Platforma pro výzkum a vývoj v kybernetické a informační bezpečnosti

15. 11. 2023
CyberSecurity Hub
CERIT Science Park II (CSP II), Šumavská 416/15 | 602 00 | Brno

Výstupy sedmého jednání Platformy

Dne 15. listopadu 2023 proběhlo v prostorách vědecko-technického parku CERIT Science Park II již sedmé jednání Platformy pro výzkum a vývoj v kybernetické a informační bezpečnosti, které bylo zorganizováno ve spolupráci s ústavem CyberSecurity Hub (CSH). Činnost Platformy je zaštitována Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). Ústředním tématem jednání byla multidisciplinarita v oblasti výzkumu a vývoje v kybernetické bezpečnosti. Jednaní Platformy se zúčastnili zástupci veřejného sektoru (Ministerstvo průmyslu a obchodu, Digitální a informační agentura, Bezpečnostní a informační služba, Ministerstvo obrany, Technologické centrum Praha, Armáda ČR, Policie ČR), soukromého sektoru (Progress, CISCO, IBM, ESET, Greycortex, ČEPS, JIC) a výzkumných organizací (Masarykovy univerzity, České učení technické v Praze, Vysoké učení technické v Brně, Vysoká škola ekonomická, CESNET). Členové Platformy mezi sebou přivítali nové členy z řad Univerzity Pardubice, Univerzity Tomáše Bati ve Zlíně a Západočeské univerzity v Plzni. Národní výzkumná komunita se rozšířila i v řadách soukromého sektoru, kdy se jednání zúčastnila také První certifikační autorita nebo společnost Tropic Square.

Na úvod jednání přivítali účastníky náměstek ředitele NÚKIB Pavel Štěpáník, který vyzdvihl potřebu posilování vzájemné informovanosti a spolupráce mezi aktéry v oblasti výzkumu a vývoje v kybernetické bezpečnosti, a ředitel CSH, Roman Čermák, který v rámci svého vstupu představil činnosti CSH a prostor Cyber Campus CZ, jež v sobě sdružuje klíčové subjekty, kompetence, aktivity i infrastrukturu v oblasti kybernetické a informační bezpečnosti.

Dopolední část programu byla věnována prezentacím. Nikola Chvátalová z Oddělení vědy, výzkumu a inovací NÚKIB představila činnosti Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost (ECCC) a Národního koordinačního centra výzkumu a vývoje v oblasti kybernetické bezpečnosti (NKC), kdy se zaměřila na aktuální priority obou center a představení dvou projektů NÚKIB zaměřených na vybudování NKC v ČR a podporu budování testovacích a certifikačních schopností. Lenka Škrábalová, vedoucí Oddělení digitální ekonomiky a společnosti Ministerstva průmyslu a obchodu, se ve svém příspěvku zaměřila na unijní finanční program Digitální Evropa (DEP), kdy účastníkům představila činnost evropských digitálních inovačních center, aktuální pracovní programy a plánované výzvy DEP. Dopolední blok zakončil vstup Aleny Turoňové z Oddělení multilaterální spolupráce NÚKIB z Bruselu, která účastníky seznámila s aktuálním děním v oblasti kybernetické bezpečnosti na poli EU a rolí zástupců NÚKIB v Bruselu.

Platforma pro výzkum a vývoj v kybernetické a informační bezpečnosti

Zbývající program přinesl tři panelové diskuze moderované zástupci NÚKIB, kde spolu diskutovali odborníci z řad soukromého sektoru, veřejné správy a akademické sféry.

