HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA 25. – 27. MARCA 2022

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Keď je situácia zúfalá, ale riešiteľná

V prípade incidentu zachovajte chladnú hlavu, postupujte rozvážne, metodicky a nebojte sa o probléme komunikovať.

SNÍMKA: DREAMSTIME

TÉMA

Ak máte problém, voláte správcovi IT. Ten volá bezpečákovi. A komu volá bezpečák, keď nevie, ako ďalej? Profesionálom, ktorí manažujú riešenie incidentov.

Čítanie o kybernetických incidentoch je napínavé a vzrušujúce, ak sa netýka nás. Je tam veľa adrenalínu, napätia, sú tam dobrí aj zlí a útoky sa opisujú ako streľba v bare v čase prohibície.

Kybernetický incident však prináša finančné straty, časový stres a pri zlom manažmente často hanbu na niekoľko rokov.

Rastie nám to

V roku 2021 bolo na Slovensku nahlásených viac ako stošesťdesiat porušení ochrany osobných údajov, takzvaných data breach. „Významnú časť tvorili práve kybernetické incidenty, ktoré medziročne vzrástli o polovicu," hovorí Martin Oczvirk, riaditeľ odboru informačnej bezpečnosti a certifikácie Úradu na ochranu osobných údajov.

Kybernetické útoky smerovali prevažne na výrobné podniky, priemysel, obchodné spoločnosti a neobchádzajú ani verejnú správu, zdravotnícke organizácie a finančný segment. Tridsaťosem útokov bolo úspešných.

Veľa? Málo? Spýtajte sa postihnutých. Zažili vážny zásah do chodu organizácie a obávajú sa straty dôvery.

Zdroje sú nekonečné

Denne sa na čiernom trhu obchoduje s miliónmi uniknutých osobných údajov a zraniteľností a na sieťach pribudnú terabajty informácií. Profesionálna zločinecká mašinéria neustále prehľadáva internet a zároveň nezaplátané zariadenia.

„Najslabším článkom naďalej zostáva človek," stručne hovorí Ján Doboš, riaditeľ odboru riešenia incidentov a dohľadového centra Národného centra kybernetickej bezpečnosti SK-CERT. Najúspešnejšie útoky sa často začínajú rôznymi phishingovými kampaňami slúžiacimi na získanie prihlasovacích údajov, prístupov do systémov a ich infekciu rôznymi typmi malvéru.

Ak ste už v tom

Najčastejšími typmi incidentu sú prieniky do informačného systému či infraštruktúry, úniky dát alebo vydieračský softvér, ktorý zašifruje dáta a zneprístupní systémy.

„Keď je v organizácii spustený ransomvér, je potrebné reagovať v priebehu hodín, identifikovať momentálne prioritné úlohy a okamžite vykonať potrebné aktivity," opisuje stav Richard Kiškováč, generálny riaditeľ Istrosec.

Ak je porušená ochrana osobných údajov, zákonná povinnosť nahlasovania incidentov je do 72 hodín. Martin Oczvirk však upozorňuje, že prioritu má zamedzenie ďalším škodám. Čiže najprv opraviť chybu, aby incident nepokračoval, a následne reportovať a zdôvodniť omeškanie.

Preteky s časom

V prípade identifikovaného incidentu profesionálny tím spúšťa proces, aby sa efektívne vykonali všetky úkony na jeho úspešné zvládnutie. Incident handling tak okrem technických postupov zahŕňa logistiku, komunikáciu, koordináciu a plánovanie úkonov.

V tesnom závese nasleduje incident response – zameriava sa na vyhodnotenie a kategorizáciu incidentu a jeho hĺbkovú analýzu. Končí sa až detailným odporúčaním pre obnovu systémov do pôvodného stavu a pre zabránenie opätovného výskytu.

Znalosti aj analytické myslenie

Riešenie incidentov je náročná oblasť. Tu nastupuje špecializovaný tím reakcie na incidenty – CSIRT. Cieľom je identifikovať, obmedziť a minimalizovať náklady na kybernetický útok alebo incident.

Nie každá organizácia si však môže dovoliť takýchto špecialistov vychovávať a zamestnávať a ani technologické vybavenie nie je nezanedbateľné. Preto koordinácia národných, vládnych a komerčných CSIRT jednotiek pri riešení incidentov je bežnou praxou na lokálnej aj medzinárodnej úrovni.

