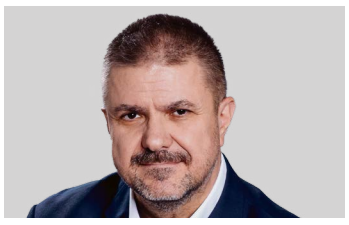
HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 30. OKTÓBRA – 1. NOVEMBRA 2020

# Koho a čoho sa treba vyvarovať?

ANKETA

Október, mesiac kybernetickej bezpečnosti sa končí. Určite lepšie pomenovanie by bolo, ak by to bol mesiac, kedy sa viacej hovorí, publikuje a diskutuje. Pozornosť si kybernetická bezpečnosť totiž vyžaduje neustále. Každý deň a v každej oblasti.

Posledná anketová otázka niektorých účastníkov pobavila, iní ju využili na apel pre zodpovedných manažérov, alebo pre koncových užívateľov. V každom prípade odpovede predstavujú reálne skúsenosti profesionálov kybernetickej bezpečnosti na Slovensku. Tie najlepšie veci nás vždy naučí prax.



**Ivan Makatura**
**generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti**

Nečinnosti a zároveň neprofesionality. To druhé ma trápi viac. Chápem, že nedostatok kvalifikovaných odborníkov núti štatutárov organizácií a HR manažérov siahnuť aj k neoverených zdrojom. Ale potom sa nemožno čudovať, keď v technickom odbore, ktorým kybernetická bezpečnosť bezpochyby je, budú bezpečnostné opatrenia navrhovať ľudia z profesií, ktoré s informačnými technológiami nikdy nemali nič spoločné. A potom je tu ešte jedna zvláštna skupina „tiežodborníkov“. Tí sa síce s problémami ochrany informácií doteraz reálne nestretli, no keď zistili, že kybernetická bezpečnosť je aktuálne v centre záujmu a taktiež lukratívna oblasť, sami seba vyhlásia za expertov a angažujú sa všade, kde sa len dá.

**Jaroslav Oster**
**predseda Správnej rady preventista.sk**

Kúzelníkov, falošného pocitu bezpečia a straty kritického myslenia. Kúzelníkov v ponímaní predajcov technických riešení garantujúcich širokospektrálnu a absolútnu bezpečnosť. Falošného pocitu bezpečia vo vnímaní rizika na úrovni „nám sa nič nemôže stať“ či „my máme všetko dokonalo zabezpečené“. A bez istej dávky kritického myslenia v dobe sociálnych manipulátorov striehnucich na každú chybičku nie je otázkou, či sa niečo môže stať, otázkou je len kedy.

**Tomáš Hettych**
**viceprezident ISACA Slovakia, Asociácia Auditu a Kontroly Informačných Systémov**

Pri implementáciách riešení kybernetickej bezpečnosti je potrebné vyvarovať sa nekvalifikovaných „odborníkov“. Kvalifikáciu špecialistov je možné si overiť prostredníctvom klientskych a projektových referencií a certifikátov. Kybernetická bezpečnosť je komplexná téma, ktorá vyžaduje široké portfólio znalostí a skúseností. Druhou oblasťou, kde je potrebné spozornieť, je ponuka tzv. all-in-one riešení, čiže ak bude dodávateľ ponúkať priamo implementáciu, bez vykonaného posúdenia, či auditu. Kvalita týchto riešení je prirodzene veľmi otázna a pravdepodobnosť budúcich problémov je pomerne vysoká.

