HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 16. – 18. OKTÓBRA 2020

Trend, ktorý si zaslúži pozornosť

ANKETA

V médiách sa často a opakovane prízvukuje, že firmy a organizácie čelia stále častejšie narastajúcim kybernetickým hrozbám. Mnoho z nich sa však stavia do defenzívy a premeškajú tak jedinečnú príležitosť získať konkurenčnú výhodu tým, že ako súčasť svojej stratégie akceptujú vylepšenú kybernetickú bezpečnosť a súkromie.

Pandémia spôsobila rozsiahle prerušenie implementácii kybernetickej bezpečnosti a očakáva sa, že to bude mať výrazný vplyv na stratégie, investície a budúce priority. Ak sa však pozeráme na súčasný stav ako na stav „nula", vzniká množstvo príležitostí a možností, ako prehodnotiť stav a zbaviť sa zastaralých postupov a falošných očakávaní. Aj pre kybernetickú bezpečnosť platí – teraz, alebo nikdy.

Prečítajte si, kam smerovať akčné rozhodnutia a ako vidia budúcnosť slovenskí lídri.

Ivan Makatura
generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti

Zvýšenú pozornosť venujem budúcemu auditu umelej inteligencie, aj keď tá s kybernetickou bezpečnosťou zdanlivo nesúvisí. Audit kybernetickej bezpečnosti je totiž posudzovanie bezpečnostných vlastností objektu voči formálnym definíciám. Statické pravidlá nebude možné uplatniť na posudzovanie umelej inteligencie, pretože tá sa učí a prispôsobuje okolnostiam. Otvára sa tým veľa technických, procesných aj etických otázok súvisiacich s auditom. Bude potrebné dohodnúť a normalizovať spoločné metodiky pre testovanie a audit kognitívnych systémov.

Rastislav Janota
riaditeľ Národného centra kybernetickej bezpečnosti SK-CERT

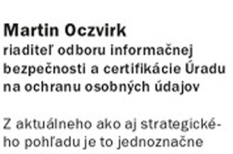
Umelá inteligencia bude hrať čoraz väčšiu rolu – nielen na strane útočníkov, ale aj na strane obrancov. Pri jej použití sú útočné aktivity efektívnejšie a obrana náročnejšia.Stupňujúce sa politické a ekonomické rozpory medzi Západom a Východom vyvolávajú zvýšené kybernetické riziká. Štátmi sponzorované aktivity a špionáž sú stále častejšie. Zároveň sa neustále otvárajú pomyselné nožnice medzi požiadavkami na vzdelaných ľudí v oblasti kybernetickej bezpečnosti a ich dostupnosťou.

Jaroslav Oster
predseda Správnej rady preventista.sk

Jedným z nespochybniteľných trendov, ktoré sú zreteľné už teraz a dá sa očakávať len ich nárast sú útoky postavené na princípoch sociálnej manipulácie. V krátkej dobe je očávateľný dynamický vzostup tém počnúc fake news, cez šírenie hoax správ až po cielený phishing na rôznych platformách (e-mailové správy, SMS, herné platformy, sociálne siete a ďalšie). Tento vzostup rizík prirodzene vytvorí tlak aj na požiadavky preventívneho pôsobenia na používateľov informačných systémov na všetkých úrovniach spoločnosti.

Tomáš Hettych
vicepredsedu ISACA Slovakia, Asociácia Auditu a Kontroly Informačných Systémov

Z môjho pohľadu audítora a konzultanta je jednou z najviac podceňovaných oblastí kybernetickej bezpečnosti analýza aktív, hrozieb a rizík. Bez týchto analýz a hlavne ich záverov je problematické vyhodnotiť pripravenosť organizácií na legislatívne a praktické požiadavky kybernetickej bezpečnosti, skôr to pripomína veštenie z kryštáľovej gule. Analýza aktív, hrozieb a rizík nám pomôže pri identifikácií kritických aktív a procesov a zároveň určuje prioritu implementácie navrhovaných opatrení. Výsledky analýz sú často dosť prekvapivé aj pre samotných vlastníkov procesov.



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

Z aktuálneho ako aj strategického pohľadu je to jednoznačne umelá inteligencia. Jej rola sa zvyšuje v kybernetickej obrane aj v kybernetických útokoch. Systémy umelej inteligencie budú čoraz komplexnejšie, dôležitejšie, ale aj dostupnejšie a bude jednoduchšie ich nasadiť. Ak bude umelá inteligencia skutočne autonómna, dokáže sa učiť omnoho efektívnejšie a rýchlejšie. A tieto vlastnosti nebudú prinášať iba úžitok a dobro, ale využijú ich aj rôzne zločinecké a teroristickými skupiny na páchanie obrovských škôd.

