Komentář ke stavu kybernetické bezpečnosti v České republice

Dokončení ze str. 1

„Tento přechod však také ukázal, jak moc jsme závislí na informačních a komunikačních technologiích. Experti z oblasti IT a kybernetické bezpečnosti na tuto závislost poukazují již léta. Ale teprve loňský rok, kdy se internet stal pro nespočet lidí jediným místem, kde šlo pracovat, uzavírat obchody, vést jednání i udržovat kontakt se svými blízkými, nám ukázal, jak obrovská tato závislost ve skutečnosti je. Ale vnímejme to jako příležitost. Virus nám pomohl v tom, co jsme doposud sami nedokázali – přesvědčit většinu společnosti o tom, že kybernetickou bezpečnost a obecně náležitosti správného chování v kyberprostoru musí řešit každý z nás.“

Tou druhou zprávou je vládou schválený Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021-2025. Zde se mohu přidat k vyjádření ing. Lukáše Přibyla ze

společnosti AXENTA a.s., které zní takto: *„Když se mi dostal do rukou „Akční plán k národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025“, tak mi srdce zaplesalo radostí. Kyberbezpečnost v naší zemi již dostala do vínku ZoKB a prováděcí vyhlášky, má dozorný orgán, ale stále jaksi pokulhává. Je dobře, že nyní máme akční plán. A je dobře, že plán má úkoly a k nim přidělené resorty a také k úkolům termíny. Všichni víme, k čemu vede úkol bez zodpovědné osoby a bez termínu, že…*

Držím tedy palce a přeji akčnímu plánu, aby byl naplněn, aby se nepotkal s úředníky, kteří ho budou ignorovat, aby měl tatínka, který za ním bude stát a bude mu pomáhat a aby v roce 2025 byl naplněn.

Uvidíme, jestli to nebylo moc ambiciózní přání…“

AXENTA

Celý článek si přečtete zde ▶

Konference BEZPEČNÁ ŠKOLA 2021 opět s atraktivními tématy a hosty

Již 6. ročník celostátní odborné Konference Bezpečná škola 2021, se bude konat 21. září 2021 v nových, moderních prostorách Konferenčního centra CITY. „Doba koronavirová“ přinesla pedagogům i žákům větší množství času stráveného na počítačích a sociálních sítích, dlouhodobou sociální odloučenost a s ní spojené negativní jevy. Kyberbezpečnost, kybervzdělávání, (kyber)šikana a kyberprevence tak budou rezonovat jako hlavní témata konference Bezpečná škola.

Přednášející však představí i komplexní přístup k bezpečnosti osob ve školním prostředí a vysvětlí možnosti a důležitost spolupráce mezi školami a krizovým řízením. Nevyhnou se ani ožehavému tématu, jakým je právě otevřená agrese ze strany dětí (vzpomeňme např. červnové napadení spolužáků nožem v Příbrami), ale i rodičů.

Novinky v zabezpečení počítačových sítí a dat ve školách, ale i termovizních systémech a prevenci Covid-19, se posluchači dozví od zástupců partnerů Konference, kterými jsou společnosti Omnilink Services, Proficomms, Siemens, VDT Technology a dále Mezinárodní bezpečnostní institut.

Konference představí i konkrétní projekty, např. Stop šikaně, NNTB – Nenech to být, Bezpečně v kyber! a bude se věnovat i možným řešením krizových situací pomocí metod prožitkového vzdělávání. Nebudou chybět ani oblíbené příklady dobré praxe v zabezpečení škol.

Součástí konference je i doprovodná výstava umístěná přímo u přednáškového sálu, která umožní seznámit se jak s nejnovějšími bezpečnostními technologiemi pro použití ve školském prostředí, tak např. s možnostmi, jak vybudovat v okolí škol bezpečná sportoviště.

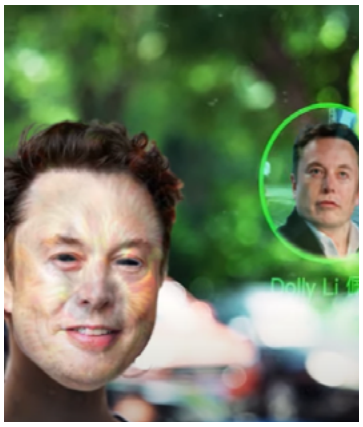
mascotte

Celý článek si přečtete zde ▶

Adversarial Octopus – nový typ útoku proti systémům rozpoznávání obličeje

Nový typ útoku, který nese název „Adversarial Octopus“ se zaměřuje na několik nástrojů rozpoznávání obličejů, které využívají umělou inteligenci. Tento typ útoku byl představen skupinou výzkumníků z firmy Adversa.

Adversarial Octopus útoky dokážou pozměnit fotografie tak, aby je rozpoznávací algoritmy vyhodnotily jako úplně jiné osoby. Dle tvůrců může být tento typ útoku využit nejen k získávání přístupu do



různých zařízení a systémů, ale také v případě vytváření pokročilých „deep fakes“, jejichž rozlišení by mohlo být problémem pro řadu v současné době dostupných nástrojů. Tento útok dokáže překonat většinu služeb, aplikací a API pro rozpoznávání obličejů. Výzkumný tým toto demonstroval na útoku proti PimEyes, což je jeden z nejpokročilejších online nástrojů pro rozpoznávání obličejů.

Komentář: Odemykání zařízení a služeb pomocí snímku obličeje se již v minulosti stalo častým terčem nových typů útoků. Předkládaný typ útoku směřuje především na algoritmy umělé inteligence, které jsou k rozpoznávání obličeje využívány. Právě nové typy útoků, které využívají slabin v umělé inteligenci by měly stát v popředí současné pozornosti výzkumné komunity v oblasti kybernetické bezpečnosti, neboť stále více roste počet zařízení a systémů využívajících umělou inteligenci.

Zdroj: Petr Martinek, NÚKIB/ Adversa AI

Celý článek si přečtete zde ▶