CYRIS Cyber Research and Inovations in Security

duben/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

5

Finsko a Španělsko představily národní strategie pro rozvoj kvantových technologií

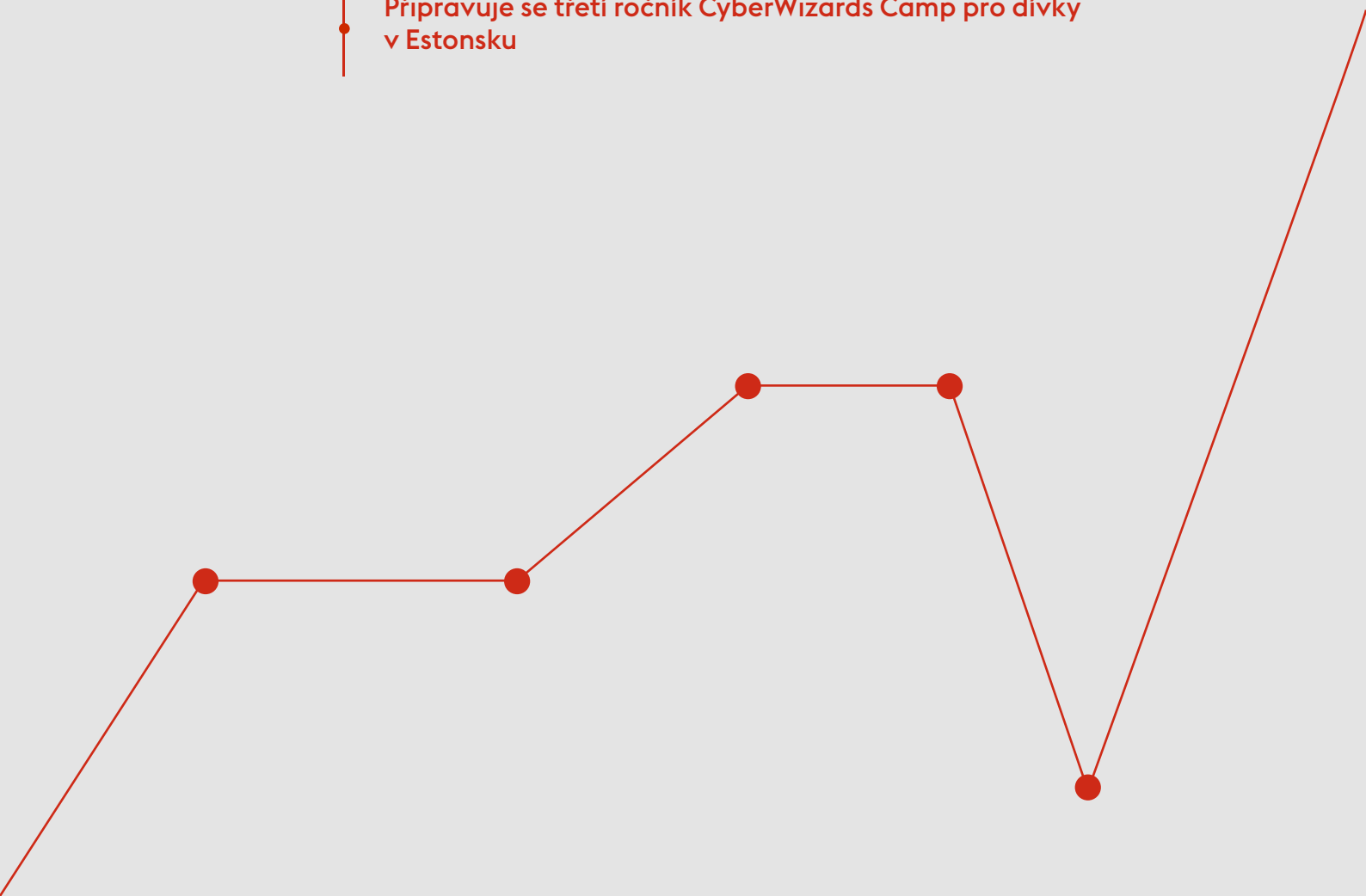
6

Britští výzkumníci získávají širší přístup k financování kvantových a vesmírných projektů v rámci programu Horizon Europe

7

Zástupci sítě NKC a správní rady Evropského kompetenčního centra se setkali ve Varšavě

Připravuje se třetí ročník CyberWizards Camp pro dívky v Estonsku



Finsko a Španělsko představily národní strategie pro rozvoj kvantových technologií

Finsko a Španělsko nedávno zveřejnily své národní strategie zaměřené na posílení postavení v oblasti kvantových technologií.