První z panelových diskuzí se zabývala tématem role státu v oblasti strategického rámce a podpory výzkumu a vývoje v oblasti kybernetické bezpečnosti. Ta nejenže přiblížila proces formování národních strategií v oblasti výzkumu a vývoje v kybernetické a informační bezpečnosti, ale také umožnila diskutujícím prezentovat svoje postoje a vnímání budoucího směřování státu a jeho priorit v této oblasti. Diskuzního panelu, který moderoval Tomáš Kellner z Oddělení národních strategií a politik NÚKIB, se zúčastnili Veronika Kramaříková z ČVUT, David Komárek z Oddělení multilaterální spolupráce NÚKIB, Pavel Burian z Digitální a informační agentury a Pavel Minařík z Progress Software. Účastníci se shodli na potřebě schopnosti státu jasně definovat zájmové oblasti a cíle a vytvářet podmínky pro spolupráci napříč zmíněnými sektory. Za hlavní priority v oblasti výzkumu a vývoje (VaV) v kybernetické a informační bezpečnosti vytyčili například umělou inteligenci a kvantové technologie.

- Veronika Kramaříková zdůraznila potřebu vycházet při přípravě Národní strategie kybernetické bezpečnosti z již zpracovaných strategií a podkladů, zaměřit se na oblasti, ve kterých je ČR silná, a na schopnost státu definovat strategické cíle; z témat, která by měla být v Národní strategii reflektována, zmínila satelitní komunikaci, sociální inženýrství, a uživatelskou bezpečnost v otázce možného vzniku nového programu na podporu VaV v kybernetické bezpečnosti konstatovala, že je spíše na místě udělat revizi stávajících výzkumných programů;
- Pavel Minařík za klíčová témata označil kvantové počítání a včasnou detekci incidentů s důrazem na schopnost automatizovaných reakcí skrze uplatnění umělé inteligence a zabezpečení systémů s využitím přístupu security-by-design; v otázce podpory VaV upozornil na roztříštěnost dotačních programů v oblasti kybernetické bezpečnosti na národní úrovni a odlišnou úroveň administrativní náročnosti, kdy z pohledu firem je upřednostňován jednotný rámec této podpory včetně požadavků při podávání žádostí a implementaci;
- Pavel Burian zdůraznil potřebu spolupráce a navrhl, aby strategický rámec reflektoval tuto potřebu a nastavil mechanismus sdílení mezi sektory, uvedl také, že spolupráce s dalšími sektory je pro stát klíčová skrze schopnost produkovat efektivní řešení, jež posouvají celonárodní výzkumné prostředí;
- David Komárek se zohledněním priorit aktuálně řešených na unijní úrovni v oblasti relevantních témat vyzdvihl například rostoucí potřebu zabezpečení přenosu signálu mezi zemí a satelity vyslanými na oběžnou dráhu a podtrhl zájem státu o reflektovaní potřeb dalších sektorů, ovšem se zachováním pevného postavení státních institucí při určování klíčových oblastí výzkumu a vývoje.

Platforma pro výzkum a vývoj v kybernetické a informační bezpečnosti

Druhá z panelových diskuzí se zabývala tématem rizik spojených s přechodem ke kvantově odolné kryptografii. Panelu se zúčastnili Bohuslav Rudolf z Pracovní skupiny kryptologických analýz NÚKIB, Miloš Soukup ze společnosti IBM, Rudolf Vohnout ze sdružení CESNET a Jan Bouda z Fakulty informatiky Masarykovy univerzity. Diskuzi moderoval Luboš Fendrych, vedoucí Oddělení vědy, výzkumu a inovací z NÚKIB. Diskutovalo se o reálnosti kvantové hrozby a lišících se predikcích, časovém rámci přechodu na kvantově odolnou kryptografii a souvisejících rizicích a výhodách jednotlivých typů post-kvantového šifrování a jejich využití. Zmíněny byly také strategické projekty v oblasti budování kvantové komunikační infrastruktury na národní úrovni s přesahem do EU.

