

Cyber Security 2026

13. října 2026 / 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 Zmenšit riziko. Zvládnout audit. Vidět souvislosti.

Pavel Škorpil - IS4 security / Bitdefender

Útočníci dnes často využívají běžné nástroje a oprávnění, která uživatelé ke své práci vůbec nepotřebují. Současně přibývají regulatorní požadavky a bezpečnostní týmy se topí v datech a výstrahách. Ukážeme, jak na tyto výzvy reagují novinky Bitdefender GravityZone. PHASR průběžně omezuje útočnou plochu podle skutečného chování uživatelů, Compliance Manager pomáhá udržet přehled o souladu s NIS2, GDPR nebo ISO 27001 a Data Lake spojuje bezpečnostní data do jednoho srozumitelného kontextu. Doplníme také stručný přehled dalších novinek, které mohou firmám i organizacím zjednodušit každodenní práci s kybernetickou bezpečností.

9:40 - 10:10 Když bezpečnost začíná už ve výrobě

David Filgas - HP Inc Czech Republic

Přednáška představí vícevrstvý přístup HP k ochraně koncových zařízení – od zabezpečení BIOSu a obnovy systému až po ochranu uživatele, dat a samotného zařízení. Na konkrétních příkladech ukážeme, jak mohou technologie HP pomoci snížit bezpečnostní rizika v moderním pracovním prostředí.

10:10 - 10:40 AI ve firmách: tři bezpečnostní výzvy, které dnes vidíme v praxi

Martin Haller - PATRON-IT

AI se ve firmách zabydluje rychleji, než na ni stíhají reagovat bezpečnostní pravidla, interní procesy a IT governance. Zaměstnanci používají nové nástroje, výrobci přidávají AI funkce do stávajících produktů a IT týmy často až za pochodu řeší, jak to celé bezpečně uchopit. V přednášce ukážu tři bezpečnostní problémy, které dnes kolem AI ve firmách reálně řešíme. Nepůjde o teoretické varování před umělou inteligencí, ale o pohled na situace, které potkáváme u zákazníků a které souvisejí s daty, přístupy, integracemi a odpovědností. Cílem je ukázat, kde firmám vznikají rizika už dnes, jak o nich přemýšlíme v praxi a co s nimi mohou IT manažeři začít dělat dřív, než se z nich stanou incidenty.

10:40 - 11:10 CISO-less company

Martin Leskovjan - Penta Hospitals CZ

Přednáška představí vizi plně autonomního ISMS, ve kterém automatizace a AI zajišťuje kompletní výkon bezpečnostních opatření, analyzuje rizika, reaguje na incidenty a opravuje zranitelnosti, které sama odhalí. Přednáška představí, jaké technologické a procesní předpoklady musí organizace splnit, aby mohla přejít od „manuálně“ řízené bezpečnosti k bezpečnosti řízené daty, automatizací a umělou inteligencí.

Budeme mluvit o základech, na kterých zdravé (a tím i automaticky říditelné) ISMS musí stát a proč největší překážkou není technologie, ale samotná organizace a její nastavení.

A také o tom, jak by se posluchači zaměstnaní v IT security v éře AI měli rozvíjet, aby jejich roli nepřevzala autonomní správa.

11:10 - 11:40 Coffee break

11:40 - 12:10 Kyberbezpečnost v éře dostupné AI: co se opravdu děje a jak na to reagovat

Michael Bátorla - České vysoké učení technické v Praze

Zprávy o AI v kyberbezpečnosti se letos točí kolem incidentů modelů z frontier laboratoří. Podstata změny hrozby pro organizace je ale prozaičtější. Schopnosti, kvalifikovaná pozornost a zdroje, které ještě loni odlišovaly specializované útočníky od těch obvyklejších, jsou dnes díky AI šířeji dostupné.

