HN
obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
28. – 30. MÁJA 2021

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Technológie v službách dobra a zla

Umelá inteligencia ako veda ponúka množstvo príležitostí pre uplatnenie v kybernetickej bezpečnosti a zároveň otvára intenzívnu diskusiu o etických aspektoch jej využívania. SNÍMKA: DREAMSTIME

TÉMA

Neutešujme sa, že sme malý štát, máme trhové limity a ťažký jazyk. Globalizácia a umelá inteligencia si už s tým poradili a kybernetický zločin má o nás záujem.

Slovensko zažíva viditeľný nárast škodlivých aktivít v kybernetickom priestore vo všetkých oblastiach.

Na množstve ohrození sa výrazne odrazilo zvýšenie aktivity kriminálnych a politických aktérov a napätá politická situácia. Zaplavili nás kampane na báze sociálneho inžinierstva, ransomvérové útoky a úniky dát.

Jednu dobrú správu však predsa len máme. Rastové čísla reprezentujú nielen objektívny nárast útokov, ale podieľajú sa na nich aj mierne zlepšujúce sa detekčné schopnosti organizácií – proste vidia lepšie do systémov.

Ransomvér na vzostupe

Vydieračský útok si nevyžaduje extrémne sofistikovaný prístup. Ransomware as a service (RaaS) je biznis model ako akýkoľvek iný. Znamená prenájom funkčnej infraštruktúry a vývoj softvéru na mieru. V minulom roku sa tak udiali dve tretiny ransomvérových útokov vo svete.

Potom stačí už vytrvalo posielať maily so škodlivým softvérom a čakať, ktorý naivný zamestnanec klikne na link alebo si stiahne aplikáciu. Útočníci po prieniku dáta skúmajú, zálohujú a šifrujú. Výkupné potom žiadajú za dešifrovanie, nezverejnenie a aj od tretej strany, ktorá je únikom postihnutá.

Tento model kybernetickej kriminality je taký agresívny a efektívny, že riešenie si vyžaduje intenzívnu komunikáciu všetkých sektorov aj štátov medzi sebou.

Toto si pamätajte

Súčasné bezpečnostné mechanizmy reagujú na zásadnú úlohu – chrániť informácie. Presun do cloudu a vzdialený prístup v covidovom roku nielen navždy zmenili svet, ale tiež nastavili budúcnosť.

Trendom sa tak stali autentizačné nástroje, viacvrstvová bezpečnosť, segmentácia, kognitívne spracovanie či zero trust princíp – zabezpečenie s nulovou dôverou, ktoré predpokladá, že každý používateľ alebo zariadenie nie sú vo svojej podstate dôveryhodné.

Vizionári v krátkodobom horizonte vkladajú nádeje do umelej inteligencie, v dlhodobom horizonte sa už zamýšľajú nad postkvantovou kryptografiou.

S umelou inteligenciou sa už poznáte

Ľudia sa nemôžu donekonečna „škálovať“, aby adekvátne chránili dynamické prostredie. Vedné odbory umelej inteligencie tu poskytujú nenahraditeľnú analýzu a identifikáciu hrozieb, na ktorú môžu odborníci reagovať, aby znížili riziko narušenia.

„V oblasti zabezpečenia dokáže AI identifikovať a uprednostniť riziká, okamžite odhaliť akýkoľvek malvér v sieti, usmerniť reakciu na incidenty a detegovať narušenie skôr, ako sa začne,“ vysvetľuje Vladimír Palečka, špecialista na kybernetickú bezpečnosť, Aliter Technologies, a. s.

Odborníci však vášnivo diskutujú o tom, že spoľahnúť sa iba na „super-evidované učenie“ je nebezpečný hazard. Algoritmy strojového učenia môžu vytvárať falošný pocit bezpečia. Systém sa totiž na základe skúsenosti učí, ktoré kódy sú súčasťou škodlivého softvéru a označuje ich. Obrana potom povolí iba softvér s „čistými“ kódmi. Čo sa však stane, ak sa hackeri dostanú do systémov bezpečnostnej firmy? Pozmenia vlastnosti kódu škodlivého softvéru, a tak ho obranný algoritmus nezachytí. Ďalší progres bude vyžadovať kombináciu hlbokých znalostí v kybernetickej bezpečnosti a zároveň v dátových vedách. „V každom prípade však umelá inteligencia patrí medzi kľúčové bezpečnostné mechanizmy v budúcnosti,“ predpovedá Vladimír Palečka.

