Čím je pre sektor príznačný rok 2020

ANKETA

Kľúčové postavy kybernetickej bezpečnosti na Slovensku sa vyjadrili k najdôležitejším témam v odvetví.

V nedávnom prieskume spoločnosti Gartner až 74 % spoločností uviedlo, že majú v úmysle presunúť časť zamestnancov natrvalo na prácu z domu. Prvou spoločnosťou, ktorá tento prístup implementovala bol Facebook, ktorý nedávno oznámil, že natrvalo presunie 50 percent svojich zamestnancov na prácu na diaľku. Keďže osobné stretnutia sú obmedzené, firmy a ich zamestnanci, viac ako kedykoľvek predtým, využívajú moderné nástroje na komunikáciu a spoluprácu. Kým spoločnosť Zoom mala v decembri 2019 asi 10 miliónov účastníkov na stretnutiach každý deň, v apríli 2020 už hlásila viac ako 300 miliónov, čo je ohromný 3 000-percentný nárast!

Rastislav Janota
riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

Rok 2020 je rokom pandémie COVID-19, rokom skokovej zmeny správania väčšiny firiem na trhu v oblasti využívania internetu. Firmy masívne zavádzajú prácu z domu. A tu je hneď problém. Robia to veľmi často v strese a bez správnej prípravy: bez procesov, prispôsobenia vlastnej infraštruktúry, len s minimálnymi alebo žiadnymi bezpečnostnými školeniami pracovníkov či zmeny správania na úrovni prevádzky vrátane bezpečnostného dohľadu. Toto všetko vytvára veľa nových možností pre úspešný útok.

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

Nielen vo svete môžeme badať veľké úniky dát a osobných údajov, ale ani Slovensko tento rok nezostalo výnimkou. Pribúdajú útoky formou sociálneho inžinierstva, súvisiace so zneužívaním pandémie COVID-19. Ďalej sú to útoky cez pomerne zanedbávanú oblasť IoT (Internet of Things), kryptoburzy a neposlednom rade ransomvérové útoky. Aj v ochrane osobných údajov pribúdajú útoky formou ransomvéru. V roku 2020 je, žiaľ, kybernetická bezpečnosť príliš často na konci priorít rôznych organizácii. Vedenie firiem jej začína venovať pozornosť, až keď už priamo pociťujú následky kybernetického útoku.

Jaroslav Oster
predseda správnej rady preventista.sk

Tento rok priniesol okrem radu iných aj 3 témy kybernetickej bezpečnosti. Do prvej patrí dynamický nárast tematicky orientovaných internetových podvodov v súvislosti s C-19, ako napríklad ponuky práce na doma, podvodné eshopy a značný nárast hoaxu k téme C-19. Druhú skupinu ohrození predstavujú rôzne formy počítačovej kriminality vo vzťahu k deťom, najmä rôzne formy kyberšikany, cybergrooming a nárast šírenia nevhodného obsahu. A do tretice - digitálna stopa a forenzná analýza digitálnej stopy v trestnom konaní prvýkrát prenikajú na Slovensku ako téma medzi odbornú i laickú verejnosť.

Ivan Makatura
generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti

Rok 2020 je prelomový. Odhodlanie útočníkov využiť jedinečné okolnosti je zreteľné. Vplýva totiž na princípy spracúvania informácií, ktoré sa oveľa viac než kedykoľvek predtým musia spoľahnúť na bezpečnostné povedomie používateľov. Nastali však aj plánované zmeny. Na základe Nariadenia EÚ o kybernetickej bezpečnosti agentúra ENISA spracovala certifikačnú schému na posudzovanie kybernetickej bezpečnosti výrobkov, služieb a procesov. Vzniká tak historicky prvá právna norma na certifikáciu bezpečnosti. EÚ zároveň zásadne zvýšila financovanie kybernetickej bezpečnosti prostredníctvom programu Horizont Europe. Jeho úlohu bude aj zriadenie Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti.

