HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 27. – 29. JÚNA 2025

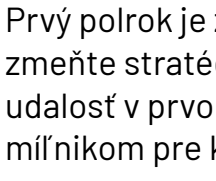
Tieto udalosti nás už navždy zmenili

ANKETA

Prvý polrok je za nami. Obzrite sa, rekapitulujte, zmeňte stratégiu, kým nebude neskoro. Ktorá udalosť v prvom polroku 2025 je významným míľnikom pre kybernetickú bezpečnosť?

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti,
Aliter Technologies

Začiatok roka bol na Slovensku doslova katasterfálny – o tom niet pochýb. V júni sme zasa boli svedkami úniku 16 miliárd hesiel Applu a Googlu. Čo však zatiaľ definuje rok 2025, je to, že sa rozprávame už o polovici roka! Tempo, respektíve rýchlosť, s akou prichádzajú nové trendy, rýchlosť, s akou je nutné reagovať na nové typy útokov či zmeny technológií na trhu, sú v tomto roku zatiaľ bezprecedentné. Zaspať na vavrínoch by mohlo znamenať začiatok konca. P. S.: Nie, v slove katasterfálny nie je preklep.



Jaroslav Oster,
predseda správnej rady,
Preventista.sk

Udalostí hodných zmienky bolo viacero. Z môjho pohľadu určite zásadne ovplyvňujúci vývoj bezpečnosti internetového sveta je 11. jún 2025. V ten deň sa v medzirezortnom pripomienkovom konaní objavil návrh na zmenu Trestného zákona zameraný na zneužívanie deepfake technológií na kriminálne aktivity. Dúfajme, že legislatívny proces nebude liknavý a skoro sa zaradíme medzi krajiny, kde použitie AI na podvody či vydieranie bude trestné.

Katarína Kročková,
odborníčka na ochranu osobných údajov,
Kročka & Partners

Za kľúčovú udalosť na Slovensku považujem útok na kataster, ktorý významne ovplyvnil chod verejnej správy. Táto udalosť spôsobila, že bežní občania si všimli dôležitosť ochrany osobných údajov a ich bezpečnosť. V tomto období som zaznamenala na sociálnych sieťach aj zvýšený počet „odborníkov" na zálohovanie a ransomvér.

Tomáš Hettych,
člen predstavenstva,
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Vďaka medializácii incidentov a útokov štatutári organizácií spozorneli a začali sa pýtať: „Ako je to u nás? Sme pripravení?" Záujem má bohužiaľ klesajúcu tendenciu. Konsolidácia štátneho rozpočtu tiež dramaticky ovplyvňuje možnosti a chuť štátnych inštitúcií investovať do kyberbezpečnosti.

Diana Legdanová,
riaditeľka divízie pre bezpečnosť,
Západoslovenská energetika

Vážim si kvalitu národnej kybernetickej súťaže CyberGame a vytrvalosť organizátorov. Potešilo ma, že tohtoročná víťazka v kategórii hráčka má len šestnásť rokov. V kategórii junior dostalo ocenenie prvýkrát dievčatko a má len trinásť rokov. Takže budúcnosť kybernetickej bezpečnosti na Slovensku vidím nádejne. Technológie, tie kúpime. Majme však čas a odvahu vychovať ľudí.

Richard Kiškováč,
generálny riaditeľ,
Elkan

Ransomvér útok na kataster považujem za kľúčovú udalosť tohto roka, ktorá mala potenciál vyvolať potrebné zmeny tak v prevencii, ako aj v reakcii. Z mojich skúseností viem, že určitá snaha o zlepšenie je prítomná, najmä na strane potenciálnych obetí. Otázne je, do akej miery bude úspešná. Koncepčné či strategické zmeny nenastali ani z pohľadu regulácie, ani v celkovom prístupe. Robiť tie isté veci a očakávať iný výsledok nie je cesta smerujúca k rozvoju, ale k stagnácii a následnej degradácii.

Tomáš Loveček,
prodekan pre vedu a výskum,
Fakulta bezpečnostného inžinierstva Žilinská univerzita

Prvý polrok bol v každom prípade bohatý na udalosti, ale na titulku by som dal kompetenčné centrá. Ako akademikovi mi nedá nespomenúť, že na šiestich slovenských univerzitách vznikajú kompetenčné centrá kybernetickej bezpečnosti, ktoré majú poskytovať podporu verejnej správe v tejto oblasti. V zmenách nezaostáva ani KCCKB. Obe udalosti nás napĺňajú očakávaním do druhého polčasu 2025.

