HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
31. MÁJ – 2. JÚNA 2024

Odborná spolupráca
NBÚ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Na osobné údaje sme veľmi citliví a zároveň zlyhávame pri ich ochrane

TÉMA

Za necelú dekádu sme prešli v osobných údajoch od fázy vystrašenia cez široké povedomie až k extrémnej precitlivenosti. A smerujeme k fáze paniky.

Naše údaje sú v mobiloch, počítačoch, na sieťach, v aplikáciách, v pokoji aj v pohybe. FOTO: DREAMSTIME

Adresy, rodné čísla, fotky, diagnózy, kamerové záznamy, čísla účtov, IP adresy a GPS súradnice už nie sú len osobné údaje, už je to potrava kybernetického zločinu.

Jednou vetou

Profesionáli aj autority sa zhodujú, že povedomie o ochrane osobných údajov je výborné, opatrenie často diskutabilné.

Slabou stránkou v ochrane osobných údajov je prílišný formálny prístup prevádzkovateľov aj sprostredkovateľov. Plnenie povinností stále vnímajú ako „nevyhnutné zlo“, hovorí odborníčka a lektorka Marcela Macová. Firmy a inštitúcie sa mylne domnievajú, že im stačí niečo ako bezpečnostný projekt, ktorý už dávno nie je aktuálny, a majú „pokoj“. Pritom dodržiavať ochranu osobných údajov je vec každodenná.

Treba ešte strašiť?

Viceprezident slovenskej pobočky ISACA Tomáš Hettych urobil viac ako 50 auditov ochrany osobných údajov a 20 implementácií. „V prvých rokoch to bolo viac o presvedčovaní vedenia, že prečo to potrebujú. S mediálnou kampaňou a po strašení pokutami sa situácia výrazne zlepšila.“

Tomáš Hettych tu poukazuje na obrovské rozdiely. Najlepšie pripravené sú nadnárodné korporácie a bankový sektor. „Majú dostatok zdrojov na prípravu dokumentácie, nastavenie procesov aj na právnikov ako osoby zodpovedné za ochranu osobných údajov.“

Málo pripravené sú výrobné podniky, stredné firmy, verejná správa a zdravotníctvo. Chýbajú im prostriedky aj motivácia niečo riešiť. Ako kriticky hovorí audítor, „niekedy radšej míňajú peniaze na právnu kanceláriu ako na samotnú ochranu“.

Keď (ne)ide štát príkladom

Aj podľa názoru Marcely Macovej verejný sektor ešte stále pristupuje k ochrane osobných údajov benevolentnejšie. „Súkromné spoločnosti sa viac obávajú sankcií a najmä poškodenia mena.“ Preto viacej dbajú na nastavenie procesov, aktualizovanú dokumentáciu, vzdelávanie zamestnancov a vyberajú si dodávateľov, ktorí dbajú na GDPR.

Profesionálov však už roky trápia „šmejdi“ na trhu. Zneužívajú neznalosť alebo finančnú tieseň obcí a miest a predávajú im nefunkčnú dokumentáciu spolu s vystrašením pred pokutami a súdmi.

Čo hovoria občania

Povedomie rastie z roka na rok aj u občanov. Dotknuté osoby sa viacej chránia a Úrad na ochranu osobných údajov hlási rastúci počet podnetov a návrhov na začatie konania.

Takže čo sa týka pokút, minulý rok ich uložil úrad najviac za porušenie zásad spracúvania osobných údajov pri kamerových informačných systémoch. V tejto oblasti bolo aj najviac kontrol. Nasledovali pokuty pre tých, ktorí nevedeli preukázať právny základ za zverejnenie osobných údajov dotknutých osôb na webových stránkach alebo ich sprístupnenie. Pokuty si vyslúžili aj zverejnenia videozáznamov a dokumentov, ktoré obsahovali osobné údaje dotknutých osôb, a nesprávna anonymizácia.

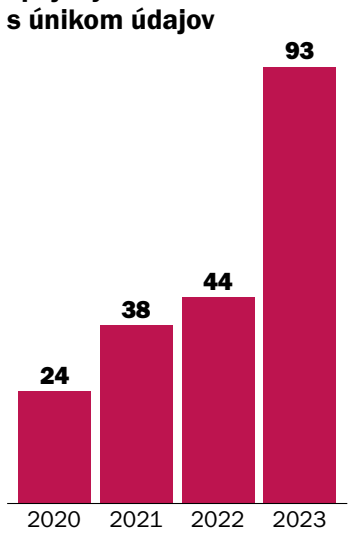
Previnilcami boli mestá, obce, štátne inštitúcie a prevádzkovatelia – veľké aj malé spoločnosti.

Naše ukradnuté údaje

V minulom roku na Slovensku viditeľne pribudol počet hlásení o únikoch osobných údajov. „Evidujeme stoosemdesiatpäť prípadov a obávame sa, že to bude rásť,“ potvrdzuje Martin Oczvirk, riaditeľ odboru informačnej bezpečnosti a certifikácie ÚOOU. A zároveň upozorňuje aj na markantný rast kybernetických incidentov.

Incidenty sú spôsobené rôznymi hackerskými útokmi, pričom najčastejšie ide o ransomvér. A príčina? Obvyklá. „Vo všeobecnosti útočníci nájdu v systéme zraniteľnosť alebo využívajú metódy sociálneho inžinierstva.“

Počet kyberincidentov spojených s únikom údajov



Zdroj: Úrad na ochranu osobných údajov

Už sa to nedá zastaviť

Či chceme, alebo nechceme, ochrana osobných údajov a kyberbezpečnosť úzko súvisia a prelínajú sa. Interní aj externí odborníci v oboch oblastiach musia spojiť sily a spolupracovať.

