HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 30. JÚLA – 1. AUGUSTA 2021

Tieto míľniky navždy zmenili svet

ANKETA

Kybernetická bezpečnosť je nedosiahnuteľný cieľ, o ktorý sa treba neustále snažiť minimalizáciou rizík. Život a prax učia bezpečákov predvídať.

Diana Legdanová,
vedúca úseku bezpečnosti, Východoslovenská energetika Holding, a. s.

Na to neexistuje jedna odpoveď. Ide o kombináciu globálneho vývoja v oblasti digitalizácie, veľkých incidentov, ktoré sa vo svete udiali, či samotného kyberzákona. Ľudia aj firmy zmenia zásadne svoj postoj väčšinou v troch prípadoch – vlastná negatívna skúsenosť, zákon alebo uvedomenie si dôležitosti. V tomto poradí. Myslím si, že na Slovensku je to práve zákon, ktorý môžeme nazvať míľnikom.

Blanka Vargová,
manažérka tímu kybernetickej bezpečnosti, U. S. Steel Košice, s. r. o.

Keďže pôsobím v rámci priemyslu, je to jednoznačne Stuxnet v roku 2010. Ten totiž bol priamo vyvinutý, aby škodil priemyselným systémom a v rámci nich na programovateľné logické automaty, ktoré priamo riadia výrobu. Ďalej na základe jeho kódu bol napísaný Duqu a Conficker si z neho tiež „zapožičal“ aspoň jednu n-dňovú zraniteľnosť. V konečnom dôsledku Stuxnet bol pôvodcom nespočetných útokov, ktorým priemyselné podniky dodnes čelia.

Tomáš Zaťko,
CEO, etický hacker, Citadelo

Stuxnet. A to aj napriek tomu, že to už je ošúchané klišé. Bol to míľnik, keď sa kybernetická bezpečnosť definitívne dostala do prostredia sveta vojny.

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

Nejestvuje žiaden konkrétny incident, ktorý by bol spôsobil búrku v tomto odbore. Prelomové bolo rozhodnutie začať vyjadrovať riziká v peňažnej hodnote. Ako inak – začali s tým banky, keď sa v roku 2004, v druhej z Bazilejských dohôd, dohodli, že okrem úverového a trhového rizika sa berie do úvahy už aj operačné riziko. Tým sa aj bezpečnostné riziká stali predmetom manažmentu podnikov a legislatívy.

Tomáš Hettych,
viceprezident, ISACA

Na Slovensku bol dôležitým míľnikom zákon číslo 122 z roku 2013 o ochrane osobných údajov, ktorý konkrétne definoval požiadavky ochrany údajov a informácií. Vtedy sa väčšina spoločností a organizácií začala zaoberať aj kybernetickou bezpečnosťou. Následný GDPR ošiaľ v roku 2018 túto iniciatívu len posilnil, hlavne vďaka vysokým deklarovaným pokutám a aktivitám spoločností v celej Európe.

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

Vznik sociálnych sietí bol ako odistený granát, ktorý dlho ležal v kybernetickej bezpečnosti bez povšimnutia. Zmenila sa hodnota súkromia, otvoril sa nekonečný zdroj informácií pre sociálne inžinierstvo a vznikla komunikačná platforma, kde jeden post mení svet takmer v priamom prenose.

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

Najzásadnejšie sú vírus I love you z roku 2000 a v 2017 prvý veľký supply chain útok NotPetya na Ukrajine, kde celkovú škodu odhadli na 10 miliárd dolárov. Na konci vlaňajšieho roka dominoval supply chain útok na SolarWinds. Napadol väčšinu FORBES 500 spoločností na svete a tiež veľa vládnych systémov. Všetky útoky spôsobili malé zemetrasenie a mali silnú mediálnu pozornosť. Prebudili aj vlády a bezpečnostné zložky.

