Cyber Security 2025

16. října 2025 / 9:00 / Konferenční centrum City Na Strži 1702/65, 140 62 Praha 4

Program akce

Hlavní blok

9:00 - 9:10 **Zahájení akce**

Jan Mazal

9:10 - 9:40 **Bezpečnost citlivých dat pěkně od podlahy až k mrakům**

Petr Kunstát - Thales

Být suverénním vládcem svých dat, ať už jsou kdekoliv, i za existence kvantových počítačů.

9:40 - 10:10 **Bitdefender - automatizované zmenšení útočné plochy**

Pavel Škorpil - IS4 security / Bitdefender

Také využíváte od roku 2008 umělou inteligenci pro kybernetickou obranu? A používáte ji jako my pro snížení útočné plochy? Příliš mnoho softwarových oprávnění zbytečně zvyšuje riziko. Bitdefender vám ukáže cestu, jak snížit útočnou plochu až o 95 %.

10:10 - 10:40 **Logování kvůli splnění zákona je povinnost, která však negarantuje žádnou bezpečnost**

Jakub Karvánek - FreeDivision

ZoKB vznikl z důvodu posílení naší bezpečnosti. Když už sbíráme logy, byla by škoda s nimi aktivně nepracovat. Správným přístupem můžeme odhalit anomálie a incidenty, automaticky na ně reagovat a následně je řádně vyšetřit. Poznejte platformu, která vám toto vše zajistí.

10:40 - 11:10 **AI v kybernetické bezpečnosti: Odpovědnost jako nutnost, nejen příležitost. Jak AI Act mění pravidla hry.**

Michal Bahník - ARTIN, Petr Žídek - Feichtinger Žídek Fyrbach advokáti

Společná prezentace expertů Michala Bahníka (ARTIN) a Petra Žídka (AKFŽ) přináší komplexní pohled na průnik AI a kybernetické bezpečnosti v kontextu nové evropské legislativy AI Act. Prezentace propojuje technické aspekty odpovědné, vysvětlitelné a sledovatelné AI s konkrétními právními povinnostmi vyplývajícími z AI Actu, přičemž zdůrazňuje, že kybernetická bezpečnost již není pouze o ochraně proti vnějším útokům, ale také o zajištění, aby samotné AI systémy byly bezpečné, spravedlivé a transparentní. Řečníci představí pět pilířů Responsible AI framework (etika, transparentnost, spravedlnost, bezpečnost a design zaměřený na člověka) a nabídnou sedm konkrétních kroků k implementaci důvěryhodné AI, která nejen splňuje legislativní požadavky, ale také minimalizuje rizika diskriminace, útoků a jiných bezpečnostních hrozeb, což je zásadní zejména pro organizace působící v kritických a vysoce regulovaných odvětvích jako jsou energetika, finance či zdravotnictví.

11:10 - 11:40 **Coffee break**

11:40 - 12:10 **Mikrosegmentace v teorii i praxi: Nezbytný pilíř ochrany byznysu proti moderním hrozbám**

Pavel Srnka - ANECT

Mikrosegmentace je klíčovým nástrojem, jak zastavit ransomware, zero-day útoky i laterální pohyb útočníků. V přednášce ukážeme, proč se bez ní moderní podniková bezpečnost neobejde, jaké jsou její přínosy i úskalí a jak ji efektivně zavést v praxi.

12:10 - 12:40 **101 odhalování kompromitovaných identit v Entra ID**

Martin Haller - PATRON-IT

V dnešní době je spousta firemních dat a služeb v cloudu. Uživatelská identita se stává klíčovým prvkem, který je nutné chránit. Kdo má přístup k identitě, má v podstatě přístup i citlivým datům. Microsoft téměř v základní verzi svých Microsoft 365 služeb nabízí nástroje pro detekci kompromitovaných identit a podezřelých přihlášení, avšak i přesto řada správců tyto informace nevyužívá, což je škoda. V této přednášce si ukážeme, jak správně interpretovat informace o rizikových uživatelích a rizikových přihlášeních z prostředí Microsoftu. Probereme, jak vyhodnotit správnost detekce, jak získat potřebné informace pro analýzu rizik a jak efektivně reagovat na zjištěné problémy. Cílem je naučit se využívat dostupné nástroje k včasné identifikaci a nápravě kompromitovaných identit, což výrazně zlepší vaši schopnost reagovat na potenciální hrozby.

