Už je to tu. Bezpečnosť v dobe cloudovej je iná

FIRMY

Ešte donedávna bol status quo taký, že informačná bezpečnosť sa primárne sústreďovala na problémy s infraštruktúrou inštalovanou v priestoroch spoločnosti. Nasleduje však grandiózna zmena.

Presun do cloudu prináša výhody a ďalšie príležitosti a zároveň riziká, ktoré treba zohľadniť. SNÍMKA: DREAMSTIME

Vostatnej dekáde niektoré spoločnosti aj začali transformačné projekty smerujúce do cloudu, keďže tam videli potenciál, ale tieto iniciatívy boli viac-menej považované za tieňové IT. A to, samozrejme, znamenalo bezpečnostné riziká.

Všetko sa však veľmi zmenilo minulý rok. Rok 2020 bol rokom, keď sa veľká časť organizácií snažila vymyslieť spôsob, ako efektívnejšie pracovať a vytvárať priestor na spoluprácu svojich zamestnancov.

A tu sa jednoznačne ukazuje výhoda cloudu. Zvládnuť takýto prechod bezpečne si však vyžaduje trochu viac než iba objednať si danú službu a začať ju využívať. Ako teda na to?

Vhodné riadenie a kontrola
Posun do cloudu by sa mal udiať bezpečne. A na to je nevyhnutné, aby organizácie dovolili svojim bezpečnostným tímom včas implementovať dostatočné riadenie a kontrolu cloudového prostredia a považovali bezpečnosť za prvoradú pri prechode do cloudu.

Identifikácia súčasného stavu
Pochopiť a kvantifikovať riziká v súčasnej infraštruktúre verejného cloudu je dôležité nielen z hľadiska bezpečnosti, ale aj riadenia efektívneho využívania zdrojov, ktoré sa premieta do nákladov pre organizáciu.

Nečakajte, až sa zlepší situácia na trhu práce
Je luxusom čakať na to, kým sa vytvoria tímy bezpečnostných profesionálov so špecializáciou na cloud, aj keď to by mal byť dlhodobý cieľ. Teraz musíme hľadať cesty, ako redukovať riziká, kým sa tento dlhodobý cieľ stane skutočnosťou.

Cloudová infraštruktúra je viac a viac z pohľadu zákazníka vnímaná ako kód, preto integrujte svoje tímy v súlade s prístupom vývoj – bezpečnosť – prevádzka. Ide o prístup, keď sú všetky tieto oblasti zahrnuté do vývoja, napríklad aplikácie, aby sa včas identifikovali a eliminovali nedostatky a slabé miesta z pohľadu bezpečnosti a prevádzky.

Technológia musí pracovať pre vás
Využitie technológie bez ohľadu na to, akú máte rozsiahlu organizačnú infraštruktúru. Rozhodne nie je efektívne využívať kapacitu špecialistov na to, čo môžete automatizovať s použitím existujúcich alebo modifikovaných pracovných postupov.

Mali by ste využiť akúkoľvek dostupnú technológiu, ktorú ste schopní zakomponovať do existujúcich procesov a riadiť súčasným personálom. Ako nevyhnutná sa ukazuje práve integrácia s infraštruktúrou ako kód.

V praxi sa to realizuje systémom prideľovania úloh v riadení bezpečnostných informácií a udalostí (SIEM) a, samozrejme, kontrolou prístupu založenou na plnených úlohách (RBAC) spojenými s precíznym riadením rolí a zodpovedností.

> Využitie technológie bez ohľadu na to, akú máte rozsiahlu organizačnú infraštruktúru.
>
> **Daniel Suchý,** bezpečnostný špecialista Aliter Technologies

Neverte univerzálnym riešeniam
Nesnažte sa nájsť jeden nástroj, ktorý vie robiť všetko. S tým, ako rastie cloud, tak rastie aj trh s podpornými nástrojmi a nie zriedka sa stretávame s riešeniami všetko v jednom. Kde všetko veľakrát znamená, že nič nie je poriadne.

