

Ako môžeme veriť systémom, ktoré sa samy učia?

Ked' rozhodujú stroje: Qubit Conference® Prague 2026 otvorí tému dôvery v ére umelej inteligencie

Dôvera v umelú inteligenciu (AI) nie je o tom, že systém je bezchybný, ale o tom, že rozumieme jeho limitom a vieme ho plne kontrolovať.

Bratislava, 11.5.2026

Umelá inteligencia, autonómne systémy, digitálna identita, dodávateľské reťazce, model nulovej dôvery, regulácia a zodpovednosť pri nasadzovaní nových technológií budú patriť medzi hlavné témy konferencie Qubit Conference® Prague 2026. Podujatie sa uskutoční 18. až 20. mája 2026 v OREA Hotel Pyramida v Prahe. Hlavnou témou konferencie bude The Trust Shift: Cybersecurity in the Age of Intelligent Autonomy (Posun dôvery: kybernetická bezpečnosť v ére inteligentnej autonómie). Bežní používatelia v súčasnosti dávajú AI agentom prístupy, ktoré boli doteraz vyhradené výlučne pre jadro operačného systému alebo špecializované bezpečnostné nástroje. Práve rastúca rola autonómnych systémov, AI a digitálna dôvera budú ústrednými témami prestížnej kyberbezpečnostnej udalosti Qubit Conference®, ktorá sa uskutoční tento mesiac v Prahe pod záštitou Národného úradu pro kybernetickú a informačnú bezpečnosť (NÚKIB).

Správanie umelej inteligencie nie je jednorazové ani izolované ako pri klasickom softvéri. Tieto systémy pracujú s pamäťou, reagujú v čase a môžu vykonať škodlivé akcie aj týždne po tom, čo uložia nebezpečný kontext. Podľa expertov sa prístup, kde funkcionálna víťazí nad bezpečnosťou, masívne presúva z uzavretých prostredí do verejnej infraštruktúry. Oficiálny program konferencie upozorňuje, že bezpečnosť sa mení v čase, keď umelá inteligencia preberá aktívnejšiu úlohu, autonómne systémy robia rozhodnutia a tradičné modely dôvery prestávajú stačiť. Tematické bloky sa budú venovať automatizovaným útokom, veľkým jazykovým modelom, autonómnej obrane, bezpečnej prevádzke bežných nástrojov umelej inteligencie, syntetickým identitám, deepfakom, cloudovej infraštruktúre, dodávateľským reťazcom, regulácii, digitálnej suverenity a zodpovednosti

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava

autonómnych systémov. „Kybernetická bezpečnosť dnes už nie je len o ochrane systémov pred útokmi zvonka. Organizácie musia riešiť aj to, aké oprávnenia dávajú umelej inteligencii, ako kontrolujú autonómne procesy a kto nesie zodpovednosť za rozhodnutia, ktoré technológie vykonávajú. Aj preto bude Qubit Conference® Prague 2026 o dôvere, o tom, ako ju budovať, overovať a nestratiť v prostredí, kde sa čoraz viac rozhodnutí presúva na algoritmy a autonómne systémy,“ informuje Mária Krahulecová spoluzakladateľka Qubit Conference®.

Hrozbou nie je len AI, ale kompromitovaná identita

Dnešné hrozby sa dynamicky menia. V priebehu posledných desiatich rokov sa pozornosť presunula z ochrany perimetra na prístup: predpokladaj narušenie a neustále overuj. Najväčší posun nie je v tom, aké hrozby existujú, ale v rýchlosti a rozsahu ich nasadzovania. Jednou z výrazných tém konferencie bude otázka, ako pristupovať k systémom umelej inteligencie, ktoré už nefungujú iba ako pasívne nástroje. Dôvera v umelú inteligenciu nemá znamenať slepé prijímanie jej výstupov, ale porozumenie limitom systému, kontrolu nad jeho oprávneniami a jasné pravidlá toho, čo môže v praxi vykonať. Používatelia môžu dávať agentom umelej inteligencie prístup k súborom, prihlasovacím údajom či komunikačným aplikáciám.