Expanzívna digitalizácia a apetít kybernetickej kriminality pridávajú kyberbezpečnosti v ochrane osobných údajov čoraz viacej úloh. Musí zabezpečiť, že údaje zostanú dôverné, integrálne a dostupné iba oprávneným osobám, chráni ich pred hrozbami. Či už ide o osobné údaje, ktoré sú v aplikáciách, v zdravotníckych zariadeniach, online obchodoch, na sociálnych sieťach alebo v štátnych systémoch.

Ideme ďalej

Dlhodobou profesionálnou agendou Jakuba Berthotyho z advokátskej kancelárie Dagital Legal je nariadenie GDPR v praxi. Slovensko vidí ako európskeho lídra v nízkom výkone nariadenia GDPR.

V porovnaní s inými členskými štátmi sa podľa neho u nás ukladajú neprimerane nízke pokuty a často aj za bezvýznamné a pre prax nezaujímavé porušenia. Uvádza, že francúzsky úrad na ochranu osobných údajov si jednou pokutou vyberie celý ročný rozpočet slovenského úradu. A pripomienky pokračujú.

„Naša štátna autorita sa zaoberá susedskými spormi a nespokojnými zamestnancami, ale nerieši Google, Facebook, TikTok, maloletých, sociálne siete, big data algoritmy a cielenie reklamy. Pritom sú to témy, kvôli ktorým GDPR vzniklo.“

A ďalšia výzva

„Úrad nemá kompetenciu riešiť tému cookies a nevyžiadanej marketingovej komunikácie podľa ePrivacy. A rovnaký problém nás čaká s ďalšími novými predpismi EÚ,“ varuje Jakub Berthoty. Pôsobnosť úradu by sa mala preto posilniť a pridať mu podstatnú časť regulácie, ktorá sa týka dát, súkromia a ľudí.

Po vzore European Data Protection Supervisor by mala byť na úrovni vlády hlavná zodpovedná osoba za ochranu údajov. Metodicky aj pokynmi by usmerňovala zodpovedné osoby v sektoroch alebo nižšie.

Súčasťou by boli aj kódexy správania v tejto oblasti, ako majú banky, poisťovne a advokáti. Prečo ich nemajú nemocnice, mestá, obce, ministerstvá, súdy a školy? Jednotný výklad a úroveň súladu by mali rešpektovať odlišnosti sektorov. A v prvom rade chrániť občanov.

TOP3 GDPR MÝTY NAJČASTEJŠIE OMYLY

„Na všetko postačí súhlas so spracovaním osobných údajov“

„Táto fantastická GDPR dokumentácia za 99 eur vyrieši všetky vaše problémy“

„V našej firme osobné údaje vôbec nemáme“

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 31. MÁJ – 2. JÚNA 2024

Precitnutie do reality. Konečne?

ANKETA

Máj je zvyčajne čas na fakty a čísla zo Správy o kybernetickej bezpečnosti Slovenska. Anketa k tomu pridáva názory profesionálov a skúsenosti z praxe. V ktorej oblasti kybernetickej bezpečnosti vnímate významný medziročný posun? V dobrom či zlom.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Zvyšujú sa investície do pokročilých bezpečnostných technológií a úsilie organizácie o vyššie povedomie zamestnancov. Podľa Slovenského inštitútu pre kybernetickú bezpečnosť investície medziročne vzrástli o 20 percent. Odvrátenou stranou je väčšie fokusovanie útočníkov už aj na Slovensko, čo prináša viac kyberútokov na kritickú infraštruktúru a záujem o citlivé dáta štátnych inštitúcií aj komerčného sektora.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Celková odolnosť prevádzkovateľov proti kyberhrozbám sa zvýšila. Skokanom roka je výrobný priemysel. Niektoré sektory prešľapujú na mieste. Na konci tabuľky sú už tradične verejná správa a zdravotníctvo. Ak by si niekto myslel, že je to nedostatkom financií, mýlil by sa. Hlavným dôvodom nesúladu je totiž nedostatočná vyspelosť manažérstva, nízka úroveň povedomia a chýbajúce procesy riadenia rizík.

Andrej Mišura,
partner
Cyllium

Ako vidno aj v správe NBU, organizácie sa konečne začínajú venovať kyberbezpečnosti. Zrejme pochopili nevyhnutnosť. Niektorí už implementujú technické opatrenia a viacerí si po prvých auditoch objednali aspoň dodanie dokumentácie. Je to krok správnym smerom, ale odporúčam nastaviť stratégiu, aby to nebolo iba „na zalepenie očí“.

Peter Dufek,
manažér kybernetickej bezpečnosti
Penta Hospitals

Asi najväčší medziročný posun v oblasti kybernetickej bezpečnosti vnímam v zlepšovaní výsledkov auditov zhody opatrení so zákonom v niektorých sektoroch zaradených do povinného overovania.

Pavol Sokol,
vedúci CSIRT-UPJS
Univerzita Pavla Jozefa Šafárika v Košiciach

Za posledný rok sa zvýšil počet zverejnených výziev na informačnú a kybernetickú bezpečnosť, či už v oblasti operatívnych činností, vzdelávania alebo výskumu. Ide o vítaný a žiadaný posun. Otázne je, ako výrazne to zmení úroveň bezpečnostného povedomia, ale aj odolnosti proti bezpečnostným hrozbám u rôznych kategórií príjemcov.