„Tento synergický efekt dokáže byť jedným z kľúčových prvkov pri zvládnutí rozsiahlych koordinovaných útokov napríklad na prvky kritickej infraštruktúry," upozorňuje Jozef Bálint, bezpečnostný špecialista Alison Slovakia.

Opora tímu

Ako odpoveď na rastúci počet útokov sa v súčasnosti kladie dôraz na prevenciu. Rôzne typy útokov a škodlivé aktivity sú detegované a mitigované automatizovane.

Stredisko bezpečnostných operácii (SOC) je zamerané na bezpečnostný dohľad nad infraštruktúrou zákazníka. Počas automatizovanej a manuálnej analýzy prebieha investigácia aktuálnych ako aj historických dát z monitorovaného prostredia.

Marek Madžo, technický riaditeľ Void SOC Soitron za najvyššiu pridanú hodnotu považuje členov tímu SOC. Postupujú podľa schválených postupov a majú vysoko odborné znalosti a praktické skúsenosti, keďže riešia bezpečnostné udalosti a incidenty v režime 24/7. Spôsob detekcie a riešenia incidentov je oveľa efektívnejší v porovnaní s riešením napríklad zamestnancami organizácie, ktorí sa v danej situácii ocitli prvýkrát.

Verili by ste?

Na základe množstva vyšetrovaní viceprezident pre digitálnu forenznú analýzu a reakciu na incidenty LIFARS a SecurityScorecard Company, Ondrej Krehel, jednoznačne konštatuje: „Dôvodom väčšiny úspešných útokov je nedodržiavanie elementárnych pravidiel kybernetickej bezpečnosti."

Najčastejšími príčinami incidentov je nedostatočná politika hesiel, neaktualizované informačné systémy či nevšímaví správcovia systému, alebo dokonca dohľadového centra. Zarážajúce je, že klienti majú aktualizáciu zaplatenú, aj k nej majú prístup, ale v čase útoku proste nebola implementovaná, lebo nebola nastavená automaticky.

Bezpečnostné prvky, ktoré mohli útok odvrátiť, boli zakúpené a používané, ale neboli zapnuté ich funkcie. „Niekto proste funkciu vypol, keď implementoval iný produkt alebo pre zvýšenie pohodlia používateľov," neveriaco krúti hlavou Ondrej Krehel.

Ak to máte za sebou

Nepoľavujte. Najčastejšou slabinou podľa Jána Doboša je, že mnoho organizácií vykoná len reaktívne opatrenia a obnoví pôvodný stav. Nehľadajú a neriešia však príčinu vzniku incidentu. Môže to byť zraniteľnosť, nesprávna konfigurácia zariadenia alebo aj chybné zadanie pre programátora. „Ak neidentifikujeme a neodstránime prvotnú príčinu, je len otázkou času, kedy sa incident zopakuje," dodáva.

Trendová predpoveď Mareka Madža totiž hovorí, že vektorom útoku zostane aj naďalej email. Preto je doležité zvyšovať povedomie o kybernetickej bezpečnosti, zabezpečiť emailovú komunikáciu podľa najlepšej praxe a zároveň monitorovať podozrivé aktivity.

Pripravujte sa až posadnuto

Odpoveď, ako sú slovenské organizácie pripravené na profesionálny manažment incidentov, sa podľa Jána Doboša nedá zovšeobecniť. „Stretli sme sa so subjektmi, ktoré mali problém preposlať vzorku mailovej komunikácie, až po tie s ukážkovým procesom. Za posledné dva roky však pozorujeme posun správnym smerom."

Vysoko však hodnotí veľkých poskytovateľov digitálnych služieb a nadnárodné spoločnosti.

Najhoršie na tom sú malé subjekty, organizácie zo štátnej správy a obce, ktoré nemajú vypracovaný ani zoznam aktív a používaných technológií. Pre útočníkov je zaujímavá práve táto skupina.

SLOVENSKO 2021 V ČÍSLACH

Hlásené porušenia ochrany osobných údajov, tzv. data breach

165

z tohto kybernetické incidenty

38

medziročný rast

+ 58 %

SPRACOVÁVANÉ BEZPEČNOSTNÉ UDALOSTI

72 085 540

medziročný rast

+ 81 %

Súčet vstupov zo zdrojov SK-CERT, CSIRT.SK a NASES, najmä detegované bezpečnostné udalosti, v prevažnej miere riešené automaticky v bezpečnostných infraštruktúrach.