Tomáš Hettych
viceprezident ISACA Slovakia

Prebiehajúca „koronakríza“ všetky organizácie prinútila dramaticky prehodnotiť svoje pracovné procesy, personalistiku, otázky efektivity vzdelávania a riadenia projektov, možnosti práce mimo pracoviska a samozrejme tiež plány kontinuity a obnovy prevádzky. Organizácie, ktoré mali skutočne dobre napísané a otestované plány kontinuity činností, ktoré sú mimochodom súčasťou riadenia informačnej/kybernetickej bezpečnosti, boli na „lockdown“ a prácu z domu podstatne lepšie pripravené. Tieto spoločnosti nemali problém dodávať svoje produkty alebo služby v pôvodnej kvalite a čase ako pri bežnej prevádzke.

Lukáš Neduchal
podpredseda správnej rady Asociácie kybernetickej bezpečnosti

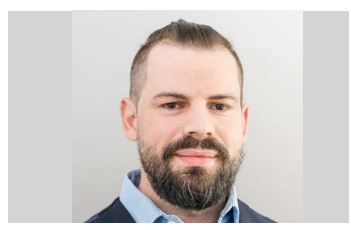
Slovné spojenie „digitálna transformácia“ dostalo v mnohých firmách reálny, nový význam a mnohokrát sa stalo podmienkou prežitia. Rast používateľov online služieb, komplexnosti prostredia a objemu dát, znamenajú nárast kybernetických hrozieb a priamych aj nepriamych útokov na fyzické a informačné aktíva spoločností a osobné údaje súkromných osôb. Dáta a z nich získané informácie sú kľúčom ku všetkému, či už konkurenčnej výhode alebo k finančným stratám vyplývajúcim z nezabezpečených IT rizík. Takže úplne zásadné je zvládnutie integrácie oblasti prediktívneho riadenia rizík, bezpečnosti správy dát a vzdelávanie používateľov.

Andrej Žucha
generálny riaditeľ Alison Slovakia

Rozvoj kyberkriminality, kyberterorizmu, kyberhaktivizmu, zvýšená miera hoaxov aj významný podiel práce a štúdia na diaľku. Svet stojí zhrozený pred zistením, že infraštruktúra tak ako je navrhnutá dnes, sa stáva slabinou. Výpočtový výkon u viacerých spoločností či štátu ako tak postačuje, avšak ukazuje sa, že prístup je z pohľadu bezpečnosti nedostatočný. Chýbajú procesy, monitoring aj včasná reakcia na ohrozenia, chýba kontrola aj riadenie. Zároveň veľa rozbehnutých a kvalitných aktivít v oblasti bezpečnosti je zabrzdených, pretože je potrebné riešiť základný chod a prežitie firiem alebo štátu. Je to rok, ktorý urobil dokonalé testovanie zraniteľnosti v celosvetovom meradle.

Peter Dostál
výkonný riaditeľ Aliter Technologies

Firemné, štátne i školské systémy sú v tomto roku vystavené väčšiemu riziku. Odhalili sa viaceré zraniteľnosti populárnych kolaboračných nástrojov. Našťastie sa podarilo ich relatívne rýchlo adresovať. S rozšírením cloud technológií narástla zložitosť odhaľovania útokov a začalo sa diskutovať o bezpečnosti 5G sietí. Aj tento rok bol achillovou pätou väčšiny IT systémov najmä ľudský faktor. A nejednalo sa iba o sociálny inžiniering alebo chyby zamestnancov. Množia sa aj prípady predaja citlivých informácií. Zvýšený počet hekerských útokov v kyber priestore potvrdzuje, ako sme veľmi zraniteľní, lebo niektorí z nás počas pandémie nadobudli pocit, že online svet je bezpečnejší ako ten skutočný.



Roman Čupka
hlavný konzultant Flowmon pre strednú a východnú Európu

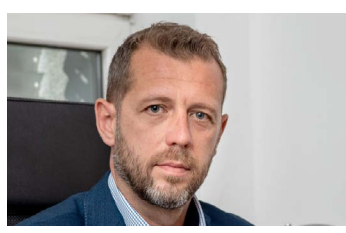
Zvýšil sa tlak na zabezpečenie poskytovaných a realizovaných služieb súvisiacich s odlevom pracovníkov počas pandémie na „prácu z domova“. Organizácie museli promptne reagovať na zachovanie kontinuity činností a nebolo to bezbolestné. Tejto situácii sa prispôsobili aj kyber útočníci. Zaregistrovali sme opäť zvýšený počet podvrhnutých emailov, či webových stránok a zneužívanie dôvernosti ľudí v rámci phishingových kampaní.

