NEXTECH

KYBERNETICKÁ BEZPEČNOSŤ

PRE FIRMY 2023

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

Váš globálny špecialista na kybernetickú bezpečnosť digitálnej infraštruktúry

Exclusive Networks Slovakia

Naša vízia plne dôveryhodného digitálneho sveta sa opiera o najlepšie technologické portfólio vo svojej triede.

Ponúkame produkty pre všetky tieto businessové výzvy dnešných dní:

Preskúmajte naše portfólio

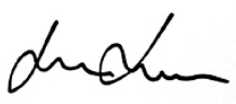
EXCLUSIVE NETWORKS

Exclusive Networks Slovakia s.r.o. | Galvanihho 7/D | 821 04 Bratislava
IČO: 50096958 | IČ DPH: SK2120250033 | Tel: +421 903 807 007
E-mail: info@exclusive-networks.sk | **www.exclusive-networks.sk**

SLOVO NA ÚVOD:

Žiadna oblasť podnikania ak chce uspieť v náročných ekonomických podmienkach a ostrom konkurenčnom boji sa nezaobíde bez efektívnej IT podpory. Jej integrálnou súčasťou je aj zber údajov z výrobných, logistických, finančných a organizačných procesov a ich analýza v reálnom čase. Takto získané informácie sú kľúčové pre operatívne rozhodovanie aj strategické plánovanie. IT infraštruktúra však okrem veľkého množstva výhod prináša aj veľa rizík. Ochrana proti čoraz sofistikovanejším útokom si vyžaduje veľa úsilia a pomerne vysoké náklady, navyše s vedomím, že 100 % zabezpečenie je v praxi bez ohľadu na náklady nedosiahnuteľné. Bez ohľadu na veľkosť firmy je potrebné k zabezpečeniu IT pristupovať ako k projektu na všetkých úrovniach IT architektúry, počnúc klientskymi zariadeniami, cez podnikové siete a servery a/alebo cloudové služby. Vo väčšine prípadov najväčším je najväčším rizikom a vstupnou bránou pre kybernetické útoky na firmu ľudský faktor. Preto je veľmi dôležité nielen definovať účinné bezpečnostné politiky, ale predovšetkým vynútiť ich dodržiavanie a taktiež pravidelné školenie zainteresovaných zamestnancov

Námetom publikácie sú návody a odporúčania, nielen technické, ale aj organizačné na dosiahnutie akceptovateľnej úrovne zabezpečenia IT pri vynaložení prijateľných nákladov a taktiež na zosúladenie zabezpečenia s legislatívnymi požiadavkami, predovšetkým čo sa týka ochrany osobných údajov pri ich spracovávaní technickými prostriedkami a na dosiahnutie požadovanej úrovne informačnej bezpečnosti podľa legislatívnych požiadaviek.



OBSAH:

TECHNOLÓGIE

PROCESY

LEGISLATÍVA

KYBERNETICKÁ BEZPEČNOSŤ PRE FIRMY 2023

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

VÝKONNÝ RIADITEĽ:
Martin Drobný

ODBORNÝ REDAKTOR:
Ľuboslav Lacko

ASISTENT VYDANIA, INZERCIA:
Ľudmila Gebauerová

GRAFIKA:
Peter Mačuga

Za obsah inzerátov zodpovedajú inzerenti.
Ďalšia reprodukcia článkov možná len so súhlasom vydavateľa.
Tlač: z dodaných reprodukčných materiálov.
Zdroj foto strana 1: rawpixel.com on Freepik.

ISBN 978-80-974206-6-6

CYBERGAME 2023

Kyberbezpečnostná hra pre študentov, talentovaných hráčov, programátorov aj profesionálov rôznej úrovne

15 scenárov
70+ úloh

Výhry v kategóriách

- Najlepší hráč
- Najlepšia hráčka
- Hráči vo vetvách
- Študent
- Najmladší hráč
- Učitelia
- Zamestnanci verejnej správy

- MALVÉROVÁ ANALÝZA
- HARDENING
- PROCESY A RIADENIE BEZPEČNOSTI
- OSINT
- FORENZNÁ ANALÝZA
- KRYPTOGRAFIA

Nominácia a tréning národného tímu na European Cyber Security Challenge 2023

Tréningová platforma pre organizácie
01/10/2023 – 31/10/2023

ODBORNÁ GARANCIA
SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

www.cybergame.sk
01/03/2023 – 10/05/2023

ALITER TECHNOLOGIES · CHECK POINT · REPUBLIC OF GAMERS · IBM · ALISON · eset Digital Security Progress. Protected. · Microsoft · elkan smart learning · BCH BUKOVINSKÝ & CHLÁPALA · VEEAM · Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · rtvs: Rozhlas a televízia Slovenska · ZIVE

THIS IS NOT A GAME, THIS IS CYBERGAME


EY
CYBER
SECURITY
TROPHY
POWERED BY EY

Súťaž EY Cyber Security Trophy (EY ESO)

EY Cyber Security Trophy (EY ESO) je jedinečná súťaž, ktorú organizuje spoločnosť EY spoločne v Českej a Slovenskej republike. Jej cieľom je oceniť spoločnosti, odborníkov a budúce talenty pôsobiace v oblasti informačnej a kybernetickej bezpečnosti a etického hackingu.

Posudzované sú štyri súťažné kategórie, z ktorých odborná porota vyberie celkového víťaza:

- Chief Information Security Officer
- DNA Born Ethical Hacker
- Cyber Security Space Innovation
- Cyber Security Future Promise

Hlavná cena EY Cyber Security Trophy

EY ESO prebieha v období od mája do novembra

Kto sa môže prihlásiť?

Právnická osoba (komerčný subjekt, subjekt verejnej správy) / fyzická osoba pôsobiaca v oblasti informačnej a kybernetickej bezpečnosti a etického hackingu

Teší nás, že sa súťaž rozšírila v roku 2022 do Českej republiky.

Viac informácií na:

www.eyeso.sk

www.eyeso.cz

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 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 obsa-

hom. 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.

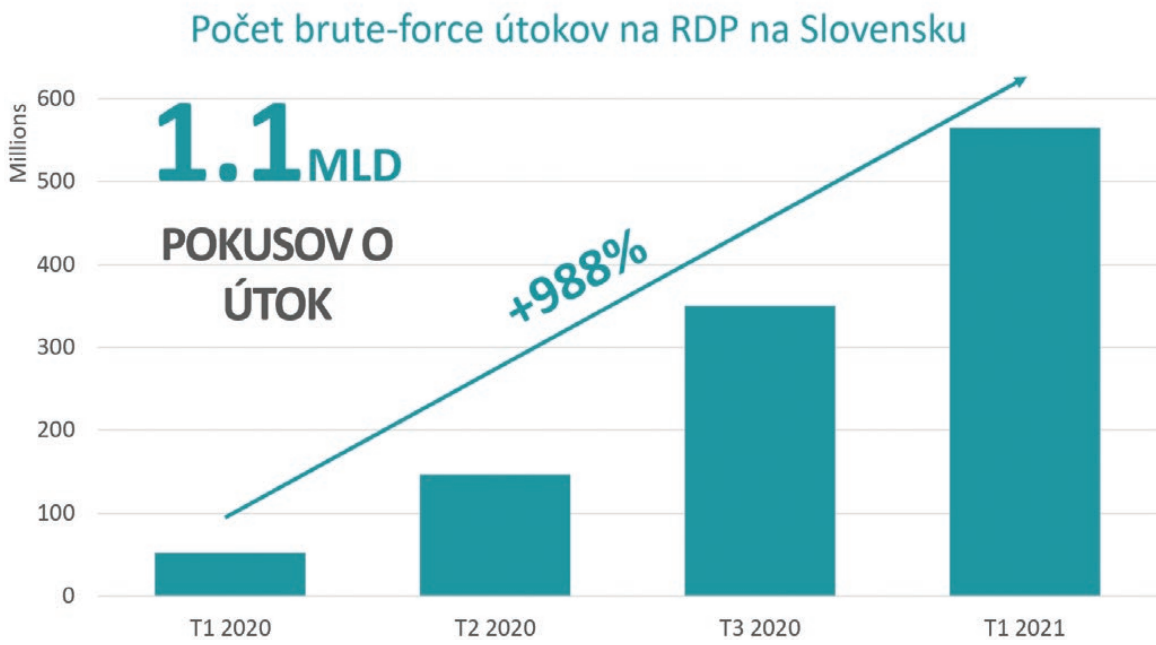
- **Hoax** je falošná poplašná správa, ktorá vystríha používateľa pred počítačovými vírusmi, nebezpečenstvom zneužitia sietí a podobne.
- **Phishing** (*v preklade rybolov*) na odvrátenie hrozby žiada od používateľa vykonať nejakú akciu, ktorá je nebezpečná, napríklad nainštalovanie a spustenie falošného 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 v strede" je v tomto prípade veľmi výstižný. Narušiteľ sa pri tomto spôsobe votrie 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 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.

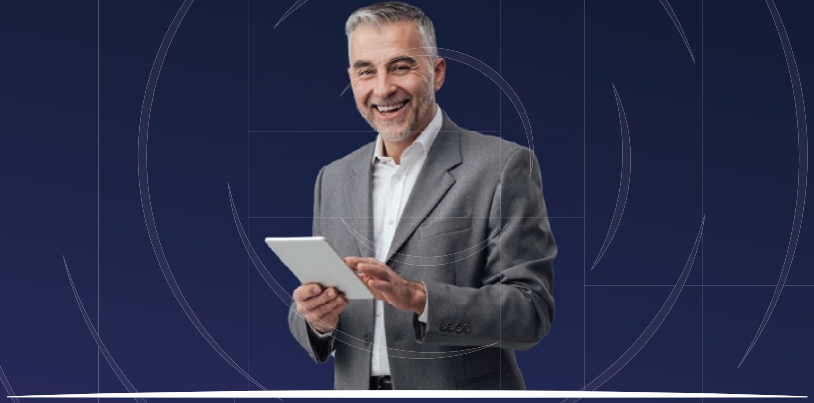
- **Ransomvér** čiže novodobé výpalné. Pri novodobých metódach zločinnosti sa dá pozorovať kopírovanie metód klasickej kriminality, povýšených na novú technologickú úroveň. Typický príklad je internetové výpalné.
- **Kybernetický útok ako služba**. Cloudovej ére, keď sa IT poskytuje ako služba, sa rýchlo 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
ÚVODNÝ OBRÁZOK OD **THOMAS BREHER** Z PIXABAY



▪ ZDROJ: ESET



Zvyšovanie ľudskej odolnosti v oblasti Kybernetickej bezpečnosti na jeden klik.

Najefektívnejšie školenie v oblasti kybernetickej bezpečnosti na svete.

Riešenia od spoločnosti CybeReady zapája do školiaceho cyklu viac zamestnancov, efektívnejšie a jednoduchšie. Náš adaptívny školiaci program v oblasti kybernetickej bezpečnosti na báze strojového učenia zaručuje zníženie rizika organizácie s takmer nulovým úsilím v oblasti IT/IS a najnižším TCO v procesoch kybernetického školenia, simulácie phishingu, auditu a compliance.

Výsledok

100%
Školenia vykonávané každý mesiac na permanentnej báze

8X
Znížené riziko v oblasti vysoko rizikových skupín zamestnancov

4X
Zvýšenie odolnosti zamestnancov vo všeobecnosti

Na naše riešenia sa spoliehajú na Slovensku veľké spoločnosti ako napríklad:

Západoslovenská Distribučná, a. s.,Východoslovenská Distribučná, a. s., Stredoslovenská vodárenská prevádzková spoločnosť, a. s., člen skupiny Veolia a Slovenská elektrizačná prenosová sústava, a. s..

ZÁPADOSLOVENSKÁ DISTRIBUČNÁ

Slovenská elektrizačná prenosová sústava

Stredoslovenská vodárenská prevádzková spoločnosť, a.s.

Pre viac informácií INDRA Slovakia, a. s.: ivan.bala@indra.sk | www.cybeready.com

CYBEREADY

ROZHOVOR: **MICHAL GROSS**, HEAD OF IT SECURITY V 365.BANK

FINANČNÝ SEKTOR BÝVA CIEĽOM KYBERNETICKÝCH ÚTOKOV **300×** ČASTEJŠIE AKO FIRMY V INÝCH ODVETVIACH

V praxi sa stretávame s tým, že podvodníci na vymámenie peňazí využívajú rôzne formy sociálneho inžinierstva. Snažia sa presvedčiť spotrebiteľov o tom, že komunikujú digitálnym kanálom alebo telefonicky so svojou bankou, políciou, telekomunikáciami či online obchodmi. Veľmi často sa vydávajú práve za banky, čo môže výrazne ohroziť osobné financie klientov. Aj preto musia finančné inštitúcie dbať na kyberbezpečnosť o to viac. O podvodných praktikách, kybernetických útokoch aj pohľade banky na bezpečnosť v kontexte rozvíjajúcich sa technológií hovorí **Michal Gross**, Head of IT Security v 365.bank.

Michal Gross, Head of IT Security v 365.bank

Do akej miery súvisí rozvoj technológií a digitalizácia s nárastom výskytu podvodov?