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

V zdravotníctve je to šokujúci a ohavný kybernetický útok na elektronické služby írskeho zdravotníctva v máji tohto roka. Unikli najcitlivejšie informácie a útok má dosah na zdravie ľudí. Ransomvérový útok odstavil kľúčové služby manažmentu pacienta, plánovaných výkonov a skríningových služieb. Útočníci neskôr poskytli dešifrovací kľúč. Obnova zašifrovaných dát beží sedem dní v týždni a doteraz nebola ukončená.

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

Prvý počítačový vírus pred päťdesiatimi rokmi, prví odsúdení za kriminalitu v tejto oblasti, napríklad Kevin Mitnick, následne séria interných únikov dát, ktorým kraľoval Snowden, DDoS útoky, úniky dát od veľkých internetových spoločností a štátnej správy až po vydieračský softvér v posledných rokoch. Je možné medzi ne zaradiť aj vznik GDPR a útvarov na boj s kyberkriminalitou.

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

Prelomové boli určite pokročilé ransomvérové útoky a ich kombinácia so supply chain útokmi, ako sú SolarWinds či NotPetya. Je len veľmi málo postupov a technológií – jednou z nich je EDR, čiže systémy na detekciu a reakciu na útoky, vďaka ktorým môžu organizácie ostať pred nimi v bezpečí. Z hľadiska kybernetickej bezpečnosti sú významné aj nariadenie GDPR, zákon o ochrane osobných údajov a zákon o kybernetickej bezpečnosti. Vďaka nim sú lepšie chránené dáta o nás všetkých.

Roman Čupka,
hlavný konzultant, Flowmon a CEO Synapsa Networks

Míľnikom bol vznik moderného internetu v 90. rokoch minulého storočia. To má za následok masívnu transformáciu spoločenského, hospodárskeho a ekonomického života do kybernetického priestoru. Umožnil okrem iného existenciu celej plejády dnes takých obľúbených platforiem pre kybernetickú kriminalitu. Od temnej časti internetu až po decentralizované digitálne meny, ako je bitcoin.

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

Za takýto míľnik by sme už z princípu mali považovať prijatie zákona č. 69 v roku 2018. Tento zákon jednak vytvára legislatívny rámec pre koncepčný prístup k otázkam kybernetickej bezpečnosti, hoci nie je dokonalý, určite je dobrým východiskovým bodom pre organizácie nakladajúce s našimi dátami.

Ivan Kopáčik,
bezpečnostný expert, Gordias, s. r. o

Prelomový míľnik je pre mňa rok 1988 – Internet worm. Bol to prvý počítačový červ, ktorý infikoval vtedajší internet. Americký študent R. Morris, ktorý ho napísal a „vypustil“, vyvolal kolaps vtedajšej infraštruktúry. Dôsledkom tohto incidentu bolo vytvorenie prvého CERT-u na Carnegie Mellon University ako centrálneho koordinačného prvku pre zvládanie rozsiahlych bezpečnostných incidentov.

Daniel Hetenyi,
regionálny manažér, CyberArk

Zasadne vnímam niekoľko prienikov. V roku 2015 hackeri ukradli 20 miliónov zamestnaneckých záznamov zo správy ľudských zdrojov štátnych zamestnancov USA, kde aj napriek veľkým výdavkom na bezpečnosť prišlo k veľkému prieniku. Na Vianoce 2016 hackeri odstavili elektrinu 230-tisíc ľuďom na Ukrajine útokom na elektrickú sieť. Ransomvérový útok na Garmin v roku 2020 ukázal, ako hackeri vedia zarábať na prienikoch.

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

Z hľadiska ochrany osobných údajov a kybernetického priestoru bol prelomový moment prijatie všeobecného nariadenia o ochrane osobných údajov GDPR a smernice NIS v roku 2016. O rok neskôr sa znova ukazuje, aká je bezpečnosť dát, hlavne bezpečnosť osobných údajov, potrebná a nevyhnutná. V roku 2017 zasiahla vlna ransomvérových útokov celú zemeguľu. Útočníci týmto momentom rozbiehajú nový druh biznisu s osobnými údajmi.

