

Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

[Česká republika nastínila priority svého předsednictví v Radě EU v oblasti výzkumu, vývoje a inovací](#)

Byly představeny dvě tematické priority pro nadcházející předsednictví ČR v Radě EU v oblasti výzkumu, vývoje a inovací. Jako prioritní témata byly zvoleny výzkumné infrastruktury a synergie ve financování vědy, výzkumu a inovací vycházející z European Research Area Policy Agenda pro roky 2022-2024. V oblasti výzkumných infrastruktur chce ČR řešit otázky týkající se ukotvení výzkumných infrastruktur jako integrální součásti kritické infrastruktury a vybudování jednotné evropské datové infrastruktury. Druhá priorita týkající se zajištění synergie ve financování vědy, výzkumu a inovací, má přinést zefektivnění a maximalizaci investic do tohoto sektoru i skrze zajištění synergie v širším pojetí, konkrétně kofinancováním projektů evropské charakteru a využíváním komunitárních programů a fondů. Bližší informace k prioritám jsou k dispozici [zde](#).

[ENISA připravuje další Cybersecurity Certification Conference, která proběhne v červnu 2022](#)

Ve dnech 2. a 3. června 2022 pořádá Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) další ročník Cybersecurity Certification Conference, která proběhne v hybridním formátu a bude přenášena z Atén. Program a odkaz k registraci bude brzy zveřejněn na [tomto odkazu](#).

[Květnová konference CHIST-ERA 2020 přináší příležitost definovat témata pro nadcházející podzimní výzvu](#)

Do 17. května je možné registrovat se na konferenci CHIST-ERA určenou pro odborníky z oblasti informačních a komunikačních technologií (ICT), která proběhne 24.-26. května 2022 v Edinburghu a online. Účastníci získají možnost podílet se na definici témat chystané podzimní výzvy CHIST-ERA Call 2022 v oblastech Security and Privacy and Decentralised and Distributed Systems (SPiDDS) a Machine Learning-based Communication Systems. Vybraní účastníci budou moci představit své projektové záměry. Více informací včetně programu a registračního odkazu je k dispozici na stránkách [TAČR](#).

[Sdružení univerzit EuroTech pořádá webinář k Evropskému aktu o čípech](#)

Ve čtvrtek 5. května 2022 proběhne webinář týkající se Evropského aktu o čípech pohledem univerzit. Evropský akt o čípech je návrh komplexního souboru opatření Evropské komise, jehož cílem je posílení konkurenceschopnosti a odolnosti Evropy v polovodičových technologiích, zajištění odolnosti dodávek do Evropské unie (EU) a zajištění jejího vedoucího postavení v této oblasti. Akce je pořádána sdružením univerzit EuroTech a na programu je přednáška a panelová diskuze. Více informací a odkaz k registraci [zde](#).

Nová metoda rychlejšího zabezpečení souborů na nevolatilních pamětech

(5. 4. 2022; [sciencedaily.com](https://www.sciencedaily.com)) Výzkumníci z North Carolina State University vyvinuli novou šifrovací techniku, která přispívá k vylepšení bezpečnosti souborů na pamětech nové generace (tzv. non-volatile memories, NVMs) a umožňuje rychlejší výkon než stávající technologie. Při simulacích bylo zjištěno, že použití nové metody zpomalilo operace o 3,8 % v porovnání s 200% zpomalením při použití současných nástrojů. Pokud by bylo nové řešení implementováno v komerčních procesorech, výrazně by se zlepšil výkon zabezpečování souborů ve velkých datových a cloudových systémech.

Komentář: Mezi hlavní přednosti NVMs patří rychlý přístup k datům, složité šifrování souborů však představuje bezpečnostní riziko. Nový objev řeší způsob, jak zabezpečit soubory uložené na NVMs, aniž by došlo ke zpomalení rychlosti, která je pro ně charakteristická.

USA varují před schopnostmi APT skupin v systémech typu ICS/SCADA

(13. 4. 2022; [cisa.gov](https://www.cisa.gov)) FBI ve spolupráci s dalšími agenturami informovala, že některé APT skupiny již dokáží získat úplný přístup k průmyslovým řídicím systémům (ICS) a SCADA systémům pro dohled, řízení a sběr dat. V případě, že aktéři za využití nových nástrojů získají přístup k síti provozních technologií, mohou vyhledávat, kompromitovat a ovládat napadená zařízení a pracovní stanice. Vydané varování cílí zejména na subjekty kritické infrastruktury v energetickém sektoru. Zpráva obsahuje technické detaily a doporučení k implementaci.

Komentář: APT, anglicky Advanced Persistent Threat, označuje velmi pokročilé techniky útoků, které se vyznačují svým specifickým zaměřením na konkrétní cíle, pokročilostí, kdy využívají doposud neobjevená slabá místa (tzv. zero-day zranitelnosti) a perzistencí, jelikož hrozba přetrvává, dokud se útočníkovi nepodaří dosáhnout cíle. APT skupiny tak patří mezi nejvíce sofistikované aktéry v kyberprostoru.

Objevují se podvodné stránky s nabídkou aktualizace na Windows 11

(20. 4. 2022; [hackread.com](https://www.hackread.com)) Výzkumníci společnosti CloudSEK objevili podvodnou stránku nabízející novou verzi Windows 11 pro zařízení, která již nesplňují minimální požadavky na systém. Místo Windows však dochází k nainstalování Inno Stealer malware, který na infikovaném zařízení vytvoří dočasné soubory, z nichž některé obsahují speciálně navržené skripty pro deaktivaci důležitých funkcí zabezpečení jako je například registr Windows.

Komentář: V důsledku upgradu na nový operační systém Windows 11 a s ním souvisejícími minimálními požadavky se zvýšil okruh uživatelů, kteří dané standardy nesplňují. Podvodníci se tak zaměřili na vytváření podvodných stránek nabízející stažení nové verze systému, které běžný uživatel nemusí odhalit. Nejbezpečnějším způsobem instalace zůstává funkce Windows Update, která zařízením splňující požadavky sama aktualizaci nabídne.

Oddělení výzkumu a evropské spolupráce, NÚKIB