HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
25. – 27. NOVEMBRA 2022

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Dá sa zomrieť na kybernetický útok?

TÉMA

V inštitúciách, ktoré zažili kybernetický útok, nahradili výpadok informačného systému zamestnanci s perom a papierom. Ale dá sa to v prípade zdravotníctva?

Prvé úmrtie pacienta spôsobené následkami kybernetického útoku zaznamenala Európska únia v roku 2020. FOTO: DREAMSTIME

Predstavte si incident v nemocničných informačných systémoch alebo pri prenose dát z laboratórií do ordinácií. Niekto zmení krvné parametre alebo predoperačné výsledky alebo zašifruje údaje.

A tu si určite viete živo predstaviť aj následky na liečbu a život pacienta. Navyše, ak sa útočníci dostanú k údajom, zašifrujú ich a vydierajú zverejnením organizáciu aj pacientov.

Kto všetko o vás vie

V zdravotníctve je okrem dôvernosti extrémne dôležitá integrita chránených dát. A to už je háklivá téma pre každého z nás. Za ostatné roky totiž povedomie o ochrane osobných údajov na Slovensku markantne narástlo najmä vzhľadom na kybernetické incidenty.

„Už len z dôvodu, s akými citlivými údajmi a v akom množstve s nimi pracujeme, sa kybernetická bezpečnosť a odolnosť voči hrozbám stanú súčasťou reputácie nemocníc," hovorí riaditeľka Nemocnice s poliklinikou sv. Lukáša v Galante Alexandra Pavlovičová.

Ide o všetko

Útočníci dnes využívajú umelú inteligenciu už vo fáze prieskumu profilov sociálnych médií a verejne dostupných zdrojov. Následne replikujú komunikáciu dôveryhodných kontaktov či subjektov, vytvárajú presvedčivé falošné zvukové alebo obrazové správy a distribuujú ich.

Phishingové útoky sú čoraz lepšie cielené a vytvorené tak, aby obišli tradičné detekcie e-mailov. V magickom trojuholníku ľudia, procesy, technológie sú jednoznačne najzraniteľnejší ľudia. V strese a pod tlakom práce robia chyby.

Aby sme nechodili ďaleko po príklad – vo phishingovom penetračnom teste v Národnom ústave tuberkulózy, pľúcnych chorôb a hrudníkovej chirurgie desať percent používateľov reagovalo na evidentne podvrhnutý mail zadaním mena a prístupového hesla do systému.

Územie nikoho

Z pohľadu financovania, poddimenzovaného personálu a podmienok, v ktorých zdravotníci pracujú, sa Alexandra Pavlovičová domnieva, že kyberbezpečnosť je u nich na pokraji záujmu: „Vnímam to tak, že sa budú musieť postupne naučiť takmer všetko."

Vedúci oddelenia informatiky v Národnom ústave tuberkulózy Jozef Zoričák našiel územie nikoho. „Aktuálne najväčšie ohrozenie je medzi stoličkou a klávesnicou koncového zariadenia nemocničného informačného systému."

V praxi sa často stretáva s tým, že akútny nedostatok zdravotníckych pracovníkov vytvára pocit beztrestnosti či ignorovanie pravidiel kybernetickej bezpečnosti v sektore. To všetko značne zvyšuje riziko bezpečnostného incidentu.

Bez kompromisov

Kybernetické útoky na nemocnice čoraz viac ohrozujú kontinuitu a kvalitu zdravotnej starostlivosti a sú čoraz častejšie a vážnejšie. „Hovoríme o úniku dát pacientov, ktoré sa následne predávajú na dark nete, o sociálnom inžinieringu s úmyslom získať prístup do špecifických aplikácií a o ransomvéri a wiperi, ktorý sa snaží zablokovať celé informačné systémy," upozorňuje Andrej Alexiev partner spoločnosti Kreston.

Riešenie vidí v tom, že musíme okamžite a adekvátne zvýšiť kybernetickú bezpečnosť vo všetkých zdravotníckych zariadeniach na Slovensku, angažovať kvalifikovaných odborníkov IT bezpečnosti a kvalitne zaškoliť celý zdravotnícky personál.