Posledné tri roky boli pre tímy kybernetickej bezpečnosti výzvou a zároveň príležitosťou modernizovať. Potreba urýchleného presunu väčšiny procesov biznisu do digitálneho sveta, práca z domu či adopcia cloudových služieb si vyžiadali investície aj do bezpečnostných opatrení a technológií.

Kybernetické útoky sú dennou súčasťou security operatívy. Stopercentné zabezpečenie je nedosiahnuteľné, preto sa treba orientovať na včasnú detekciu a incident response, aby sa útok zachytil vo fáze,

keď ešte možno útočníka zastaviť pred dosiahnutím jeho cieľa, prípadne čo najviac minimalizovať jeho dosah. Bezpečnostné tímy pracujú s obmedzenými zdrojmi a útočník má navyše neobmedzený čas na premyslenie sofistikovaných stratégií útokov.

Ako zvládnuť kyberútok? Existuje prevencia?

Účinnou formou prípravy na kyberútok sú cvičenia, ktorými sa trénuje reakcia nielen v rámci bezpečnostných tímov a test technickej a procesnej odolnosti, ale aj vnímanie hrozieb zamestnancami. Vždy je výhodnejšie poučiť sa na vlastných chybách pri simulácii útoku.

Do akej miery musia s technologickým rozvojom aj na strane podvodníkov rátať banky?

Možnosti, ktoré banky priniesli svojim klientom, otvárajú priestor na kreativitu podvodníkov, ako zneužiť digitálne dostupné produkty vo svoj prospech. Zároveň sa rozšíril perimeter banky, ktorý treba chrániť – technicky, procesne, ale aj vzdelávaním ľudí. Je potrebné chrániť aj aplikáciu na mobilnom zariadení klienta ako súčasť infraštruktúry banky. Banky implementujú inteligentné nástroje na identifikáciu podozrivých udalostí s možnosťou automatizovanej reakcie na báze 24×7.

Akým kybernetickým útokom môžu banky čeliť v súčasnosti?

Finančný sektor býva cieľom kybernetických útokov tristokrát častejšie ako iné odvetvia, banky preto implementujú komplexné programy na ochranu pred bezpečnostnými hrozbami. Kybernetická kriminalita je v tomto sektore primárne finančne motivovaná a útoky sú cielené na najslabší článok, ktorým bývajú nedostatočne obozretní klienti, ale aj zamestnanci bánk. Ďalším z cieľov môže byť aj kompromitácia IT prostredia banky, zašifrovanie, prípadne exfiltrácia dát a žiadosť o výkupné. Vstupnou bránou býva nedostatočne patchovaný softvér alebo úspešný phishing na používateľa v banke.

Posledné dva roky priniesli výrazný nárast počtu incidentov spojených s phishingom. Čo je dôvodom?

Podvodníci sa vždy snažia vyťažiť z aktuálnej situácie – či to boli útoky so scenárom doručenia zásielky po zaplatení poštovného, keď ľudia počas lockdownu využívali najmä doručenie nákupov cez online služby a bolo pre nich ťažšie zorientovať sa pri niekoľkých paralelných objednávkach, alebo minuloročné scenáre založené na strachu z inflácie a možnosti investovania do kryptomien na predídenie straty hodnoty úspor. Nárast prípadov je ovplyvnený úspešnosťou podvodníkov, keď dokážu za relatívne krátky čas zarobiť desiatky až stovky tisíc eur. To ich motivuje na vytváranie nových, prepracovanejších scenárov.

Ktoré používateľské zvyklosti najviac ohrozujú osobnú a firemnú IT bezpečnosť?

Zvyklosti, ale aj nevedomosť sú bránou pre manipuláciu používateľov aj pre únik dát cez technológie. Nedostatočné venovanie pozornosti pri inštalácii, používanie aplikácií z neoverených zdrojov, laxnosť pri konfigurácii práv aplikácií a opakované používanie jednoduchých hesiel môžu viesť k rýchlemu úniku osobných údajov a zneužitiu využívaných služieb.

Aké témy budú dominovať v kybernetickej bezpečnosti v roku 2023?

Bezpečnostné požiadavky pri vývoji a prevádzke aplikácií budú naďalej zmazávať hranice medzi vrstvou infraštruktúry a aplikácií. Rastúca integrácia riešení cez rozhrania API zväčšuje riziká, ktoré treba adresovať medzi partnermi. Geopolitické riziká a ich dosah na dodávateľský reťazec môžu naďalej spôsobovať prevádzkové výzvy. Nevyhnutnou sa stáva automatizácia na inteligentný proces detekcie a odpovede na incidenty spolu s ransomvérovou ochranou záloh.

Predpokladám, že frekvencia podvodov ľudí naučí byť opatrnejšími, no zároveň posunie hranice sofistikovanosti útokov na nové úrovne.

■ 365.BANK

S ÚNIKOM DÁT SA STRETLI AŽ DVE TRETINY MALÝCH A STREDNÝCH FIRIEM

ŠPECIÁLNY PROJEKT

Až dve tretiny malých a stredných firiem majú skúsenosti s únikom dát. Pri bezpečnostných incidentoch pritom strácajú státisíce eur. Začínajú sa preto čoraz častejšie obracať na sofistikované bezpečnostné riešenia XDR/MDR. Vyplýva to z medzinárodného prieskumu SMB Digital Security Sentiment Report 2022, ktorý vypracovala spoločnosť ESET.

Nečudo, že pri dôsledkoch kybernetických útokov sa firmy najviac obávajú práve straty dát. Okrem právnych a prevádzkových problémov môže únik citlivých údajov spoločnosti napáchať aj škody na reputácii a viesť k strate dôvery zákazníkov. Ružovo to nevyzerá so sebavedomím firiem čeliť digitálnym hrozbám. Iba 48 % respondentov uviedlo, že si verí oblasti kybernetickej odolnosti ich firmy.

ÚNIK DÁT MÔŽE STÁŤ FIRMU STÁTISÍCE EUR

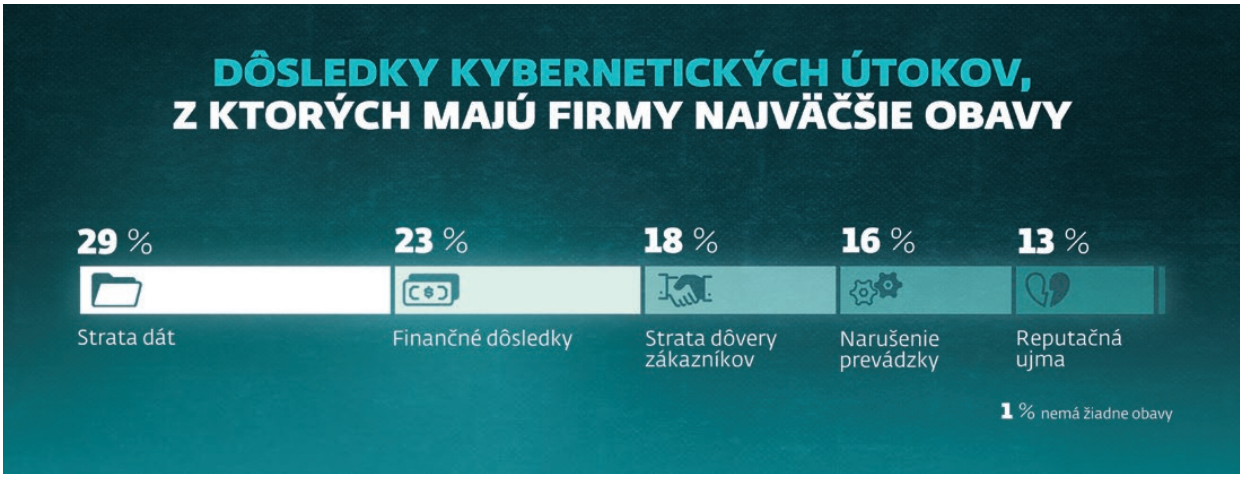
Prieskum spoločnosti ESET sa zameral na to, ako vnímajú v čase turbulentných globálnych udalostí malé a stredné firmy kybernetické hrozby. Medzi respondentmi bolo viac ako 1200 predstaviteľov s rozhodovacími právomocami v oblasti IT bezpečnosti v malých a stredných firmách v Európe a Severnej Amerike.

Z odpovedí manažérov vyplýva, že pre firmy predstavuje únik dát veľký problém. S únikom dát alebo vážnym podozrením na únik dát sa počas uplynulého roka zaoberali až viac ako dve tretiny firiem. Dôsledky podobných bezpečnostných incidentov spôsobujú spoločnostiam značné škody. V priemere prišla zasiahnutá firma o 220-tisíc eur.

PROBLÉMOM JE NÍZKE POVEDOMIE ZAMESTNANCOV

Najvýznamnejší faktor, ktorý prispieva k riziku, že sa firma stane obeťou kybernetického útoku, je podľa opýtaných nedostatočné povedomie zamestnancov o digitálnych nástrahách. Tento problém predstavuje pre spoločnosti ešte väčšieho strašiaka ako vojna na Ukrajine či práca na diaľku, ktorá sa v mnohých firmách stala štandardom po pandémii COVID-19.

Aj napriek tomu, že si manažéri uvedomujú nebezpečenstvo prameniace z hrozby kybernetických útokov, až 70 % z nich uviedlo, že investície firiem do zabezpečenia nestíhajú dynamickým zmenám v spôsobe práce.



ZDROJ: ESET

ČORAZ VÄČŠÍ ZÁUJEM O SOFISTIKOVANÉ RIEŠENIA

Zaujímavé je zistenie, že čoraz viac malých a stredných firiem využíva sofistikované bezpečnostné riešenia na detekciu a reakciu XDR alebo MDR, prípadne sa po nich obzerá. Nástroje pôvodne navrhnuté pre veľké korporácie sa ukazujú ako odpoveď na pribúdajúce a neustále sa vyvíjajúce kybernetické hrozby aj v prípade menších či stredných firiem.

Aktuálne tieto sofistikované riešenia využíva približne tretina firiem SMB, pričom ďalšia tretina ich plánuje nasadiť v priebehu najbližšieho roka.

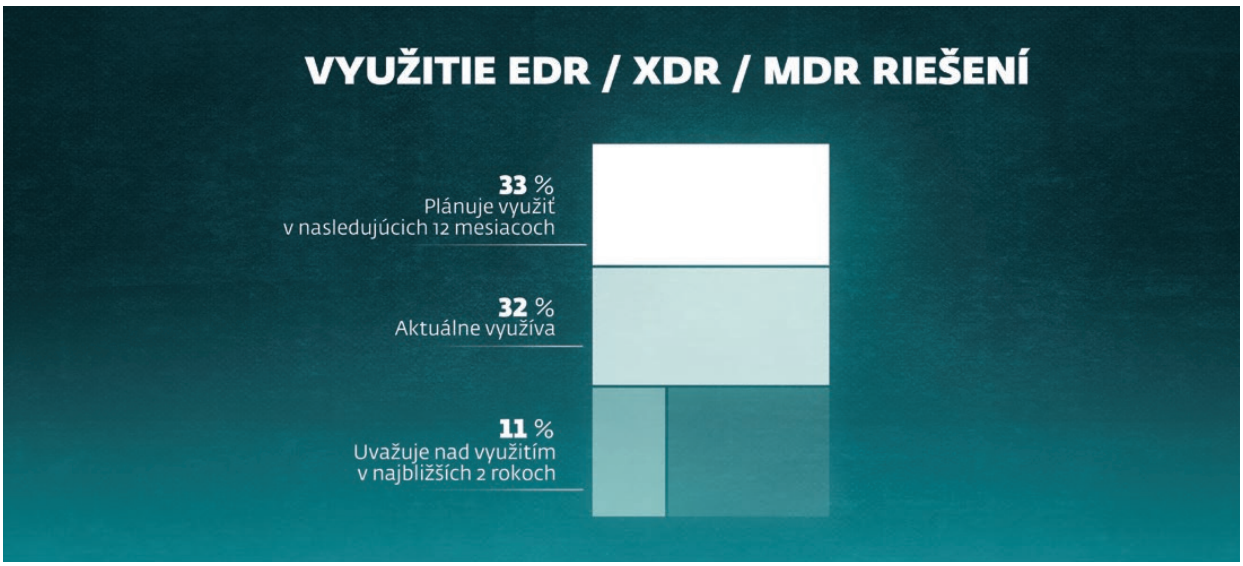
Rozšírená detekcia a reakcia (XDR) je pokročilé riešenie, ktoré poskytuje firmám úplný prehľad o dianí v sieti a dokáže rýchlo reagovať na bezpečnostné incidenty. Aby z nástroja vedeli firmy vyťažiť maximum, je potrebná jeho profesionálna správa. Špecialistov s takýmito zručnosťami je však málo.

Riešením pre firmy, ktoré nemajú vlastných profesionálov, ale chcú využívať XDR, sú služby riadenej detekcie a reakcie (MDR), ktoré spoločnosti kompletne odbremenia od starostí so správou digitálnej bezpečnosti. V portfóliu spoločnosti ESET je táto služba zahrnutá v balíku ESET PROTECT MDR.

