Kronika roka od októbra do októbra

ANKETA

Pred rokom začali vychádzať špecializované prílohy Hospodárskych novín o kybernetickej bezpečnosti. Je to naliehavá téma naprieč všetkými segmentmi, sektormi a činnosťami. Ak ste online, ste ohrození.

EURÓPSKY MESIAC KYBERNETICKEJ BEZPEČNOSTI

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

Za posledný rok vidíme snahu vylepšovať narýchlo prijaté riešenia počas pandémie a pokračujúci presun do virtuálneho priestoru. Dôraz bol kladený na identifikáciu a autentifikáciu. Boli sme svedkami série rôznych útokov a s tým spojených únikov dát. Očakávame, že tento trend v spojení s využívaním a komplexnosťou cloudu bude pretrvávať.

Preto očakávame dôraz na šifrovanie a správu šifrovacích kľúčov. Phishingové útoky boli aj v poslednom roku najčastejším typom útokov. Ľudská psychológia funguje po stáročia rovnako a nestačila sa prispôsobiť dynamickému rastu technológií. Tie najzraniteľnejšie časti našej psychiky preto vyžívajú útočníci na manipuláciu. Oblasť vzdelávania vidíme ako jednu z najdôležitejších v prevencii pred kybernetickými útokmi.

Andrej Žucha
generálny riaditeľ ALISON Slovakia

Dlhý čas, rádovo v rokoch, sa hovorilo o posilnení bezpečnosti Slovenska na úrovni štátu. Až dnes môžeme povedať, že Slovensko má funkčné Národné centrum kybernetickej bezpečnosti SK-CERT. Každý štát by dnes už mal disponovať špičkovým útvarom, ktorý zabezpečuje národné a strategické aktivity v riadení kybernetickej bezpečnosti, v oblasti analýzy hrozieb aj koordinácie riešenia kybernetických bezpečnostných incidentov na celonárodnej úrovni. Jeho úlohy sú aj v oblasti výučby, vzdelávania, tréningov, ako aj výskumu.

Zároveň je na Slovensku tesne pred dokončením aj projekt dobudovania vládnej jednotky CSIRT. SK pre riešenie počítačových incidentov, ktorá je zameraná na služby spojené so zvládaním bezpečnostných incidentov a odstraňovaním ich následkov vo verejnej správe.

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

Lockdowny poslali milióny ľudí na home office, a to si uvedomili aj kybernetickí zločinci. Do internetu je „vystavených“ čoraz viac systémov, čo stálo aj za nárastom útokov hrubou silou, ktoré majú za cieľ prelomiť heslo. Útočníci sú neustále aktívnejší. Výrazne dominuje ransomvér, krádeže dát či vydieranie. Na Slovensku sa zintenzívnili podvody falošnej technickej podpory a oveľa uveriteľnejšie sú aj phishingové útoky.

Pozitívom napríklad bolo, že aj vďaka medzinárodnej spolupráci sa podarilo zničiť jeden z najrozšírenejších botnetov Emotet, čo spôsobilo pokles škodlivého kódu či škodlivých makier až o polovicu. Spoločná európska legislatíva v oblasti kybernetickej bezpečnosti priniesla zlepšenia kybernetickej ochrany sietí. Firmy či organizácie si zároveň uvedomili, aké veľké sú digitálne riziká, čoho dôkazom je nárast požiadaviek na tréningy zamestnancov.

Rastislav Janota
riaditeľ Národné centrum kybernetickej bezpečnosti SK-CERT

Objem zaznamenaných útokov rastie aj na Slovensku. Je to objektívny fakt a k nárastom štatistík zároveň prispieva aj postupný rast schopnosti detegovať útok. Najrozšírenejšou formou útoku je v súčasnosti phishing. Mailom alebo v kombinácii s telefonickým hovorom útočníka s obeťou, alebo prostredníctvom esemesiek. Útoky sú zároveň čoraz viac cielené – na konkrétnych používateľov a skupiny, alebo útoky nastavené s presne definovaným cieľom.

Pri dnešnej, typicky veľmi nízkej úrovni zabezpečenia vo firmách je ransomvérový útok často až prekvapivo úspešný a dokáže spôsobiť obrovské priame aj nepriame škody. Pri akejkoľvek stratégii obrany alebo budovaní odolnosti by sme mali mať na pamäti, že súčasné útoky sú postavené na zneužívaní jednoznačne najslabšieho prvku v bezpečnostnom reťazci, ktorým je človek, na ľudských chybách a na našej dôverčivosti a neznalosti.

