CYRIS Cyber Research and Inovations in Security

srpen/2025

NEWSLETTER

AKTUALITY VE VÝZKUMU A VÝVOJI V KYBERNETICKÉ BEZPEČNOSTI

Národní úřad pro kybernetickou a informační bezpečnost
NÚKIB

Staňte se členy národního výzkumného a inovačního ekosystému!

Benefity z členství v CYRIS:

Buďte v kontaktu

Komunikujte napřímo s dalšími členy národního ekosystému v oblasti výzkumu a vývoje v kybernetické bezpečnosti, předávejte si klíčové informace a hledejte partnery pro Vaše projekty!

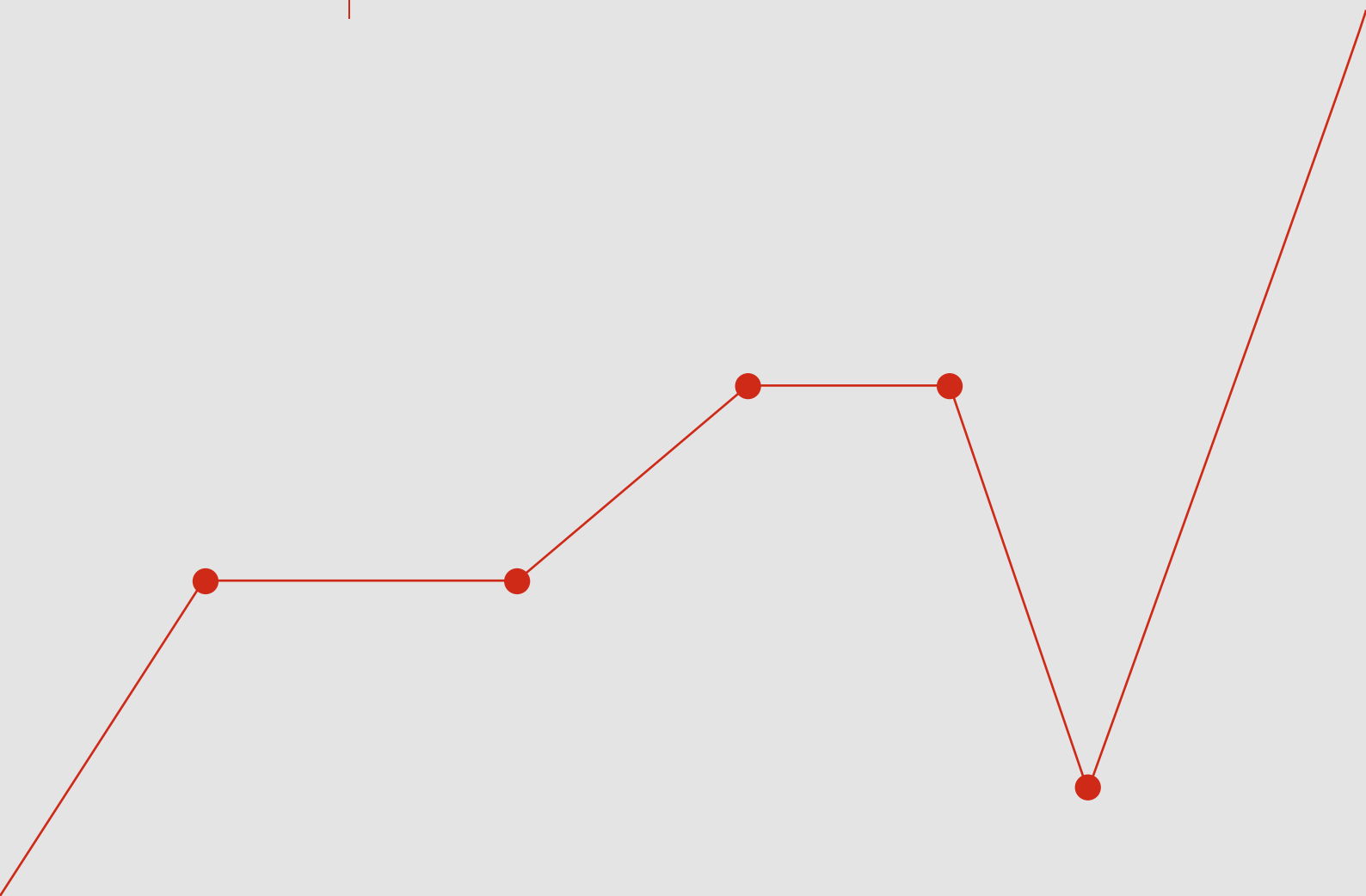
Přehled o aktuálním dění

Mějte přehled o tom, co se děje v oblasti výzkumu, vývoji a inovací v kybernetické bezpečnosti! Získejte tipy na zajímavé akce, publikace a zjistěte bližší informace o novinkách v oblasti podpory, aktuálních projektů a nových technologií.