> Na Slovensku máme asi 15-ročný dlh voči celej IT prevádzke v zdravotníctve.
>
> **Andrej Mišura,** audítor kybernetickej bezpečnosti

„Ochranu musíme postaviť na troch pilieroch, ako je architektúra nulovej dôvery, automatizácia a aktívne prvky bezpečnosti," prízvukuje po rokoch skúseností v bezpečnostnej brandži.

Sme v hodine dvanástej

Andrej Alexiev poukazuje na to, že zatiaľ čo sa snažíme znížiť deficit a zabezpečiť vyvážené hospodárstvo, vytvárame si nový – kybernetický dlh, ktorý môže byť gigantickejší ako všetky, ktoré sme dodnes spoznali.

Pridáva sa aj audítor kybernetickej bezpečnosti Andrej Mišura zo spoločnosti auditori.it: „Na Slovensku máme asi 15-ročný dlh voči celej IT prevádzke v zdravotníctve. Opravujeme len to, čo sa aktuálne pokazilo a chýbajú peniaze."

A pritom do plánu obnovy si Slovensko napísalo ciele ako digitalizácia a telemedicína. Z hľadiska IT a bezpečnosti sú to zásadné zmeny, keďže súvisia so zdieľaním citlivých údajov a ich publikovaním „do sveta" za chránený perimeter.

Ani zásuvka, ani polica

Audit kybernetickej bezpečnosti by už dnes mala mať za sebou väčšina organizácií zaradených medzi prevádzkovateľov základnej služby.

Auditová správa by nemala byť len pre Národný bezpečnostný úrad, ale je dôležitá pre samotné organizácie, pre manažérov bezpečnosti a štatutárov. Výsledok auditu môže byť dobrý návod, ako uchopiť riadenie bezpečnosti. A to vlastne platí pre všetky organizácie, keďže auditová správa neskreslene ukazuje slabé miesta v bezpečnostných opatreniach.

Už keď sa vedenie rozhodne

Pri výbere dodávateľa služieb kybernetickej bezpečnosti stoja všetci pred úlohou, ako nájsť toho dôveryhodného. Preto by si zadávatelia mali overovať referencie, komunikovať s kolegami z podobných organizácií a pozvať si potenciálnych dodávateľov na stretnutie.

Ak nemáte expertízu interne alebo chcete len počuť iný názor, zavolajte si aj nezávislých odborníkov na posúdenie kandidátov. Prípadne spolu pripravte otázky tak, aby ste jasne definovali ciele spolupráce. Najnižšia cena nie je vždy práve to, čo potrebujete.

Ako veľký fanúšik zdieľania zdrojov odporúča Andrej Mišura spojiť sa napríklad s inými nemocnicami v regióne: „Vytvorte klaster a objednajte si služby a bezpečnostné technológie spoločne. Prinesie to minimálne dva efekty – ušetríte a vytvoríte priestor pre zdieľanie know-how a vlastných skúseností."

Ítečkári nemôžu čakať

Siete súkromných nemocníc majú vytvorené odbory kybernetickej bezpečnosti a zariadenia sú interne prepojené. Jozef Zoričák poukazuje na to, že tu sú v nevýhode štátne nemocnice, ktorým rezort zdravotníctva nepomáha finančne, metodicky ani technicky.

Dobrou myšlienkou je spolupráca zariadení a hľadanie spoločných riešení. Zástupcovia IT oddelení štátnych nemocníc preto iniciovali Fórum kybernetickej bezpečnosti nemocníc Slovenska ako platformu pre spoluprácu.

A hlavná úloha zdravotníckych zariadení? Kybernetická bezpečnosť vyžaduje veľké finančné prostriedky, preto sa treba usilovať získať ich aj z operačných programov. „Musíme sa naučiť zvládnuť administratívne náročnú žiadosť a následne projekt zrealizovať a aplikovať v praxi," uzatvára správca IT systémov s takmer tridsaťročnými skúsenosťami.