Alfa a omega bezpečnosti

Dnes už takmer každé zariadenie obsahuje mikropočítač, ktorý neustále zbiera a vyhodnocuje údaje, ukladá ich alebo odosiela na analýzu iným systémom. Základom zabezpečenia informácií proti neautorizovanému sprístupneniu a zneužitiu je ich šifrovanie.

Nástup kvantových počítačov preto sprevádzajú očakávania i ľahká panika. Podstatné zvýšenie výpočtového výkonu počítačov umožní rozvoj nových vedných odborov aj prelomenie súčasných šifier. Terabajty dát zostanú bez ochrany.

Prakticky použiteľný kvantový počítač v tomto desaťročí asi neuvidíme. „Čakáme na zásadný prelom v technológii. No nemali by sme to podceňovať, ak prelom príde, už nebude dostatok času, bude to len otázka peňazí, veľa peňazí,“ varuje Peter Kopriva, bezpečnostný architekt Tatra banka.

> Dáta budú unikať vždy, či už v dôsledku technických, alebo ľudských chýb. Dôležité však je, ako budú šifrované.
>
> **Peter Rakšány,** špecialista ALISON Slovakia na ochranu utajovaných skutočností

Éra šifrovania

Väčším problémom ako zlomenie súčasných šifrovacích metód v budúcnosti je dnešok. „Súbežne s kvantovými počítačmi sa totiž vyvíja aj kryptografia a viac nás trápi súčasnosť,“ hovorí Peter Rakšány, špecialita ALISON Slovakia na ochranu utajovaných skutočností.

Povedomie o nebezpečenstvách v dôsledku laxného prístupu k údajom zostalo niekde v minulom storočí. Používatelia si bežne posielajú dáta do cloudu či ukladajú na prenajaté úložiská a nepýtajú sa, kto má „kľúče“ k ich chráneným dátam.

Ak je budúcnosť ekonomiky v cloude, tak budúcnosť cloudu je v šifrovaní. „Dáta budú unikať vždy, či už v dôsledku technických, alebo ľudských chýb. Dôležité však je, ako budú šifrované,“ uzatvára Peter Rakšány.

Tam, kde sú peniaze, tam sú útoky

„Sociálne inžinierstvo je z technologického hľadiska triviálne jednoduché, ale aktuálne je to jeden z najväčších problémov kybernetickej bezpečnosti,“ varuje Milan Pikula, zástupca riaditeľa Národného centra kybernetickej bezpečnosti SK-CERT. Tento fenomén stojí za drvivou väčšinou kybernetických útokov a miliónovými škodami. Zneužíva ľudskú naivitu, súcit, obavy, ale aj chamtivosť.

Je takmer nemožné ho eliminovať. A prečo odborníkom „uniklo“ sociálne inžinierstvo a vymklo sa? „Nestačí kúpiť škatuľu alebo napísať lepší softvér, treba vymeniť človeka. Ľudská psychológia funguje stáročia rovnako,“ vysvetľuje Milan Pikula.

Pre klasický marketing totiž platí množstvo obmedzení, ktoré zakazujú manipulatívnu reklamu a podprahové vnemy. Kybernetická kriminalita naopak – pracuje vo phishingových kampaniach presne s tými najzraniteľnejšími časťami vedomia a podvedomia.

Halier k halieru

V reálnom živote je oveľa menej spôsobov, ako nám niekto môže predať predražené hrnce alebo kradnuté auto. A tak najväčším problémom dneška, ktorému dominuje masívne využívanie umelej inteligencie na útok aj obranu, nie je auto hacknuté z letiaceho dronu.

Problémom sú obyčajné podvodné stránky a telefonáty. Lákajú od používateľov osobné údaje obratom použité na nákup tovarov a služieb na druhom konci sveta či prístupové heslá. Skutočnou zlatou baňou pre kybernetickú kriminalitu je masa bežných ľudí používajúcich internet.

MOTIVÁCIE KYBERNETICKÝCH ÚTOKOV

VIDINA PEŇAZÍ

ŠPIONÁŽ

NARUŠENIE ČINNOSTÍ

POLITICKÉ DÔVODY

ODVETA

350
MILIÓNOV USD
je priznaný objem výkupného v roku 2020.

43
PERCENT
je nárast priemerného zaplateného výkupného za prvý kvartál 2021 v medziročnom porovnaní.

287
DNÍ
trvá priemerne zotavenie z ransomvérového útoku.

SLOVENSKO

446
INCIDENTOV
je počet riešených incidentov škodlivého kódu v roku 2020.

325
PERCENT
je zvýšenie hlásených incidentov v zdravotníctve v roku 2020.

Zdroj: ENISA, Ransomware Task Force, NCKB SK-CERT

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. MÁJA 2021

Kedy konať rýchlo a ešte rýchlejšie

ANKETA

Dlhodobo a trpezlivo nám odborníci vysvetľujú, že kybernetická bezpečnosť je strategický a komplexný proces. Dnes sa ich však pýtame: ktorá oblasť kybernetickej bezpečnosti si vyžaduje extrémne pružné a dynamické rozhodovanie?

