HN
obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
26. – 28. JANUÁRA 2024

Odborná spolupráca

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

SK CERT
NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

Táto trojica kyberhrozieb naberá sily

TÉMA

Vo svete dominovali ransomvér, hacktivizmus a umelá inteligencia. Liek na kyberzúfalstvo a proti finančným stratám nekúpite. Pripraviť sa však môžete.

Profesionáli varujú pred finančnými stratami, manipuláciou volieb a polarizáciou spoločnosti. FOTO: DREAMSTIME

Svetové ekonomické fórum zostavuje každý rok zoznam globálnych rizík v horizonte dvoch až desiatich rokov. V správe Global Risks Report v roku 2024 sa na druhé miesto prepracovali misinformácie a dezinformácie generované umelou inteligenciou

Jednoduché používateľské rozhrania a AI nástroje umožnili explóziu skreslených, zavádzajúcich, zmanipulovaných a sfalšovaných informácií. Dostali vlastné označenie „syntetický obsah“. Znamená to všetko od sofistikovaného klonovania hlasu a obrazu až po falošné webové stránky.

Sme opäť pri tom istom

Michal Srnec zo spoločnosti Aliter Technologies však poukazuje na to, že situácia na Slovensku je zložitejšia kvôli zvýšenej náchylnosti na dezinformácie. Index mediálnej gramotnosti nás totiž zaraďuje až do tretieho klastra z piatich.

Index zahŕňa 41 štátov a meria potenciálnu zraniteľnosť voči dezinformáciám v Európe, Spojenom kráľovstve a na Balkáne. Do úvahy sa berie kvalita vzdelania, sloboda médií, miera dôvery v spoločnosti a využívanie nových nástrojov participácie. Vyššie skóre naznačuje lepšiu odolnosť spoločnosti voči vplyvu dezinformácií a súvisiacich javov. Slovensko dosiahlo 48 bodov zo sto, čo nám prinieslo pozíciu tak v strede rebríčka.

Trend hovorí jasne

Umiestnenie Slovenska v rebríčku mediálnej gramotnosti a expandujúce riziko dezinformácií sú veľmi znepokojivé trendy. Táto kombinácia spôsobuje, že sa prepadáme čoraz nižšie v schopnosti odolávať dezinformáciám, pričom hrozby s nimi spojené raketovo rastú.

Ako sa brániť? „Prvým krokom je kritické myslenie pri prijímaní informácií,“ hovorí Michal Srnec. Dôležité je overovanie správ, ideálne cez alternatívne komunikačné kanály. „Uvedomte si tiež taktiky sociálneho inžinierstva, ktoré často vyvíjajú tlak na jednotlivcov. Práve tento tlak je spoločným menovateľom mnohých kyberútokov.“

Kybernetické útoky

Piatym najväčším globálnym rizikom sú podľa Správy WEF práve kybernetické útoky. Nové technologické nástroje otvárajú nové trhy pre zločinecké siete. Kybernetická kriminalita ako zdroj príjmov organizovaného zločinu má čoraz nižšie riziko a náklady. Predstavuje to významné ohrozenie pre jednotlivcov, inštitúcie, firmy aj štáty.

Podvody neustávajú

Prevažná väčšina kyberútokov sa začína podvodným mailom či škodlivým softvérom na webových stránkach. Detekčné systémy spoločnosti ESET vo svete hlásia, že najviac škodlivých detekcií predstavujú stále phishingové hrozby. A ani Slovensko v tomto nie je výnimkou.

Znepokojivým trendom je nárast množstva webových stránok infikovaných škodlivým JavaScript kódom, ktorý dokáže zariadenie obete využiť na ďalšie útoky. Pri tejto hrozbe stačí na kompromitáciu zariadenia iba to, že obeť navštívi infikovaný web.

Čoraz viac peňazí

Analytická spoločnosť IDC hlási, že výdavky na kyberbezpečnosť vo svete boli v roku 2023 historicky najvyššie – až 219 miliárd dolárov – a v nasledujúcich dvoch rokoch predpovedá dvojmiestny rast. Vyvstáva otázka, prečo nevidíme drastické zníženie počtu kybernetických incidentov.

> Technológie napredujú a aktéri hrozieb nachádzajú stále nové spôsoby.
>
> **Tomáš Vobruba,** bezpečnostný špecialista

„Realita je taká, že kybernetické útoky budú rásť ešte intenzívnejšie. Technológie napredujú a aktéri hrozieb nachádzajú stále nové spôsoby,“ predikuje Tomáš Vobruba, bezpečnostný špecialista Check Point Software Technologies. „Tieto roky nám ukazujú, že väčšina ozbrojených konfliktov sa začína práve kyberútokom.“

Phishingové útoky

Pre kyberzločincov je jednoduchšie prihlásiť sa do systému pomocou ukradnutých prihlasovacích údajov než prácne prelamovať obrany a striehnuť na zraniteľnosti.

Vzhľadom na relatívny úspech a jednoduchosť phishingových kampaní bude čoraz viac útokov, ktoré používajú kradnuté prihlasovacie údaje. Navyše, phishingové taktiky budú s využitím umelej inteligencie personalizovanejšie a účinnejšie, čo ešte viac sťaží identifikáciu škodlivých aktivít.

Hackeri aktivisti

Ak bude geopolitická nestabilita pokračovať, hacktivistických útokov bude pribúdať.

Mnohé hacktivistické skupiny síce využívajú ako dôvod na útoky politickú agendu, ale často tak maskujú skryté motívy. Trend naznačuje, že hranice medzi hacktivizmom a komerčnými útokmi sa budú stierať, pretože hackerské skupiny využívajú ransomvér ako zdroj príjmov na financovanie rôznych aktivít.