I keď si to vyžaduje zvýšené úsilie, je potrebné hľadať riešenia, ktoré zodpovedajú vašim požiadavkám a ponúkajú to najlepšie na trhu v danej oblasti. Takýmto spôsobom si viete vyskladať to najlepšie riešenie pre seba.

Rozdiel medzi úspechom a katastrofou
Cloud sa dynamicky vyvíja a veľakrát poskytuje značnú konkurenčnú výhodu pre organizácie, ktoré sú schopné bezpečne ho implementovať a integrovať do procesov. Avšak slovo bezpečne by sa nemalo nikdy vytratiť, pretože toto slovo je veľakrát jediný rozdiel medzi úspechom a katastrofou.

PRAX

Ako si môžu pomôcť obce a malé mestá

Kybernetické útoky za nevyhýbajú ani Slovensku a už vôbec nie mestám a obciam.

„V praxi sa stretávame s phishingovými mailami hromadne rozposielanými zamestnancom, krádežami identity na sociálnych sieťach či hackerskými útokmi na úrady a firmy," upozorňuje certifikovaný audítor kybernetickej bezpečnosti Michal Ďorda zo spoločnosti auditori.it.

Krajina malých obcí
Mestá a obce majú povinnosť urobiť audit kybernetickej bezpečnosti nielen preto, aby mali formálny papier, ale najmä aby chránili bezpečnosť obyvateľov.

„Je však obrovský rozdiel medzi obcou s tisíckou obyvateľov či mestom s desaťtisíc obyvateľmi, alebo bratislavskou mestskou časťou," hovorí na základe skúsenosti z terénu bezpečnostný špecialista Alison Slovakia Miroslav Macko. Technické a personálne vybavenie či bezpečnostné povedomie je diametrálne odlišné, ale povinnosť majú rovnakú.

Samohodnotenie
Preto bolo novelizáciou zavedené samohodnotenie. Účelom je zjednodušiť splnenie zákonnej povinnosti malým a menším poskytovateľom základnej služby. Tým, ktorí majú povinnosť auditu, ale ich informačný systém nepredstavuje úplne sofistikovanú architektúru.

Formulár k samohodnoteniu je od novembra dostupný na webovej stránke Národného bezpečnostného úradu.

Michal Ďorda však upozorňuje: „Samohodnotenie je možné realizovať len za určitých podmienok." Obec musí mať určeného manažéra kybernetickej bezpečnosti a nesmie mať informačný systém III. kategórie.

Náročné úlohy
Zodpovednosť za riadenie kybernetickej bezpečnosti má vždy prevádzkovateľ základnej služby a jeho štatutárny orgán, čiže starostovia a primátori.

Pochopiteľne, úlohy, ktoré si vyžadujú odborné spôsobilosti, je možné realizovať aj využitím dodávateľských služieb. Nie je však možné na dodávateľa preniesť zákonom stanovené povinnosti.

Fakty a dokumenty
Dotazník samohodnotenia na základe aktuálneho stavu vypĺňa manažér kybernetickej bezpečnosti pravdivo a tak, aby bolo možné uvedené tvrdenia v prípade potreby preveriť.

Štátna autorita odporúča pripojiť aj dokumenty podporujúce tvrdenia. Zároveň je potrebné pridať aj plán implementácie opatrení kybernetickej bezpečnosti na nasledujúce obdobie schválený štatutárom.

Vyplnený formulár s plánom implementácie treba podpísať kvalifikovaným elektronickým podpisom a doručiť Národnému bezpečnostnému úradu.

Dobrá robota
Poctivo spravené samohodnotenie spolu s prijatým plánom opatrení a jeho realizáciou dokáže v malej obci zastúpiť náročný audit kybernetickej bezpečnosti.

