Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

QuantERA Call 2023: Chystá se mezinárodní výzva v oblasti kvantových technologií

V průběhu ledna roku 2023 bude vyhlášena výzva QuantERA Call 2023, která se zaměřuje na podporu výzkumu v oblasti kvantových technologií, a to konkrétně prostřednictvím témat *Quantum Phenomena and Resources* a *Applied Quantum Science*. Výzva cílící na podniky a výzkumné organizace je financována z Národního plánu obnovy. Bližší informace jsou k dispozici zde.

Identifikace výzkumných potřeb v Programu bezpečnostního výzkumu pro potřeby státu

Ministerstvo vnitra České republiky (MV ČR) vyhlásilo druhou identifikaci výzkumných potřeb v Programu bezpečnostního výzkumu pro potřeby státu 2022-2027 SecPro (SECurity PROcurement), během které mohou úřady a bezpečnostní sbory do 15. února 2023 specifikovat požadavky na znalosti a technologie. Bližší informace k procesu jsou k přečtení na webu MV ČR.

Vyhlášení výzvy k poskytnutí dotace pro Národní kofinancování Evropských center digitálních inovací (EDIHs)

Ministerstvo průmyslu a obchodu (MPO) zahájilo 23. prosince 2022 příjem žádostí o poskytnutí dotace, které by měly pomoci malým a středním podnikům v digitální transformaci. EDIHs mají v různých odbornostech poskytovat služby, které podpoří místní soukromý a veřejný sektor v digitální a ekologické transformaci na regionální úrovni. Z oblastí aktivit lze zmínit například umělou inteligenci, pokročilé digitální dovednosti a kyberbezpečnost. Bližší informace k výzvě, která se uzavírá 28. února 2023, jsou k dispozici zde.

Pracovní programy Horizontu Evropa na období 2023-2024 byly zveřejněny

Evropská komise (EK) zveřejnila podobu pracovních programů Horizontu Evropa pro období 2023-2024 s rozpočtem přibližně 13,5 miliardy EUR. V oblasti výzkumu a vývoje v kybernetické bezpečnosti jsou relevantní zejména programy Klastru 3 Civilní bezpečnost a společnost a Klastru 4 Digitalizace, průmysl a vesmír. Některé z výzev napříč klastry již byly na začátku prosince otevřeny, mimo jiné například v oblasti trustworthy and ethical AI. Bližší informace k otevřeným i chystaným výzvám jsou na stránkách F&T Opportunities Portal.

Spuštění veřejné konzultace o programech EU Horizont

EK spustila veřejnou konzultaci s cílem shromáždit vstupy od co nejširšího spektra zúčastněných stran včetně podniků, výzkumných a nevládních organizací i státní správy, které by měly sloužit při tvorbě strategického programu Horizont Evropa na období 2025–2027, k ex-post zhodnocení programu Horizont 2020 a průběžnému hodnocení programu Horizont Evropa. Veřejná konzultace je otevřena do 23. února 2023. Bližší informace jsou k přečtení zde.

Tipy na nadcházející akce

Technologické centrum Praha zveřejnilo harmonogram plánovaných akcí k programu Horizont Evropa, které se zaměřují na různé aspekty podávání žádostí o projekty, včetně přípravy projektů nebo pravidel financování.

Dále dne 14. února 2023 proběhne Konference České dny pro evropský výzkum (CZEDER), kdy prostor bude věnován například zhodnocení výsledků českého předsednictví v Radě EU v oblasti výzkumu, vývoje a inovací a prezentaci úspěšných projektů s českou účastí.

Výzkumníci otestovali novou metodu automatické detekce doxingu

(12. 12. 2022; sciencedaily.com) Výzkumníci z Penn State's College of Information Sciences and Technology přišli s novým automatizovaným způsobem detekce doxingu, který může účinněji ochránit uživatele sociálních sítí. Metoda má zajistit snazší a rychlejší identifikaci případů doxingu, kdy jsou zveřejňovány a dále sdíleny osobní informace s cílem dotyčné osoby zastrašit či pomluvit. Nový přístup, který byl otestován na Twitteru, používá techniky strojového učení a dosáhl přesnosti 96 %.

Komentář: Doxing představuje jednu z forem kyberšikany, kdy bývají veřejně sdíleny citlivé osobní informace, což může mít vážné dopady pro životy dotčených osob. Výzkum nových metod detekce doxingu je aktuální zejména s ohledem na narůstající oblíbenost sociálních sítí, které dovolují poškodit oběti v mnohem větším rozsahu.

EarSpy attack: útočníci dokáží za využití pohybových senzorů a reproduktorů odposlouchávat soukromé konverzace

(29. 12. 2022; hackread.com) Tým výzkumníků z amerických univerzit popsal tzv. EarSpy útok, který dovoluje odposlouchávat soukromé konverzace na některých Android zařízeních a zjistit tak následně například pohlaví či identitu volajícího. Výzkumníci byli schopni identifikovat pohlaví volajícího s až 93% přesností. Útok zneužívá pohybové senzory a kvalitní reproduktory uložené v chytrých telefonech, které dokáží detekovat jemné vibrace.

Komentář: Možnost odposlouchávání soukromých konverzací patří mezi příklady vážného narušení, které mohou mít závažné bezpečnostní dopady. Odborníci jako jeden ze způsobu snížení rizika špionáže navrhují, aby výrobci telefonů umisťovali senzory co nejdál od reproduktorů.

Oddělení vědy, výzkumu a inovací, NÚKIB