# Seminář

**České pobočky AFCEA a**
**fakulty bezpečnostního managementu Policejní akademie ČR**
*organizovaný ve spolupráci s*
*Národním bezpečnostním úřadem ČR a*
*Národním centrem kybernetické bezpečnosti ČR*

# Computer Emergency Response Team

## *Security Operations Centers (SOC)*

**31. března 2015**

Policejní akademie ČR, Praha

# PROGRAM SEMINÁŘE

**09:30** **Zahájení**
Josef POŽÁR, Děkan, Fakulta bezpečnostního managementu, Policejní akademie ČR v Praze

**09:35** **Úvod do problematiky**
Petr JIRÁSEK, Předseda, Pracovní skupina kybernetické bezpečnosti AFCEA

**09:45** **NCKB/GovCERT.CZ a další spolupracující CERT a bezpečnostní týmy**
Ondřej ŠRÁMEK, NCKB, Národní bezpečnostní úřad ČR

**10:15** **Budování CERT/CSIRT týmu v organizaci**
Andrea KROPÁČOVÁ, Národní CERT, CSIRT.CZ, NIC.CZ
*Přednáška se bude zabývat budováním bezpečnostního týmu typu CERT/CSIRT a jeho ukotvením v organizační struktuře organizace. Probrány budou aspekty od výběru členů týmu, zlepšováním jejich kvalifikace, schopností, definováním služeb týmu, procesů, po nastavení a rozvoj národní a mezinárodní spolupráce. Prezentace bude čerpat ze zkušeností z procesu budování týmu interního typu a Národního týmu.*

**10:55 – 11:20 Přestávka**

**11:20** **Schopnosti a zralost kybernetické obrany organizací**
Petr HNĚVKOVSKÝ, Senior Sales Engineer, ArcSight Specialist, Hewlett-Packard
*20% SOC týmů není vůbec přiraveno reagovat na hrozby ovlivňující jejich organizaci. Jak si stojí Vaše organizace? Umíme měřit efektivitu zabezpečení a využít ji pro kontinuální zlepšení? A jak se vyvarovat opakovaných chybám a slepým uličkám? Málokdo si chce přiznat vlastní chyby, ukažme si pár reálných příkladů i s dopady.*

**11:50** **Budujeme SOC – best practices**
Peter JANKOVSKÝ, Architekt bezpečnostních dohledů NSM Cluster
*SOC – Security Operational Center je v posledních dvou letech často omílaná zkratka. Její opravdový obsah a její opravdový smysl už ale tak známý není. Jak se SOC staví, jak se provozuje a kolik stojí jeho pořízení a provoz? Jaká jsou úskalí implementace? A co nesmíme zanedbat při jeho provozu? Na tyto otázky a ještě spoustu dalších si odpovíme v naší prezentaci.*

**12:15** **Praktické zkušenosti z budování a provozu SOCA**
Ivan SVOBODA, ANECT a.s.

**12:45 – 13:20 Přestávka**

**13:20** **Aktivity CSIRT týmu Active24**
Tomáš HALA, Active24

**13:40** **Dohledové centrum eGovernmentu (SOCCR)**
Jan MIKULECKÝ, Ředitel odboru bezpečnosti a podpory, Česká pošta s.p., o.z. ICT Služby

**14:00** **Forenzní analýza jako doplněk SIEMu**
Jiří SLABÝ, Deloitte Advisory, s.r.o.
*V roce 2014 se začal prosazovat princip, kdy se přední výrobci bezpečnostních SW snaží doplnit nástroje pro usnadnění vyšetřování bezpečnostním technikům přímo do SIEM systémů. Tyto doplňky se snaží být snadno dostupné z jednoho GUI a využívat data z log managementu (logy, toky) i SIEMu (eventy). Společnost IBM zatím jediná takový modul nabízí komerčně. IBM QRadar Incident Forensics modul využívá tzv. packet capture metody (PCAP), kdy krom logů a síťového provozu systém ukládá a analyzuje kompletní pakety síťového provozu. Ty poté parsuje a koreluje s detekovanými incidenty. Je takový přístup tím správným rozvojem SIEM platforem do budoucna?*

**14:20** **Aktivity AFCEA v oblasti kybernetické bezpečnosti**
Petr JIRÁSEK, Předseda, Pracovní skupina kybernetické bezpečnosti AFCEA
- *Plán aktivit Pracovní skupiny kybernetické bezpečnosti AFCEA pro rok 2015-16*
- *Aktivity AFCEA International Cyber Committee*
- *Czech Cyber Security Working Group na LinkedIN*

**14:40** **Závěrečná diskuse**
Moderuje: Petr JIRÁSEK

**15:00** **Závěr**
Josef STRELEC, President, Česká pobočka AFCEA

## Hlavní Partneři

ANECT

## Partneři

Deloitte.

# PŘIPRAVOVANÉ AKCE

19. 5. Konference **SECURITY TRENDS** (IDET 2015 – Brno)
20. 5. Pilotní projekt: **Vzdělávání vedoucích pracovníků v oblasti kybernetické bezpečnosti** (Brno)
16. 6. Seminář: **Sociální sítě a bezpečnost** (místo: bude upřesněno)
30. 9. Seminář: **Kybernetická bezpečnost III** (PA ČR, Praha)
18.11. Seminář: **MLS III** (PA ČR, Praha)
7. – 10. 12. **European Cyber Conference & Exhibition** (Sofie, Bulharsko)

Více informací najdete na internetových stránkách České pobočky AFCEA: **www.afcea.cz**