Andrej Aleksiev
riaditeľ slovenskej pobočky Check Point Software Technologies

Svet sa zmenil! Spôsob spolupráce, ktorý dnes vnímame ako „nový normál“ nás donútil hľadať cesty ako spolu komunikovať, spolupracovať a navyše byť produktívny. V Check Point sa za dva týždne od vypuknutia pandémie 99 percent organizácie presťahovalo do domácich kancelárií, čo bolo prvýkrát v histórii. Keď sme zisťovali, aké dosahy mal tento „nový normál“, 78 percent našich zamestnancov uviedlo, že ich produktivita bola dokonca vyššia a zároveň dokázali lepšie zosúladiť svoj pracovný a osobný život. Komunikačné platformy hlásia až tisícnásobné nárasty, avšak tento nový spôsob práce a komunikácie so sebou prináša aj bezpečnostné riziká. A preto „nový normál“ bude hovoriť o bezpečnosti stále a všade.

Igor Urban
regionálny manažér Forcepoint pre východnú Európu

Forcepoint už ostatné tri roky tvrdí, že novým perimeterom sú ľudia, a toto sa v roku COVID naplno preukázalo. Témou číslo 1 bolo, ako zabezpečiť vzdialený prístup v rôznych oblastiach. Neprehliadajme však hrozby typu Deepfake a nadchádzajúce prezidentské voľby v USA. Každý z vás si už určite pozrel atraktívne video, na ktorom má osoba modifikovanú výpoveď a zrazu sme šírителmi dezinformačnej kampane. V súčasnosti už hovoríme o Deepfake as a Service s využívaním umelej inteligencie a tzv. deep learning technique. Do tretice sú tu riziká spojené s masívnym prechodom organizácií do cloudu bez potrebnej miery zabezpečenia dát a monitorovania správania sa používateľov v cloude.



Marek Král
výkonný riaditeľ Sec Tec

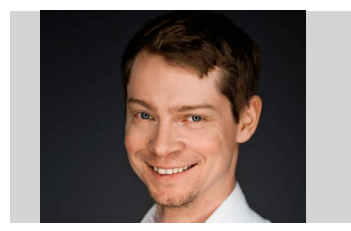
Tento rok priniesol nový spôsob myslenia a urýchlil veľa rozhodnutí. V krátkom čase sme sa posunuli až skokom k väčšej efektivite prace a bezpečnejšiemu zmýšľaniu. Bezpečnejšie sa správame nielen kvôli ochrane svojho zdravia, ale začíname si viac uvedomovať aj svoju zraniteľnosť v kybernetickom priestore. Táto zmena správania a napríklad aj správy o úniku citlivých zdravotníckych informácii zvyšujú povedomie o bezpečnostných hrozbách. Pozornosť, ktorú si kybernetická bezpečnosť zaslúži, by sa mala odraziť nielen v zvýšených investíciách, ale najmä vo vzdelávaní a budovaní povedomia.

Vladimír Frčo
Telekom & Network Security Specialist Orange Slovensko

Technicko-organizačné opatrenia súvisiace s pandémiou postihli tento rok asi každú firmu. Keďže u nás približne 90 percent ľudí mohlo pracovať z domu už predtým, mali sme priestor venovať sa aj iným oblastiam, napríklad vzdelávaniu v bezpečnosti používania (nielen) firemných zariadení. Keď sme napríklad zistili, že na firemných počítačoch stúpa množstvo opakujúceho sa malwaru a vzrástlo aj používanie video konferencií, dávali sme ľuďom návody, ako sa správať užívateľsky zodpovedne, čo robiť a čoho sa vyvarovať, aby čo najviac eliminovali riziká.