Rafinovanejšie vydieranie

Očakáva sa, že príde k rozšíreniu „Living Off The Land“ techník, ktoré používajú na útoky legitímne systémové nástroje. Tento subtílnejší prístup je ťažšie odhaliť a akcentuje nutnosť preventívnych stratégií. Ide najmä o riadené detekcie a reakcie, ktoré dokážu presne určiť anomálie v správaní zariadení a sietí.

Aj keď organizácie posilňujú obranu proti ransomvéru, strát alebo únikov dát bude pravdepodobne pribúdať. Dôležitým faktorom môže byť rastúca závislosť od SaaS platforiem, ktoré ukladajú citlivé dáta ako súčasť aplikačných služieb.

Kontrola dodávateľov

Počet incidentov týkajúcich sa dodávateľského reťazca je alarmujúci a vplyv takéhoto útoku môže byť ďalekosiahly. Pre organizácie to znamená, že budú musieť dôslednejšie posudzovať bezpečnostné opatrenia dodávateľov.

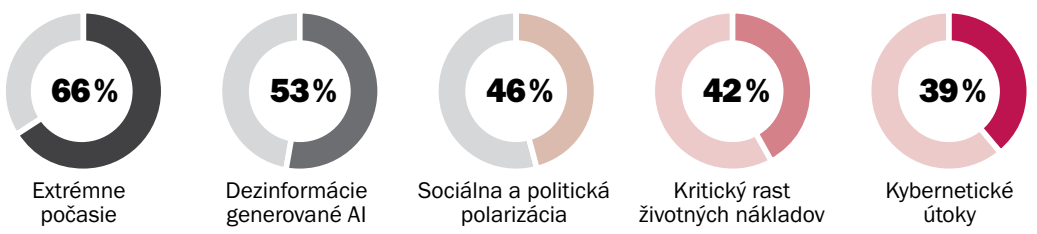
Tu majú zásadný význam prísnejšie bezpečnostné protokoly v dodávateľskom reťazci. Kyberzločinci sa totiž zameriavajú na menších dodávateľov, aby získali prístup k väčším spoločnostiam.

Nožnice sa roztvárajú

„S rastúcimi a novými rizikami sa mení aj stratégia kybernetickej obrany,“ predikuje Jozef Bálint zo spoločnosti Alison Slovakia. Keďže bezpečnostný softvér a hardvér zaznamenávajú markantný vývoj, kyberobrana sa stáva čoraz viac sofistikovaná.

Zároveň však bude musieť obrana viac pracovať s tými najslabšími. Kyberútoky sa budú čoraz viac sústreďovať na digitálne menej gramotných jednotlivcov a nedostatočne zabezpečené infraštruktúry a systémy.

Súčasné globálne riziká



Zdroj: Global Risk Report 2024, World Economic Forum

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 26. – 28. JANUÁRA 2024

Keď technológie predbiehajú rozum

ANKETA

Aké sú odporúčania v boji proti falšovaným informáciám, dezinformáciám a klamlivému obsahu? Čo robiť a na čo sa sústrediť? Kde začať? Povedzte nám vaše skúsenosti.

Miroslav Michalko,
riaditeľ
Univerzitný vedecký park TECHNICOM

Odpoveď na tieto otázky je netriviálna. Overenie pravosti informácií a ich interpretácie si vyžaduje čas, napríklad na posúdenie dôveryhodnosti zdroja a kritické zhodnotenie z viacerých perspektív. Vzhľadom na obrovské množstvo informácií je kľúčové vyberať si médiá a zdroje, ktoré dodržiavajú princípy objektívnosti, či už v spravodajstve, vo vede alebo v medicíne.

Jaroslav Ďurovka,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Falošná alebo klamlivá informácia je takmer vždy základným znakom podvodu alebo kybernetického útoku založenom na sociálnom inžinierstve. Aj preto je dôležité v prevencii systematicky zvyšovať povedomie ľudí, ako rozpoznať klamlivú informáciu alebo manipulatívne techniky útočníkov. Ľudia musia pochopiť, že nie všetko, čo si prečítajú na internete alebo v e-maile, je pravda. Odosielateľovi nesmiete bezvýhradne dôverovať.

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

Začať treba vo vzdelávaní. Veriť len dôveryhodným zdrojom. Dôraz dávať na kritické myslenie a tvoriť si schopnosť vedieť si overiť pravosť informácie. Pri pretlaku informácií a polarizácii spoločnosti je to však čoraz ťažšie. Dobrý dezinformátor totiž vie zabaliť dezinformáciu do pravdivého obsahu. Osobne odporúčam prečítať si knižky od bývalých defektorov, ktorý sa tejto problematike venovali.

Ivan Kopáčik,
bezpečnostný expert
Gordias

Tento boj sa začína pri budovaní a posilňovaní kritického myslenia, v každom veku. Nedá sa spoliehať na žiadne blokovanie obsahu ani filtrovanie AI nástrojmi, ktoré navyše u viacerých vyvoláva pachuť cenzúry. Sústrediť sa treba na svoj „personálny mentálny firewall“ a pravidelne ho aktualizovať kritickým myslením.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Nástup AI a s tým ruka v ruke deepfake je výzvou. V dobe, keď sú Facebook a sociálne siete pre väčšinu hlavnou platformou, odkiaľ berú spravodajské informácie, je dôležité byť si vedomý možných rizík a využívať možnosti na overenie si zdrojov. Rozoznať vplyv umelej inteligencie je veľký problém. Aj spoločnosť OpenAI musela svoj program na rozoznávanie pre falošnú pozitivitu minulý rok stiahnuť. Rozvoj digitálnej a mediálnej gramotnosti je nevyhnutný na ochranu pred manipuláciou a dezinformáciami v digitálnom svete.

