8. ročník konferencie EPI Kybernetická bezpečnosť sa zameriava na strategické a multidisciplinárne témy, ktoré odrážajú zásadný posun v prístupe ku kybernetickej bezpečnosti, digitálnej dôvere a riadeniu technológií. Tento posun je prirodzene vyvolaný aj výrazným presadzovaním umelej inteligencie do reálnej praxe – nie ako experimentu, ale ako integrálnej súčasti podnikových procesov, rozhodovania a infraštruktúry.

V tomto kontexte sa kybernetická bezpečnosť stáva manažérskou témou a konferencia vytvára priestor pre pohľady, ktoré prepájajú technológie, bezpečnosť, reguláciu a rozhodovanie vedenia organizácií.

Hľadáme príspevky, ktoré prinášajú praktické skúsenosti, strategický nadhľad a konkrétne riešenia – od AI governance a podnikovej architektúry, cez agentické systémy a preemptívnu bezpečnosť, až po riadenie kybernetických a AI rizík na úrovni vedenia organizácií.

Konferencia EPI Kybernetická bezpečnosť sa aj v 8. ročníku vedome odlišuje od väčšiny odborných podujatí. Preto tento rok neuvádzame len hlavné tematické okruhy, ale aj konkrétne návrhy prezentačných tém ako inšpiráciu pre spíkrov a jasné vyjadrenie smerovania konferencie. Zámerne sa vyhýbame opakovaniu všeobecných a izolovaných diskusií o regulácii a právnych predpisoch. Buzzword “NIS2” na EPI konferencii nesmie zaznieť.

Posúvame sa do praktickej roviny každodenného fungovania prevádzkovateľov základných služieb a ich dodávateľov. Zároveň si zachovávame odbornú neutralitu a non-vendor princíp – prezentácie zamerané primárne na marketing produktov alebo služieb nebudú akceptované. Konferencia EPI Kybernetická bezpečnosť nie je priestorom na prezentácie postavené na opakovaní regulatorných buzzwordov (napr. „NIS2“) bez konkrétnej praktickej hodnoty pre prevádzkovateľov základných služieb a ich dodávateľov.

Hlavné tematické okruhy konferencie a oblasti, ku ktorým očakávame návrhy príspevkov:

Digitálna dôvera ako nový bezpečnostný perimeter

- Od detekcie a reakcie k predvídaniu a prevencii
- Bezpečnosť už vo fáze návrhu (alebo - čl. 25 GDPR v praxi)
- Preemptívna kyberbezpečnosť (uplatňovanie princípu “predict -deceive – disrupt”)
- Preukazovanie digitálneho pôvodu a integrity (SBOM, MLBOM, digitálne vodoznaky)
- Súlad ako konkurenčná výhoda, kybernetická bezpečnosť ako “go-to-market” argument
- Kybernetická odolnosť ako strategický prvok prevencie a kontinuity
- Digitálna dôvera v ére neľudských identít (API, služby, AI agenti)

Vzostup agentickej AI v podnikových procesoch

- AI ako infraštruktúra organizácie
- Prechod od „chatbotov“ k agentickým ekosystémom
- Riadenie umelej inteligencie (AI governance) ako téma pre štatutárne vedenie
- Riadenie zodpovednosti AI agentov, interoperabilita, sledovateľnosť a bezpečnosť
- AI-natívne vývojové platformy, „tiny teams“ a agentické vývojové prostredia
- Presun AI z digitálneho do fyzického sveta *(robotika, OT, IoT, digitálne dvojčatá)*
- Prepojenie IT – OT – AI v praxi
- Orchestrácia agentických systémov a multiagentových prostredí
- Bezpečnostné platformy s integrovanou umelou inteligenciou
- Použitie AI pre vyhľadávanie zraniteľností a SOC
- Viditeľnosť a dohľad nad AI riešeniami v celom ich životnom cykle

Komunikácia kyberbezpečnosti pre vlastníkov a vedenie organizácií

- Riadenie bezpečnosti tretích strán a dodávateľského reťazca
- Kybernetické riziká ako biznisové riziká
- Ako komunikovať kybernetickú bezpečnosť predstavenstvu a vlastníkom organizácie
- Storytelling, „škola hrou“ a simulačné prístupy v kybernetickej bezpečnosti
- Risk reporting zrozumiteľný pre biznis
- Metódy kvantifikácie dopadov kybernetických rizík jazykom biznisu
- Skúsenosti z incidentov a zlyhaní (čo nefungovalo a prečo)
- Rozhodovacie dilemy medzi bezpečnosťou, prevádzkou a rozpočtom

Kvantové počítače a postkvantová kryptografia – reálne riziká a praktická pripravenosť

- QC ako bezpečnostná hrozba – čo je reálne dnes a čo ešte nie
- Postkvantová kryptografia: stav štandardizácie a praktické dopady na organizácie
- Kedy a prečo sa začať pripravovať na postkvantovú kryptografiu
- Inventarizácia kryptografie v organizácii ako prvý krok ku kvantovej pripravenosti
- Kryptoagilita v praxi – ako navrhovať systémy pripravené na zmenu kryptografie
- Dopady postkvantovej kryptografie na existujúce IT a OT prostredia
- Riziko „harvest now, decrypt later“ a jeho význam pre dlhodobú ochranu dát
- Postkvantová kryptografia v regulovaných prostrediach a kritickej infraštruktúre
- Migrácia na postkvantové algoritmy – technické, prevádzkové a organizačné výzvy
- Postkvantová kryptografia z pohľadu riadenia rizík a investičných rozhodnutí

- Prečo výmena algoritmu nestačí: systémové dôsledky kvantovej zmeny
- Skúsenosti z pilotných nasadení postkvantovej kryptografie

Podniková architektúra a kyberodolnosť organizácií

- Plánovanie založené na schopnostiach (Capability-based planning) v praxi riadenia podnikov
- Riadiace mechanizmy digitálnej transformácie
- Podniková architektúra ako integračná vrstva biznisu, IT a regulácie
- Prepojenie umelej inteligencie, kybernetickej bezpečnosti a biznisu prostredníctvom informačnej architektúry

Bezpečnosť systémov priemyselnej automatizácie

- Kybernetická bezpečnosť OT systémov v reálnej prevádzke
- Kybernetické bezpečnostné incidenty v OT prostredí – príčiny, dopady a poučenia
- Riadenie kybernetických rizík v ICS/SCADA systémoch
- Kyberbezpečnostné špecifiká OT oproti IT
- Zavádzanie bezpečnostných opatrení v OT bez ohrozenia dostupnosti a bezpečnosti prevádzky
- Prepojenie OT bezpečnosti s riadením kybernetickej bezpečnosti organizácie
- Monitorovanie, detekcia a reakcia na incidenty v OT prostredí
- Bezpečnosť dodávateľského reťazca v OT – servisné prístupy, vzdialený prístup a zodpovednosť
- Audit a hodnotenie kybernetickej bezpečnosti OT systémov v praxi
- Dopady umelej inteligencie a autonómnych systémov na bezpečnosť OT prostredí