Ovlivňujte budoucnost výzkumu

Získejte možnost udávat směr vývoje českému výzkumnému ekosystému v oblasti kybernetické bezpečnosti! Poskytujte vstupy a připomínkujte klíčové dokumenty na národní i evropské úrovni.

Aktuality, události a financování



Česko – švýcarská spolupráce v oblasti výzkumu

Ministerstvo školství, mládeže a tělovýchovy vyhlásilo výzvu k podávání žádostí o dotaci na podporu bilaterálních projektů mezi Českou republikou a Švýcarskem.

Cílem je posílit mezinárodní spolupráci ve výzkumu, vývoji a inovacích, zejména v oblasti výzkumných infrastruktur. Program podporuje mobilitu, vzdělávání, otevřený přístup k výzkumným kapacitám a transfer znalostí z praxe.

Výzva je určena konsorciím evropských výzkumných infrastruktur se sídlem v ČR, které spolupracují se švýcarskými partnery. **Projekty mohou být realizovány v letech 2025–2028. Celková alokace činí přes 295 milionů Kč a žadatelé mohou získat 100 % dotaci bez nutnosti spolufinancování.**

msmt.gov.cz

CzechInvest podpoří 40 startupů částkou 68 milionů korun

Agentura CzechInvest v rámci páté výzvy programu Technologická inkubace rozdělí 68 milionů korun mezi 40 inovativních startupů.

Program, jenž je součástí iniciativy The Country for the Furture, cílí nejen na finanční podporu začínajících firem, ale také na pomoc s jejich etablováním se na trhu a přípravou na vstup investorů.

Každý startup tak v rámci tzv. inkubačního balíčku získá kromě finanční podpory, také manažera, workshopy, odborné konzultace a napojení na klíčové aktéry ekosystému.

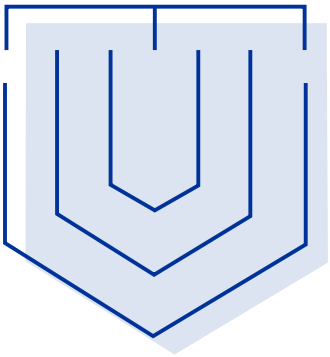
Startupy se mohly hlásit do oblastí jako AI, mobilita, ekologie, medicína, biotechnologie či pokročilé materiály. **CzechInvest zároveň plánuje další výzvy, které by měly být otevřeny ještě do konce letošního roku**. Program představuje důležitý nástroj pro rozvoj inovačního podnikání v ČR.

vedavyzkum.cz

CZECHINVEST

Pozvánka na první ročník konference k CRA v Bukurešti

Dne 8. října 2025 se v Bukurešti uskuteční první ročník konference CRA – Making the EU Market Resilient, zaměřené na nové požadavky na kybernetickou bezpečnost výrobků s digitálními prvky vyplývající z Aktu o kybernetické odolnosti (CRA).



Akci pořádá ENISA ve spolupráci s rumunským National Cyber Security Directorate (DNSC) a Evropským kompetenčním centrem (ECCC). Program a odkaz k registraci jsou k dispozici na webu ENISA.

Konference CRA se uskuteční jako navazující akce na **Bucharest Cybersecurity Conference** 2025 (6.–7. října), kterou pořádá DNSC. Pro účast je nutná samostatná registrace. Více informací na webu DNSC.

