrovaným údajom nik nedostane. Konkrétnejšie je v článku 34 GDPR podchytená situácia, kedy je a kedy nie je potrebné oznámiť porušenie ochrany osobných údajov dotknutej osobe: „Oznámenie dotknutej osobe uvedené v odseku 1 sa nevyžaduje, ak je splnená ktorákoľvek z týchto podmienok: prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a tieto opatrenia uplatnil na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä tie opatrenia, na základe ktorých sú osobné údaje nečitateľné pre všetky osoby, ktoré nie sú oprávnené mať k nim prístup, ako je napríklad šifrovanie.“

AUDIT A PROJEKT

Aby ste mohli osobné údaje účinne a v súlade s GDPR chrániť, musíte mať v prvom rade o nich prehľad. Relačné lokálne, prípadne cloudové databázy, proprietárne dokumenty či tabuľky Excelu na lokálnych počítačoch... Hlavne vo väčších firmách bude problém s heterogénnou štruktúrou údajov uložených v rôznych systémoch. Takže začať treba procesom, ktorý sa už po tisícročia osvedčil ako „spytovanie svedomia“ a po novom sa nazýva audit, aj keď v tomto prípade by bol výstižnejší pojem inventarizácia osobných údajov. Každá firma bez ohľadu na veľkosť a poriadok či chaos vo svojich štruktúrovaných či heterogénnych úložných riešeniach by mala byť schopná odpovedať na niekoľko jednoduchých otázok.

Aké údaje o osobách (zamestnancoch, členoch, zákazníkoch...) zbiera, skladuje a vlastní,

- nakoľko sú tieto údaje citlivé,
- kde sú osobné údaje fyzicky uložené,
- kto k nim má prístup a prečo,
- aké sú dátové toky vnútri firmy či organizácie,
- komu sa osobné údaje poskytujú a prečo.

Bez odpovedí na tieto základné otázky nemožno dosiahnuť súlad s GDPR.

V „jednočlovekových“ alebo rodinných firmách spravidla získanie odpovedí na tieto otázky nebude problém, poverený pracovník ich môže dohľadať aj manuálne, no počnúc malými firmami si takéto manuálne prehľadávanie vyžiada väčšie úsilie. Výsledkom takéhoto auditu je prehľad, ktorý dokumenty roztriedi nielen podľa miesta a spôsobu uloženia, ale navyše dokáže identifikovať osobné údaje a kategorizovať ich, teda odlíšiť údaje, ktoré nariadenie považuje za citlivé.

Analýza rizík by mala s výhodou využiť informácie o vyriešených incidentoch z minulosti, prípadne o incidentoch alebo rizikových faktoroch, ktoré na údaje aktuálne pôsobia. V mnohých prípadoch odhalíte posielanie citlivých údajov na súkromné e-maily, prípadne využívanie nezašifrovaných médií na prenos dokumentov, napríklad USB diskov či kľúčov. Odporúčame zamyslieť sa nielen nad triviálnym kritériom, čiže akú vysokú pokutu by ste podľa GDPR za súčasný stav zaplatili, ale aké dôsledky by pre vašu firmu mal prípadný incident, napríklad odcudzenie a následné zneužitie databázy zákazníkov. Aké by boli ekonomické straty a či vôbec dokážete vyčísliť s tým spojenú stratu reputácie firmy.

Výsledky auditu vám ukážu priority v zabezpečení údajov, na ktoré by sa firma mala zamerať. Ďalším krokom bude návrh opatrení vo forme projektu.

ĽUBOSLAV LACKO, NEXTECH

ROZHOVOR: **Ing. Jozef Priesol, PhD.,** bezpečnostný manažér a DPO, Slovanet, a. s.

POVINNOSTI A ZODPOVEDNOSTI V OBLASTI LEGISLATÍVY A MANAŽMENTU KYBERNETICKEJ BEZPEČNOSTI

Dnešná doba prináša značnú mieru digitalizácie a vplyvu digitálnych technológií. Závažné bezpečnostné incidenty, ktoré spôsobujú čoraz sofistikovanejšie a frekventovanejšie kybernetické útoky, sú na vzostupe. Je zrejmé, že uvedený trend bude v budúcnosti pokračovať, keďže sa očakáva, že do roku 2024 bude na celom svete na internet vecí napojených 22,3 miliardy zariadení. V roku 2018 vstúpil do účinnosti zákon o kybernetickej bezpečnosti. Na túto tému sme sa rozprávali s **Ing. Jozefom Priesolom, PhD.**, bezpečnostným manažérom a DPO v spoločnosti Slovanet, a. s.

Čo nové vám priniesli legislatívne zmeny v oblasti kybernetickej bezpečnosti?

Jozef Priesol: Kybernetická bezpečnosť je pre nás, ako prevádzkovateľa základnej služby a poskytovateľa digitálnej služby, jedna z kľúčových oblastí, ktorej sa intenzívne venujeme. Tak z pohľadu organizačného, procesného, ako aj technologického. Pre nás, ako telekomunikačného operátora, je samozrejmosť plniť všetky legislatívne povinnosti a robíme ešte viac. Napríklad spomeniem certifikáciu ISO/IEC 27018. Zefektívnili sme množstvo procesov, musíme správne reagovať na hrozby, dôsledne analyzovať a minimalizovať bezpečnostné riziká. Takisto sme nastavili systém identifikácie, riadenia a notifikovania bezpečnostných incidentov.

Spomínate legislatívu, čo je jej cieľom?

Jozef Priesol: V oblasti kybernetickej bezpečnosti je cieľom zabezpečiť ochranu informačných systémov a sietí pred narušením. Môžeme to vnímať v dvoch rovinách. To, čo firma robí proaktívne v tejto oblasti dlhodobo a čo musí robiť, lebo to vyžadujú právne predpisy. Jednotlivé kritériá vychádzajú z viacerých všeobecne záväzných právnych predpisov. Na prvom mieste je to zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti. Identifikačné kritériá pre jednotlivé kategórie závažných kybernetických incidentov a podrobnosti ich hlásenia upravuje vyhláška č. 165/2018 Z. z. Základnú službu a jej identifikačné kritériá upravuje vyhláška č. 164/2018 Z. z. Dôležitá oblasť je rozsah bezpečnostných opatrení, štruktúra bezpečnostnej dokumentácie, ktorú upravuje vyhláška č. 362/2018 Z. z. Audit kybernetickej bezpečnosti upravuje vyhláška č. 436/2019 Z. z.

Ako viem, či som prevádzkovateľ základnej služby?

Jozef Priesol: Zjednodušene je PZS orgán verejnej moci alebo subjekt, ktorý poskytuje aspoň jednu základnú službu uvedenú v zozname základných služieb, ktorý vedie Národný bezpečnostný úrad. Patrí sem napr. poskytovanie bankových produktov, systému doménových mien na internete, poštových služieb.

Ktoré základné kroky zabezpečia súlad s legislatívou v oblasti kybernetickej bezpečnosti?

Jozef Priesol: V prípade, ak vás úrad z vlastného rozhodnutia nezaradí medzi PZS a došlo k identifikovaniu kritérií a ich rozsahu, prvé je oznámenie prekročenia identifikačných kritérií na NBÚ. Tým bola služba zaradená do zoznamu základných služieb a prevádzkovateľ do registra prevádzkovateľov základných služieb. Do dvoch rokov od účinnosti zákona bolo potrebné prijať opatrenia, keďže doba uplynula, terajšie subjekty tak musia urobiť do šiestich mesiacov. Realizácia opatrení by mala vychádzať z analýzy rizík vo vzťahu k prevádzkovanej službe. U každého PZS môže byť situácia iná. Najdôležitejšia je komunikácia s NBÚ, fáza analýzy a implementácia a odstránenie nesúladov, ak sa identifikovali. Povinnosťou je vykonanie zákonného auditu, ktorého správa sa postúpi v predpísanej lehote na NBÚ.