DÁTOVÝCH ÚNIKOV PRIBÚDA

82 percent
narušení ochrany údajov vo svete spôsobil ľudský faktor

Vektory kybernetických útokov
- Phishing
- Ukradnuté používateľské oprávnenia
- Chyby

61 percent
incidentov spôsobili útoky cez dodávateľský reťazec

Finančné dôvody
sú najčastejšia motivácia útokov

67 percent
incidentov v zdravotníctve malo za výsledok neoprávnený prístup k uniknutým údajom

Zdroj: 2022 Data Breach Investigations Report

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · ESET · Progress · MICRO FOCUS · Qubit · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 25. – 27. NOVEMBRA 2022

Čo nás neminie a čoho sa obávať

ANKETA

Bezpečnostní profesionáli mapujú udalosti a technológie a každý deň sa pripravujú na ten ďalší. Ktoré trendy a témy v kybernetickej bezpečnosti považujú za kľúčové v roku 2023?

Ján Grujbár,
generálny riaditeľ
Aliter Technologies

V rámci kybernetickej bezpečnosti budú naďalej dominovať existujúce vektory útokov zamerané na koncových používateľov. Očakávame naďalej zvýšené množstvo phishingových a ransomvérových útokov či sofistikovanejšie využívanie techník sociálneho inžinierstva. To, čo je „nové“ a bude prítomné aj v ďalšom období, sú hacktivisti a ich šírenie hoaxov a dezinformácií, na ktoré je Slovensko mimoriadne náchylné a stále nie je spôsobilé im efektívne čeliť.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Požiadavky, ktoré kladie súčasný svet na bezpečnosť, presahujú kapacity iba jednej technológie a jedného výrobcu. Bezpečnostné riešenia sú už teraz zložené z viacerých vrstiev a smerujú k maximálnej adaptabilite. A ani to už nebude stačiť. Začína sa etapa bezpečnostných služieb.

Matej Šalmík,
riaditeľ odboru vzdelávania, podpory a medzinárodnej spolupráce
Národné centrum kybernetickej bezpečnosti SK-CERT

Verím, že budúci rok, ako aj tie nasledujúce budú pokračovať rastúcim záujmom o tému kybernetickej bezpečnosti. Dosť už bolo sťažovania sa a lamentovania. Znamená to nepoľaviť v našej snahe urobiť pre tému maximum, aby sme vytvorili dobrý základ pre ďalšiu generáciu nadšených bezpečákov, ktorí bezpochyby prídu.

Martin Florián,
generálny riaditeľ sekcie kybernetickej bezpečnosti
MIRRI SR

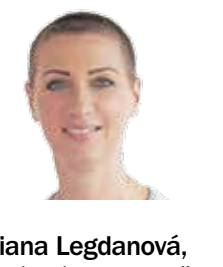
Tým, že sa škodlivý softvér stáva lacný a ľahko dostupný, predstavuje kybernetický zločin drastickú hrozbu najmä pre malé a stredné podniky a pre samosprávu. Týmto subjektom chýbajú kapacity takmer vo všetkých oblastiach informačnej bezpečnosti, a tak zatiaľ čo sa schopnosti útočníkov zlepšujú, zraniteľnosť menších organizácií rastie kritickým tempom. Sme v kybernetickej vojne a za kľúčovú povinnosť považujem budovanie kybernetického štítu pre Slovensko.

Ján Adamovský,
riaditeľ bezpečnosti
Slovenská sporiteľňa

Pokračujúcu konsolidáciu bezpečnostných technológií a automatizáciu procesov a reakcií na podozrivé udalosti. Vnímam výrazný nárast počtu útokov, či už voči spoločnostiam, ako aj jednotlivým osobám. Útoky a pokusy o podvod sa stávajú ľahko dostupnou komoditou. Považujem preto za nevyhnutné si doma vo firmách upratať a zefektívniť vnútorné fungovanie v oblasti kybernetickej bezpečnosti, aby boli naše spoločnosti dostatočne pripravené čeliť prichádzajúcim výzvam.

