

Cyber Security 2020

11. listopadu 2020 / 9:00 / Akce proběhne online

Program akce

Hlavní blok

- 9:00 - 9:10 Úvodní slovo**
Jan Mazal
- 9:10 - 9:40 V2X. V2H? H2V? WFT?**
Rafal Jaczynski - HUAWEI Ads
Bezpečnost nikdy není nezáživná a vždy je o tom dělat věci správně. A to od samého začátku. Je komunikace mezi vozidlem a jeho okolím (Vehicle to Everything) dobrým příkladem zabezpečení implementované již od prvotního návrhu? Anebo jsme chtěli mít to nejlepší, ale dopadlo to stejně jako vždy?
- 9:40 - 10:10 Jak chránit chráněná data?**
Aleš Koreček - DELL Technologies
Firemní data určená pro obnovu businessu se sama stávají terčem útoků. Řešení pro business continuity a data protection dokonce mohou být sama zdrojem zranitelností s dopadem na celou infrastrukturu. Přednáška bude pojednávat o principech, které umožní návrh těchto řešení jako datového ostrova odolného proti napadení.
- 10:10 - 10:40 Zabezpečený přístup k firemním aplikacím**
Jiří Doubek - F5 Networks
Bezpečnostní perimetr tak, jak ho známe, už neexistuje. Aplikace mohou pobývat ve stávajícím datovém centru, v cloudu nebo je můžeme čerpat jako službu SaaS (např. Office 365). Autentizace, kterou každá aplikace vyžaduje, pro organizace implikuje komplexní architekturu založenou na různých protokolech a technologiích od několika dodavatelů. Na prezentaci se dozvíte, jak technologie F5 pomůže s implementací architektury Zero Trust, nasazením funkce Single Sign-On (jednotné uživatelské identity napříč aplikacemi) a – dnes už nezbytné – vícefaktorové autentizace, to vše s nepřetržitým monitoringem uživatelů.
- 10:40 - 11:10 Microsoft Zero Trust**
David Šostý - MICROSOFT
Představíme zefektivnění a posílení firemních bezpečnostních principů na základě využití principů Zero Trust od společnosti Microsoft.
- 11:10 - 11:25 Přestávka**
- 11:25 - 11:55 Autentizace založená na Zero Trust a Passwordless**
Petr Kunstát - Thales Group Inc.
Z hlediska práce s citlivými daty ať už lokálně nebo vzdáleně je nejzranitelnějším místem uživatelská identita. Pokud je chráněna pouze heslem, je snadným terčem Phishingových nebo Lazy Phishingových útoků. Útočník má pak snadnou cestu k citlivým datům. Ukážeme si jak uživatelskou identitu a samotná data efektivně chránit. U ochrany samotných dat se zaměříme na to, abychom nasazením šifrování IT uživatele neodradili a práce se nezpomalila.
- 11:55 - 12:25 Úspěšná obnova dat po útoku ransomwaru**
Boris Mittelman - Veeam Software
Mít NĚJAKÉ ZÁLOHY při současné vyspělosti kybernetických hrozeb již zdaleka nestačí.
Jak postavit odolné zálohovací řešení, správná zálohovací pravidla a jak postupovat při obnově jednotlivých souborů, celých NAS úložišť, či Office365 je předmětem této prezentace.
- 12:25 - 12:55 Využití automatizace a ML algoritmů pro zastavení pokročilých hrozeb**
Jakub Jiříček - Palo Alto Networks
- 12:55 - 13:25 Analytické nástroje pro vyšetřování a proaktivní reakci na kybernetickou hrozbu**
Filippo Sitzia - McAfee
V přednášce přiblížíme řešení pro detekci hrozeb v koncových bodech a následnou reakci (EDR).

13:25 - 13:45 Přestávka

13:45 - 14:15 Příběhy z "bitevního pole" s kyberzločinci

Martin Haller - PATRON-IT

Už ani nespočítám, kolik se na naši firmu, za posledních několik let obrátilo obětí ransomware. Řešili jsme více i méně závažné útoky, vyjednávali s útočníky a pomáhali platit výkupné. Nasbíral jsem tak hromadu praktických postřehů a rád bych se s Vámi o ně podělil. Například zdali jsou hackeři čestní, proč jsou jejich útoky tak fatální, jestli nenapadají své oběti vícekrát, či zdali jsou lepší než obránci.

14:15 - 14:45 Jak postupovat při kybernetickém útoku - role právníků

Jana Pattynová - PIERSTONE

Řešení kybernetických útoků je doménou IT odborníků, ale role právníků je v takové situaci také významná. Je nutné řešit různé informační a ohlašovací povinnosti, rizika odpovědnosti za škodu a odpovědnosti statutárních orgánů, otázky spojené s úvahami o platbě výkupného, koordinaci s orgány činnými v trestním řízení a řadu dalších otázek. Presentace Vás provede tématy, se kterými jsou právníci konfrontováni v případech kybernetických útoků a incidentů a shrne některé praktické zkušenosti z těchto situací.

14:45 - 15:15 Jak změni 5G sítě požadavky na kybernetickou bezpečnost

Aleš Špidla - Ing. Aleš Špidla

5G sítě už nejsou za dveřmi, už pomyslný práh překročily a jejich vstup do našich životů je realitou. Je nutno si uvědomit, že se nejedná jen o zrychlení stahování filmů do mobilů apod. Jedná se také o docela zásadní dopad na kybernetickou bezpečnost.

15:15 - 15:45 Pozor!! Nepřítel naslouchá

Jiří Nápravník - SALAMANDR

Špionáž je jedno z nejstarších řemesel na světě. Je to neetické, je to často i trestné, ale špionáž používaly a používají firmy i státy. Po roce 2000 jsem často slyšel názory, že špionáž již patří minulosti, protože jdeme do EU a NATO. Ten názor byl velmi naivní a dokládají to například špionážní aféry mezi firmami v rámci EU. V době Internetu a mobilů dostala špionáž úplně novou podobu. Používají ji státy, podvodníci i technologické firmy. Dnes, víc jak kdykoliv v minulosti, platí heslo: „Pozor! Nepřítel naslouchá“, jenže je těžké rozpoznat, kdo je nepřítel.

15:50 Předpokládaný konec akce