Cyber Security 2024

17. října 2024 / 9:00 / GRAND HOTEL PRAGUE TOWERS Kongresová 1655/1, 140 00 Praha Nusle

Program akce

Hlavní blok

9:00 - 9:10 **Zahájení akce**

Jan Mazal

9:10 - 9:40 **XDR je tu pro všechny**

Pavel Škorpil - IS4 security / Bitdefender

Bezpečnostní platformy narážejí na problematiku nejednotných nástrojů pro správu zabezpečení. I bez ohledu na NIS2 ale musí organizace řešit ochranu svých dat.
Pomocí jednotné a robustní XDR platformy ale zvládne zabezpečit svou síť i menší organizace. A to bez zbytečných nákladů na lidské zdroje nebo outsourcing SIEM systémů.

9:40 - 10:10 **Logování, alertování a reakce – aneb SIEM, SOAR velmi jednoduše (Živá ukázka)**

Jakub Karvánek - FreeDivision

Poznejte nové řešení, které v jedné platformě poskytuje nástroje Log Management, SIEM a služby SOAR, Threat Intelligence. Řešení, které si může dovolit jakýkoli zákazník a přitom ho zvládne ovládat i obchodník.

10:10 - 10:40 **From Scrapers to DDoS: Understanding and Mitigating Bot Threats**

Michal Orzechowski - Websec

Akamai Bot Manager effectively detects bot traffic and mitigates malicious bots at the edge, while effectively managing good bots — all without impacting user experience. It protects your apps and assets, regardless of how or where customers choose to interact with you.

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

11:10 - 11:40 **Mějte zabezpečené své uživatele, koncová zařízení a data.**

Václav Petrželka - HP Inc Czech Republic

Tato prezentace se zaměřuje na bezpečnostní řešení společnosti HP, která pomáhají chránit uživatele, zařízení a data před kybernetickými hrozbami. Prezentuje několik klíčových bezpečnostních funkcí a technologií, které jsou součástí HP Wolf Security, včetně ochrany před phishingovými útoky, ransomwarem, BIOS a firmware útoky, vizuálním hackováním a ztrátou nebo krádeží zařízení.

11:40 - 12:10 **Aktuální stav nového zákona o kybernetické bezpečnosti**

Martin Švéda - Národní úřad pro kybernetickou a informační bezpečnost

Právní regulace kybernetické bezpečnosti zažívá nebývalé změny – v souvislosti se směrnicí NIS2 připravuje Česká republika nový zákon o kybernetické bezpečnosti. V jaké fázi legislativního procesu se zákon nachází, co to pro budoucí adresáty znamená a proč by měli řešit kybernetickou bezpečnost bez ohledu na legislativu bude předmětem této přednášky.

12:10 - 12:25 **Quantum Safe: Zabezpečení pro dnešní i kvantovou budoucnost**

Walter Pavliš - DATERA

Kvantové počítače přinášejí revoluční technologie, ale také nové bezpečnostní výzvy. Tato přednáška představí, co znamená koncept „Quantum Safe“ a jak se organizace mohou připravit na ochranu svých dat před hrozbami, které budou kvantové počítače představovat. Účastníci se dozvědí o aktuálních metodách zabezpečení a inovativních přístupech k šifrování, které zajistí, že i v budoucí kvantové éře zůstane citlivý obsah bezpečný.

12:25 - 12:45 **Správa Privilegovaných Účtů s IBM Verify Privilege Vault**

Václav Říha - DATERA

Tato přednáška se zaměří na důležitost správy privilegovaných účtů (PAM) pro ochranu klíčových firemních dat. Účastníci se seznámí s řešením IBM Verify Privilege Vault, jeho funkcionalitami a přínosy v oblasti zabezpečení, správy a monitorování přístupu k citlivým zdrojům organizace. Diskutována bude také implementace PAM v podnikových prostředích a osvědčené postupy pro minimalizaci rizik spojených se zneužitím privilegovaných přístupů.

12:45 - 13:15 **Cloud, uměla inteligence a regulace kybernetické bezpečnosti**

Dominik Vítek - PIERSTONE

Cloudové technologie a umělá inteligence jsou předmětem komplexních pravidel kybernetické bezpečnosti. Prezentace Vás provede požadavky na kybernetickou bezpečnost při nasazováni těchto technologií a jejich dodávkách zákazníkům v regulovaných sektorech, včetně státní správy.

13:15 - 14:15 **Oběd**

14:15 - 14:45 **Jazykové modely LLM (genAI) v hackingu a kybernetické kriminalitě**

Daniel Hejda - Cyber Rangers

V rámci přednášky si řekneme o dosud viděných modelech údajně využívaných pro kybernetické a kriminální operace. Vysvětlíme si jak tyto modely vznikají a zda mohou fungovat, či nikoliv a jak jsou vytvářeny. Během přednášky si ukážeme některé deepfake možnosti a opomenuta nebude ani syntéza hlasu nebo velmi sofistikované klonování internetových stránek podvodníky. Jako bonus si řekneme zda lze nebo nelze vytvářet tzv. instant avatary cizích osob.

14:45 - 15:15 **Bezpečnostní kritéria eGovernment Cloudu**

Petr Kopřiva - Národní úřad pro kybernetickou a informační bezpečnost, Helena Ulrychová - Digitální a informační agentura

Na přednášce věnované tématu „eGovernment cloud“ se dozvíte odpovědi nejen na tyto otázky:

- Jaké jsou povinnosti a příležitosti pro správce informačních systémů veřejné správy při využití cloud computingu?
- Co je a k čemu slouží katalog cloud computingu?
- Jaká bezpečnostní kritéria musí splnit poskytovatelé, pokud chtějí nabízet své služby?

15:15 - 15:45 **Jak ZoKB změní vaše smlouvy s dodavateli?**

Ondřej Hanák - eLegal advokátní kancelář

Nový zákon o kybernetické bezpečnosti a jeho vyhlášky budou pro každý povinný subjekt znamenat nutnost projít si smlouvy s dodavateli. To zní samozřejmě pro každou firmu jako velká zábava. Ale je dobré to brát jako skvělou příležitost, jak si ve smlouvách udělat pořádek. Zároveň to pomůže pohlídat, že dodávky budou fungovat a pokud ne, tak budete mít jasně stanovená pravidla řešení. Můžete se totiž nakrásně snažit dodržovat kyberbezpečnost, ale nevhodný, nepřipravený nebo neřízený dodavatel vám může způsobit problém. Minimálně ve vyšším režimu povinností je nutné dodavatele skutečně zásadně zapojit i do havarijních plánů a řešení incidentů. V příspěvku Ondřeje Hanáka se dozvíte, na co si, hlavně ve smlouvách, dávat pozor, jak se z toho nezbláznit a do čeho všeho jaké dodavatele zapojit.

15:45 - 16:00 **Tombola**

16:00 **Předpokládaný konec**