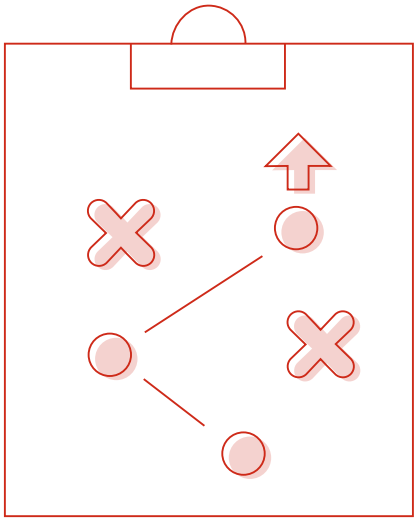
Finská strategie (2025–2035) **obsahuje osm klíčových opatření, která mají za cíl vytvořit světově vedoucí prostředí pro kvantové výpočty, rozvíjet infrastrukturu podporující vývoj kvantových zařízení a posilovat dovednosti a kompetence v této oblasti.**

Dále se zaměřuje na dlouhodobý program výzkumu a vývoje, financování růstu firem na globálním trhu a mezinárodní spolupráci.

Španělská strategie (2025–2030) zahrnuje investici přes 800 milionů eur s cílem posílit výzkumný ekosystém, stimulovat průmyslové využití a připravit společnost na transformaci srovnatelnou s digitální revolucí. Strategie se zaměřuje na **tři hlavní oblasti: kvantové výpočty, komunikaci a senzory**.

Obě strategie reflektují rostoucí význam kvantových technologií a snahu předních evropských zemí o stabilizaci své pozice v této klíčové oblasti.

1. thequantuminsider.com
2. thequantuminsider.com



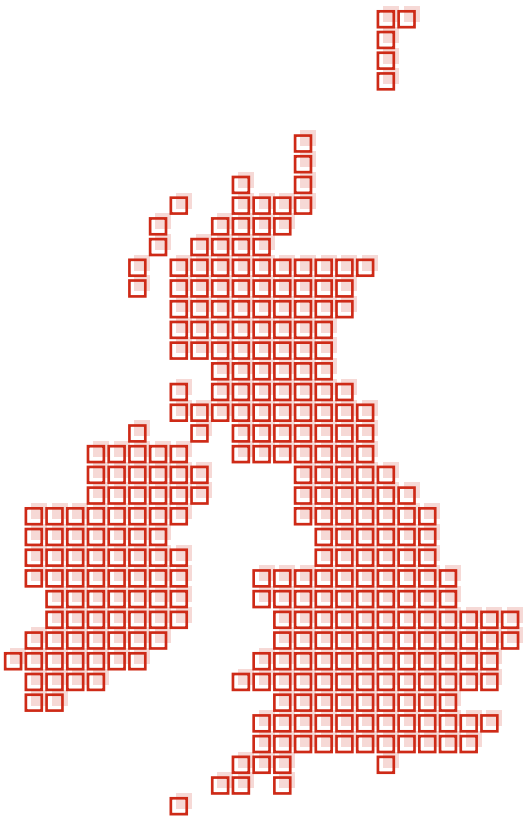
Britští výzkumníci získávají širší přístup k financování kvantových a vesmírných projektů v rámci programu Horizon Europe

Spojené království rozšiřuje své zapojení do programu Horizon Europe, s cílem posílit výzkum v oblasti kvantových technologií a vesmíru. Tento krok přichází po zveřejnění pracovního programu Horizon Europe pro rok 2025, který otevírá nové možnosti financování pro britské vědce a podniky.

Rozšířený přístup k financování v rámci programu Horizon Europe umožní britským výzkumníkům a podnikům posílit mezinárodní spolupráci a podpořit ekonomický růst prostřednictvím inovací v klíčových technologických oblastech.

