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.