Tibor Szabo,
vedúci Oddelenia auditu IT
Všeobecná úverová banka

Vieme sa technicky brániť voči škodlivému kódu, vírusom či útokom hackerov, ale voči dezinformáciám nie. Je potrebné začať vzdelávaním a zvyšovaním povedomia ľudí v každej vekovej kategórii a byť trpezlivý. Žiaľ, stretávam sa s dezinformáciami v pracovnom živote, v súkromí, a to hlavne na sociálnych sieťach. A som presvedčený, že efektívnejší spôsob ako vzdelávanie som zatiaľ neobjavil.

Július Selecký,
senior technický špecialista
ESET

Bežné rady ako overovanie faktov či kritické myslenie nemusia stačiť. V súčasnosti čelíme z rôznych strán sofistikovaným koordinovaným dezinfo kampaniam, často aj pod záštitou cudzích štátov. Preto je dôležité riešiť tento problém systémovo, na národnej úrovni.

Pavol Vrabec,
manažér kybernetickej bezpečnosti
Univerzitná nemocnica Martin

V tejto dobe je už pre každého z nás veľmi zložité sa úplne vyhnúť alebo nepodľahnúť falošným a klamlivým informáciám. Pre odporúčanie, ako reagovať, by som použil takzvané pravidlo troch Z. Zastaviť sa pri spracúvaní informácií. Zamyslieť sa, či je informácia relevantná alebo sa aspoň sčasti môže zakladať na pravde. Zareagovať alebo zdieľať informáciu až následne.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies Slovensko

Čelíme zložitým otázkam, ktoré sú viac filozofické a morálne ako technologické a potrebujeme tu spoluprácu viacerých zainteresovaných strán. Poskytovatelia AI musia prijať proaktívne opatrenia na to, aby zabránili zneužívaniu jej postupov a regulačné orgány aktualizovať normy a predpisy. Základnou podmienkou hodnotenia informácií je kontext, v ktorom sa objavujú. Patrí sem pochopenie zdroja informácie, identity hovoriaceho a jeho motivácie.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Od škôlky až do dôchodku ľuďom trpezlivo a neúnavne pripomínať, že vecná argumentácia je len taká, ktorá sa opiera o FAKTY, nie o NÁZORY. Argument sa dá považovať za vecne správny iba v takom prípade, že východisková časť úsudku je podložená DÔKAZOM. Subjektívne názory sú nedôveryhodné a v žiadnej slušnej komunikácii nemôžu byť akceptované. O to menej v serióznych médiách a zdrojoch.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti
Aliter Technologies

Asymetria medzi úsilím, ktoré je nutné vynaložiť na vytvorenie falošnej správy a medzi úsilím, ktoré je nutné na jej vyvrátenie, je priam astronomická – vyvracanie falošných správ je extrémne časovo náročné. Samotný boj teda netkvie v ex post vyvracaní, hoci aj to je potrebné, ale v ex ante prevencii. Preto by sa pri prijímaní informácií malo zapojiť kritické myslenie, overovanie informácií a uvedomiť si, že nie všetko, čo je na internete napísané, je nutne pravda.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť
Západoslovenská energetika

Mimoriadne ťažká otázka, takže veľmi ocením odpovede kolegov. Bezpečnosť nie je iba profesia, je poslaním všade a každý deň. Môj „recept“, ako pristupovať k informáciám, je jasný – snažím sa používať sedliacky rozum, sústredím sa na dôveryhodnosť zdroja a ak ma konkrétna téma zaujíma, využívam „priateľov na telefóne“, ktorí sa v danej problematike orientujú.

Matej Síleš,
manažér IT bezpečnosti
UPC Broadband Slovakia

Informácie je potrebné čerpať z viacerých zdrojov, overovať si ich a hlavne myslieť kriticky. To znamená, že ak nájdem na internete nejakú bombastickú informáciu, tak sa k nej musím postaviť s nedôverou a radšej si overím zdroj informácie. Pokúsim sa nájsť viac zdrojov takejto informácie a medzi nimi nájsť tie, ktoré sú mi známe a považujem ich za dôveryhodné. Tomuto spôsobu je potrebné učiť a školiť používateľov.

Ivan Kotuliak,
dekan
Fakulta informatiky a informačných technológií STU Bratislava

Dezinformácie a klamlivý obsah je veľmi ťažké odlíšiť, keďže na Slovensku, ale ani celosvetovo nie sú médiá odolné na sto percent. Preto je dôležité kľúčové informácie overovať z viacerých zdrojov. Prioritne by to mali byť zdroje, kde sú jasní pôvodní autori správy a majú dôveryhodnú históriu. Treba zdôrazniť, že je dôležité overovať si kľúčové informácie a nielen tie, ktoré nám nesedia.

Tomáš Zaťko,
etický hacker, CEO
Citadelo

Ľudí priťahujú senzácie, odhalenia a sladký pocit že „viem viac“. Je tam komfort, a preto sa z dezinfo vlaku ťažko vystupuje. Zorientovať sa vo svete rozporuplných informácií a posúdiť ich dôveryhodnosť si vyžaduje mentálnu a časovú investíciu. Musíme si zvoliť, pre aké informácie chceme túto investíciu robiť. A pri ostatných prijať, že na väčšinu vecí vo svete nie je možné mať dôveryhodný názor.

