Novinky v oblasti výzkumu a vývoje v kybernetické bezpečnosti

VEŘEJNÁ PODPORA

Program DELTA2

Technologická agentura České republiky vyhlásila dne 12. května 2021 třetí veřejnou soutěž v Programu na podporu aplikovaného výzkumu, experimentálního vývoje a inovací DELTA 2. Předmětem této veřejné soutěže je především podpora mezinárodní spolupráce skrze společné projekty subjektů podporovaných TAČR a zahraničních partnerů. Více informací o možnostech zapojení naleznete zde.

AKCE

Cybersecurity Festival

V průběhu následujícího června proběhne Cybersecurity festival a to ve třech různých termínech – 16., 23. a 30. 06. Tato akce je konferencí pro všechny profese a téměř všechny oblasti kybernetické bezpečnosti. Akce mimo jiné působí i jako síťovací akce pro odborníky z různých zemí. Registrace je zdarma a více informací můžete nalézt na tomto odkazu.

Program GAMA 2 – webinář

Technologická agentura České republiky bude pořádat online seminář k 3. veřejné soutěži Programu na podporu aplikovaného výzkumu, experimentálního vývoje a inovací GAMA 2, podprogram 2. Webinář proběhne 9. 6. 2021 od 10:00 do 12:00. Možnosti registrace a více informací naleznete zde.

Annual Privacy Forum 2021

ENISA, DG CONNECT a Univerzita v Oslu organizují další ročník konference za zaměřené na ochranu osobních údajů Annual Privacy Forum. Letošní ročník proběhne plně online a to 17. a 18. června. Více informací a možnost registrace naleznete na tomto odkazu.

PUBLIKACE

Nová strategie pro mezinárodní spolupráci v oblasti výzkumu a inovací

Evropská komise představila dne 18. 05. 2021 novou strategii pro mezinárodní spolupráci. Strategie potvrzuje závazek EU k zachování otevřenosti v mezinárodní spolupráci v oblasti výzkumu a inovací. Nový rámcový program Horizon Europe zůstává i nadále otevřen možnostem spolupráce pro země mimo EU. Dále strategie klade větší důraz na vyváženou spolupráci, oblast klimatu a životního prostředí, digitální transformaci nebo globální zdraví. Celou strategii naleznete na tomto odkazu.

Candidate EUCC Scheme V1.1.1

ENISA vydala novou aktualizovanou verzi Candidate EUCC Scheme, která je výsledkem komentářů a připomínek získaných od odborné veřejnosti. Aktualizace tak obsahuje nové a přesnější definice používaných pojmů, vyjasnění některých termínů nebo zjednodušení a aktualizaci některých příloh. Aktualizovanou verzi dokumentu naleznete zde.

DeepSloth – nový typ útoku směřující na systémy strojového učení

(25. 05. 2021; portswigger.net) Nový typ útoku, který směřuje výhradně na systémy strojového učení, vyvinuli výzkumníci z University of Maryland. DeepSloth útok se zaměřuje na využití slabiny v optimalizačním přístupu pro strojové učení nazývaném „multi-exit architectures“. Ten zjednodušeně funguje tak, že jakmile neuronová síť strojového učení dosáhne maximálních přípustných výpočetních hodnot tak se systém přestane daným problémem zabývat. DeepSloth útok však dokáže pozměnit vstupní data tak, aby nikdy nedošlo k předčasnému ukončení výpočetních úkonu daného problému. Systém umělé inteligence je tak přetěžován, což postupně vede k jeho zpomalení, nebo až k úplnému přetížení. V podstatě tedy DeepSloth útok funguje jako denial-of-service útok pro systémům umělé inteligence.

Komentář: Tento typ útoku představuje i podle autorů samotných v současné době spíše pouze teoretický příklad možností útoků proti systémům strojového učení. Přesto se jej autoři snaží využít k tomu, aby upozornili na podobné typy útoků, které se mohou vyskytovat i v budoucnu. Strojové učení je v současné době velmi rychle se rozvíjející oblast. Upozornění na podobné možnosti útoků nám tak může ukázat s jakými možnými bezpečnostními hrozbami se můžeme v kybernetické bezpečnosti v budoucnu potýkat.

Automatické hledání chyb v počítačových programech

(12. 05. 2021; gacr.cz) „Verifikace a hledání chyb v pokročilém softwaru“ bylo tématem vědců z VUT v Brně a Univerzity Karlovy. Vědci se ve svém projektu zabývali například analýzou a verifikací paralelních programů, které jsou v současné době velmi populární, nebo tzv. dynamickými datovými strukturami. Výzkumníci dokonce ověřili, že některé velmi jednoduché techniky vyhledávání chyb mohou být často mnohem efektivnější než složitější a komplexní přístupy. V průběhu projektu se vědcům podařilo vyvinout metody, které přispěly k rozšíření skupiny programů, které je možno automaticky analyzovat. Některé z těchto metod byly dokonce implementovány v prototypech softwarových nástrojů, které je možnost experimentálně nasadit i v praxi.

Komentář: Snaha o minimalizaci chyb v programech je vlastní jak komerční, tak akademické sféře. Důležitým tématem je to však i pro kybernetickou bezpečnost, protože právě chyby v programech představují častý přístupový bod útočníků do systému. Rozšíření možností automatizovaného vyhledávání chyb je tak skvělým přínosem. Tento výzkum je navíc i důkazem, že i v našem národním prostředí vzniká řada důležitých výzkumů, které mají přesah do kybernetické bezpečnosti.

PETR MARTINEK; p.martinek@nukib.cz
Oddělení výzkumu a evropské spolupráce, NÚKIB