Aktuální partner search příležitosti:

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH
– DISKUS Polska Sp. z o.o. hledá partnery do konsorcia; expertíza: bezpečná likvidace dat, zabezpečení informací na konci životního cyklu. Kontakt: tomasz.filipow@diskus.pl

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH
– HUN-REN SZTAKI hledá v roli koordinátora partnery (nemocnice/poskytovatele péče a národní a regionální koordinátory) do konsorcia; téma: SOC pro zdravotnictví. Kontakt: erno.rigo@sztaki.hun-ren.hu

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH
– Paldata, S.A. hledá v pozici project/WP leader nebo participant partnery; téma: zajištění odolnosti a kybernetické bezpečnosti nemocnic. Kontakt: paulo.domingos@paldata.pt

HORIZON-CL3-2025-02-CS-ECCC-01 (Generative AI for Cybersecurity Applications)
– University of Maribor hledá možnosti zapojení do konsorcia jako partner; expertíza: kryptografie, správa digitálních identit, AI v kyberbezpečnosti. Kontakt: marko.holbl@um.si

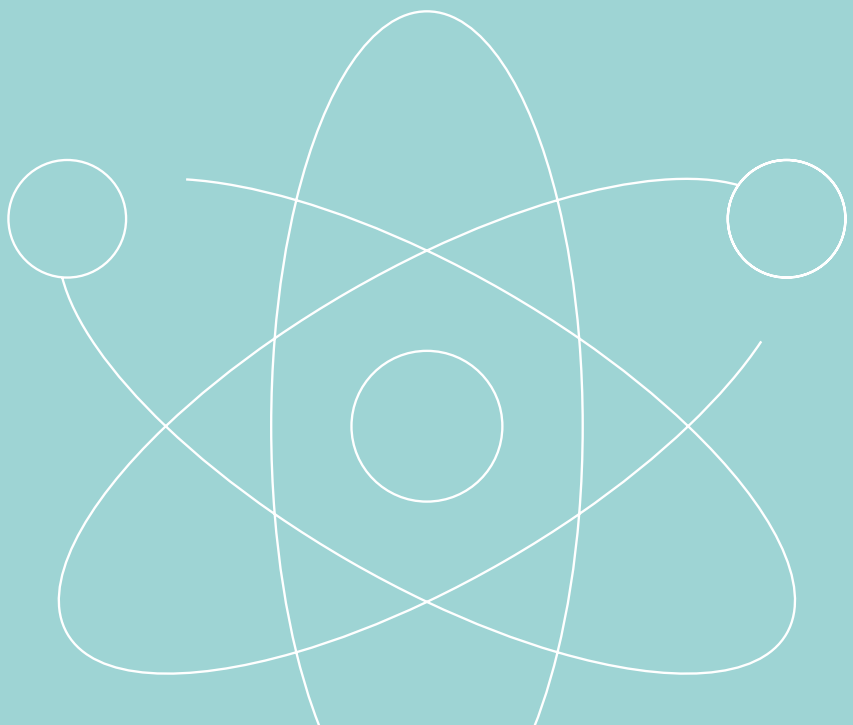
HORIZON-CL3-2025-02-CS-ECCC-05 (Security of implementations of PQC algorithms)
– Inha University hledá z pozice WP leader partnery do konsorcia; témata: návrh/optimalizace PQC algoritmů. Kontakt: jongpil@inha.ac.kr

Bližší informace k partnerským nabídkám naleznete na **webu NKC v sekci Aktuality**. Chcete sdílet svou nabídku? Pošlete info na **ncc@nukib.gov.cz** (výzva/program, role, expertíza, kontakt).

NCC-CZ CZECHIA CYBERSECURITY COORDINATION CENTRE
Spolufinancováno Evropskou unií
ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Podpořeno z programu Digitální Evropa v rámci projektu National Coordination Centre in the Czech Republic (č. 101127941). Názory a stanoviska uvedené vyjadřují pouze názory autora(ů) a nemusí nutně odrážet názory Evropské unie ani Evropského centra kompetencí pro kybernetickou bezpečnost. Evropská unie ani poskytovatel dotace nenesou za tyto názory odpovědnost.

Technologické novinky, objevy a zprávy



Nový výzkum propojuje kvantový výpočetní výkon s bezpečností kryptografických systémů

