CYRIS Cyber Research and Inovations in Security

listopad/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!

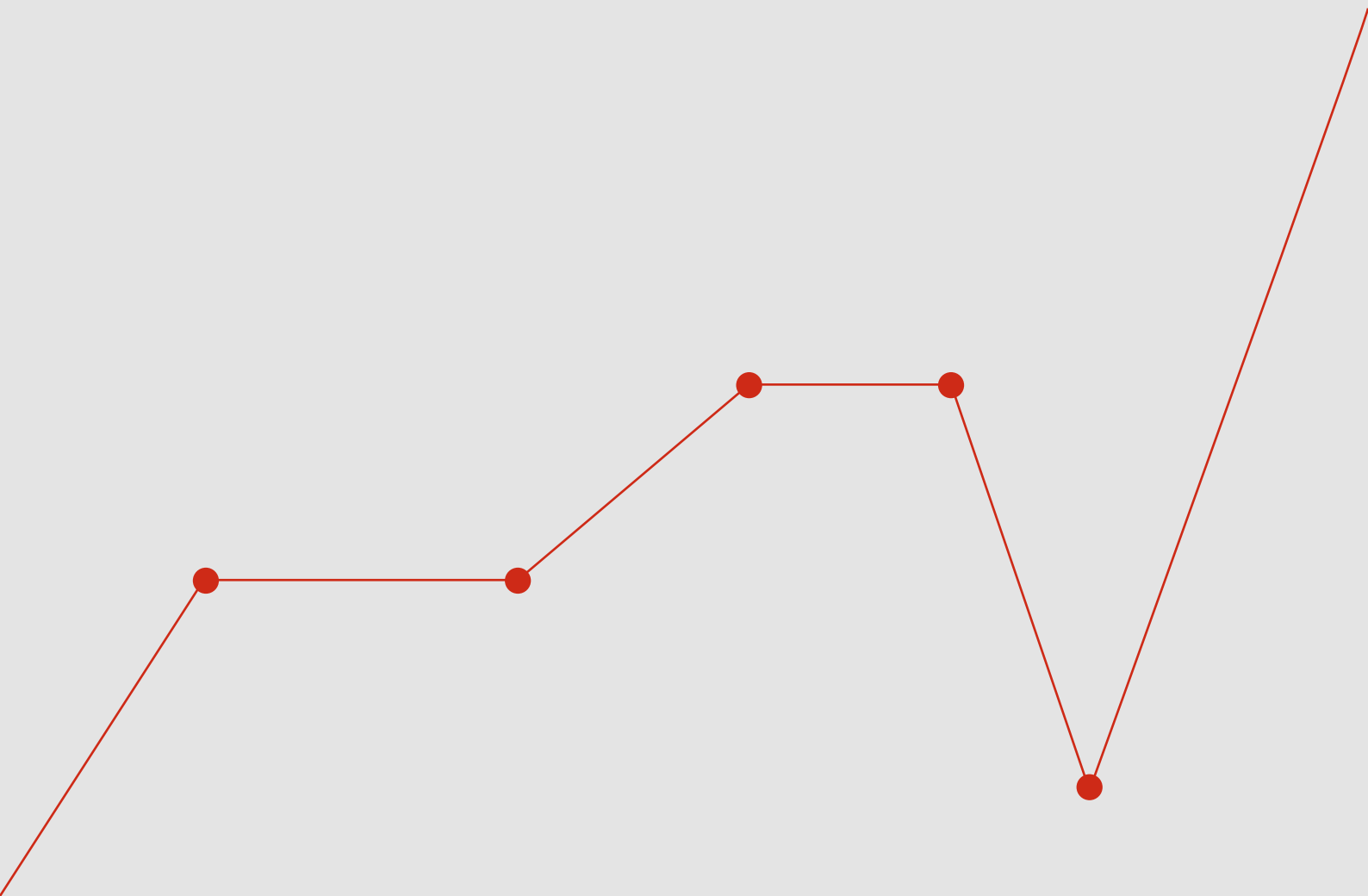
Přehled o aktuálním dění

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



Onsemi dostává zelenou na velkou investici do čipů v Rožnově

Americká **firma Onsemi získala souhlas Evropské komise na rozšíření výroby čipů v Rožnově pod Radhoštěm**. Česko tak může firmě poskytnout státní pobídku ve výši 11 miliard Kč, zatímco **celková investice dosáhne až 42 mld Kč**.