Roman Čupka
hlavný konzultant spoločnosti Flowmon a CEO Synapsa Networks

Z prieskumov o stave informačnej a kybernetickej bezpečnosti pripravených spoločnosťami Flowmon, Synapsa, SecTec a Qu-Bit, do ktorých sa minulý aj tento rok zapojila zakaždým viac ako stovka slovenských organizácií, vidieť výrazný nárast obáv z ransomvéru a phishingu. Obavy sú na mieste, keďže incidenty spôsobené ransomvérom priznalo o tretinu viac respondentov než minulý rok.

Dobrá správa je, že rastie aj počet organizácií, ktoré plánujú zvýšiť rozpočet na bezpečnosť IT – medziročne ich je o 17 percent viac. Posúva sa tiež vnímanie v rámci technologických trendov, kde čoraz viac spoločností uvažuje nad zabezpečením cloudových služieb. Čo sa nezmenilo – a ani neočakávam, že sa mení bude – sú dve najväčšie potreby pre plnenie povinností v rámci bezpečnosti v organizáciách, a to vzdelávanie a dostupnosť ľudských zdrojov.

Ivan Makatura
generálny riaditeľ Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Najpodstatnejším míľnikom bolo prijatie Nariadenia Európskeho parlamentu č. 887, ktorým sa zriaďuje Európske centrum priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier. Tým sa začína nová éra spolupráce a podpory zo strany EÚ. A to s takým veľkým objemom peňazí, ktorý nebude možné minúť, ak nenájdeme dostatok zmysluplných projektov. Teraz je to už v kybernetickej bezpečnosti viac o našich reálnych schopnostiach než o sľuboch politikov a sladkých rečiach plagiátorov.

Minulý rok o takomto čase sme štartovali, pomerne odvážne, sériu príloh pri príležitosti Európskeho mesiaca kybernetickej bezpečnosti. Aj tohtoročný október nám pripomína, že posilniť spôsobilosti v kybernetickej bezpečnosti nie je až také zložité, ak si osvojíme niekoľko základných znalostí a niekoľko dobrých digitálnych zručností.

Igor Urban
regionálny manažér Forcepoint pre východnú Európu

To, o čom hovoríme u nás už dva roky, a plánovali sme, že to bude trvať ďalší rok, sa udialo zo dňa na deň. Mám na mysli masívny prechod infraštruktúry a aplikácií do cloudu, pracovníci po celom svete, potreba zabezpečenia vzdialeného prístupu a bezpečnosť dát.

Zaznamenali sme nárast počtu spoločností, ktoré sa cez noc stali „bezpečnostnými expertmi“ a chceli sa zviezť na tejto vlne. Pozitívne vnímam zvýšený záujem o informačnú bezpečnosť, táto téma sa celkovo dostáva viac do povedomia aj laickej spoločnosti, vidíme zvýšený nárast workshopov a inovatívnych foriem diskusií na sociálnych sieťach a podobne. Či sa to prejaví aj na vyššej miere bezpečnosti Slovenska ako takej, to ukáže čas, zatiaľ to tak nevnímam.

Anna Stehlíková
manažérka pre bezpečnostné licencie Micro Focus

Ak uplynulé mesiace niečo skutočne ukázali, tak to je schopnosť prispôsobiť sa zmenám. Vzdialený prístup je jednou z rozsiahlych a akútnych hrozieb. Manažéri kybernetickej bezpečnosti musia porozumieť, aké metódy kyberzločinci používajú. Ak dokážeme využiť umelú inteligenciu v oblasti hrozieb, automatizácia a reakcie sa stanú skvelým partnerom pre ochranu podnikov.

Zároveň mnoho firiem hľadalo cloudové riešenia, snažili sa zjednotiť a zjednodušiť komplexné IT a podnikanie. Schopnosť nielen detegovať, identifikovať, brániť sa, ale tiež predpokladať, rozporovať, obnoviť a rozvíjať je cestou od kybernetickej bezpečnosti ku kybernetickej odolnosti.

Vladimír Mlynarčík
riaditeľ pre región SR a ČR republiky Clico

Asi v máloktorom odvetví sa veci dejú a menia tak dynamicky ako v IT, a špeciálne v kyberbezpečnosti. Máme za sebou mesiace bohaté na incidenty, ktoré, aspoň tomu chceme veriť, by mali zásadným spôsobom meniť pohľad na priority v tejto oblasti. Za všetky spomeniem ransomvérový útok na taiwanský gigant ACER, ktorý vyústil v doteraz najväčšie výkupné – 50 miliónov amerických dolárov.

