NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

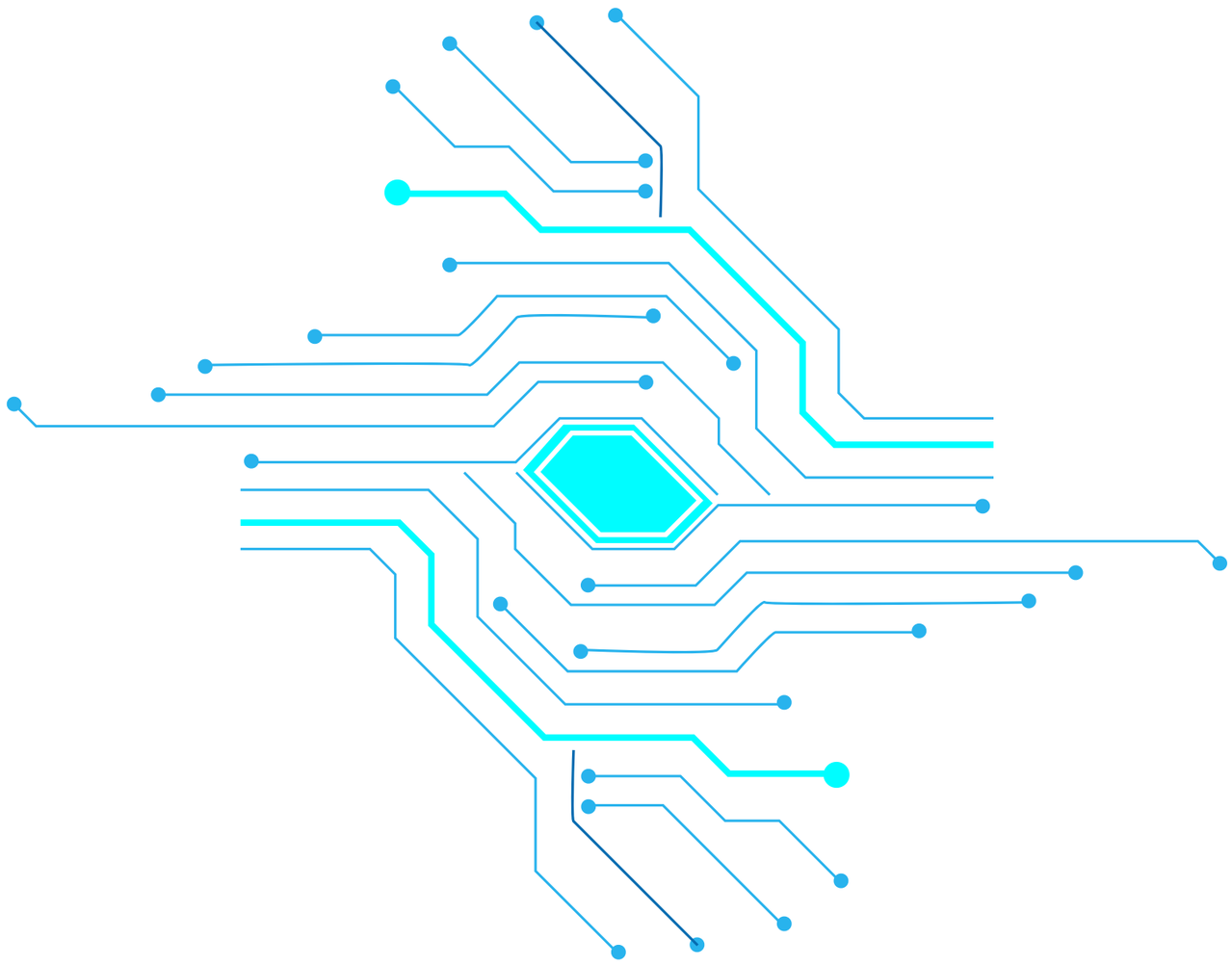
Aktuality ve výzkumu a vývoji v kybernetické bezpečnosti