Miroslav Chlipala,
partner Advokátska kancelária Bukovinský & Chlipala

Kybernetická bezpečnosť musí byť takou samozrejmosťou, akou je zamykanie bytu, dodržiavanie bezpečnosti na ceste, pri práci alebo na lyžiarskom svahu. Je potrebné sústrediť sa na prebudenie záujmu o kybernetickú bezpečnosť na úrovni jednotlivca. Oplatí sa to!



Diana Legdanová,
vedúca úseku bezpečnosti
Východoslovenská energetika Holding

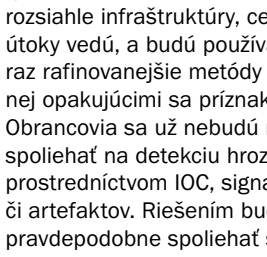
Závisí od uhla pohľadu a vyberám si ten netechnický. Kľúčovou témou bude naďalej vytváranie podmienok pre výchovu a vzdelávanie nových kyberšpecialistov, od študentov až po junior-medior-seniorov.

Tomáš Masný,
riaditeľ informačnej bezpečnosti
Slovak Telekom & T-Mobile
Česká republika

Domnievať sa, že implementácia nových bezpečnostných technológií a zapojenie partnerov stačí na znižovanie rizík v kybernetickej bezpečnosti, je naivné. Uvedomelý postoj „ja som zraniteľnosť“ je základným predpokladom úspešnej bezpečnostnej stratégie. Takýto jednotlivec je ďalšou vrstvou obrany. Systematické budovanie bezpečnostnej DNA spoločnosti, „ja som zodpovedný“, bude kľúčové.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC
Soitron

V oblasti kybernetických hrozieb bude pokračovať nepríjemný trend zvyšovania ich sofistikovanosti. Útočníci dokážu čoraz rýchlejšie postaviť (a demontovať) rozsiahle infraštruktúry, cez ktoré útoky vedú, a budú používať čoraz rafinovanejšie metódy s menej opakujúcimi sa príznakmi. Obrancovia sa už nebudú môcť spoliehať na detekciu hrozieb prostredníctvom IOC, signatúr či artefaktov. Riešením bude pravdepodobne spoliehať sa viac na detekciu anomálií, využívanie strojového učenia a umelej inteligencie.



Róbert Mramúch,
manažér kybernetickej bezpečnosti
MH Teplárenský holding

Veľa subjektov bude stále doťahovať medzery v základných oblastiach kybernetickej bezpečnosti – manažment rizík, vyhodnocovanie dátových tokov, aktivity spojené so zabezpečením kontinuity činností. U nás sa postupne dostávame k využitiu behaviorálnej analýzy používateľského správania v digitálnom priestore. Pričom vo svete už rezonuje využitie umelej inteligencie v SIEM.

Marián Trizuliak,
architekt kybernetickej bezpečnosti
Západoslovenská distribučná

Osobne sa domnievam, že bude ešte veľmi veselo. Zvyšujúca sa sofistikovanosť phishingových útokov – správne zvolená téma pre cieľovú skupinu adresátov, zaslaná v správnom čase a správnym spôsobom ako e-mail, SMS alebo whatsappka, nám ešte narobí veľa vrások. Druhý trend, ktorý vnímam ako oveľa nebezpečnejší, je veľmi jednoduché podliehanie a akceptácia fake news.

Peter Dufek,
manažér kybernetickej bezpečnosti
Procare a Svet zdravia

Vzhľadom na súčasnú geopolitickú, hospodársku a energetickú situáciu očakávam zvýšený záujem o poskytovateľov cloudových služieb. Nielen pre rastúci trend práce z domu, ale aj z dôvodu finančných a energetických úspor. S tým pôjde ruka v ruke výraznejšie zapojenie umelej inteligencie v eliminácii nezákonného, dezinformačného a škodlivého obsahu na internete.

