

Kybernetická bezpečnost se dnes již neobejde bez spolupráce státního a soukromého sektoru, zaznělo opakovaně na konferenci NÚKIB

21.3.2024 - | Národní úřad pro kybernetickou a informační bezpečnost

Akce byla zahájena zdravicí, kterou pro účastníky PCSC natočil prezident České republiky Petr Pavel: „Prague Cyber Security Conference má za cíl podnítit debatu a sblížit nás při řešení výzev, kterým čelíme. Věřím, že tato diskuse přispěje budoucnosti kybernetické bezpečnosti nejen České republiky, ale celého demokratického světa.“ Na projev prezidenta Pavla navázala zdravice místopředsedkyně Evropské komise Evy Jourové, která ve svém projevu zdůraznila hrozbu v podobě malware a uvedla, že je k posílení kybernetické bezpečnosti nutná mezinárodní spolupráce. Stejnému tématu se věnovala ve svém příspěvku i Anne Neuberger z USA, National Deputy Security Advisor pro kybernetickou bezpečnost a přelomové technologie, která v kontextu malware vypíchla mezinárodní ransomware iniciativu a poděkovala partnerům, včetně České republiky, že k ní též patří.

Hosty konference pak osobně přivítal ředitel NÚKIB Lukáš Kintr: „Tato konference je víc než jen diskuse. Setkávají se zde odborné znalosti a myšlenky zaměřené na posílení odolnosti kybernetické bezpečnosti mezinárodní komunity.“ Ve svém projevu ředitel pořadající organizace hovořil dále o potřebě adaptovat se na změny v kyberbezpečnostním prostředí: „Dramaticky pozměněná globální bezpečnost vyžaduje, abychom jednali nyní, neboť již včera bylo pozdě. Abychom mohli čelit novým výzvám v kyberprostoru, je nutné změnit náš přístup k nebezpečným aktérům i k bezpečnosti jako takové. Ve světle stále se vyvíjejících výzev slouží tato konference jako důležitá platforma pro diskusi a sdílení zkušeností, znalostí, podporu mezinárodní spolupráce a prosazování inovativních řešení.“

Samotný diskusní program pak zahájil blok, ve kterém si účastníci akce připomněli Pražské návrhy k bezpečnosti 5G sítí z roku 2019, od jejichž vzniku a přijetí uběhlo pět let, a které jsou významným milníkem v celosvětovém úsilí o zajištění bezpečnosti sítí dalších generací. Další panelové diskuse se v obou dnech věnovaly jak okruhům napříč kybernetickou, tak informační bezpečností. Debaty tak reagovaly především na narůstající diverzitu hrozeb v kybernetickém prostoru a na rozvíjející se příležitosti spojené s vývojem nových technologií. Hovořilo se např. o bezpečnosti podmořských kabelů, které přenáší téměř veškerá internetová data po celém světě a jejichž případné poškození tak může výrazně ovlivnit fungování kritické infrastruktury. Tématem byla i umělá inteligence, s jejímž rozvojem se v tuto chvíli západní svět srovnává a hledá způsoby, jak řešit příležitosti i rizika s AI spojené. Diskuse nemohla opomenout ani Akt o umělé inteligenci, který před pár dny přijala Evropská unie.

Jedním z bodů programu byla také bezpečnost cloudu, což je v poslední době jedním z klíčových témat transatlantické spolupráce. Řečníci v tomto panelu přinesli různé pohledy z vládní i průmyslové perspektivy. Nechyběla ani diskuse na téma post-quantových technologií. Bezpečnostní komunita si velmi uvědomuje, že s nadcházejícím průlomem v kvantové výpočetní technice se současné šifrovací metody používané k zabezpečení citlivých informací stanou potenciálně zranitelnými a bude tak potřeba vyvinout a přejít na kvantově odolnou kryptografii. Debata se proto zaměřila na strategie v oblasti post-quantového šifrování, na výzvy spojené s načasováním a standardizací a také na příležitosti pro mezinárodní spolupráci mezi vládami, výzkumnými a průmyslovými partnery. Poslední panel se věnoval jedné z největších kybernetických hrozeb

současnosti: ransomwaru, jejíž zvládnutí vyžaduje opravdu komplexní přístup. Důkazem závažnosti této hrozby a potřeby čelit jí je mj. společné prohlášení proti platbám výkupného při ransomwarových útocích. Česká republika se k němu připojila spolu s dalšími více než 40 státy v listopadu 2023.