Tento krok je součástí širší strategie Spojeného království zaměřené na posílení jeho postavení jako vědecké a technologické velmoci.

www.gov.uk

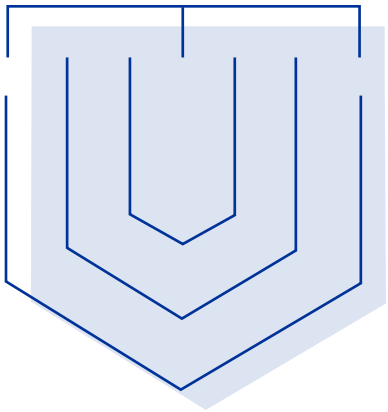


Zástupci sítě NKC a správní rady Evropského kompetenčního centra se setkali ve Varšavě

Ve dnech 7.–9. 4. 2025 se ve Varšavě konalo setkání zástupců sítě NKC a členů správní rady Evropského kompetenčního centra (ECCC).

V rámci jednání **byly diskutovány přístupy členských států ve věci budování NKC a sdíleny zkušenosti s poskytováním finanční podpory třetím stranám (FSTP).**

Součástí bylo také společné zasedání správní rady ECCC s řídící radou ENISA, kdy byla diskutována spolupráce v různých oblastech a koordinace při implementaci EU legislativy. Došlo ke znovuzvolení předsedy a místopředsedkyně správní rady ECCC a byly diskutovány chystané výzvy v rámci pracovního programu Digitální Evropa část Kyberbezpečnost na roky 2025–2027. Oficiální tisková zpráva je k přečtení zde.



Připravuje se třetí ročník CyberWizards Camp pro dívky v Estonsku

V termínu 11.–16. 8. 2025 proběhne v Estonsku již třetí ročník CyberWizards kempu, který je určen pro dívky ve věku 13–16 let se zájmem o oblast kybernetické bezpečnosti.

Uzávěrka přihlášek pro týmy je stanovena do začátku června 2025, při naplnění kapacit dříve. Bližší informace jsou k dispozici na webu, kontaktní osobou je Tiina Pau (tiina.pau@ria.ee).

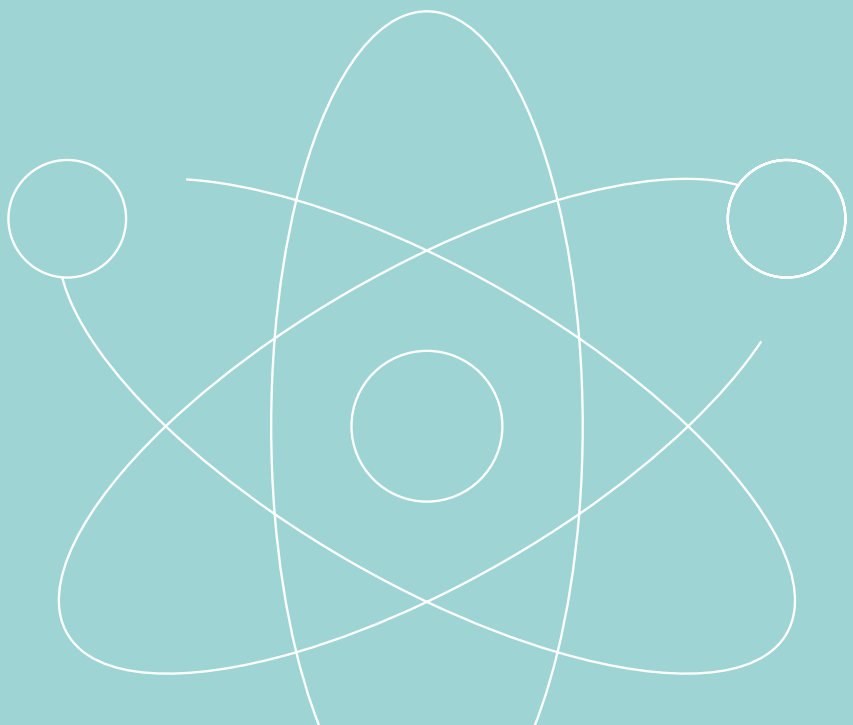
NCC-CZ
CZECHIA CYBERSECURITY COORDINATION CENTRE