„Na audite ušetrené prostriedky sa dajú investovať do budovania či zvyšovania bezpečnostného povedomia zamestnancov spolu s procesnými a technickými opatreniami v praxi," uzatvára Miroslav Macko. Práve to, že používatelia nesprávne používajú IT zariadenia, je podľa prieskumov najčastejším vektorom útokov na Slovensku.

Máme viacej ako 2800 obcí a miest, kde žije menej ako desaťtisíc obyvateľov. SNÍMKA: DREAMSTIME

TRENDY

Menia sa pravidlá a dnes rýchlejší vyhrávajú nad silnejšími

Rozšírená a virtuálna realita nám otvára bránu do kybernetického sveta, v ktorom umelá inteligencia dokáže predpovedať budúcnosť alebo vdýchnuť pomyselný život do chladného železa.

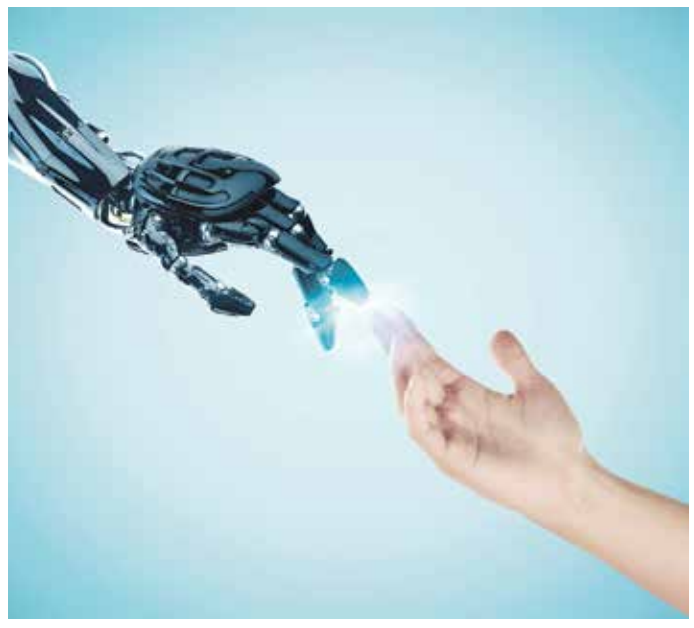
Robotika je novým odvetvím, ktoré nám sľubuje blahobyt. Najväčšími hrozbami sa stávajú útoky hackerov, ktorých sa môžeme obávať aj vo fyzickom svete. Získanie veľkých dát predstavuje ohromné bohatstvo a matematici sú znovu v kurze. Nové platidlá negarantujú banky hmotným bohatstvom a ani rezervami.

Yuval Harari, profesor histórie na Jeruzalemskej univerzite, predpovedá novú éru vývoja človeka – Homo deus, kde technológie budú súčasťou človečenstva.

Áno, život menia technológie, ktoré sa dostávajú aj na menej očakávané miesta, akými sú umenie, šport, výchova. Kto adoptuje nové technológie, prežije. Ochránia vás napríklad pred sofistikovanými kybernetickými útokmi hackerov, ale aj pred primitívnym útokom vandalov.

Predstavte si technológiu, ktorá by chránila váš príbytok tak, že umožní vstup len známym osobám. O neznámej osobe by vás proaktívne informovala a dvere by sa otvorili len overenej osobe. V prípade, že by sa v okolí objavili viaceré neznáme osoby, dostali by ste počet a opis osôb.

Mám na mysli nový technologický startup priamo z MIT, za ktorým stojí slávna investičná skupina Sequoia. Investori, ktorí stáli pri úspechu firiem ako Apple, PayPal, Oracle, Instagram, LinkedIn, WhatsUp, Zoom či Cisco Meraki, sa najnovšie rozhodli podporiť firmu Verkada.



Umelá inteligencia je na ceste stať sa hlavnou technológiou budúcnosti. SNÍMKA: DREAMSTIME

Verkada je systém, ktorý využíva umelú inteligenciu na spracovanie zvukového a obrazového záznamu nielen na detekciu, ale hlavne na prevenciu pred nebezpečenstvom. Jeho integrácia na alarmy, senzory, kamery a manažment vstupu vytvára nepreniknuteľnú bariéru pre podozrivé osoby alebo vozidlá.