Experti dostupní na zavolanie sa postarajú o všetko – inštaláciu, konfiguráciu, proaktívne vyhľadávanie hrozieb aj správu špičkového bezpečnostného riešenia XDR ESET Inspect, optimalizovaného pre infraštruktúru zákazníka.

■ ESET

ÚVODNÉ FOTO : RAWPIXEL.COM / **ON FREEPIK.COM**



ZDROJ: ESET

AUDIT KYBERNETICKEJ BEZPEČNOSTI

Audit nie je bezpečnostným opatrením, ale metódou získavania dôkazov o stave bezpečnosti. Jeho cieľom je posúdiť mieru zhody prijatých bezpečnostných opatrení s požiadavkami podľa zákona o kybernetickej bezpečnosti a súvisiacich osobitných predpisov.

Zároveň sa auditom určuje efektívnosť implementovaných opatrení a spôsob ich prevádzkovania či vykonávania. Prostredníctvom auditu je možné proaktívne identifikovať nedostatky v kybernetickej bezpečnosti, primárne neodhalené riziká. Na základe toho je možné prijať opatrenia na ich odstránenie a nápravu a predísť tak riziku kybernetických bezpečnostných incidentov.

POŽIADAVKA NA AUDITING

Začiatkom roka 2018 vstúpil do platnosti slovenský zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti. Vznik tohto právneho predpisu bol priamo vyvolaný požiadavkou smernice EÚ o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (skráteným názvom Smernica NIS) [1]. Jednou z činností, ktorú zákon vyžaduje od povinných osôb, je posudzovanie úrovne bezpečnosti formou auditu. Požiadavka na audit sa nakoniec dostala aj do novelizovanej smernice NIS2 [2].

Aj 4 roky od účinnosti zákona má odborná verejnosť otázky ohľadom cieľov auditu, stanovenia jeho rozsahu, metodiky, mechanizmu ohodnocovania auditných zistení a najmä spôsobu, akým audítor interpretuje svoje zistenia vo výslednej správe. Vzhľadom na blížiace sa zákonné lehoty zaznieva v odbornej verejnosti čoraz častejšie otázka, akým spôsobom zabezpečiť audit kybernetickej bezpečnosti. Zamestnanci, zodpovední za obstarávanie, sa samozrejme zamýšľajú aj nad odhadom prácnosti a s ňou súvisiacich nákladov.

ČO JE TO AUDIT?

Existuje niekoľko rôznych definícií . Líšia sa v detailoch, väčšinou podľa cieľa auditu a podľa objektu posudzovania. Všetky definície sa však zhodujú vo všeobecnej časti v tom, že **audit je systematický, nezávislý a zdokumentovaný proces získavania podkladov, konštatovaní faktov alebo iných dôležitých informácií a ich objektívneho posudzovania s cieľom**

určiť mieru, v akej sa splnili určené vopred legislatívou definované požiadavky.

Často dochádza k zamieňaniu testovania a auditu, resp. sú považované za ekvivalentné činnosti. Medzi nimi je však zásadný rozdiel.

Bezpečnostným testovaním (vrátane penetračných testov alebo testovania zraniteľností softvéru) sa overuje splnenie očakávaných bezpečnostných charakteristík testovaných objektov. Tieto charakteristiky môžu byť stanovené interne alebo na základe najlepšej praxe. Pri testovaní je **dôraz najmä na opakovateľnosti použitého postupu.** Táto opakovateľnosť je základom pre tzv. testovacie scenáre.

Pri audite je **dôraz kladený na systematickosť, nezávislosť a zdokumentovanie procesu** a následne nestranné posúdenie získaných auditných dôkazov. Pre kvalifikované posúdenie zhody formou auditu je potrebná formálna špecifikácia, ktorou je všeobecne záväzný právny predpis alebo technická norma. V slovenských podmienkach je touto formálnou špecifikáciou 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 v znení neskorších predpisov.

V súvislosti s auditom je tu však ešte jedna podstatná požiadavka. Zatiaľ čo testovať môže subjekt aj svojpomocne (alebo pomocou zručného dodávateľa), **audit môže vykonávať len nestranný kvalifikovaný audítor.** Kým testovanie nevyžaduje nestrannosť a nekladie špeciálne nároky na spôsobilosť a prax, pre audit kybernetickej bezpečnosti je nestrannosť a kvalifikácia vyžadovaná priamo zákonom.

Cieľom auditu kybernetickej bezpečnosti (ďalej už len „audit") je najmä posúdiť zhodu prijatých bezpečnostných opatrení s požiadavkami podľa Zákona a súvisiacich osobitných predpisov. Zároveň sa auditom určuje efektívnosť implementovaných opatrení v prostredí prevádzkovateľa základnej služby (ďalej len „PZS").

Je potrebné vziať na zreteľ, že transpozíciou smernice NIS2 do novelizovaného zákona o kybernetickej bezpečnosti sa zvýši počet povinných osôb z doterajších približne 1500 až na 9000. A povinnosť vykonať audit sa tým dotkne aj takých subjektov, ktoré doteraz túto zákonnú povinnosť nemajú.

KTO MÔŽE VYKONAŤ AUDIT?

Opakovane je potrebné zdôrazniť, že audit kybernetickej bezpečnosti je veľmi špecifická odborná činnosť, pre ktorú sú vyžadované určité spôsobilosti a rozsiahla prax. Na otázku, kto je schopný vykonať audit kybernetickej bezpečnosti, sa dá odpovedať až vtedy, ak pochopíme, čo vlastne audítor posudzuje.

Všeobecným cieľom auditu je proaktívne identifikovať nedostatky v kybernetickej bezpečnosti, najmä neodhalené hrozby a riziká. Na základe toho je možné prijať opatrenia na ich odstránenie a nápravu a predchádzať tak riziku kybernetických bezpečnostných incidentov.

Audítor kybernetickej bezpečnosti musí byť spôsobilý overiť plnenie povinností podľa zákona. Preto by mal veľmi dobre ovládať príslušné právne predpisy. Audítor zároveň musí vedieť posúdiť efektívnosť a nedostatky prijatých bezpečnostných opatrení a zhodnotiť spôsob prevádzkovania informačných a komunikačných technológií. Z toho vyplýva, že na audítora kybernetickej bezpečnosti sú kladené veľmi vysoké požiadavky na jeho vedomosti a zručnosti. Dôležitá je aj prax audítora. Začiatočník či absolvent vysokej školy nemá dostatočnú skúsenosť, najmä nie z prostredia a kultúry podnikov. Rovnako tak človek bez kvalifikácie v IT oblasti nedokáže objektívne posúdiť výsostne technické opatrenia, napríklad v oblasti bezpečnosti počítačových sietí, hardeningu serverov, bezpečnostnej architektúry, šifrovania alebo bezpečnosti softvérového kódu.

Audit kybernetickej bezpečnosti je forma koncesovanej činnosti a podnikaním podľa osobitného pred-

[1] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

[2] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo dňa 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148

pisu . V zmysle § 29 ods. 3 Zákona **audit kybernetickej bezpečnosti vykonáva výhradne certifikovaný audítor kybernetickej bezpečnosti,** ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby.

Certifikáciu audítora kybernetickej bezpečnosti vykonáva osoba akreditovaná podľa osobitného predpisu [3)] ako orgán certifikujúci osoby (ďalej len „Certifikačný orgán") v oblasti kybernetickej bezpečnosti. Posúdiť spôsobilosť uchádzačov o výkon práce audítora kybernetickej bezpečnosti sú v Slovenskej republike v čase vydania tejto publikácie oprávnené dva certifikačné orgány, ktoré boli na túto činnosť akreditované Slovenskou národnou akreditačnou službou. Zoznam certifikovaných audítorov, ako aj zoznam právnických osôb, ktoré zamestnávajú certifikovaných audítorov, je verejne dostupný na webovom sídle Národného bezpečnostného úradu.

Vzhľadom na prácnosť štandardného auditu a zároveň vysoký počet prevádzkovateľov základných služieb, ktorí prevádzkujú len I. a II. kategóriu sietí a informačných systémov, zákonodarca prostredníctvom prechodného ustanovenia k úpravám Zákona [6] účinným od 1. augusta 2021 v § 34a ods. 2 umožnil, aby prevádzkovatelia mohli v období od 1. augusta 2021 do 31. decembra 2023 pre I. a II. kategóriu sietí a informačných systémov zabezpečiť plnenie povinnosti podľa § 29 v znení účinnom od 1. augusta 2021 vykonaním preverenia účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených zákonom samohodnotením. Podmienkou je že **samohodnotenie vykoná manažér kybernetickej bezpečnosti** podľa § 20 ods. 4 písm. a) funkcionalitou jednotného informačného systému kybernetickej bezpečnosti.

METODIKA PRE VÝKON AUDITU KYBERNETICKEJ BEZPEČNOSTI

Predmetom auditného posudzovania je konštatovanie zhody, alebo nezhody požiadaviek, vzťahujúcich sa na bezpečnosť sietí a informačných systémov, od ktorých závisí poskytovanie základnej služby.

Existujú rôzne metódy auditu kybernetickej bezpečnosti. Metóda, ktorú navrhne audítor, závisí od cieľov, predmetu a kritérií auditu a aj od požiadaviek na jeho trvanie a požiadaviek na miesto, kde je audit vykonávaný. Kombinácia rôznych metód auditu zvýši jeho efektívnosť. Zároveň sa tým zamedzí možným nepresnostiam auditných zistení.

Metódy auditu sa delia do štyroch tried podľa miery súčinnosti auditovaného a spôsobu interakcie medzi audítorom a auditovaným.

Činnosti auditu na mieste sa vykonávajú primárne v sídle prevádzkovateľa. V prípade auditu na diaľku sú auditné činnosti vykonané audítorom bez jeho fyzickej prítomnosti v sídle PZS.

Činnosti auditu **pri osobnej vzájomnej súčinnosti** znamenajú komunikáciu medzi pracovníkmi PZS a audítorským tímom. Činnosti auditu **bez osobnej**

[3)] Zákon č. 505/2009 Z.z. o akreditácii orgánov posudzovania zhody a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

METÓDY AUDITU:

Súčinnosť	Spôsob výkonu činností	
	Na mieste	**Na diaľku**
Osobná vzájomná súčinnosť	• Vykonanie auditných rozhovorov • Doplnenie kontrolných záznamov a dotazníkov za spoluúčasti PZS • Vykonanie preskúmania objektu posúdenia za spoluúčasti PZS • Vzorkovanie	• Cez interaktívne komunikačné prostriedky: - vykonanie rozhovorov - pozorovanie vykonávania práce s diaľkovým navádzaním - doplnenie kontrolných záznamov a dotazníkov - vykonanie preskúmania objektu posúdenia za spoluúčasti PZS
Bez osobnej vzájomnej súčinnosti	• Vykonanie preskúmania objektu posúdenia (napr. záznamy a analýza údajov) • Pozorovanie výkonu práce • Vykonanie návštevy na mieste • Doplnenie kontrolného zoznamu • Vzorkovanie (napr. produktov)	• Vykonanie preskúmania objektu posúdenia • Pozorovanie výkonu práce pomocou prostriedkov dohľadu • Posúdenie predpisov a regulačných požiadaviek • Analýza údajov

vzájomnej súčinnosti nezahŕňajú žiadnu osobnú vzájomnú súčinnosť s osobami zastupujúcimi PZS, avšak znamenajú analýzu zariadení, vybavenia a dokumentácie.

Pri určovaní metódy auditu musí vedúci audítor zvažovať:

- finančné a časové zdroje, nevyhnutné na prípravu, riadenie a zlepšovanie auditu,
- individuálnu a celkovú dostupnosť iných audítorov a technických expertov, ktorí majú vhodné kompetencie na určité čiastkové ciele programu auditu,
- rozsah programu auditu, riziká a príležitosti programu auditu,
- čas a náklady na cestu, ubytovanie a ďalšie potreby auditovania,
- vplyv rozdielnych časových pásem v prípade, že klient auditu prevádzkuje geograficky vzdialené prevádzky,
- dostupnosť technológií podporujúcich vzdialenú spoluprácu pri audite na diaľku (napr. cloudové riešenia, telekonferenčné systémy atď.),
- dostupnosť nevyhnutných zdokumentovaných informácií určených v priebehu tvorby programu auditu,
- požiadavky týkajúce sa utajovaných skutočností, fyzickej bezpečnosti a kryptografických mechanizmov.

URČENIE ROZSAHU AUDITU KYBERNETICKEJ BEZPEČNOSTI

Prevádzkovateľ je povinnou osobou, ktorá musí vykonať audit v rozsahu stanovenom podľa zákona. Avšak za konkrétne určenie rozsahu auditu zodpovedá audítor kybernetickej bezpečnosti.

Do výpočtu rozsahu vstupujú rôzne atribúty vo vzťahu k prostrediu a procesom prevádzkovateľa základnej služby. Výpočet je závislý od metodiky auditu, tá je však známa len vymedzenému okruhu zainteresovaných odborníkov. Povedzme si teda niečo o auditných postupoch, na základe ktorých je možné odhadnúť prácnosť a rozsah auditu kybernetickej bezpečnosti.