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



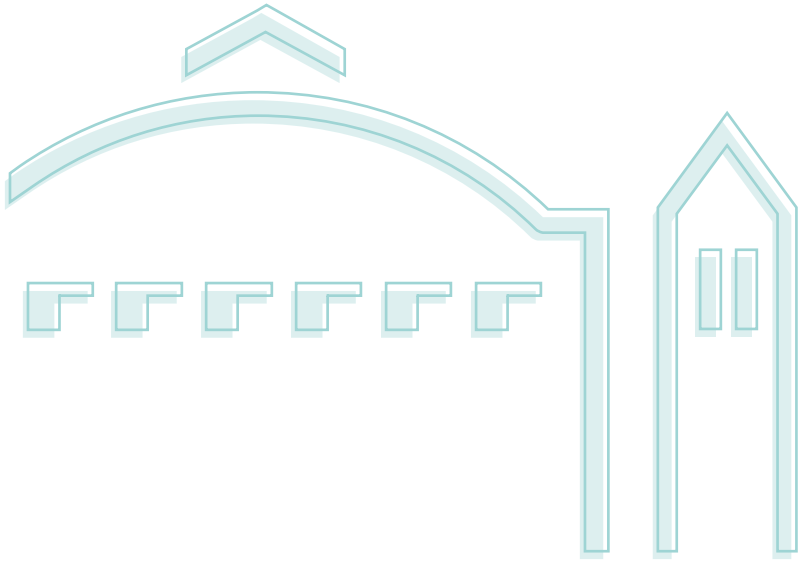
Zvýšená odolnost supravodivých qubitů vůči šumu je důležitým milníkem pro škálovatelnost kvantových počítačů

Vědci z Lawrence Berkeley National Laboratory **představili inovativní výrobní metodu**, která výrazně zlepšuje odolnost supravodivých qubitů vůči šumu. Tato technika spočívá v zavěšení superinduktoru nad křemíkový substrát, čímž se snižuje šum způsobený materiálovými nedokonalostmi. Výsledkem je **zvýšení indukčnosti o 87 %** ve srovnání s tradičními metodami.

Supravodivé qubity jsou klíčovou součástí kvantových počítačů, ale jejich výkon je často omezen šumem a dekoherencí. Nový přístup přináší významné zlepšení stability a spolehlivosti těchto qubitů, což je nezbytné pro škálovatelnost kvantových systémů.

Tato práce je součástí programu Quantum Systems Accelerator, financovaného americkým ministerstvem energetiky, který se zaměřuje na vývoj kvantových technologií pro řešení vědeckých problémů, jež jsou mimo dosah klasických počítačů. Nová výrobní technika představuje **důležitý krok směrem k praktickému využití kvantových počítačů ve vědě a průmyslu**.

thequantuminsider.com



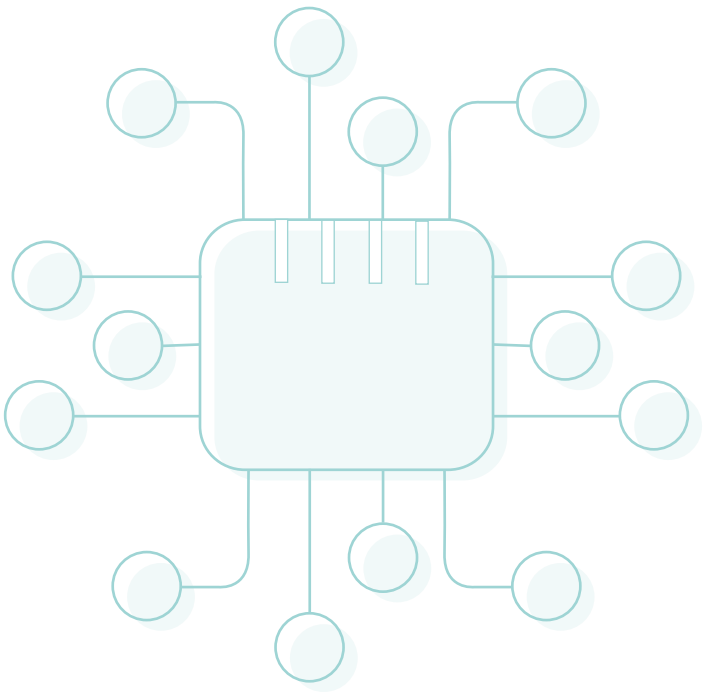
Nové České polovodičové centrum zahájilo činnost v Brně

V Brně bylo slavnostně otevřeno České polovodičové centrum, které má posílit pozici České republiky v oblasti výzkumu, vývoje a výroby polovodičových technologií. Centrum vzniklo v rámci evropské iniciativy „Chips for Europe“ a je součástí širšího plánu na zvýšení technologické suverenity Evropy v oblasti čipů.