Zdroj: ÚOOU, NCKB SK-CERT

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

auditori.it · eset · Progress | Flowmon · Qubit · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Keď je studená kybernetická vojna, nastupujú hackeri

Hackerské skupiny a komunity a tímy pracujú službách štátov aj súkromného sektora . SNÍMKA: DREAMSTIME

ANALÝZA

Fenomén čiernej labute vymyslel jeho autor, aby pomenoval mimoriadne udalosti s veľkým dosahom. Práve jednu takú zažívame.

Predpovede a kľúčové výzvy v kybernetickej bezpečnosti na rok 2022 sa týkali odolnosti dodávateľských reťazcov, nákladov za úniky dát, zraniteľností v mikroslužbách, ale aj zneužívania deepfake technológií či vzostupu penetračných nástrojov.

Máme za sebou prvý kvartál a karty už stihla zamiešať čierna labuť v podobe rusko-ukrajinského konfliktu.

Každý kope za seba

Špičková bezpečnostná spoločnosť Check Point Technologies ako jednu z predikcií ešte koncom minulého roka uviedla, že budeme svedkami zintenzívnenia studenej kybernetickej vojny. Studenú vojnu minulého storočia charakterizovali konflikty, v ktorých súperiace veľmoci nestáli proti sebe priamo, ale v podobe zástupných ozbrojencov.

Dnes rovnaký trend pozorujeme v kybernetickom priestore, kde sa virtuálny konflikt vedie pomocou tieňových hackerských skupín. To okrem iného znemožňuje jednoznačnú atribúciu takýchto aktivít štátu.

V skutočnosti nejde iba o to, že globálne veľmoci na pozadí diplomatickej konfrontácie nadobúdajú čoraz sofistikovanejšie kybernetické spôsobilosti. Dostupnosť digitálnych technológií môže významne zjednodušiť úsilie aj politickým aktivistom či teroristickým organizáciám.

Na rozdiel od studenej vojny teda nie sú kybernetické zbrane výsadou vyvážených súperiacich blokov. Kúpiť či dokonca interne vyvinúť si ich dokážu aj menej zdatní hackeri bez ohľadu na ich ideologické presvedčenie. Paleta úmyslov, ktoré dnes stoja za hackerskými útokmi, je neporovnateľne pestrejšia.

Vzájomne zaručené zničenie neexistuje

Istú historickú paralelu so studenou vojnou dnes naozaj môžeme pozorovať. Štáty s cieľom odstrašovania ostatných rozširujú svoj arzenál jednotiek a núl, čím roztáčajú špirálu zbrojenia.

Utiekanie sa k stratégii „najlepšia obrana je útok“ má viacero dôvodov. Jedným z nich je počiatočná nevýhoda defenzívy, ktorá je navyše nepomerne vyčerpávajúcejšia na technologické a ľudské zdroje.

> Napadnutie kritickej infraštruktúry dokáže spoločnosť dlhodobo paralyzovať, no nie bezprostredne zničiť.
>
> **Daniel Suchý,**
> bezpečnostný špecialista
> Aliter Technologies

Udržateľnosť zbrojenia v medziach studenej vojny je však veľmi krehká – závisí od vyrovnanosti síl a vzájomne zaručeného zničenia. V prípade jednotiek a núl garancia úplného zničenia seba spolu s protistranou neexistuje.

Napadnutie kritickej infraštruktúry dokáže spoločnosť dlhodobo paralyzovať, no nie bezprostredne zničiť. Nasadenie kybernetických zbraní v praxi vedie k odvetným útokom, ktoré vyčerpávajú, no neničia, a teda eskalujú celý konflikt. Namiesto odrádzania od útoku sú všetky strany motivované k ďalšiemu zbrojeniu.

Na kybernetickú vojnu doplácajú najzraniteľnejší

Štátom ani škodlivým neštátnym aktérom dnes nič nebráni rozvíjať deštruktívny potenciál kybernetických nástrojov naplno. Celá škála útočníkov testuje nedefinované hranice kybernetického priestoru s vedomím, že ich činy zostanú v reálnom svete bez následkov.

Už kampaň NotPetya cielená na Ukrajinu nám pred niekoľkými rokmi ukázala, aké globálne dôsledky môže niesť hrozba jedného ukradnutého exploitu.