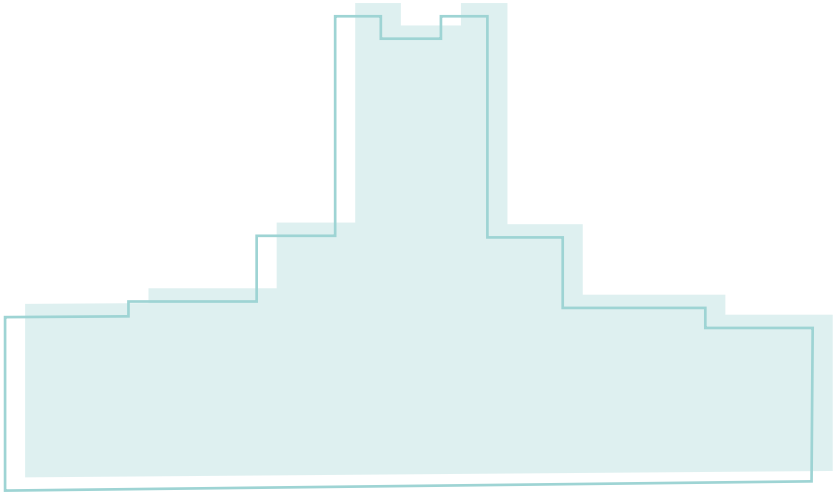
Nový výzkum z Kjótské univerzity, který byl prezentovaný na konferenci Annual ACM Symposium on Theory of Computing v Praze propojuje kvantové výpočty s bezpečností moderních kryptografických systémů.

Vědci se zaměřili na ověřovaní tzv. kvantové výhody skrze koncept **„inefficient verifier proofs of quantumness“**, což jsou interaktivní protokoly, u kterých ne-kvantový verifikátor (verifikátor nevyužívající kvantové výpočty) může ověřit, že partner používá kvantový počítač. **Tento přístup je zásadní pro budoucí testování kvantových zařízení v běžném prostředí a může výrazně usnadnit jejich širší nasazení**.

Klíčovým zjištěním je, že existence kvantové výhody závisí na existenci tzv. jednosměrných hlavolamů (one-way puzzle), jakožto základních stavebních prvků kryptografie. **Výzkum poprvé komplexně charakterizuje kvantovou výhodu a dokazuje, že pokud by neexistovala, mohla by být ohrožena bezpečnost většiny současných kryptografických systémů** včetně těch používaných v bankovnictví, komunikaci a státní správě, a to jak klasických, tak i post-kvantových.

Tento objev tak přímo sjednocuje oblast kvantových výpočtů a odolných kryptografických systémů. Zároveň otevírá cestu k dalšímu výzkumu, a to jak na úrovni teorie, tak i experimentálního ověřování. **Výsledky mohou mít dopad na návrh budoucích bezpečnostních protokolů, které budou vůči kvantovým útokům odolné a zároveň efektivní pro praktické použití.**

phys.org



Pentesty jednou ročně nestačí: Nastal čas pro ofenzivní SOC

Tradiční přístup k penetračnímu testování (autorizovanému simulovanému kybernetickému útoku na systém s cílem odhalit zranitelnosti a slabiny, které by mohl zneužít útočník se zlými úmysly) jednou ročně už neodpovídá realitě objemu dnešních kybernetických hrozeb. Techniky útočníků se vyvíjí neustále, proto je na místě otázka, zda současný přístup neinovovat.

Jedním z nabízených řešení je například **přechod od jednorázové obrany k trvalé ofenzivě a vybudovat Ofenzivní bezpečnostní operační centrum** (Offensive Security Operations Center).

Role ofenzivního SOCu spočívá ve vybudovaní interního týmu v rámci organizace, který každý den myslí a jedná jako útočník. Využívá nástroje jako Breach and Attack Simulation (BAS – automatizovaná simulace kybernetických útoků k testování a ověřování bezpečnostního stavu organizace) a automatizované penetrační testování, které simulují reálné útoky a odhalují slabiny dříve, než je někdo zneužije.

Cílem interního ofenzivního týmu v rámci organizace je **nepřetržitě odhalovat zranitelnosti skrze kontinuální simulaci útoků a řetězení exploitů**.

Současný přístup zaměření se na cyklické testování připravenosti organizace na obranu proti útokům, je ofenzivním SOC přístupem zásadně přehodnocen. Nejde už jen o snahu zabránit útočníkovi ve zneužití zranitelnosti, ale okamžitou identifikaci všech zranitelností a jejich co nejrychlejší mitigaci.

Organizacím může pro vybudovaní tohoto přístupu a převod jeho dopadů do měřitelných výsledků pomoci například platforma Picus Security. Aktuální data z této platformy ukazují, že **ofenzívní SOC může snížit výskyt kritických zranitelností o více než 50 % a zrychlit jejich mitigaci až o 81 %**. Ofenzivní SOC přitom nepředstavuje náhradu penetračních testů, ale jejich evoluci a cestu k neustálému zlepšování bezpečnosti.

thehackernews.com

Největší český dataset pro detekci hrozeb a predikci síťového provozu vznikl na FIT ČVUT

Výzkumný tým z Oddělení nástrojů pro administraci a bezpečnost sdružení CESNET a Fakulty informačních technologií ČVUT v Praze, zveřejnil doposud nejrozsáhlejší veřejně dostupnou datovou sadu pro výzkum kybernetické bezpečnosti.