Otevření centra je v souladu s Národní polovodičovou strategií, která byla schválena vládou České republiky v říjnu 2024. Tato **strategie si klade za cíl zvýšit podíl ČR na evropském trhu s polovodiči a vytvořit podmínky pro rozvoj domácího výzkumu a výroby čipů**. Brněnské centrum představuje klíčový krok k dosažení těchto ambiciózních cílů.

Hlavním cílem centra je vytvořit komplexní ekosystém, který propojí výzkumné instituce, univerzity a průmyslové partnery. Tímto způsobem se má podpořit inovace, transfer technologií a vzdělávání nových odborníků v oblasti polovodičů. Centrum bude rovněž sloužit jako platforma pro mezinárodní spolupráci, zejména s partnery z Tchaj-wanu, což má přispět také k posílení globální konkurenceschopnosti českého polovodičového průmyslu.

vedavyzkum.cz



Útočníci zintenzivňují útoky na vývojářská tajemství

Kybernetičtí útočníci stále častěji **cílí na vývojářská tajemství**, jako jsou **API klíče, přístupové tokeny a konfigurační soubory**, které jsou mnohdy omylem zveřejněny ve veřejných repozitářích jako je GitHub. V dubnu došlo k významnému nárůstu skenování z IP adres velkých cloudových poskytovatelů, zaměřených na soubory jako. env a. git, což naznačuje koordinované úsilí v tomto sofistikovaném typu útoku.

V číslech:

Podle zprávy společnosti GitGuardian bylo v roce 2024 veřejně odhaleno téměř **24 milionů tajemství, což je více než dvojnásobek oproti předchozímu roku.**

Přibližně **65 %** těchto úniků pocházelo **z konfiguračních souborů s proměnnými prostředí.**

Mnoho vývojářů, zejména těch, **kteří využívají nástroje pro generování kódu pomocí AI**, nevědomky zahrnuje tyto soubory do svých nasazení, čímž vystavují své aplikace velkému riziku.

Nebezpečí tohoto útoku se dále váže na častokrát nedostatečné omezování oprávnění v rámci sítí jednotlivých organizací. Například téměř **95 %** tokenů na GitHubu má plný přístup v rámci sítě, což v případě úniku značně zvyšuje potenciální škody. Útočníci totiž **mohou tyto informace využít k laterálnímu pohybu v rámci systémů** (získávat přístupy k dalším účtům v síti) **a kompromitovat tak celé organizace**.

Společnost GitHub zavedla opatření jako Push Protection, které automaticky detekuje a blokuje nahrávání tajemství do veřejných repozitářů. Přesto je **klíčové, aby vývojáři dodržovali osvědčené bezpečnostní postupy**, včetně pravidelných auditů kódu, omezení oprávnění a využívání nástrojů pro správu tajemství, aby **minimalizovali riziko úniku citlivých informací**. Nárůst tohoto typu útoku dokumentuje **nezbytnost dodržovaní zásad kybernetické bezpečnosti** také při realizací výzkumných a vývojových projektů.