Dôvod, prečo za určenie dĺžky trvania auditu zodpovedá výhradne audítor, je jednoduchý – niet nikoho kvalifikovanejšieho, kto by vedel efektívne, vopred, aj bez posúdenia prostredia (teda takpovediac „naslepo“) odhadnúť, ako dlho môže konkrétny audit trvať. Určiť sa to dá len kvalifikovaným odhadom. A zároveň je tu určitý paradox. Totiž ten, kto je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom vykonaním auditu kybernetickej bezpečnosti, je PZS. A náklady na audit kybernetickej bezpečnosti (okrem auditu, ktorý nariadil úrad) taktiež znáša PZS. Teda prirodzeným záujmom prevádzkovateľa základnej služby je čo najviac znížiť náklady na audit.

Spôsob určenia rozsahu auditu je stanovený v prílohe č. 3 vyhlášky NBÚ č. 493/2022Z. Z.z. o audite kybernetickej bezpečnosti.

V záujme audítora je určiť časový rozsah trvania auditu tak, aby bol rozsah dostatočný na posúdenie. Ak tento čas audítor podcení, nebude schopný identifikovať všetky riziká a vyhodnotiť z nich vyplývajúce nezhody a teda ani v dostatočnom detaile ich opísať. Nevýhodou, vyplývajúcou z takto zníženej kvality, však bude trpieť prevádzkovateľ. Pretože nezíska informácie, ktoré by mu inak mohli byť užitočné.

Pre výkon auditu sa primárne predpokladá výkon činností na mieste, s osobnou vzájomnou súčinnosťou. Uprednostňovanou auditnou metódou sú auditné rozhovory, doplnenie kontrolných záznamov a dotazníkov za spoluúčasti pracovníkov PZS, preskúmanie objektov posúdenia za spoluúčasti PZS, výkon testov vzoriek. Rozsah vzoriek určuje audítor s ohľadom na vykonanú klasifikáciu informácií a kategorizáciu sietí a informačných systémov, vykonanú analýzu rizík kybernetickej bezpečnosti a na vypovedaciu schopnosť auditu.

Ako teda audítor určí predpokladaný rozsah auditu?

Zohľadňuje informácie, ktoré získa zo žiadosti prevádzkovateľa o vykonanie auditu kybernetickej bezpečnosti. V prípade potreby si môže vyžiadať dodatočné údaje.

Informácie, ktoré determinujú rozsah auditu, sú podľa vyhlášky najmä:

- počet používateľov,
- počet zamestnancov, zúčastňujúcich sa na prevádzke sietí a informačných systémov,
- kategórie sietí a informačných systémov,
- rozsah účasti tretích strán na prevádzke sietí a informačných systémov a implementácii bezpečnostných opatrení,
- množstvo, rozsah a komplexnosť dokumentácie, súvisiacej s prevádzkou informačného systému a implementáciou bezpečnostných opatrení, vrátane výsledkov predchádzajúcich auditov a vykonaných analýz rizík.

Detaily sú uvedené v spomenutej vyhláške.

Súčasťou určenia rozsahu auditu je aj výber metód auditu, voľba procedúr, výber nástrojov a výber kritérií pre vyhodnotenie auditných dôkazov.

Audítor na základe informácií, ktoré získal zo žiadosti o vykonanie auditu, spracuje návrh programu auditu.

VYKONATEĽNOSŤ AUDITU

Odhad vykonateľnosti auditu má zaručiť, že ciele auditu budú dosiahnuté. Pri určení vykonateľnosti by sa mali vziať do úvahy dostupnosť informácií na plánovanie a vykonanie auditu, súčinnosť s prevádzkovateľom základnej služby a primeraný čas a zdroje na vykonanie auditu.

Tak, ako aj v iných oblastiach obstarávania, býva bežné, najnižšia cena vôbec neznamená aj dostatočnú kvalitu. Má prevádzkovateľ základnej služby chcieť najlacnejší audit? Alebo má mať na zreteli čo najpresnejšie identifikovanie možných rizík a nezhôd vo svojej organizácii v oblasti kybernetickej bezpečnosti?

Ak sa audit na základe odhadu nedá vykonať, potom je účelnejšie prevádzkovateľovi odporučiť odklad výkonu auditu až do doby relevantnej zmeny, ktorá poskytne predpoklad nového stanovenia vykonateľnosti auditu. V opačnom prípade je najvyšší čas, aby sa prevádzkovatelia základných služieb začali vážne zaujímať o svoju povinnosť vykonať audit kybernetickej bezpečnosti a najmä o lehoty vyplývajúce zo zákona.

■ IVAN MAKATURA

ÚVODNÉ FOTO **TOWFIQU BARBHUIYA** ON UNSPLASH

CHRISTINA @ WOCINTECHCHAT.COM ON UNSPLASH

HAVARIJNÝ PLÁN, REAKCIE NA INCIDENTY, POSTUP OBNOVENIA FUNGOVANIA IT

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.

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

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 informačne bezpečnosti na strategickej, taktickej aj operatívnej úrovni. Ana-

lýza 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 oddelenie 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. wSkúmajú 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. 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.

NEPRIJATEĽNÁ ÚROVEŇ RIZIKA ZNAMENÁ OHROZENIE ČI DOKONCA ZÁNIK FIRMY, A PRETO NEVYHNUTNE VYŽADUJE PRIJATIE PREVENTÍVNYCH OPATRENÍ NA JEHO ZNÍŽENIE.

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

ÚVODNÉ FOTO **KASIA DERENDA** ON UNSPLASH

INVENTARIZÁCIA SOFTVÉRU

Nelegálny softvér sa vo firme môže používať buď úmyselne, alebo vinou nepozornosti či nevedomosti, alebo často aj vďaka osobnej iniciatíve zamestnancov, ktorí si ho na svoje firemné počítače svojvoľne nainštalujú. Preto treba nelegálny softvér vnímať ako hrozbu. Vo väčšine prípadov má takáto inventarizácia softvéru pre firmu veľký ekonomický prínos, pretože dokáže odhaliť aj nepoužívaný softvér či neaktualizované licencie z minulosti.

Cieľom procesu inventarizácie je nielen overiť „licenčnú čistotu", teda zisťovať, do akej miery je softvér používaný firmou v súlade s licenčnými právami poskytovanými autormi softvéru, ale pre firmu najdôležitejšia úloha auditu je analýza využívania softvéru. Výsledky takejto analýzy môžu byť dôležitým podkladom na konsolidáciu a implementáciu efektívneho softvérového manažmentu. Pre softvérový audit sa spravidla rozhodnú firmy, ktorých manažment sa domnieva, že audit nemôže preukázať zásadné nedostatky, no môže pomôcť odhaliť prostriedky neefektívne viazané v nevyužívaných licenciách, prípadne firmy a organizácie, v ktorých sa zmení majiteľ alebo vedenie a nový manažment chce začať podnikať v právne usporiadaných vzťahoch.

Audítori najskôr zozbierajú informácie o IT infraštruktúre spoločnosti. V tejto etape začínajú spravidla na najnižšej úrovni granularity, keď zisťujú počet a druh počítačov, počet ich koncových používateľov vrátane ich pracovnej náplne. Následne sa dokumentuje stav architektúry LAN/WAN, stav softvéru na úrovni middleware, stav softvérového manažmentu, správa licencií, systém nákupu softvéru a súvisiace obchodné procesy. Veľmi dôležité je dokumentovanie bezpečnostných aspektov softvérového manažmentu, t. j. hardvérovej a softvérovej ochrany konfigurácií, skladovania inštalačných médií, politiky a predpisov. Popritom sa zbierajú informácie o licenciách, pričom sa posudzujú ich nadobúdacie doklady, zaplatené faktúry, objednávky, resp. dodacie listy a vyhlásenia od dodávateľov. Významným pomocníkom v tejto fáze sú špeciálne softvérové nástroje. Zber potrebných informácií s využitím týchto nástrojov sa realizuje skenovaním počítačov cez sieť. Skenovanie klientskych počítačov prebieha na pozadí, takže počítač sa zaťažuje iba minimálne. No ak firma využíva nadštandardné sieťové zabezpečenie a systémové politiky, zber údajov týmto spôsobom by bol veľmi problematický. V takomto špecifickom prípade treba jednotlivé pracovné stanice skenovať manuálne.

Na inventarizáciu softvéru má nezanedbateľný vplyv aj ľudský faktor, teda ochota pracovníkov firmy spolupracovať pri inventarizácii. Najnáročnejší proces je spravidla získavanie údajov pre potreby klasifikácie systémov a procesov. Analýza softvérového prostredia preto vo veľkých firmách zahŕňa aj rozhovory s manažérmi a kľúčovými zamestnancami, cieľom ktorých je posudzovanie jednotlivých systémov a procedúr týkajúcich sa schvaľovania, objednávania, distribuovania a inštalovania softvéru v rámci ich oblasti pôsobnosti.

■ ĽUBOSLAV LACKO

ÚVODNÉ FOTO **THISISENGINEERING RAENG** ON UNSPLASH.COM

SPRÁVA A ZABEZPEČENIE KONCOVÝCH 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 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 virtualizované 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 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 server, 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

ÚVODNÝ OBRÁZOK OD **WYNN POINTAUX** Z PIXABAY

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 Wi-Fi sietí 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 aplikácie 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 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, Dvice 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
ÚVODNÝ OBRÁZOK **MALIHA MANNAN** ON UNSPLASH

VÝSLEDOK PRIESKUMU, KTORÉ ZARIADENIA SÚ VO FIRMÁCH ADEKVÁTNE CHRÁNENÉ A ZABEZPEČENÉ

S rastúcim prostredím mobilných hrozieb viac ako polovica (54 %) odborníkov v oblasti kybernetickej bezpečnosti uvádza, že ich organizácia chráni mobilné zariadenia vlastnené spoločnosťami pomocou platformy na zabezpečenie koncových zariadení. Zlepšuje sa aj zabezpečenie IoT zariadení. Naproti tomu je problémom model práce odkiaľkoľvek prostredníctvom zariadení vlastnených zamestnancami, či už sa jedná o notebooky a stolné počítače (38 %) alebo mobilné zariadenia (35 %).

• ZDROJ: ENTERPRISE STRATEGY GROUP

POSÚDENIE KYBERNETICKÝCH HROZIEB
PROGRAM CTAP

Informačné systémy firiem čelia čoraz sofistikovanejším hrozbám v kybernetickom priestore. Obavy o dostatočnosť zabezpečenia infraštruktúry proti najnovším útokom sú preto na mieste. Príležitosť na overenie bezpečnosti a vyťaženosti vašej infraštruktúry prináša program CTAP v spolupráci s Fortinetom. Vďaka cielenej analýze firma získa objektívne zhodnotenia stavu svojej siete, a to všetko zadarmo.

Ako to funguje? Zariadenie **FortiGate** niekoľko dní monitoruje prevádzku v sieti. Následne vytvorený report poskytne detaily o **všetkých hrozbách**, ktoré obchádzajú existujúce bezpečnostné kontroly v spoločnosti. Zariadenie FortiGate sa nasadzuje ako pasívny prvok do siete.

ČO MÔŽETE V REPORTE OČAKÁVAŤ?

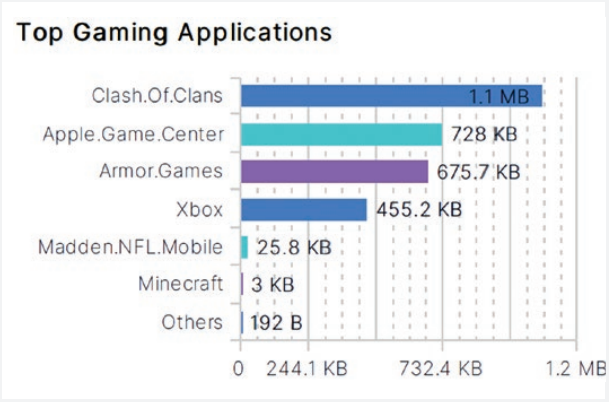
- **Zabezpečenie** – poskytuje informácie o **zraniteľnostiach** používaných aplikácií, t. j. aký malvér alebo botnety boli zistené vo vašej infraštruktúre, ako aj o rizikových zariadeniach.
- **Produktivita** – sprístupní prehľad o využívaní rôznych typov aplikácií v sieti, napr. peer-to-peer, hry, multimédiá, rôzne úložiská atď. Informácie vám dajú obraz, či je používanie webových a tradičných aplikácií klient-server v súlade s vašou firemnou politikou.
- **Využitie siete** – poskytne cenné údaje o priepustnosti vašej siete a požiadavkách na **šírku pásma** počas špičiek. To umožní overiť, či je vaše bezpečnostné riešenie správne dimenzované a optimalizované na základe skutočného využitia.