Michal Ďorda,
audítor kybernetickej bezpečnosti
Auditori.it

Boj s hoaxmi sa nedá vyhrať, ani prehrať. Avšak prečo by sme nemohli využiť umelú inteligenciu? Hľadala by a zbierala po celom internete všetky zdroje, kde sa daná informácia nachádza a poskytla všetky objavené zdroje ako atribút, takzvané metadáta k samotnému článku. Potom už je to len na čitateľovi, ako funguje jeho kritické myslenie a ktorú informáciu akceptuje alebo považuje za dezinformáciu.

Tibor Paulen,
manažér informačnej bezpečnosti
Stredoslovenská distribučná

Pri skúmaní dôveryhodnosti získanej informácie sa mi osvedčilo najskôr sa prepnúť z emotívneho do racionálneho módu a následne si zodpovedať nasledujúce otázky: Kto alebo čo je primárnym zdrojom informácie? Akú mám dôveru k predošlým informáciám z tohto zdroja? Ako dopadlo overenie cez alternatívne dôveryhodné zdroje? Ako informácia zapadá do logického rámca ostatných informácií, ktorým dôverujem?

Stanislav Smolár,
manažér oddelenia bezpečnosti
Soitron

Mne osobne sa najviac osvedčilo verifikovanie informácií voči iným zdrojom. Pokiaľ existuje nejaká informácia len v rámci jedného komunikačného kanála, napríklad Telegram či Facebook, tak je to okamžitý dôvod na opatrnosť. Takisto aj každé komerčné médium má nejakú mieru zaujatosti, a preto sa správy vždy snažím vnímať aj vzhľadom na to, kto a kedy ich publikuje.

Richard Kiškováč,
generálny riaditeľ
Elkan

Pri riadení kybernetickej bezpečnosti je škodlivý obsah vnímaný skôr ako nástroj alebo prostriedok, ktorý sa využíva na kybernetický útok a kompromitáciu systémov. Falošné informácie sa na tento účel využívajú najmä v sociálnom inžinierstve. Pre komplexné posudzovanie obsahu je však potrebný úplne iný druh expertízy, akým disponujú kyberbezpečnostní odborníci.

Jaroslav Oster,
predseda správnej rady
Preventista.sk

Najschodnejšie riešenie dostupné okamžite a pre každého používateľa je jednoduché a elementárne – rozmýšľať. Väčšina prípadov, kde ľudia prepadnú manipulatívnym informáciám a stanú sa obeťami rôznych foriem podvodu, nemusela nastať. Stačilo len pouvažovať, či je to logické, overiť si došlú informáciu či fotografiu, posúdiť a zvážiť. A až potom konať – poslať osobné údaje, zaplatiť niečo kartou a podobne. Jednoducho dvakrát merať a raz rezať.

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov
Tatra banka

Odporúčam čitateľom dezinformáciám neveriť a vyhýbať sa im. Ako dezinformácie odhaliť? Napríklad – ak dostanú rýchle a jednoduché riešenie problému, ktorý sa nepodarilo spoločnosti vyriešiť dlhý čas. Vzťahy medzi ľuďmi, menšinami, väčšinami, národmi je možné vysvetliť zopár slovami. Riešenie nikto nepopíše preto, lebo tomu bráni známa, ideálne malá záujmová skupina alebo bohatý štát.

Miroslav Chlipala,
riadiaci partner
BCH Advokáti Chlipala

Z mojich skúseností odporúčam aktívnu prevenciu. Potrebujeme vzdelávacie programy pre verejnosť aj nástroje na identifikáciu klamlivého obsahu. Rovnako dôležité sú kampane o dôsledkoch šírenia falošných informácií a podpora informovanej online komunity. Komplexný prístup spočíva v kombinácii vzdelávania, technologických riešení a právnych opatrení.

Róbert Mramúch,
manažér kybernetickej bezpečnosti
MH Teplárenský holding

Čerpajte z overených zdrojov a periodík, kde zverejnená informácia podlieha širšej revízii. Čítajte s porozumením, ideálne všetko a do konca. Používajte zdravý rozum a nenaleťte senzáciám. Načúvajte vedcom a odborníkom, zatraťte snahy poblúdencov z „alternatívnej scény“ a trollích fariem. Preverujte, preverujte, preverujte.

Ján Andraško.
SOC manažér
Binary Confidence

Sedliacky rozum a overovanie informácií. Ku každej novej informácii sa implicitne stavať tak, že to nemusí byť pravda. Ak niečo znie príliš dobre alebo neuveriteľne, takmer určite to bude blud. A špeciálne to platí pri vyjadreniach našich politikov.

Dominik Procházka,
riaditeľ odboru bezpečnosti
AGEL SK

Hneď mi napadlo len jedno: používať sedliacky rozum.

Čomu sa už nevyhneme

LEGISLATÍVA

Európska smernica o bezpečnosti informačných systémov NIS2 ovplyvní všetky členské štáty. Niekde to budú zmeny na úrovni prestavby, niekde iba korekcie. Aj slovenský zákon o kybernetickej bezpečnosti čaká tohto roku novelizácia.

Ivan Makatura generálny riaditeľ Kompetenčného a certifikačného centra kybernetickej bezpečnosti vyzýva k spolupráci.

FOTO: HN/ PETER MAYER

Akby sa mali ambície bezpečnostnej legislatívy zhrnúť v troch bodoch, tak by to boli prehľadnejšia identifikácia regulovaných subjektov, vyššia miera interoperability a zníženie negramotnosti v kybernetickej bezpečnosti.

