TLAČOVÁ SPRÁVA č. 07/2025
13. NOVEMBER 2025

Ako pracovať s umelou inteligenciou? Najohrozenejšie sektory so súčasne najväčším potenciálom sú bankovníctvo, zdravotníctvo, priemysel či školstvo

Umelá inteligencia dnes mení spôsob, akým fungujú firmy, inštitúcie aj vzdelávacie systémy. Prináša obrovské možnosti, no zároveň otvára otázky zodpovednosti, etiky a bezpečnosti. Práve o tom, ako tieto výzvy zvládnuť a ako sa na éru inteligentných technológií pripraviť v praxi, diskutovali odborníci počas piateho ročníka Qubit Conference® Slovakia 2025 v Jasnej.

Bratislava, 13.11.2025

Firmy, školy aj verejné inštitúcie musia na nástup umelej inteligencie reagovať nielen technicky, ale aj kultúrne s jasnými pravidlami, etickými štandardmi a investíciou do ľudí. „AI dokáže zefektívniť procesy, zvýšiť produktivitu a priniesť inovácie, no len za predpokladu, že jej používanie bude bezpečné a zodpovedné," zdôraznila Mária Krahulecová, spoluzakladateľka a organizátorka Qubit Conference®. Podľa nej sa ukazuje, že najlepšou ochranou pred rizikami umelej inteligencie je prevencia. Od interného školenia zamestnancov cez aktualizácie systémov až po jasné etické smernice.

Podľa odborníkov z Qubit Conference® 2025 patria medzi najohrozenejšie sektory tie, ktoré sú najviac závislé od dát a rutinných procesov – najmä bankovníctvo, zdravotníctvo, energetika, priemysel či školstvo. Práve v týchto oblastiach má však umelá inteligencia aj najväčší potenciál priniesť pokrok, ak sa bude používať rozumne, eticky a bezpečne. „Úspešné organizácie budúcnosti nebudú tie, ktoré sa umelej inteligencii vyhnú, ale tie, ktoré ju pochopia a naučia sa s ňou spolupracovať," dopĺňa M. Krahulecová.

TLAČOVÁ SPRÁVA č. 07/2025

13. NOVEMBER 2025

AI ako spojenec aj hrozba: Bezpečnosť sa stáva kľúčovým faktorom

S rastúcou digitalizáciou sa kybernetické útoky stávajú bežnou súčasťou reality najmä v odvetviach ako IT, telekomunikácie či priemysel. Firmy dnes fungujú v prostredí, ktoré je neustále vystavené pokusom o prienik, a rozdiel medzi úspešným útokom a včasnou obranou často spočíva len v schopnosti rýchlo ho odhaliť. Útočníci sa v systémoch pohybujú dlhšie, než zaútočia. Testujú ich slabé miesta, mapujú hodnotné dáta a pripravujú pôdu na presne cielený zásah. Preto je nevyhnutné zachytávať aj zdanlivo drobné anomálie, výpadky služieb, zmeny konfigurácií či nezvyčajné záznamy v logoch a vnímať ich ako možné varovné signály narušenia bezpečnosti.

Dôležitou súčasťou diskusií bola aj otázka, ako riadiť umelú inteligenciu v praxi. AI sa čoraz viac mení z nástroja na spolupracovníka, ktorý rozhoduje, odporúča a učí sa zo správania používateľov. S týmto posunom však prichádzajú nové výzvy. Umelá inteligencia má dve tváre. Môže byť obrancom, ktorý pomáha riešiť bezpečnostné incidenty, no zároveň aj útočníkom, ktorý dokáže vytvoriť presvedčivé phishingové e-maily či falošné obsahy. Jedným z najväčších rizík sú tzv. halucinácie, keď model generuje nepresné alebo neexistujúce informácie, a tie môžu mať v praxi závažné dôsledky. Rizikom je aj tzv. shadow AI. Používanie nástrojov umelej inteligencie mimo oficiálnych IT politík organizácie, bez vedomia a kontroly bezpečnostných tímov. Tieto systémy môžu spracúvať citlivé dáta bez adekvátnej ochrany a vystavujú firmy riziku úniku informácií či porušenia legislatívy. Preto je nevyhnutné, aby mali organizácie jasne nastavené pravidlá, kto má kontrolu nad dátami aj nad samotnými modelmi, a aby umelá inteligencia bola pevnou súčasťou bezpečnostnej architektúry, nie výnimkou z nej. Cieľom je, aby sa umelá inteligencia riadila rovnako prísne ako akákoľvek iná technológia a aby bola prepojená s celkovým rámcom kybernetickej a dátovej bezpečnosti.