**Martin Oczvirk**
**riaditeľ odboru informačnej bezpečnosti a certifikácie Úradu na ochranu osobných údajov**

Hlavne si nenamýšľať, že „mne sa to nemôže stať“. Druhým omylom je, keď si myslíme, že už máme zavedenú bezpečnosť a sme v bezpečí na sto percent a naveky. Ako bežní používatelia by sme sa mali vyhnúť inštalovaniu aplikácií z neoverených zdrojov a nepovoľovať na svojich zariadeniach služby a prístupy, ktoré nie sú nutné. Ak chce od vás aplikácia na kreslenie lokalizačné údaje a prístup k mikrofónu, tak vám to musí znieť podozrivo. A určite nezdieľať osobné údaje. Už len fotka z kancelárie alebo bytu môže útočníkovi poskytnúť cenné informácie, ktoré môže zneužiť.

**Lukáš Neduchal**
**podpredseda Správnej rady Asociácie kybernetickej bezpečnosti**

V oblasti kybernetickej bezpečnosti je takmer nemožné vyhnúť sa útoku. Otázkou nie je či áno, ale kedy sa tak stalo a ako dlho to trvalo, v lepšom prípade sa pýtam, kedy sa tak stane. Vystríhajte sa zjednodušeného pohľadu „nám sa to nemôže stať, nie sme zaujímavý cieľ“ a podobne. Každé bezpečnostné opatrenie niečo stojí a zvlášť v dnešnej dobe musia manažéri vedieť, ako predchádzať nevhodne vynaloženým prostriedkom a zdrojom. Ideálny začiatok je urobiť si zoznam aktív spoločnosti, vrátane tých informačných a urobiť reálnu analýzu a hodnotenie rizík.

**Andrej Žucha**
**generálny riaditeľ Alison Slovakia**

Pre všetky aktivity, možno s výnimkou štatistiky J platí, že nie je dobre, ak sa robia od stola. Alebo ako hovoríme - cez vetu „Vyplňte si priložený excel“. Tieto riešenia nie sú systémové, a patria do kategórie Len aby bolo, alebo Aby bol pokoj od práce. Takže vyhýbajte sa povrchnosti a dodávateľom s excelovou tabuľkou. Naopak, dobre si zmapujte existujúci stav, poznajte, čo máte, čo potrebujete a následne si naplánujte implementáciu opatrení. To najhoršie, čo sa môže stať, je ignorovať kybernetickú bezpečnosť, lebo nie je pravdou, že problém, ktorý nevidím, neexistuje.

**Peter Dostál**
**generálny riaditeľ a predseda Predstavenstva Aliter Technologies, a. s.**

Každý z nás by sa mal vyvarovať presvedčenia, že „mne sa to nemôže stať“. Ako používatelia by sa sme sa mali vyvarovať slabých hesiel, používania toho istého hesla bez dvojfaktorového overenia na rôznych weboch a otvárania príloh a liniek v emailoch, ktoré nepoznáme. Ak je nutné prezerať si potenciálne nebezpečné web stránky, je vhodné na to použiť izolovaný operačný systém napríklad na USB kľúči (sandbox) alebo aspoň vyhradiť jeden prehliadač na tento účel a zvýšiť na ňom zabezpečenie aj za cenu zníženej funkčnosti. Rovnako dôležité je vyvarovať sa prideľovania práv, o ktoré inštalovaný softvér žiada, ak na to nemáme jasný dôvod.

**Roman Čupka**
**hlavný konzultant Flowmon pre strednú a východnú Európu**

Z pohľadu bežného používateľa IT treba byť obozretný najmä pri otváraní príloh a klikaní na webové odkazy. Väčšina kybernetických incidentov je spôsobená zneužitím dôvernosti a pozornosti ľudí, na čo cielia emailové phishingové kampane, a tie sú čoraz sofistikovanejšie. Preto je dôležité neustále šírenie osvety a plošné vzdelávanie. Z pohľadu firiem a verejnej správy sa treba vyvarovať falošného pocitu bezpečia, ktorý by mohla navodzovať ochrana koncových zariadení. Okrem nich je dnes nevyhnutné mať aj viditeľnosť do siete a vedieť detegovať hrozby a reagovať na ne v čo najkratšom čase.