Dajme veci na pravú mieru

Smernica NIS2 je fakticky dôvodom na novelizáciu zákona o kybernetickej bezpečnosti. Vzhľadom na to, že náš zákon patrí v Európe k tým prísnejším, NIS2 zásadnejšie zmeny na Slovensku nevyvolá.

O to viac ma udivuje, že sa na trh vyrojilo množstvo pseudokonzultantov a právnikov, korí smernicu NIS2 vykladajú v úplne nezmyselnom kontexte. Straší klientov údajnými novými povinnosťami NIS2, pričom im radi ihneď ponúknu pomoc s ich „implementáciou“. Pravdaže, nie zadarmo.

Isté veci sa transpozíciou NIS2 do zákona síce zmenia, avšak neustále je potrebné zdôrazňovať, že tí, ktorí dodržujú zákon dnes, nemusia mať vážnejšie obavy, že by boli v nesúlade so zákonom po jeho novelizácii.

Aktualizovaný zoznam

Pozornosť priťahujú najmä sektory a činnosti, na ktoré sa vzťahujú povinnosti v oblasti kyberbezpečnosti. Novelizácia zákona bude zároveň rozlišovať kľúčové a dôležité subjekty.

Kľúčové subjekty podnikajú v energetike, doprave, bankovníctve, infraštruktúre finančných trhov, zdravotníctve, priemysle, riadení služieb IKT, pitnej a odpadovej vode a patrí sem verejná správa a vesmírny sektor.

Dôležitými subjektmi sú tie, ktoré prevádzkujú poštové a kuriérne služby, odpadové hospodárstvo, výrobu a distribúciu chemických látok či potravín, výrobu zdravotníckych pomôcok, motorových vozidiel, dopravných prostriedkov, elektroniky a v neposlednom rade poskytovatelia digitálnych služieb a výskum.

Počet regulovaných subjektov

Jedným slovom? Vzrastie. Základné kritérium, či ide o regulovaný subjekt, bude veľkosť podniku v príslušnom sektore. K súčasným prevádzkovateľom základnej služby tak pribudnú ďalší.

Budú sem patriť verejné alebo súkromné podniky uvedeného druhu, ktoré zamestnávajú 50 a viac zamestnancov a ročný obrat alebo ročná súvaha predstavujú aspoň 10 miliónov eur.

Oznamovanie aj pomoc

Z praktického hľadiska pribudnú požiadavky reakcie na incidenty. Regulovaný subjekt musí určiť osobu zodpovednú za plnenie zákonných povinností, manažéra kybernetickej bezpečnosti.

Všetky závažné kybernetické incidenty sa budú hlásiť sektorovému tímu CSIRT. Do 24 hodín bude potrebné predbežné upozornenie, do 72 hodín podať aktualizovanú správu. Do jedného mesiaca bude treba vyhotoviť finálnu správu o prebiehajúcom riešení incidentu.

Cieľom je umožniť rýchlu reakciu, spoluprácu, zaistiť účinné riešenie a minimalizáciu negatívnych dosahov incidentov.

Rozsah riadenia rizík

Pripravovaná legislatíva sa sústreďuje aj na predchádzanie incidentu kontrolou zraniteľností a podčiarkuje výkon auditu kyberbezpečnosti. V úsilí zvýšiť úroveň kybernetickej bezpečnosti dáva dôraz na prácu s ľuďmi ako najzraniteľnejším článkom.

Smernica NIS2 obsahuje aj takzvaný koncept správy rizika, kde by mali spozornieť štatutári. Štatutárne orgány budú mať povinnosť schváliť opatrenia na riadenie rizík kyberbezpečnosti, pričom smernica stanovuje aj možnosť vyvodenia osobnej zodpovednosti.

Zdieľanie aj sankcie

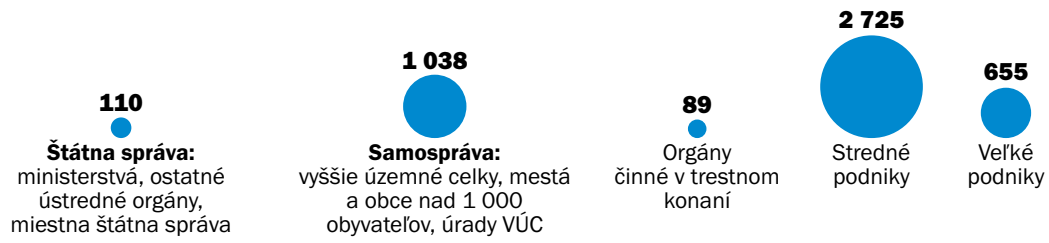
Do novelizácie zákona sa premietnu vyššie nároky na bezpečnostné požiadavky v dodávateľskom reťazci, v používaní šifrovania a aj pri zverejňovaní zraniteľností.

Smernica zavádza aj nový sankčný mechanizmus a zvyšujú sa pokuty. Maximálna výška pokuty v prípade kľúčových subjektov bude desať miliónov eur alebo dve percentá z celosvetového obratu. Pre dôležité subjekty je strop pokuty sedem miliónov eur alebo 1,4 percenta celosvetového obratu.

Časový horizont

Predpokladá sa, že Národný bezpečnostný úrad predloží prvý návrh novelizácie zákona pre odbornú verejnosť v marci. Do konca polroka by malo byť ukončené medzirezortné pripomienkové konanie, aby sa novelizácia dostala na rokovanie Národnej rady v septembri.