Ján Golais,
poradca bezpečnosti
Slovak Telekom

Povedomie sa postupne zvyšuje, stále však nedosahuje dostatočnú úroveň. Zvyšuje sa totiž aj počet „odborníkov“ predávajúcich copy paste dokumentáciu. Bohužiaľ, stále nemáme nástroj, ako regulovať tieto aktivity realizované už aj predajom od dverí k dverám.

Marián Klačo,
vedúci oddelenia bezpečnosť informácií
Volkswagen Slovakia

Jednou z oblastí je osveta. Viac sa hovorí o kyberbezpečnosti, o nástrahách a rizikách, ktoré na používateľov číhajú. Nastal podstatný posun vo vnímaní kyberbezpečnosti ako témy na Slovensku. Najmä v súvislosti s očakávanou implementáciou NIS2 a rozšírením zoznamu dotknutých subjektov. Viaceré organizácie sa pripravujú na novú verziu zákona o kyberbezpečnosti a na nové výzvy, ktoré im z nej môžu vyplynúť.

Ivan Kopáčik,
bezpečnostný expert
Gordias

Posun k lepšiemu vnímam v oblasti bezpečnostného povedomia občanov. Rôzne druhy kybernetických podvodov zamerané na najširšie vrstvy obyvateľstva sú na dennom poriadku. Ak ľudia nechcú opakovane naletieť podvodníkom, musia získať aspoň elementárne kyberbezpečnostné návyky a zručnosti. Bohužiaľ, často sa poučia až v dôsledku vlastných chýb.

Július Selecký,
senior technický špecialista
ESET

Z hľadiska sektorov by som vyzdvihol smer, akým sa uberá kybernetická bezpečnosť v zdravotníctve. Zo skúseností vieme, že významné narušenie IT bezpečnosti v nemocnici sa môže skončiť aj ohrozením životov pacientov. A toto si štatutári zjavne uvedomujú.

Tibor Szabo,
vedúci oddelenia auditu IT
Všeobecná úverová banka

Oceňujem progres v oblasti auditu, kde spolupracujú audítori a AI špecialisti, čo pocítime uvoľnením zdrojov pre najrizikovejšie oblasti. Umelá inteligencia nenahradí audítorov, len podstatne urýchli audit a „živý“ audítor sa bude môcť sústrediť na hodnotiace a analytické činnosti, kde je potrebný jeho úsudok.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť
Západoslovenská energetika

Aktuálna bezpečnostná situácia vo svete a najmä na našich hraniciach ovplyvňuje kybernetické správanie firiem. Výsledkom je významný posun v nasadení technicko-organizačných opatrení. To je tá lepšia správa. Druhá strana mince je, že kyberhrozby sa rovnako významne rozširujú a zintenzívňujú. Nie, nežijeme v úplne bezpečnom svete.

Dominik Procházka,
riaditeľ odboru bezpečnosti
AGEL SK

Vnímam významný posun v spoločnostiach, ktoré patria do nášho zdravotníckeho holdingu. Viac si uvedomujú význam kybernetickej bezpečnosti, aktívne sa zapájajú pri podozreniach a spolupracujú.

Miroslav Chlipala,
riadiaci partner
BCH Advokáti Chlipala

Lepšia znalosť zákonného rámca, podpora vzdelávania a financovanie zo zdrojov EÚ zvýšili povedomie o kybernetických hrozbách a odolnosti. Prispieva k tomu aj aktívna kyberkomunita a podujatia zamerané na kyberbezpečnosť. Dôležité je stále pokračovať.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies

Chcem byť optimista a skutočne vidím posun. O kyberbezpečnosti sa hovorí všade, dokonca už aj na pive pri vedľajšom stole. Únia uvoľňuje na zvýšenie bezpečnosti čoraz vyšší objem financií pre členské štáty aj vybrané sektory. A to zákonite musí prinášať aj reálne výsledky. Nesmieme však poľaviť a už vôbec nie zaspať a myslieť si, že je to už dobré. Zlo nespí.

Roman Čupka,
hlavný konzultant
Progress a CSO Istrosec

Ostatné dva roky evidujeme enormné množstvo úspešných ransomvérových útokov. Následkom je významný posun v zmýšľaní organizácií, ktoré sú často aj prvkami kritickej infraštruktúry. Sú rozhodnuté investovať nemalé prostriedky do svojej odolnosti a hľadajú najmä serióznych partnerov na zvládanie incidentov. Začínajú si uvedomovať, že kvalitné partnerstvá znižujú riziko negatívnych dosahov a zlepšujú ich pripravenosť.

Martin Orem,
hacker
Binary House

Zaznamenali sme zvýšený dopyt po preventívnych službách ofenzívnej bezpečnosti z väčšiny sektorov. Na druhej strane vnímame nárast rôzne motivovaných DDoS a ransomvérových útokov, ktoré odrážajú dianie na geopolitickom poli. Útoky sú často koordinované a viac či menej sofistikované, čo môže poukazovať na prepojenie medzi zločincami a štátmi.