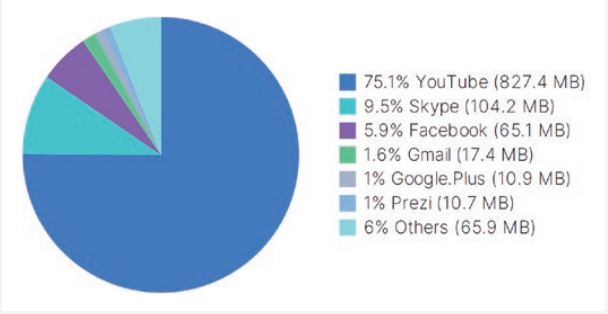
Vďaka programu **CTAP** (https://www.digmia.com/sk/blog/ctap/) tak firma získa cenné informácie o svojich zraniteľnostiach bez potreby investovania do hardvéru a inštalovania nových systémov.

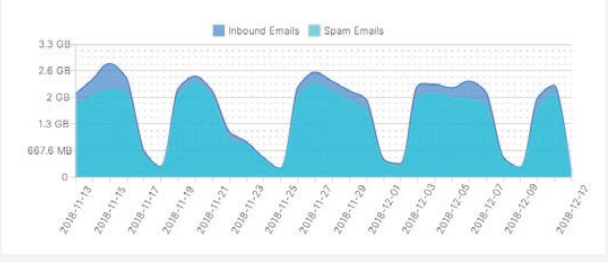
■ DIGMIA

ÚVODNÉ FOTO : SHUTTERSTOCK.COM

#	Risk	Application	Category	Technology	Users	Bandwidth	Sessions
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
4	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
5	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
6	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
7	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
8	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
9	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
10	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38







TECHNICKÉ VYNÚTENIE DODRŽIAVANIA BEZPEČNOSTNÝCH POLITÍK

Nie je žiadna novinka, že pri životnom cykle bezpečnostných politík musíme brať do úvahy všetky aspekty a prostriedky, ktoré budú s touto politikou späté – technické prostriedky, procesy a ľudí. Všetky tieto aspekty a prostriedky musíme zohľadňovať už pri návrhu bezpečnostnej politiky. Navyše to, čo veľkou mierou determinuje ako sa bude bezpečnostná politika dodržiavať, je jej správna definícia s ohľadom na legislatívne a bezpečnostné praktiky a hlavne jej správna definícia vzhľadom na ciele organizácie. Aj tá najlepšia bezpečnostná politika sa bude obchádzať, resp. jej dodržiavanie bude technicky veľmi náročné, ak nebude v súlade s cieľmi organizácie. V ideálnom prípade by mala bezpečnostná politika tieto ciele podporovať.

Technické opatrenia hrajú prím

Nielen ľudská hlúposť a vesmír, ako by povedal slávny fyzik 20. storočia Albert Einstein, ale aj ľudská vynaliezavosť je nekonečná. Na tento fakt by sme mali myslieť zakaždým, keď zvažujeme, aké technické, procesné či ľudské aspekty bude treba použiť pri vynucovaní bezpečnostnej politiky. Keby navyše bezpečnostná politika nepodporovala incentívy jej používateľov či nesledovala ciele spoločnosti, dostali by sme takmer „dokonalú" kombináciu, v ktorej bude extrémne náročné zabezpečiť vynucovanie akejkoľvek bezpečnostnej politiky.

Technologické opatrenia hrajú prím. Na dosiahnutie optimálnych výsledkov pri vynucovaní bezpečnostných politík je dôležité primárne sa sústrediť na technické opatrenia. V ideálnom prípade by nastavenie technológií malo reflektovať nastavenie bezpečnostnej politiky a minimalizovať tak priestor na svojvoľné správanie používateľov. Hoci môže takéto tvrdenie znieť príliš represívne, musíme si uvedomiť, že ak nastavenie technológie nasleduje ciele spoločnosti a motivačné faktory používateľov, potom dostávame ideálny model, kde sú používatelia motivovaní dodržiavať bezpečnostné pravidlá, no zároveň vychádzame z najlepších bezpečnostných odporúčaní, kde je presne definované, čo a ako používatelia môžu vykonávať, pričom všetko ostatné je zakázané. Samozrejmou výhodou pri používaní technických prostriedkov je, že ich môžeme považovať za deterministické (ak odhliadneme od náhodných a softvé-

rových problémov) v porovnaní s ľudským správaním, ich správanie sa nemení a nie je náchylné na náhodné chyby. Použitie technologických prostriedkov vieme veľkou mierou automatizovať a takisto modulárnosť takéhoto prístupu je oveľa väčšia.

Moderné bezpečnostné nástroje využívajúce metódy behaviorálnej analýzy či umelej inteligencie nám zároveň pomáhajú tieto politiky, resp. technické prostriedky nastaviť oveľa dynamickejšie. Bezpečnostné politiky môžu byť oveľa granulárnejšie, môžeme v nich zohľadniť kontext používateľa, ako aj jeho správanie a podľa toho prideliť represívnejšiu či voľnejšiu politiku.

Myšlienku môžeme ilustrovať na politike hesiel, ako verím, každému čitateľovi veľmi dobre známej. O dôležitosti dobre zvolených a komplexných hesiel nemusíme polemizovať, poďme sa však pozrieť na dva spôsoby, ako vynútiť takúto politiku bezpečného hesla.

Klasický spôsob: Technickými prostriedkami nastavíme vynucovane veľmi silného hesla. Hoci je toto nastavenie technicky v poriadku, pri veľmi komplexnom hesle skončíme ľahko v stave, keď nemalá časť používateľov začne túto politiku obchádzať – heslá na papierikoch pod klávesnicou či na monitore by neboli prekvapujúce. V takomto prípade technicky správne nastavená politika priniesla ku koncu dňa zníženie informačnej bezpečnosti.

Vyvážený spôsob: Technickými prostriedkami nastavíme vynucovanie menej komplexného hesla. Toto heslo bude použité pri prihlasovaní v rámci lokálnej LAN, keď sa vykonalo overenie PC alebo sa realizovala behaviorálna analýza používateľa a jeho kontextu (ako a kedy sa prihlásil, ako rýchlo sa prihlásil, pohyby myšou...). Pri pripojení z VPN, prípadne ak kontext nebude potvrdený, budeme vyžadovať potvrdenie cez druhý faktor, napr. potvrdením push notifikácie na mobile či iného HW prvku.

Samozrejme, použitie vyváženého spôsobu prináša použitie pokročilých technologických opatrení, no zároveň veľmi efektívne vynucuje bezpečnostnú politiku prihlásenia, pričom používatelia nie sú motivovaní na jej obchádzanie. Takýmto nastavením by sme docielili zvýšenie úrovne informačnej bezpečnosti s ohľadom na motiváciu používateľov – jednoduché prihlásenie do informačných systémov.

Záver

Hoci technologické prostriedky hrajú pri uvažovaní o ideálnom nastavení bezpečnostnej politiky prím, bolo by naivné si myslieť, že samotné nastavenie týchto technologických prostriedkov je dostačujúce. Domnievam sa, že aj v tomto prípade by sme vedeli vhodne aplikovať Paretov princíp, keď väčšinu ťarchy presunieme na bedrá technológie, no zďaleka nehovoríme o celej ťarche. Správna definícia interných procesov či pravidelné vzdelávanie a zvyšovanie povedomia v oblasti informačnej bezpečnosti ostáva naďalej veľmi dôležitou súčasťou všetkých bezpečnostných politík. Aj v ideálnom prípade musíme nad technológiou udržiavať procesy, ako sú pravidelné aktualizácie či skúmanie logovacích záznamov na overenie funkčnosti a auditných záznamov.

V každej organizácii nastanú situácie, keď napriek tomu, že vhodná technológia existuje, z objektívnych dôvod nemôže byť použitá. V takomto prípade musíme využiť dostupnú technológiu a dodržiavanie bezpečnostných pravidiel ošetriť napr. dodatočnými kontrolnými procesmi či zvýšenou aktivitou v oblasti vzdelávania používateľov.

Vynucovanie bezpečnostných politík predstavuje neustále balansovanie medzi tým, aké technické opatrenia, aké procesy či vzdelávacie aktivity použiť. Navyše tento balans musí zohľadňovať aj faktory, ako sú súlad s legislatívou a v neposlednom rade súlad so smerovaním organizácie.

MICHAL **SRNEC**, CISO ALITER TECHNOLOGIES

ÚVODNÝ OBRÁZOK **FREEPIK ON FREEPIK.COM**

Za obsah a inšpiráciu k tejto téme ďakujeme

www.aliter.com

ALITER TECHNOLOGIES

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.

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.

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 situácií 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 obmedzení 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 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 podľa 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

MOTIVÁCIA NA ZABEZPEČENIE IT SYSTÉMOV

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 zákazníkom 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.

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.

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 rovi-

nách. 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 CISO (Chief Information Security Officer), resp. CSO (Chief Security 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.

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
PHOTO BY **FLY:D** ON UNSPLASH

FAKTORY VPLÝVAJÚCE NA ÚROVNE KYBERNETICKEJ BEZPEČNOSTI

▪ ZDROJ: SLOVAK BUSINESS AGENCY

MANAŽÉRSTVO INFORMAČNEJ BEZPEČNOSTI, BEZPEČNOSTNÝ PLÁN

Systém manažérstva je súbor politík, procesov a postupov používaných organizáciou na zabezpečenie zlepšovania výkonnosti, stanovením opakovateľných krokov, ktoré organizácia vedome implementuje na dosiahnutie svojich cieľov a zámerov, a vytváraním organizačnej kultúry, ktorá sa reflexívne zapája do nepretržitého cyklu sebahodnotenia, opráv a zlepšovania prevádzky a procesov prostredníctvom zvýšeného povedomia zamestnancov a riadiacich schopností.

Vzťahovať pojem „manažment informačnej bezpečnosti" len na technickú infraštruktúru jen zavádzanie čitateľa, alebo nepochopenie podstaty riadenia informačnej bezpečnosti.

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 kybernetickú 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

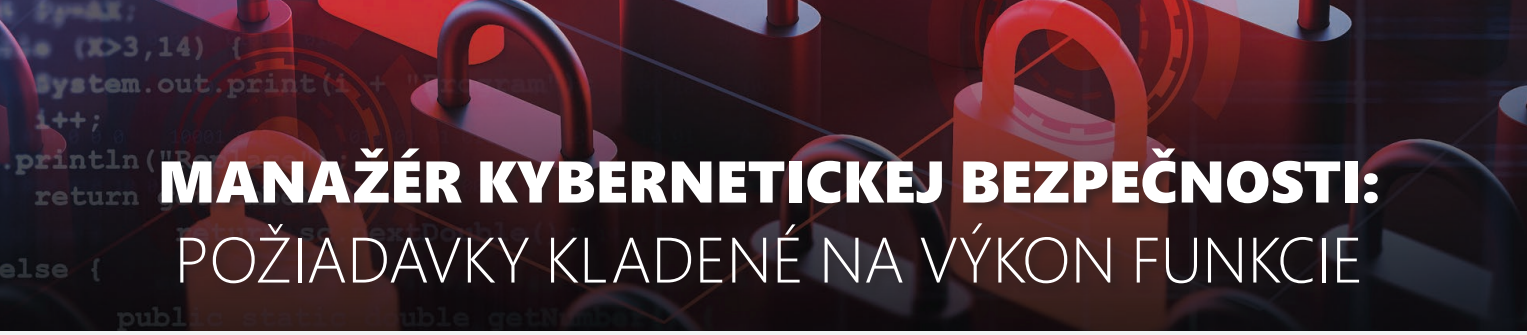
Rozdiel medzi bezpečnostnou politikou a bezpečnostným plánom, ktorý je rozpracovaním implementácie bezpečnostnej politiky, je zrejmý z nasledujúcich príkladov.

- **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
PHOTO BY CHRISTINA @ WOCINTECHCHAT.COM ON UNSPLASH.COM/



MANAŽÉR KYBERNETICKEJ BEZPEČNOSTI: POŽIADAVKY KLADENÉ NA VÝKON FUNKCIE

Jedna zo základných povinností, ktorý prináša zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a s ním súvisiaca 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, je zriadenie **funkcie manažéra kybernetickej bezpečnosti** (skratka MKB). Požiadavka určenia MKB je uvedená v § 20 ods. 4 písm. a) zákona a § 5 písm. a) vyhlášky Národného bezpečnostného úradu.

Základnou úlohou MKB je zodpovednosť za organizovanie systému riadenia kybernetickej bezpečnosti. Cieľom tohto prístupu je obmedziť škody, ktoré by mohli vzniknúť v dôsledku chýb, omylov alebo neoprávneného použitia sietí a informačných systémov. Úloha MKB je úplne kľúčová pre správne nastavenie fungovania systému riadenia kybernetickej bezpečnosti.