Tak ako v kinetickom konflikte, aj v kybernetickej vojne je potrebné myslieť na tých, ktorí jej dôsledky pocítia najviac. Sú nimi prvky kritickej infraštruktúry, malé a stredné podniky živiace ekonomiku a ich zákazníci.

Plátanie zraniteľností a budovanie digitálnych opevnení je mitigačný prístup, ktorý však nerieši základný problém rastúcej hrozby. Komplexné riešenie bude nevyhnutne vyžadovať celospoločenský prístup so zapojením štátu, technologických spoločností, mäkkých cieľov, ako aj verejnosti.

CYBERGAME

Ak to zažijete, pochopíte

Ak poviete profesionálom, že sa idú hrať, ich tvrdý tréning bude lepší. Aj preto vznikajú kyberbezpečnostné hry.

V kybernetickej bezpečnosti sa spájajú technológie, legislatíva aj sociálne vedy a je to náročný odbor. Silnou devízou profesionálov v tejto brandži je však uvažovanie mimo rámca a kreatívny prístup.

Kyberbezpečnostné cvičenia a hry vznikli z rovnakého dôvodu ako tréning v akejkoľvek oblasti – zlepšovať pripravenosť a schopnosti. Simulácia reálnych situácií pripravuje účastníkov na skutočnú prevádzku na rôznych pozíciach.

Pre širokú verejnosť je kyberbezpečnostná hra exkurziou do sveta profesionálov. Veď ak nám už odrástla ďalšia generácia hráčov počítačových a online hier, prečo neskúsiť nájsť talent v tejto sfére?

Príspevkom slovenskej odbornej komunity k vzdelávaniu aj budovaniu povedomia je práve takáto trendová hra CyberGame. Je určená pre individuálnych hráčov a šancu dostávajú nielen profesionáli, ale aj študenti, učitelia, programátori a talentovaní hráči.

Súťaž má parametre kybernetického cvičenia a obsahuje úlohy rôznej náročnosti. CyberGame sa hrá v štyroch hracích vetvách – malvérová analýza, obfuskácia a kryptografia, forenzná analýza a OSINT analýza. Hráčom stačí vlastný počítač a voľne dostupné analytické nástroje a môžu hrať všetky vetvy alebo sa špecializovať.

V prípade firiem a inštitúcií slúži kyberbezpečnostná hra ako skvelá tréningová platforma, keďže úlohy pripravili profesionáli z praxe. Už v tomto ročníku sa prihlásili napríklad zamestnanci operátorov, strediska bezpečnostných operácií či audítori kybernetickej bezpečnosti.

Od vyhlásenia hry je registrovaných viac ako osemsto účastníkov. V študentskej kategórii aktívne hrá vyše dvesto stredoškolákov a vysokoškolákov, najsilnejšia je účasť profesionálov zo súkromnej sféry, nasleduje verejná správa a hrá aj pár desiatok učiteľov.

Pre trojicu najlepších je pripravená cesta do malvérového laboratória ESET v Montreale. Na exkurziu pôjde hráč s najvyšším počtom bodov, najlepšia hráčka a hráč, ktorý je študentom.

Odborným garantom súťaže je Národné centrum kybernetickej bezpečnosti SK-CERT a úlohy vytvoril tím jeho profesionálov.

Úlohy v kyberbezpečnostnom cvičení majú všetci zamestnanci a rôzne profesie. Aj takýmto spôsobom sa hľadajú talenty. SNÍMKA: CYBERGAME

TRENDY

Tieto skratky sú vaša opora detekcie a reakcie na incidenty

Veľkou výzvou pre IT bezpečnostné oddelenia je pokrytie kompletného perimetra spoločnosti tak, aby sa nenašla ani malá medzierka, kadiaľ by útočníci prepašovali škodlivý kód. A ďalšie výzvy predstavuje neustále vzdelávanie a znalosť trendov.

EDR je minimum

Práca bezpečnostných špecialistov vo firmách spočíva najmä v tom, že sa starajú o zabezpečenie tisícov firemných zariadení. Každý zamestnanec môže mať laptop, niekto aj desktop a k tomu mobilné zariadenia a, samozrejme, servery.

Sumár môže byť enormný a všetky tieto zariadenia sú pripojené do firemnej siete. Ako výrobca bezpečnostného softvéru túto situáciu dobre poznáme a reagujeme na potreby zákazníkov neustálym inovovaním portfólia bezpečnostných riešení.

