**Pracovní skupina kybernetické bezpečnosti české pobočky AFCEA**
**Policejní akademie ČR v Praze**
ve spolupráci s
**Národním úřadem pro kybernetickou a informační bezpečnost ČR**

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

# Kybernetická bezpečnost VII

- ***aktuální stav kybernetické bezpečnosti v ČR***
- ***praktické zkušenosti se zaváděním kybernetické bezpečnosti***
- ***aktuální technologické trendy a řešení v oblasti kybernetické bezpečnosti a obrany***
- ***umělá inteligence a kybernetická bezpečnost***

## **26. září 2019, od 9:00**, Policejní akademie ČR v Praze

*9:00* ***Přivítání***
Petr JIRÁSEK, Předseda, Pracovní skupina kybernetické bezpečnosti AFCEA

### Úvodní sekce

9:10 – 10:30 **Úvodní slovo**
Dušan NAVRÁTIL, Ředitel, NÚKIB ČR
**Aktuální stav kybernetické bezpečnosti v České republice**
Adam KUČINSKÝ, NÚKIB ČR
***Q&A***

10:30 – 11:00 **Zranitelnosti, o kterých nevíme, aneb jak a proč testovat (nejen) perimetr**
Jan KOPŘIVA, Senior Lead, CSIRT, ALEF NULA, a.s.
*BlueKeep, DejaBlue a mnoho dalších zranitelností skloňují v poslední době často i populární média. Dalo by se tedy očekávat, že IT specialisté, administrátoři systémů připojených k internetu a techničtí pracovníci zodpovědní za správu perimetrů sítí spolehlivě zajistí záplatování těchto zranitelností, nebo alespoň zablokují přístup k postiženým systémům. Ne vždy je tomu ale tak. V této přednášce si jmenovanou skutečnost společně ukážeme na příkladu BlueKeep - jedné z nejzávažnějších zranitelností letošního roku. Blíže zmíníme její princip a podíváme se na několikaměsíční trendy v počtech z internetu dostupných zranitelných systémů v České republice a v mnoha dalších zemích světa. Následně si představíme procesní a technické možnosti pro identifikaci této a dalších zranitelností a podíváme se co je potřeba, abychom všechny podstatné zranitelnosti identifikovali a záplatovali před tím, než je v našem perimetru odhalí útočníci.*

*11:00 – 11:30* *Přestávka*

## Sekce praktických příkladů a řešení v oblasti kybernetické bezpečnosti

11:30 – 12:00 **Využití komerčních cloudových služeb pro splnění požadavků VKB**

Tomáš MIROŠNÍK, Microsoft CZ/SK

*Účinnost nové VKB č. 82/2018 Sb. vede správce systémů pod ZKB k nové vlně vymezení a hodnocení svých systémů řízení bezpečnosti informací (ISMS). Máme zabezpečení aktiv adekvátní hodnocení jejich důležitosti? Není potřeba aktualizovat úroveň zabezpečení a související interní politiky? Jak je na tom klasifikace aktiv a řízení přístupu, zejména u privilegovaných uživatelů? Pokusíme se ukázat jak ulehčit život manažerům a architektům kybernetické bezpečnosti při zavádění ISO 27001 a zajištění souladu s požadavky VKB.*

12:00 – 12:20 **BVS - Business Visibility Suite**

Tomáš PŘIBYL, CEO; Václav KONEČNÝ, Corpus Solutions, a.s.

12:20 – 12:40 **Přínosy integrace nástrojů detekce a reakce pro budování kybernetické bezpečnosti**

Jindřich ŠAVEL, Obchodní ředitel, Novicom, s.r.o.

*Stále sofistikovanější kybernetické hrozby iniciovaly vznik mnoha úspěšných detekčních nástrojů a metod. Vystačíte si ale pouze s detailní informací o hrozbě? Jste schopni reagovat dostatečně rychle, abyste zabránili škodám? Bez integrovaných nástrojů reakce, zahrnujících detailní visibilitu zařízení a řízení sítě (DDI/NAC), a umožňujících sdílet tyto prostředky s externími bezpečnostními specialisty (SOC), to asi nepůjde...*

12:40 – 13:00 **Role Flow monitoringu v kybernetické bezpečnosti**

Zoltán CSECSÖDI, Czech Sales Director, Flowmon Networks

*Součástí spolehlivého provozu celé IT infrastruktury je i monitorování síťového provozu, automatická detekce anomálií a monitorování provozu kritických aplikací. Sledování všech těchto oblastí lze realizovat za pomocí nástrojů původního českého řešení Flowmon. V prezentaci zazní nejnovější trendy využití technologie NetFlow/IPFIX.*

*13:00 – 13:45* *Oběd*

13:45 – 14:05 **Kyberbezpečnost bez růžových brýlí**

Tomáš FILIP, Head of Cyber Defense Center, AEC a.s.

*Se stále narůstající závislostí na informačních systémech vzrůstá také význam informační bezpečnosti. Jsme však připraveni nával digitalizace bezpečně zvládat? Je jen otázkou času, kdy budeme muset běžně čelit kybernetickým útokům, kterým dennodenně čelí země na západ od nás. Rád bych se podělil o vlastní zkušenosti (z globálního i lokálního prostředí), které indikují, že je před námi často ještě hodně práce, pokud chceme být připraveni.*

14:05 – 14:30 **Umělá inteligence – Transformace zabezpečení k lepšímu a horšímu**

Martin REHÁK, zakladatel a CEO, Bulletproof AI - Secure and Fair Machine Learning

*Umělá inteligence (AI) je na samém vrcholu svého humbukového cyklu. Pojďme mluvit o skutečných schopnostech, které nabízí obránci a útočníkovi, o jejích silných a slabých stránkách a proč by to neohrozilo lidstvo před tím, než všichni odejdeme do důchodu – pokud to neuděláme sami.*

14:30 – 14:50 **Celostní kybernetická bezpečnost**

Miroslav NEČAS, Tovek

14:50 – 15:10 **Specifika řízení kybernetické bezpečnosti dodavatelského řetězce**

Martin UHER, předseda představenstva, CyberG Europe, a.s.

*15:15* ***Závěr***

## *Partneři akce*

ALEFNULA

Microsoft

CORPUS SOLUTIONS CYBERSECURITY EXPERTS

CYBERG

Flowmon Driving Network Visibility

AEC

novicom

TOVEK

## Další připravované akce:


Od 9. září 2019 probíhá 4. ročník Středoškolské soutěže v kybernetické bezpečnosti. Podpořte mladé talenty, budoucí experty na kybernetickou bezpečnost a obranu. Více informací na https://www.kybersoutez.cz.

| | |
|---|---|
| 1. 10. 2019 | **Workshop 5G – Strategie, koncepce, zkušenosti a kybernetická bezpečnost**<br>https://www.cybersecurity.cz/5G |
| 23. – 24. 10. 2019 | **AFCEA TechNet Europe - Information Dominance and Cyber Security at various Crossroads – Challenges and Solutions in the Cyber-Physical World**<br>Bratislava, Slovensko<br>https://eu.eventscloud.com/ehome/200190114/TNE19Foreword/ |
| 4. – 5. 11. 2019 | **2. CEE SCADA SECURITY konference**, Hotel DAP, Praha<br>http://future-forces-forum.org/events/default/32_scada-security-conference?lang=cs |