Tomáš Zaťko,
CEO, etický hacker,
Citadelo

Rekordná lúpež 1,5 miliardy dolárov, keď severokórejskí hackeri vo februári okradli burzu ByBit. Analytici označujú útok za najväčšiu krádež v histórii kryptomien. Je to ďalšia z mnohých ukážok, že svet technológií a internetu je už dávno súčasťou svetového bojiska. Očakávam, že štátom sponzorovaných útokov bude čoraz viac na všetky svetové strany.

Július Selecký,
senior technický špecialista,
ESET

Globálne významnejšia než útok na kataster či transpozícia NIS2 bola správa, že USA plánovali zastaviť financovanie systému CVE – databázy pre jednotné označovanie softvérových zraniteľností. Firmy, výskumníci aj štáty by prišli o koordinovaný systém identifikácie zraniteľností, čo by sťažilo zdieľanie informácií a následnú reakciu. EÚ spúšťa vlastnú databázu EUVD s cieľom zvýšiť nezávislosť.

Jana Puškáčová,
vedúca špecialistka IT bezpečnosti,
Slovnaft

V júni 2025 sa na dark webe objavilo viac ako 16 miliárd prihlasovacích údajov – mená a heslá k účtom Apple, Google, Facebook, GitHub, ku cloudovým službám, k e-mailom a VPN. To sú dva účty na každého človeka na Zemi. Keď sa stratí dôvera v digitálnu identitu, prestáva fungovať online svet – od bankovníctva po štátne služby. Kyberbezpečnosť už nie je len technická disciplína. Stáva sa podmienkou stability spoločnosti.

Andrej Žucha,
generálny riaditeľ,
ALISON Slovakia

Panika po incidente na katastri sa skončila po dvoch týždňoch. Ak služby katastra fungujú, neznamená to, že príbeh mal šťastný koniec. To vôbec. Škody sa ešte stále počítajú. Dôležitejšie však je, či incident a jeho dosah zmenili prístup štátu a firiem ku kyberbezpečnosti. Ďalšiu skúšku našej kyberodolnosti by nemali robiť útočníci. Aký závažnejší cieľ by si vybrali? Sociálny alebo daňový systém? Zdravotníctvo?

Jaroslav Ušiak,
prodekan pre vedu a výskum,
Fakulta politických vied a medzinárodných vzťahov UMB Banská Bystrica

Dlhšie trvajúci kyberútok skupiny APT31 na české ministerstvo zahraničných vecí, ktorý 28. mája česká vláda pripísala Číne. Alebo vyhlásenie spojencov z 21. mája o ruskej kyberkampani proštátnej skupiny GRU APT28 na kritickú infraštruktúru krajín NATO a Ukrajiny. Obe ukazujú čoraz väčšiu kyberzranitelnosť nášho regiónu. Kyberdoména sa stala novým bojiskom svetových mocností. Ticho na Slovensku neznamená bezpečnosť, ale skôr nedostatok detekcie alebo zamlčiavanie.

Dominik Procházka,
riaditeľ odboru bezpečnosti,
Agel

Smernica EÚ NIS2, implementovaná na Slovensku novelou zákona o kybernetickej bezpečnosti, a rekordná krádež kryptomien. Ukázali, že ignorovať riziká, či už technické alebo legislatívne, sa v roku 2025 skutočne nevypláca. Treba konať a nečakať.

Benjamin Würfl,
obchodný zástupca,
Eviden Slovakia

Začiatkom roka Slovensko čelilo kybernetickému útoku na systém katastra nehnuteľností. Keďže ide o súčasť kritickej infraštruktúry štátu, incident poukázal na jej zraniteľnosť a na naliehavú potrebu lepšie chrániť informačné systémy štátu. V kontexte aktuálneho diania vo svete a pribúdajúcich geopolitických konfliktov vyvstáva otázka: Sme na podobné útoky dostatočne pripravení?

Ivan Kopáčik,
bezpečnostný expert, Gordias

Únik údajov z Bieleho domu prostredníctvom neoprávnenej osoby cez komunikačnú aplikáciu. Opäť sa potvrdila potreba dôsledného dodržiavania pravidiel kybernetickej bezpečnosti aj vo vrcholových štátnych inštitúciách, bez ohľadu na prostredie či pozíciu osoby.

Viktória Blažíčková,
vedúca oddelenia riadenia informačnej a kybernetickej bezpečnosti,
Národná diaľničná spoločnosť

Kybernetická bezpečnosť už nie je len technická téma. V prvej polovici roku 2025 priniesla Smernica NIS2 nové výzvy, no aj zodpovednosť. V doprave, kde ide o ľudské životy, sa digitálna ochrana stáva rovnocennou s fyzickou. A s nástupom AI hrozieb musíme byť nielen pripravení, ale aj predvídaví.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC,
Soitron

Za výnimočné v kyberbezpečnosti v 2025 považujem to, že sa čoraz častejšie dostávala do centra pozornosti celého Slovenska. Žiaľ, za vysokú cenu v podobe nefunkčných služieb či igelitiek s peniazmi vyhodených z balkóna. Zostáva len dúfať, že sa dá poučiť aj z chýb iných.