Požiadavky na MKB a jeho povinnosti:

- **Priamy prístup k štatutárovi** – MKB má povinnosť informovať priamo štatutárny orgán prevádzkovateľa základnej služby o činnostiach vyplývajúcich z výkonu jeho úlohy, teda najmä o funkčnosti kybernetickej bezpečnosti.
- **Nezávislosť od prevádzky** – MKB musí byť nezávislý od útvaru zaisťujúceho prevádzku IT. Mal by to byť človek, ktorý sa vyzná v informatike, ale zároveň v tejto oblasti aktívne u prevádzkovateľa nepracuje. Jedným zo schodných riešení je externý odborník.
- **Vzdelanie a prax** – MKB by mal mať medzinárodne uznaný certifikát a minimálne 5 rokov praxe v oblasti informačných technológií.
- **Osobnostné predpoklady** – myslieť a konať v súvislostiach, poskytovať spätnú väzbu, schopnosť viesť pracovný tím.
- **Všeobecné/špecifické/odborné kompetencie** – digitálna, ekonomická, finančná a technická gramotnosť, analytické, strategické a koncepčné myslenie, schopnosť prijímať rozhodnutia a niesť zodpovednosť.

Okrem iného by to mal byť človek, ktorý rozumie nielen dokonale informačno-komunikačným technológiám, ale má aj značné skúsenosti v riadení rizikových procesov. Požiadavky kladené na MKB sú náročné a naplnenie pracovného času MKB u jedného prevádzkovateľa na plný úväzok je problematické. Preto najschodnejšie riešenie je zabezpečiť si výkon tejto funkcie externým odborníkom, ktorý dokáže dostatočne pokryť tieto široké a komplexné úlohy a nepožaduje plný úväzok.

Základné úlohy MKB:

- Riadenie bezpečnosti
- Manažment hrozieb a rizík
- Aplikácia bezpečnostných opatrení
- Výkon operatívnych bezpečnostných činností
- Riadenie súladu

MKB je jeden zo základných pilierov tvorby bezpečnostných opatrení prevádzkovateľa základnej služby a ich aplikácie do praxe. Mal by detailne poznať zavedené procesy a mal by disponovať dostatočnou znalosťou vnútorných IT procesov. Takisto by mal kontrolovať fungovanie zavedených procesov informačnej bezpečnosti a ich dodržiavanie nielen zamestnancami informatiky, ale aj ostatnými zamestnancami.

Spoločnosť SOMI Systems, a. s., sa informačnej bezpečnosti venuje už 30 rokov. Disponuje tímom certifikovaných odborníkov (certifikát manažéra kybernetickej bezpečnosti pod záštitou NBÚ) a funkciu MKB vykonáva pre viac ako 50 prevádzkovateľov základnej služby naprieč Slovenskom.

Nezabúdajte, že určujúcimi prvkami kybernetickej bezpečnosti sú ľudia, procesy a technológie. Skúsený MKB je zodpovedný za manažment týchto prvkov v širokom kontexte kybernetickej bezpečnosti.

■ RNDr. DANIEL **SCHIKOR,**
Certifikovaný manažér kybernetickej bezpečnosti, www.somi.sk

KONCOVÝ POUŽÍVATEĽ AKO PRVÝ KROK KYBERNETICKEJ BEZPEČNOSTI

Za posledné roky sú phishing a ransomware jednými z hlavných kybernetických útokov, ktorým čelí množstvo podnikov bez ohľadu na ich veľkosť. Práve z tohto dôvodu sú zamestnanci a koncoví používatelia prvou líniou obrany. Aj napriek snahe informovať o dôležitosti implementácie bezpečnostných protiopatrení na zmierňovanie kybernetických incidentov, existuje množstvo podnikov, ktoré nespĺňajú základné požiadavky kybernetickej bezpečnosti.

Počet kybernetických útokov neustále rastie a odhaduje sa, že denne sa vytvorí približne 300 000 nových softvérov škodlivého obsahu, ktorý sa zameriava na jednotlivcov ale aj organizácie. Kybernetické útoky môžu mať rôzne podoby, od využívania ľudského pochybenia až po spustenie sofistikovaných útokov, ktoré sú schopné obísť rôzne bezpečnostné systémy.

Podľa Check Point Research vzrástli kybernetické útoky medziročne o 50%, pričom každá organizácia čelí 925 kybernetickým útokom týždenne na celom svete. Podľa štatistík zaznamenali podniky v roku 2021 o 50 % viac útokov týždenne v porovnaní s rokom 2020. Odhaduje sa, že každý deň je napadnutých v priemere 30 000 webových stránok. V skutočnosti sa spoločnosť stane obeťou kybernetického útoku každých 39 sekúnd a viac ako 60 % organizácií na celom svete zažilo aspoň jednu formu kybernetického útoku.

Podľa Ponemon Institute a IBM's Cost of a Data Breach Report z roku 2021 sa priemerné celkové náklady vzniknuté s porušením ochrany údajov zvýšili z 3,86 milióna USD v roku 2020 na 4,24 milióna USD v roku 2021. Zo správy vyplýva 10 % medziročný nárast priemerných celkových nákladov, čo je najviac za posledných 17 rokov histórie týchto štatistík. Osobné informácie zákazníkov predstavovali najdrahší typ záznamu s priemernou cenou 161 USD za stratený alebo ukradnutý záznam.

Útočníci sa zameriavajú predovšetkým na koncových používateľov a zamestnancov organizácií. Najnovšie štatistiky popisujú, že až 80% útokov je iniciovaných z interného priestoru organizácií pomocou webových kanálov, ktoré sú najčastejšie pre vznik phishingových útokov, napadnutie malvérom alebo napadnutie ransomvérom. Najčastejšie spúšťače týchto útokov sú: e-mail, webový kanál, DNS, SMS, využívanie nezodpovedných a nedôveryhodných kanálov (verejné cloudové úložiská a pod.) a v neposlednom rade aj procesné chyby, ktoré majú za následok únik dát a údajov.

Pre zabezpečenie kybernetickej bezpečnosti na predchádzanie útokom tohto typu je možné implementovať tieto kroky ako prvý krok k zlepšeniu bezpečnosti:

1. Implementácia politík a postupov kybernetickej bezpečnosti

Ak ešte nedisponujete dokumentom, ktorý popisuje postupy a politiky kybernetickej bezpečnosti, je nutné ho vytvoriť a implementovať. Tento dokument by mal obsahovať časti, ktoré podrobne popisujú činnosti v prípade, že sa vaši koncoví používatelia alebo koncové systémy ocitnú pod kybernetickým útokom. Dokument by mal predstavovať príručku s popisom jednotlivých scenárov ako pristupovať k bezpečnostným incidentom.

Uvádzame aj zopár tipov, ako pristupovať k bezpečnostným incidentom:

- Ako prvé, určite odporúčame nepanikáriť
- Je vhodné mať vytvorenú kontaktnú maticu s popisom rolí (koho je potrebné kontaktovať v prípade bezpečnostného incidentu)
- Ďalším krokom je útok Detekovať
- Odpojiť infikované zariadenie od internetu a počítačovej siete (ak je to možné)
- Odkontrolovať dostupné zálohy (Dostupnosť existujúcich záloh a ich stav. Identifikovať či je možné zálohy použiť na obnovenie prevádzky.)
- Systematizovať postup riešenia bezpečnostného incidentu
- Informovať vlastníka firmy, resp. kontaktnú osobu o stave incidentu
- Identifikovať rozsah poškodenia (Je možné využiť dokumentáciu spracovávaných údajov na jednotlivých serveroch a koncových zariadeniach – pokiaľ organizácia disponuje takýmto typom dokumentácie. Je potrebné vedieť aké informácie a údaje potrebujeme nájsť, aby sme identifikovali rozsah poškodenia.)
- Ďalšími krokmi sú kontrola logov a zaistenie stôp
- Zmena všetkých hesiel na všetkých systémoch, prípadne vytvorenie nových certifikátov
- Implementácia obranných opatrení
- Pripojenie k počítačovej sieti a internetu
- Zistenie či nedošlo k úniku dát
- Vypracovať správu o incidente
- Poučenie sa z incidentu

2. Vybudovanie stratégie kybernetickej bezpečnosti založenej na vzdelávaní koncových používateľov

Vzdelávanie je prvoradé pre budovanie úspešnej stratégie. Každý zamestnanec má e-mailovú adresu a prístup na internet. Takáto jednoduchá služba, ktorá je poskytovaná všetkým zamestnancom, bohužiaľ predstavuje približne 80% narušení bezpečnosti, ktoré dnes vidíme. Veľmi zriedka sa stretneme s „Hollywodskou verziou", kde útočník prelomí firewall spoločnosti, aby ohrozil internú sieť. Tento prístup je z pohľadu náročnosti, časovej náročnosti a financií neefektívny a neúmerný. Z pohľadu hackera je oveľa jednoduchšie vygenerovať phishingový e-mail, ktorý rozpošle zamestnancom spoločnosti, aby ich nechal urobiť všetku ťažkú prácu za neho.

3. Zavedenie nástrojov kybernetickej bezpečnosti, ktoré pomáhajú predchádzať potenciálnym incidentom

Vzdelávanie je samozrejme neoddeliteľná súčasť kybernetickej bezpečnosti, avšak ochrana nepochádza len z toho, že koncový používateľ neklikne na odkaz s potencionálnou hrozbou. Zamestnanci sú ľudia, ktorý sa vždy môžu zmýliť. Pre zabránenie a zníženie hrozby zlyhania ľudského faktora je odporúčané disponovať nástrojmi pre podporu kybernetickej bezpečnosti pre prípad, že sa vaši zamestnanci zlyhajú. Nástroje tohto typu povoľujú alebo zakazujú prístup k niektorým webovým lokalitám, prípadne filtrujú e-mailovú prevádzku a odhaľujú vírusy, malvér alebo potencionálny phishinng.

BRAIN:IT

Ing. MICHAL ŠTERBÁK, Manažér kybernetickej bezpečnosti
Úvodné foto zdroj: SHUTTERSTOCK.COM

VZDELÁVANIE 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.

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 hodiny, 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

NEDOSTATKOVÉ ZNALOSTI A SKÚSENOSTI PRACOVNÍKOV KYBERNETICKEJ BEZPEČNOSTI

▪ ZDROJ: SLOVAK BUSINESS AGENCY PRIESKUM STAVU KYBERNETICKEJ BEZPEČNOSTI V SEKTORE MSP

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

CLASHING: ZVÝŠTE POVEDOMIE ZAMESTNANCOV O KYBERNETICKEJ BEZPEČNOSTI

Prečo sú vzdelávacie online hry dobrou prevenciou proti kybernetickým útokom?

Martin Valko: Kybernetické útoky sú v posledných rokoch výrazne sofistikovanejšie a častejšie. Z prieskumov vyplýva, že veľkou slabinou firiem z pohľadu informačnej a kybernetickej bezpečnosti je práve správanie zamestnancov. Systematické a pravidelné vzdelávanie a budovanie povedomia o bezpečnom správaní bežných používateľov v oblasti kybernetickej bezpečnosti je kľúčové z pohľadu eliminovania rizík – či už v rámci organizácie, alebo mimo nej.

Skúsenosti 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 vzory správania.

Čo môžeme zlepšiť v oblasti vzdelávania svojich zamestnancov v informačnej bezpečnosti?

Martin Valko: Je dôležité ľudí motivovať a vzbudiť záujem, aby sami chceli, aby rozumeli, prečo sa majú správať bezpečne a aké následky môže mať ich správanie. Najvyššia méta je, aby sa ľudia bezpečne správali podvedome a automaticky, bez rozmýšľania vedeli, čo majú urobiť. Preto je náš pohľad na oblasť vzdelávania iný. Nesnažíme sa iba posunúť informácie, naším cieľom je meniť podvedomé správanie ľudí. A tak kartový súboj medzi kolegami, ktorý prinesie do vzdelávania emócie, súťaživosť a zábavu, má vysokú šancu zaujať, udržať pozornosť a dosiahnuť, aby ľudia zmenili svoje správanie v online priestore.

Ako podľa vás hra Clashing mení pohľad na firemné školenia?

Martin Valko: Clashing je online kartová hra, ktorá mení pohľad na firemné školenie v oblasti informačnej bezpečnosti pútavým a jednoduchým spracovaním témy, ktorá je pre bežných používateľov príliš vzdialená.

Ide o kartový súboj, v ktorom 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 asi 10 – 15 minút.

Aké témy informačnej a kybernetickej bezpečnosti Clashing pokrýva?

Martin Valko: Aby bolo vzdelávanie pútavé a stručné, rozdelili sme obsah do tematických dejísk, ako napríklad Kancelária, Internet a sociálne siete, Home office alebo Počítač a mobil. V každom dejisku sa používateľ oboznámi s rozličnými nástrahami. Pre začínajúcich hráčov je k dispozícii zjednodušená zá-

kladná verzia hry a pre tých skúsenejších pokročilá s pridanými prvkami. A vždy je obsah v súlade s platnými normami.

Clashing dnes hrá 25 000 používateľov, máme 7 jazykových mutácií a vývoj hry stále pokračuje. Dopĺňajú sa v nej nové karty s aktuálnymi hrozbami a obrannými kartami a pripravujeme ďalšie verzie hry. Naším cieľom je, aby Clashing hrala aj širšia verejnosť, nielen zamestnanci organizácií, čím by sa zvyšovala celková kybernetická gramotnosť.

Uviedli ste, že je dôležitý aj súlad vzdelávacieho obsahu s legislatívou. Ako konkrétne sa to prejavuje v hre Clashing?