Na čo by sa nemalo zabudnúť pri implementácii a zladení s právnymi predpismi?

Jozef Priesol: Ako som spomínal, komunikovať s NBÚ pred registráciou a vždy v prípade závažných kybernetických incidentov. Fázu implementácie a zladenia odporúčam riadiť projektovo. Jej nosné časti sú: identifikácia, inventarizácia, klasifikácia a kategorizácia aktív, analýza a komplexný manažment rizík, analýza obchodných procesov a dosahov (BCM, BIA, MTPD, RTO, RPO), bezpečnostná dokumentácia, úprava zmluvných vzťahov a v neposlednom rade realizácia bezpečnostných technických opatrení. Dôležité je brať veci zodpovedne. Ak si nevieme poradiť, je tu možnosť osloviť špecialistov.

SLOVANET

O RIZIKÁCH ÚNIKU DÁT AJ LEGISLATÍVE

Čoraz častejšie sa stretávame s reálnymi prípadmi, keď dochádza k úniku citlivých dát a útočník následne žiada vysoké výkupné, prípadne poškodením dát vyradí organizáciu z prevádzky. Takmer 50 % Slovákov si aj napriek tomu myslí, že sú v bezpečí.

ČO JE TO KYBERNETICKÁ BEZPEČNOSŤ

Národný bezpečnostný úrad (NBÚ) opisuje kybernetickú bezpečnosť ako proces zahŕňajúci procesy, postupy, technologické a personálne zabezpečenie ochrany systémov, sietí a zariadení pred hrozbami v kybernetickom priestore. Je to aj stav pripravenosti na odhaľovanie útokov, riešenie kybernetických bezpečnostných incidentov a minimalizáciu následkov po incidente. Cieľom kybernetickej bezpečnosti je udržať dáta, informácie, systémy a zariadenia v bezpečí pred možnými únikmi, krádežou, znehodnotením či iným výpadkom.

TÝKA SA NÁS KYBERNETICKÁ BEZPEČNOSŤ?

Potreba hovoriť o hrozbách v digitálnom priestore vyplýva predovšetkým z obrovského nezáujmu verejnosti o túto tému. V nedávnom prieskume spoločnosti Alison Slovakia uvádza takmer 50 % slovenskej populácie využívajúcej internet a digitálne komunikačné prostriedky, že kybernetická bezpečnosť sa ich netýka.

Kybernetický priestor nemá hranice a deje sa v ňom veľká časť osobného i pracovného života každého z nás. Neriešenie prípadných hrozieb a zraniteľností môže mať vážny dosah. Spoločnosti nemajú dostatok odborného personálu, často sa stretávame aj s podceňovaním témy kybernetickej bezpečnosti a požiadaviek vyplývajúcich z legislatívy. Keď k tomu prirátame ešte nízke povedomie o bezpečnosti, vzniká obrovský problém.

SPOLOČNOSTI HROZBÁM A ÚNIKU DÁT NEVENUJÚ DOSTATOČNÚ POZORNOSŤ

Väčšina firiem, ktorých obchodná činnosť nie je primárne zameraná na IT sféru, má pomerne zložitú situáciu a je pre ne náročné sledovať legislatívu a súčasné trendy v kybernetickej bezpečnosti v takej miere, ako si to dnešná digitálna doba vyžaduje.

Spoločnosti zároveň nevynakladajú na IT vybavenie dostatok prostriedkov a ich systémy sú prevádzkované na zastaraných a neaktualizovaných zariadeniach. V minulosti na ochranu firemnej IT infraštruktúry možno stačilo zabezpečiť vnútornú sieť firewallom a na všetky koncové zariadenia nainštalovať antivírus. Toto však dnes už neplatí, firmy prechádzajú na moderné aplikácie a cloudové riešenia umožňujúce pracovať odkiaľkoľvek.

PANDÉMIA PRINIESLA ZÁSADNÚ ZMENU

Uplynulý rok v znamení pandémie priniesol mnohým firmám jednu z najzásadnejších výziev a zmien oproti minulosti, ktoré spoločnosti boli nútené realizovať v rekordne krátkom čase. S tým úzko súvisí aj presun zamestnancov do domáceho prostredia a práca formou home office. Na základe legislatívnych nariadení a pokynov pandemickej komisie sa zo dňa na deň práca z domu stala núteným štandardom, aby zamestnanci mohli vôbec pracovať. Reálny stav ukázal, že firmy a inštitúcie neboli na takúto situáciu pripravené a jedinou cestou boli núdzové, kritické riešenia, často aj za cenu nižšej IT bezpečnosti.

LEGISLATÍVA PRINÁŠA NOVÉ PRÁVOMOCI PRE NBÚ

V súčasnosti sú organizácie nútené venovať sa oblasti bezpečnosti oveľa viac – tlačí na ne zvyšujúca sa digitalizácia, prinášajúca vyššie riziko potenciálnych útokov, ale aj nová legislatíva. Európska únia a jednotlivé krajiny sprísňujú a zavádzajú nové legislatívne normy najmä z dôvodu ochrany údajov svojich občanov. V Slovenskej republike vstúpili v roku 2018 do platnosti dva zákony upravujúce základné práva a povinnosti pre ochranu informačných aktív a práv klientov a subjektov. Sú nimi zákon o kybernetickej bezpečnosti č. 69/2018 Z. z. a zákon o informačných technológiách vo verejnej správe č. 95/2019 Z. z. Okrem spomenutých nesmieme zabudnúť ani na najdôležitejšie citlivé dáta – osobné údaje. Nakladanie s nimi reguluje zákon o ochrane osobných údajov č. 18/2018 Z. z., resp. nariadenie EÚ č. 2016/679, známe aj ako GDPR.

Ústredný orgán štátnej správy pre oblasť bezpečnosti je Národný bezpečnostný úrad. Pre oblasť kybernetickej bezpečnosti bol vytvorený samostatný útvar Národné centrum kybernetickej bezpečnosti SK-CERT. NBÚ prostredníctvom tohto útvaru zabezpečuje národné a strategické aktivity v oblasti riadenia kybernetickej bezpečnosti, analýzy hrozieb, ale aj koordinácie riešenia bezpečnostných incidentov na celonárodnej úrovni.

Onedlho by mala byť prijatá novela zákona o kybernetickej bezpečnosti, ktorá má značne posilniť postavenie a právomoci NBÚ v oblasti predchádzania a riešenia bezpečnostných incidentov. Na základe tejto novely by NBÚ v budúcnosti mohol reagovať na existujúce hrozby a všetky škodlivé aktivity či škodlivý obsah zablokovať.