Jaroslav Ďurovka,
riaditeľ
Národné centrum kybernetickej bezpečnosti

Zlepšuje sa prístup kľúčových subjektov a obchodných spoločností ku kyberbezpečnosti. Hoci nejde o skokový progres, je dôležité aj postupné zlepšovanie ich odolnosti proti meniacim sa hrozbám. Riziká stúpajú s meniacou sa štruktúrou a kvalitou útočníkov, hekerských komunít a APT skupín. Tie čoraz častejšie používajú sofistikované postupy a nástroje a okamžite zneužívajú novoobjavené zraniteľnosti. Výsledkom sú napríklad vážne ransomvérové a vysokoobjemové DDoS útoky.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti
Aliter Technologies

Posun na Slovensku je v tomto roku významný. Kým vlani sa kyberbezpečnosť dostala za okrúhly stôl vedenia firiem, tento rok prenikla aj do mainstreamu. Tomu pomohli hojne debatovaná legislatívna zmena NIS2, nedávne úniky dát a štátmi sponzorované kybernetické útoky. Negatívom, ktorý bohužiaľ naberá na trakcii, je vplyv dezinformácií spojených aj s AI, ktoré sa šíria aj na Slovensku.

Ján Benka,
cybersecurity konzultant
Soitron

Počet útokov na malé firmy rastie a zároveň sa posúva ich sofistikovanosť. Je vidieť, že útočníci si dávajú záležať aj na útokoch na menšie spoločnosti, dokonca aj na našom malom trhu. Organizácie, žiaľ, vo väčšine nie sú na kyberútoky pripravené a nevedia na ne reagovať. Alebo len na čas strčia hlavu do piesku a dúfajú, že keď sa znova obzrú, bude všetko v priadku. No, zdá sa, že už ani na Slovensku sa len tak neschováme.

Richard Kiškováč,
generálny riaditeľ
Elkan

Nevnímam významný medziročný posun v kyberbezpečnosti. Všetky jej atribúty prechádzajú pomalým vývojom tak ako dosiaľ. Kyberbezpečnosť je natoľko komplexná oblasť, že potrebuje na rozvoj aj adekvátny čas. Tento rozvoj urýchlia väčšinou len mimoriadne udalosti s výrazným dosahom. Preto je možno lepšie, keď nie sme nútení sa posúvať takýmto drastickým spôsobom.

Katarína Kročková,
odborníčka na ochranu osobných údajov
Kročka & Partners

Ochrana akýchkoľvek kategórií údajov by mala byť v každej organizácii prioritou, napriek tomu sa vyspelosť kyberbezpečnosti v jednotlivých sektoroch líši. Preto vítam a posun vidím najmä v malých a stredných podnikoch, ktoré zavádzajú bezpečnostné opatrenia, a tak chránia svoje údaje, aj tie osobné. Žiaľ, často sa stretávam aj s povrchným prístupom a formálnymi riešeniami.

Vladimír Frčo,
SOC bezpečnostný špecialista
Alanata

Spoločnosti, ktorých sa dotkne implementácia smernice NIS2 do nášho zákona o kybernetickej bezpečnosti, sa výrazne posúvajú v snahe implementovať bezpečnostné produkty. Obávam sa však toho, ako budú naplnené tieto požiadavky v samospráve na úrovni miest a obcí. S ich napätými rozpočtmi je veľmi ťažké odolávať moderným kybernetickým hrozbám, ktoré sa za posledný rok stali oveľa efektívnejšie.

Jaroslav Oster,
predseda správnej rady
Preventista.sk

Za najväčší „posun“, ale v negatívnom zmysle slova, považujem dynamický nárast prieniku technológií umelej inteligencie do oblasti sociálno-manipulatívnych útokov. Rad dnes už reálne vyšetrovaných prípadov napríklad v oblasti vydierania umelo generovanou pornografiou ukazuje v plnej miere, že prvotné nadšenie k potenciálnym prínosom AI bude mať aj tienisté stránky. A na tieto bežný používateľ nie je pripravený.

Tomáš Zaťko,
CEO, etický hacker
Citadelo

Kyberbezpečnostné opatrenia sa môžu realizovať „naozaj“ alebo „akože“. A pomer „naozaj“ a „akože“ sa zlepšuje. Čoraz viac firiem a ľudí sa o kybernetickú bezpečnosť zaujíma s cieľom skutočne ju riešiť. Nielen získať čarovný papier s pečiatkou, ktorý ukážu pri prípadnej kontrole.

Maroš Trnka,
vedúci odboru informačných technológií
Vodohospodárska výstavba štátny podnik

Vidím pokrok vo zvyšovaní bezpečnostného povedomia a vo vzdelávaní o kybernetických hrozbách. Dúfam, že sa pozitívne mení aj pomer medzi podnikmi, ktoré prijali opatrenia iba vo forme internej dokumentácie, a podnikmi, ktoré aj reálne implementujú nové bezpečnostné štandardy v rovine technických opatrení. Negatívne vnímam stále rastúci počet útokov na malé a stredné podniky, ktoré nie sú dostatočne pripravené.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 31. MÁJ – 2. JÚNA 2024

Hrozby, útoky, incidenty, škody, fakty

SPRÁVA

Najviac kybernetických bezpečnostných incidentov za minulý bolo hlásených zo sektorov verejná správa, bankovníctvo a zdravotníctvo.

Slovensko 2023: Najvýznamnejšie hrozby

1. Sociálne inžinierstvo

Sociálne inžinierstvo sa využíva v podvodných kampaniach na efektívnejšie dosiahnutie cieľa

Masívne phishingové kampane

- Napodobňovanie doručovateľských služieb, poskytovateľov internetového pripojenia, bankových a finančných inštitúcií, polície a Interpolu a orgánov štátnej správy.
- Zneužívanie známych online predajných platforiem a fór. Útočníci sa snažili vylákať od obetí citlivé informácie, najmä údaje z platobných kariet alebo prihlasovacie údaje do internetbankingu.
- Fenomén sexuálneho vydierania, pričom útočníci nemusia mať žiadny prístup k údajným citlivým materiálom.
- Podvody s kryptomenami. Útočník si získava dôveru obete tým, že prvotne vypláca provízie a potom sa stratí. Podvodné kampane podporujú masívna komunikácia na sociálnych sieťach a osobné stretnutia.