Daniel Chromek,
riaditeľ informačnej bezpečnosti
ESET

Za kľúčový trend považujem nárast požiadaviek na súlad. Najmä kvôli prichádzajúcim reguláciám, ako je napríklad direktíva NISv2. Tieto následne ovplyvnia aplikovanie bezpečnostných opatrení vo viacerých odvetviach a vo viacerých oblastiach informačnej bezpečnosti.

Zuzana Halásová,
vedúca oddelenia kybernetickej bezpečnosti
Ministerstvo vnútra SR

Za kľúčový trend považujem legislatívne zmeny. Bude zaujímavé sledovať národný prístup k transpozícii novej smernice NIS2. Začína rezonovať množstvo notifikačných povinností, ktoré majú prevádzkovatelia či poskytovatelia smerom k národným regulátorom. Bude potrebné ich optimalizovať a časom zjednocovať, ako aj odstraňovať kolízie v existujúcich predpisoch. Rok 2023 bude aj rokom druhého kola auditov kybernetickej bezpečnosti a predpokladám, že sa začnú aj ďalšie správne konania a prvé súdne konania v tejto oblasti.

Anna Stehlíková,
manažérka pre bezpečnostné licencie ČR a SR
Micro Focus

Počet kybernetických útokov a ich kombinácií bude rásť. Uvedomuje si to čoraz viac firiem a hľadajú komplexné riešenia vrátane Threat Intelligence nástrojov. Nevyhnutnou už bude automatizácia na princípoch umelej inteligencie, ktorá zvyšuje efektivitu detekcie hrozieb a pomáha zamerať sa na skutočné riziká a ich redukciu v čase. Kybernetická bezpečnosť sa stáva súčasťou obchodných procesov, aplikácií aj kultúry organizácií.

Tibor Paulen,
manažér informačnej bezpečnosti
Stredoslovenská distribučná

Vývoj v poslednom období spôsobil, že najslabším článkom kybernetickej bezpečnosti sa stal používateľ. Teda my všetci. Už sa nedá spoliehať len na to, že nás ochráni náš poskytovateľ IT služby. Stali sme sa aktívnou súčasťou hry a bolo by dobré poznať jej pravidlá. Mali by sme sa začať o túto tému viac zaujímať a vzdelávať, aby sme pochopili, kde sme ako používatelia zraniteľní a čo s tým vieme urobiť.

Marián Illovský,
audítor kybernetickej bezpečnosti
Auditori.it

Myslím si, že v roku 2023 budeme musieť začať viac riešiť použitie, respektíve zneužitie umelej inteligencie pri výrobe falošných zvukových nahrávok a videí. Pokrok v tejto oblasti je enormný a možno sa dočkáme aj toho, že v súčasnosti používaná hlasová biometria bude zrazu nepoužiteľná. Všetky možnosti, ako a kde všade sa dá táto technológia zneužiť, si asi ani nevieme v súčasnosti predstaviť.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií
Volkswagen Slovakia

Mali by to byť témy, akými sú kontinuálne zvyšovanie bezpečnostného povedomia vo firmách, v školách a v súkromí. Za významné tu považujem testovanie schopnosti reakcie na kybernetický útok, čiže overovanie efektívnosti bezpečnostných opatrení a reakcie na evolúciu kyberútokov. Pozornosť bude treba venovať aj „starým“ témam, ako sú zabezpečenie prevádzkových technológií a kritickej infraštruktúry a IoT zariadení či zabezpečenie cloudových služieb.

František Mesiarkin,
špecialista pre informačnú bezpečnosť
Letové prevádzkové služby

Trendov je veľa, ale všetko stojí a padá na uvedomení si závislosti našich životných činností od zabezpečenia kybernetickej bezpečnosti. Ak chýba uvedomenie, aj najsofistikovanejšie riešenia sa budú aplikovať len formálne. Začať treba výmenou relevantných (aj zlých) skúseností a poznatkov na úrovni, kde si osoby rozumejú a majú zhodné chápanie pojmov. Výsledkom zdieľania bude precitnutie a následne potreba vedieť a robiť viac.