Investice usilují o zavedení komplexního řetězce výroby čipů na bázi karbidu křemíku (SiC), který je klíčový pro elektromobily, datová centra s AI i obnovitelné zdroje.

Projekt byl Evropskou komisí schválen navzdory lobby německých a italských konkurenčních firem jako prospěšný pro strategickou polovodičovou autonomii. Spuštění komerčního provozu se očekává v průběhu roku 2027.

lupa.cz

onsemi™

Nové příležitosti financování z EU

Evropská unie vyhlásila **druhé kolo výzvy Fortissimo Plus** pro malé a střední podniky, které chtějí rozvíjet **inovativní projekty v generativní AI a HPC**.

Podpora, o kterou se lze hlásit od 3. prosince 2025 do 25. února 2026, může pokrýt až 100 % nákladů za celkového rozpočtu **4 miliony eur**.

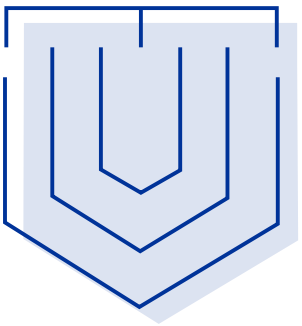
V **nové výzvě programu Digitální Evropa** je možné získat **až 10 milionů eur** při 50% spolufinancování na **konsolidaci evropské sítě digitálních inovačních hubů s důrazem na AI a integraci do evropského AI ekosystému**. Výzva je otevřená EDIH, neziskovým organizacím, výzkumným institucím, univerzitám i malým a středním podnikům.

1. ec.europa.eu

2. ec.europa.eu

Zahájení registrace do Komunity a výzva k přihlášení do Strategické poradní skupiny

NÚKIB jako NKC zahájil registraci členů do **evropské Komunity kompetencí pro kybernetickou bezpečnost** dle Nařízení EU 2021/887 a nového zákona č. 264/2025 Sb., o kybernetické bezpečnosti.



Žádost lze podat elektronicky na Portálu NÚKIB. NKC provádí posouzení základní a zvláštní způsobilosti žadatelů o členství, kteří mají sídlo na území ČR. Bližší informace jsou k dispozici na webu NKC.

Současně Evropské kompetenční centrum (ECCC) otevřelo výzvu pro členství ve **Strategické poradní skupině (SAG)**, která bude poskytovat strategické poradenství výkonnému řediteli ohledně agendy, ročního i víceletého pracovního programu. Podmínkou je členství instituce ve výše zmíněné Komunitě. Uzávěrka přihlášek je **30. 12. 2025** (23:59 EET). Přihlášky se podávají online přes EU Survey a musí obsahovat formulář, Europass CV a motivační dopis. Více informací naleznete na webu ECCC.

Nová výzva DEPLOY-CYBER-09 a aktualizace WP DEP Kyberbezpečnost

Evropské kompetenční centrum (ECCC) otevřelo novou výzvu **DIGITAL-ECCC-2025-DEPLOY-CYBER-09** v rámci programu Digitální Evropa část Kyberbezpečnost. Termín pro podání projektových návrhů je **31. března 2026 (17:00 CET)**. Celkový rozpočet činí 50 mil. EUR a zahrnuje témata:

CYBER-09-CYBERAI – Cybersecure tools, technologies and services relying on AI

CYBER-09-UPTAKE – Uptake of innovative cybersecurity solutions for SMEs

CYBER-09-COORDPREP – Coordinated preparedness testing and other preparedness actions –

CYBER-09-CABLEHUBS – Regional Cable Hubs

Podrobnosti naleznete v tzv. **call dokumentu**.

Současně ECCC schválilo **aktualizaci pracovního programu DEP Kyberbezpečnost 2025–2027**. Nově zahrnuje strategickou iniciativu **AI Gigafactories** a podporu bezpečnosti podmořských kabelů prostřednictvím **Regional Cable Hubs**. Aktualizovaný dokument je dostupný na webu ECCC.

V případě dotazů se na nás neváhejte obrátit na ncc@nukib.gov.cz.