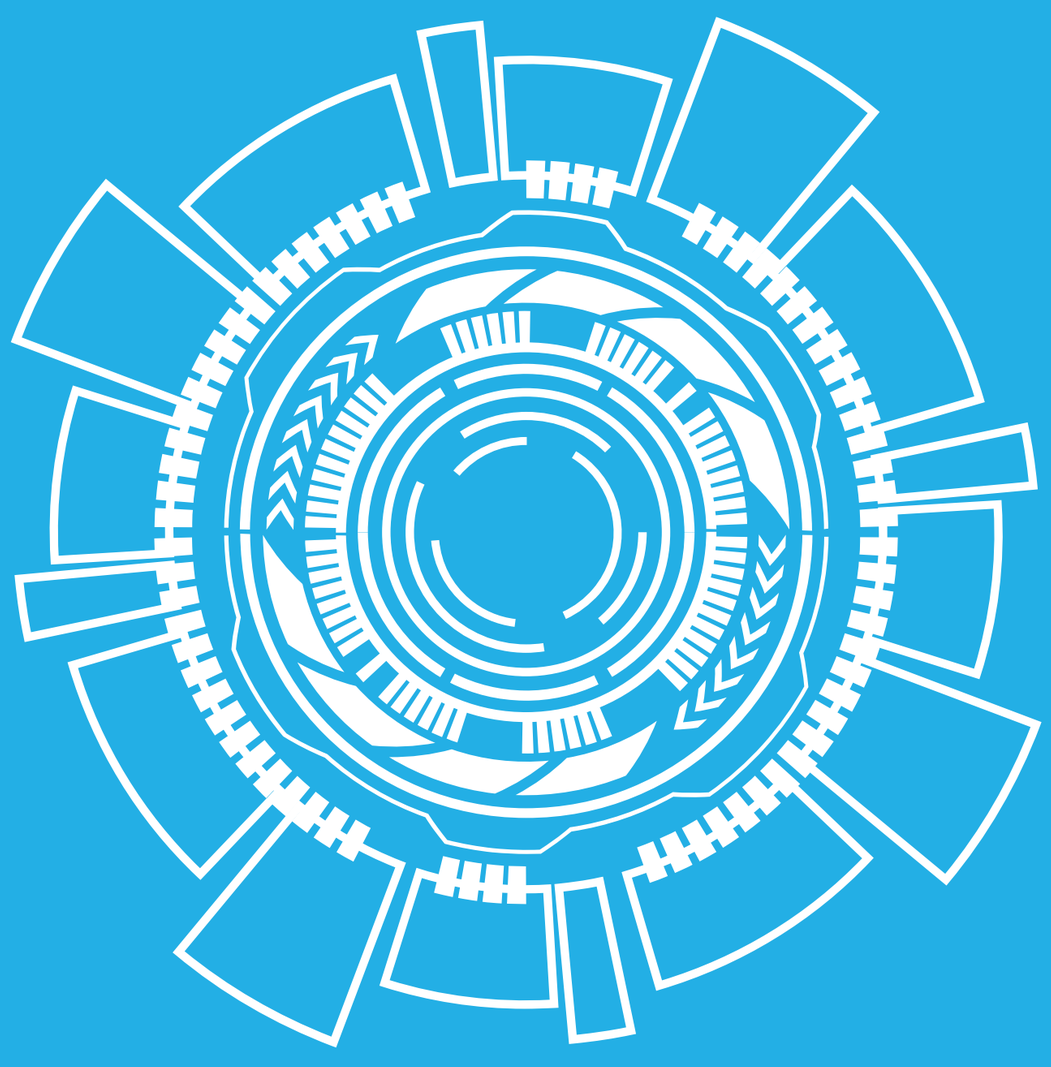
07/2024

ČERVENEC

Odstartovala Letní akademie Cybersecurity Twister

EDIH Cybersecurity Innovation Hub (EDIH CSH) pořádá od 10. července 2024 letní akademii Cybersecurity Twister. EDIH CSH se zaměřuje na podporu znalostí a dovedností v oblasti kybernetické bezpečnosti pro veřejné organizace a malé a střední podniky. Akademie nabídne celkově čtyři online školení po čtyřech hodinách od předních univerzitních expertů, a to každou druhou prázdninovou středu od 8:30 do 13:00 na platformě MS Teams. Účastníci se mají možnost dozvědět o útočnících v kyberprostoru, obraně proti útokům, kombinacích online a fyzických útoků a aktuálních kyberbezpečnostních trendech.