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

Prvý počítačový vírus BRAIN vytvorili bratia Alviovci z Pakistanu v januári 1986. Šíril sa pri iniciovaní operačného systému z externej diskety a následne pri jej používaní. Úmyslom nebolo škodiť a aj tvorcovia boli zaskočení tým, ako rýchlo sa šíril. Počítačový „červ“ Stuxnet sa zas považuje za najdlhšie a s najvyššími nákladmi vyvíjaný škodlivý kód. Úmyslom vlád USA a Izraelu bolo získať kybernetickú zbraň, čo sa podarilo útokom na iránske jadrové zariadenie v roku 2009.

Ján Lichvár,
konateľ, Axenta, s. r. o.

V dôsledku ransomvérového útoku v roku 2019 bola nemocnica v Benešove vyradená na tri týždne z poskytovania zdravotnej starostlivosti. Následná diskusia bola v Česku podnetom na vyčlenenie zdrojov na riešenie informačnej bezpečnosti v zdravotníctve. U nás chýba diskusia medzi sektormi a osveta. Potrebujeme osobu, ktorá si tému naozaj zoberie za svoju a stane sa lídrom v kybernetickej bezpečnosti s primeranými kompetenciami.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov, Tatra banka

Bodom zlomu bol útok na blog Krebs on Security. Zaútočilo všetko možné: chladničky, kamery, žiarovky. Úplne všetko, čo sa hackerom podarilo ovládnuť. Obrovská telekomunikačná firma Akamai útok nezvládla a blog vypla. Odvtedy sa veľa zmenilo. Ochrana systémov sa riadi podľa manažmentu rizík. Firmy sa cielene chránia pred rôznymi zničujúcimi útokmi. Riešia sa problémy bezpečnosti internetu vecí.

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

Od prvých vírusov, ktoré znemožnili nabootovanie operačného systému, je tých míľnikov viac. Prelomovým sa podľa mňa stalo prvé použitie ransomvéru Cryptolocker, ktorého obmeny vidíme dnes veľmi často. Rozvoj malvéru a útočných techník priniesol postupný vznik silného kyberkriminálneho podsvetia s extrémnymi ziskmi a taktiež možností viesť kybernetickú vojnu.

Robert Mramúch,
manažér kybernetickej bezpečnosti, MH Teplárenský holding

Spôsob práce s informáciami – virtuálnym majetkom, ktorú so sebou priniesla digitálna transformácia. Míľnik v kyberbezpečnosti predstavuje prechod od spracovania privátnych dát na vlastnom serveri do vzdialených cloud riešení. Logickým dôsledkom je štandardizácia v podobe kvalitatívnych či bezpečnostných noriem a legislatívy, kde bol na Slovensku významný rok 2018.

Jaroslav Oster,
predseda Správnej rady, Preventista.sk

Nesporne vznik Budapeštianskeho dohovoru Rady Európy o počítačovej kriminalite v roku 2001 a jeho prijatie Národnou radou SR v roku 2007, respektíve prípravy na jeho aktualizáciu v tomto roku. Bol to nepochybne prvý krok k spoločnému postupu v tvorbe legislatívy a boja proti novým formám trestnej činnosti, akými sú javy počítačovej kriminality a podvodov v digitálnom svete.