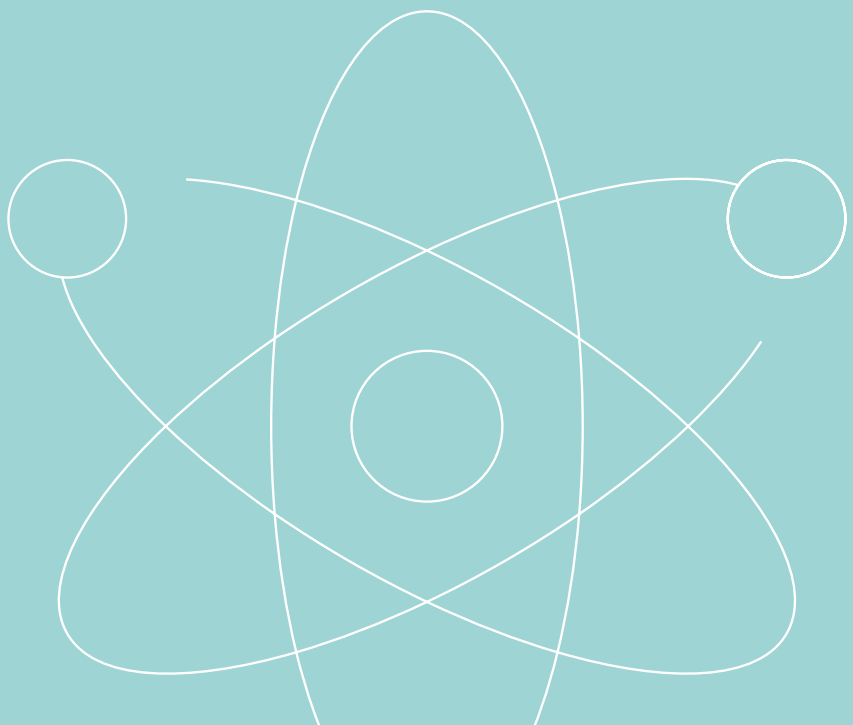
NCC-CZ
CZECHIA CYBERSECURITY COORDINATION CENTRE

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



Průlom v kvantových nanodiamantech: tisícinásobné zrychlení výroby

Mezinárodní tým vědců vedený Petrem Cíglerem z Ústavu organické chemie a biochemie AV ČR vyvinul revoluční metodu PTQ (Pressure and Temperature Qubits), která vytváří svítící kvantová centra v nanodiamantech během pouhých čtyř minut. **Za týden tak lze vyrobit tolik materiálu, kolik by běžným způsobem trvalo čtyřicet let**.

Takto produkované nanodiamanty mají navíc lepší optické a kvantové vlastnosti. Proces tvorby napodobuje podmínky zemského pláště, kdy se diamantový prášek lisuje pod extrémním tlakem a teplotou. V diamantech následně vzniknou fluorescenční NV centra (nitrogen vacancy center), tedy atom dusíku vedle prázdného místa v diamantové mřížce, v němž chybí atom uhlíku.

Vzniklé nanodiamanty jsou menší než virus a jsou schopné měřit magnetická pole, náboj i teplotu v buňkách. Díky NV centrům navíc detekují jednotlivé molekuly jako **supersenzor**.

Celkově se týmu podařilo zrychlit výrobní tempo tisícinásobně, což umožňuje během týdne vyprodukovat několik kilogramů nanodiamantů. Tento průlomový objev otevírá dveře rozvoji nových technologií v oblasti lékařství, kryptografie či bezpečnostních senzorech.

vedavyzkum.cz

PTQ

Česká AI urychluje kyberbezpečnost

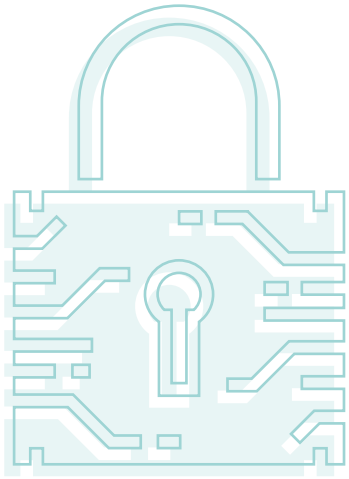
Český kyberprostor zažívá rozmach AI nástrojů poskytujících řešení pro pomalou obranu proti útokům. V dosavadním kyberbezpečnostním prostředí se jednalo o klíčový problém a platilo, že útočníci zneužívají známé zranitelnosti dříve, než firmy stihnou reagovat. **Využívání AI systémů však redukuje bezpečnostní odpověď až na minuty**, což přináší zásadní pozitivní změnu.