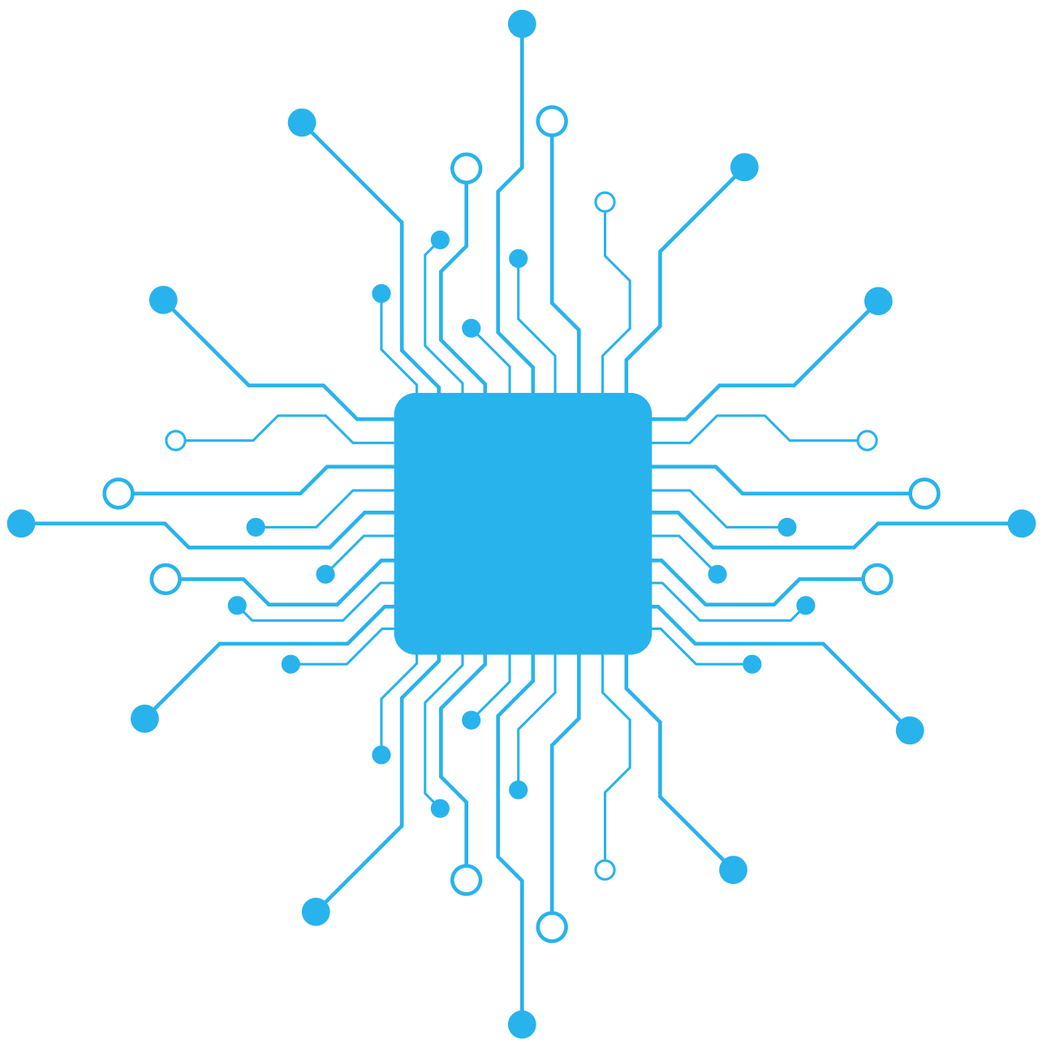


Národní strategie kybernetické bezpečnosti je otevřená veřejnému připomínkování

Národní úřad pro kybernetickou a informační bezpečnost zahájil proces přípravy nové Národní strategie kybernetické bezpečnosti (NSKB) a vybízí veřejnost, aby se aktivně zapojila do této iniciativy. Tento krok představuje příležitost pro jednotlivce a organizace přispět svými nápady a poznatky, které mohou ovlivnit budoucí směřování kybernetické bezpečnosti České republiky. NÚKIB sbírá vstupy zejména v oblasti budoucích hrozeb a silných a slabých stránek systému. Apelováno může být i na větší důraz NSKB na vědecko-výzkumné aktivity.