Whaling, napriek nižšiemu výskytu stále relevantný. Napríklad formou impersonácie riaditeľa spoločnosti so žiadosťou o stav účtu a platbu, pričom obeť je urgentne nasmerovaná odoslať finančné prostriedky domnelému nadriadenému či dodávateľovi.

Šírenie škodlivého obsahu cez dokumenty vytvorené v balíku MS Office klesá. Aktéri hrozieb využívajú v kampaniach e-mailové prílohy s príponami.lnk,.iso,. rar a podobne.

Interaktívne formy sociálneho inžinierstva spojené s phishingovými útokmi

Phishingové weby často obsahujú interaktívny chat, kde útočník vedie obeť online alebo telefonicky na vzdialenú správu a predstiera služby technickej podpory.

Podvodné kampane na sociálnych sieťach

Útočníci sa pokúšajú získať prístup k pracovným účtom alebo účtom s vysokým počtom sledovateľov, aby šírili škodlivý obsah. Modifikujú obsah platenej reklamy, zdieľajú podvodné príspevky alebo šíria ilegálny obsah.

Zneužívanie SMS platobných brán

Útočník pripraví žiadosť o SMS platbu na číslo obete a následne obeť presviedča, aby poslala SMS na štvorčíslie, ktorým sa platba potvrdí. Útočníci tak kupujú kľúče na odomknutie hier alebo iných rýchlo predateľných produktov, ktoré následne speňažia.

2. Nedostupnosť služieb a DDoS útoky

Rast DDoS útokov na kritickú infraštruktúru, bankový sektor a dopravu

Útoky smerovali z IP adries TOR, VPN, Open Proxy aj z kompromitovaných zariadení, často z botnetov prenajímaných hackerskými skupinami ako služba, ktoré útočníci používajú na maskovanie aktivity.

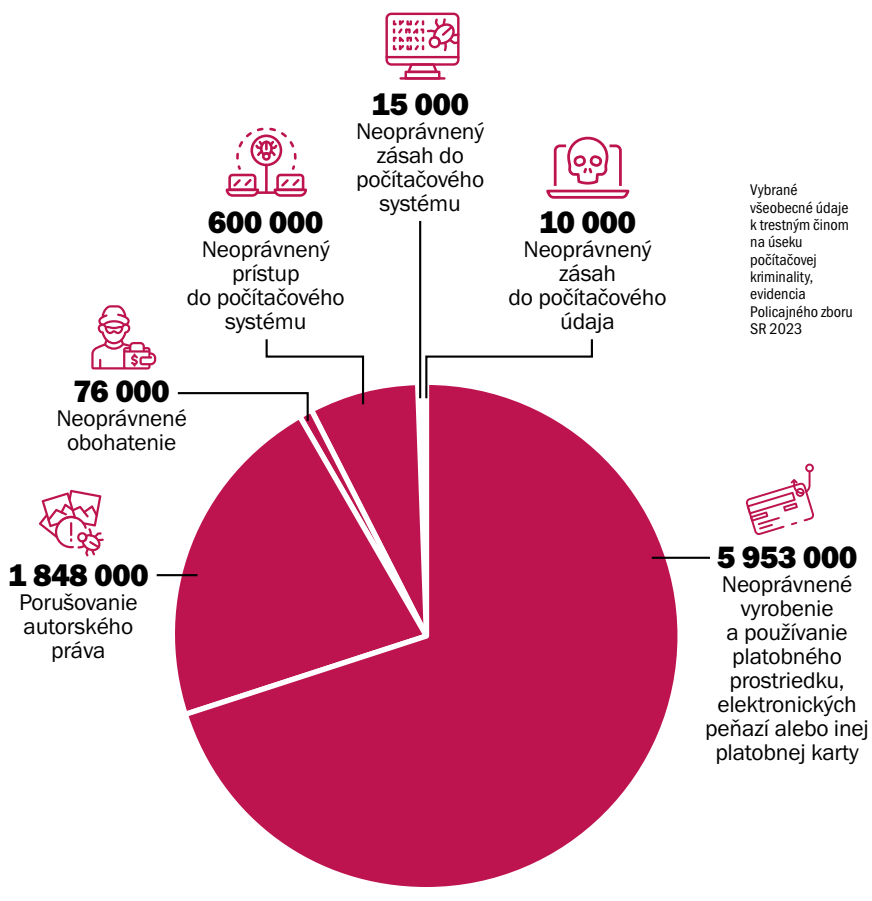
Výpadky a nedostupnosť systémov spôsobili aj nepripravenosť systémov na veľký nával legitímnych návštevníkov, zle vykonávaná údržba systémov, nesprávne implementovaná aktualizácia systémov či zavádzanie nových netestovaných prvkov a podobne.

Pozitívny jav

Narastajúca odolnosť infraštruktúry obetí po útoku a dôraz na prevenciu.

Aké škody napáchala počítačová kriminalita?

(spôsobená škoda v eurách)



Vybrané všeobecné údaje k trestným činom na úseku počítačovej kriminality, evidencia Policajného zboru SR 2023

Počet zistených prípadov

Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty	Porušovanie autorského práva	Neoprávnené obohatenie	Neoprávnený prístup do počítačového systému	Neoprávnený zásah do počítačového systému	Neoprávnený zásah do počítačového údaja
2 116	44	9	23	8	5

3. Malvér

Boli zaznamenané početné infekcie zariadení rôznymi rodinami malvéru.