Ivan Makatura,
generálny riaditeľ, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Kybernetická bezpečnosť nie je disciplína každodenných zmien. Identifikácia zraniteľností a forenzná analýza si vyžadujú rozvahu a hlboké vedomosti, nie povrchné informácie a rýchle rozhodovanie. Aj reakcia na incidenty je proces, ktorého účinnosť je vyššia, ak bol vopred definovaný, otestovaný a nacvičený. Čo sa týka plánovaných úloh – ani jediná už neznesie odklad. Pridlho sa mnohé odkladali.

Rastislav Janota,
riaditeľ, Národné centrum kybernetickej bezpečnosti SK-CERT

Kybernetická bezpečnosť je vyváženým mixom strategického uvažovania a precízneho myslenia pre oblasť prevencie, budovania odolnej organizácie a dynamického rozhodovania pod stresom vo chvíli reálneho incidentu. Pre oba scenáre treba mať silný vedomostný základ, a to firmám väčšinou chýba.

Tomáš Hettych,
viceprezident, ISACA Slovakia

Aspoň dve oblasti si vyžadujú rýchlu reakciu: prvou je detekcia, prevencia a riešenie incidentov, druhou oblasťou je spustenie havarijných plánov alebo plánov kontinuity činností. Ak má organizácia dobre pripravené a otestované procesy riadenia kontinuity, pozná svoje riziká a infraštruktúru, tak je schopná rýchlo a efektívne reagovať na pravdepodobné krízové situácie a vyriešiť následky väčšiny incidentov.

Lukáš Neduchal,
podpredseda správnej rady, Asociácia kybernetickej bezpečnosti

Obe strany IT služieb, poskytovateľ aj príjemca, musia v prípade incident manažmentu reagovať pružne a dynamicky na základe dostupných parametrov a informácií. Minimalizovať dosahy krízovej situácie znamená vedieť sa rýchlo rozhodovať, čo, ako, s kým a v akom poradí treba vykonať, a to veľakrát aj mimo predpripraveného scenára. To, čo na papieri vyzerá ako jasne definovaný postup, je často dynamická, komplexná a kreatívna činnosť.

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

Jedna z dôležitých je oblasť monitoringu zraniteľností. Potom je to, samozrejme, aj určenie významnosti jednotlivých úloh pri riešení bezpečnostných incidentov. Každý deň sa objavujú nové hrozby, ktoré majú za následok možné bezpečnostné incidenty. Vždy sa treba zamyslieť, aké opatrenia môžem použiť? Ak nasadím do systému záplatu, znefunkční mi táto oprava inú funkcionalitu? Čím viac rozličných technológií, tým väčší rozsah možných zraniteľností.

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

V strese je dôležité dať každému špecialistovi a odborníkovi správnu úlohu a kompetenciu, povzbudiť ich a motivovať. Kybernetická bezpečnosť sa až nepredvídane špecializuje a stavia nás pred úlohy, ktoré sme si nevedeli ani predstaviť. Súhra tímu a identifikácia talentov budú mať čoraz vyššiu dôležitosť.

Tomáš Zaťko,
CEO, etický hacker, Citadelo

Reakcia na incidenty. Bezpečnostné prieniky aj havárie. Oboje znamenajú požiar, ktorý treba hasiť. Treba ho hasiť rýchlo, ale rozvážne. Aby sme nedbalým hasením nezničili to, čo ešte nezhorelo. Aby sme nezničili stopy vedúce k podpaľačovi.

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

Sledovanie zverejnených chýb v softvéri a opisov známych útokov spolu s monitorovaním a identifikáciou nových útokov si vyžadujú bezodkladný zásah vedúci k ochrane aktív. Všetky oblasti kybernetickej bezpečnosti si však vyžadujú extrémne pružné a dynamické rozhodovanie. S určitosťou môžeme povedať, že to, čo v tejto oblasti platilo včera, treba dnes prehodnotiť, bez ohľadu na krátkoči dlhodobé plány.

