

Plán? Čo firma, to digitálna pevnosť

TÉMA

Zmierte sa s tým – bezpečnosť nie je projekt, ale proces. Overte si, ako máte v digitálnej dobe zvládnutú fyzickú bezpečnosť, ochranu informácií a svoj prístup k téme.

Už stokrát ste počuli, že digitalizácia zmenila svet, v ktorom žijeme. Bezpečnosť firiem sa presunula do digitálneho sveta a roky platné bezpečnostné pravidlá majú nový formát. Pozrime sa na to helikoptérovým pohľadom.

Najlepšie základy

Fyzická ochrana a zabezpečenie priestorov je o komplexom opatrení. Začína sa to stavbou, čiže vybudovaním priestorov a použitím materiálov, pokračujeme prístupovými systémami, zabezpečením priestorov až po elektronické zabezpečovacie systémy a kamerové systémy.

Ako vysvetľuje technologický konzultant Radoslav Masnica zo spoločnosti Aliter Technologies, dnes sú elektronické zabezpečovacie systémy spolu s kontrolou vstupu základným pilierom objektivej bezpečnosti. Umožňujú vstup do citlivých alebo obmedzených priestorov len oprávneným osobám na základe čipových kariet alebo biometrických údajov, ako sú odtlačky prstov či rozpoznávanie tváre.

Od bondoviek k praxi

Technológie ako viacfaktorová autentifikácia a biometria sú v súkromnom sektore masovo využívané takmer desaťročné, čipové karty aj dlhšie. Plošné a strategické uplatnenie nastalo začiatkom tohto desaťročia a v súčasnosti ide o štandard najmä v regulovaných a technicky zrelých firmách.

Elektronické zabezpečovacie systémy sú často prepojené s kamerovým dohľadom, so záznamom vstupov a výstupov a s automatickými zámkami. Znižujú tak riziko neoprávneného fyzického prístupu k zariadeniam alebo dátam.

Niečo ako pancier

Pri spracúvaní dôležitých a citlivých informácií je potrebná aj ochrana proti úniku elektromagnetického žiarenia. Používajú sa takzvané tempestované zariadenia, čiže špeciálne upravený hardvér. Takáto konštrukcia minimalizuje neúmyselné vyžarovanie signálov, ktoré by mohli byť zachytené a zneužitú na odpočúvanie či reverzné inžinierstvo.



Všetci a bez výnimky. Kybernetická odolnosť je taká silná ako jej najslabšie ohnisko.

FOTO: DREAMSTIME

Ochrana informácií sa v tomto kontexte neopiera len o šifrovanie dát počas prenosu alebo uloženia, ale aj o fyzické a technické zabezpečenie zariadení, ktoré s nimi pracujú.

Ochrana informácií

Šifrovanie už dávno nie je téma iba pre políciu, armádu a Finančnú správu. Potrebu bezpečného zaobchádzania s informáciami vyžaduje aj súkromný sektor, odborné profesie či dokonca bežní používatelia digitálnych služieb.

V súčasnosti sa šifrovanie používa pri e-mailovej komunikácii, pri čotoch alebo videokonferenciách, pri ukladaní údajov na diskoch, serveroch alebo USB zariadeniach. Využíva sa aj pri vytváraní bezpečnostných kanálov, pre vás známych ako VPN, v mobilnej a rádiovkej komunikácii, v cloude aj pri autentifikácii používateľov do systémov a služieb.

Od šifrovania ku kryptografii

Výrobcovia softvéru a hardvéru už bežne ponúkajú šifrovacie programy. Omnoho vyššie nároky na ochranu informácií sú v prípade, ak sú klasifikované zo zákona o ochrane utajovaných skutočností alebo z kyberzákona.

Na ochranu klasifikovaných informácií kryptografickými metódami sú určené prostried-

ky šifrovej ochrany informácií. V praxi sú to hardvérové zariadenia, napríklad šifrovacie moduly alebo kryptografické procesory a aplikácie na šifrovanie údajov či elektronickej komunikácie. „V ostatných troch rokoch sa extrémne zvýšil dopyt po zariadeniach šifrovej ochrany informácií. Súvisí to s geopolitickou situáciou a reguláciami,“ hodnotí trend Andrej Žucha zo spoločnosti Alison Slovakia.