Pred niekoľkými rokmi sme priniesli EDR riešenie, vďaka ktorému je umožnené nepretržité monitorovanie siete a aktivity na koncových zariadeniach v reálnom čase, analýza podozrivých procesov a okamžitá reakcia na incidenty. Tento typ riešenia okrem vizibility pridáva možnosti šetrenia, pátrania, kde a v akom čase došlo k narušeniu bezpečnosti, a následne vykonania opatrení.

XDR je trend

V dnešnej dobe, keď mnoho zamestnancov pracuje z domu, je tlak na zabezpečenie ešte vyšší, a preto sa viac sústreďujeme na platformu, ktorá dokáže jednotlivé slabé miesta pokryť. Už teda nehovoríme o jednotlivých produktoch v portfóliu, ale o úrovniach zabezpečenia, ktoré zákazník potrebuje dosiahnuť. ESET PROTECT ekosystém je XDR platforma, ktorá pozostáva z rôznych komponentov. Ochrana koncových bodov a systém detekcie a reakcie sa tu spájajú do jedného riešenia.

EDR, XDR, MDR sú technológie a služba zabezpečenia
koncových bodov.

Sú koncipované tak, aby zdokonalili viditeľnosť, detekcie hrozieb a reakciu na koncových bodoch v rámci celej spoločnosti.

Potreba takýchto riešení dnes nevyplýva len v spojitosti s požiadavkami na kybernetickú bezpečnosť v zmysle zákona, ale aj z neustáleho rastu sofistikovaných útokov typu APT, čiže pokročilých pretrvávajúcich hrozieb. Kybernetický priestor predstavuje nové vojnové pole, v ktorom sa zatiaľ žiadne krajiny nedohodli na podmienkach a pravidlách fungovania.

Dnes by pre každú organizáciu, firmu či štátny podnik mala byť bezpečnostná stratégia samozrejmosťou. Hrozby číhajú všade – zero-day zraniteľnosti, APT, ktoré sa vyznačujú dlhodobým zbieraním informácií o systéme a snahou zotrvávať v sieti bez odhalenia dlhšie obdobie, či kybernetická špionáž. Preto je dôležité myslieť na neustálu analýzu rizík, viacvrstvovú ochranu, nepriestrelnú politiku aj proaktívnu a rýchlu detekciu a reakciu.

Naša XDR platforma spája viacero komponentov do jedného funkčného celku – multiplatformový prístup k detekcii a reakcii koncových bodov, viacvrstvový model zabezpečenia, zhromažďovanie a korelácia aktivít v sieti. Predstavuje tak ďalšiu fázu vývoja EDR. Poskytuje detekciu a ochranu vrátane cloudovej infraštruktúry s využitím sily strojového učenia, automatizácie či prvkov umelej inteligencie. Súčasťou riešenia je aj cloudový sandbox, teda izolované prostredie, ďalšia vrstva ochrany pred úplne novými, dosiaľ neznámymi hrozbami.

MDR je budúcnosť

Na Slovensku overiteľne chýba vyše desaťtisíc IT špecialistov. Situácia s IT bezpečnostnými špecialistami je ešte komplikovanejšia. Naše riešenia dávajú do rúk bezpečnostným špecialistom vo firmách možnosti, ako reagovať na jednotlivé hrozby a ako správne zaplátať bezpečnostné diery.

V prípade, že spoločnosti takýchto ľudí nemajú, chýba im potrebné know-how, prichádza na scénu MDR – Managed Detection and Response. Nie je to iba ďalšia technológia, sú to prispôsobené, integrované proaktívne služby, ktoré poskytujú špičkoví odborníci ESET-u.

Je to cesta k tomu, aby technológie naplno využívali v spoločnostiach, ktoré majú obmedzené zdroje alebo im chýbajú odborné znalosti na nepretržité monitorovanie potenciálnych útokov.

Július Selecký, senior technický špecialista ESET, spol. s r. o., odborný asistent Fakulta managementu UK

Už je to navždy: nová éra bezpečnosti

ANKETA

Čo vás prekvapilo, potešilo, alebo aký zlom ste vo svojej brandži a vo vnímaní verejnosti za toto obdobie zaznamenali?