Richard Kiškováč
Security consultant Digital Systems

So zavedením opatrení proti šíreniu nákazy došlo k rapídnej zmene požiadaviek na bezpečnosť, na ktoré bol len málokto vopred dostatočne pripravený. Dochádzalo najmä k nutnosti používania ad-hoc, čiže rýchlych riešení na komunikáciu alebo prácu na diaľku, kde bezpečnosť nebola prioritou číslo jedna. Rapídne sa rozšírili príležitosti pre prípadné útoky – attack surface. Stredobodom sa stal používateľ, zamestnanec a jeho úroveň bezpečnostného povedomia. V plnej miere sa prejavili teórie o neexistujúcom perimetri, ktoré mimochodom nie sú novinkou. V každom prípade táto nová situácia priniesla mnoho nových výziev pre bezpečnostných manažérov a ukázala významné priority.



Tomáš Zaťko
výkonný riaditeľ Citadelo

Na prácu z domu často neexistovali bezpečnostné opatrenia, neboli pripravené bezpečné vzdialené prístupy a niektorí používali súkromné počítače infikované malvérom. Do toho chaosu prišiel zvýšený výskyt phishingových útokov a tie manipulujú ľudí k vyzradeniu prístupových hesiel a citlivých údajov. Zločinci pristupujú k agresívnym praktikám, ako je výzva „zaplaťte výkupné, ináč nakazíme vás aj vašu rodinu COVID-19“. Zamestnanci s radosťou otvoria prílohu s predmetom „COVID-19 bonus“ a bonusom nie je výplata, ale infikovaný počítač.

Marián Trizuliak
architekt kybernetickej bezpečnosti Západoslovenská distribučná

Dramatická situácia ohľadne pandémie a jej dôsledky. Prvým dôsledkom, ktorý sme pocítili asi všetci je okamžitý prechod na prácu na diaľku (z domu). Druhým, je zneužívanie tejto situácie útočníkmi na sofistikované útoky. Najvyšší dopad má ransomware (malware, ktorý zašifruje obsah pevného disku). Denne sa na internete objavujú informácie o malých, ale aj veľkých spoločnostiach, ktoré boli takto poškodené (12/2019 – poliklinika v českom Benešove). Útokom bezprostredne predchadzajú úniky informácií, čo v prípade veľkých spoločností zahŕňa nie len citlivé obchodné informácie, ale často aj osobné údaje zákazníkov.

Pavol Adamec
poradca pre riadenie rizík KPMG Slovensko

Tento rok výraznejšie ukázal, ako sa rozchádzajú porozumenie potrebám s realitou v našom prostredí. Či už kvôli novým zákon a reguláciám, novým útokom alebo novým pandémiám, firmy stále rozmýšľajú o čiastkových záplatách na aktuálny problém namiesto systematického prístupu k bezpečnostným rizikám. Neexistuje nejaká „bezpečnosť“ pre GDPR, „nejaká“ bezpečnosť kvôli audítorom, „nejaká“ kvôli požiadavkám odberateľa, „nejaká“ pre Zákon o kybernetickej bezpečnosti, „nejaká“ kvôli hackerom útočiacim na home office. Jedna firma znamená jedny bezpečnostné riziká a potrebu konzistentnej odpovede na ne.

Jana Puškáčová
manažérka útvaru IT bezpečnosti MOL IT & Digital Slovensko

Ak doteraz budovanie bezpečnostného povedomia koncových používatelov nemalo najvyššiu prioritu, v tomto roku nastáva zmena. Používateľ v obave o svoje zdravie v kombinácii s prácou z domu sa môže stať oveľa ľahšie obeťou kybernetického útoku. V minulosti sme dokázali aspoň približne identifikovať obsah ci typické znaky škodlivého mailu ci webovej stránky. Dnes je téma COVID-19 živnou pôdou nielen pre overené a neoverené fakty a informácie, ale aj vhodným odrazovym mostíkom pre prienik do firemných informačných systémov cez najslabšie ohnivko reťaze.

Ján Adamovský
Chief Security Officer Slovenská sporiteľňa

Pandémia kompletne zmenila mentálne nastavenie v korporátnom svete. To, čo sme kedysi považovali za nemožné, robiť z domu či vzdialene, sa zrazu stalo absolútne nevyhnutným pre zabezpečenie základného fungovania firiem. Prirodzenou výzvou bolo urobiť túto digitalizáciu bezpečne. Zaujímavým trendom sú aj nové typy útokov, kde sa viac pre-