Odhady odborníkov na kybernetickú bezpečnosť, podporené objektívne merateľnými ukazovateľmi, sa pri predikcii ďalšieho vývoja stretávajú v očakávaní ďalšieho nárastu počtu kybernetických útokov, vzniku nových typov útočných vektorov a najmä zvyšovaní sofistikovanosti útočníkov. Okrem samozrejmej povinnosti prispôsobovať sa vývoju bezpečnostnej situácie a prijímať adekvátne protiopatrenia, stavia Národný bezpečnostný úrad najmä na rozširovaní existujúcich foriem spolupráce. A to nielen so zaintresovanými štátnymi orgánmi a zahraničnými partnermi, ale tiež so súkromnou sférou a akademickou obcou.

**Národný bezpečnostnú úrad:** Správa o kybernetickej bezpečnosti v slovenskej republike za rok 2019

**Andrej Aleksiev**
**riaditeľ pobočky Check Point Software Technologies na Slovensku**

Vyvarujme sa ľudí, ktorí zľahčujú dnešnú situáciu z pohľadu kyber-bezpečnosti. Situácia je vážna a preto neopakujme chyby, ktorých sme sa dopustili my sami alebo iné entity. Kto by bol povedal, že hackeri sa budú snažiť získať kontrolu nad vodárňou s úmyslom zvýšenia hladiny chlóru vo vode a tak otráviť obyvateľstvo?

**Igor Urban**
**regionálny manažér Forcepoint pre východnú Európu**

Odpoveď na túto otázku je jednoduchá a v princípe univerzálna. Ľudskej hlúposti. A to ako pri strategickom rozhodovaní o smerovaní kybernetickej bezpečnosti na rôznych úrovniach, tak pri denno-dennom používaní IKT nástrojov vrátane sociálnych sietí. Niekedy nie je na škodu spomenúť si na obyčajný sedliacky rozum, pridať k tomu trochu rozvahy so štipkou zdravej drzosti, nebáť sa byť inovatívny a zároveň si povedať veci tak, ako sú. Hrať sa na schovávačku a zatvárať si oči pred realitou sa v kybernetickom priestore väčšinou nevypláca. A následky môžu byť šokujúce.

**Marek Král**
**generálny riaditeľ SecTec**

Neád by som sa opakoval, pretože v tomto seriáli bolo poukázané na viac dôležitých tém, ktoré si vyžadujú pozornosť. Určite neodporúčam spoliehať sa na „dúfam“. Dúfam, že som dobre ochránený a dúfam, že mne sa nič nestane. Toto môže byť drahá stratégia. Taktiež sa stretávame, že zákazníci riešia bezpečnosť na open source riešeniach. Bezpečnosť je tak komplexná téma, že určite odporúčam implementáciu komerčných riešení, za ktorými sú veľké investície do vývoja, teamy špecialistov a garantovaná podpora. Nájsť si tú správnu cestu, ako budovať a neustále dopĺňať bezpečnosť, nie je vôbec jednoduché. Preto by som upozornil na Príručku kybernetickej bezpečnosti, ktorá vychádza v prílohe HN na pokračovanie a ponúka zjednodušený návod, ako na to.

**Jana Puškáčová**
**manažérka útvaru Informačná bezpečnosť MOL IT & Digital Slovensko**

Na jednej strane je potrebné si uvedomiť, že kybernetická bezpečnosť existuje v každej firme len vďaka biznisu a nie naopak. Presadzovanie rigidných bezpečnostných požiadaviek bez ohľadu na charakter biznisu a analýzu rizík má zvyčajne za následok silnú rezistenciu. Ak chce kybernetická bezpečnosť vo firme uspieť, mala by implementovať také riešenia, ktoré transparentné ošetrujú biznis rizika. Na druhej strane sa treba vyvarovať presvedčenia, že kybernetická bezpečnosť je čisto IT záležitosť. Presadzovanie a dodržiavanie princípov kybernetickej bezpečnosti by sa malo stať nedeliteľnou súčasťou fungovania každého zamestnanca firmy, či tretej strany, vrcholové vedenie firmy nevynímajúc.