Ivan Makatura
generálny riaditeľ Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Ruské vojnové ťaženie zvyšuje obavy verejnosti z vojny v kybernetickom priestore. Stav bezpečnosti sa však neodvíja od pocitu, ale od odolnosti voči zraniteľnostiam. Prekvapilo ma, že niektoré firmy sa zobudili až teraz, keď sú konfrontované s bezprostrednou hrozbou. Potešilo ma, že sa u nás našli odborníci, ktorí sú v tejto dobe ochotní pomáhať v ochrane kyberpriestoru aj bez nároku na odmenu.

Marek Zeman
vedúci oddelenia bezpečnosti informačných systémov Tatra banka

Slovensko zažívalo rozkvet za posledné roky vo všetkých smeroch. Napriek možnostiam sa nenašiel element, ktorý by spájal a riadil informačnú bezpečnosť jasným smerom na úrovni štátu. Teraz je situácia kritická, sú tu dezinformácie či prvky hybridnej vojny, stále sa nenašiel element, ktorý by osvieteným riadením nastavil smer. Verím, že príde. Želám si, nech to nie je osamotený jedinec, diktátor.

Igor Práznovský
riaditeľ odboru bezpečnosti informačných systémov Sociálna poisťovňa

23. februára nás prekvapil desaťnásobný záujem o našu stránku z ruských IP-čok. 24. ráno sa začala spamová kampaň, v ktorej sme denne dostali skoro dva milióny e-mailov. Už menej ma prekvapil malvér odchytený počas prvých dní invázie, ktorý VirusTotal pred našou analýzou ešte nevidel. Je tých „náhod“ v tejto hybridnej vojne viacero.

Tomáš Hettych
viceprezident ISACA

Neprekvapilo ma, že sa v tomto výnimočnom období opäť vyrojilo množstvo „odborníkov“ na kybernetickú bezpečnosť, ktorí takmer denne komentujú aktivity štátnych inštitúcií aj odborných organizácií. Títo kvázi-experti väčšinou neovládajú ani samotnú problematiku, ani terminológiu, zdieľajú pochybné zdroje a násilne prezentujú svoj názor ako jedinú pravdu. A potešilo ma, že sa stále nájde dostatok dobrých ľudí.

Ján Grujbár
generálny riaditeľ Aliter Technologies

Príjemne ma prekvapil počet firiem, ktoré, podobne ako naša spoločnosť, ponúkli štátu alebo kritickej infraštruktúre pro bono pomocnú ruku v čase zvýšeného rizika kyberútokov. Verím, že to je dôležitý signál, že súkromný sektor, štátne inštitúcie a napokon i občianska spoločnosť sú pripravené spolupracovať v akejkoľvek situácii.

Andrej Žucha
generálny riaditeľ ALISON Slovakia

V kybernetickej vojne sme už dávno a teraz sa to prejavilo vo vyhrotenej podobe a v priamom prenose. Profesionáli sú si toho vedomí a pracujú s obrovským nasadením. Ak predstavitelia štátu hľadajú riešenia, ako zabezpečia plyn a obilie, pýtajme sa ich súčasne, ako ochránia obyvateľov pred kybernetickými hrozbami a dezinformáciami. A snaha je v tomto prípade málo.

David Dvořák
audítor kybernetickej bezpečnosti Auditori.it

V ostatných dňoch som smutný z poznania, že až vojnový konflikt, a teda bezprostredné ohrozenie je drajverom pre zvýšenie rozpočtu na obranu. Áno, zatiaľ chápeme, že treba zvýšiť konvenčnú obranu. Ale časť z toho veľmi reálneho strachu by sa mala prejaviť v rozpočtoch na kybernetickú obranu. Doteraz sme hrozbu a obranu len veľmi nešikovne modelovali. Po dvoch rokoch pandémie a otvoreného vojenského konfliktu v Európe je čas na reálne a konkrétne riešenia.

Stanislav Smolár
manažér oddelenia bezpečnosti Soitron

V súvislosti s konfliktom na Ukrajine ma najviac prekvapil útok na KA-SAT SATCOM terminály, keď náhle prestali fungovať desiatky tisíc terminálov vo viacerých európskych krajinách. Predpokladal som, že ide o klasický Denial of Service útok, ale nakoniec sa zistilo, že terminály sú poškodené a nefunkčné. Keďže satelitný internet sa primárne používa ako záloha, ide o veľmi závažný útok. Aspoň čiastočne sa ho podarilo minimalizovať rýchlym nasadením StarLink od SpaceX.