Predpokladaný aktualizovaný počet prevádzkovateľov základných služieb



SPOLUPRÁCA

Musíme spojiť komunitu

Nikto nezvládne kyberbezpečnosť bez spolupráce. Týka sa to firiem, inštitúcií, profesií aj štátov. Je to náročná multidisciplinárna oblasť, ktorá extrémne rýchlo napreduje.

Rozhodnutie Európskej únie cielene budovať kyberbezpečnostnú komunitu vzniklo dávno pred vojenským konfliktom na jej východných hraniciach a akceleráciou kybernetických hrozieb.

Únia síce disponuje znalosťami a skúsenosťami vo výskume, v technológiách a priemyselnom rozvoji v kybernetickej bezpečnosti, ale roztrieštenosť odvetvových a výskumných komunít znižuje jej konkurencieschopnosť v globálnom priestore. A tým sa znižuje aj účinná ochrana sietí a systémov, či už ide o štáty, firmy alebo občanov.

Digitalizácia je nezastaviteľná

Na európskej úrovni sa preto rozvíja spolupráca siete národných koordinačných centier, pričom na Slovensku plní toto poslanie Kompetenčné a certifikačné centrum kybernetickej bezpečnosti už druhý rok.

Rozhodne tou najakútnejšou úlohou je prepojenie verejného a súkromného sektora v kybernetickej bezpečnosti a vzájomná dôvera.

Kompetenčné centrum sa preto v súčasnosti sústreďuje na spájanie kyberbezpečnostnej komunity a získanie financií z európskych zdrojov. V súlade s európskou legislatívou pripravuje certifikáciu kybernetickej bezpečnosti digitálnych produktov a služieb a sprostredkuje poznatky o vývoji v tejto oblasti vrátane produktov, postupov a technických noriem.

Ľudia a zas ľudia

Aby komunita fungovala efektívne, je organizovaná do pracovných skupín vzhľadom na potreby jednotlivých sektorov. Osem špecializovaných a jedna strategická poradná skupina umožňujú členom zdieľať znalosti a skúsenosti v kybernetickej bezpečnosti.

Členmi komunity sa môžu stať právnické osoby so sídlom v Slovenskej republike. Podľa sektorového zaradenia členstvo zahŕňa aj aktívnu účasť v príslušnej pracovnej skupine a je bezplatné.

Rád nikdy nie je dosť

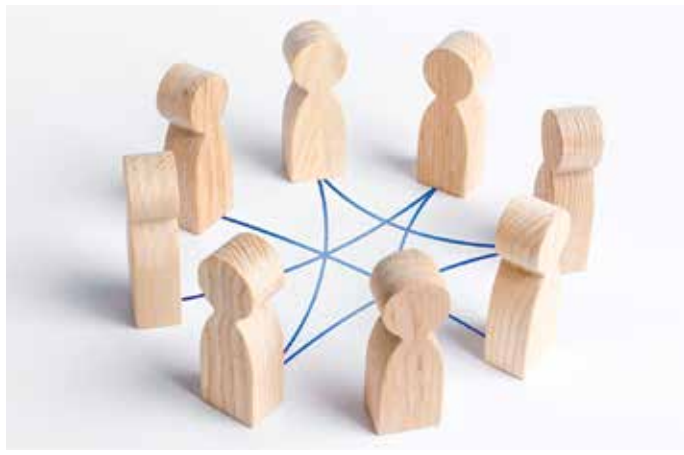
Aj slovenské Národné koordinačné centrum reaguje na nedostatok vzdelávacích a personálnych kapacít. Poskytuje poradenské služby pre podnikateľov a organizácie v kybernetickej bezpečnosti, či už ide o legislatívu alebo transfer poznatkov do praxe.

Pre záujemcov organizuje školenia, webináre a workshopy a pre vybrané sektory vytvára vysoko špecializované vzdelávacie kurzy.

Ako súčasť európskej siete je Kompetenčné centrum zodpovedné za cezhraničnú spoluprácu a zúčastňuje sa na harmonizácii legislatívy.

PRACOVNÉ SKUPINY

- Veľké podniky a telekomunikácie
- Malé a stredné podniky
- Výrobcovia a poskytovatelia služieb
- Verejná správa
- Školstvo a vzdelávanie
- Veda, výskum a inovácie
- Jednotky pre riešenie počítačových incidentov CSIRT (Computer Security Incident Response Team)
- Občianske združenia a mimovládne neziskové organizácie



Budúcnosť kyberbezpečnosti je v spolupráci odborov a profesií. FOTO: DREAMSTIME

SERVIS

Európske finančné výzvy sú otvorené. Hláste sa o grant aj vy

Financie z programu Digitálna Európa slúžia na spolufinancovanie projektov kybernetickej bezpečnosti a dajú sa získať rýchlo a efektívne

Priamo riadené programy EÚ sa vyznačujú rýchlym rozhodovaním, komunikáciou s Bruselom, jednoduchou administráciou a aj implementáciou.

Tento typ finančnej pomoci je manažovaný priamo Európskou komisiou a poskytuje rýchly a jednoduchý proces implementácie bez zbytočnej byrokracie.

Európska komisia otvára výzvy určené na podporu určitého typu projektov alebo oblastí. Žiadatelia, ktorí majú záujem o podporu, sa môžu prihlásiť na tieto výzvy a podávať žiadosti online.

Projektový formulár môže mať maximálne 70 strán a obsahuje informácie o projekte – ciele, opis aktivít, harmonogram a finančný plán. Štúdie uskutočniteľnosti nie sú potrebné a grantová schéma umožňuje väčšiu slobodu pre individuálne nápady.