Dôležitou témou bude aj digitálna identita a odolnosť štátu. Podľa Josepha Carsona, bezpečnostného experta s viac ako 30-ročnou praxou a poradcu pre vlády, útočníci dnes systémy neprelamujú, ale jednoducho sa do nich prihlasujú pomocou platných údajov. Umelá inteligencia podľa neho akceleruje útoky prostredníctvom automatizácie a phishingu, no zároveň je kľúčová pre rýchlejšiu detekciu anomálií zo strany obrancov. Zásadný rozdiel oproti minulosti vidí Carson v tom, že organizácie už nemajú jasne vymedzený periméter. Kým pred desiatimi rokmi bola bezpečnosť postavená najmä na snahe udržať útočníkov mimo systému, dnes sú firmy cloudové, prepojené a závislé od digitálnych identít. „Posun nastal od prístupu ‚zistiť a zablokovať‘ k prístupu ‚predpokladať narušenie a neustále overovať‘. Útočníci sú rýchlejší, tichší a trpezlivejší. Najväčšou zmenou je, že samotná dôvera sa stala hlavnou zraniteľnosťou,“ konštatuje Carson. Kybernetické útoky pritom podľa neho neohrozujú iba dáta alebo jednotlivé organizácie. „Môžu narušiť celé ekonomiky. Bankovníctvo, logistiku, energetiku aj komunikáciu. Ich dosah nie je len finančný. Ovplyvňujú dôveru, stabilitu a národnú bezpečnosť,“ dodáva Carson.

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava

Akí rečníci s akými témami vystúpia na Qubit Conference® v Prahe?

Aktuálnym výzvam, reálnym hrozbám a budovaniu odolnosti sa bude venovať program konferencie, na ktorej okrem iných vystúpia poprední medzinárodní rečníci:

Dave Lewis (Global Advisory CISO, 1Password) vystúpi s témou Agentive Gremlins. Vo svojej prednáške sa zameria na autonómne AI systémy ako na nový nástroj útokov. Rozoberie riziká ako „prompt injection“, hrozby v dodávateľských reťazcoch a reálne incidenty týkajúce sa nekontrolovaných akcií či škodlivých rozšírení.

Joseph Carson (Chief Security Evangelist & Advisory CISO, Segura) vo svojej prednáške From Cyber War to Digital Trust priblíži reálny kybernetický útok na Estónsko a transformáciu prístupu štátu smerom k decentralizovanej digitálnej dôvere a národnej odolnosti, čo je strategický model aplikovateľný aj pre bežné firmy a kritickú infraštruktúru.

Nicol Daňková (Head of Security Operations Center, Henkel) prinesie praktické skúsenosti z vedenia globálneho SOC oddelenia s nepretržitým monitoringom (24/7). Podelí sa o poznatky z threat intelligence, digitálnej forenzej analýzy a zabezpečovania globálnych sietí s obrovským množstvom koncových zariadení.

Mackenzie Jackson z Aikido Security povedie školenie How to Secure AI Generated Code Using Open Source Tools (*Ako zabezpečiť kód vytvorený umelou inteligenciou pomocou otvorených nástrojov*),

Shyam Sundar R. zo spoločnosti Arctic Wolf Networks školenie How to analyze Android malware (*Ako analyzovať škodlivý softvér pre Android*).

Tamas Buzgo zo spoločnosti Sandoz školenie Practical OT Security Roadmap (*Praktický plán zabezpečenia prevádzkových technológií*).

Qubit Conference® Prague 2026 otvorí praktickú diskusiu o tom, ako sa mení kybernetická bezpečnosť v prostredí, kde organizácie čoraz viac využívajú umelú inteligenciu, automatizáciu a autonómne systémy. Témou nebude iba technológia samotná, ale aj dôvera, kontrola, identita, zodpovednosť a schopnosť štátov aj firiem fungovať v situácii, keď dôjde k narušeniu digitálnych služieb.

WEB

www.qubitconference.com

EMAIL

info@qubitconference.com

OFFICE

Qubit Conference®
Martinčekova 17
821 01 Bratislava