12:40 - 13:10 **Jak pracovat s aktivy a jejich riziky podle metodiky NÚKIB**

Jakub Karvánek - FreeDivision, Petr Sobotka - FreeDivision

Reputace je něco, co se dlouho buduje, ale často se naopak rychle ztrácí. Kyberbezpečnost je přitom pořád nový prostor, kde se nároky neustále zvyšují s tím, jak přichází nové směrnice a normy. Často o důvěru přijdeme jen kvůli nedostatku zdrojů. Naštěstí si můžeme vzít na pomoc různé nástroje a automatizovaná řešení. Nejinak je tomu v době nastupující platnosti směrnice NIS2 a novely ZoKB. Správná reakce na bezpečnost vašich aktiv začíná u jejich evidence včetně hodnocení. Následné pojmenování rizik mířících na evidovaná aktiva vám pomůže se včasnou reakcí na blížící se hrozby. Pochopení problematiky je klíčem k bezpečnosti ve vašem prostředí a k naplnění zákonných povinností.

13:10 - 13:40 **Jaké změny přináší nový zákon o kybernetické bezpečnosti?**

Jana Pattynová - PIERSTONE

Kybernetická bezpečnost se stává jednou z priorit evropské i české legislativy. Klíčovým impulzem je evropská směrnice NIS2, která zásadně mění dosavadní rámec – rozšiřuje okruh regulovaných subjektů, zpřísňuje požadavky na bezpečnostní opatření, zavádí důslednější dohled a přináší vyšší sankce za porušení povinností. V České republice má být směrnice transponována prostřednictvím nového zákona o kybernetické bezpečnosti, jehož účinnost Národní úřad kybernetické bezpečnosti předpokládá již k 1. listopadu 2025.
Přednáška přiblíží hlavní změny, které nový zákon přinese, a jejich praktické dopady na organizace působící v klíčových sektorech – ve veřejné správě, energetice, zdravotnictví, dopravě či oblasti digitální infrastruktury. Účastníci se dozvědí, zda jejich organizace bude nově regulována, jaké povinnosti na ni dopadnou a jak se na nové požadavky připravit.

13:40 - 14:40 **Oběd**

14:40 - 15:10 **Regulace dodavatelů informačních technologií v nZKB**

Jan Rudolf - Národní úřad pro kybernetickou a informační bezpečnost

Prezentace se zaměří na definování regulovaných služeb v rámci odvětví Digitální infrastruktura a služby v rámci nového zákona o kybernetické bezpečnosti. Představí specifika poskytovatelů regulovaných služeb v tomto odvětví a rozebere jejich povinnosti. Krátce se dotkne i regulace kritické infrastruktury v tomto odvětví.

15:10 - 15:40 **OSINT a právo – hranice legálního využití informací**

Milan Listík - LISTIK LEGAL

Tato přednáška vám ukáže, jak se obratně pohybovat mezi právními předpisy při využívání veřejně dostupných informací v kontextu Open-source Intelligence (OSINT), dále jak nahlížet na práci s indexovanými důvěrnými dokumenty a možným použitím uniklých dat i osobních dat při investigaci včetně jejich využití například u soudního řízení. Dozvíte se, kde je hranice mezi legálním sběrem informací a průmyslovou špionáží a jak se právní pravidla liší v soukromém a veřejném právu. Vše na konkrétních příkladech z praxe.

15:40 - 16:10 **Jak se bránit kyberzáhubě**

Aleš Špidla - Ing. Aleš Špidla

Kybernetická a informační bezpečnost není otázkou zákonů, je otázkou pudu sebezáchovy. Chci vydělávat dnes i zítra, chci plnit zákonné povinnosti dnes i zítra, chci sloužit občanům dnes i zítra, chci léčit dnes i zítra. Nechci být v novinách ani dnes ani zítra. Nechci být trestně stíhaný ani dnes ani zítra ... ale jak z toho ven ... kyberven.

16:10 **Předpokládaný konec akce**