Příkladem je startup Aisle, jehož AI vytváří živý model firemního softwaru, identifikuje skryté chyby neviditelné pro experty a navrhuje opravy po schválení člověkem. Podle zakladatele startupu Ondřeje Vlčka má být obrana alespoň stejně tak rychlá, jako útok, čehož AI dosahuje díky **autonomní detekci zranitelností a zajištěním oprav** prostřednictvím analýzy kódu v reálném čase.

Prevence v podobě začlenění AI do kybernetické obrany je klíčová především k ochraně softwaru před exploatacemi, které způsobují až dvě třetiny kybernetických incidentů.

Česká republika zapojováním inovativní AI nahrazuje manuální zdlouhavější procesy, přispívá k resilienci globálních kyberbezpečnostních ekosystémů a posiluje strategickou suverenitu. Aisle je přitom důležitým a inspirativním článkem, který ukazuje, že efektivní obrana může předčit samotný útok.

wired.cz



Smishing Simulation: nová tréninková platforma

Francouzská kyberbezpečnostní firma Arsen představila **nový modul Smishing Simulation, který umožňuje firmám testovat a zlepšovat odolnost svých zaměstnanců proti pokročilému sociálnímu inženýrství**. Jeho inovativní nástroje přináší spolehlivý prostor pro posilování obrany před čím dál sofistikovanějšími podvody v digitální rovině.

Po vyvinutí bezpečného a úspěšného tréninkového prostředí pro phishingové a vishingové situace se společnost Arsen zaměřila na problém smishingu, tedy nebezpečných SMS zpráv lákající osobní citlivé údaje. V současnosti patří mezi nejrychleji rostoucí hrozby a týká se firemních i soukromých mobilních zařízení.

Modul navazuje na teoretickou průpravu **praktickými simulacemi smishingových scénářů ve velkém měřítku**. Firmy si tedy mohou kalibrovat situace „na míru“ svým zaměstnancům, sledovat reakce jednotlivých skupin v čase, kontrolovat jejich průběh i trénovat realistické scénáře v bezpečném prostředí.

Mezi funkce patří využívání AI pro autentické textové zprávy, nastavitelné domény, zkracovače odkazů a integrovaná firewallová ochrana cílových webových stránek.

Otestovaný modul je dostupný všem zákazníkům od října 2025 samostatně či v rámci obranného balíčku.

hackread.com

Fortinet spustil Secure AI Data Center

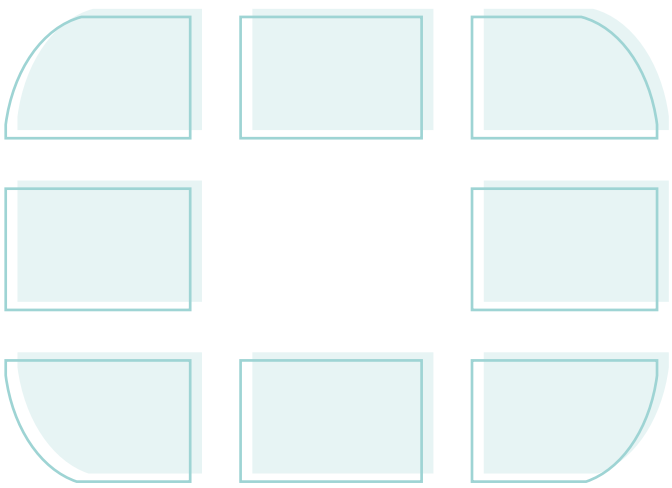
Americká firma Fortinet uvedla Secure AI Data Center, první komplexní řešení pro ochranu AI struktur. Zabezpečuje celý AI stack od datových center a GPU clusterů až po velké jazykové modely (LLM). Obsahuje síťové segmentace pro ochranu modelů a dat proti únikům, prompt injections či exploitům.