Významné zastúpenie mali infekcie ransomvéru, čo súviselo s činnosťou skupín pokročilých hrozieb.

Najvýznamnejšie vektory prieniku

- Sociálne inžinierstvo
- Zlá bezpečnostná politika – používanie vlastných zariadení a služobných účtov na súkromné účely a podobne
- Navštevovanie kompromitovaných webových stránok
- Inštalácia trojanizovaného softvéru

4. Zraniteľnosti a pokusy o prienik do systému

Phishingové útoky boli najčastejším vektorom prieniku

Sú najefektívnejší spôsob, ako útočník prekoná bezpečnostné nastavenia systému.

Zraniteľnosti

Zraniteľnosti najmä vo verejne dostupných službách vzdialeného prístupu a výmeny dát.

Nesprávna konfigurácia zariadení

V prihlasovacích rozhraniach do priemyselných riadiacich systémov s nastaveniami z výroby a s pôvodnými heslami alebo rozhrania bez prihlasovania. Prípadne zlá politika hesiel.

Kompromitácia e-mailovej schránky

Kompromitácia ako následok phishingu a reťazové rozposielanie phisingových správ na kontakty kompromitovaného konta.

Kde sú nedostatky?

- Organizácie často zlyhávajú pri monitoringu a riadení zraniteľností, na základe čoho neboli schopné reagovať na prípadné hrozby v adekvátnom čase
- Zanedbávaná údržba zastaraných a výrobcom nepodporovaných zariadení, pretože predstavujú vysoké finančné a personálne zaťaženie. Následkom je nedostatočné riadenie aktualizácií alebo adekvátneho znižovania ohrozenia.

Zdroj: Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2023, NBU 2024

Nič nové pod slnkom?

Efektívna ochrana si vyžaduje spoluprácu odborníkov z legislatívy, aj z technológií. FOTO: DREAMSTIME

VÍZIA

V časoch, keď sú dáta novou „ropou“ spoločností a ich úniky čoraz častejšie, je ochrana osobných údajov kľúčovou úlohou.

Ochranu údajov z technologického pohľadu nemožno vnímať len ako konkrétny izolovaný problém, ktorý sa dá vyriešiť „technologickou krabičkou“. Ide skôr o to využiť etablované technológie a princípy na správne dáta a na základe ich povahy nastaviť technológie či princípy.

Povedzme si to na rovinu

Jednou z najdôležitejších ochrán osobných údajov je šifrovanie. Možnosti šifrovania, respektíve výber správnej metódy, šifry či dokonca princípu siaha ďaleko za možnosti tohto článku. Čo je však dôležitejšie a, bohužiaľ, často opomínané, kde sa samotné dáta šifrujú. Je nutné minimálne zvážiť šifrovanie dát pri prenose, používaní a aj počas toho, keď sa s nimi nepracuje. Dokonca aj pri zálohovaní.

Ak vieme, „kde“ sa dáta nachádzajú, prichádza na rad druhá, nemenej dôležitá otázka. Aké dáta? Inými slovami, aká je povaha dát, ktoré spracúvame, či tých na úložiskách? Klasifikácia dát je širší kontext, ktorý všeobecne odpovedá na otázku, aké dáta spracúvame vzhľadom na legislatívny či normatívny rámec. A identifikácia osobných údajov je len časť z nich.

Ak už vieme, „kde a aké“ dáta, máme ideálny počiatočný stav na stanovenie adekvátnej ochrany osobných údajov. Na výber sú rôzne prístupy šifrovania, logického oddelenia a samotného prístupu k dátam.

Prístup k dátam predstavuje ďalší stavebný kameň. Musí byť správne použitý, inak bude identifikácia a klasifikácia dát irelevantná. Hoci by sme implementovali správne šifrovanie na správne dáta, vytúžený efekt ochrany by sa nedostavil, ak by k dátam mali prístup neoprávnené osoby. Prístup je teda vhodné nastaviť pomocou princípov minimálnych oprávnení a nevyhnutnej znalosti.

Nové technológie

Niektoré technológie či trendy môžu priniesť výrazné zlepšenie pri ochrane osobných údajov. Jedným z nich je aj architektúra nulovej dôvery – Zero Trust. Koncept vychádza z predpokladu, že nikomu vnútri ani mimo siete nemožno dôverovať. Tento prístup potom znižuje riziko vnútorných hrozieb a zabezpečuje robustnú ochranu systémov v našej správe.

> Ochrana osobných údajov nie je nikdy uzavretý problém.
>
> **Michal Srnec,**
> vedúci oddelenia informačnej bezpečnosti Aliter Technologies

Prevratnou technológiou, ktorá by mohla zmeniť pohľad na ochranu osobných údajov, je blockchain. Prináša decentralizáciu, nemennosť a transparentnosť, čo sú vlastnosti, ktoré môžu významne prispieť k ochrane osobných údajov. Blockchain by mohol byť využitý na vytváranie bezpečných digitálnych identít a zabezpečenie, že údaje sú nemenné a transparentné. Je však nutné poznamenať, že nápad je len v rovine myšlienkového smeru či skorej idey.

Komplexný proces

Ochrana osobných údajov nie je nikdy uzavretý problém, ktorý by sa dal vyriešiť zázračnou krabičkou od renomovaného výrobcu. Je nutné dodržať základné princípy a hlavne si „poupratovať doma“, a teda vedieť, kde máme aké dáta a ako ich spracúvame.