Július Selecký
senior technický špecialista ESET

Ruskom vyvolaná vojna trvá už pár týždňov, ale vojnu v kyberpriestore evidujeme roky. Prekvapilo ma, že spolu s inváziou sa nespustil aj rozsiahly kybernetický útok, ktorý by významne poškodil Ukrajinu. Hrozby kybernetickej vojny zo strany Ruska sú obrovský problém. Po anexii Krymu v roku 2014 Ukrajina začala posilňovať nielen armádu, aby bola pripravená na konvenčnú vojnu, ale aj kybernetickú bezpečnosť krajiny, čo môže zohrávať dôležitú rolu.

Roman Čupka
hlavný konzultant spoločnosti Flowmon a CEO Synapsa Networks

Zintenzívňujú sa útoky z rizikových krajín, ktoré využívajú súčasne viaceré techniky. Napríklad odstavovanie služieb slúži ako maskovací manéver, keď sa útočníci v skutočnosti snažia „prepašovať“ do organizácií skryté hrozby, aby kompromitovali jednotlivcov alebo IT infraštruktúry. Očakávam stupňovanie sofistikovaných útokov, prehlbovanie polarizácie spoločnosti spôsobené informačnou vojnou a verím, že dôraz na bezpečnosť v kybernetickom priestore naberie na obrátkach.

Martin Fábry
konzultant pre kyberbezpečnosť kritickej infraštruktúry Accura

Udalosti majú značný dopad aj na našu profesiu, kedže paralelne prebieha aj kybernetická vojna. Kritická infraštruktúra, napríklad energetika, zatiaľ odoláva kybernetickým útokom na rozdiel od útokov na government systémy. Ani jedna strana zatiaľ nevytasila tie najdevastujúcejšie kybernetické zbrane, nachystané ako zbrane poslednej inštancie. Aktivácia by znamenala značné škody na oboch stranách. Toto obdobie bude mať dosahy aj na kyberbezpečnosť našej kritickej infraštruktúry, lebo útočníci budú prakticky preverovať odolnosť kybernetickej obrany. Treba sa dôkladne pripraviť.

Ján Golais
poradca bezpečnosti Slovak Telekom

Zarmucuje ma nedostatočné vnímanie doby, ktorú žijeme. Nezabezpečené stránky, slabé heslá, odovzdávanie údajov z platobných kariet na zavolanie. Prístup vedení inštitúcií a obchodných spoločností k podpore a bezpečnosti pri spracúvaní dát. Berú to ako nutné zlo. Zlomom by bolo pochopenie a zohľadnenie rizík najmä business continuity management a spustenie testovania disaster recovery plan. Potešil ma prístup Národného bezpečnostného úradu k blokovaniu dezinfowebov.

Ivan Kopáčik
bezpečnostný expert Gordias

Potešila ma (na pomery EÚ) vízia radikálnej akcelerácie európskych strategických aktivít kybernetickej bezpečnosti. Čo by trvalo roky, bude trvať mesiace. A všetko nasvedčuje tomu, že konečne bude praktický efekt zodpovedať reálnym potrebám. Bohužiaľ, opäť sa tak stalo, až keď situácia zašla do krajnosti, keďže súčasťou konfliktu na Ukrajine je aj kybernetický priestor.

Martin Fischer
manažér oddelenia bezpečnosti Všeobecná zdravotná poisťovňa

Ľudia sa v tejto situácii prirodzene začali viac zaujímať o svoju bezpečnosť, čo sa prenieslo aj do oblasti informačnej bezpečnosti. Vyššia ostražitosť štátnych inštitúcií a súkromných firiem preveruje ich pripravenosť na krízové situácie a môže v konečnom dôsledku posunúť úroveň kybernetickej bezpečnosti zas o krok ďalej.

Peter Kolarov
generálny riaditeľ Crayonic

Trochu ma prekvapilo, že v už aj tak tradične zdrojmi obmedzenej kyberbezpečnosti firiem a inštitúcií sa aj v týchto dňoch pristupuje k prevencii s hlavou v piesku. Tí, čo môžu robiť rozhodnutia na posilnenie kyberbezpečnosti, tak robia, žiaľ, až po funuse. Ale teší ma aspoň zvýšený záujem o našu prácu a azda aj to, že nie som CISO kritickej infraštruktúry pod priamou paľbou – týmto všetkým CISO-m držím palce!