Datová sada obsahuje přes 800 000 časových řad anonymizovaného síťového provozu z páteřních linek národní akademické sítě CESNET.

Primárním cílem přípravy veřejně dostupné datové sady je zlepšit schopnost odhalovat hrozby, jako jsou DDoS útoky či zneužití zařízení, které často unikají tradičním metodám. **Dataset umožňuje pokročilou detekci anomálií, predikci síťového provozu a testování modelů umělé inteligence v realistických podmínkách**. Data navíc umožňují testování algoritmů i v prostředí, kde je většina provozu šifrována, což výrazně zvyšuje jeho praktickou hodnotu.

Součástí projektu je i open-source knihovna CESNET TS-Zoo, která usnadňuje práci s daty a podporuje sdílení metodologie pro práci se sadou, a to prostřednictvím benchmarků. V kombinaci s realistickou datovou sadou jsou tak metody nejen transparentnější ale experimenty i rovněž lépe reprodukovatelné. V neposlední řadě je datovou sadu možné využívat pro testování nasazení AI v nástrojích pro zabezpečení síťového provozu.

fit.cvut.cz

Postkvantová kryptografie posiluje bezpečnost 5G sítí díky spolupráci Patero a Eridan

Společnost Patero specializující se na post kvantovou kryptografii a společnost Eridan zaměřená na technologie Open RAN (přístup k návrhu a nasazení síťové infrastruktury mobilních sítí, který rozděluje tradiční „uzavřené“ systémy na virtuální, softwarově definované a otevřeně propojené komponenty, pro jednoduší kombinaci hardwarových a softwarových komponentů od různých dodavatelů v standardizovaném prostředí) oznámily úspěšnou integraci poskvantové kryptografie (PQC) do technologie Open RAN pro 5G sítě.

Řešení spojuje generátor klíčových párů CryptoQoR od Patero s 5G rádiovými jednotkami Eridan, využívajícími energeticky efektivní modulaci (způsob řízení energie, který minimalizuje ztráty a maximalizuje užitečnou práci).

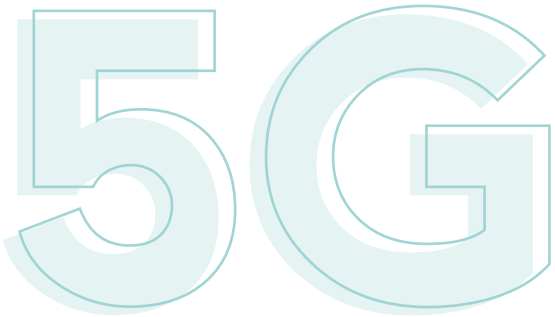
Spojením nízkoenergetických a výkonných rádií s kvantově odolným šifrováním vzniká **robustní řešení pro kritickou infrastrukturu**, které je energeticky účinné a škálovatelné.

Výsledek umožňuje chránit komunikaci v soukromých 5G sítích, proti budoucím kvantovým hrozbám, a to v různých prostředích od měst, přes letiště, univerzitní kampusy až po zemědělské podniky.

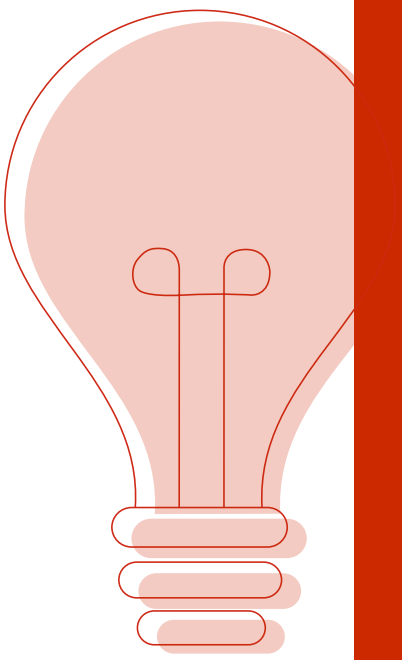
Technologie podporuje kryptografickou flexibilitu a odpovídá standardům NIST pro kvantově bezpečné algoritmy.