Paradoxne, komplexná ochrana osobných údajov môže viesť k technologicky relatívne lacným riešeniam, ak budú vhodne nastavené a „šité na mieru“ danej organizácii. Tento princíp môže byť výhodný tak pre malé podniky, ako aj pre nadnárodné korporácie.

Napriek tomu, že Zero Trust architektúra a blockchain ponúkajú sľubné riešenia, základné bezpečnostné praktiky zostávajú nezmenené. Technológie klasifikácie dát pomocou umelej inteligencie nám môžu dokonca pomôcť s identifikáciou dát najmä pri rozsiahlych úložiskách.

Finálne vyhodnotenie a nastavenie opatrení bude vždy do značnej miery pozostávať z kombinácie základných stavebných kameňov a princípov overených časom v mnohých implementáciách.

PORADŇA

Recyklácia je „in“, pri heslách to však neplatí

Vo svete kybernetickej bezpečnosti sa pozeráme na prihlasovacie údaje ako na prvú líniu obrany podniku v boji proti čoraz sofistikovanejším hrozbám. Mať silné a bezpečné prihlasovacie údaje je preto kľúčové. Napriek ich dôležitosti môžu byť heslá kompromitované mnohými, aj relatívne jednoduchými spôsobmi.

Zneužitím prihlasovacích údajov sa to však vo väčšine prípadov nekončí a reťazec kybernetického útoku pokračuje. Výsledkom je zneužitie systémov a krádež citlivých údajov, finančné straty a poškodenie dobrého mena.

Čo hovoria dáta

Globálne štatistiky potvrdzujú, že bezpečnosť podnikových dát a systémov je čoraz častejšie narušená „prelomeným“ heslom. Podľa správy IBM X-Force 2024 ide o medziročný nárast o 71 percent.

No aj napriek rastúcej dostupnosti nových metód prihlasovania a túžbe po „bezheslovej“ budúcnosti vidíme, že práve heslá zostávajú najrozšírenejšou metódou autentifikácie. Zároveň sú však veľmi obľúbeným cieľom kyberzločincov.

Podľa Google Cloud 2023 Threat Horizons Report v uplynulom roku až 86 percent prípadov úniku firemných údajov pramenilo zo zneužitia ukradnutých prihlasovacích údajov. K tým sa útočníci môžu dostať rôznymi spôsobmi – od využitia sociálneho inžinierstva a phishingu cez malvér až po prelomenie viacfaktorovej autentifikácie či útoky hrubou silou. No napríklad aj tak, že ich ukradnú z vášho prehliadača.

Pozor na recykláciu hesiel

V ideálnom svete by sme sa preto mali snažiť útočníkom ich snahy čo najviac sťažiť. Prax však ukazuje pravý opak – podľa Google Cloud 2023 Threat Horizons Report môže za 60 percent globálnych kybernetických incidentov práve nedostatočná politika hesiel.

Tá v praxi vyzerá aj tak, že vaši zamestnanci heslá recyklujú – napríklad opakovane používajú ako prihlasovacie meno rovnaký e-mail a heslo, a to na viacerých zariadeniach, weboch či aplikáciách. Ak sa prostredníctvom nezabezpečeného webu kybernetický zločinec dostane k prihlasovacím údajom zamestnanca, ktorý ich používa zároveň aj v práci, zrazu má v rukách „kľúče od vášho kráľovstva“.

Heslá jedine bez papierika

Okrem toho môžu byť heslá vašich zamestnancov pre kyberzločincov veľmi ľahko uhádnuteľné. Zložité heslo by ideálne malo vyzerať ako dlhý reťazec znakov bez zmyslu. A ten sa dá len veľmi ťažko prelomiť, ak vôbec. Zároveň je však takéto heslo ťažko zapamätateľné. Riešením je správca hesiel, tzv. password manager.

Jedna vec je vytvoriť heslo bezpečné a jedinečné, druhá zas jeho spoľahlivá ochrana. A tá sa zanedbáva. Potvrdzujú to aj dáta – správcu hesiel musí globálne v práci používať iba 25 percent zamestnancov. Zapisovanie hesiel „na papierik“ alebo ich zdieľanie ďalším členom tímu je tak smutná prax nielen na Slovensku.

Bezheslová budúcnosť

Ako vidíme, v dnešnom digitálnom prostredí sa tradičné metódy autentifikácie založené na heslách ukazujú ako nedostatočné na to, aby vyhovovali vyvíjajúcim sa bezpečnostným potrebám. Aj preto sa čoraz viac organizácií obracia na alternatívne riešenia autentifikácie „bez hesiel“ využívajúce biometriu, hardvérové tokeny či mobilné push upozornenia. Tie zvyšujú bezpečnosť, ale aj zlepšujú používateľskú skúsenosť zamestnancov.

Aj keď tieto alternatívne riešenia zatiaľ nie sú uplatniteľné všade, predpokladáme, že nás čaká nová éra autentifikácie bez hesiel.

Silvia Strežová,
void SOC,
centrum kybernetickej bezpečnosti Soitron

RIEŠENIA

Ak ste si už upratali, postavíme pevnosť a pridelíme agentov

Legislatívne nariadenia sú silný donucovaní faktor na ochranu údajov, ale pozrite sa na to aj z hľadiska aktuálnych hrozieb. Ransomvérové útoky znamenajú nielen nedostupné dáta, ale aj ich predaj a viacnásobné vydieranie.