Jádrem je nový firewall FortiGate 3800G s ASIC čipy NP7 a SP5. Podporuje 400 GbE konektivitu, propustnost až 800 Gbps a zvládá 200 milionů souběžných sessions. Navíc oproti tradičním řešením snižuje spotřebuenergie o 69 % a zajišťuje ultra-nízkou latenci pro náročné AI úlohy.

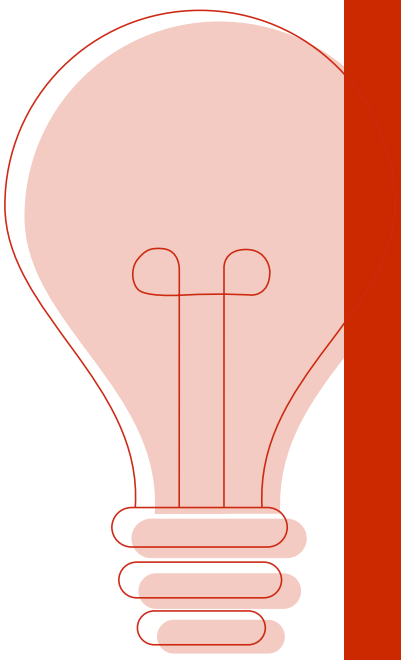
Zahrnuje kvantově bezpečné technologie (post-quantum cryptography – PQC, quantum key distribution – QKD) proti budoucím hrozbám, brání únikům dat i škodlivým vstupům, data poisoningu a exploitům LLM. Současně je plně v souladu s požadavky evropské legislativy v rámci Aktu o umělé inteligenci (AI Act).

Řešení Secure AI Data Center tak nabízí výkonné, a přitom energeticky úsporné a efektivní škálování umělé inteligence s bezpečnostním monitoringem.

finance.yahoo.com



Tip na akci



Interaktivní výstava Věda ve veřejném zájmu

CzechInvest otevírá sedmou výzvu programu Technologická inkubace (TISUP-2502) pro startupy s celkovou alokací **100 milionů Kč** na podporu minimálně 20 inovativních projektů. Přihlášky lze podávat výhradně přes AIS **od 24. listopadu 2025 do 9. ledna 2026**. Nabízen je režim Inkubace PLUS s finanční podporou až 4,5 milionu Kč bez ztráty podílu ve firmě, inkubaci v délce 18–24 měsíců a nepřímou podporu (workshopy, pitchy, konzultace) v hodnotě 500 000 Kč. Cílové oblasti zahrnují AI, pokročilé materiály, mobilitu, kreativní průmysly, ekologii, medicínu a bezpečnostní technologie. Podmínkou je ukončení projektů do 31.12. 2028.

vedavyzkum.cz

Věděli jste, že

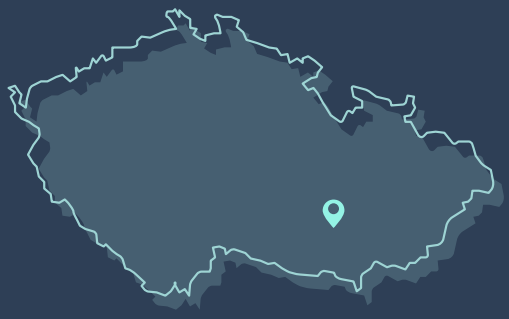
Proton spustil Data Breach Observatory, první veřejnou platformu pro sledování úniků dat z dark webu v reálném čase. V roce 2025 ověřili 794 identifikovatelných breachů s více než 300 miliony záznamů, kde přibližně 70 % cílů tvořily malé a střední firmy. Mezi nejvíce napadané sektory přitom patří maloobchod (25 %), technologie (15%) a média (11%).

engadget.com

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

Díky novému postupu můžou laboratoře i firmy na celém světě získat velké množství velmi kvalitních nanodiamantů s NV centry, což otevírá dveře novým technologiím. Od precizních senzorů pro lékařskou diagnostiku až po lokální detektory molekul využívající například principy magnetické rezonance.

Petr Cígler z Ústavu organické chemie a biochemie AV ČR o nové metodě výroby nanodiamantů.