Martin Valko: Aby platforma Clashing mala zmysel pre našu cieľovú skupinu spoločností, je dôležitý súlad vzdelávacieho obsahu so zákonom o kybernetickej bezpečnosti alebo normami, ako je ISO 27000 pre systém riadenia informačnej bezpečnosti. Naši konzultanti sa citlivo zamerali na to, aby obsah pokrýval všetky dôležité oblasti a zároveň bol zrozumiteľný bežným používateľom.

Hráči majú k dispozícii unikátne karty, ktoré obsahujú široké spektrum kybernetických útokov, hrozieb z bezpečnosti informácií či fyzických bezpečnostných útokov a reakcií na ne. Hracie karty obsahujú presne tie základné oblasti, na ktoré je dôležité ľudí upozorňovať. Rovnako je dôležitý manažment používateľov a presný prehľad, kto zo zamestnancov školenie absolvoval a kedy. Administrátorské rozhranie Clashingu vám dá práve potrebný prehľad o minulých a prebiehajúcich školeniach.

Pre koho je hra primárne určená? Aké výsledky už priniesla firmám, ktoré vzdelávacou online hrou školia svojich zamestnancov?

Martin Valko: Clashing sa dá jednoducho nasadiť v akejkoľvek spoločnosti, ktorá si uvedomuje dôležitosť zvyšovania povedomia ľudí o kybernetických hrozbách. Cloudová forma umožňuje rýchle nasadenie a integráciu na jednoduché prihlasovanie používateľov.

Aj v menšej firme, ktorá sa dnes vezie na vlne digitalizácie a kde sú dáta cenným aktívom, je dôležité dbať na zásady informačnej bezpečnosti. Pri väčších spoločnostiach by informovanie o hrozbách v kybernetickom priestore a zlepšovanie návykov zamestnancov malo byť samozrejmosťou.

*Clashing naučí zamestnancov ochrániť firmu proti kybernetickým hrozbám a zlepší bezpečnostné návyky ľudí vo vašom tíme. Osvojte si tie správne formy obrany a vyskúšajte demo na **www.clashing.com**.*

Ing. MARTIN VALKO, Business Development Manager spoločnosti ANECT, a. s.

ÚVODNÉ FOTO: **FAUXELS / PEXELS.COM**

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 nesprávne 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.

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.

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.

AK ZAMESTNÁVATEĽ PODCENÍ PREVENCIU, V OKAMIHU PREPUSTENIA ZAMESTNANCA JE PRAKTICKY BEZMOCNÝ.

■ ĽUBOSLAV LACKO , ÚVODNÉ FOTO **COWOMEN** ON UNSPLASH/

OCHRANA 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.

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 au-

toritami, 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.

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. 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. 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. 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.

■ ĽUBOSLAV LACKO
ÚVODNÝ OBRÁZOK **MIKHAIL NILOV** ON PEXELS.COM

FOTO ZDROJ: **DCSTUDIO** ON FREEPIK

ZABEZPEČENIE SIETÍ

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. 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.

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

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.

PHOTO BY PRIVECSTASY ON UNSPLASH.COM

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 otestovať 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. 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.

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.

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
ÚVODNÝ OBRÁZOK **RAWPIXEL.COM ON FREEPIK.COM**

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?

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.

AŽ 40 % **UVIEDLO BEZPEČNOSŤ AKO NAJVÄČŠIU PREKÁŽKU ĎALŠIEHO ROZŠÍRENIA CLOUDU.**

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.

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

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).

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
ÚVODNÝ OBRÁZOK **SHUTTERSTOCK.COM**

PREHĽAD ZÁKONOV A VYHLÁŠOK

Zákon č. 69/2019 Z.z. o kybernetickej bezpečnosti a vykonávacie predpisy.

Tento zákon upravuje

a) organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti,

b) národnú stratégiu kybernetickej bezpečnosti,

c) jednotný informačný systém kybernetickej bezpečnosti,

d) organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT") a ich akreditáciu,

e) postavenie a povinnosti prevádzkovateľa základnej služby a poskytovateľa digitálnej služby,

f) bezpečnostné opatrenia,

g) systém zabezpečenia kybernetickej bezpečnosti,

h) kontrolu nad dodržiavaním tohto zákona a audit.

Kybernetickú bezpečnosť riešia aj ďalšie vyhlášky a zákony:

- **Vyhláška Národného bezpečnostného úradu 362/2018 Z. z.**, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- **Zákon 95/2019 Z. z.** o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
- **Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu 179/2020 Z. z.**, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

NA SLOVENSKU SA KYBERNETICKOU BEZPEČNOSŤOU ZAOBERÁ V SÚČASNOSTI TAKMER TRETINA MALÝCH A STREDNÝCH PODNIKATEĽOV (31,3 %) NAPRIEK TOMU, ŽE IM TO LEGISLATÍVA NEPRIKAZUJE. DVE TRETINY MSP SA KYBERNETICKOU BEZPEČNOSŤOU NEZAOBERAJÚ (66,3 %). DVE PERCENTÁ (2,4 %) MALÝCH A STREDNÝCH PODNIKATEĽOV NEMÁ JASNÚ PREDSTAVU, ČO TO KYBERNETICKÁ BEZPEČNOSŤ JE.

Zdroj: Slovak Business Agency Prieskum stavu kybernetickej bezpečnosti v sektore MSP

BEZPEČNOSTNÁ IT POLITIKA VO FIRME

TYPY POLITÍK, BEZPEČNOSTNÝ PROJEKT, URČENIE ZODPOVEDNOSTI VEDÚCICH ZAMESTNANCOV

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 časť tá 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.

Kybernetická bezpečnosť 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.

Kybernetická bezpečnosť 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 definované bezpečnostné politiky riešia hlavne prevenciu proti útokom na ktorýkoľvek podsystém alebo komponent informačného systému, či už ide o útoky z

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.

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.

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.

INTERNÉ SMERNICE

Firmy a organizácie by mali mať záväzné interné smernice schválene vedením spoločnosti, ktoré upravujú niektoré práva a povinnosti všetkých zamestnancov, prípadne aj zmluvných partnerov v oblasti ochrany informačných aktív, hlavne čo sa týka spracúvaných osobných a iných citlivých údajov v informačných systémoch. V podstate sa jedná o vykonávací predpis legislatívnych požiadaviek definovaných zákonom č. 69/2019 Z.z. o kybernetickej bezpečnosti s ohľadom na špecifické podmienky organizácie.

Smernice by mali 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. Smernice by zároveň mali poskytnúť odpovede na základné okruhy otázok:

- 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 smernice či projekty 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.

ŠTRUKTÚRA BEZPEČNOSTNÝCH POLITÍK

Štruktúru bezpečnostných politík definuje Príloha č. 1 k Vyhláške Národného bezpečnostného úradu č. 362/2018 Z. z *(pozri tabulku č. 1)*.

Ak je v článku uvedená iná štruktúra, založená na subjektívnom vnímaní autora, povedie to ku zmäteniu čitateľov. Ak títo sú povinnými osobami zo zákona, môže to viesť až k nesúladu.

Pri definovaní bezpečnostnej politiky v podnikovej praxi sa osvedčili tieto kroky

- **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

Bezpečnostné politiky	Súvisiace bezpečnostné štandardy
1. Organizácia bezpečnosti	• Riadenie bezpečnostnej architektúry • Systém riadenia kybernetickej bezpečnosti • Riadenie identít a prístupových práv • Riadenie privilegovaných prístupov • Bezpečnostný monitoring a správa bezpečnostných záznamov
2. Riadenie bezpečnostných rizík	• Testovanie a bezpečnostná certifikácia systémov • Metodika posudzovania vplyvu na ochranu osobných údajov • Metodika posudzovania rizík • Fyzická bezpečnosť a bezpečnosť prostredia • Riešenie bezpečnostných incidentov
3. Riadenie informačných aktív	• Klasifikácia informácií a kategorizácia sietí • Registratúrny poriadok a registratúrny plán
4. Pravidlá správania a dobrej praxe	• Práca na diaľku a používanie mobilných zariadení • Riadenie personálnej bezpečnosti • Pravidlá komunikácie
5. Riadenie dodávateľských vzťahov	• Riadenie dodávateľských služieb • Akvizícia informačných systémov
6. Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií	• Vývoj a testovanie informačných systémov • Postupy údržby informačných systémov Riadenie technických zraniteľností a manažment záplat
7. Riadenie a prevádzka informačno - komunikačných technológií	• Pravidlá prepájania systémov a prenosu elektronických informácií • Riadenie bezpečnosti sietí • Riadenie zmien infraštruktúry • Riadenie kapacity systémov a služieb • Riadenie kryptografických opatrení
8. Riadenie súladu	• Audit kybernetickej bezpečnosti • Spracúvanie osobných údajov a klasifikovaných informácií • Poskytovanie súčinnosti tretím stranám
9. Riadenie kontinuity procesov a činností	• Plány kontinuity prevádzkových činností • Plány havarijnej obnovy prevádzky • Metodika zálohovania a obnovy informácií

Tabuľka č. 1

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

Dobrou inšpiráciou pre vypracovanie bezpečnostného projektu firmy sú pokyny v prílohe č. 3. Vyhlášky 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, kde je vypracovanie bezpečnostného projektu vyžadované legislatívou.

Bezpečnostný projekt IS pozostáva z dvoch hlavných výstupov: **bezpečnostného zámeru** a **analýzy bezpečnosti**.

Bezpečnostný zámer

určuje kontext a zameranie bezpečnostného projektu a mal by obsahovať:

- formuláciu základných bezpečnostných cieľov vyplývajúcich z relevantných právnych východísk vrátane interných predpisov, technických noriem a štandardov dobrej praxe,
- zoznam právnych predpisov aplikovaných v bezpečnostnom projekte, ako aj interných riadiacich aktov,
- metodický prístup ku kvalitatívnej analýze rizík, ktorá je v bezpečnostnom projekte vykonaná,
- rámcovú špecifikáciu technických opatrení, organizačných opatrení a personálnych opatrení na zabezpečenie ochrany IS, jeho služieb a údajov v ňom spracúvaných s ohľadom na kategóriu, do ktorej je informačný systém zaradený,
- vymedzenie okolia IS a jeho vzťah k možnému narušeniu bezpečnosti vrátane zoznamu integrácií na informačný systém,
- vymedzenie kritérií na akceptáciu rizika a identifikovaných prijateľných úrovní rizika,
- ohraničenia bezpečnostného projektu (explicitné vysvetlenie oblastí, ktoré bezpečnostný projekt nezahŕňa alebo kladie požiadavky na ich riešenie mimo projektu IS),
- postupy revízie/aktualizácie bezpečnostného zámeru.

Analýza bezpečnosti

jej súčasťou je kvalitatívna analýza rizík. Rizikom sa v bezpečnostnom projekte chápe miera kybernetického ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami. Analýza rizík je zameraná na získanie aktuálnych a vierohodných poznatkov o pravdepodobných rizikách týkajúcich sa aktív informačného systému a jeho okolia. Analýza rizík sa vykonáva pre IS počas celého projektu v súlade so zákonom a priamo nadväzuje na dokument bezpečnostný zámer. Analýza rizík pozostáva z výkonu týchto činností:

- vytvorenie podkladových katalógov na analyzované riziká určených na identifikáciu aktív, identifikáciu hrozieb a zraniteľností a identifikáciu vplyvov,
- identifikácia a opis analyzovaných rizík v štruktúre podľa oblastí ustanovených osobitným predpisom alebo podľa technickej normy,
- priradenie aktív, hrozieb, zraniteľností a vplyvov ku každému z identifikovaných rizík,
- identifikácia realizovaných bezpečnostných opatrení,
- vyhodnotenie rizík spôsobom kombinácie pravdepodobnosti realizácie scenáru rizika a závažnosti vplyvu,
- opis navrhovaných bezpečnostných opatrení.

Pri každom riziku sa zohľadňuje pravdepodobnosť situácie, pri ktorej hrozby využijú existujúce zraniteľnosti a spôsobia negatívny vplyv na aktíva orgánu riadenia. Pri hodnotení závažnosti výsledného vplyvu sa zohľadňuje celková závažnosť vplyvov, ktoré môžu byť spôsobené pri realizácii rizika. Úroveň vplyvov sa určuje osobitne pre každé analyzované riziko a zahŕňa

všetky aktíva dotknuté príslušným rizikom. Výsledná miera rizika musí zohľadňovať aj všetky realizované bezpečnostné opatrenia.

Metodický postup výkonu analýzy rizík musí byť v súlade s technickou normou, napríklad STN EN ISO/IEC 27002 Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti (ISO/IEC 27002) (36 9784).

Výsledné vyhodnotenie rizík podľa použitej metodiky musí byť premietnuté do trojstupňovej stupnice nízke riziko, stredné riziko, vysoké riziko.

Pri tvorbe navrhovaných bezpečnostných opatrení je potrebné určiť prostriedky a procesy odstraňovania nedostatkov zistených v rámci jednotlivých rizík. Cieľom návrhu bezpečnostných opatrení je vytvorenie takého okruhu bezpečnostných opatrení, že po ich implementácii a následnom prehodnotení rizík sú všetky zvyškové riziká akceptovateľné.