NAJČASTEJŠIE TYPY ÚTOKOV

- **DDoS** je jeden z najstarších typov útoku, zameraný na znefunkčnenie verejne dostupných služieb či internetových stránok. Priebeh útoku je pomerne jednoduchý, server, kde beží služba, je vystavený obrovskému počtu požiadaviek, čím dochádza k jeho preťaženiu, zrúteniu a následnej nedostupnosti služieb. Príkladom môže byť odstavenie stránok napr. počas volieb alebo aj nedávne problémy NCZI, keď pri snahe množstva občanov, ktorí sa chceli prihlásiť na očkovanie, došlo k zlyhaniu prevádzkovanej služby, a teda k jej nedostupnosti. V tomto prípade nemuselo ísť nevyhnutne o cielený útok, ale je takmer dokonalým príkladom toho, ako útoky DDoS prebiehajú.
- **Phishing** je typ útoku, keď sa útočník snaží získať citlivé údaje priamo od používateľa prostredníctvom dôveryhodne pôsobiacej nástrahy. Vo väčšine prípadov ide o falošné e-maily, SMS správy, telefonáty, falošné webové stránky alebo príspevky na sociálnych sieťach vydávajúce sa za reálne existujúce služby. Obeť tak odovzdá útočníkovi svoje citlivé údaje v mylnej domnienke, že ich zadáva na prihlásenie k reálnej službe. Získané dáta sú najčastejšie prihlasovacie údaje k digitálnym službám a údaje o platobných kartách.
- **Ransomvér** je druh škodlivého softvéru, ktorý po preniknutí do počítača zašifruje a uzamkne dáta nachádzajúce sa v zariadení, prípadne v sieti, kde sa zariadenie nachádza. Za opätovné sprístupnenie dát útočníci požadujú zaplatenie výkupného, najčastejšie prostredníctvom kryptomien, aby útočníka nebolo možné vystopovať. Pomerne nový postup je tzv. dvojité vydieranie, keď je ransomvérový útok kombinovaný s krádežou citlivých dát.

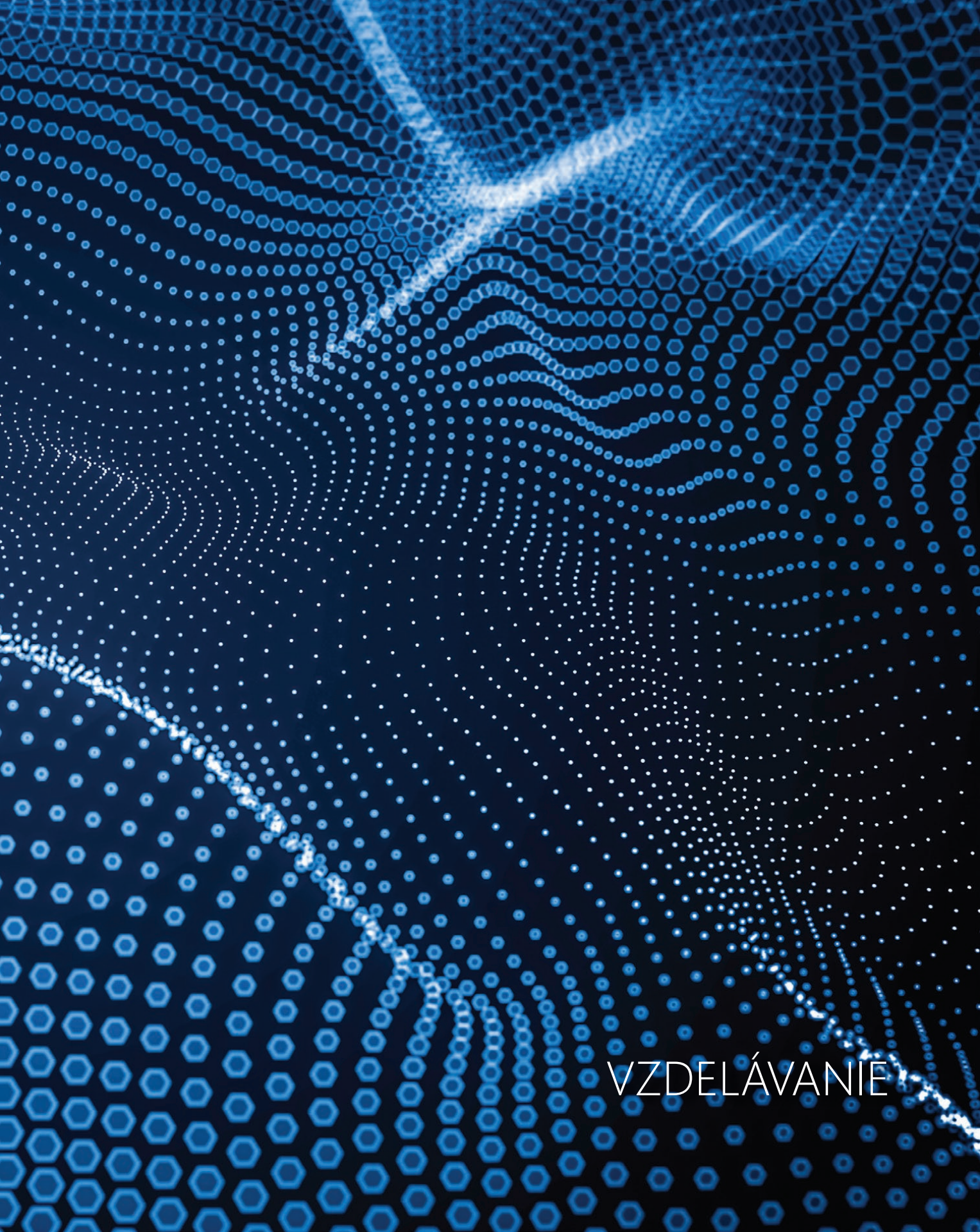
Podľa správy NBÚ o kybernetickej bezpečnosti na Slovensku za rok 2020 budú práve ransomvérové útoky v najbližších rokoch predstavovať jednu z najväčších kybernetických hrozieb nielen pre obchodné spoločnosti a organizácie, ale aj pre individuálne osoby.

TREND NA TRHU JE VYUŽITIE EXTERNÝCH EXPERTOV A RIEŠENIA „AS A SERVICE"

Pandémia a presun procesov do online prostredia zvýšili dôležitosť celej IT infraštruktúry v jednotlivých spoločnostiach. Otázka digitalizácie služieb a interných procesov vo firmách tak dostáva výrazne vyššiu prioritu, než to bolo v minulosti. Organizáciám však chýba know-how, technické vybavenie, ale aj interní experti na digitálnu bezpečnosť.

Mnoho spoločností preto siaha po praktickom riešení a využívajú služby „as a service", čo znamená delegovanie starostlivosti o IT bezpečnosť na expertov externých spoločností. Výhodná je úspora financií, kapacít, času a vedomie, že kybernetická bezpečnosť je plne v rukách skúsených odborníkov, ktorí vás od tejto povinnosti odbremenia a využijú na to tie najlepšie technológie. Nemusíte riešiť, aké technológie bude potrebné aplikovať, nemusíte investovať do vlastného bezpečnostného technika. Jednoducho zveríte ochranu svojho IT do rúk špecialistom, ktorí disponujú know-how, skúsenosťami a dokážu sledovať zmeny v legislatíve a vo vývoji témy kyberbezpečnosti v rámci globálneho aj domáceho trhu.

RENÉ PAVLO, bezpečnostný expert, DATALAN



VZDELÁVANIE

PREČO JE VZDELÁVANIE V IT DÔLEŽITÉ?

Iste sa zhodneme, že vzdelávanie je vo všeobecnosti dôležitá činnosť. V prípade vzdelávania v IT je to ešte dôležitejšie, keďže ide o dynamickú oblasť, ktorá sa neustále rozvíja a mení. Aj vzhľadom na túto skutočnosť sa dá povedať, že neexistuje sektor, v ktorom by vzdelávanie nebolo potrebné, a teda vzťahuje sa aj na malé spoločnosti.