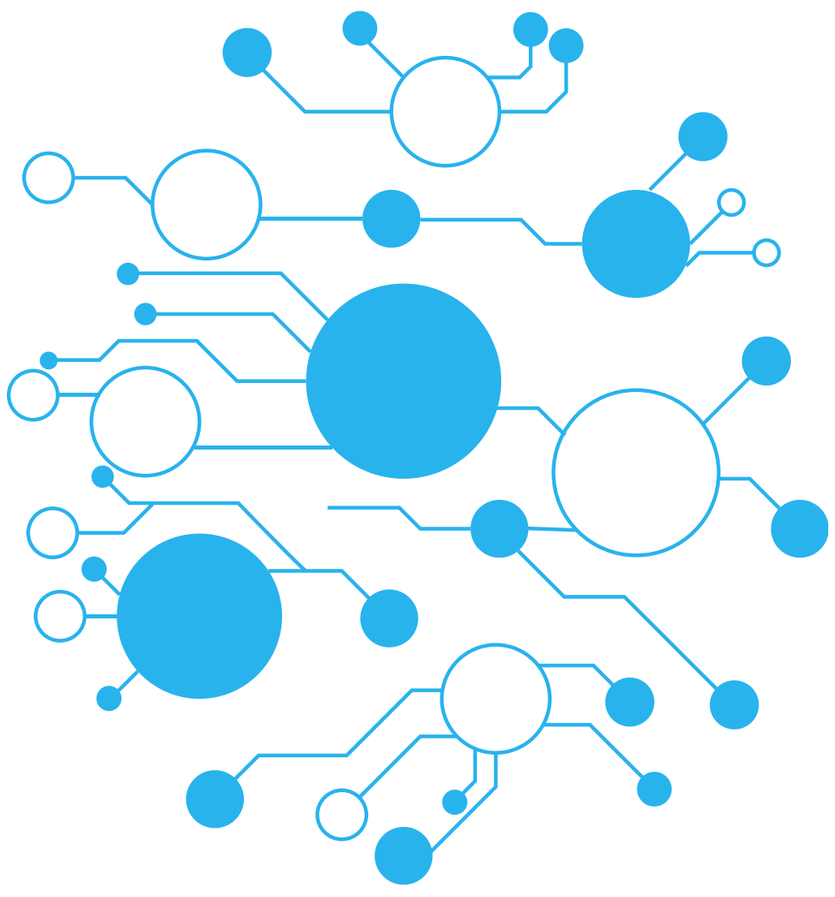
CERIS připravuje výroční akci o výzkumu v boji proti trestné činnosti a terorismu

Akce pořádaná Komunitou pro evropský výzkum a inovace v bezpečnosti (CERIS) se letos zaměří na témata online škod a zapojení odborníků z praxe do bezpečnostního výzkumu. Pravidelně pořádaná akce zaměřená na průřezová témata v oblasti bezpečnostního výzkumu má za cíl podpořit sdílení zkušeností, identifikovat úspěchy a posílit spolupráci na evropské úrovni. První den se zaměří na zkoumání současných a budoucích technik pro způsobení online škod a vlivu AI Act na boj proti online zločinu. Druhý den je věnován výzvám, se kterými se odborníci a výzkumníci potýkají při své účasti ve výzkumných konsorciích, včetně diskuze o příkladech dobré praxe. Akce s **otevřenou registrací** se uskuteční v Bruselu 24. - 25. září 2024.