Lukáš Neduchal
podpredseda Správnej rady Asociácie kybernetickej bezpečnosti

Vyberám jeden z trendov, ktorý bude v budúcnosti stále významnejším. Neustále sa zvyšujú nároky na znalosti pracovníkov IT bezpečnosti, a to nielen vzhľadom na tempo vývoja technológií, ale aj na množstvo zraniteľností a hrozieb. A čo viac, nedostatok tých špecialistov je stále väčší. Tieto faktory budú podporovať vzostup automatizácie štandardných činností, prediktívneho správania sa systémov a zapájanie umelej inteligencie, už aj s využívaním algoritmov deep learning a umelých neurónových sietí. A to – bohužiaľ aj na strane finančne zaistených a motivovaných útočníkov.

Andrej Žucha
generálny riaditeľ Alison Slovakia

Kvantové technológie. Majú až fascinujúci vplyv na budúcnosť kybernetickej bezpečnosti a trestuhodne im chýba publicita a záujem politických lídrov. Využitie kvantových počítačov umožní dešifrovať nepredstaviteľné kvantum informácií a zmení silové polarizácie v politickom a následne hospodárskom usporiadaní sveta. Kvantová bezpečnosť nie je len technokratická otázka kryptovania, ale otázka budúceho usporiadania sveta.

Peter Dostál
generálny riaditeľ a predseda predstavenstva Aliter Technologies, a. s.

V poslednom období sme, aj z dôvodu pandémie COVID 19, zaznamenali častejšie prechody firiem so svojimi IT infraštruktúrami do cloudu. Zvyšujúca sa dôvera vo verejný, súkromný a hybridný dátový cloud pripravuje cestu pre nové výzvy. Cloudové bezpečnostné hrozby dávajú priestor prísnejším bezpečnostným protokolom a funkciám testovania bezpečnosti. Poskytovatelia a prevádzkovatelia cloudových riešení budú musieť čeliť tejto výzve a prinášať nové, kvalitnejšie riešenia a ešte viac a lepšie spolupracovať s poskytovateľmi bezpečnostných riešení.

Roman Čupka
hlavný konzultant Flowmon pre strednú a východnú Európu

Ľudské zdroje a s tým spojená automatizácia. Momentálne len v Európe chýba zhruba 300 tisíc špecialistov na kybernetickú bezpečnosť. Je to dvakrát viac ako vlani a tento rok sa nedostatok ešte prehĺbi. Ak má byť prevencia, detekcia a reakcia na kybernetické hrozby v súlade s legislatívnymi a biznis požiadavkami, je automatizácia nevyhnutná. Na druhej strane to neznamená, že na ľuďoch prestáva záležať. Práve naopak, človek naďalej zostáva tým najslabším článkom reťazca. Preto treba popri automatizácii dbať na kvalitné a plošné vzdelávanie, a to ako bezpečnostných špecialistov, tak aj bežných používateľov.

Andrej Aleksiev
riaditeľ pobočky Check Point Software Technologies na Slovensku

Najrozšírenejším malwarom dnešnej doby je jednoznačne cryptomining, ktorý predstavuje 17 percent všetkých útokov. Aktuálne známymi sú napríklad Emotet a XMRig a to ešte nie je to najhoršie. Cryptomining síce využíva výkon vášho zariadenia pre vlastné obohacovanie, avšak nie je taký deštrukčný ako DOUBLE EXTORSION ransomware typu Maze. Tento ransomware je síce menej rozšírený, ale dáta najprv zakryptuje a následne ich dekryptované publikuje na internete.

Igor Urban
regionálny manažér Forcepoint pre východnú Európu

Je nepochybné, že technológie nás menia a tak jednoznačným trendom je prechod z tzv. ukazovateľov kompromitácie na indikátor používateľského správania sa. Samozrejme to ide ruka v ruke s postupným prechodom organizácií do cloudu. Očakávame väčší nárast BYOD - využívania vlastných zariadení na prácu, nástup 5G a vzostup práce a vzdelávania na diaľku. Toto sú celosvetové trendy, aj keď Slovensko, či celá východná Európa v tejto oblasti ešte zaostávajú. A stále platí, že monitorovanie správania sa používateľov v cyber priestore je a bude kľúčové, akokoľvek strašidelne to vyznieva.