Predstavte si proaktívne vyhľadávanie ľudí na základe farby trička alebo pohlavia, vozidlá zas na základe továrenského typu. To všetko bez nutnosti vytvárania dátového centra a drahých serverov, diskových polí, switchov alebo firewallov.

Pamätám sa na jeden príklad, kde zákazníkovi ukradli zlodeji „poolové" auto. Služobné vozidlo, ktoré si zamestnanec mohol na deň požičať, stálo počas karantény v garáži. Samozrejme, všetko zabezpečené, pod kamerou. Službukonajúci bezpečnostný operátor si ani nevšimol v húfe malých obrazoviek na monitore, že sa niečo deje. O krádeži sa dozvedeli až po skončení karantény.

Teraz si predstavte systém, ktorý by vám poslal notifikáciu hneď, ako si do auta sadá neznáma osoba a odchádza.

Thomas Friedman vo svojej knihe Zem je plochá napísal, že naše storočie nebude priať silným tak, ako diktovala história. Budúcnosť praje pripraveným, ktorí dokážu rýchlo adoptovať najnovšie technológie. **Andrej Aleksiev**

Scenáre, ktoré by sme nemali zažiť

ANKETA

Vedia veľa o tom, čo nás ohrozuje, a robia všetko pre to, aby zabránili stratám a ujmám. Ako vyzerá nočná mora profesionálov kybernetickej bezpečnosti?

Rastislav Janota,
riaditeľ,
Národné centrum kybernetickej bezpečnosti SK-CERT

Nikto z vás by sa nechcel zobudiť na to, že mu zaklope na dvere polícia, že z jeho počítača bol vedený útok. Alebo z inej oblasti – lekár na pohotovosti sa spolieha na zdravotný záznam o vašej krvnej skupine. Čo keď ho však v systéme niekto zmení?

Ján Adamovský,
riaditeľ bezpečnosti,
Slovenská sporiteľňa

V noci zazvoní telefón a v ňom sa ozve: „Asi máme nejaký vírus, nič nám nefunguje, ani výroba, ani distribúcia, stratili sme aj zmluvy... niekto chce výkupné milión v bitcoinoch.“ „A čo zálohy?“ spýtate sa. „Zálohy, tie sme plánovali tento rok začať robiť...“ Situácia, ktorá môže zruinovať veľmi solídne rozbehnutú firmu doslova v priebehu minút. Spýtajte sa aj v tej vašej, ako ste na ransomvér pripravení.

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

Najväčšia nočná mora pre bezpečáka je ignorancia bezpečnosti ako takej zo strany vedenia organizácie a nezáujem investovať do bezpečnosti. A to vrátane budovania bezpečnostného povedomia firmy. Pre mňa osobne sú to dve mory, ktoré idú ruka v ruke. Jednou je obava, že niekto ťahá citlivé údaje z organizácie a ja o tom neviem. Druhá je, ak mi niekto znefunkční a odstaví systém a dáta. Aj keď systém obnovím, reputácia už, žiaľ, ostáva pošramotená.

Ján Lichvár,
konateľ, Axenta, s. r. o.

Zasiahol vás útok? Komunikujte! To je jedna z najdôležitejších zásad, keď vám opatrenia nestačia a ocitnete sa v „tme“. Rýchla komunikácia s partnermi – dodávateľmi, odberateľmi, autoritami – vám pomôže vyriešiť problém a zmenší stále prítomné hrozby. Získate tak čas potrebný na zlepšenie opatrení a znížite riziko do budúcnosti. Vychádzam z reálnych skúseností, že na Slovensku sa všetci snažia veci ututlať a nerozprávajú o prienikoch, hrozbách, aby sa sami a aj druhí poučili.