Tomáš Valenta,
riaditeľ,
Check Point Software Technologies na Slovensku

Všetkým sú známe udalosti na slovenskom katastri alebo vojnové konflikty, ale v prvom polroku 2025 došlo aj k netradičným kyberincidentom – AI phishing zasiahol aj skúsených expertov, z iránskej banky unikli údaje miliónov klientov, výskum odhalil, že pagery možno zneužiť na kyberfyzické útoky, a hack 4chanu ukázal, že anonymita na fórach nie je samozrejmosťou. Dôsledky sú globálne.

Ivan Makatura,
predseda,
Asociácia kybernetickej bezpečnosti

Legislatívne prostredie sa zásadne zmenilo: zákon o kybernetickej bezpečnosti, zákon o kritickej infraštruktúre, nariadenia DORA a CRA. Iránsky konflikt môže spôsobiť globálny „spillover" efekt – vďaka celosvetovej vzájomnej závislosti IT služieb útok na jeden systém ovplyvní mnohé ďalšie. Atribúcia, teda určenie zodpovednosti, bude pri takýchto incidentoch zložitejšia.

Ján Adamovský,
riaditeľ bezpečnosti,
Slovenská sporiteľňa

Za najvplyvnejšiu oblasť kybernetickej bezpečnosti v prvej polovici roku 2025 považujem rozvoj AI a jej využívanie podvodníkmi a hackermi. AI spôsobuje „demokratizáciu" podvodov a útokov, ktoré sa stávajú dostupnejšie pre ľudí s minimálnymi technickými znalosťami. Byť hackerom už nie je otázkou schopností, dobrým hackerom sa môže stať aj nespokojný klient.

Pavol Vrabec,
manažér kybernetickej bezpečnosti,
Univerzitná nemocnica Martin

Okrem legislatívnych zmien je zatiaľ udalosťou roka 2025 kybernetický útok na katastrálny úrad. Téma kyberbezpečnosti sa dostala na titulné stránky a medzi bežných ľudí, čo sa nestáva často. Z mojej skúsenosti incident priniesol manažérom kybernetickej bezpečnosti silné argumenty pri presadzovaní investícií a zmien. Ešte viac by pomohlo, keby boli príčiny incidentu transparentne vysvetlené.

Jaroslav Ďurovka,
riaditeľ,
Národné centrum kybernetickej bezpečnosti

Za jednu z významných udalostí na Slovensku v prvom polroku je možné považovať novelizáciu zákona o kybernetickej bezpečnosti. Novela nadobudla účinnosť 1. januára 2025 a predstavuje dôležitý krok k posilneniu kybernetickej bezpečnosti verejného aj súkromného sektora, ako aj k zvýšeniu celkovej odolnosti štátu voči kybernetickým hrozbám.

Lenka Gondová,
prezidentka, ISACA Slovensko

Roku 2025 dominujú tri legislatívne nástroje. Novelou kyberzákona sa slovenská legislatíva zladila s požiadavkami smernice NIS2. Nariadenie EÚ o kybernetickej odolnosti síce začne platiť s odstupom, no už dnes ovplyvňuje stratégie výrobcov digitálnych produktov a softvéru. Nariadenie o umelej inteligencii postupne zavádza účinné povinnosti. Táto trojica spoločne odzrkadľuje akútnu potrebu riešiť zásadné výzvy: prudký nástup digitálnych technológií, rozšírenie AI a exponenciálny nárast kybernetických hrozieb.

Robert Runčák,
technický riaditeľ,
Skupina Cyllium

Nadšenie alebo smútok z novej verzie služby Microsoft Active Directory 2025? Zraniteľnosť s označením BadSuccessor, opísaná výskumníkom Y. Gordonom zo spoločnosti Akamai, umožňuje útočníkovi s nízkymi oprávneniami získať prístup typu Domain Admin, a to zneužitím novej funkcie delegovaných MSA účtov. Kde sa stala chyba pri testovaní tejto novej funkcie už v takej rozšírenej službe Active Directory?

Róbert Mramúch,
manažér oddelenia bezpečnosti a krízového riadenia,
MH Teplárenský holding

Korporátna, respektíve integrovaná bezpečnosť je v roku 2025 nevyhnutnosťou aj v teplárenskej energetike. Kybernetický útok na SCADA systém môže mať rovnaké následky ako fyzická sabotáž. Aj preto sme prešli na jednotný model riadenia – bez rozdielu medzi kybernetickým a fyzickým svetom. Vidíme v ňom zmysel aj efekt.