Marek Král
generálny riaditeľ SecTec

Téma kybernetickej bezpečnosti je veľmi komplexná a som rád, že sa jej ako celku dostáva viac pozornosti. Bezpečnosť sa chvalabohu za posledné krátke obdobie dostala natoľko do povedomia, že už nie je len luxusom, ale súčasťou rozpočtov a stratégií nielen firiem rôznych veľkostí a zameraní, ale aj štátov. Keďže kybernetické hrozby sú stále sofistikovanejšie a ich počet narastá, vytvára sa tak stále väčší tlak na bezpečnostné teamy a dobre vieme, že už dnes máme nedostatok bezpečnostných špecialistov. Preto sa treba zamerať na moderné next generation technológie, automatizáciu, AI alebo machine learning a špecializované SOC služby.

Jana Puškáčová
manažérka útvaru Informačná bezpečnosť MOL IT & Digital Slovensko

Automatizácia a digitalizácia síce uvoľňujú pre trh pracovnú silu, tá však nedisponuje potrebnými predpokladmi, znalosťami askúsenosťami na to, aby potlačila trend pretrvávajúceho nedostatku kvalitných a kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti.

Richard Kiškováč
Security Consultant Digital Systems, a. s.

O trendoch v kybernetickej bezpečnosti je možné hovoriť v dvoch rovinách - o útokoch a o ochrane pred nimi. Pri kybernetických útokoch môžeme očakávať stále vyššiu sofistikovanosť a profit. Pri ochrane vidím ako jasný trend postupný prechod k bezpečnostnému modelu, ktorý sa nazýva Zero Trust. Je založený na data-centrickom prístupe v kombinácii s využitím umelej inteligencie na identifikáciu hrozieb v reálnom čase a podporený efektívnym zvyšovaním bezpečnostného povedomia.

Tomáš Zaťko
CEO Citadelo, etický hacker

Bug bounty programy, ako napríklad slovenské HackTrophy. Ide o model testovania bezpečnosti, kedy organizácia dovolí etickým hackerom neustále hľadať diery v systémoch. Ak nejakú dieru nájdu, nahlásia ju a dostanú odmenu. V budúnosti budú takéto programy nevyhnutnou súčasťou bezpečnosti. Bez nich bude obrana systémov neudržateľná. Tlak množstva hackerov kriminálnikov z celého sveta je obrovský. Obrancov je spravidla menej. V takejto asymetrii obrancovia nemôžu vyhrať. Bug bounty programy tú nerovnosť pomáhajú zlepšiť v prospech obrancov.

Pavol Adamec
výkonný riaditeľ oddelenia Riadenie rizík KPMG Slovensko

Za zásadný trend považujem zameranie útočníkov viac na používateľa a ľudské slabiny ako na najnovšie a najvyspelejšie technológie. Tento trend je tu výrazne prítomný už niekoľko rokov. Čím viac technológií sa používa a rastie počet používateľov, tým je väčší rozdiel medzi možnosťami technológií a schopnosťou ľudí pochopiť ich možnosti a obmedzenia. Je jednoduchšie urobiť jeden systém bezpečným, ako naučiť tisíce jeho používateľov správať sa bezpečne. Priestor na strednodobú zmenu tohto trendu vidím v znižovaní komplexnosti systémov a súčasnom zvyšovaní ich bezpečnosti.

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

Fenomén Internet of Things (IoT) sa postupne dostáva do bežného života. Veci riadime na diaľku a veci riadia nás. Bohužiaľ, bezpečnosť v tejto oblasti je v plienkach. Použitie komponentov viacerých výrobcov, komplikovaná údržba, nezáujem výrobcu udržiavať softvér aktuálny - toto všetko nahráva útočníkom a navyše, ani zneužitie zraniteľností im nikto nekomplikuje. Vo svete je už zdokumentovaných viacero kybernetických útokov spôsobených zneužitím IoT zariadení a ich nedostatočným zabezpečením. A dôsledky takýchto útokov na bežný život môžu byť katastrofické.

Ján Adamovský
Chief Security Officer Slovenská sporiteľňa

V kybernetickej bezpečnosti dlhodobo platí veľká nerovnováha medzi útočníkom a obrancom. Obranca musí ochrániť všetky svoje systémy, pričom útočníkovi stačí nájsť jednu malú chybičku a už je vnútri v sieti. Za veľmi zaujímavý považujem trend „deception", čiže klamlivých technológií, kde spoločnosť rozmiestni do svojej siete rôzne falošné návnady a vhodným spôsobom sa na ne snaží útočníkov nalákať. Získava tak výhodu skoršieho zistenia útoku a možnosti reakcie pred tým, než je príliš neskoro.

V ďalších anketách sa každý októbrový piatok dozviete viac o kybernetickej bezpečnosti

- Najviac nedocenená oblasť na Slovensku
- Koho a čoho sa treba vyvarovať