Roman Čupka,
hlavný konzultant spoločnosti Flowmon a CEO Synapsa Networks

Pružná a dynamická musí byť predovšetkým detekcia, reakcia a forenzné vyšetrovanie. Tieto činnosti vyžadujú pokročilé technológie, ktoré musia byť schopné pomocou behaviorálnych analýz a prvkov umelej inteligencie identifikovať podozrivé udalosti a incidenty, ale kladú tiež vysoké nároky na bezpečnostných špecialistov, ktorí sa preto pri svojej práci nezaobídu ani bez nástrojov na automatizáciu.

Vladimír Mlynarčík,
riaditeľ pre región Českej a Slovenskej republiky, Clico

Všeobecne najväčšie riziko v oblasti kyberbezpečnosti predstavujú zamestnanci. Práve táto skupina vyžaduje najdynamickejší spôsob manažmentu, respektíve rozhodovania o záležitostiach nastavení bezpečnostných politík, change manažmentu alebo iných bezpečnostných opatrení.

Richard Kiškováč,
bezpečnostný konzultant, Digital Systems, a. s.

V práci bezpečnostného manažéra je vyžadované extrémne pružné a dynamické rozhodovanie najmä pri riešení bezpečnostných incidentov. Každé rozhodnutie tu môže mať veľmi zásadný dosah. Musí to však byť odborné rozhodnutie, ktoré je výhradne v jeho kompetencii. Nie je vhodné, aby manažér bezpečnosti robil rozhodnutia v oblastiach, za ktoré zodpovedajú iní bez ohľadu na pružnosť a dynamiku prebiehajúcej udalosti.

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

Denne treba rozhodovať o tom, ako riadiť kybernetickú bezpečnosť v kontexte biznisu firmy, aby nebola považovaná len za záležitosť IT divízie. Nadmerné investovanie do najmodernejších technologických „hračiek“, podcenenie komplexnosti technického prostredia alebo nedostatočné pokrytie celého reťazca majú za následok neefektívny systém kybernetickej bezpečnosti. Čo v žiadnom prípade neznesie odklad, je kontinuálne vzdelávanie a budovanie bezpečnostného povedomia koncových používateľov.

Vojtech Gáborík,
riaditeľ úseku informačných technológií, Prvá stavebná sporiteľňa

Ak to zjednoduším, v kybernetickej bezpečnosti žijeme v troch oblastiach – prevencia, detekcia a reakcia. Každá oblasť vyžaduje inú dynamiku rozhodovania, ale pre všetky platí rovnaké pravidlo – rozhodnutie musí prísť v správnom čase. Najväčší časový luxus je v oblasti prevencie, to je jediná oblasť, v ktorej iniciatívu máte vo svojich rukách. Detekciou útoku začína rýchlo bežať čas a správne reakcie sú zásadné.

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

Reakcia na bezpečnostné udalosti, čiže udalosti, incidenty, zraniteľnosti a varovania. Kým pred pár rokmi stačilo na zraniteľnosti reagovať v dňoch až v týždňoch, posledné mesiace nám ukázali, že oneskorená reakcia znamená rozhodovanie o živote a smrti. Druhou oblasťou je aplikovanie dlhodobých bezpečnostných opatrení – čo je aplikované dnes (často aj veľmi drahé), už o pár dní nemusí platiť a musíte byť veľmi kreatívni a flexibilní pri hľadaní vhodných opatrení.

Pavol Adamec,
výkonný riaditeľ oddelenia Riadenie rizík, KPMG Slovensko

Neexistuje oblasť, v ktorej by ste si mohli dovoliť ísť „podľa skriptu“ a nereflektovať na okolie. Pre mňa je najzaujímavejšia pružnosť a dynamika potrebná, keď vytvárame pre klienta niečo úplne nové, úplne nový rámec. Nikdy nerobíte tú istú vec rovnakým spôsobom. Každý klient má inú kultúru, iné zvyky, iný regulačný rámec, iný systém rozmýšľania. Ak to nepochopíte, zlepšenie sa u klienta nechytí.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov, Tatra banka

Dnes je rýchle rozhodovanie nevyhnutné pri vytváraní inovatívnych riešení. Takéto riešenie väčšinou rúca zabehané bezpečnostné bariéry. Často spoluvytvárame nové prvky a postupy informačnej bezpečnosti, aby sme mohli naplniť štandardné aj vysnívané požiadavky klienta. Napriek novátorstvu rozhodnutia musia byť profesionálne, zodpovedné a funkčné, preto ich sprevádza aj nadšenie a aj časový stres.