- Miloš Soukup upozornil na dlouhou dobu, kterou by organizacím trvalo přejít na post-kvantovou kryptografii a v této souvislosti zdůraznil potřebu přípravy na tento přechod, zároveň zdůraznil potřebu nasměrovaní výzkumu a vývoje ze strany státu na témata, které považuje za nejdůležitější;
- Jan Bouda upozornil na zaostávání ČR v oblasti kvantových technologií, přičemž zdůraznil potřebu jejich podpory ze strany státu, kde v současnosti existuje významný prostor pro výrazné zlepšení jak na národní, tak unijní úrovni;
- Rudolf Vohnout uvedl, že v rámci EU disponujeme dostatkem odborníků na kvantové technologie, je však potřeba více podporovat výzkum a vývoj v této oblasti, konkrétně zmínil potřebu vyšší podpory start-upů působících v této oblasti ze strany EU;
- Bohuslav Rudolf zdůraznil potřebu obezřetnosti vůči QKD, jakožto širokospektrálnímu řešení, a také podpořil vytváření systémových doporučení a postupů napříč celou národní výzkumnou komunitou.

Po přestávce následoval poslední odpolední panel zaměřený na vzdělávaní a cvičení na poli kybernetické a informační bezpečnosti. Panelu se zúčastnili Andrea Konopásková ze společnosti Cisco, Jan Vykopal z Fakulty informatiky Masarykovy univerzity a Jakub Čegan ze CyberSecurity Hub. Diskuzi moderovala ředitelka odboru cvičení a vzdělávání NÚKIB Alena Tovarňák Leciánová. Úvodem panelové diskuze představil Jakub Čegan projekt REWIRE zaměřený na oblast dovedností v oblasti kybernetické bezpečnosti, jehož cílem je mimo jiné snižovat kvalifikační rozdíly, dále prezentoval činnost platformy KYPO a evropský kvalifikační rámec European Cybersecurity Skills Framework (ECSF). Následně byly diskutovány inovativní přístupy ke vzdělávání v této oblasti, téma ECSF a otázka měření úspěšnosti vzdělávacích aktivit. V této souvislosti se účastníci shodli na tom, že nástroje a metodologie měření sice existují, nemáme však k dispozici neomezené množství kontrolních skupin a je třeba zohlednit přesnost takových dat a rozdíl mezi teoretickou a praktickou znalostí uživatelů.

Platforma pro výzkum a vývoj v kybernetické a informační bezpečnosti

- Jan Vykopal v oblasti inovativních přístupů ke vzdělávání zmínil například trend automatizace simulace kybernetických incidentů a využití velkých jazykových modelů pro generování scénářů i obsahu cvičení, které je možné přizpůsobit různým věkovým kategoriím a potřebám organizací, z jeho pohledu se státu daří definovat strategické cíle, nedostatky však spatřuje například v absenci systémovější podpory pro vznik vzdělávacího obsahu v návaznosti na poskytnutí podpory pro vývoj některé z nových technologií;
- Andrea Konopásková vyzdvihla spolupráci v rámci kyber komunity vzniklé okolo KYBERCENTRA, v oblasti vzdělávání upozornila na potřebu přizpůsobení aktivit různým věkovým kategoriím, kdy vyzdvihla projekt Kyberpohádky, který je určen ke vzdělávaní dětí v mateřských školách, podotkla také, že organizace chtějí čím dál více měřit, zda poskytnuté vzdělávání přineslo nějaký efekt, upozornila však na rozdíl mezi teoretickou a praktickou znalostí
- Jakub Čegan hovořil o trendu pořádání multidisciplinárních cvičení s přesahem do jiných oborů a měření vlivu stresu a práce pod tlakem při řešení krizových situací účastníky; v otázce podpory vzdělávacích aktivit hlavní nedostatek spatřuje v nedostatečném financování udržitelnosti již podpořených projektů ze strany EU.

V závěru programu poděkovali zástupci NÚKIB všem prezentujícím a účastníkům za jejich účast a aktivní zapojení do diskuzí. Příští setkání členů Platformy je předběžně plánováno na jaro roku 2024 do Prahy. NÚKIB uvítá od členů Platformy jakékoliv podněty k činnosti Platformy, návrhy témat k diskuzi i dalších partnerů k zapojení.

