Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

Proběhlo třetí setkání Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti

31. března se v prostorách Technologické agentury ČR konalo již třetí setkání Platformy k výzkumu a vývoji v kybernetické a informační bezpečnosti. V rámci akce byla diskutována témata související s posilováním spolupráce v oblasti výzkumu a vývoje kybernetické bezpečnosti a zapojováním do projektů na národní i mezinárodní úrovni.

Otevřené druhé kolo výzev v programu Digitální Evropa

Bylo zveřejněno druhé kolo výzev k předkládání žádostí v rámci programu Digitální Evropa. Výzvy se týkají několika oblastí, například podpory kybernetické bezpečnosti ve zdravotnickém sektoru, umělé inteligence, inovací ve vzdělávání a training kurzů v klíčových oblastech jako je umělá inteligence a kybernetická bezpečnost. Deadline pro podávání návrhů je 17. května 2022. Přehled otevřených výzev je k dispozici zde.

ENISA uspořádá webinář zaměřený na problematiku cybersecurity skills gap

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) pořádá 5. dubna 2022 webinář, který se má věnovat problému nedostatku kvalifikovaných odborníků na trhu práce v oblasti kybernetické bezpečnosti. Probírat se bude také European Cybersecurity Skills Framework (ECSF), který si klade za cíl vytvoření společného vymezení rolí a kompetencí k narovnání mezery v dovednostech v kyberbezpečnosti. ECSF má také usnadňovat uznávání schopností, podporovat vzdělávací programy a zaměstnanost. Registrace není nutná, webinář lze sledovat živě na YouTube, či ze záznamu. Více informací a odkaz zde.

Technologické centrum AV ČR pořádá akce pro koordinátory projektů Horizont Evropa

S ohledem na probíhající výzvy v programu Horizont Evropa pořádá Technologické centrum Akademie věd ČR 7. dubna 2022 workshop pro budoucí koordinátory projektů Horizont Evropa se zaměřením na životní cyklus projektu, právní otázky a doporučení pro zpracování návrhů. 11. dubna poté proběhne seminář zaměřený na přípravu rozpočtů a vykazování nákladů v projektech Horizont Evropa, včetně představení finančních novinek v programu.

Nové publikace ENISA z oblasti kybernetické bezpečnosti

ENISA zveřejnila na svém webu v průběhu března několik nových publikací zabývajících se standardy v oblasti kybernetické bezpečnosti 5G, možnostmi spolupráce mezi CSIRT týmy, orgány činnými v trestním řízení a prokurátory a soudci, dále guidelines pro poskytovatele sítí a služeb elektronických komunikací v oblasti informování uživatelů o hrozbách a dokument zabývající se metodami a nástroji řízení rizik.

Výzkumníci demonstrovali nový typ útoku postranním kanálem

(3. 3. 2022; thehackernews.com) Výzkumníci z North Carolina State University a Dokuz Eylul University demonstrovali první útok postranním kanálem (tzv. side-channel attack) na homomorfní šifrování, který může být zneužit k úniku dat během šifrovacího procesu. Byla objevena možnost, jak lze číst data v procesu jejich šifrování, a to pomocí sledování spotřeby energie v zařízení, které data kóduje. Tento typ útoku využívá chybu v šifrovací knihovně Microsoft SEAL.

Komentář: Útoky postranním kanálem představují v kryptografii zjednodušeně řečeno útoky, které nehledají slabiny přímo ve struktuře algoritmu, ale cílí na zneužití informací během běhu kryptografického algoritmu. Nový typ útoku dokazuje, že ani šifrovací metody nové generace nejsou před kybernetickými útoky imunní.

Nová phishingová technika browser-in-browser

(19. 3. 2022; bleepingcomputer.com) Byl zveřejněn phishing kit, který dovoluje vytváření efektivních podvodných přihlašovacích oken napodobujících webový prohlížeč Chrome. Vytvoření simulovaného přihlašovacího okna je možné s použitím běžného HTML, CSS a Javascriptu. Tento typ útoku získal označení Browser in the Browser attack (BitB) a vyznačuje se otevřením podvodného okna v rámci běžného okna prohlížeče. Tento typ útoku zneužívá častý způsob přihlašování do různých aplikací, které vedle vytvoření nového účtu dovolují přihlášení skrze již existující účty (například Google či Apple účet), ke kterému je možné se přihlásit ve vyskakovacím okně.

Komentář: Sofistikovanost phishingových útoků spadajících do technik sociálního inženýrství se neustále zvyšuje, odhalit tedy pokus o podvod může být pro běžného uživatele velmi složité. V tomto konkrétním případě nestačí ani kontrola ikony zámku v adresním řádku (HTTPS protokol).

HEAT útoky: nová kategorie kybernetických hrozeb

(22. 3. 2022; helpnetsecurity.com) Podle výzkumu společnosti Menlo Security škodliví aktéři zneužívají čím dál častějšího používání webových prohlížečů (například k přístupům ke cloudovým aplikacím) v zaměstnání, čímž se zvyšuje riziko HEAT útoků. Zkratka HEAT označuje novou skupinu kybernetických hrozeb, tzv. Highly Evasive Adaptive Threats. Již ve druhé polovině roku 2021 byl zaznamenán 224% nárůst těchto typů útoku. Jednou z HEAT technik je například HTML smuggling, které v loňském roce úspěšně využívala ruská hackerská skupina Nobelium k šíření malware a ransomwarovým útokům.

Komentář: HEAT hrozby obcházejí tradiční bezpečnostní obranu včetně firewallů, zabezpečené webové brány, detekce phishingu a dalších. Útočníci zneužívají toho, že organizace nemění dostatečně rychle přístupy k zajišťování bezpečnosti v důsledku rychle se měnícího bezpečnostního prostředí.

Oddělení výzkumu a evropské spolupráce, NÚKIB