Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

V září proběhne European Conference on Security Research in Cyberspace

Ve dnech 12.-14. září se v Brně uskuteční European Conference on Security Research in Cyberspace, která je pořádána v rámci českého předsednictví v Radě EU a představuje příležitost ke sdílení informací a zkušeností v oblasti kybernetické bezpečnosti mezi výzkumníky, státní správou i zahraničními partnery. Bližší informace k programu, řečníkům a k registraci jsou k dispozici na webu konference.

Spuštění registrace na CyberCon 2022

Byl zahájen prodej vstupenek na letošní ročník konference CyberCon 2022, která se koná ve dnech 13.-15. září v prostorách Fakulty sociálních studií Masarykovy univerzity a Kina Scala. Zájemci se koupí vstupenky mohou registrovat na jednotlivé dny konference – den workshopů zaměřený na praktické řešení problémů v kyberbezpečnosti, dále den určený pro povinné osoby, v rámci kterého budou účastníkům představeny novinky v regulaci, a finálně policy den, jehož součástí budou diskuze o současných výzvách v kybernetické bezpečnosti. Více informací zde.

Národní výzkumná a inovační strategie pro inteligentní specializaci ČR (RIS3)

V červnu Evropská komise schválila Národní výzkumnou a inovační strategii pro inteligentní specializaci ČR 2021-2027. Jejím úkolem je definovat priority v oblasti výzkumu a inovací, které by následně měly být podporovány z operačních fondů i národních programů. Koncentrace finančních prostředků na podporu prioritních témat v oblasti výzkumu a inovací je důležitým krokem k posílení oblastí, ve kterých může ČR získat konkurenční výhodu. V souvislosti se schválenou strategií byl spuštěn portál RIS3 o chytré specializaci, který má informovat, vzdělávat a sdílet data z oblasti aplikovaného výzkumu a inovací. Více informací zde.

Návrh rozpočtu Evropské komise na rok 2023

Evropská komise představila a zároveň předložila k hlasování v Evropském parlamentu a Radě EU nový rozpočtový návrh na rok 2023, díky kterému by se mělo navýšit financování programu Horizont Evropa v porovnání s rokem 2022 až o 100 milionů Eur. Pro program Horizont Evropa navrhuje Komise rozpočet ve výši 12,3 miliardy Eur, který bude doplněn o 1,8 miliardy Eur z evropského fondu obnovy. V následujících letech se Komise plánuje zaměřit na finanční podporu evropského aktu o čipech a na klastr 5 – klima, energetika a mobilita, v důsledku čehož může být omezeno financování klastru 4 – digitalizace, průmysl a vesmír až o 80 milionů Eur. Více informací zde.

Otevřené výzvy Horizont Evropa

V rámci unijního programu Horizont Evropa je s termínem pro podání žádosti do konce listopadu otevřeno několik výzev spadajících do oblasti informačních a komunikačních technologií týkajících se například post-kvantové kryptografie, monitoringu hrozeb a detekce průniku.

Systémy na rozpoznávání obličejů lze obejít pomocí speciální roušky

(12. 7. 2022; helpnetsecurity.com) Výzkumníci z univerzit Ben-Gurion a Tel Aviv demonstrovali, jak lze za pomocí roušky se speciálním potiskem obejít moderní systémy na rozpoznávání obličejů. Systémy byly schopny rozpoznat účastníky s upravenou rouškou pouze ve 3,34 % případech v porovnání s 83,34% úspěšností v případě jiného typu ochrany dýchacích cest.

Komentář: V důsledku pandemie se systémy na rozpoznávání obličejů musely adaptovat na nošení roušek ve veřejném prostoru. V reakci na experiment je možné přistoupit k úpravě obrazu na standardní chirurgickou roušku, se kterou systémy již umí dobře pracovat.

Nová technika de-anonymizačního útoku

(14. 7. 2022; wired.com) Výzkumnici z New Jersey Institute of Technology nalezli způsob, jakým lze identifikovat návštěvníky webové stránky. Útočníci mohou po nasměrování uživatele na škodlivý web zjistit, zda jej prohlíží konkrétní osoba, kterou spojí skrze veřejný identifikátor (například e-mail, účet na sociální síti). Útok funguje na všech známých prohlížečích, včetně prohlížeče Tor. Bližší vysvětlení zde.

Komentář: Při útoku dochází k narušení soukromí uživatelů, v rukou některých aktérů se však může jednat o represivní nástroj, pokud jsou cílem například novináři.

Spyware CloudMensis útočí na macOS

(19. 7. 2022; eset.com) Analytici společnosti ESET objevili nový špionážní malware CloudMensis, který cílí na uživatele zařízení s macOS. Spyware může vykonat 39 příkazů, dokáže například odcizit dokumenty, zaznamenávat stisknuté klávesy, pořizovat snímky obrazovky či prohlížet e-maily. CloudMensis používá pro příjem příkazů i odesílání dokumentů cloudová úložiště (pCloud, Yandex Disk a Dropbox).

Komentář: Z poměrně omezené distribuce spywaru lze usuzovat, že je využíván cíleně ke konkrétním operacím.

Přenos dat z air-gapped počítače

(19. 7. 2022; thehackernews.com) Výzkumníci ze Cyber Security Research Center na izraelské Ben Gurion univerzitě ukázali, že je možné přenést data z air-gapped počítače na blízkou vzdálenost za využití SATA kabelu jako bezdrátové antény.

Komentář: Pomocí air-gappingu, tedy fyzické izolace, jsou chráněny vysoce zranitelné systémy, které jsou cílem sofistikovaných aktérů.

Nový malware cílí na firemní účty na Facebooku

(26. 7. 2022; threatpost.com) Malware Ducktail cílí na uživatele s přístupem k firemním účtům na Facebooku. K nalákání uživatele ke stažení škodlivého souboru slouží phishingová kampaň, malware poté k odcizení dat a účtu využívá uložené soubory cookies v prohlížeči včetně relací na Facebooku.

Komentář: Útočníci cílí na uživatele s přístupem k firemním účtům na sociálních sítích, nejčastěji se proto zaměřují na zaměstnance v oddělení marketingu a lidských zdrojů.

Oddělení výzkumu a evropské spolupráce, NÚKIB