Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

Jsou otevřeny první výzvy programu Digitální Evropa

Je vypsáno prvních 28 výzev programu Digitální Evropa. Výzvy jsou otevřeny do 22. 2. 2022 a týkají se např. oblastí data spaces, AI, cloud-to-edge, či zavádění digitálních řešení ve zdravotnictví a zemědělství. Seznam otevřených výzev je k dispozici zde. Program Digitální Evropa má za úkol podpořit digitální transformaci Evropy a poskytovat finanční podporu na projekty v pěti klíčových oblastech včetně kybernetické bezpečnosti. Výzvy představují příležitost získat finanční prostředky na zavádění špičkových technologií na český trh a posílit strategickou autonomii EU.

Byl představen plán akcí Národního informačního centra pro evropský výzkum k Horizontu Evropa

Technologické centrum AV ČR představilo plán akcí k Horizontu Evropa na první pololetí roku 2022. Mezi plánované akce patří například informační den ke 2. výzvě Iniciativy Evropského inovačního a technologického institutu (EIT) pro vysokoškolské instituce, dále pak představení strategického zaměření připravovaného pracovního programu na roky 2023-24. Podrobnější rozpis akcí je k dispozici zde.

V únoru proběhne virtuální AI Week

Univerzita v Tel Avivu pořádá 7.-9. února 2022 AI Week. Akce nabízí tři dny plné workshopů a přednášek expertů z oblasti AI. Konference je zdarma, nutná je registrace. Více informací zde.

Rozpoznávání pomocí pohybu jako metoda autentizace pro mobilní zařízení

(10. 12. 2021; sciencedaily.com) Vědci z *University of Plymouth* testovali možnost využití senzorů pohybu v mobilních zařízeních pro rozpoznávání uživatelů. V rámci výzkumu byli uživatelé chytrých telefonů snímáni pohybovými senzory. Výzkumu se zúčastnilo 44 osob ve věku 18 až 56 let, z nichž každý byl vybaven běžně dostupným smartphonem – ten zaznamenával data zachycená gyroskopem a akcelerometrem během různých fyzických aktivit. Každý účastník vygeneroval v průběhu testu v průměru 4 000 vzorových aktivit, které byly rozděleny do záznamů zobrazujících kromě normální a rychlé chůze také chůzi do a ze schodů. Závěr výzkumu je takový, že v 85 % až 90 % případů byl systém pro rozpoznání pohybu schopný správně určit svého majitele.

Komentář: Výzkumníci z University of Plymouth se dlouhodobě věnují novým a alternativním formám autentizace. V tomto případě se jedná o tzv. *gait authentication*, která využívá toho, že každý člověk má svůj specifický styl chůze. Poměrně velká úspěšnost experimentu ukazuje značný potenciál této metody autentizace pro mobilní zařízení, která stále do značné míry spoléhají na jednoduše prolomitelné způsoby autentizace jako jsou PIN kódy nebo jednoduchá hesla.

Tlukot srdce uživatele jako nová metoda ověření identity

(9. 1. 2022; cc.cz) Česko-německý startup *CardioID* vyvíjí technologii biometrického ověřování založenou na EKG, kdy je za pomoci umělé inteligence totožnost uživatelů ověřována na základě jejich srdečního tepu. EKG člověka má být unikátnější než otisk prstu. Technologie by měla fungovat tak, že náramek změří EKG osoby na jejímž základě vygeneruje umělá inteligence jedinečný identifikátor, který ověří totožnost. V současné chvíli je dokončena základní technologie a pracuje se na návrhu hardwaru, který bude vyráběn ve formě náramků či jako pevná součást chytrých telefonů a hodinek.

Komentář: Hlavním důvodem pro výzkum nových způsobů ověření identity je fakt, že současné přístupy jako je rozpoznávání obličeje či hlasu, skenování sítnice či otisků prstu lze snadno obejít. Využití metody tlukotu srdce je očekáváno ve spotřebitelském, firemním i vládním sektoru – např. u zpravodajských služeb či armády a výrobců chytrých hodinek a telefonů. Projekt podporuje transformaci do světa bez hesel, kde má každý člověk ověřenou a zabezpečenou digitální identitu.

Nový typ malware: multiplatformní backdoor SysJoker

(12. 1. 2022; cybernews.com) Výzkumníci ze společnosti *Intezer* identifikovali nový multiplatformní backdoor SysJoker cílící na operační systémy Windows, Linux a macOS. Dle informací se SysJoker maskuje jako aktualizace systému a cílí na vzdělávací instituce. Předpokládá se, že může být využit jako nástroj kyberšpionáže, kdy jsou shromažďovány informace o zasažené instituci, případně zneužit k nasazení ransomwaru. Jelikož byl škodlivý kód napsán od nuly, pro tři operační systémy a zatím nebyl identifikován u jiných typů útoků, dá se předpokládat, že je dílem pokročilého aktéra. Bližší analýza malware zde.

Komentář: Nově identifikovaný malware potvrzuje trend, kdy se vzdělávací instituce stávají čím dál častějším terčem kybernetických útoků. Jako subjekty pracující s velkým množstvím citlivých informací a dat jsou ideálním terčem kyberšpionážní i ransomwarové kampaně.

Nový způsob jak skrýt malware ve firmware SSD disků

(9. 1. 2022; cyware.com) Jihokorejští výzkumníci odhalili nový typy útoků na SSD disky (solid-state drive), které umožňují uložení malwaru mimo dosah uživatele a bezpečnostní řešení. Týká se to skryté oblasti zvané Over-Provisioning (OP), která je výrobci využívána pro optimalizaci výkonu úložišť založených na pamětech NAND Flash a je neviditelná pro operační systém a aplikace. Hackeři mohou změnit velikost oblasti a vytvořit tak zneužitelný a prakticky neviditelný prostor pro data.

Komentář: Útočníci zneužívající tuto slabinu by mohli získat přístup k potenciálně citlivým informacím, případně využít OP oblast ke skrytí malwaru před uživatelem.

Oddělení výzkumu a evropské spolupráce, NÚKIB