

## Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

### Otevření mezinárodní výzvy CHIST-ERA

Začátkem listopadu byla otevřena mezinárodní výzva k předkládání projektů v oblasti výzkumu informačních a komunikačních technologií. Tématy letošní výzvy jsou „Security and Privacy in Decentralised and Distributed Systems (SPiDDS)“ a „Machine Learning-based Communication Systems, towards Wireless AI (WAI)“. Lhůta pro podávání návrhů projektů potrvá do 2. února 2023. Bližší informace o výzvě financované z Národního plánu obnovy jsou k dispozici [zde](#).

### Výzvy v programu Digitální Evropa

Evropská komise otevřela 15. listopadu 2022 další část výzev k financování projektů z programu Digital Europe. Lhůta pro podání žádostí je stanovena na 15. února 2023. Výzvy se týkají například zabezpečení 5G infrastruktur a technologií, Security Operation center, testovacích a certifikačních kapacit a implementace směrnice NIS. Bližší informace jsou k dispozici [zde](#).

### Vyhlášení veřejné soutěže v programu TREND

Dne 23. listopadu 2022 vyhlásila Technologická agentura ČR (TA ČR) společně s Ministerstvem průmyslu a obchodu v pořadí devátou veřejnou soutěž v Programu na podporu aplikovaného výzkumu a experimentálního vývoje TREND. Cílem výzvy je nastartovat výzkumné a vývojové aktivity v podnicích, které dosud tento typ činností pravidelně nerealizovaly. Předkládat projekty je

možné do 11. ledna 2023. Bližší informace k výzvě jsou k nalezení na webu [TA ČR](#).

### Výdaje České republiky na výzkum a vývoj dosáhly úrovně 2 % HDP

Český statistický úřad uvedl ve výstupu statistického šetření za rok 2021, že celkové výdaje na výzkum a vývoj (VaV) dosáhly poprvé v ČR hranice 2 % HDP (122 mld. Kč). Jako odvětví s nejdynamičtějším růstem výdajů na VaV byly označeny informační a komunikační technologie, kdy konkrétně podniky v oblasti IT vynaložily v roce 2021 na VaV 19,2 miliardy Kč, což je o polovinu více než před 3 lety. Mezinárodní hodnocení European Innovation Scoreboard (EIS) taktéž potvrzuje, že ČR patří k evropským premiantům ve vzdělávání a zavádění ICT technologií. Analýza statistických výstupů včetně identifikace slabých míst je k přečtení [zde](#).

### Blíží se druhý ročník Summitu Evropské rady pro inovace

Ve dnech 7. a 8. prosince 2022 se v Bruselu uskuteční summit pořádaný Evropskou radou pro inovace (EIC), který je určen především zástupcům technologických start-upů, investorům, expertům, výzkumníkům a tvůrcům inovačních politik. Účastníci budou diskutovat o problémech rozvoje inovací v Evropě, seznámí se s příklady úspěšných projektů a získají praktické rady pro zapojení do programu. Akci bude možné sledovat online na [webu události](#).

## ENISA vydala Threat Landscape a identifikovala nejvýznamnější hrozby

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) publikovala [zprávu Threat Landscape 2022](#) analyzující bezpečnostní prostředí s důrazem na hlavní trendy v oblasti hrozeb, škodlivých aktérů a technik útoků. ENISA taktéž identifikovala a seřadila 10 kybernetických hrozeb, které považuje za nejzásadnější do roku 2030. Můžeme jmenovat například útoky na dodavatelské řetězce, zneužití umělé inteligence i nedostatek dovedností. Více informací [zde](#).

## AI chrání před datovými úniky

(09. 11. 2022; [sciencedaily.com](#)) Odborníci na ochranu soukromí a osobních dat vyvinuli algoritmus umělé inteligence (AI), který dokáže automaticky testovat míru rizika úniku dat ze systémů určených k jejich ochraně. Skupina Imperial's Computational Privacy Group se zabývala útoky na tzv. query-based systémy (QBS) a vytvořila metodu QuerySnout, která s podporou AI takové útoky odhaluje. Jedná se o první využití AI k automatickému odhalování zranitelností v tomto typu systémů.

**Komentář:** Systémy QBS poskytují přístup ke statistickým údajům o jednotlivcích, jako je poloha a demografické údaje. Využívají je například velké komerční společnosti jako Google nebo Meta.

## Wi-Peep dokáže přes zdi identifikovat a lokalizovat zařízení připojená k WiFi

(03. 11. 2022; [sciencedaily.com](#)) Výzkumný tým University of Waterloo vyvinul dronem poháněné zařízení Wi-Peep, které dokáže identifikovat a lokalizovat všechna zařízení připojená k WiFi

uvnitř budovy. Zařízení zneužívá bezpečnostní mezeru přezdívanou jako „polite WiFi“, kdy i přestože je síť chráněna heslem, chytrá zařízení automaticky „zdvořile“ reagují na pokusy o kontakt z dalších zařízení v dosahu. Wi-Peep tak může změřit délku jejich odezvy, což mu umožní určit polohu zařízení s přesností na metr.

**Komentář:** Možnost identifikovat a lokalizovat zařízení uvnitř budov představuje bezpečnostní riziko. Jedním z řešení je zavedení náhodné variability doby odezvy zařízení, díky čemuž by výpočty potřebné k jejich lokalizaci byly nepřesné.

## Nový navigační systém s vysokou přesností

(16. 11. 2022; [sciencedaily.com](#)) Výzkumníci z Delft University of Technology, Vrije Universiteit Amsterdam a VSL vyvinuli alternativní systém určování polohy, který využívá mobilní telekomunikační síť namísto satelitů. Nový systém určování polohy má být robustnější a přesnější než GPS, a to zejména v městských oblastech. Funkční prototyp systému dosáhl přesnosti na 10 cm. Tato nová technologie má být využitelná v automatizovaných vozidlech, kvantované komunikaci a mobilních komunikačních systémech nové generace.

**Komentář:** V současnosti nejrozšířenější navigační systémy GPS a Galileo využívají satelitní rádiové signály – ty však mohou být zvláště ve městech odraženy nebo blokovány budovami.

Oddělení výzkumu a evropské spolupráce, NÚKIB