NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

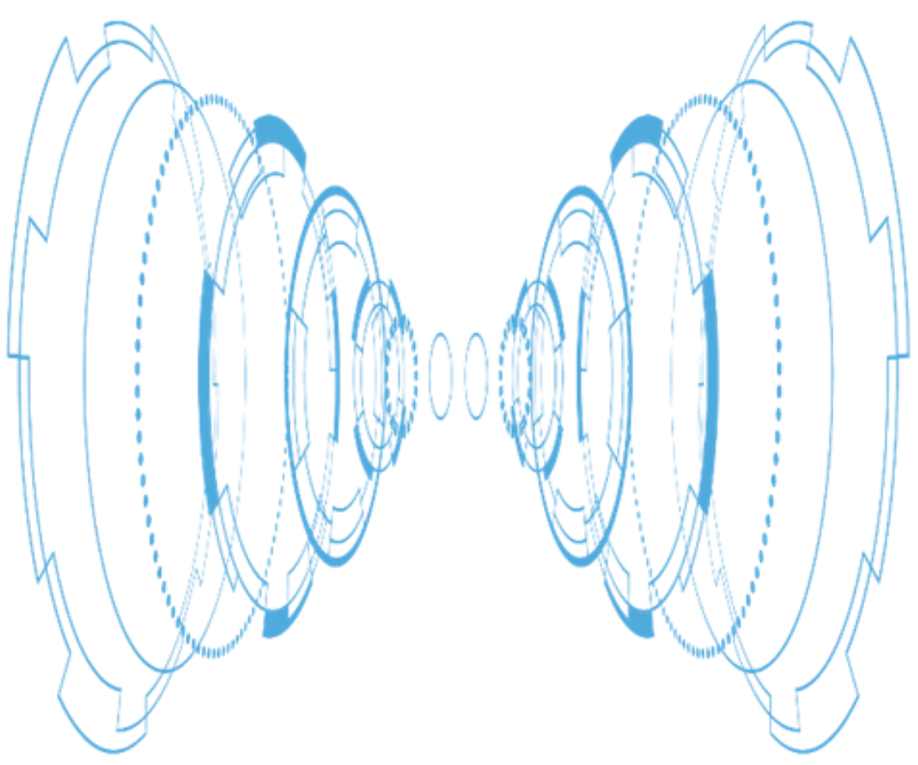
Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

01/2023

LEDEN

Rozšíření spolupráce Česka a USA v oblasti kybernetické bezpečnosti

Čeští vědci budou mít možnost efektivněji spolupracovat s těmi americkými na výzkumných a vývojových projektech týkajících se kybernetické bezpečnosti. Příležitostí pro vznik nových mezinárodních projektů přichází díky navázání spolupráce mezi Grantovou agenturou ČR a americkou grantovou agenturou National Science Foundation. Výše podpory na toto téma se bude pohybovat v řádu několika milionů korun ročně, přičemž náklady na jednotlivé projekty si budou jednotlivé agentury dělit.



NÚKIB součástí mezinárodního projektu CHESS Excellence Hubs

Ve dnech 26. - 27. ledna se v prostorách Kybernetického polygonu Masarykovy univerzity v Brně uskutečnilo úvodní setkání partnerů mezinárodního výzkumného projektu CHESS, na kterém se bude spolupodílet také NÚKIB. Projekt vychází z nového schéma evropského programu Horizont Evropa, známého jako Excellence Hubs, jehož cílem je posílit regionální inovační ekosystémy mezi členskými státy EU. CHESS si klade za úkol zformovat Excellence Hub se zaměřením na kybernetickou bezpečnost a propojit v této oblasti regiony Estonska a jižní Moravy.

Ministerstvo průmyslu a obchodu zintenzivňuje podporu výzkumu, vývoje, inovací a digitalizace

Rozšíření podpory výzkumných, vývojových a inovačních projektů ze strany Ministerstva průmyslu a obchodu navazuje na výzvu realizovanou v roce 2022. Celkový objem finančních prostředků alokovaných pro Operační program Technologie a aplikace pro konkurenceschopnost, zkráceně OP TAK, dosahuje 650 milionů korun. Podpora je zaměřena především na rozvoj výzkumných a vývojových aktivit malých a středních podniků. Balík má přispět nejen k intenzifikaci vývoje, ale také k posílení spolupráce mezi výzkumnou sférou a podniky. Zájemci o podporu se mohou obrátit na Agenturu pro podnikání a inovace, která jim pomůže s přípravou žádosti a administrací projektu.