Peter Dufek
manažér kybernetickej bezpečnosti Procare a Svet zdravia

Aj hackeri zo zoskupenia Anonymous preukázali, že majú nesmierne bojového ducha. Na pozadí až ťažko uveriteľnej vojnovej reality sa ich aktivity doteraz pre nás označované ako škodlivé aktuálne ukázali ako vysoko pozitívne vnímaná sofistikovaná súčasť hybridnej vojny. A tento spôsob boja nepozná hranice krajín.

Diana Legdanová
vedúca úseku bezpečnosti Vychodoslovenská energetika Holding

Sme deväťdesiat kilometrov od východnej hranice. Obávala som sa, že keď sa niečo zomelie, tak to bude práve v štýle „kybervojny“, a čo to bude znamenať pre náš security útvar, firmu, región alebo celú spoločnosť. Potešil ma však prístup kolegov, ako opäť zafungovalo celé krízové riadenie situácie z kyberpohľadu. Je dôležité vedieť, že sa môžete spoľahnúť. Zarmucuje ma na tom len nezmyselnosť a dôsledky celého diania.

Robert Mramúch
manažér kybernetickej bezpečnosti MH Teplárenský holding

V súvislosti s hrôzyplnými udalosťami posledných týždňov – nie je čas odkladať bezpečnosť. Nie je priestor na dočasné a kompromisné riešenia. Dopadajúce bomby na tepláreň by spôsobili vo výsledku rovnakú škodu ako infikovanie riadiacich systémov škodlivým kódom – čiastočnú alebo úplnú nedostupnosť základnej služby, ktorú by v tomto prípade pocítilo obyvateľstvo doslova „na vlastnej koži“.

Dominik Procházka
riaditeľ odboru bezpečnosti AGEL SK

Udalosti posledných týždňov nenechajú asi nikoho v pokoji ani na poli kybernetickej bezpečnosti. Detekčné systémy hlásia nárast aktivity a do médií sa čoraz viac dostávajú články o útokoch rôznych skupín. Vývoj situácie ešte viac zdôraznil nevyhnutnosť zavádzania prísnych pravidiel a regulácií v oblasti kybernetickej bezpečnosti. Ukazuje sa, že riešenia je potrebné aplikovať práve teraz a nečakať.

Matej Síleš
manažér IT bezpečnosti UPC Broadband Slovakia

Manažéri bezpečnosti musia vždy myslieť na to najhoršie, a tak nás aktuálna situácia veľmi nezaskočila. Kybernetická bezpečnosť sa práve v takýchto chvíľach dostáva do popredia, a to má za následok zlepšovanie jej stavu a tiež zvyšovanie povedomia laickej verejnosti o tom, ako sa chrániť pred hrozbami. My ako manažéri musíme túto situáciu využiť na presadenie našich potrieb, aby organizácie boli na budúcnosť lepšie pripravené.

Miroslav Chlipala
partner Advokátska kancelária Bukovinský & Chlipala

O medzinárodnom práve ozbrojených konfliktov sme učili zo skrípt z 80. rokov minulého storočia. Bol som presvedčený, že sa učím o niečom, čo patrí do histórie. Až teraz som si uvedomil, ako som sa hrozne mýlil. Ďalšia učebnica asi bude obsahovať nové pravidlá a medzinárodné dohovory pre vedenie vojny v piatej doméne. Je mi to ľúto.

Henrich Šnajder
manažér IT bezpečnosti Orange Slovensko

V predpokladanej hybridnej vojne ma prekvapuje, akému enormnému nárastu kybernetických útokov a incidentov treba čeliť. Zatiaľ evidujeme v našom sektore skôr pokles. Predpokladám, že sily a prostriedky sú presmerované na záujmové ciele. Udalosti v spojitosti s ozbrojeným konfliktom na Ukrajine nás donútili prehodnotiť riadenie kontinuity podnikania na úrovni celej korporácie.

Jaroslav Oster
predseda správnej rady Preventista.sk

Zlomom je narastajúci záujem laickej verejnosti o témy bezpečnosti, a tým aj istý nárast bezpečnostného povedomia. Zarmucujúcim je akútny nedostatok profesionálov pre praktickú realizáciu i verejnú diskusiu úloh vyplývajúcich z Akčného plánu kybernetickej bezpečnosti, čo znižuje kvalitu, odbornosť i efektívnosť radu aktivít zvyšovania bezpečnosti.