Rastislav Beňo,
manažér informačnej bezpečnosti
Mitsubishi Chemical Advanced Materials

V situácii, keď je potrebné reagovať na nové hrozby, integrovať svet informačných a prevádzkových technológií a prevádzkovať čoraz robustnejšie systémy, je veľmi ťažké nájsť špecialistov informačnej bezpečnosti. Vzdelávacie inštitúcie opúšťa veľmi málo kvalifikovaných špecialistov, a tak prevychovávame itečkárov, ktorých je tiež nedostatok. Nepovažujem to za chybu, ale akútny problém to nerieši.

Roman Čupka,
hlavný konzultant Progress | Flowmon a CEO Synapsa Networks

Bude to opäť téma umelej inteligencie a automatizácie v konštelácii s prijímaním a implementáciou týchto trendov v technologických firmách. Tie následne prostredníctvom svojich produktov a služieb signifikantným spôsobom menia správanie spotrebiteľov a ovplyvňujú používateľské návyky firiem a verejných inštitúcií. A v konečnom dôsledku formujú celý trh s kybernetickou bezpečnosťou.

Timea Tomčová,
manažérka kybernetickej bezpečnosti Uniqa

Kľúčová téma na rok 2023 sa prirodzene odvíja a líši od úrovne vyspelosti danej organizácie v oblasti informačnej, respektíve kybernetickej bezpečnosti. Určite by som ani pri vyspelej organizácii nepodceňovala pripravenosť ľudí a procesov na riešenie reálneho kybernetického incidentu. Ťažko na cvičisku, trošku ľahšie na bojisku – takže medzi kľúčové témy odporúčam zaradiť rôzne formy tabletop cvičení, ktoré pomáhajú preveriť pripravenosť organizácie na rozličné scenáre kybernetických incidentov.

Miroslav Michalko,
vedúci Laboratória počítačových sietí
Technická univerzita v Košiciach