Ale rovnako máme, a aj lokálne, za sebou skvelé aktivity v oblasti vzdelávania zákazníkov. Tento mesiac sme po dlhšej prestávke absolvovali live konferenciu QuBit, kde zazneli skvelé myšlienky a skutočne inovatívne stratégie v dátovej bezpečnosti. Rok 2021 bude teda „výživný“, a od roku 2022 máme prirodzene ešte ambicióznejšie očakávania.

Daniel Hetenyi
regionálny manažér CyberArk

Pandémia spravila digitálnu transformáciu aj na Slovensku. Viac sa využívajú hotové cloudové aplikácie a používatelia majú možnosť vzdialenej práce. Týmto sa dostala do centra pozornosti v IT bezpečnosti ochrana identít. Mnohí spravili upratovanie a prepojili HR systémy s riadením identít. Používateľ tak dostával okamžite prístupy do systémov a aplikácií podľa svojej pracovnej roly.

Zároveň pre vyššiu ochranu identity vzdialeného používateľa sa začali využívať multifaktorové overovania, najčastejšie potvrdzovania v mobile cez push. Pre jednoduchšie nasadenie multifaktorovej autentifikácie sa začali využívať portály jednotného prihlásenia (single sign-on), ktoré raz overia používateľa a ten dostane prístup ku všetkým svojim aplikáciám. Firmy si tým zjednodušili správu identít, odľahčili VPNkám, zvýšili používateľský komfort prístupov a bezpečnosť identít sa posunula o pár úrovní vyššie.

Marek Král
generálny riaditeľ SecTec

Pretrvávajúca pandémia len potvrdila nové trendy a urýchlila zmeny. Náš život sa ešte viac posunul do online prostredia a badať zvýšený záujem a pochopenie, že rozumné investície do IT bezpečnosti sú nutnosť. Keďže mainstream určuje trend aj pre útočníkov, priestor na zlepšenie vidím práve v oblastiach ochrany identity, prístupu, šifrovania dát a bezpečnosti aplikácií už pri ich vývoji. Na to nadväzuje SIEM a to vytvára čoraz väčší tlak na automatizáciu. Popritom je potrebné neustále zvyšovať povedomie o bezpečnosti u bežných používateľov.

Slovensko nie je v oblasti IT bezpečnosti na tom až tak zle v porovnaní s inými krajinami. Problém Slovenska je byrokracia, a tým veľmi pomalá implementácia projektov, čo je hlavne v bezpečnosti kľúčové, keďže práve v tejto oblasti je potrebné reagovať rýchlo.

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

Od októbra 2020 vidíme neustále sa zvyšujúci nárast kybernetických incidentov, a to aj v oblasti ochrany osobných údajov. Na úrade evidujeme zvýšený počet incidentov, a to hlavne ransomvéru. Pribúdajú aj útoky na nezaplátané servery, ktoré mali známe zraniteľnosti a ktoré firmy často, či už vedome alebo nevedome, ignorovali. Útočníci sa takto potom ľahko dostali k osobným údajom. Nový model fungovania a práce formou vzdialeného prístupu sa stáva štandardom a prináša ďalšie možné riziká, ktoré budú útočníci využívať, aby sa dostali k dátam.

V tomto roku nám pribudla aj novela zákona o kybernetickej bezpečnosti. Avšak narazila na množstvo zásadných pripomienok zo všetkých sektorov, ako aj odbornej verejnosti.

Andrej Aleksiev
riaditeľ slovenskej pobočky Check Point Software Technologies

Už za prvý polrok toho roku vzrástol počet útokov na jednu organizáciu na Slovensku takmer o tretinu, ak to porovnávame s druhým polrokom 2020. Každá organizácia tu bola vystavená útokom priemerne 418-krát týždenne. Najvyššiu frekvenciu útokov zaznamenávajú banky a finančný sektor, až vyše šesťsto týždenne, potom nasleduje s počtom takmer stopäťdesiat pokusov priemyselná výroba.

Najpočetnejšími sú stále útoky vedené cez botnet a ich frekvencia sa zvyšuje. Zároveň zaznamenávame výrazný rast ransomvérových útokov, ktoré prichádzajú vo vlnách. Tento masívny nárast útokov búra zažitú predstavu, že nie sme zaujímavý štát pre hackerov. Práve naopak – sme súčasťou Únie a Severoatlantickej aliancie a pri súčasnom stave kybernetickej bezpečnosti na Slovensku slúžime ako tréningový priestor pre skupiny kybernetického zločinu a najmä sponzorovaných štátmi.