www.tum.de

Google nasazuje agentní AI pro boj s kybernetickými hrozbami

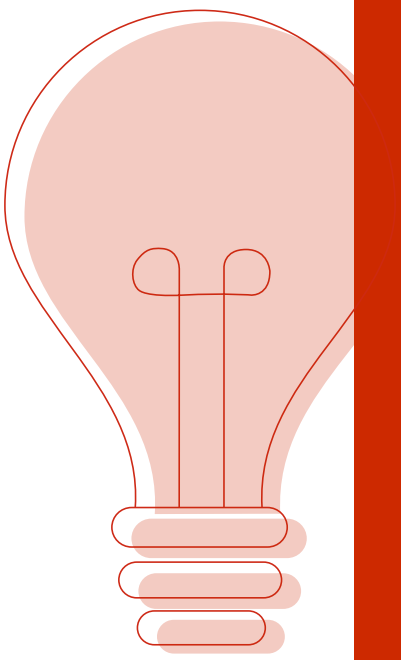
Google představil novou platformu Unified Security, která využívá agentní umělou inteligenci k posílení kybernetické bezpečnosti. Tato technologie kombinuje informace o hrozbách z Mandiant s bezpečnostními operacemi, cloudovou ochranou a bezpečným podnikových prohlížením, vše podpořeno systémem Gemini AI.

Agentní AI, schopná samostatného rozhodování a učení, automatizuje rutinní úkoly jako je třídění výstrah, vyšetřování incidentů a analýza malwaru. Tím umožňuje bezpečnostním týmům soustředit se na komplexnější hrozby. Nové funkce, jako „Curated Detections“ a „Applied Threat Intelligence Rule Packs“, pomáhají identifikovat škodlivé aktivity, včetně malwaru a kompromitace cloudových služeb.

Zpráva M-Trends 2025 uvádí, že i přes mírný pokles zneužití zero-day zranitelností v roce 2024, útoky zaměřené na podnikové technologie tvořily **44 %** všech exploitací. Zneužití odcizených přihlašovacích údajů a phishingové útoky také zaznamenaly nárůst, přičemž finanční sektor byl hlavním cílem.

Google tímto krokem reaguje na rostoucí sofistikovanost kybernetických hrozeb a nedostatek kvalifikovaných pracovníků v oblasti bezpečnosti. Implementace agentní AI představuje významný posun směrem k proaktivní a automatizované ochraně digitální infrastruktury.

hackread.com



Tip na akci

Konference SCI-PO 2025

Ve čtvrtek 29. května se v Praze uskuteční již šestý ročník konference SCI-PO, strategického fóra veřejné politiky v oblasti výzkumu, vývoje a inovací. Letošní ročník se zaměří na udržitelné financování výzkumu, vývoje a inovací po roce 2027. Program konference bude hledat odpovědi na otázky jako například jak přejít od závislosti na unijním financování k odolnějším modelům nebo jak minimalizovat dopady omezení evropských zdrojů a posílit odolnost systému? Konference je spoluorganizovaná Technologickým centrem Praha, ALEVIA, CERGE-EI, CESES UK a Univerzitou Palackého Olomouc. Registrace na konferenci je otevřená.

tc.cz

Věděli jste, že

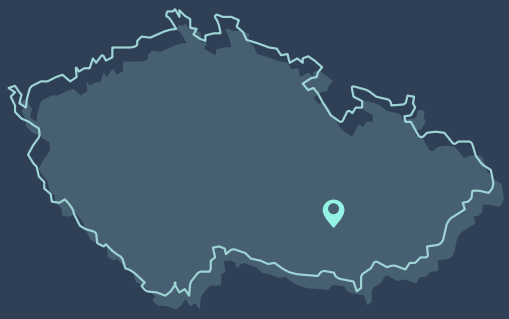
Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) byla zneužita při dezinformační kampani? Prostřednictvím sociálních sítí a různých komunikačních aplikací se v průběhu dubna šířili informace, že k výpadkům proudu v některých částech jižní Evropy došlo v důsledku kybernetických útoků. Dále byly šířeny také nepravdivé informace o údajném kybernetickém útoku na evropské banky. V obou případech byla za zdroj těchto informací falešně uváděna právě ENISA. Agentura před touto skutečností sama varovala, vyzvala veřejnost k obezřetnosti a doporučuje ověřovat si informace prostřednictvím oficiálních zdrojů.

enisa.europa.eu

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

Založení Českého polovodičového centra je strategickým krokem pro budoucnost naší země. Jde o klíčový projekt, díky kterému si Česká republika udrží konkurenceschopnost, ale i bezpečnost a technologickou suverenitu v době, kdy o tyto hodnoty probíhá globální zápas,

předseda vlády ČR Petr Fiala při příležitosti otevření Českého polovodičového centra