Michal Čábela,
riaditeľ riadenia rizík, Deloitte

V histórii kybernetickej bezpečnosti je viacero míľnikov, avšak až útoky ako Stuxnet bot alebo WannaCry, prípadne ďalšie sofistikované útoky Meltdown alebo Spectre, ktoré využili zaujímavé a nečakané zraniteľnosti, dostali túto problematiku do povedomia širšej verejnosti. Novú éru v tejto oblasti predstavuje rýchly rozvoj kvantových počítačov a vývoj nových kvantovo rezistentných kryptografických algoritmov.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií/IT manažment kvality, Volkswagen Slovakia

Vznik ransomvéru ako kyberhrozby. Ten prešiel od roku 1989, keď vznikol ako AIDS Trojan, evolúciou. Napríklad útok na kliniku Vastaamo v októbri 2020 ukázal nový prístup útočníkov. Tí nielen „štandardne“ ukradli spoločnosti údaje a vydierali ju, ale vydierali aj pacientov. Útok na Colonial Pipeline zasa ukázal prepracované nasadenie „ransomvéru ako služby“. A vývoj sa týmto určite nekončí.

David Dvořák,
audítor kybernetickej bezpečnosti, Asociácia kybernetickej bezpečnosti

Hackeri zvyčajne potrebovali aktívnu účasť používateľa, aby sa dostali do nášho zariadenia. Preto je zaujímavá správa o spôsobe prienikov skupiny NSO prostredníctvom systému. Sledovací softvér Pegasus vie totiž preniknúť do mobilného telefónu úplne bez našej „pomoci“. Navyše to je ďalší klinček do rakvy dobrej povesti iPhonu ako bezpečného zariadenia. Pre nás, ktorí sa snažíme posilňovať povedomie o správnom používaní mobilných zariadení a počítačov, bude o dosť zložitejšie vysvetľovať, ako sa chrániť pred niečím, čo si nájde cestu k nám aj samo.

Ďalšie rady o hygiene, ak sa chystáte cestovať

TRENDY

Čím viac opäť cestujeme a pripájame svoje zariadenia do internetu, tým väčšiemu kybernetickému riziku čelíme. Základné praktiky kybernetickej bezpečnosti, čiže bezpečnostnú hygienu, je potrebné dodržiavať aj počas dovolenky alebo pracovnej cesty.

Dnes už drvivá väčšina ľudí cestuje s notebookom alebo mobilnými zariadeniami. SNÍMKA: DREAMSTIME

PRED CESTOU

ZÁLOHUJTE

Záloha vášho zariadenia na domáce alebo cloudové úložisko pred cestou uchová vaše dáta v bezpečí pre prípad straty alebo krádeže zálohovaného zariadenia.

ČISTÉ ZARIADENIE

Ak cestujete do rizikových krajín, je vhodnejšie použiť čistý počítač, ktorý neobsahuje žiadne firemné dáta. Pripomíname, že každá spoločnosť by mala mať vyhodnotené riziká.

AKTUALIZUJTE SI SOFTVÉR

Operačný systém má zabudované aj bezpečnostné komponenty, ktoré výrobca pravidelne aktualizuje. Aktualizovaný systém a aplikácie dávajú vyššiu mieru bezpečnosti, keďže odstraňujú známe zraniteľnosti.

ZVYKNITE SI ZAMYKAŤ

Použitie komplexných prístupových hesiel je dôležité, ale počas cestovania je ešte dôležitejšie, aby ste svoje zariadenia uzamykali, tak predídete možnému neoprávnenému vstupu do zariadenia.

KEĎ UŽ STE NA MIESTE

DEAKTIVUJTE AUTOMATICKÉ PRIPOJENIE

Ak je funkcionalita aktívna, zariadenie vyhľadáva a snaží sa pripojiť na dostupné WiFi siete alebo Bluetooth pripojenia. Môže sa stať, že sa neúmyselne pripojíte k škodlivému zariadeniu alebo podvrhnutej WiFi sieti.

PREMYSLITE SI TO, NEŽ SA PRIPOJÍTE

Overte si správnosť mena siete a presný postup prihlásenia, čím sa uistíte, že daná WiFi sieť je legitímna. V žiadnom prípade nerealizujte transakcie platobnou kartou alebo nespracovávajte osobné alebo firemné citlivé informácie. Použitie priameho dátového pripojenia je omnoho bezpečnejšie ako pripojenie na verejnú WiFi sieť.