Partnerství mezi společnostmi má umožnit budování bezpečných, efektivních a odolných sítí pro kritickou infrastrukturu a přispět k širšímu přijetí kvantově bezpečné komunikace v praxi. Projekt je zároveň praktickou ukázkou toho, že kvantová bezpečnost se stává reálnou součástí moderních telekomunikačních řešení.

quantumcomputingreport.com



Tip na akci



Pozvánka k účasti na veletrhu it-sa Expo&Congress se vstupem zdarma

Ve dnech 7. – 9. října 2025 se v areálu norimberského výstaviště bude konat významný mezinárodní veletrh kybernetické bezpečnosti it-sa Expo&Congress. Veletrh představuje jednu z největších evropských akcí zaměřených na bezpečnost IT sektoru a nabízí komplexní přehled aktuálních informací, networkingových příležitostí a prostoru pro sdílení znalostí v oblasti ochrany dat a IT bezpečnosti. Součástí veletrhu bude také Český národní stánek, který naleznete v hale 7, číslo 7-418. Stánek bude poskytovat prostor pro propagaci českých řešení a účastníci jej mají možnost navštívit v průběhu celého trvání akce. Souhrnný online katalog vystavovatelů a jejich produktů naleznete zde a podrobné informace o veletrhu i doprovodnému programu jsou k dispozici na webu pořadatele. Permanentní vstupenku získáte zdarma po registraci e-kódu itsa25CZ na webové stránce pořadatele v sekci Visit. Vstupenka vám poslouží také jako jízdenka na MHD po celou dobu konání se veletrhu. V případě dotazů k veletrhu či registraci e-kódu se můžete obracet na zástupce veletržní společnosti NürnbergMesse v ČR na PROveletrhy s.r.o., info@proveletrhy.cz.

cyris.cz

Věděli jste, že

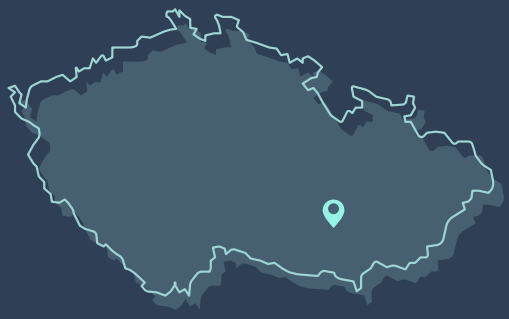
aliance Quantum-Safe 360 složena z firem Keyfactor, IBM Consulting, Thales a Quantinuum zveřejnila první společný dokument zaměřený na přechod k postkvantové kryptografii (PQC)? Bílá kniha s názvem „Digital Trust & Cybersecurity in the Era of Quantum Computing“ nabízí strategický plán pro podniky, jak se připravit na éru kvantových technologií. Strategie vyzdvihuje nutnost spolupráce, protože žádné jediné a samostatné řešení k úspěšnému přechodu nestačí. Klíčová témata zahrnují kryptografickou agilitu, zabezpečení interní podpory a rizika nečinnosti. Cílem aliance je nabídnout vzájemně kompatibilní řešení a jasné vedení pro organizace, které chtějí být připraveny na kvantovou budoucnost. Je důležité začít s přípravou co nejdříve, protože kvantové počítače mohou prolomit dnešní šifrování dříve, než se čeká.

horizontevropa.cz

Kontaktní informace

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31
616 00 Brno
Tel.: +420 541 110 777
P. O. BOX 17, Brno 16, CZ 616 00



Oddělení vědy, výzkumu a inovací

Olšanská 36/9
130 00 Praha
Tel.: +420 607 032 806
e-mail: vyzkum@nukib.gov.cz

Národní úřad pro kybernetickou a informační bezpečnost
NÚKIB

Naším cílem bylo poskytnout komunitě realistickou datovou sadu pro vývoj a testování algoritmů, které mohou chránit sítě i v době, kdy je většina provozu šifrována. Dataset otevírá cestu k lepší detekci neznámých hrozeb, protože vychází z reálného a komplexního prostředí. Díky tomu jsou výsledky z této datové sady věrohodnější než na existujících datových sadách. Věříme, že přispěje k vývoji bezpečnější a inteligentnější infrastruktury nejen v akademické sféře

Ing. Josef Koumar,
hlavní autor největší české otevřené datové sady