Extrémne prísna kontrola

Profesionálne bezpečnostné riešenia podliehajú prísny testom. „Certifikácia je proces, kde dochádza v renomovaných

organizáciách a akreditovaných laboratóriách k dôkladnému overeniu bezpečnostných vlastností zariadení na základe štandardizovaných metodík a kritérií,“ potvrdzuje Bibiana Magáthová z Kompetenčného a certifikačného centra kybernetickej bezpečnosti.

Certifikácia zabezpečuje, že zariadenie spĺňa požiadavky, ktoré deklaruje výrobca. Jeho implementácia nevykazuje známe zraniteľnosti alebo chyby, ktoré by mohli byť zneužitú útočníkom.

Preto je pochopiteľné, že požiadavky na certifikáciu v bezpečnosti rastú. Európska agentúra pre kybernetickú bezpeč-

nosť ENISA pripravuje viacero schém certifikácie kyberbezpečnostných služieb. Dlhoočakávané sú certifikácie cloudových služieb a 5G sietí a bude nasledovať certifikácia manažovaných bezpečnostných služieb.

Menia sa hrozby

Ak firmu kedysi chránila fyzická SBS-ka, dnes potrebujeme firewally, antivírusy, systémy na ochranu koncových zariadení EDR či strediská bezpečnostných operácií SOC. Monitorujú dianie v sieti, zaznamenávajú podozrivé správanie a upozorňujú na možné incidenty. Rozdiel je v rýchlosti. V kyberpriestore sa útok môže rozšíriť v priebehu minút.

Tradične sa kládol dôraz na školenie o bezpečnosti pri práci, požiarnych predpisoch či ochrane zdravia. Dnes je nevyhnutné, aby každé školenie zahŕňalo aj kybernetickú bezpečnosť od rozpoznávania phishingových e-mailov až po správu hesiel.

Skladačka zapadla do seba

Premena klasickej bezpečnosti na kybernetickú nie je len o náhrade zámku heslom či trezoru cloudom. Manažéri, majitelia aj prevádzkoví riaditelia by mali chápať, že kybernetická bezpečnosť nie je iba úloha IT oddelenia – je to tímová zodpovednosť.

„Kybernetická bezpečnosť v spektre bezpečnosti dnes predstavuje jeden z najdynamickejších rastúcich pilierov,“ konštatuje Roman Varga, manažér kybernetickej bezpečnosti v zdravotnej poisťovni Dôvera.

Tento rast významu kyberbezpečnosti akceleruje zavádzanie nových produktov, adaptácie umelej inteligencie a technologický rozvoj. Z pôvodne technickej disciplíny sa kyberbezpečnosť stáva strategickým prvkom riadenia rizík a odolnosti. Jej význam rastie úmerne s digitalizáciou procesov, prepojením systémov a rastúcim počtom hrozieb.

Kyberkapitola a podkapitoly

Roman Varga pôsobí v kyberkomunitě v sektore zdravotníctva viac ako dve dekády. Za ten čas mal možnosť riešiť incidenty, nastavovať politiky, zavádzať technológie a najmä učiť sa z praxe, inšpirovať sa od kolegov a kyberkomunity.

Jeho presvedčenie je neochvejné: „Komplexita kyberbezpečnosti podľa môjho vnímania spočíva v prepojení štyroch hlavných pilierov – technológie, procesov, ľudského kapitálu a legislatívy. Nestačí mať len technické riešenia. Dôležité je, ako sú nastavené procesy, ako sú vyškolení ľudia a či sú všetky kroky v súlade s reguláciami.“

AKÁ JE KYBERNETICKÁ BEZPEČNOSŤ?

Požiadali sme popredné osobnosti slovenského kyberbezpečnostného prostredia, aby na jednoduchú otázku odpovedali sloganom. Čítajte pravidelnú anketu.



Stručne. Podľa možnosti aj originálne

ANKETA

Žijeme v dobe meme a TikToku. Chceme funkčné a krátke informácie. Aj o ťažkých témach. Požiadali sme profesionálov, aby napísali niečo ako slogan. Aká je kybernetická bezpečnosť?