Platforma pro výzkum a vývoj v kybernetické a informační bezpečnosti

15. 11. 2023
CyberSecurity Hub
CERIT Science Park II (CSP II), Šumavská 416/15 | 602 00 | Brno

Medailonky účastníků panelových diskuzí

Role státu v oblasti strategického rámce a podpory výzkumu a vývoje v kybernetické bezpečnosti

Veronika Kramaříková (ČVUT)

Veronika Kramaříková je v současné době prorektorkou pro strategii a rozvoj ČVUT v Praze. Před tím působila 17 let ve státní správě a kromě jiného měla na starosti přípravu aktualizace RIS 3 strategie, vedla jeden z pilířů strategie Digitální Česko, a to pilíř Digitální společnost, a podílela se na tvorbě Národní strategie umělé inteligence, kterou vláda schválila v roce 2019. V současné době vede Národní inovační platformu pro digitalizaci v rámci RIS3 strategie.

Pavel Minařík (Progress Software)

Pavel Minařík původně působil jako technologický ředitel společnosti Flowmon Networks, která se po akvizici stala součástí Progress Software. V Progress Software v současnosti zastává roli vice-prezidenta pro technologie a vede tým experimentálního vývoje. Podílel se na 15 projektech VaV včetně H2020 projektů realizovaných ve spolupráci s akademickými partnery.

Pavel Burian (DIA)

Pavel Burian působí v rámci Digitální a informační agentury. Pracuje na odboru hlavního architekta, kde vykonává pozici manažera kybernetické bezpečnosti. Digitální a informační agentura se věnuje digitalizaci státní správy a implementaci informačních systému veřejné správy.

Přechod ke kvantově odolné kryptografii – teorie a praxe

Jan Bouda (Sherpa EuroQCI ČR)

Jan Bouda je výzkumným pracovníkem na Katedře počítačových systémů a komunikací Fakulty informatiky Masarykovy univerzity. Participuje na mnohých projektech v oblasti kvantových technologií a kryptografie na národní úrovni.

Miloš Soukup (IBM)

Miloš Soukup v současnosti působí jako bezpečnostní specialista a Quantum Ambassador ve společnosti IBM. Zapojuje se do řady aktivit v oblasti post-kvantové kryptografie včetně implementací navrhovaných kryptografických algoritmů na prostředcích IBM. Absolvoval dvě vysoké školy a v minulosti působil na několika manažerských a technických pozicích zaměřených na kybernetickou bezpečnost ve firmách Indra, Kapsch a S&T.

Rudolf Vohnout (CESNET)

Rudolf Vohnout pracuje ve sdružení vysokých škol a Akademie věd České republiky CESNET, kde působí na oddělení optických sítí a věnuje se počítačovým sítím a jejich bezpečnostním aspektům, optimalizaci sítí, optickým přenosovým systémům a kvantové distribuci klíčů.

Vzdělávání a cvičení na poli kybernetické a informační bezpečnosti

Andrea Konopásková (CISCO)

Andrea Konopásková 9 let vedla školicí centra u nadnárodního IT distributora. Nyní působí ve společnosti Cisco Systems, kde má na starosti veřejný sektor. Je místopředsedkyní středoškolské soutěže v kybernetické bezpečnosti.

Jakub Čegan (CSH)

Jakub Čegan se od roku 2015 věnuje technickým kyberbezpečnostním cvičením. V současné době je manažerem platformy KYPO Cyber Range. Zároveň působí v rámci oddělení oborové spolupráce Centra vzdělávání, výzkumu a inovací v oblasti informačních a komunikačních technologií na Fakultě informatiky Masarykovy univerzity.

Jan Vykopal (MUNI)

Jan Vykopal vyučuje kyberbezpečnost a zkoumá, jak ji učit lépe. Usiluje o praktické vzdělávání studentů i osvětu oboru. Využívá interaktivní výuková prostředí i metody, na jejichž tvorbě se podílí. Je také spoluzakladatelem Laboratoře kyberbezpečnosti Fakulty informatiky MU a udržuje odborné vazby s institucemi v Evropě, USA i v Asii.