Tibor Paulen,
manažér informačnej bezpečnosti, Stredoslovenská distribučná, a. s.

Jednoznačne je to reakcia na závažný bezpečnostný incident. Možných scenárov je tak veľa, že nie je možné sa na každý z nich vopred detailne pripraviť. Ak by takáto situácia nastala, budeme ju riešiť metódami krízového riadenia. Každý krok budeme plánovať dynamicky na základe vyhodnotenia úspešnosti predchádzajúcich krokov a vývoja samotnej situácie. Zvládnutie incidentu si vyžaduje extrémne pružné a dynamické rozhodovanie

Vladimír Jančok,
vedúci oddelenia Informačná bezpečnosť, VÚB, a. s.

Typickou oblasťou je riešenie bezpečnostných incidentov, či už externých alebo interných v rámci organizácie. Často je potrebné pružne rozhodovať v momentoch, keď bezpečnostný incident priamo obmedzuje poskytovanie základných služieb a je nutné čo najskôr identifikovať jeho príčinu, rozsah a prijať opatrenia na zamedzenie škodám. Dynamické rozhodovanie musí byť podporené dobrým plánovaním zdrojov.

Henrich Šnajder,
manažér informačnej bezpečnosti Orange Slovensko, a. s.

Ak sa dozviete o bezpečnostnej hrozbe alebo vážnej zraniteľnosti, na ktorú špeciálne neexistuje ani len záplata, a vaše systémy sú vystavené do verejnej siete, je čas bezodkladne konať s cieľom vyhnúť sa bezpečnostnému incidentu. Rovnako to platí aj pri samotnom incidente, ak naň včas a správne zareagujete, je veľmi pravdepodobné, že dokážete odvrátiť vážne škody.

Robert Mramúch,
manažér kybernetickej bezpečnosti, MH Teplárenský holding

Každodenná agenda spočíva v úlohách, ktorých základom je podporovať a chrániť predmet činnosti alebo služby daného podniku. Pod úlohami si predstavme čokoľvek – od kontroly a analyzovania logov, teda systémových akcií zaznamenaných v každom PC, až po tvorbu politík a smerníc. K denným povinnostiam patrí sledovanie zraniteľností systémov – ak sa také u vás objavia, je potrebné bezodkladne konať.

Ján Adamovský,
riaditeľ bezpečnosti, Slovenská sporiteľňa

Kľúčová je reakcia na prebiehajúci bezpečnostný incident. Toto je oblasť, kde je dôležitá čo najrýchlejšia detekcia, identifikácia dosahu na spoločnosť, zapojenie všetkých stakeholderov a návrh opatrení. Bez pružného a dynamického rozhodovania môže zlyhať podstatný krok – samotné prijatie opatrení. Preto odporúčam takéto krízové situácie, vrátane robenia rozhodnutí, trénovať v pokojných časoch. Aby bola aj vaša organizácia pripravená čeliť prípadným útokom či krízam.

Jaroslav Oster,
predseda správnej rady, Preventista.sk

Vzhľadom na reálny stav riadenia bezpečnosti vo všetkých sektoroch by bolo možné povedať, že pružné a dynamické rozhodovanie vyžaduje každá oblasť riadenia bezpečnosti. Zvláštnu pozornosť najmä z hľadiska operatívneho rozhodovania si určite vyžaduje incident manažment, a to od okamihu identifikácie incidentu cez proces jeho analýzy, hľadania nápravných opatrení až po jeho vyriešenie.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií, Volkswagen Slovakia

Určite je to rozhodovanie o opatreniach minimalizujúcich dosah bezpečnostného incidentu. Špeciálne pri závažných incidentoch, ako napríklad šírenie malvéru alebo hekerský útok. V takýchto prípadoch musí rýchlo a pružne fungovať celý tím. Dynamicky a flexibilne niekedy tiež treba reagovať na operatívne požiadavky úprav opatrení kybernetickej bezpečnosti v prostredí nepretržitej výroby, akými sú urgentné zmeny, bezpečnostné výnimky a podobne.

Roman Varga,
manažér kyberbezpečnosti, Dôvera, zdravotná poisťovňa, a. s.

V sektore zdravotníctva úspešne realizovaný kybernetický útok dokáže ochromiť kľúčové digitálne služby na niekoľko týždňov. Bezodkladná je reakcia na takéto úspešné kybernetické útoky, a to v podobe správneho nastavenia postupu eliminácie škôd a zabezpečenia dôkazov. Bezodkladná je následne komunikácia dovnútra spoločnosti a na dotknutých odberateľov kompromitovaných služieb.