Práve malé a stredné spoločnosti by mali venovať pozornosť vzdelávaniu v oblasti IT, najmä v oblasti kybernetickej bezpečnosti. Prečo? Pretože veľké spoločnosti majú túto oblasť vo väčšine prípadov riešenú komplexne a vo väčšej miere. Budujú špecializované oddelenia, ktorých úlohou je dohľad nad kybernetickou bezpečnosťou, a využívajú rôzne technológie, ktoré pomáhajú v boji proti hrozbám z IT sveta. V porovnaní s malými spoločnosťami majú teda viac prostriedkov a možností, ako sa brániť. A pritom v oboch prípadoch platí, že aj veľké, aj malé spoločnosti čelia takmer rovnakým hrozbám.

Boj s kybernetickými hrozbami je nikdy nekončiaci príbeh. Nič také ako stopercentná bezpečnosť nie je. Neexistuje žiadna technológia, žiadne riešenie, ktoré by nás dokázalo úplne ochrániť pred týmito hrozbami, nielen pred tými súčasnými, ale už vôbec nie pred tými, ktoré prídu v budúcnosti. Ak teda nevieme odstrániť riziká, môžeme sa aspoň brániť a znižovať pravdepodobnosť toho, že sa staneme obeťou takéhoto rizika. Možno to dosiahnuť kombináciou opatrení, technických, metodických a personálnych. Technické opatrenia sú v podstate rôzne technológie, ktoré nám pomáhajú v tomto úsilí, ako napríklad antivírus. Metodické opatrenia sú predpisy a postupy, ktoré opisujú prácu s prostriedkami IT v rámci spoločnosti a ktoré by mali opisovať aj zásady bezpečného používania týchto prostriedkov.

Posledným článkom tohto reťazca sú ľudia. Prečo práve ľudia? Odpoveď je celkom jednoduchá. Práve človek je totiž jedno z tých rizík, na ktoré musíme pamätať. Ľudia sú tí, ktorí využívajú IT prostriedky zamestnávateľa. Tí, ktorí otvárajú elektronickú poštu a ktorí navštevujú rôzne stránky na internete. Každá z týchto aktivít v sebe nesie bezpečnostné riziko. Dokonca v niektorých prípadoch je jednoduchšie „zneužiť zraniteľnosť" u človeka ako sa snažiť nabúrať do systému pomocou technických prostriedkov. Tomuto spôsobu sa hovorí sociálne inžinierstvo. Môžeme mať špičkovú technológiu, perfektné postupy, ale vždy tam bude človek, ktorý nám to môže celé zrútiť ako domček z kariet. Či už z neznalosti, alebo úmyselne. Je preto dôležité investovať čas a peniaze do zvyšovania bezpečnostného povedomia, aby sme dokázali znížiť aj toto riziko.

Cieľom každej spoločnosti je chrániť svoje aktíva a svoje investície. Toto sa dá dosiahnuť aj znižovaním kybernetického rizika tak, ako sme opísali v predošlej časti. Treba si uvedomiť hodnotu jednotlivých aktív a takisto následky, ktoré prináša ich znehodnotenie. Na druhej

strane pomyselných váh stoja investície do bezpečnostných technológií a do zvyšovania bezpečnostného povedomia zamestnancov. Je takmer isté, že tá hodnota bude vyššia na strane aktív. A nie sú to len hmatateľné aktíva, ktoré sa dajú vyjadriť finančnou hodnotou. Existujú aj škody spôsobené kybernetickým útokom, ktoré sú nefinančné, ale dôsledky bývajú katastrofálne. V tomto prípade hovoríme napríklad o reputačnom, strategickom alebo právnom riziku. Čo to znamená v praxi? Môžeme si to ukázať na príklade. Máme finančnú inštitúciu, ktorá bola obeťou kybernetického útoku, počas ktorého unikli informácie o klientoch, ich osobné a finančné údaje. Z pohľadu priamych škôd tento útok nebol príliš „škodlivý", dáta boli obnovené zo zálohy a chod tejto inštitúcie z pohľadu IT prevádzky bol krátko po útoku opäť v bežnom režime. Väčší problém bol práve únik informácií, ktoré sa dostali ku konkurencii, boli voľne dostupné na internete, ktokoľvek si ich mohol pozrieť a vyhľadať v nich to, čo ho zaujímalo, o osobách, ktoré ho zaujímali. Bolo len otázkou času, kedy si situáciu všimnú médiá. Pár článkov v novinách, reportáž vo večernom spravodajstve, pár nahnevaných ľudí na sociálnych sieťach. Aký bol výsledok? Strata dôvery u klientov, existujúcich, ale aj potenciálnych, žaloby, pokuta v zmysle GDPR (ochrana osobných údajov), strata reputácie veľkého rozsahu. Tento príklad sa môže zdať nafúknutý a pritiahnutý za vlasy, pre niekoho možno ďaleko od reality. Žiaľ, takýchto príbehov je veľa, často aj s fatálnym koncom. A teraz čerešnička na torte: tento scenár, ktorý sme opísali, môže byť jedného dňa aj vaším príbehom. Zrejme to nie je príjemná predstava. Vôbec pritom nemusí ísť o finančnú spoločnosť, pokojne to môže byť napríklad advokátska kancelária (dáta o klientoch, často citlivého charakteru, osobné údaje), zdravotnícka ambulancia (informácie o pacientoch, ich chorobách, liečbe, závislostiach), obecný úrad (detailné informácie o občanoch, občianskych konaniach, finančné informácie), ale napríklad aj malá pekáreň (informácie o klientoch, dodávateľských zmluvách a cenách, recepty a postupy výroby). Tu už možno viacerí z vás spozorneli, pretože sa v týchto spoločnostiach našli, prípadne si uvedomili reálnosť tejto hrozby.

Našťastie pravdepodobnosť takejto situácie sa dá znížiť. V prvom rade si treba uvedomiť reálnosť kybernetických rizík a hrozieb. Nie, riziko a hrozba nie je to isté. Pojem informačné bezpečnostné riziko sa zmieňuje o škode, ktorú by mohlo spôsobiť porušenie alebo útok na systém informačných technológií (IT). Riziko je viac koncepčný pojem – niečo, čo sa môže alebo nemusí stať, zatiaľ čo hrozba je konkrétna - skutočné nebezpečenstvo. Riziko je každá primerane rozpoznateľná okolnosť alebo udalosť, ktorá môže mať nepriaznivý vplyv na bezpečnosť. Informačná bezpečnosť je udržiavanie akceptovateľnej miery identifikovaného rizika, ktoré pôsobí na aktíva procesmi a činnosťami zameranými na odvrátenie alebo zmenšenie rizík a prejavov hrozieb. Chcete príklad? Keď prechádzate cez rušnú ulicu, riskujete, že vás zrazí auto. Riziko môžete zmierniť, ak ste sa uistili, že cesta je voľná, skôr, ako prejdete. Hrozba nastane, ak sa blíži auto a hrozí, že do vás narazí. Platí, že hrozby sa ťažšie kontrolujú.

Čo s tým teda vieme urobiť? Odložme trošku bokom technické prostriedky a metodiku, aj keď tvoria dôležitú a neoddeliteľnú časť riadenia kybernetickej bezpečnosti. Zamerajme sa viac na už spomenutý najrizikovejší faktor – ľudí. Základná požiadavka je, aby ľudia mali informácie nielen o metodike a postupoch, ale aj všeobecný prehľad o tom, s akými nástrahami sa môžu pri používaní informačnej techniky (sem patria napríklad aj mobilné telefóny) stretnúť, ako ich vedieť rozpoznať a ako sa proti nim účinne brániť. Toto je základ, na ktorom sa dá ďalej stavať a ktorý by mal byť tým informačným a vzdelanostným minimom každého zamestnanca. Len dostatočne vzdelaný zamestnanec znamená nižšie riziko pre aktíva spoločnosti, takisto znamená vyššiu odolnosť proti kybernetickým útokom. A nie sú to len aktíva, stačí si spomenúť na nefinančné riziká a ich následky.