Většina bezpečnostních programů přitom na limitech na straně útočníka alespoň implicitně stojí. Co považujeme za pravděpodobný cíl a úroveň úsilí, kterou může útočník vyvinout, kolik slabin v našem prostředí vůbec někdo najde, do jaké míry opatření vytvářejí útočníkům překážky nebo kolik času je mezi jeho prvním a posledním krokem. Přitom roste i to, co máme bránit. Ať objem kódu, který se dostává do produkce, či počet strojových identit. Přednáška pojmenuje oblasti, které se v bezpečnosti strukturálně změnily, a u každé z nich to podstatné: co se liší oproti tomu, jak organizace bezpečnost stavěly doposud.

Dostupnost ale není jednostranná. Stejná změna zpřístupňuje obráncům s pomocí AI nástroje a opatření, která byla dosud mimo dosah většiny organizací. Projdeme, které z nich mají největší efekt v jednotlivých oblastech, a hlavně jak si projít vlastní portfolio opatření: kde se změnila účinnost, kde nákladnost, kde je nutné zvýšit kapacitu a kde je potřeba jiný přístup než dosud.

12:10 - 12:40 Žebříček omylů: kde organizace nejčastěji chybují při compliance se ZKB

Olga Pincová - Perspia (MoyaKybeon)

Každá organizace je jiná, ale některé chyby se u ZKB opakují znovu a znovu – ať jde o malou firmu, nebo velký podnik. Ve spolupráci s partnery, kteří organizace při plnění ZKB doprovázejí, jsem sestavila přehled těch nejčastějších: od podcenění rozsahu povinností přes formální dokumentaci bez reálného obsahu až po chybějící vazbu na skutečné procesy ve firmě. Cílem není strašit výčtem paragrafů, ale ukázat na reálných příkladech, kde firmy nejčastěji tápou a jak se tomu dá předejít. Tipnete si chybu č. 1?

12:40 - 13:10 Od AI Actu k praxi: Jak nastavit AI compliance ve firmě

Štěpánka Bátorla

Rok 2026 je pro evropskou regulaci umělé inteligence zásadní. Další část povinností podle AI Actu se stává použitelnou a firmy musí přejít od obecných debat o regulaci AI ke konkrétním krokům v praxi. Přednáška představí, jaké nové povinnosti AI Act přinese, kterých organizací a AI systémů se týká a jak se na ně prakticky připravit. Zaměří se zejména na to, jak zmapovat používání AI ve firmě, správně určit její roli podle AI Actu, identifikovat vysoce rizikové a další regulované případy použití a nastavit odpovídající governance, dokumentaci, interní pravidla a odpovědnosti. Stranou nezůstanou ani požadavky na transparentnost nebo praktické řízení AI dodavatelů. Cílem není projít AI Act článek po článku, ale ukázat, co by měla firma v roce 2026 reálně udělat, aby dokázala AI používat bezpečně a zároveň splnit nové regulační požadavky.

13:10 - 14:10 Oběd

14:10 - 14:40 Ukradeno, nebo naučeno? Práva k výstupům AI a spory o trénovací data

Milan Listík - LISTIK LEGAL

Navazujeme na loňský příspěvek o OSINT. Letos se zaměříme na dvě otázky, které se během roku zásadně posunuly: komu patří výstupy generativní AI (USA, EU, Čína, Japonsko, Indie, UK) a za jakých podmínek lze cizí obsah použít k tréninku modelu. Projdeme rozhodnutí z posledních dvanácti měsíců — LAION, GEMA, Getty, Bartz v. Anthropic, ANI v. OpenAI — a povinnosti podle AI Actu účinné od srpna 2026. Důraz na praktické závěry pro sporovou i smluvní agendu.

14:40 - 15:10 Vlastní LLM v cloudu

Michal Roth - DesignDev

V DesignDev provozujeme vlastní LLM stack na pronajatých H100, vLLM + LiteLLM pro interní nástroje i klienty s citlivými daty. V přednášce ukážu reálná čísla – kolik to skutečně stojí, jak funguje on-demand provoz, kdy se self-hosting vyplatí oproti komerčním API a kdy je naopak zbytečný. A hlavně praktické záseky z provozu, které nenajdete v dokumentaci ani blozích – od chování vLLM přes kvantizaci po tiché změny v ekosystému. Žádná teorie, konkrétní zkušenosti a čísla z reálného nasazení.

15:10 Předpokládaný konec akce