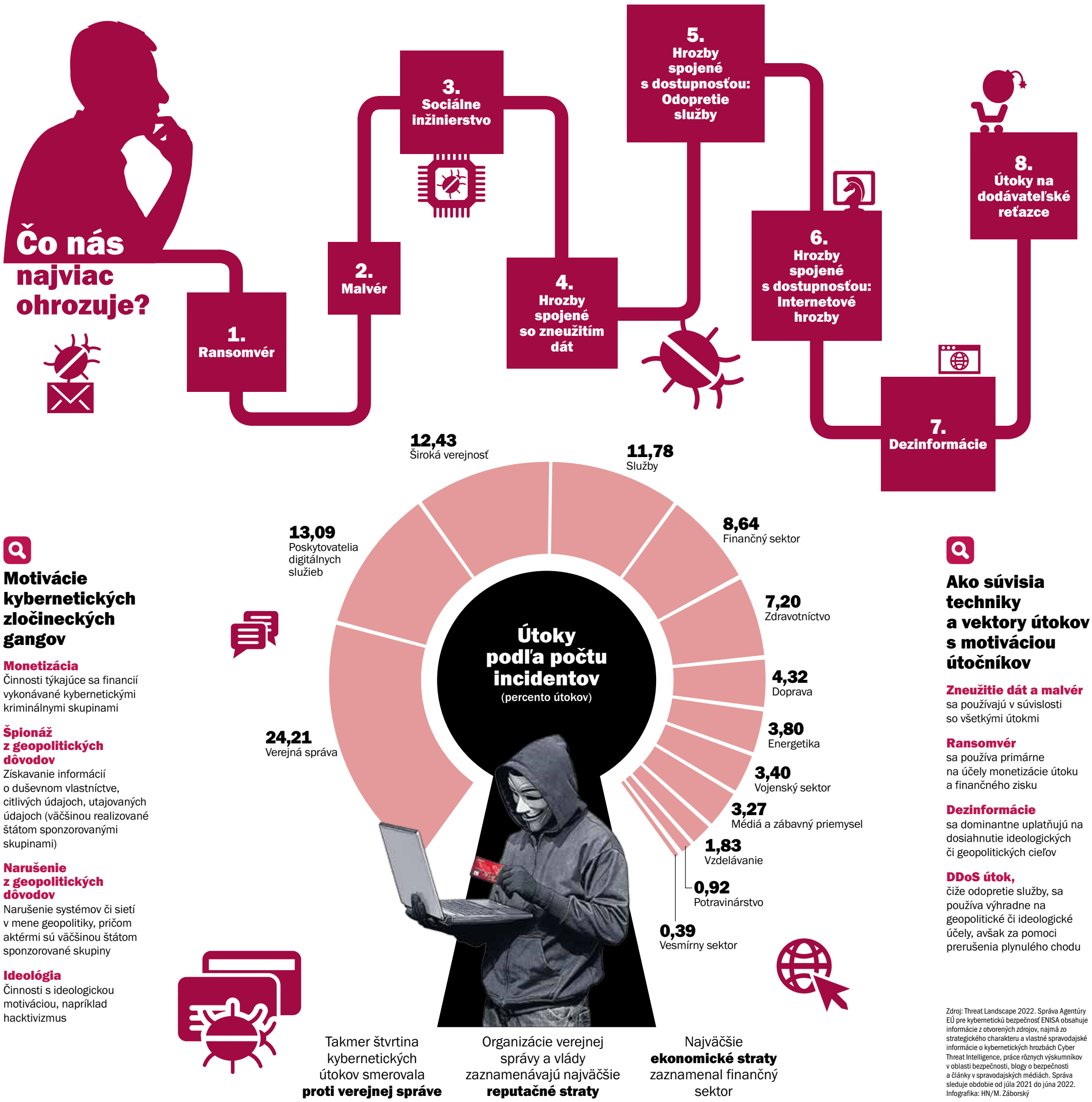
Počet útokov a ohrození bude narastať a s tým aj medializácia tejto témy. Jedným z kľúčových trendov bude zvyšovanie povedomia spoločnosti o rizikách internetu a cielené vzdelávanie zamestnancov v oblasti kybernetickej bezpečnosti. Dúfam, že sa tento trend dostane do vzdelávacích plánov na všetkých stupňoch škôl a rovnako bude i súčasťou interného vzdelávania vo firmách.

Jaroslav Oster,
predseda správnej rady
Preventista.sk

Predpokladateľne dominantnými témami roku 2023 budú narastajúci objem i „kvalita“ útokov postavených na báze sociálnej manipulácie, čoho sprievodným javom bude narastajúci objem škôd. Neodvratným trendom bude intenzívnejšie hľadanie odborníkov v oblasti bezpečnosti vyvolané okrem iného aj príchodom smernice NIS2. Prirodzene pokračujúcim bude zvýšený tlak na edukáciu, a to najmä v školskom sektore.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 25. – 27. NOVEMBRA 2022

Verejnú správu ťaží nápor útokov, na súkromný sektor cielia vydierači



Motivácie kybernetických zločineckých gangov

Monetizácia
Činnosti týkajúce sa financií vykonávané kybernetickými kriminálnymi skupinami

Špionáž z geopolitických dôvodov
Získavanie informácií o duševnom vlastníctve, citlivých údajoch, utajovaných údajoch (väčšinou realizované štátom sponzorovanými skupinami)

Narušenie z geopolitických dôvodov
Narušenie systémov či sietí v mene geopolitiky, pričom aktérmi sú väčšinou štátom sponzorované skupiny

Ideológia
Činnosti s ideologickou motiváciou, napríklad hacktivizmus

Ako súvisia techniky a vektory útokov s motiváciou útočníkov

Zneužitie dát a malvér
sa používajú v súvislosti so všetkými útokmi

Ransomvér
sa používa primárne na účely monetizácie útoku a finančného zisku

Dezinformácie
sa dominantne uplatňujú na dosiahnutie ideologických či geopolitických cieľov