Dôležitosť vzdelávania v IT je teda zrejmá. Aby malo efekt a zmysel, treba k nemu pristupovať systematicky a koncepčne. Len tak možno dosiahnuť lepšiu pripravenosť na ochranu aktív v rámci spoločnosti. A nielen ochranu aktív, ale aj ochranu zamestnancov. Závažné bezpečnostné incidenty môžu mať v niektorých prípadoch dohru v réžii orgánov činných v trestnom konaní, čo je situácia, v ktorej sa nechce vidieť ani zamestnávateľ, ani zamestnanec. V tomto prípade platí známy výrok, že neznalosť neospravedlňuje.

QUBIT

ŠKOLENIE ZAMESTNANCOV

Vždy platilo a aj naďalej platí, že ľudia sú najslabším článkom pomyselnej reťaze zabezpečenia IT infraštruktúry. Firmy používajú na identifikáciu IT zraniteľností sofistikované technologické metódy, ako napríklad služby monitorujúce hrozby či penetračné testy. Zanedbávajú však odbornú prípravu svojich pracovníkov v oblasti bezpečnosti informačných technológií. Takzvané sociálne inžinierstvo čiže manipulácia ľudí je pritom už dlho štandardná zbraň v každom arzenáli počítačových zločincov.

BEZPEČNOSTNÉ ŠKOLENIA

Podobne ako priebežné vzdelávanie zamestnancov v iných oblastiach aj bezpečnostné školenia sa realizujú buď prezenčnou formou, teda účasťou na prednáškach či seminároch, alebo formou e-learningu.

Cieľom pravidelných školení zainteresovaných zamestnancov ohľadne zabezpečenia informačných systémov a ostatných zamestnancov o ich bezpečnom používaní je budovanie bezpečnostného povedomia, zníženie počtu incidentov, ochrana informačných aktív a minimalizácia prípadných strát. Zamestnanci sa na školení oboznamujú s internými predpismi, ktoré sú povinní dodržiavať, naučia sa, akých činností sa majú vystíhať, a aj to, aké by to mohlo mať následky. Takisto sa naučia osvedčené postupy nielen pri vykonávaní rutinných úloh, ale aj v rôznych neobvyklých situáciách.

ŠKOLENIA FORMOU E-LEARNINGU

Táto metóda školenia umožňuje zamestnancom individuálnu formu vzdelávania. Môže sa realizovať synchrónne alebo asynchrónne. Pri synchrónnom e-learningu sa uskutočňuje školenie viacerých zamestnancov súčasne v reálnom vopred dohodnutom čase a za aktívnej asistencie lektora. Táto forma je vhodná pre firmy s viacerými pobočkami, pretože zamestnanci ani lektor nemusia cestovať. Inak povedané, ak má pravidelné školenie trvať hodinu, zamestnanci pri ňom strávia hodinu, a nie celý deň, ako by museli, keby cestovali na prezenčné školenie z iného mesta. Výhoda asynchrónneho e-learningu je v tom, že každý zamestnanec si môže vybrať vhodný čas, v ktorom si preštuduje materiály a absolvuje test. To umožní optimálne zladiť školenie s pracovnými povinnosťami. Nevýhodné je, že školenie prebieha bez priamej prítomnosti lektora. Preto sa asynchrónny e-learning nielen pri bezpečnostných školeniach, ale vo firemnej praxi všeobecne najčastejšie využíva ako doplnková forma ku klasickým školeniam. Prípadne sa školenie uskutoční ako kombinácia prezenčnej formy pre zamestnancov, ktorí sa na ňom môžu zúčastniť, a synchrónneho e-learningu pre zamestnancov, ktorí nemôžu prísť.

CLOUDOVÝ E-LEARNING

Zatiaľ sme neriešili, že na to, aby firma mohla realizovať e-learning, potrebuje softvérové riešenie nazývané LMS (Learning Management System). Tento systém spravuje informácie o kurzoch, študijných materiáloch, generuje testy a vyhodnocuje ich, a to vrátane evidencie zamestnancov, či školenie absolvovali a aký výsledok dosiahli pri teste. Jedna z moderných alternatív je e-learning formou služby. Firma namiesto investovania do LMS a zaťažovania vlastnej serverovej infraštruktúry platí iba za aktuálne využívanie služby. Kurzy si firmy pripravia pomocou portálu cloudovej služby. Stačí krátke zaškolenie na konkrétne cloudové riešenie a pracovníci IT oddelenia môžu začať vytvárať vnútropodnikové kurzy vrátane testov a ďalších vzdelávacích aktivít.

ĽUBOSLAV LACKO, NEXTECH

CLASHING: EFEKTÍVNE VZDELÁVANIE V KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI

Zamestnanci väčšiny spoločností žijú v predstavách, že kybernetická bezpečnosť sa ich netýka, a vedenie spoločnosti predpokladá, že pred potenciálnymi útokmi alebo stratou dát ich ochránia implementované technológie.

Kybernetické útoky sú však v posledných rokoch výrazne sofistikovanejšie a častejšie. Nie je tak prekvapením, keď z prieskumov vyplýva, že práve správanie zamestnancov je najväčšou slabinou firiem z pohľadu kybernetickej a informačnej bezpečnosti.

Systematické a pravidelné budovanie bezpečnostného povedomia, vzdelávanie bežných používateľov v oblastiach kybernetickej bezpečnosti je znakom spoločností pripravených na digitálnu transformáciu. Základné znalosti zamestnancov o potenciálnych hrozbách a spôsoboch ochrany by mali byť pre vašu spoločnosť kľúčové.

„Skúsenosti z praxe s rôznymi online vzdelávacími nástrojmi nám ukázali, že zamestnanci si odovzdané informácie neosvoja, a čo je horšie, nemenia svoje správanie. V rámci interného programu inovácií sme v ANECTe rozvinuli ideu vzdelávacej platformy, ktorá ľudí vtiahne do deja. Emócie a súťaživosť vás prinútia opakovane rozmýšľať o kybernetických hrozbách a podprahovo si osvojiť dobré vzorce správania," uviedol Martin Valko, COO spoločnosti ANECT a.s.

Prinášame tak platformu Clashing, online kartovú hru, ktorá mení pohľad na firemné školenie v oblasti bezpečnosti. Ide o kartový súboj, kde kolegovia hrajú proti sebe. Jeden na pozícii Hackera, ktorý sa snaží útočiť na firmu, a druhý má v súboji rolu Zamestnanca, ktorý firmu obraňuje pred hrozbami a útokmi. Môžeme hrať aj v móde proti počítaču, ale oveľa zážitvnejšie sú priame súboje s ľuďmi, kolegami. Vzdelávanie prebieha formou krátkych kartových súbojov, štandardne 10 – 15 minút. A zamestnanci sa postupne vystriedajú v každej role aby lepšie pochopili riziká svojho správania aj z pohľadu útočníkov.

Hráči majú k dispozícii unikátne karty, ktoré obsahujú široké spektrum kybernetických útokov, hrozieb z bezpečnosti informácií či fyzických bezpečnostných útokov a reakcií na ne.

Aktuálne je k dispozícii 5 herných prostredí – Kancelária, Mimo kancelárie, Home-office, Počítač a Mobil, Internet a Sociálne siete. Celá hra je dostupná v 3 jazykových mutáciách – slovenskej, českej a anglickej.