Opis navrhovaných bezpečnostných opatrení zohľadňuje:

- opatrenia ustanovené legislatívou
- náležitosti implementácie a prevádzky analyzovaného IS a spôsob uplatňovania bezpečnostných opatrení v konkrétnych podmienkach orgánu riadenia,
- opatrenia realizovateľné v pôsobnosti analyzovaného IS, ale aj opatrenia vo vzťahu k jeho okoliu,
- dostupné možnosti prístupu k riadeniu rizika,
- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení.

Výstupný dokument analýzy bezpečnosti s výsledkami analýzy rizík obsahuje najmä

- ciele a priority analýzy rizík,
- opis použitej metodiky analýzy rizík,
- opis rizík založený na identifikácii aktív, identifikácii hrozieb pre tieto aktíva, identifikácii zraniteľností a na identifikácii vplyvov na aktíva najmä v dôsledku straty dôvernosti, integrity a dostupnosti,
- vyhodnotenie rizík podľa použitej metodiky,
- opis navrhovaných bezpečnostných opatrení pre identifikované riziká v závislosti od ich závažnosti,
- celkové zhrnutie výsledkov analýzy rizík, vrátane zoznamu vysokých a stredných rizík usporiadaných podľa dôležitosti, s opisom navrhovaného postupu ich riadenia a kľúčových navrhovaných bezpečnostných opatrení,
- postupy revízie/aktualizácie analýzy bezpečnosti.

Bezpečnostný projekt verejnej správy musí obsahovať všetky náležitosti, ktoré mu ukladá legislatívna.

Bezpečnostný projekt firmy by mal 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
PHOTO BY **FAUXELS** ON PEXELS.COM/

DODRŽIAVANIE 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.

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

Vynútenie dodržiavania bezpečnostných politík je zakomponované aj do medzinárodného štandardu ISO/IEC 29146:2016 Information technology — Security techniques — A framework for access management, pričom táto norma definuje politiky v kontexte riadenia prístupov. Norma 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. 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. ■

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.

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**

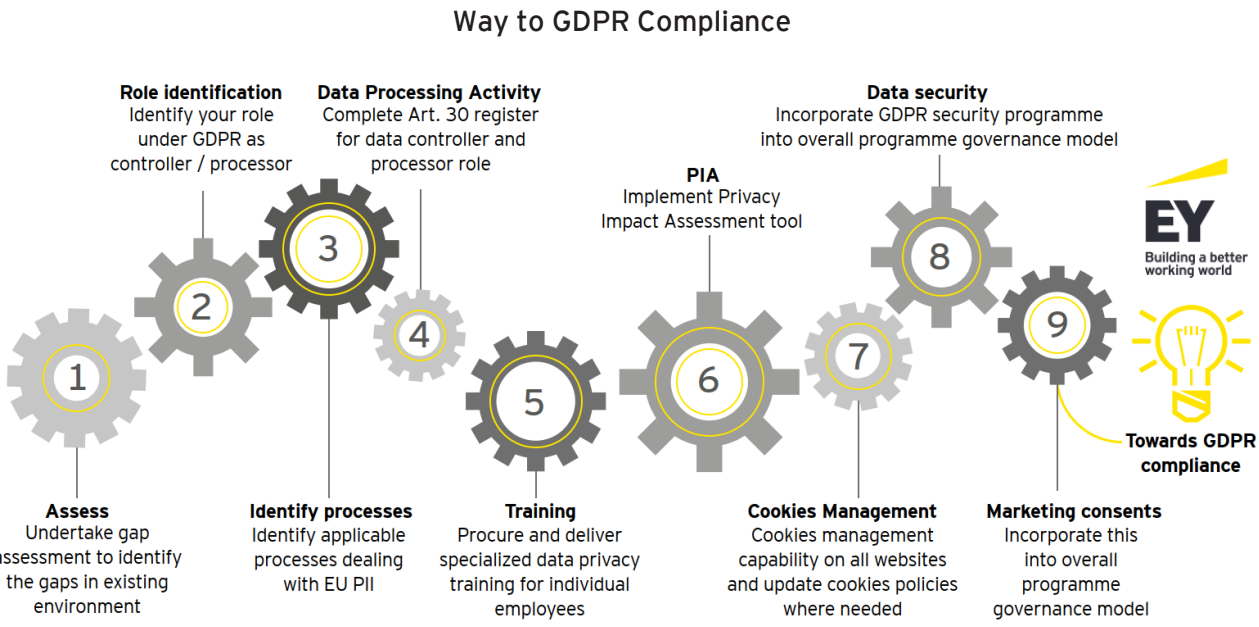
Ak niekto potrebuje spracúvať osobné údaje, mal by si ozrejmiť, na základe ktorého dôvodu to môže robiť, a ak nenájde iný dôvod mimo súhlasu, bude musieť spracovávať osobné údaje na základe súhlasu dotknutej osoby. Praktická realizácia súhlasu môže byť napríklad zaškrtávacie políčko vo formulári na webovej 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. 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" 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 zodpovedať 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
ÚVODNÝ OBRÁZOK **SHUTTERSTOCK.COM**

EY Building a better working world

„Analýza rizík by mala s výhodou využiť informácie o vyriešených incidentoch z minulosti, prípadne o incidentoch alebo rizikových faktoroch, ktoré na údaje aktuálne pôsobia. Odporúčame zamyslieť sa nielen nad triviálnym kritériom, teda akú vysokú pokutu by ste podľa GDPR za súčasný stav zaplatili, ale aj 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."

Juraj Richter, senior manažér na oddelení poradenstva, EY

365.bank
Dvořákovo náb. 4
811 02 Bratislava
www.365.bank

Alanata a.s.
Krasovského 14
851 01 Bratislava
www.alanata.sk

ALISON Slovakia s.r.o.
Tomášikova ulica 64
831 04 Bratislava
www.alison-group.sk

Aliter Technologies, a.s.
TRADE CENTER II,
Mlynské Nivy 71
821 05 Bratislava
www.aliter.com

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

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

auditori.it, s.r.o.
Bottova 2A
811 09 Bratislava - Staré mesto
www.auditori.it
info@auditori.it

brainit.sk, s.r.o.
Veľký Diel 3323, 010 08 Žilina
info@brainit.sk
www.brainit.sk

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

ECTA, s.r.o.
Révová 7, 811 02 Bratislava
info@ecta.sk
www.ecta.sk

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

Exclusive Networks Slovakia s.r.o.
Galvaniho 7D, 821 04 Bratislava
info@exclusive-networks.sk
www.exclusive-networks.sk

Ernst & Young, s. r. o.
Žižkova 9, 811 02 Bratislava
ey@sk.ey.com
www.ey.com/sk_sk

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

HP Inc Slovakia, s.r.o.
Galvániho 7
820 02 Bratislava 22
www.hp.sk

INDRA Slovakia,a.s.
Westend Plazza
Lamačská cesta 3/B
841 01 Bratislava

LYNX s.r.o.
Jelačičova 8A
821 08 Bratislava
www.lynx.sk

MIM, s.r.o.
Slnečná 211/1, 010 03 Žilina
Hraničná 18, 821 05 Bratislava
info@mim.sk, www.mim.sk

PricewaterhouseCoopers Slovensko, s.r.o.
Twin City A, Karadžičova 2
815 32 Bratislava
www.pwc.com/sk

SAFELab.sk - IT bezpečnosť
Klincová 37/B
821 08 Bratislava
www.safelab.sk

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

NEXTECH
Mliekarenská 10
821 09 Bratislava
www.nextech.sk

ZOZNAM POUŽITEJ LITERATÚRY:

- Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2021. NBU, 2022
- Krátky úvod do informačnej a kybernetickej bezpečnosti a Malý výkladový slovník. MIRRI, 2022
- Gruber, D – Ludell, B.: Security Megatrends and Their Impact on Endpoint Security. IBM 2021
- Prieskum stavu kybernetickej bezpečnosti v sektore MSP. Slovak Business Agency, 2022
- Firemná literatúra ESET, AV

PREDPLATNÉ NA ROK 2023

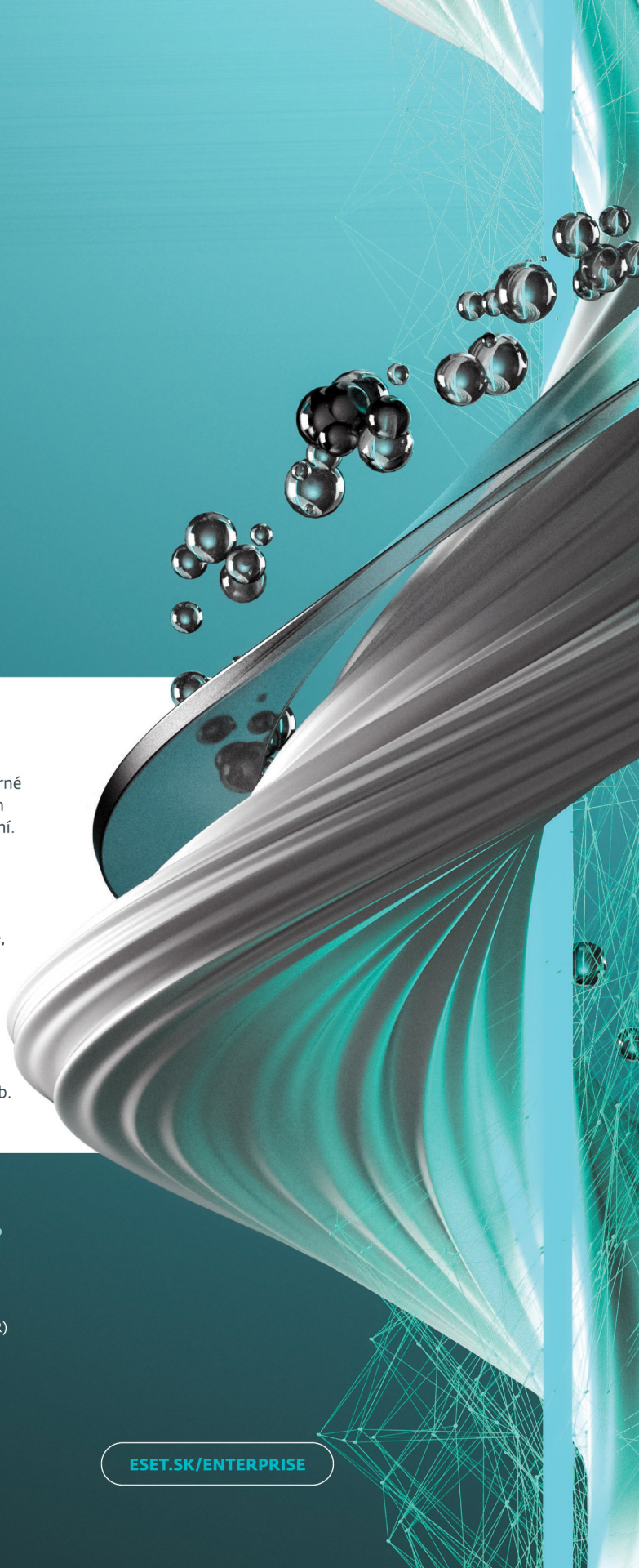
UŽ OD 12 € NA CELÝ ROK!

PREDPLATNÉ	Print	Web	PDF	SUMA
NEXTECH komplet	✓	✓	✓	**30 €**
NEXTECH print	✓			28 €
NEXTECH digital		✓	✓	20 €
NEXTECH PDF			✓	15 €
NEXTECH web		✓		12 €

Objednávky: **www.nextech.sk**, e-mail: **predplatne@nextech.sk**

PROTECT MDR

Špičková bezpečnostná technológia pre firmy skombinovaná so službami poskytovanými priamo expertmi spoločnosti ESET.



ESET PROTECT MDR poskytuje ochranu najmodernejšími technológiami obohatenú o neustále dostupnú podporu od špecialistov spoločnosti ESET a ich bezkonkurenčné odborné znalosti. Firmy majú s týmto produktovo-službovým balíkom istotu maximálneho využitia všetkých bezpečnostných riešení.

Vo svete dynamicky sa vyvíjajúcich hrozieb je kľúčové komplexné zabezpečenie celej firmy tak, aby sa nenašla ani jedna bezpečnostná medzera, ktorú by využili útočníci. Mnohé spoločnosti síce majú sofistikované obranné nástroje, no chýbajú im špecialisti, ktorí ich dokážu správne ovládať. Konzola na správu bezpečnosti ESET PROTECT, jednotná platforma na správu zabezpečenia s možnosťami rozšírenej detekcie a reakcie (XDR), ponúka dokonalý prehľad o dianí na celej sieti a služby riadenej detekcie a reakcie (MDR) pod dohľadom odborníkov spoločnosti ESET sa postarajú o proaktívne vyhľadávanie a monitorovanie hrozieb.

- Nasadenie prostredníctvom cloudu alebo lokálnej konzoly
- Prémiová podpora
- Rozšírená detekcia a reakcia (XDR)

Progress. Protected.

ESET.SK/ENTERPRISE