DDoS útok,
čiže odopretie služby, sa používa výhradne na geopolitické či ideologické účely, avšak za pomoci prerušenia plynulého chodu

Zdroj: Threat Landscape 2022. Správa Agentúry EÚ pre kybernetickú bezpečnosť ENISA obsahuje informácie z otvorených zdrojov, najmä zo strategického charakteru a vlastné spravodajské informácie o kybernetických hrozbách Cyber Threat Intelligence, práce rôznych výskumníkov v oblasti bezpečnosti, blogy o bezpečnosti a články v spravodajských médiách. Správa sleduje obdobie od júla 2021 do júna 2022.
Infografika: HN/M. Záborský

KOMENTÁR

Trend sú dezinformácie aj kybernetické útoky na objednávku

Prestížna publikácia Agentúry EÚ pre kybernetickú bezpečnosť ENISA v desiatom ročníku publikácie Threat Landscape mapuje stav a zároveň prináša varovania a indikuje trendy.

Úroveň kybernetickej bezpečnosti sa v súčasnosti stáva silným konkurenčným faktorom, ktorý môže na roky posunúť alebo zabrzdiť rozvoj štátov aj celého regiónu. Ak budeme poznať ohrozenia, vieme sa pripraviť na znižovanie rizika. Odstrániť ho totiž nedokážeme nikdy. Medzi pomyselnými víťazmi na tomto zlovestnom zozname sú obligátne hrozby spojené s ransomvérom, malvérom či so sociálnym inžinierstvom. Nasledujú hrozby spojené so zneužitím dát či odstavenie služby. Na poslednom mieste sa umiestnili dezinformácie či útoky na dodávateľské reťazce.

Hlavným motivátorom na zmenu, respektíve umiestenie v rebríčku je, samozrejme, stále pokračujúci otvorený konflikt medzi Ukrajinou a Ruskom. V rámci neho pozorujeme nárast takzvaných hacktivistických skupín.

Nie je žiadnou výnimkou, že tieto skupiny sú často motivované, či dokonca financované priamo štátom. V prípade otvoreného konfliktu Ukrajiny a Ruska môžeme povedať, že práve hacktivistické skupiny prenášajú tento konflikt aj do kybernetického priestoru.

Ďalším trendom, na ktorý je špecificky Slovensko veľmi náchylné, je šírenie dezinformácií. K šíreniu tejto hrozby však radikálne prispievajú aj nové technológie v oblasti umelej inteligencie, ako je deepfake. Obávam sa, že tento trend bude mať dlhodobý efekt aj po skončení otvoreného konfliktu neďaleko našich hraníc.

Znepokojujúcim trendom v roku 2022 bolo aj používanie takzvaných zero-day zraniteľností. Znamená to, že hackeri sú viac kompetentní a motivovaní tieto zraniteľnosti objavovať a využívať. Ruka v ruke s touto kompetenciou potom rastie aj spôsob, ako sa tieto zraniteľnosti „predávajú“.

Nie je žiadnym prekvapením, že samotný útok si môžeme dnes objednať ako službu, a to v niektorých prípadoch rádovo za stovky eur. S rastúcimi kompetenciami môžu útočníci rozšíriť svoje pole pôsobnosti a útočiť na dodávateľský reťazec organizácie s využitím zraniteľnosti jej potenciálneho partnera. Takýmto spôsobom môžu získať prístup do vybranej organizácie.

Inými slovami, postoj „my sme malý dodávateľ, nás sa kybernetická bezpečnosť netýka, kto by na nás útočil“ už nie je relevantný.

So samotnou kompetenciou útočníkov rastie aj sofistikovanosť útokov. Už v tomto roku sme mohli pozorovať vo zvýšenej miere používanie umelej inteligencie či pokročilých metód sociálneho inžinierstva pri takzvaných spear phishingových útokoch. Sú špecifikované na konkrétnu udalosť v rámci organizácie či geopolitickej situácie a pridávajú na dôveryhodnosti týmto útokom, čím ich robia oveľa efektívnejšími.

Michal Srnec,
CISO Aliter Technologies