„Aby platforma Clashing mala zmysel pre našu cieľovú skupinu spoločností, je dôležitý súlad vzdelávacieho obsahu s legislatívou, zákonom o kybernetickej bezpečnosti alebo normami, ako je ISO 27000 pre systém riadenia informačnej bezpečnosti.

A teda práve do tvorby adekvátneho obsahu a niekoľkých revízií obsahu boli zapojení naši konzultanti pre oblasť procesov, informačnej bezpečnosti," hodnotí Martin Valko zo spoločnosti ANECT a.s.

V rámci manažmentu platformy Clashing máte k dispozícii správu účtov zamestnancov s informáciami o už absolvovaných školeniach, možnosti na plánovanie vzdelávacích kampaní alebo rebríčky úspešnosti. Manažment alebo tím HR tak má rôzne možnosti, ako kreatívne nasadiť vzdelávaciu platformu, ktorú si ľudia v spoločnosti obľúbia.

Práve gamifikácia rôznych oblastí je dnes cesta, ako ľudí upútať, pravidelne podprahovo vzdelávať. My veríme, že gamifikácia témy, ako je kybernetická a informačná bezpečnosť, bude prínosom pri dosiahnutí nášho cieľa zvyšovať povedomie o téme v spoločnosti. Clashing naučí zamestnancov ochrániť firmu proti kybernetickým hrozbám a zlepší bezpečnostné návyky ľudí vo vašom tíme.

MARTIN VALKO, ANECT

VYŽADUJE VZDELÁVANIE V IT SLOVENSKÁ LEGISLATÍVA?

Legislatíva SR v oblasti kybernetickej bezpečnosti je relatívne veľmi mladá. V platnosti máme zákon o kybernetickej bezpečnosti, nariadenia, ako je napríklad GDPR, a viacero vyhlášok, ktoré sa venujú riadeniu kybernetickej bezpečnosti. Z pohľadu vzdelávania je však táto oblasť ešte stále takpovediac v plienkach. Aj napriek tomu sa veci posúvajú vpred a vzdelávanie je čoraz potrebnejšie, nevyhnutnejšie. A to nielen z pohľadu slovenskej legislatívy, ale aj na európskej úrovni.

Potreba vzdelávania v IT je dôležitá téma, ktorá je súčasťou našich pracovných, ale aj súkromných životov. Aby sme sa nepohybovali iba v teoretickej rovine, prejdime si zopár právnych a technických noriem, v ktorých sa vyskytuje požiadavka na vzdelávanie, resp. zvyšovanie bezpečnostného povedomia. Ide predovšetkým o nasledujúce:

- Všeobecné nariadenie o ochrane údajov (GDPR), resp. zákon č. 18/2018 Z. z. o ochrane osobných údajov, napr.:
  - Recitál 132: Činnosti dozorných orgánov zamerané na zvyšovanie povedomia verejnosti by mali zahŕňať špecifické opatrenia zacielené na prevádzkovateľov a sprostredkovateľov vrátane mikropodnikov a malých a stredných podnikov, ako aj na fyzické osoby, predovšetkým v kontexte vzdelávania.
  - čl. 39: Medzi úlohy zodpovednej osoby patrí: monitorovanie súladu s týmto nariadením, s ostatnými právnymi predpismi Únie alebo členského štátu týkajúcimi sa ochrany osobných údajov a s pravidlami prevádzkovateľa alebo sprostredkovateľa v súvislosti s ochranou osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy personálu, ktorý je zapojený do spracovateľských operácií, a súvisiacich auditov;
  - čl. 57: Dozorný orgán zvyšuje povedomie verejnosti a jej chápanie rizík, pravidiel, záruk a práv súvisiacich so spracúvaním. Osobitná pozornosť sa venuje činnostiam špecificky zameraným na deti;
- Zákon o kybernetickej bezpečnosti č. 69/2018 Z. z.
  - § 5 (1)w: Úrad vydáva znalostné štandardy a v spolupráci s Ministerstvom školstva, vedy, výskumu a športu Slovenskej republiky vykonáva a zabezpečuje budovanie bezpečnostného povedomia,
  - § 7 (2)f: Národná stratégia - určenie vzdelávacích programov, programov na budovanie bezpečnostného povedomia, zvyšovanie informovanosti a odbornej prípravy,
  - § 9 (1)d: Ústredný orgán buduje bezpečnostné povedomie, koordinovanú spoluprácu na všetkých stupňoch riadenia kybernetickej bezpečnosti a aplikuje bezpečnostné opatrenia a politiku správania sa v kybernetickom priestore,
- Vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení:
  - § 7 b) Personálna bezpečnosť pozostáva najmenej: zo zavedenia plánu rozvoja bezpečnostného povedomia a vzdelávania spočívajúceho v oboznámení používateľov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov s bezpečnostnými politikami a v pravidelnom zvyšovaní ich bezpečnostného povedomia počas trvania pracovnoprávneho vzťahu alebo iného obdobného pracovného alebo zmluvného vzťahu,
  - § 7 d) Personálna bezpečnosť pozostáva najmenej: z hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia zamestnancov, administrátorov, osôb zastávajúcich niektorú z bezpečnostných rolí a dodávateľov,
  - § 7h) Personálna bezpečnosť pozostáva najmenej: z vykonania poučenia o manipulácii s informáciami pre osoby, ktoré vykonávajú činnosť alebo sa oboznamujú s informáciami podľa osobitného predpisu

- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe,
- Vyhláška č. 179/202 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy:
  - Príloha 2: minimálne bezpečnostné opatrenia: Personálna bezpečnosť Kategória I:

a) Ustanoviť plán rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrebných školení, a vykonať bezpečnostné vzdelávanie na zvýšenie bezpečnostného povedomia najmenej každé tri roky.

b) Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.

c) Zamestnávateľ povinnej osoby a tretia strana zabezpečia, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.

- Zákon č. 583/2008 Z. z. o prevencii kriminality a inej protispoločenskej činnosti
- programové vyhlásenia vlády SR Stratégia prevencie kriminality a inej protispoločenskej činnosti
- ISO/IEC 27002: článok 7.2.2

Na základe uvedeného môžeme vidieť, že dokumentov, ktoré sa venujú požiadavkám na vzdelávanie, je vcelku dosť. Potreba zvyšovania vzdelávania má teda oporu aj v slovenskej legislatíve a je dôležité, aby sa požiadavky stanovené touto legislatívou vo veľkej miere plnili aj v praxi.

QUBIT

AKÉ MOŽNOSTI VZDELÁVANIA MÔŽE FIRMA VYUŽIŤ?

Základný predpoklad na vzdelávanie je podpora manažmentu. Je dôležité, aby si práve manažment uvedomoval riziká, ktoré prinášajú kybernetické hrozby, a škody, ktoré môžu takéto hrozby napáchať. Možností, ako to dosiahnuť, je niekoľko, či už z pohľadu cieľových skupín, pre ktoré je vzdelávanie určené, ako aj z pohľadu formy. Pod cieľovými skupinami si môžeme predstaviť napríklad bežných používateľov, ktorých pracovnou náplňou nie sú informačné technológie. Ďalšou skupinou môže byť napríklad tím IT odborníkov, ktorí sa starajú o prevádzku informačných technológií. Pre každú skupinu sú k dispozícii rôzne úrovne odbornosti a hĺbky podľa zvolených požiadaviek a očakávaní. Je logické, že práve obsah týchto úrovní by mal reflektovať cieľovú skupinu. Je predsa nezmysel vzdelávať napríklad administratívnych zamestnancov technickou analýzou útoku DDoS (Denial of Service) a naopak, pre IT odborníkov bude zrejme rovnakým nezmyslom hovoriť o spôsobe otvárania e-mailových príloh. Dá sa povedať, že vzdelávanie jednotlivých cieľových skupín sa bude navzájom líšiť vzhľadom na mieru pripravenosti jednotlivých skupín pochopiť podávané informácie a zároveň ich uplatniť v pracovnom, ale aj v osobnom živote.