Nezapomeňte

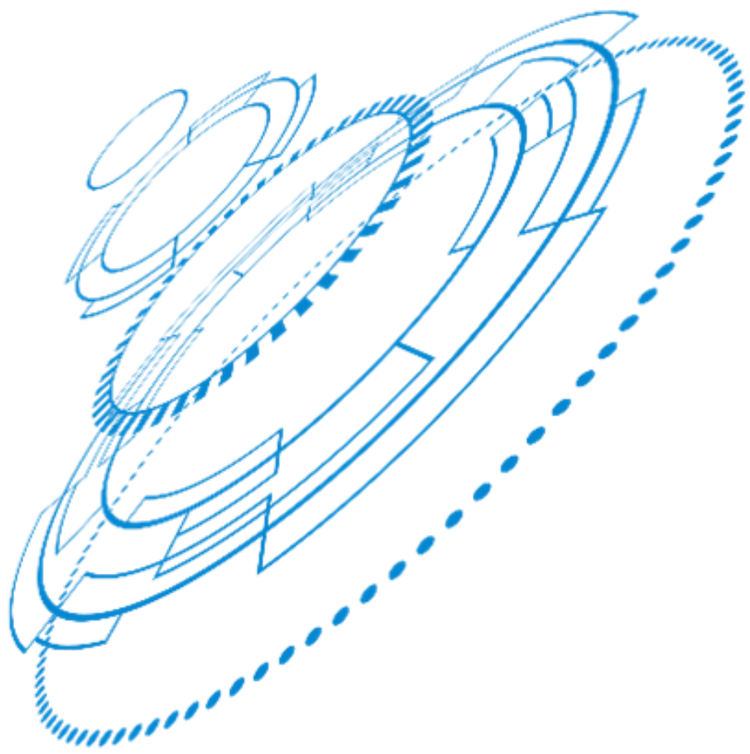
V minulém čísle Novinek z oblasti výzkumu a vývoje jsme Vás informovali o termínu předkládaní Identifikace výzkumných potřeb programu Ministerstva vnitra ČR (MV ČR), známého pod zkratkou SecPro, který byl stanoven na 15. únor 2023. MV ČR ovšem dne 20. ledna vydalo aktualizaci, která posunula uzávěrku procesu identifikace na 15. března.

Grantová agentura České republiky oznámila veřejné soutěže pro tento rok

Vypsání standardních projektů, mezinárodní projektů a projektů JUNIOR STAR a POSTDOC INDIVIDUAL FELLOWSHIP, které pravidelně vyhlašuje Grantová agentura České republiky je možné v tomto roce očekávat již v polovině února. Dále bude také v průběhu roku vyhlášena soutěž na principu LEAD a předpokládá se, že během letošního roku bude možné podávat společné projekty také s chorvatskými vědci. Naproti tomu soutěž EXPRO zaznamená roční přestávku a její obnovení se plánuje až pro rok 2024. Zadávací dokumentace jednotlivých soutěží neplánují žádné výrazné změny, a tudíž mohou zájemci o účast v některé z nich promýšlet své výzkumné projekty již nyní. Pokud máte zájem o podrobnější informace o jednotlivých soutěžích a podmínkách pro uchazeče, GA ČR připravila dva semináře s předsedou agentury prof. Petrem Baldrianem. První seminář se uskuteční 16. února v Praze, druhý poté 1. března v Brně.

ChatGPT odhalil potenciální bezpečnostní rizika spojená s dalším rozvojem umělé inteligence

Generative Pre-training Transformer představuje jazykový model vyvinutý společností OpenAI sídlící v kalifornském San Franciscu. Jedná se o neuronový model navržený a vycvičený k předpovídání slov v textu na základě jeho předchozího znění tak, aby věta zněla co nejpřirozeněji. Texty vytvořené ChatGPT jsou tedy téměř nerozeznatelné od těch lidských, a navíc je lze vytvářet prakticky v jakémkoli jazyce, včetně češtiny. Pokrok ve vývoji umělé inteligence v podobě ChatGPT však také upozornil na bezpečnostní rizika a možné formy zneužití, které tato technologie přináší. Možnost reagovat na komentáře, články nebo přepisy veřejných výstupů bez nutnosti lidského zásahu otevírá prostor například pro lobbing. Miliony souběžně probíhajících interakcí totiž mohou vytvářet dojem existence určité zájmové skupiny, jejímž prostřednictvím lze vytvářet tlak na dosažení určitých ideologických nebo politických cílů. Mnohem závažnější jsou pak kybernetické zločiny, které ChatGPT za svou relativně krátkou existenci dokázal usnadnit. Volného přístupu k němu totiž využili hackeři, kteří pomocí umělé inteligence vytvořili škodlivý software určený k dalšímu šíření.