Július Selecký,
architekt bezpečnostných riešení,
ESET

Kybernetická bezpečnosť je ako poistenie - nechceš ju platiť, kým sa nič nedeje, ale keď príde problém, zachráni ti firmu. Preto to nie je zbytočný výdavok, ale investícia, ktorá ťa môže udržať pri živote.



Dominik Procházka,
riaditeľ odboru bezpečnosti,
AGEL

Kybernetická bezpečnosť je prehlíadaná - až do prvého incidentu. Je to dlhodobý proces, ktorý si vyžaduje systematickú prácu a schopnosť adaptácie. Útočník nespí, a preto ani my. Je to výzva aj príležitosť na rast.



Lenka Gondová,
prezidentka,
ISACA

Kybernetická bezpečnosť je ako dôvera - ťažko sa buduje, ľahko stratí, a bez nej je každý biznis zraniteľný.



Tomáš Valenta,
riaditeľ,
Check Point Software
Technologies

Kybernetická bezpečnosť je ako Rokfort. Chráni tvoje digitálne tajomstvá pred smrťozrútmí internetu. Silné heslo je tvoj Patronus, multifaktorová autentifikácia ako Fénix Fawkes a antivírus ako Auror. Neklikaj na podvodné sovy a zálohuj ako Hermiona - vždy pripravený!



Tomáš Zaťko,
etický hacker, CEO,
Citadelo

Kybernetická bezpečnosť je nekonečná šachová partia, v ktorej majú útočníci vždy výhodu prvého ťahu.



Ivan Makatura,
predseda,
Asociácia kybernetickej
bezpečnosti

Kybernetická bezpečnosť je NE-JASNÁ. Vyhodnotenie správ auditu nie je štatisticky relevantným ukazovateľom skutočného stavu a vývoja kybernetickej bezpečnosti na Slovensku. To by sa však čoskoro malo zmeniť prijatím metodiky tvorby indexu KB. Index kyberbezpečnosti má zatiaľ meraný len EÚ prostredníctvom agentúry ENISA - aj to len prvý rok.



Viktória Blažičková,
vedúca oddelenia riadenia
informačnej a kybernetickej
bezpečnosti,
Národná diaľničná spoločnosť

Kybernetická bezpečnosť je digitálna empatia. Nie je len o technológiách - je aj o ľuďoch, ich chybách, návykoch a potrebe ochrany. Aj preto ju budujeme dôsledne každý deň.



Richard Kiškováč,
generálny riaditeľ,
Elkan

Kybernetická bezpečnosť je komplexná a dynamická. Komplexná preto, že zahŕňa veľmi veľa aspektov od ľudského faktora, hardvéru, softvéru až po geopolitiku. Dynamická preto, že je spojená so stále novými a vyvíjajúcimi sa hrozbami, ktoré priamo korešponujú s vývojom a so zmenami v technologických prostrediach. Tomu všetkému zodpovedajú aj nároky na zdroje, či už finančné, alebo ľudské. Je však veľmi dôležité a kľúčové, ako efektívne sú tieto zdroje využívané.



Tomáš Hettych,
člen predstavenstva,
Kompetenčné a certifikačné
centrum kybernetickej
bezpečnosti

Kybernetická bezpečnosť je subjektívne vnímanie stavu pripravenosti organizácie na nové hrozby a legislatívne požiadavky.



Michal Srnec,
vedúci oddelenia informačnej
bezpečnosti,
Aliter Technologies

Kybernetická bezpečnosť je komplexná disciplína. Zorientovať sa v nej a správne ju uchopiť neznamená len hlboké porozumenie množstvu technológií, ale aj vedieť, ako tieto technológie implementovať, nastaviť a dlhodobo udržiavať a rozvíjať. A to všetko takým spôsobom, aby biznis podporovali a nedušili v neustále sa meniacom a dynamickom prostredí. Útočníci nikdy nespia, a tak nesmieme ani my. Čo ma privádza k druhému atribútu kybernetickej bezpečnosti, a tým je nepochybne dôležitosť, ktorú, ako pevne verím, vo svetle neustálych útokov už netreba veľmi pripomínať.