Možností, ako to dosiahnuť, je hneď niekoľko – od samoštúdia po rôzne formy odborného vzdelávania. Pokiaľ má vzdelávanie splniť účel, treba vybrať vhodnú formu. A nielen to. Zamestnanec, ktorý sa má zúčastniť na vzdelávaní, by mal byť oboznámený s potrebami, prečo je dôležité absolvovať takéto školenie. Toto je práve úloha manažmentu, aby vhodným spôsobom vysvetlil požiadavky a ciele, ktoré dané školenie prinesie nielen pre spoločnosť, ale aj pre zamestnanca.

Často sa totiž stáva, že školenie sa pre zamestnanca stáva len akousi stratou času, prípadne to berie ako príležitosť „uliať sa" z práce. Školenie pasívne a unudene presedí. Berie to ako nutné zlo, možno ako možnosť dobre sa najesť z pripraveného občerstvenia.

Aké sú teda možnosti, z ktorých si môžeme vyberať? Tu sú niektoré z nich.

ONLINE

V poslednom čase ide o najčastejšiu formu vzdelávania. Výhodou v tomto prípade je, že účastníci nemusia opustiť pohodlie svojho domova, nikto na nich nebude ukazovať prstom, ak budú oblečení vo svojom obľúbenom domácom oblečení alebo dokonca v pyžame. Nevýhodná je však chýbajúca interakcia s prednášajúcim a pasivita, čo môže viesť k nedostatočnému pochopeniu preberanej problematiky. Medzi hlavné formy online vzdelávania môžeme zaradiť napríklad semináre, workshopy (s live prednášajúcim a možnosťou diskusie medzi prednášajúcim a účastníkmi), prípadne podcasty a videá, ktoré sú bez možnosti takejto interakcie. Obe formy majú opodstatnenie. V prípade live foriem ide o možnosť klásť otázky a pýtať sa, ak je účastníkom niečo nejasné. Pre lektora je výhodná predovšetkým možnosť s účastníkmi viesť otvorenú diskusiu. Pri neinteraktívnych formách je zase výhodou možnosť vzdelávať sa v čase, keď to účastníkovi vyhovuje. V prípade potreby si môže danú aktivitu pozrieť alebo vypočuť ešte raz.

ONSITE

Onsite školenie je typ vzdelávania prezenčnou formou. Je presne určený čas a miesto, kde takéto vzdelávanie bude prebiehať. Tento typ vzdelávania prináša okrem samotných informácií z pohľadu preberanej témy aj možnosť väčšej interakcie nielen s prednášajúcim, ale aj s ostatnými účastníkmi. Pridanou hodnotou je aj výmena skúseností a diskusia o prípadných problémoch naprieč všetkými zúčastnenými, čo následne znamená ešte väčšie množstvo získaných informácií. Cieľom pre účastníka by určite nemalo byť len nečinne sedieť, pasívne počúvať a zjesť všetko, čo je k dispozícii, ale aktívne sa zapájať, aby po skončení vzdelávania odchádzal so znalosťami, ktoré budú prínosom tak preňho samotného, ako aj pre spoločnosť, v ktorej pracuje.

IN-HOUSE ŠKOLENIA

In-house školenie je forma onsite vzdelávania s tým rozdielom, že účastníci sú z jednej spoločnosti a vo väčšine prípadov sa koná priamo v priestoroch spoločnosti. Veľká výhoda v tomto prípade je možnosť prípravy vzdelávacieho kurzu podľa potrieb a požiadaviek spoločnosti, pre ktorú sa vzdelávanie organizuje. Výsledkom je obsah a informácie, ktoré korešpondujú s očakávaniami danej organizácie a jej manažmentu. Ďalší dôležitý faktor je aj to, že účastníci sa vo veľkej väčšine poznajú, a tak nemajú problém s interakciou, ako to môže byť v prípade klasických onsite školení. Vzdelávacia aktivita je v ich „domácom" prostredí, ktoré poznajú, kde funguje kolektívna spolupráca a účastníci majú viac odvahy. To je veľký prínos nielen pre nich, ale aj pre prednášajúceho, ktorý na základe týchto vstupov dokáže reflektovať ich požiadavky. Pri takejto forme vzdelávania je výhodná najmä detailnosť a presnosť, keď možno absolvovať vzdelávací proces, ktorý bude prínosom nielen pre účastníkov, manažment, ale aj pre ďalšie fungovanie spoločnosti.

CERTIFIKÁCIE

Certifikácie z pohľadu vzdelávania sú v podstate dvojakého typu. Prvý typ je takzvaný účastnícky certifikát, resp. potvrdenie o absolvovaní vzdelávania, druhým je potvrdenie po úspešnom zvládnutí testu. Pre niekoho možno iba zdrap papiera za odsedené dopoludnie, ktorý nemá žiadnu pridanú hodnotu, pre iného symbol nových vedomostí a ocenenie úsilia, ktoré získaniu certifikátu venoval. Iste sa zhodneme, že ten dobrý pocit je určite lepší. A nie je to len pre ten pocit. Je dôležité dosiahnuť, aby práve certifikát odzrkadľoval získané vedomosti, aby nebol iba kusom papiera, ktorý skončí niekde v spodnej zásuvke. Iste, získanie mnohých certifikátov znamená oveľa viac úsilia, ako je absolvovanie workshopu, ale akékoľvek získanie certifikátu, najmä v oblasti kybernetickej bezpečnosti, by malo byť podporované aj zamestnávateľom. Je vhodné, aby snaha,

ktorá prinesie osoh obom stranám, bola motiváciou pre zamestnávateľa vyslať zamestnancov na vzdelávacie kurzy a zároveň pre zamestnanca takéto vzdelávanie absolvovať.

KONFERENCIE

Konferencie nám dávajú možnosť poskytovať vzdelávanie väčšiemu množstvu účastníkov naraz. Ich počet nie je taký limitovaný, ako je to napríklad v prípade onsite školení, konferencie môžu mať rádovo stovky účastníkov. Výhodou z pohľadu získaných vedomostí je možnosť oboznámiť sa s viacerými riešeniami, rôznou problematikou a často z pohľadu viacerých vendorov. Účastníkom to umožňuje získať prehľad o trhu a lepšie sa orientovať v problematike kybernetickej bezpečnosti. V neposlednom rade je to skvelá príležitosť na osobné diskusie a rozhovory s odborníkmi, ktorí sú na konferenciách k dispozícii. Konferencie sú zároveň cenovo dostupné, mnohé ponúkajú bezplatný vstup, čím sú atraktívne aj pre menej finančne zabezpečené spoločnosti s nízkym rozpočtom na vzdelávanie.

KTORÁ FORMA VZDELÁVANIA DOMINUJE?

Na základe doterajších skúseností spoločnosti Qubit ľudia preferujú onsite formu vzdelávania, pretože priama interakcia s lektorom a možnosť klásť otázky je významná pridaná hodnota pre každého účastníka.