**Richard Kiškováč**
**Security Consultant Digital Systems, a. s.**

Z praxe konzultanta jednoznačne konštatujem, že z pohľadu bežného používateľa je potrebné vyvarovať sa unáhlených rozhodnutí v kybernetickej bezpečnosti, prílišnej chuti na senzácie alebo odmeny bez platenia. Z pohľadu organizácií je potrebné vyvarovať sa hlavne nekvalifikovaného a laxného riadenia kybernetickej bezpečnosti, ktorú väčšinou zosobňuje pozícia jej manažéra. Organizácie všetkých typov a na všetkých úrovniach by sa mali vystríhať nerovnováhy medzi troma základnými piliermi bezpečnosti, ktorými sú ľudia, procesy a technológie.

**Tomáš Zaťko**
**CEO Citadelo, etický hacker**

Vyvarovať sa treba univerzálnych riešení. Magických krabičiek. Prehnane sebavedomých manipulátorov, ktorí sú majstri sveta. Zaručeným obranám. Bezpečnostným procesom bez bezpečnostných technológií. Taktiež bezpečnostným technológiám bez bezpečnostných procesov. Taktiež sa treba vyvarovať prílišnému optimizmu a spánku na vavrínoch. Bezpečnosť je veľmi náročná disciplína. Jej dynamika vie meniť situáciu a vašu odolnosť extrémne rýchlo.

**Pavol Adamec**
**výkonný riaditeľ oddelenia Riadenie rizík KPMG Slovensko**

Najväčšou chybou je myslieť si, že kybernetická bezpečnosť nie je váš problém. Že vás sa to netýka. Že vám sa to nemôže stať. Že nie ste pre nikoho zaujímaví. Že vám sa nič nemôže stať, pretože máte firewall, či IDS, antivír, penetračný test, šifrovanie, ... – nahraďte magické slovo v kontexte svojej organizácie. Nové technológie, novo odhalené zraniteľnosti, nové skutočne kreatívne nápady útočníkov, ako oklamať svoje potenciálne obete, pribúdajú závratne rýchlo. Pocit, že vy ste mimo tejto reality, vás môže priniesť na titulné stránky novín nechceným spôsobom.

**Marián Trizuliak**
**architekt kybernetickej bezpečnosti, Západoslovenská distribučná, a. s.**

“Čo môžeš urobiť dnes, odlož na zajtra a získaš deň voľna.” Kybernetická bezpečnosť je o neustálej bdelosti, pozornosti, pohotovosti a zdravej dávke paranoje. Je nevyhnutné sa vyvarovať lenivosti, ľahostajnosti a nepodliehať falošnému pocitu bezpečia. Konečný stav bezpečnosti neexistuje a zároveň dúfam, že ani nebude existovať (nemal by som čo robiť). Každý z nás si musí osvojiť predpoklad, že digitálny svet nie je anonymný a je zraniteľný - my sme zraniteľní. Musíme sa podľa toho správať - najlepšie už dnes.

**Ján Adamovský**
**Chief Security Officer Slovenská sporiteľňa**

Rozhodne sa treba vyvarovať pocitu falošnej bezpečnosti, vyplývajúceho z chybného predpokladu, že „Ja alebo moja firma sme pre digitálnych zlodejov nezaujímaví a preto mi nič nehrozí“. V novinách sa dočítame iba o veľkých, mediálne atraktívnych spoločnostiach, ktoré sa stali terčom kybernetického útoku. Paradoxne však platí, že čím je firma väčšia, tým viac je schopná investovať do bezpečnosti a je lepšie chránená. Väčšina útokov sa preto deje práve voči bežným ľuďom a malým firmám. Preto téma kybernetickej bezpečnosti je rozhodne témou každého z nás.