

## ODBORNÝ SEMINÁŘ

# ICT SECURITY & KYBERNETICKÁ BEZPEČNOST

9:00 – 9:05

### Privítání

9:05 – 9:25

### Kybernetická kriminalita, největší byznys budoucnosti

Dnešní hacking je dobře zavedený sektor ekonomiky. Jeho hodnota se odhaduje někde mezi 450 miliardami až 1 bilionem dolarů. Mají-li manažeři pocit, že se jich kybernetická kriminalita netýká, protože jim nemá kdo, co ukrást, hluboce se mýlí. Dnešní automatizované útočné zbraně umožňují napadat své cíle rovnou po tisících. A hlavně je cíle, které lze snadno dobýt. Krátké zamýšlení a něco statistik na téma ICT bezpečnosti.

*Dag Jeger, JerSoft*

9:25 – 9:50

### O peníze jde až v první řadě

Cílem kybernetické kriminality je vydělat peníze. Cílem ICT bezpečnosti je peníze ochránit. Jak se mění bezpečnostní prostředí ICT, jak se mění přístup k ICT bezpečnosti a lze vůbec ICT zabezpečit bez enormních nákladů?

*Moderovaná diskuse specialistů, do níž se zapojují i účastníci semináře*

9:50 – 10:20

### Aktuální trendy v bezpečnosti

Bezpečnostní expert společnosti ESET software seznámí účastníky prezentace s trendy v oblasti bezpečnosti, probereme aktuální hrozby, sociální inženýrství, stále aktuálnější ransomware, a také bezpečnost mobilních zařízení, která je velmi opomíjená.

*Petr Šnajdr, Eset*

10:20 – 10:30

### Přestávka na kávu

10:30 – 11:15

### