Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

V Lucemburku se sešli členové Správní rady Evropského kompetenčního centra

Ve dnech 19. a 20. října 2022 se v Lucemburku uskutečnilo setkání členů Správní rady Evropského kompetenčního centra (ECCC) a zástupců Evropské komise a Agentury EU pro kybernetickou bezpečnosti (ENISA), v rámci kterého byly řešeny záležitosti týkající se strategických priorit a budoucího fungování ECCC. Zástupci členských států EU zhodnotili dosavadní činnost několika pracovních skupin a diskutovali otázky spojené například se vznikem jednotlivých Národních koordinačních center (NKC) a nastavováním registračního procesu členů do vznikající Komunity v oblasti kybernetického výzkumu a vývoje. Tisková zpráva je k přečtení na webu ECCC.

Kybernetická bezpečnost na Future Forces Forum

Future Forces Forum, veletrh zaměřující se na aktuální potřeby a trendy v oblasti bezpečnosti, proběhl ve dnech 19.-21. října 2022 v Praze. Návštěvníci měli příležitost setkat se se zástupci státní správy, vědecko-výzkumných center a univerzit i průmyslových podniků z celého světa. Kromě výstavy moderních bezpečnostních technologií byly součástí akce taktéž prezentace a panelové diskuse zaměřující se na aktuální bezpečnostní otázky, včetně kybernetické bezpečnosti. NÚKIB se akce aktivně účastnil a přispěl k šíření povědomí o problematice kyberbezpečnosti a aktuálních výzvách a hrozbách v této oblasti. Bližší informace jsou k dispozici zde.

Listopadová konference EU Secure and Innovative Digital Future

Úřad vlády, Ministerstvo průmyslu a obchodu a NÚKIB společně pořádají v rámci českého předsednictví v Radě EU ve dnech 3. a 4. listopadu 2022 konferenci o vývoji bezpečných digitálních inovací. Akce se uskuteční v Kongresovém centru Praha a bude rozdělena do dvou hlavních diskuzních bloků. První den konference se zaměří na téma bezpečnosti dodavatelského řetězce, druhý den budou řešeny témata související s rozvojem evropského digitálního ekosystému. Veřejnou část prvního dne konference je možné sledovat online zde, v rámci druhého dne pak zde.

Vyhlášení veřejné soutěže v programu IMPAKT 1

Ministerstvo vnitra vyhlásilo veřejnou soutěž s lhůtou pro podávání návrhů projektů do 9. listopadu 2022, jejímž cílem je podpořit rozvoj internacionalizační iniciativy v komunitě bezpečnostního výzkumu. Právě otevřená výzva spadá v rámci programu Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019-2025 (IMPAKT 1) do podprogramu 3 s podtitulem „Rozvoj iniciativy v bezpečnostním výzkumu“. Bližší informace jsou k dispozici zde.

Program TREND: vyhlášení veřejné soutěže

Technologická agentura ČR (TA ČR) vyhlásila v průběhu měsíce října osmou veřejnou soutěž ve výzkumu a experimentálním vývoji v programu

TREND a podprogramu 1 s názvem „Technologičtí lídři“, jejímž cílem je podpořit projekty zabývající se vývojem technologií 5G a vyšších. Lhůta pro podání návrhů projektů je do 23. listopadu 2022. Podrobné informace k soutěži jsou k dispozici zde.

Termální útoky jako nová metoda k získání hesel

(10. 10. 2022; zdnet.com) Výzkumníci z University of Glasgow's School of Computing Science upozornili na novou techniku útoku, která umožňuje za využití kombinace termálního zobrazování a umělé inteligence získat počítačová a mobilní hesla uživatelů. Odborníci demonstrovali schopnost systému přečíst tepelné stopy po dotycích prstů na počítačových klávesnicích i displejích chytrých telefonů, a to během několika sekund. S využitím speciální termální kamery je možné získat fotku, ze které lze díky identifikaci míst dotyků určit heslo nebo pin, což může potenciálně představovat velmi vážné bezpečnostní riziko. Umělá inteligence takto dokáže odhalit až 86 % hesel během 20 sekund.

Komentář: Význam této hrozby se úměrně zvyšuje s klesající cenou termokamer a rozšiřujícím se přístupem k umělé inteligenci a algoritmům strojového učení. Z tohoto důvodu existují obavy z využití technologie kyberkriminálními aktéry.

Nová forma výpočetní architektury využívá pro hluboké učení světlo

(20. 10. 2022; sciencedaily.com) Výhoda této architektury spočívá především ve schopnosti provádět pokročilé výpočty strojového učení s pouhým zlomkem výkonu a paměťové kapacity dnešních zařízení. Zrychlení výpočetních procesů je realizováno převodem dat na světelné vlny, které pak mohou být v mnohem větším množství a rychlosti přenášeny mezi datovými centry. Metoda může také přispět ke zvýšení bezpečnosti, jelikož uživatelská data již nebudou muset procházet centrálním výpočetním střediskem.

Komentář: Architektura je využitelná například v automobilech s autopilotem, které se budou moci rozhodovat v reálném čase a s výrazně nižší spotřebou energie.

Nástroj RSA Mobile Lock přispívá k vyššímu zabezpečení mobilních telefonů

(21. 10. 2022; helpnetsecurity.com) Čím dál více pozornosti je věnováno zabezpečení mobilních zařízení, které je z pohledu firem vysoce žádoucí, avšak vytváří celou řadu požadavků na straně zaměstnanců. Objevují se proto aplikace jako například RSA Mobile Lock, jejichž primárním účelem je zajištění ochrany uživatelů mobilních zařízení a v nich uložených dat prostřednictvím detekce kritických hrozeb. Pokud aplikace tohoto typu zjistí, že konkrétní zařízení čelí vážné hrozbě, okamžitě zablokují přístup k podnikovým systémům a provedou další kroky, čímž znemožní šíření hrozby z jednoho zařízení na další potenciální uživatele, data a systémy.

Komentář: Nejslabším článkem kybernetické bezpečnosti typicky nebývají technologie, nýbrž člověk. Až 82 % bezpečnostních incidentů týkajících se mobilních zařízení je způsobeno nesprávnou manipulací. Téma mobilní bezpečnosti je tak vysoce relevantní.

Oddělení výzkumu a evropské spolupráce, NÚKIB