Technologická ochrana údajov je iba súčasťou veľkej skladačky kybernetickej bezpečnosti.

Rozhodne si pamätajte mantru dátovej bezpečnosti DPL, Data Lost Prevention, čiže prevenciu úniku dát. Je to obvykle kus softvéru na pracovnej stanici alebo na vstupnej bráne. Pozerá sa do dát a na základe klasifikácie či iných pravidiel bráni skopírovaniu alebo prenosu citlivých súborov kamkoľvek inam, než je dovolené.

Tradičné špecializované kyberbezpečnostné firmy nastupujú, keď „je upratané“, čiže nerieši klasifikáciu a správu dát podľa tagov. Organizácia, identifikácia, označovanie a správa dát na základe ich citlivosti a významu je doménou účtovníckeho alebo manažérskeho softvéru. Kyberbezpečnostné riešenia potom dokážu adekvátne chrániť aj komplexné dátové typy podľa normatívnych bezpečností, akými sú nariadenie GDPR či štandardy bezpečnosti údajov v platobných kartách a ochrane zdravotných informácií.

Šikovné sety na správu

Správcovia bezpečnosti v organizácii tak majú obvykle celý technologický set na to, aby nastavili bezpečnostné politiky podľa interných pravidiel aj legislatívy.

Pre dáta v pohybe je základným pravidlom, že nesmie dôjsť k nemonitorovanému úniku. Cieľom je teda všetko monitorovať a logovať. Na to slúžia prostriedky na ochranu koncových zariadení. Rovnaké bezpečnostné opatrenia platia aj na vstupných bránach, či už pri e-mailovej komunikácii, alebo v prehliadačoch. Problémom na týchto bránach je však fakt, že dáta prenášané cez internet sú šifrované. Protokol HTTPS tak síce zvyšuje bezpečnosť komunikácie, ale zároveň môže sťažiť detekciu škodlivého obsahu.

Preto potrebujeme zároveň aj analyzovať a kontrolovať šifrované prenosy, aby sme sa uistili, že neobsahujú škodlivý obsah alebo neporušujú bezpečnostné politiky organizácie. Jednoducho vykonávať HTTPS inšpekciu – a tú nikto väčšinou nemá nasadenú.

Takže základným stavebným kameňom bezpečnosti zostáva najmä ochrana koncových zariadení. Výhodou je, že už netreba riešiť šifrovacie kanály, keďže sme na konci „šifrovacej trubky“.

Tu sa na zvýšenie úrovne ochrany, monitorovania a správy systémov inštalujú agenti. Na počítačoch, laptopoch, či mobilných zariadeniach slúžia na monitorovanie, detekciu a reakciu na hrozby v reálnom čase. Rovnako na zariadeniach a sieťových bránach sú agenti na monitorovanie a kontrolu pohybu citlivých dát, aby sa predišlo ich úniku.

Sem patria aj antivírusový a antimalvérový softvér, šifrovacie zariadenia a automatizácia aktualizácií a záplat.

Agenti na zariadeniach na vzdialenú správu a monitorovanie umožňujú IT tímom sledovať a spravovať zariadenia z centrálnej konzoly. Vyššia úroveň je zber a odosielanie bezpečnostných udalostí a logov do centrálneho SIEM systému na analýzu a koreláciu.

Zariadeniami na kontrolu prístupu privilegovaných používateľov sa minimalizuje riziko zneužitia privilégií. Na sieťových zariadeniach a koncových bodoch sa monitoruje sieťová prevádzka, detegujú sa anomálie a hrozby.

Behaviorálna analýza sa využíva pri monitorovaní správania používateľov a systémov, čím sa identifikuje, a reaguje na neobvyklé a potenciálne škodlivé aktivity.

Takýchto agentov však môže byť na pracovnej stanici až príliš, pretože správcovia IKT obvykle hľadajú riešenia na ucelenú ochranu a chcú minimalizovať správu a zložitosť prostredia.

Daň za pohodlie

Ucelené kyberbezpečnostné produkty obvykle neponúkajú hlbokú granularitu. To je doména špecialistov. Na druhej strane, ak kvalifikovaný bezpečák využije celý potenciál komplexných riešení, dokáže získať „veľa muziky za menej peňazí“. Vždy sú tam však kompromisy.

A ak by pri ransomvérovom útoku zlyhali agenti, vždy tam ešte máte na bráne DLP ochranu a tá minimalizuje stratu dát.

Pre dáta v pokoji je nutné, aby boli na všetkých úložiskách, USB zariadeniach a na pevnom disku pracovnej stanice chránené pred nechceným čítaním napríklad šifrovaním.

Ďalšou kapitolou je ochrana webových aplikácií, kde sú uložené citlivé údaje ako e-maily, čísla platobných kariet, transakcie či rodné čísla.

Tu je nutné ošetriť ochranu dát už na programátorskej úrovni a penetračnými testmi. Iba samotné šifrovanie neposkytuje stopercentnú ochranu. Hacknutá aplikácia má totiž prístup k údajom, aj keď sú zašifrované.

Takéto varovanie platí aj pre cloud, kde pri používaní aplikácií software-as-a-service často vôbec netušíme, kto a na akej úrovni má prístup k našim dátam. Výrazne to zvyšuje riziko kyberútokov v dodávateľských reťazcoch a extorzie dát. Lebo aj keď nie ste priamo napadnutí vy, vaše údaje sú ohrozené. Stačí, že cieľom útoku bol váš dodávateľ alebo softvér, ktorý používate.

Tomáš Vobruba,
bezpečnostný špecialista Check Point Software Technologies