Projekt hodnotia nezávislí európski hodnotitelia a medzi podaním projektu a zverejnením výsledkov neuplynie viac než tri mesiace.

Ak je projekt úspešný, Európska komisia so žiadateľom uzatvorí grantovú dohodu. Rozpočty nemajú národné kvóty, čo vytvára rovnakú „štartovaciu čiaru“ pre všetky projekty.

V procese implementácie nie sú potrebné žiadne zo zahlcujúcich dokumentov, známe z národných projektov financovaných z eurofondov. Platby sú posielané rovnako priamo, bez sprostredkovateľských orgánov.

Priamo riadené projekty majú takzvanú výnimku z pravidiel štátnej pomoci.

Michal Ohrablo o programe Digitálna Európa. FOTO: HN/ PETER MAYER

Priestor pre vaše nápady

Otvorené výzvy reagujú na súčasný vyvoj v kybernetickej bezpečnosti a legislatíve s dosahom na veľký počet subjektov. Uzávierka je 26.3. 2024, pričom percentuálna miera financovania z celkových oprávnených nákladov je 50 percent.

Umelá inteligencia pre strediská bezpečnostných operácií (SOC)

Aktivity by mali smerovať k vývoju a nasadeniu systémov a nástrojov pre kybernetickú bezpečnosť založené na podporných technológiách

Nasadenie postkvantovej kryptografie v systémoch v priemyselných sektoroch

Integrácia štandardizovaného PQC (Post Quantum Cryptography) protokolu do digitálnej bezpečnosti a komunikačných sietí v automobilovom, automatizačnom, finančnom alebo energetickom sektore

Nástroje na implementáciu požiadaviek a povinností vyplývajúcich z Nariadenia o kyberodolnosti

Návrh a vývoj nástrojov na uľahčenie a podľa možnosti automatizácie dodržiavania požiadaviek Nariadenia o kyberodolnosti (CRA) s osobitným zameraním na automatizované nástroje pre dodržiavanie súladu V prípade malých a stredných podnikov financovanie 75 percent oprávnených nákladov.

Ak potrebujete poradiť, alebo máte otázky, napíšte na **projektyEU@cybercompetence.sk** Podrobnejšie informácie na **www.kyberkomunita.sk**

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 26. – 28. JANUÁRA 2024

Svet ide ďalej, aj hrozby sa menia

REPORT

Správa o kybernetickej bezpečnosti ESET Threat Report H2 2023 upozorňuje na hrozby v druhej polovici roka 2023. Globálna štatistika je zostavená na základe údajov z detekčných systémov spoločnosti ESET a práce výskumných centier.

1.

Najčastejšie zachytávanou hrozbou na Slovensku v druhom polroku 2023 bol phishingový podvod evidovaný ako HTML/Phishing. Agent. Táto detekcia tvorila viac ako **19 percent zachytených škodlivých vzoriek.**

Kybernetický útok sa začína HTML prílohou, ktorá obsahuje falošné prihlasovacie okno imitujúce prihlásenie do rôznych populárnych služieb, ako napríklad Outlook.

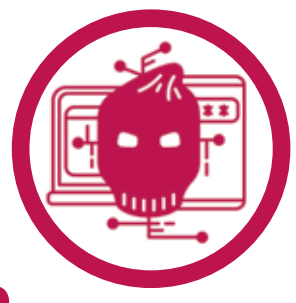
Bežne sa distribuuje prostredníctvom e-mailov a slúži najmä na krádež prihlasovacích údajov.

2.

Druhé miesto s podielom takmer **12 percent detekcií** patrí hrozbe s názvom DOC/Fraud.

Tento podvod zneužíva sexuálnu tematiku.

Útočníci obetiam pošlú e-mail, v ktorom tvrdia, že im infiltrovali zariadenie a zachytili ich v chúlostivej situácii. Vyhrážajú sa, že ak obeť nezaplatí požadované výkupné, rozpošlú kompromitujúci materiál. V skutočnosti však diskreditujúcimi zábermi kyberzločinci nedisponujú a spoliehajú sa len na strach obete.



3.

Detekcie JS/Agent tvorili takmer **10 percent zachytených škodlivých vzoriek.** V porovnaní s minulým polrokom narástli o 125 percent, čím sa v štatistike hrozieb vyšvihli zo šiestej pozície na tretiu.

Zariadenie obete sa infikuje aj bez toho, aby návštevník čokoľvek zo stránky sťahoval.

Do tejto kategórie patria rôzne škodlivé JavaScript kódy. Útočníci ich umiestňujú na zraniteľné, ale legitímne webové stránky s cieľom kompromitovať návštevníkov. Útočníci zvyčajne infikujú webové stránky, ktoré využívajú komponenty s bezpečnostnými zraniteľnosťami.

Takmer 45 -tisíc webových stránok vo svete

sa stalo obeťou škodlivého kódu JavaScript

Jedna dobrá správa

Po dvoch rokoch kontinuálneho rastu klesol v druhom polroku 2023 celkový počet zachytených hrozieb na Slovensku približne o štvrtinu v porovnaní s prvým polrokom. Početnosť sa tým vrátila na úroveň spred dvoch rokov.

„Dramatický nárast kybernetických hrozieb súvisel práve s vojnou, ktorá prebieha aj v kyberpriestore. Postupný pokles hrozieb sme detegovali v iných regiónoch už skôr, na Slovensku sa prejavil trend až v druhej polovici minulého roku," vysvetľuje Ondrej Kubovič, špecialista na digitálnu bezpečnosť spoločnosti ESET.