Byly oznámeny společné projekty EU a Korejské republiky v oblasti vývoje a výroby čipů

Evropská unie a Jižní Korea oznámily podporu čtyř společných projektů v oblasti vývoje polovodičů s celkovou investicí přibližně 12 milionů EUR, přičemž polovina finančních prostředků bude pocházet z EU a druhá polovina z Národní výzkumné nadace Koreje (NRF). Projekty mají rozvinout široké spektrum poznatků z různých oblastí od heterogenní integrace až po neuromorfní computing. Projekty nesou název ENERGIZE (energeticky úsporné obvody bez centralizovaných datových bodů), NEHIL (laserový radar pro vysoko efektivní a přesné měření), HAETAE (čipy využívající světlo k přenosu dat) a ViTFOX (čip pro zlepšení efektivity a výkonu u AI zpracovávající vizuální data). Iniciativa bude trvat tři roky a má za cíl posílit spolupráci a inovace mezi EU a Jižní Koreou.



Výstupy z ECCC Info Day k aktuálním výzvám DEP

Evropské kompetenční centrum (ECCC) uspořádalo 9. července 2024 v Bruselu Info den k tématu aktuálně otevřených výzev v programu Digitální Evropa (DEP) v oblasti kybernetické bezpečnosti. V rámci akce bylo řešeno téma procesu hodnocení způsobilosti žadatelů, dále byly sdíleny tipy, jak napsat úspěšný projekt a diskutována byla taktéž zkušenost s řízením DEP projektů z pozice úspěšných projektových koordinátorů. Prostor byl také věnován roli Národních koordinačních center (NKC) v kyberbezpečnostním ekosystému. ECCC nyní sdílelo výstupy z akce (prezentace a záznamy vystoupení), které jsou k dispozici na webových stránkách ECCC.

Save the Date: konference na téma evropských certifikací

Národní úřad pro kybernetickou a informační bezpečnost připravuje konferenci na téma evropských certifikací kybernetické bezpečnosti, kde se mimo jiné můžete těšit na představení projektu TEST-CERT-CZ, který se zaměřuje na budování testovacích a certifikačních kapacit v ČR. Konference se uskuteční 14. listopadu 2024. Pro pravidelný odběr aktuálních informací o akci stačí vyplnit krátký formulář.

Vědeli jste, ŽE...

...vítězkou ocenění European Inventor Award 2024 v kategorii Výzkum se stala počítačová vědkyně pracující s umělou inteligencí, Cordelia Schmidt? Toto ocenění, které uděluje European Patent Office již od roku 2006, vzdává hold výzkumníkům, vědcům a badatelům s vášní pro nové objevy a inovace. Kategorie Výzkum oceňuje vynálezce působící v akademických a výzkumných institucích, jejichž vynálezy vedou k technologickému pokroku a rovněž zvyšují reputaci instituce. Schmidt z INRIA se zabývá směřováním AI za hranice základního rozpoznávání objektů až k chápání kontextu vizuálních scén, interpretací lidského jednání a dokonce předpovídání budoucích událostí ve videu.

Čeští vědci transformují počítačové viry do podoby vizuálních obrazců a následně učí umělou inteligenci je rozpoznávat

Vědci z Fakulty elektrotechniky a informatiky (FEI) Vysoké školy Báňské v Ostravě vyvinuli inovativní metodu, která propojuje zákonitosti fraktální geometrie s využitím v kybernetické bezpečnosti. Jejich výzkum se zaměřil na vizualizaci počítačových virů a malware pomocí fraktálních obrazců, které umělá inteligence využívá k rozpoznávání nebezpečného software. Metoda je založena na převodu dynamického chování malware na vizuální obrazce, které AI dále analyzuje a učí se je rozpoznávat. Po zpracování přibližně 130 000 obrázků dokázala AI rozpoznat malware až s úspěšností 91 % a stále dochází k jejímu zlepšování a zpřesňování. Tato technika nejen, že zvyšuje přesnost detekce malware, ale také přináší možnost získávat nové poznatky o jeho chování. Vědecký tým, který za metodou stojí, plánuje ve výzkumu pokračovat a rozšířit ji o statické analýzy se zaměřením na rychlejší odhalování škodlivých software. Využití fraktální geometrie představuje novou metodu vizualizace kybernetických hrozeb, přičemž rovněž přispívá k rozvoji tohoto odvětví. Významný přínos totiž spočívá také v pomoci při vývoji nových bezpečnostních nástrojů a strategií, které se lépe přizpůsobí aktuálním trendům v kybernetických útocích. Metoda má tedy potenciál přispět nejen k zlepšení bezpečnostních postupů, ale také k rozvoji interdisciplinárního přístupu v oblasti kybernetické bezpečnosti, který zahrnuje matematiku, umění a informatiku.