Zamestnanci s vyšším stupňom odbornosti v konkrétnej oblasti oceňujú predovšetkým školenia v malých skupinách, kde predpokladajú účasť s relatívne rovnakou úrovňou odborníkov. Majú tak možnosť venovať sa už len praktickým diskusiám a navzájom si vymieňať cenné informácie z každodennej praxe. Vítaný formát sú aj menej formálne stretnutia odbornej verejnosti ku konkrétnym témam vo forme klubov, kde si pod taktovkou chairmana vymieňajú svoje názory na riešenie problémov. Informácie v rámci klubov neprúdia jednosmerne od lektora k auditóriu, ale účastníci si ich vymieňajú navzájom. Konfrontujú svoje tvrdenia a prispievajú tak k hľadaniu riešení, ktoré v žiadnom tutoriáli určite nenájdete. 🙂 V neposlednom rade takéto menšie a neformálne vzdelávacie formáty prinášajú neoceniteľné prepojenia a kontakty medzi účastníkmi, ktoré im často slúžia ešte dlho po skončení školenia.

Aktuálna situácia predstavovala pre onsite podujatia veľkú výzvu. Efektívnym riešením sa stali práve online školenia/workshopy so „živým" lektorom, ktorý vie reagovať na otázky účastníkov priamo počas výkladu. Výhodou naďalej ostáva menší počet účastníkov, ako aj prítomnosť dvoch lektorov súčasne tak, aby mohol jeden z nich odpovedať na otázky položené napríklad cez čet v aplikácii.

SYSTEMATICKOSŤ A PRAVIDELNOSŤ VZDELÁVANIA ZAMESTNANCOV

Ako sme uviedli v predošlej časti, možnosti a dostupnosť vzdelávania sú naozaj široké a nie je problém si vybrať. Čo však problémom môže byť, je práve podpora vedenia spoločnosti. Aj zo skúseností z praxe môžeme povedať, že si zamestnanci mnohokrát potrebu vzdelávania uvedomujú a majú oň reálny záujem, ale práve rozhodnutie zo strany manažmentu im ho neumožní. V niektorých spoločnostiach nemajú na vzdelávacie aktivity vytvorený rozpočet vôbec, prípadne je obmedzený. Je však určite veľmi dôležité pre obe strany (zamestnancov aj zamestnávateľov), aby boli všetci zamestnanci vzdelávaní v oblasti kybernetickej bezpečnosti. Hovorí sa, že reťaz je taká silná, aký silný je jej najslabší článok. Rovnako to platí aj v tomto prípade. Takisto je dôležité, aby sme vzdelávanie nebrali ako jednorazovú záležitosť, ale vzhľadom na dynamiku vývoja kybernetických hrozieb by malo ísť o pravidelnú aktivitu. Tak ako opakovane absolvujeme školenia bezpečnosti a ochrany zdravia pri práci (BOZP), mali by sme rovnako pristupovať aj k bezpečnosti v oblasti informačných technológií. A to najmä preto, aby sme získané vedomosti mohli preniesť do praxe a nepoužívali ich iba preto, že to od nás niekto vyžaduje.

Ideálny postup v tomto prípade je vytvorenie vzdelávacieho plánu, ktorý bude tvorený jednotlivými pracovnými rolami. K týmto rolám bude priradený rozsah vedomostí a spôsob (forma), ako ich dosiahnuť. Takto bude možné zabezpečiť systematickosť a pravidelnosť vzdelávania zamestnancov.

QUBIT

Accenture Slovakia
Plynárenská 7/C
821 09 Bratislava
www.accenture.com

Aliter Technologies, a.s.
Turčianska 16
821 09 Bratislava
www.aliter.com

ANECT a.s.
Jarošova 1, 831 03 Bratislava
www.anect.com

Aon Central and Eastern Europe, organizačná zložka
Sky Park Offices, Bottova 2A
811 09 Bratislava
info@aon.sk

Atos IT Solutions and Services s.r.o.
Pribinova 19, 811 09 Bratislava
www.atos.net/sk

citadelo s.r.o.
Lazaretská 12, 811 08 Bratislava
info@citadelo.com
www.citadelo.com

DATALAN, a.s.
Krasovského 14
851 01 Bratislava
info@datalan.sk, kc.datalan.sk

Deloitte na Slovensku
Digital Park II, Einsteinova 23
851 01 Bratislava
www.deloitte.com

EMM, spol. s.r.o.
Sekurisova 16, 841 02 Bratislava
www.emm.sk, emm@emm.sk

eMsec s.r.o.
Varšavská 3, 040 13 Košice
www.emsec.sk

ESET, spol. s r.o.
Einsteinova 24
851 01 Bratislava
www.eset.sk

FORTINET
Explora Jupiter
Bucharova 14/2641
158 00 Praha
www.fortinet.com

GAMO a.s.
Kyjevské námestie 6
974 04 Banská Bystrica
www.gamo.sk

HP Inc Slovakia, s.r.o.
Galvániho 5890/7
821 04 Bratislava
www.hp.sk

LYNX - spoločnosť s ručením obmedzeným Košice
Gavlovičova 9, 040 17 Košice
www.lynx.sk

MIM, s.r.o.
Slnečná 211/1, 010 03 Žilina
info@mim.sk, www.mim.sk

Qubit Academy
J. Kozáčeka 2
960 01 Zvolen
www.qubitacademy.com

Slovak Telekom, a.s.
Bajkalská 28, 817 62 Bratislava
www.telekom.sk

Slovanet, a.s.
Záhradnícka 151
821 08 Bratislava 2
www.slovanet.sk

SOMI Systems a.s.
Lazovná 69
974 01 Banská Bystrica
www.somi.sk

KYBERNETICKÁ BEZPEČNOSŤ PRE FIRMY

Vyšlo vo vydavateľstve Digital Visions v 2021
ako bezplatne distribuovaná publikácia.

VYDÁVA:
Digital Visions, s. r. o.
Kladnianska 60, 821 05 Bratislava
e-mail: info@dvnet.sk, http: www.nextech.sk

VÝKONNÝ RIADITEĽ:
Martin Drobný

ODBORNÝ REDAKTOR:
Ľuboslav Lacko

ASISTENT VYDANIA, INZERCIA:
Ľudmila Gebauerová

GRAFIKA:
Peter Mačuga

JAZYKOVÁ REDAKTORKA:
Brigita Keszeliová

Za obsah inzerátov zodpovedajú inzerenti.
Ďalšia reprodukcia článkov možná
len so súhlasom vydavateľa.
Tlač: z dodaných reprodukčných materiálov.

ISBN 978-80-973581-6-7

OBČIANSKE ZDRUŽENIE
TECHNO LAND

MAGAZÍN
NEXTECH

PRINÁŠA PRE UČITEĽOV INFORMATIKY A ICH ŽIAKOV
ZÁBAVNÉ NÁVODY A VIDEÁ V SERIÁLI

IoT prakticky

OBSIAHNE TÉMY:
internet vecí, robotiky
a využívania Micro-bit, Raspberry,
Python, Arduino, PLC...

Viac sa dozvieš na stránke:

https://www.nextech.sk/IoT

Skratka k vášmu bezpečnému IT

Ochránime vaše podnikanie pred IT hrozbami. O toto všetko sa pre vás postaráme:

Zabezpečenie pracovných staníc
- Virtual storage
- Telekom cloud server

Zabezpečenie konektivity a dátovej prevádzky
- Network protector (DDoS)
- Managed Firewall
- WAF/WebShield

Zabezpečenie serverov
- Virtual storage
- Telekom cloud server

Viac na: https://www.telekom.sk/biznis/it-bezpecnost-na-mieru

ZAŽIME TO SPOLU