Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

Členové Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti se setkali v Ostravě

22. června 2022 proběhlo na půdě VŠB Technické univerzity Ostrava (VŠB-TUO) setkání členů Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti. Během akce byla diskutována témata související s novým Národním plánem výzkumu a vývoje v kybernetické a informační bezpečnosti a s budováním Evropského kompetenčního centra a Národního koordinačního centra pro kybernetický výzkum a vývoj. Experti z VŠB-TUO představili účastníkům tematické zaměření výuky, publikací i výzkumu včetně konkrétních výzkumných projektů. V odpolední části programu proběhl workshop k projektu NESPOQ a exkurze do národního superpočítačového centra IT4Innovations. Zájemci o členství v Platformě se mohou hlásit skrze e-mail ncc@nukib.cz. Příští setkání je plánováno na podzim.

Kybernetická bezpečnost je jednou z priorit českého předsednictví v Radě EU

Vláda České republiky schválila pět hlavních priorit předsednictví ČR v Radě EU, mezi které patří vedle energetické odolnosti, zvládnutí uprchlické krize a strategické odolnosti evropské ekonomiky právě posílení evropských obranných kapacit a bezpečnosti kybernetického prostoru. Zvolené priority mají reflektovat strategické zájmy a hodnoty, které ČR dlouhodobě zastává. V oblasti kybernetické bezpečnosti se ČR bude zaměřovat na zajištění vysoké společné úrovně kybernetické bezpečnosti institucí, orgánů a agentur EU a bezpečnost ICT produktů a souvisejících služeb. Významným tématem je zajištění kybernetické bezpečnosti dodavatelského řetězce ICT, což je oblast, na kterou se ČR dlouhodobě zaměřuje. Do stanovených priorit se mohou promítnout také kybernetické hrozby plynoucí z války na Ukrajině. Více informací ke zvoleným prioritám zde.

Kvalita vzdělávání a výzkumu v ČR

Projekt Index prosperity Česka zveřejnil analýzu, která porovnává a měří prosperitu ČR vůči dalším členským státům Evropské unie, a to z hlediska různých ukazatelů, mezi které patří právě kvalita vzdělání a výzkumu. Schopnost inovovat je přímo závislá na vzdělávání i na podpoře vědy a výzkumu, důležitou roli hraje také spolupráce mezi vědci a firmami. V analýze jsou zmíněny konkrétní nedostatky, například úroveň kvality vysokoškolského vzdělávání a nízký počet vysokoškolsky vzdělaných mladých lidí. Řešena je také nedostatečná spolupráce mezi firmami a univerzitami, což vede ke snížení inovační kapacity ČR, a dále zastaralá legislativa a byrokracie, které brání vyššímu zapojení soukromého sektoru do podpory vzdělávání a výzkumu. České financování vědy a výzkumu je v evropském srovnání hodnoceno průměrně.

V červenci se spouští první výzva v rámci programu Technologická inkubace

Nový program Technologická inkubace má představovat zásadní investici do budoucnosti

českého průmyslu, kdy cílem je v následujících pěti letech podpořit až 250 inovativních startupů v sedmi klíčových oblastech, mezi které patří například umělá inteligence a chytrá řešení v kybernetické bezpečnosti. První výzva projektu bude otevřena od 1. do 31. července 2022 a bude se týkat čtyř oblastí (oblasti mobility, kreativních průmyslů, ekologie, cirkulární ekonomiky a umělé inteligence). Více informací k programu zde.

Čeští vědci mohou využívat jeden z nejvýkonnějších superpočítačů

(6. 6. 2022; vedavyzkum.cz) Superpočítač LUMI, který je instalován ve finském Kajaani, nabízí část své výpočetní kapacity i české vědecké komunitě, a to díky členství národního superpočítačového centra IT4Innovations, které je součástí VŠB-TUO, v konsorciu LUMI. V průběhu srpna by měla být zahájena druhá pilotní fáze systému LUMI pro vybrané uživatele a od září 2022 by měl být systém všeobecně dostupným.

Komentář: V Evropě se superpočítač LUMI řadí v žebříčku nejvýkonnějších superpočítačů na první místo, ve světové konkurenci pak na třetí. Superpočítač by měl podpořit inovace v klíčových oblastech, mezi které patří například výzkum umělé inteligence a její aplikace v praxi.

GhostTouch: útočníci se displeje mobilního zařízení nemusí přímo dotýkat

(14. 6. 2022; portswigger.net) Některé útoky na mobilní zařízení vyžadují fyzický přístup k zařízení a interakci s dotykovou obrazovkou. Výzkumníci z Technické univerzity v Darmstadtu a Zhejiang University v Číně však popsali tzv. GhostTouch, což je typ útoku, který dovoluje provádět klepnutí či přejetí prstem po obrazovce telefonu i ze vzdálenosti 40 milimetrů. Útok by dle výzkumníků mohl fungovat na veřejných místech, jako v konferenčních halách či kavárnách, kdy uživatelé pokládají na stůl telefony obrazovkou dolů. Pokud by měl útočník zabudované speciální zařízení pod stolem, mohl by přikročit ke konkrétním akcím na obrazovce, jako například přijetí hovoru, odemknutí zařízení, zadání hesla, spuštění škodlivého odkazu a dalším.

Komentář: Výzkumníci v této souvislosti zkoumali zařízení s kapacitními dotykovými obrazovkami, které jsou citlivé na dopad elektromagnetické inference (EMI), což může v některých případech vést k náhodným dotykům na obrazovkách. Zaměřovali se konkrétně na to, zda lze použít EMI k vytvoření kontrolovaných dotyků a spuštění procesu na tomto typu dotykových obrazovek.

Varování před novým spyware cílícím na uživatele Android a iOS

(24. 6. 2022; threatpost.com) Odborníci z Google Threat Analysis Group zaznamenali případy útoků, v rámci kterých byl uživatelům v Kazachstánu a Itálii rozesílán unikátní odkaz, který se tvářil jako aktualizace legitimních uživatelských aplikací, v reálu však vedl ke stažení a instalaci spyware s názvem Hermit, který umožňuje krást data a zaznamenávat a provádět hovory.

Komentář: Využívání podobných programů je velmi často přisuzováno vládám, které se skrze ně zaměřují na disidenty, novináře, aktivisty a opoziční politiky. Z tohoto důvodu existují důvody se domnívat, že za kampaní může být státní aktér.

Oddělení výzkumu a evropské spolupráce, NÚKIB