Henrich Šnajder,
manažér IT bezpečnosti,
Orange Slovensko

Kybernetická bezpečnosť je poslanie chrániť to, na čom záleží. V digitálnom svete to nie je len o dátach, ale aj o dôvere, slobode a budúcnosti. Verím, že každý má právo cítiť sa bezpečne - či už ide o firmu, školu alebo jednotlivca.



Jaroslav Ďurovka,
riaditeľ,
Národné centrum kybernetickej
bezpečnosti

Kybernetická bezpečnosť je zásadná téma v kontexte súčasného geopolitického priestoru a má mať popredné miesto medzi ďalšími prioritami každej krajiny. Posilnenie súčasnej úrovne kybernetickej bezpečnosti musí byť vnímané ako strategická otázka, bez ktorej nebude dobre fungovať jednotný trh EÚ.



Peter Kočík,
manažér systémových
inžinierov,
Fortinet

Kybernetická bezpečnosť je komplexná digitálna imunita. Hrozby môžu prichádzať zvonka aj zvnútra. Ak sa o ňu nestaráš, raz tvoje telo skolabuje. Procesy, ľudia a technológie musia spolupracovať ako živý ekosystém. Treba ju neustále zlepšovať - ak ju vnímaš ako stav, prehrávaš. Ak ju berieš ako vývoj, máš šancu. Prevencia, detekcia a reakcia musia byť v rovnováhe. A musí byť 24/7, ani imunitný systém nemá dovolenku.



Tibor Szabo,
vedúci oddelenia auditu IT,
Všeobecná úverová banka

Kybernetická bezpečnosť je v konečnom dôsledku umením udržať rovnováhu medzi otvorenosťou a ochranou. Je o nájdení harmónie medzi jednoduchým prístupom k informáciám a múrmi, ktoré chránia súkromie a dôvernosc. Je to neviditeľná niť, ktorá drží pohromade a v bezpečí digitálne srdce modernej civilizácie. Je to náš priateľ a strážca, ktorý nás chráni pred búrkami v kyberpriestore. Včera to bola drahá vymoženosc, dnes je to potreba a zajtra to bude nevyhnutosc.



Benjamin Würfl,
obchodný zástupca,
Eviden Slovakia

Kybernetická bezpečnosť je istota a nevyhnutosc v digitálnom svete. Dnes online vybavujeme takmer všetko - od práce po nákupy. Keby som sa nemohol spoľahnúť na to, že sú moje údaje v bezpečí, necítil by som sa ani zďaleka komfortne. Vnímam ju preto ako niečo nevyhnutné, napríklad ako zámok na dverách.



Peter Dufek,
manažér kybernetickej
bezpečnosti,
Penta Hospitals

Kybernetická bezpečnosť je neviditeľný štít, čo chráni digitálne svety pred hrozbami zla, a aj tichý strážca, bdejúci nad každým počítačom, sieťou a internetom. Neustále vedie svoj boj s temnými silami tam vonku. A hoci ju nevidno, je ako vietor - cítiť ju vždy, keď sa zdvihne búrka. Je to náročná a veľká výzva, ktorá spája oddanosť, technológie, právo, ľudské správanie a riadenie rizík.



Tibor Paulen,
manažér informačnej
bezpečnosti,
Stredoslovenská distribučná

Kybernetická bezpečnosť znamená akceptovať skutočnosť, že sme vo vojnovnej zóne, a tomu zodpovedajúcim spôsobom prispôbiť svoje správanie. Znamená to, že musíme byť neustále v strehu, pripravení čeliť hrozbám a útokom, ktoré môžu prísť kedykoľvek a akokoľvek. Je to boj proti neviditeľným nepriateľom, ktorí sa snažia prekonať naše obranné línie. Podobne ako v skutočnej vojnovnej zóne, aj tu každý chybný krok môže byť fatálny.



Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Kybernetická bezpečnosť je ako multižánrový televízny seriál. Nájde sa v ňom sci-fi príbehy o dodávateľských zázrakoch bezpečnostných riešení, detektívne a investigatívne príbehy pri vyšetrovaní, tragické okamihy pri riešení dosahov incidentu, prvky reality show z okamihov presvedčovania zodpovedných v téme „áno, týka sa vás to“. A mnoho ďalších. Miestami i komediálne a satirické diely.



Ján Adamovský,
riaditeľ bezpečnosti,
Slovenská sporiteľňa

Kybernetická bezpečnosť je výzva, ktorá si nikdy neberie dovolenku. Útočníci neprestávajú hľadať nové spôsoby, ako obísť naše obranné línie, a práve preto je práca v kybernetickej bezpečnosti taká fascinujúca. Núti nás neustále sa zlepšovať a inovovať.



Žaneta Steklová,
konzultantka kybernetickej
bezpečnosti,
Cyllium

Kybernetická bezpečnosť je ako vzduch - neviditeľná, kým nechýba. Zvyčajne si ju neuviedomujeme, no v momente narušenia jej hodnotu okamžite pocítime. Chrání naše dáta, identitu, dôveru. Preto by nemala byť len reakciou na hrozby, ale trvalou súčasťou našej digitálnej kultúry.



Jakub Berthoty,
advokát,
Digital Legal

Kybernetická bezpečnosť je ako statika budovy. Môže to dlho stať aj bez nej, ale raz to spadne. Robiť ju potom už bude neskoro.



Ivan Kopáček,
bezpečnostný expert,
Gordias

Kybernetická bezpečnosť je dynamicko-komplexne-evolučno-reaktívna. A ani to ju úplne nevystihuje. Má mnoho podôb. Je skrátka taká, aká je doba, v ktorej žijeme.



Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Kybernetická bezpečnosť je nekonečný príbeh. Keď už máte pocit, že ste aspoň na chvíľu „vyhrali“, tak sa objaví niečo nové, čo musíte riešiť, aby ste mali čisté svedomie, že ste urobili maximum na ochranu svojho alebo zákazníkovho IT prostredia.



Ján Andraško,
SOC manažér,
Binary Confidence

Kybernetická bezpečnosť je ako tímový šport. Každý musí vedieť, kde má stáť a čo robiť, inak vznikne diera v obrane. Aj malá nepozornosť jedného člena môže znamenať veľký problém pre celý tím.



Miroslav Chlipala,
advokát,
Advokáti Chlipala

Kybernetická bezpečnosť je poznanie, ktoré chráni. Skutočná bezpečnosť sa nezačína technológiou, ale porozumením. Prevencia sa začína vzdelaním - o hrozbách, riešeniach aj právnych pravidlách. Vzdelávanie a porozumenie práva premieňa kybernetickú bezpečnosť z reakcie na proaktívny nástroj ochrany. Znalosť je najlepšou obranou v digitálnom priestore.

AKO HODNOTÍ ODPOVEDE AI APLIKÁCIA?

Požiadali sme popredné osobnosti slovenského kyberbezpečnostného prostredia, aby na jednoduchú otázku odpovedali sloganom. Výsledkom je pestrá mozaika metafor, výziev aj postrehov z praxe.

Odborníci prirovnávajú kyberbezpečnosť k poisteniu, imunitnému systému, dôvere, statike budovy či dokonca Rokfortu. Spája ich však jedno: vedomie, že nejde o technickú rutinu, ale živý a neustále sa meniaci proces, ktorý musí reflektovať riziká dnešného digitálneho sveta.

Z odpovedí cítiť volanie po prevencii, vzdelaní, zodpovednosti a dôvere na ľudský faktor. Opakovane zaznieva myšlienka, že útočníci nespia, a preto ani obrancovia nemôžu. Niektorí zároveň upozorňujú na potrebu systematického merania stavu kyberbezpečnosti a silnejšieho strategického ukotvenia tejto témy na úrovni štátu. Hoci sa názory líšia štýlom aj dôrazmi, jedno je isté: kyberbezpečnosť je náš každodenný zápas, výzva i kultúrna hodnota. A ako viacerí pripomenuli - je lepšie ju budovať vopred, než po útoku narýchlo opravovať škody.