Vždy sa pripájajte na zabezpečené stránky cez https://. Aktivujte si VPN, ktorá vytvorí bezpečný šifrovaný komunikačný kanál a ochráni dôvernosť dát.

PREMYSLITE SI TO, NEŽ KLIKNETE

Pred každým kliknutím na odkaz alebo stiahnutím súboru si overte, či ide o legitímny zdroj. Aj keď spam filtre na e-mailovom účte alebo riešenia na firemných e-mailových serveroch sú schopné odfiltrovať väčšinu škodlivej pošty, môže sa stať, že niečo unikne.

> Ak cestujete do rizikových krajín, je vhodnejšie použiť čistý počítač, ktorý neobsahuje žiadne firemné dáta.
>
> **Daniel Suchý,** bezpečnostný špecialista, Aliter Technologies, a. s.

Vždy zmažte e-maily, ktoré vyzerajú podozrivo alebo sú od neznámeho odosielateľa. Keď potrebujete nainštalovať aplikáciu do mobilného zariadenia, vždy sa dobre oboznámte s tým, aké informácie zdieľate.

KEĎ TO MÁTE RADI, ZAMKNITE SI TO

V hotelovej izbe, v konferenčnej miestnosti, v reštaurácii, na letisku, v lietadle alebo počas iného spôsobu dopravy nikdy nenechávajte zariadenie bez dozoru. Zlodeji často cielia na cestovateľov.

NEZDIEĽAJTE VŠETKO

Zdieľanie polohy a fotiek na sociálnych sieťach prináša so sebou riziko, že prípadní útočníci vedia zistiť, kde sa nachádzate.

POZOR NA PLATOBNÉ KARTY

Postačí, ak sa skenovacie zariadenie skryté v ruksaku priblíži na niekoľko centimetrov k vašej platobnej karte a za veľmi krátky čas naskenuje dáta potrebné na zneužitie karty.

Používajte obal na kartu alebo peňaženky s RFID ochranou, alebo si aktivujte platobnú kartu v smart telefóne.

PO NÁVRATE Z CESTY

ČAKAJTE TO NAJHORŠIE

Ak ste sa v zahraničí pripojili na verejnú sieť a máte podozrenie, že zariadenie mohlo byť kompromitované, v prípade súkromného zariadenia vyhľadajte odbornú pomoc, v prípade firemných zariadení sa obráťte na oddelenie kybernetickej bezpečnosti vo svojej spoločnosti.

FIRMY

Bezpečnostné tipy pre vzdialenú prácu

Počas pandémie sme si zažili množstvo bezpečnostných faux pas – od vážnych finančných strát až po úsmevné chyby. Nie je žiadnym prekvapením, že vo svete, kde ešte stále veľa ľudí nevie ovládať tlačidlo MUTE, nieto ešte chrániť firemné dáta alebo svoju identitu, mali hekeri široké pole realizácie. Napriek optimizmu, ktorý sprevádza návrat do normálu aj na pracoviská, veľká časť zamestnancov aj zostane pracovať aspoň čiastočne z domu. Preto si predostrime päť bezpečnostných rád práce na diaľku.

Ochrana koncových zariadení

Firemné pracovné stanice sa stali novým perimetrom. Až 57 percent zamestnancov priznalo, že ich firemné notebooky počas pandémie využívala aj rodina. I keď je to nepopulárne opatrenie, firemný hardvér treba obmedziť len na firemné použitie. Využívajte dôslednú aplikačnú kontrolu na pracovných staniciach a dajte používateľom len najnižšie možné oprávnenia, ktoré potrebujú.