Bylo vyvinuto elektronické zařízení klíčové pro umožnění masivního nástupu sítí 6G

Portál Nature Electronics v červenci zveřejnil výzkum katedry telekomunikací a systémového inženýrství Barcelonské univerzity, který se zabýval vývojem nového spínače užívaného v telekomunikačních zařízeních, který je schopný pracovat na velmi vysokých frekvencích s nižší spotřebou energie než již existující zařízení. Tento pokrok je významný pro nástup 6G sítí a navíc je provozován v souladu s evropskými podmínkami udržitelnosti. Na rozdíl od momentálně nejrozšířenějších spínačů využívaných v elektronických komunikačních zařízeních vyrobených z křemíku, nově vyvinuté spínače určené k ovládání signálů jsou vyrobeny z netěkavého materiálu zvaného hexagonální nitrid bóru. Oproti křemíkovým spínačům jsou schopné provozu na dvojnásobné operační frekvenci, nevyžadují konstantní připojení k napětí a k jejich aktivaci postačuje jednorázový impuls.

Chladicí systém nové generace pomůže datovým centrům zvýšit jejich energetickou účinnost

Udržování datových center provozujících vysoce výkonné počítače, na nichž běží systémy AI, vyžaduje obrovské množství energie k jejich chlazení. Výzkumníci z University of Missouri navrhli nový typ chladící technologie, který je schopný operovat s významně nižší spotřebou energie než dosud využívané technologie. Univerzitní výzkumný tým vyvíjí dvoufázový chladící systém schopný odvádět teplo z čipových serverů prostřednictvím změny fáze. V případě využití pouze části výkonu je systém v některých případech schopen fungovat dokonce téměř energeticky pasivně. Tato práce je v souladu s cíli Centra pro energetické inovace, a tak v jejich spolupráci vznikají v rámci univerzitního kampusu budovy umožňující další mezioborové zkoumání energetických problémů spojených s nárůstem využívání AI.

Chatbot na bázi umělé inteligence láká podvodníky a zároveň sbírá informace o jejich nekalých praktikách

Během posledních dvou let výzkumníci z britské firmy Netcraft zkoumali nová využití pro umělou inteligenci na obranu proti podvodům. Experiment ukázal, jak může AI zvrátit situaci s kyberzločinci tím, že získá citlivé informace o jejich finančních podvodech. Firma Netcraft použila pokročilý chatbot založený na OpenAI ChatGPT k interakci se tzv. scammery (podvodníky). Chatboty simulují pozici potenciální oběti scammerů a lákají útočníky, aby se pokusili získat jejich citlivá data. Chatboty reagují na e-mailové zprávy určené k získání zpravidla finančních prostředků od oběti a komunikují s útočníkem tak dlouho, až prozradí důležité informace o své vlastní kriminální činnosti. V rámci testování dokázaly chatboty tímto způsobem odhalit zločineckou infrastrukturu tvořenou bankovními údaji z více než 600 finančních institucí v 73 zemích, které jsou využívány k převodu ukradených peněz. Odhaleny byly tisíce účtů podvodníků, přičemž většina z nich byla lokalizována v USA a Velké Británii. V rámci průměrné konverzace odeslali kyberzločinci 32 zpráv, na které jim chatbot 15krát odpověděl. Experiment naznačuje, že AI chatboty se v budoucnu mohou stát důležitým strategickým prvkem v monitorování phishingových útoků a obraně proti scammerům. Netcraft plánuje postupně do modelu přidávat další jazyky, čímž bude jeho účinnost rozšířena i mimo anglojazyčné geografické lokality.

„Vzhledem k tomu, že se oblast kybernetické bezpečnosti vyvíjí a stále se objevují nové hrozby, budou podobné interdisciplinární metody zásadní pro to, abychom si před těmito nebezpečími zachovali náskok.”

Ivan Zelinka
profesor FEI VŠB-TUO

Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Kontaktní informace

07/2024

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: vyzkum@nukib.gov.cz