Bude vás zaujímať

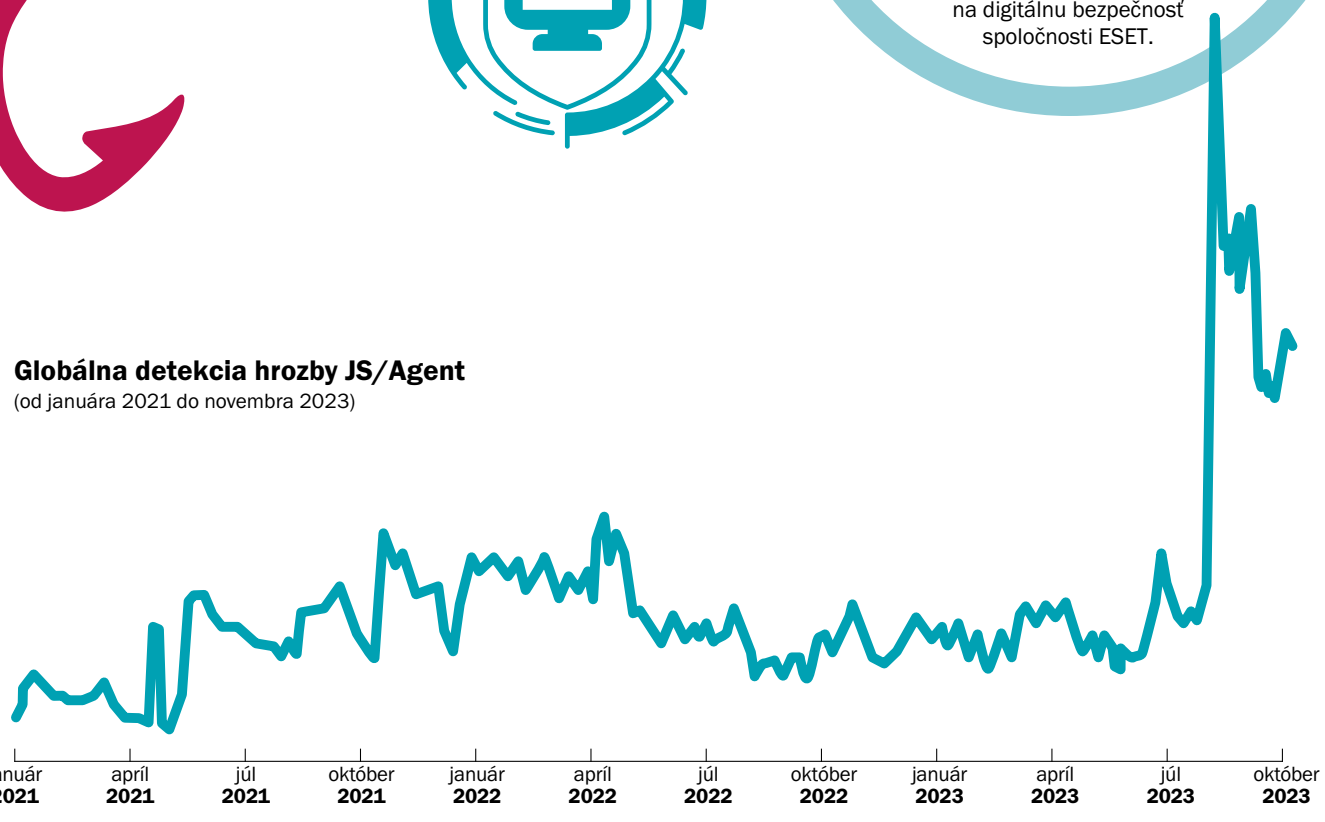
Výskumníci hlásia 89-percentný nárast **sledovacieho softvéru** – spyvéru v Android zariadeniach. Škodlivý kód sa nachádza v softvérovom vývojovom balíku pre mobilný marketing. Po inštalácii funguje aplikácia ako spyvér, pričom vynáša rôzne údaje z napadnutého zariadenia.

Smartfóny, tablety, inteligentné televízory a TV boxy s operačným systémom Android sú čoraz častejšie terčom kyberútočníkov. Malvér dokáže zneužiť infikované zariadenia na vykonávanie DDoS útokov. Výskumníci zaznamenali masívne útočné aktivity v septembri 2023 a botnet identifikovali ako Android/Pandora.

Spoločnosť ESET zaznamenala a zablokovala vo svete 675-tisíc pokusov o prístup k škodlivým doménam, ktoré obsahujú v názve **„ChatGPT"**. Hrozby spojené s týmito doménami zahŕňajú najmä webové aplikácie. Tie môžu kradnúť kľúče k OpenAI API, spojené s prístupom k všetkým AI aplikáciám tohto prevádzkovateľa a k fakturácii pre používateľa.

Threat Report H2 2023 nájdete na webovej stránke Bezpečne vo firme

Globálna detekcia hrozby JS/Agent
(od januára 2021 do novembra 2023)



Odporúčania

Správcovia webových stránok by si mali dávať pozor na to, aké pluginy inštalujú. Ide najmä o publikačný systém WordPress, na ktorom je postavených množstvo webových stránok na Slovensku. Dôležité je, aby administrátori nasadzovali aktualizácie hneď, ako sú dostupné. Jedine tak dokážu zabrániť zneužitiu existujúcich zraniteľností v pluginoch alebo v samotnom softvéri.

Najlepšou ochranou pred webovými stránkami so skrytým škodlivým kódom je bezpečnostné riešenie, ktoré dokáže hrozby automaticky detegovať a okamžite blokovať.