Bezpečné pripojenie do firmy

Pre ochranu vzdialeného prístupu k firemným zdrojom je nutné mať zapnuté stále pripojenie cez VPN. Ak sa používateľ potrebuje flexibilne pripojiť len k niektorým vybraným aplikáciám napríklad z mobilu, firmy začali využívať tzv. aplikačné brány. Tie vedia publikovať aplikáciu bez VPN a silne overiť vzdialeného užívateľa.

Multifaktorové overovanie

Firmy nerady nasadzujú multifaktorové overenie, lebo je to otravné. No bezpečnostné výhody silného overenia sú nesporné – budete si istí, kto k vám pristupuje, a nemusíte sa obávať, že zamestnanec nevyužíva silné, unikátne heslá.

Čoraz populárnejšie sú cloudové MFA systémy, ktorými si zjednodušíte ich nasadenie a správu. Zamestnanci získajú komfortnú obsluhu – overenie môže byť pushom do mobilu, skenovaním QR kódu alebo biometricky.

Manažment hesiel

Už pred pandémiou platilo, že heslá sú najväčšou slabinou bezpečnosti. A stále platí, že obzvlášť dôležité je používať komplexný manažment hesiel s auditnou stopou využitia hesiel, ich automatickou rotáciou a možnosťou zdieľať heslá medzi používateľmi.

Vzdelávanie používateľov

Žiadna technológia nie je odolná proti kreativite používateľa. Podľa štúdie CyberArk až 67 percent používateľov obchádzalo v ostatnom roku bezpečnostné opatrenia, keď pracovali. Preto stále vysvetľujte, prečo sa treba chrániť a ako pracovať, aby sa nenarušila bezpečnosť.

Dokonalá bezpečnosť neexistuje, ale je mnoho menších krokov, ktoré pomôžu znížiť riziká. Ak sa sústreďujete na oddelenie pracovných a osobných zariadení, zavedenie multifaktorového overenia a vynútenie najnižších potrebných oprávnení, tak ste na dobrej ceste.

A berte zreteľ na jednoduchosť, aby používatelia nemali dôvod bezpečnosť obchádzať.

Daniel Hetenyi, regionálny manažér CyberArk

Ešte pred pár rokmi bola kancelária na pláži nemožná. SNÍMKA: DREAMSTIME

TECHNOLÓGIE

Prečo potrebujeme neustále monitorovanie temného webu

Nielen Mesiac má svoju odvrátenú stranu. Analógiu možno nájsť aj v prípade webu. Pre bežného používateľa sú rôzne časti webu neviditeľné. Podobne ako keby ste chceli ďalekohľadom pozorovať odvrátenú stranu Mesiaca.

Tradičným spôsobom, prostredníctvom vyhľadávačov, ako sú Google alebo Bing, sa k dátam na deep webe nedostaneme.

Temný web

Dark web, alebo temný web, tvorí iba mizivé percento odvrátenej strany webu. Je často vykresľovaný ako záhadný, hlavne plný ilegálnych aktivít a pre používateľov bez špecifických odborných znalostí nedostupný.

Pre odborníkov z kybernetickej bezpečnosti predstavuje dark web zdroj informácií v boji a prevencii proti kybernetickým útokom. Okrem potenciálne užitočných informácií sa tu však nachádza aj množstvo nepotrebného materiálu a balastu ako aj na tradičnom webe. Ak sa však dostaneme za hranicu informačného šumu, tak zistíme, že temný web je nesmierne cenným zdrojom informácií.

Ako funguje

V podstate ide o subsystém internetu. Je prístupný pomocou špeciálneho nástoja ako napríklad Tor. Ten umožňuje používateľom a prevádzkovateľom webových stránok zostať v anonymite.

Webové stránky na tomto webe fungujú vo svojom vlastnom jedinečnom prostredí oddelenom od komerčne dostupných webov, ako sú napríklad Facebook či Amazon. Práve anonymita je to, prečo je táto časť webu taká príťažlivá pre používateľov.