V závěru konference pak vystoupil ministr zahraničních věcí České republiky Jan Lipavský: *„Dnes, kdy uzavíráme pražskou konferenci o kybernetické bezpečnosti, vidíme, že bezpečnost kritické infrastruktury je naléhavější než kdy jindy. Kybernetický svět je bitevním polem, kde čelíme mnoha výzvám. Spolupráce s podobně smýšlejícími partnery je klíčovým prvkem, který zajistí, že v technologickém závodě neprohrájeme. Dalším z nich je úzká spolupráce se soukromým sektorem. Koneckonců jsme všichni součástí tohoto úsilí o utváření budoucnosti svobodného a demokratického světa.“*

Kybernetická bezpečnost se neobejde bez mezinárodní spolupráce, a právě konference jsou skvělou příležitostí pro uskutečnění bilaterálních jednání. Nejinak tomu bylo na PCSC. Zástupci NÚKIB využili akce k setkání s delegacemi z NATO, Jižní Koreje, Taiwanu, USA, Austrálie, Japonska, Singapuru, Belgie, Chorvatska a Litvy. A jak častokrát v průběhu celé konference zaznělo, nezbytná je v kyberbezpečnosti také spolupráce se soukromým sektorem, proto v rámci akce proběhla také jednání NÚKIB s několika zástupci soukromého sektoru.

A právě soukromému sektoru se letos pražská konference otevřela historicky poprvé. Jeho role totiž v kontextu zajišťování kybernetické bezpečnosti stále nabývá na relevanci. *„V dnešní době již nemůžeme ignorovat význam a potenciál spolupráce s klíčovými hráči ze soukromého sektoru. Pouze celospolečenský přístup a vzájemná synergie mezi státem a vybranými technologickými a kyberbezpečnostními společnostmi je do budoucna tou jedinou cestou. Musíme postupně propojovat silné stránky státu, soukromého sektoru a také akademické obce v jednu koordinovanou reakci na kybernetické hrozby jak na národní, tak i mezinárodní úrovni,“* sdělil ředitel NÚKIB Lukáš Kintr k tématu spolupráce napříč sektory.

Partnery letošního ročníku konference se staly společnosti Amazon Web Services (AWS), MSD, CISCO, Mastercard, Appsec, a ICZ. *„Společnost AWS již více než deset let spolupracuje s vládami a regulačními orgány v celé Evropě, aby rozuměla jejich potřebám v oblastech, jako je kybernetická bezpečnost, ochrana osobních údajů a digitální suverenita. Diskuse mezi všemi zúčastněnými stranami na pražské konferenci o kybernetické bezpečnosti podtrhuje zásadní význam spolupráce mezi vládami, veřejnými institucemi a soukromými organizacemi. Taková spolupráce je hnacím motorem inovací a podporuje odolnost na kontinentu i v celosvětovém měřítku,“* uvedl Arnaud David, ředitel pro veřejnou politiku v oblasti digitálních technologií a umělé inteligence pro Evropu, Blízký východ a Afriku ve společnosti Amazon Web Services.

<https://nukib.gov.cz/cs/infoservis/aktuality/2098-kyberneticka-bezpecnost-se-dnes-jiz-neobejde-bez-spoluprace-statniho-a-soukromeho-sektoru-zaznelo-opakovane-na-konferenci-nukib>