Július Selecký,
senior technický špecialista,
ESET, spol. s r. o.

Keďže sa celý pracovný život pohybujem v IT security, je táto otázka na samostatný článok :). Zničujúca je kombinácia ransomvéru a útoku na dodávateľský reťazec v hybridnom režime fungovania na pracovisku. Následkom môže byť výrazné narušenie bezpečnosti údajov, únik dát, poškodenie dobrého mena až zastavenie prevádzky. V súčasnej situácii by takýto útok na nemocnice mohol viesť až k ohrozeniu životov.

Tomáš Zaťko,
CEO, etický hacker,
Citadelo

399: Je rok 2023. Telefón mi oznámil, že moje najchúlostivejšie dáta sú vonku. Interné firemné dokumenty? Nahaté fotky? Osobné a finančné údaje o mojich zákazníkoch? To, čo najviac zabolí práve mňa, precízne vybrala umelá inteligencia. Trafila sa. Vidím dôkaz, že moje dáta sú naozaj u útočníka. Vidím zoznam kontaktov, ktoré k mojim dátam dostanú prístup, ak nesplním rozkazy útočníka. Šaliem od zlosti.

Roman Varga,
manažér kybernetickej bezpečnosti,
Dôvera zdravotná poisťovňa, a. s.

Prekonaná kyberobrana a cielený útok na systémy zdravotnej starostlivosti sa dotknú toho najcennejšieho a môžu mať fatálne následky. Ako by sme reagovali, ak by útočník zverejnil naše citlivé zdravotné informácie na internete? Nočnou morou je nenávratný výmaz zdravotných záznamov alebo ich pozmenenie pred operáciou. Po úspešnom kyberútoku môže byť obmedzená starostlivosť týždne až mesiace.

Andrej Aleksiev,
riaditeľ slovenskej pobočky,
Check Point Software Technologies

Dodnes ma prekvapuje, ako veríme internetu a koľko dát sme ochotní zdielať so sociálnymi sieťami. Nielen preto, že spomínané informácie sa môžu zneužiť pri phishingových útokoch, ale z dôvodu narastajúcej hrozby krádeže identity. Nikdy nebolo ľahšie získať úver online, tak ako získať osobné dáta záujemcov o finančnú pôžičku.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Európa je konfrontovaná radom bezpečnostných hrozieb, kyberterorizmom či premyslenými útokmi na kritickú infraštruktúru. Čoraz viac otvorene zaznieva, že masívnejšie útoky môžu byť sponzorované priamo štátmi. Európska komisia s podporou Europolu pokračuje v prijímaní zásadných rozhodnutí, týkajúcich sa online terorizmu aj bezpečnosti volieb. Nočnou morou profesionálov je, ak sa zodpovední tvária, že táto téma neexistuje.

Diana Legdanová,
vedúca úseku bezpečnosti,
Vychodoslovenská energetika Holding, a. s.

Stať sa môže všeličo, scenáre sú rôzne. Nočné mory sú asi rovnaké, či už v priváte alebo biznise, len majú iný rozmer a rozsah. Pocit je však úplne ten istý. Najhoršia je bezmocnosť, keď útočník ovládne váš priestor. Neviete, kto to je, kde je, čo všetko vie, ako hlboko je a čo má v pláne. Nemáte situáciu pod kontrolou, neviete, akými zbraňami bojovať. Príde strach, neistota, chyby. Želaný stav je presný opak.

Tomáš Hettych,
viceprezident,
ISACA

Falošný pocit bezpečia vo viacerých rovinách. „Nám sa nemôže nič stať“ – čiže dramatické podceňovanie následkov kybernetických incidentov. „Papiere to vyriešia“ – vnímanie bezpečnosti len ako potrebnej dokumentácie, bez procesov a nástrojov. „Hádam to nie je až také zlé“ – nesprávna interpretácia výsledkov analýz a auditov. „Dodávateľ to vyrieši“ – presun výkonu aj zodpovednosti na tretie strany.
Výsledky auditov ukazujú, že tieto skutočnosti platia rovnako pre verejný aj súkromný sektor.