Nové optické vlákno chrání data i po ohnutí

Výzkumníci z britské University of Bath vyvinuli optické vlákno, které je schopné chránit datové toky i před fyzickým poškozením způsobeným zkroucením nebo ohnutím. Pomocí matematického konceptu topologie také zajišťují, že vlákno zachovává vysokorychlostní přenos informací i na velké vzdálenosti. V optických sítích tvoří optická vlákna kanál, kterým proudí data ve formě světla, jakožto média pro přenos informací. V případě, že dojde k mechanickému poš-

kození při jejich přílišném prohnutí tok informací se zastaví. Nově vyvinuté optické vlákno ovšem brání vzniku takového poškození, a to především svou mimořádnou flexibilitou. Takto modifikovaná optická vlákna jsou také snadno škálovatelná, takže se jejich struktura nemění ani na vzdálenost tisíců kilometrů. Očekává se, že nové vlákno přispěje k rozšíření robustnosti optických sítí, které jsou klíčovou součástí dnešní informační infrastruktury a jejichž význam bude s nástupem kvantových technologií dále růst.

„Pokud si nejste jisti legitimitou webové stránky nebo e-mailu, můžete si rychle vyhledat, zda je ostatní nenahlásili jako podvodné,“

umělá inteligence ChatGPT

Projekt Evropské komise s názvem DNS4EU povede česká firma Whalebone

Společnost Whalebone se postaví na čelo třináctičlenného konsorcia rozloženého napříč deseti členskými státy Evropské unie, jehož společným cílem bude vytvořit evropskou alternativu k americkým veřejným DNS překladačům. Projekt DNS4EU by měl občanům, firmám a institucím v EU poskytnout bezpečnou a výkonnou rekurzivní "telefonní spojovatelku internetu". Historickou profesi telefonních spojovatelek si Evropská komise pro popis projektu vybrala z důvodu její výstižnosti směrem k povaze práce, kterou DNS překladače, nazývané také resolvery, vykonávají. Tato

technologie totiž zajišťuje převod textové domény zadané do prohlížeče na číselný řetězec, se kterým pak prohlížeč pracuje. Zjednodušeně řečeno poskytuje "spojení" mezi lidsky srozumitelným textem a sadou čísel zpracovatelnou webovým vyhledávačem. Nejvýznamnějším rozdílem oproti v současnosti nejpoužívanějším DNS resolverům od společností Google nebo IBM je možnost procházet web pouze pomocí doménových jmen bez nutnosti jejich transformace na řetězce čísel. Projekt počítá s využitím stávající infrastruktury telekomunikačních operátorů a poskytovatelů internetu. Českou stopu obsahuje také další klíčová složka projektu, neboť škodlivé internetové domény bude monitorovat umělá neuronová síť vyvinutá ve spolupráci s ČVUT.

Vývoj PlugX je stále živý a zůstává aktivní hrozbou

Odborníci na kybernetickou bezpečnost ze společnosti Palo Alto Networks odhalili škodlivý software PlugX, který infikuje připojená vyměnitelná média USB s cílem šířit se do dalších systémů. Společnost uvedla, že malware objevila při reakci na ransomwarový útok Black Basta. Varianta PlugX s vazbou na USB je pozoruhodná tím, že používá specifický symbol Unicode zvaný non-breaking space (U+00A0) pro skrytí souborů na vyměnitelném zařízení připojeném k pracovní stanici. Po připojení infikovaného USB má PlugX za úkol nejen implantovat malware do hostitelského počítače, ale také zkopírovat sám sebe do jakéhokoli vyměnitelného zařízení, které je k hostiteli připojené. V něm se zamaskuje do nové složky předstírající, že je „Koš". Tento postup následně funguje díky tomu, že „Průzkumník souborů systému Windows“ ve výchozím nastavení nezobrazuje "Skryté položky". Malware toho využívá a při zapnutém výchozím nastavení se jeho škodlivé soubory, které jsou uloženy v „Koši“, nezobrazují. Další varianta PlugX pak dokáže také stahovat a ukládat všechny soubory Adobe PDF a Microsoft Word z hostitelského počítače do jiného skrytého souboru na infikovaném USB.

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Kontaktní informace

01/2023

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31

616 00 Brno

Tel.: +420 541 110 777

P.O. BOX 17, Brno 16, CZ 616 00

Oddělení vědy, výzkumu a inovací

Olšanská 36/9

130 00 Praha

Tel.: +420 607 032 806

e-mail: a.janovec@nukib.cz