Firmy musia zvládnuť umelú inteligenciu zodpovedne

Odborníci sa zhodli, že firmy by sa mali na nástup umelej inteligencie pripraviť komplexne. Od technických opatrení až po zmenu organizačnej kultúry. Základom je podľa Krahulecovej vzdelávať a školiť zamestnancov, pretože väčšina kybernetických incidentov vzniká z nevedomosti alebo podcenenia rizika. Firmy by mali zároveň zaviesť jasné pravidlá pre používanie AI, definovať, kde a ako sa technológia môže uplatniť. Napríklad pri práci s dátami či v komunikácii. Bezpečnostné opatrenia musia byť kontinuálne, od dvojfaktorovej autentifikácie až po nepretržité monitorovanie systémov. Rovnako dôležité je overovanie zdrojov a informácií, keďže generatívna AI dokáže vytvárať realistické, no falošné texty a videá. Napokon, úspešné organizácie by mali budovať etickú kultúru, v ktorej technológia podporuje ľudí, nie ich nahrádza, a rozhodovanie zostáva transparentné a zodpovedné.

TLAČOVÁ SPRÁVA č. 07/2025
13. NOVEMBER 2025

Štátny tajomník Štefánek: Štát pripravuje zriadenie národného regulačného sandboxu

Na konferencii vystúpil aj štátny tajomník Ministerstva investícií, regionálneho rozvoja a informatizácie SR Radoslav Štefánek, ktorý zodpovedá za informatizáciu a rozvoj umelej inteligencie. Pripomenul, že umelá inteligencia prestala byť laboratórnym experimentom už pred niekoľkými rokmi a stala sa infraštruktúrou nášho každodenného života. Od odporúčaní na obrazovkách až po rozhodnutia, ktoré ovplyvňujú zdravotníctvo, energetiku, dopravu či verejnú správu. Podľa neho máme všetky predpoklady na to, aby sa umelá inteligencia rozvíjala správnym smerom, od kvalitných univerzít a silnej energetiky až po skúsenosti v bezpečnostnom sektore. Zároveň však upozornil, že s obrovským potenciálom prichádza aj zodpovednosť a to znamená budovať umelú inteligenciu, ktorá je dôveryhodná. Taká vzniká z kvalitných dát, robustných modelov, transparentných procesov a zodpovedného riadenia rizík.

Nové ocenenie: Audítor kybernetickej bezpečnosti roka

Počas konferencie v Jasnej sa konalo aj vyhlásenie voľby Audítor kybernetickej bezpečnosti – ocenenie si prevzal Ján Drahoš. „Osvedčuje sa mi ľudský prístup, keďže každý pracuje v rôznych podmienkach a podmienky legislatívy nemusí byť vždy jednoduché splniť. Ľudský prístup, ale profesionálny výkon sú kľúčom dobrého audítora. Veľmi vážim ľudí, ktorí ma nominovali a vážim si aj rozhodnutie komisie, znamená to pre mňa zodpovednosť a záväzok dobre meno komunity šíriť aj do budúcnosti ďalej.“ Ocenenie Audítor kybernetickej bezpečnosti roka vzniklo ako pocta profesionálom, ktorí nielen dohliadajú na bezpečnosť organizácií, ale aj posúvajú komunitu dopredu – zdieľaním poznania, skúseností a dobrej praxe. „Chceme vyzdvihnúť ľudí, ktorí v kybernetickej bezpečnosti a audite spájajú odbornosť s otvorenosťou, inšpirujú ostatných, podporujú spoluprácu a pomáhajú zvyšovať úroveň povedomia o bezpečnosti na Slovensku,“ vysvetľuje M. Krahulecová, organizátorka podujatia.

Už teraz je známy termín medzinárodnej Qubit Conference® Prague 2026, 18.-20. máj 2026. Hlavnou témou konferencie bude Kyberbezpečnosť v ére inteligentnej autonómie, od ľudského úsudku k algoritmickej kontrole – môžeme ešte dôverovať? Bezpečnosť sa mení v reálnom čase. AI preberá riadenie, autonómne systémy rozhodujú a protokoly bežia bez človeka. Po rokoch budovania odolnosti prichádza nová výzva – dôvera v autonómiu. Dôvera v systémy, ktoré sa učia, nespia a ktorým nerozumieme. The Trust Shift je tiché zemetrasenie pod základmi kyberbezpečnosti. Manuálna kontrola ustupuje, staré modely dôvery padajú a musíme prehodnotiť všetko – od identity po právo rozhodovať. Presne o tom bude Qubit Conference® Prague 2026.

WEB
www.qubitconference.com

EMAIL
info@qubitconference.com

OFFICE
Qubit Conference®
Martinčekova 17
821 01 Bratislava