Peter Katrinec,
obchodný manažér,
Flowmon a CEO bug bounty platformy Hacktrophy

Apatia, strach z neznámeho a nekomunikovanie o kybernetickej bezpečnosti. Stav, keď má spoločnosť hlavu v piesku, ale telo v reálnom svete. Vtedy sa zlí hackeri tešia, lebo o ich činnostiach ani nevieme a odhaľujeme incidenty príliš neskoro. Za najdôležitejšie považujem zdieľanie poznatkov a zároveň schopnosť tie informácie prijímať a riešiť. V osobnom živote je nočnou morou nepochybne krádež prístupu do vlastného password manažéra.

Peter Dostál,
generálny riaditeľ a predseda Dozornej rady,
Aliter Technologies, a. s.

Vzhľadom na určenie systémov, o ktoré sa staráme pre našich zákazníkov, nemôžem hovoriť o konkrétnych dosahoch. Ale skúste si hypoteticky predstaviť, že niekto vymení v systéme na zobrazenie spriatelených a nepriateľských síl identifikované objekty. No dôvodom na nočné mory môže byť aj menšia udalosť, ako napríklad dlhé rady nespokojných ľudí čakajúcich na vydanie dokladu alebo nevyplatené mzdy.

Ivan Kopáčik,
bezpečnostný expert, Gordias, s. r. o.

Jedného dňa zistíte, že máte vo svojej sieti a systémoch dômyselne zamaskované neznáme programy bežiace na pozadí. Neviete, ako dlho tam sú, čo už vykonali a čo všetko idú spôsobiť. Neviete, či práve doposielajú niekam poslednú časť vašich citlivých databáz alebo niekto neznámy ovláda vaše privilegované prístupy vo vašich aplikáciách. Neviete nič, a očakávať môžete hocičo...

Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Nočnou morou každého prevádzkovateľa informačného systému, či už v domácom alebo vo firemnom prostredí, je situácia, keď zistí, že po incidente spôsobujúcom stratu alebo znepristupnenie dát nedokáže vykonať obnovu do pôvodného stavu. Dôvodov môže byť mnoho – nemá žiadne zálohy, alebo ich má, ale sú nepoužiteľné – nečitateľné médium, netestované zálohy a rad ďalších nepríjemností. A preto nestačí len zálohovať.

Blanka Vargová,
manažérka tímu kybernetickej bezpečnosti, U. S. Steel Košice, s. r. o.

Mojou doslova nočnou morou je, že raz mi uprostred noci zazvoní služobný mobil a na druhom konci bude bezradný kolega, ktorý mi oznámi, že stojí niektorá z kritických častí závodu a nik nemá ani šajnu, prečo sa tak stalo. Tento scenár, nanešťastie, môže nastať kedykoľvek a u kohokoľvek.

Juraj Koník,
bezpečnostný manažér,
Allianz – Slovenská poisťovňa, a. s.

Rozhodne sú to úniky dát mimo kancelárií. Cloudové úložiská, hybridná kancelária a umelá inteligencia dokážu zmanipulovať a zneistiť už aj tak dosť zmäteného zamestnanca. A zároveň vytvárajú ideálne podmienky, aby digitalizácia a Priemysel 4.0 pripravili nejedno nečakané prekvapenie. Dáta už neunikajú zo serverov, ale z domáceho prostredia používateľa, ktorý nedostatočne dbá na bezpečnosť svojho počítača, tabletu či mobilu.

Róbert Mramúch,
manažér kybernetickej bezpečnosti,
MH Teplárenský holding

Pre oblasť utilít ide primárne o bezpečnosť OT, teda výrobných systémov. V teplárenstve zabezpečujú výrobu a dodávku tepla obyvateľom, výrobným podnikom a iným inštitúciám. Prípadné dosahy sa rôznia podľa typu odberateľa, poskytovanej služby či ročného obdobia. Hrejúce radiátory či horúcu vodu vo vani berieme ako samozrejmosť, ktorú však niekto musí zabezpečiť a neustále chrániť.