Často tu pôsobia rôzni jednotlivci či skupiny, ktorí ponúkajú množstvo služieb, a nehovoríme len o ilegálnych aktivitách. Bežne sa tu však môžete stretnúť s ponukou na vykonanie útoku či so škodlivým kódom ako službou. Pojem „as a service“ je populárny aj v týchto komunitách.

Napriek popularite spájanej hlavne s nelegálnou činnosťou má temný web aj veľa legitímnych stránok a používajú ho ľudia ako novinári, aktivisti, prípadne orgány činné v trestnom konaní.

Ako sa tam dostať

Ak by si niekto myslel, že inštalácia prehliadača Tor mu otvorí svet temného webu, nebude to celkom pravda. Aj temný web má svoje skryté časti.

Mnoho informácií je síce prístupných každému, ale tie z „relatívne“ ľahko dostupných častí majú obmedzenú pridanú hodnotu. Zaujímavejšie časti sú spravidla limitované pozvánkou a vyžadujú špeciálny prístup. Niekedy až roky praxe, keď si používateľ buduje identitu a dôveryhodnosť akceptovanú v určitých komunitách.

Ako to zužitkovať

V uzavretej časti temného webu môžu ľudia častejšie nájsť informácie pochybnej pridanej hodnoty. Tieto kanály, známe tiež ako kriminálne podsvetie, často presahujú z temného webu až do súkromných kriminálnych fór či skupín hosťovaných na šifrovaných komunikačných platformách.

Ak viete informácie na temnom webe uchopiť správne, tak vám poskytnú jedinečný pohľad na to, ako premýšľajú a fungujú počítačoví kriminálnici. Bude jednoduchšie identifikovať aktivity, ktoré sa niekto chystá vykonať, ale stále ešte nie triviálne.

Všetko zlé je na niečo dobré

Temný web rovnako ako iné siete je možné monitorovať a zhromaždené informácie o hrozbách potom použiť na prevenciu pred útokmi.

Samotný nástroj na prvý pohľad vyzerá ako prehliadač nastavený na pokročilé vyhľadávanie, je to však spravodajská platforma (Intelligence Platform). Stačí vhodne formulovať požiadavku a pomocou umelej inteligencie a strojového učenia sa informácie zozbierajú a zobrazia v prehľadnom okne. Jazykovú bariéru preklenú pokročilé metódy na spracovanie prirodzeného jazyka, a tým rozšíria dopyt globálne.

Prostredníctvom platformy Recorded Future však odborníci prehľadávajú nielen zdroje na temnom webe, ale napríklad aj na sociálnych médiách či rôznych fórach.

Používanie takýchto platforiem umožní proaktívne identifikovať a zmierňovať riziko, hneď ako sa informácia objaví.

Martin Vívodik, bezpečnostný konzultant Clico, s. r. o.

SVIETI ČERVENÁ KONTROLKA

Ak sa tieto indikátory objavia na temnom webe, naznačujú bezpečnostným tímom, že niečo nemusí byť v poriadku. Toto je ukážka tých najrozšírenejších.

Prihlasovacie údaje
E-mailové adresy a heslá organizácií sú často na predaj formou aukcie, kde býva časť z nich zverejnená zdarma vopred.

Prístup do organizácie
Ponúka sa prístup do organizácie prostredníctvom chyby zabezpečenia, prípadne prihlasovacích údajov. Automatizovaná identifikácia ponuky proaktívne zabráni zneužitiu.

Zmienky o spoločnosti
Aktéri hrozieb diskutujú o svojich útokoch a pripravovaných plánoch na diskusných fórach. Pozorným a automatickým sledovaním zmienok o organizáciách či o tretích stranách môžete predchádzať kybernetickým útokom.

Zmienky o zraniteľnostiach
Sledujme, ktoré zraniteľnosti sú cieľom diskusie a útokov. Pomáha nám to priorizovať odstránenie zraniteľností.