Henrich Šnajder,
manažér IT bezpečnosti,
Orange Slovensko, a. s.

Od nezabezpečeného domáceho WiFi smerovača cez zariadenia v domácnosti až po dáta vo vašej firme alebo heslá od internetbankingu? Áno, práve nezabezpečená domáca sieť a pripojené zariadenia bez aktualizácií, navyše s prednastavenými heslami od výrobcu, predstavujú nočnú moru nielen pre súkromné osoby. V kombinácii so slabým zabezpečením vzdialeného prístupu do firemného prostredia sú nočnou morou aj pre váš biznis.

Petra Zorvanová,
špecialistka informačnej bezpečnosti,
Lidl Slovenská republika

Nočnou morou kybersveta je vo veľkej miere sociálne inžinierstvo, útoky na jednotlivca – zamestnanca, ktorý musí byť pozorný a obozretný pri otváraní príloh či hyperlinku v tele e-mailu. Často sa stretávame aj s telefonickými útokmi, ktoré sa pod nátlakom snažia zmanipulovať osobu na druhej strane. Je preto dôležité túto tému pravidelne rozoberať a školiť zamestnancov na všetkých hierarchických úrovniach.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií/IT manažment kvality,
Volkswagen Slovakia

V biznis živote je nočnou morou kybernetický útok, ktorý ochromí fungovanie firmy. Takéto situácie majú negatívny dosah aj na jej zamestnancov. Štandardný scenár môže byť phishing, ransomvér alebo iný malvér, ochromenie infraštruktúry alebo strata dát. V osobnom živote sme ešte zraniteľnejší. Preto buďme ostražití, vzdelávajme sa a chráňme seba a svojich blízkych pred nástrahami online sveta.

Pavol Adamec,
výkonný riaditeľ oddelenia Riadenie rizík,
KPMG Slovensko

Len jeden z mnohých príkladov na tému „uuups, na toto sme zabudli“. Často koluje presvedčenie, že naše systémy sú oddelené, nám sa nič nemôže stať. Až jedného dňa niekto na nejakom pracovisku potrebuje robiť nejaké jednoduché administratívne práce, nájde v kúte dlho nepoužívaný počítač a zapne ho. A o pár dní je zavírená celá firma. Len súhra doplňajúcich sa opatrení má šancu.

Ivan Makatura,
generálny riaditeľ,
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Nočnou morou kybernetickej bezpečnosti sú šmejdi, príštipkári a samozvaní odborníci. Tým v mnohých ohľadoch napomáhajú novinári alebo PR manažéri, ktorí kybernetickú bezpečnosť (logicky) považujú za príťažlivú tému.

Tibor Paulen,
manažér informačnej bezpečnosti,
Stredoslovenská distribučná, a. s.

Pracujem v spoločnosti, ktorej hlavnou náplňou je distribúcia elektrickej energie do firiem a domácností. Nočnou morou je pre mňa scenár, ktorý sa udial v roku 2015 na Ukrajine. Kybernetický útok vtedy zasiahol tri distribučné spoločnosti a prerušil dodávku elektriny pre viac ako 230-tisíc zákazníkov. Škoda pri takomto type útoku je obrovská. Bez elektriny môžu zostať nemocnice a kritické prevádzky.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov,
Tatrabanka

Mojou nočnou morou informačnej bezpečnosti je očakávanie komplexného, uveriteľného útoku na obyvateľov, ktorý spojí známe informačné kanály, jazykovú zdatnosť, techniky sociálneho inžinierstva, kybernetické zraniteľnosti a rýchle „instantné“ platby, ktoré prídu po Novom roku. Povedomie obyvateľov nie je pripravené na komplexný útok. Ak bude útočníkmi múdro nastavený, dosah útoku bude zdrvujúci.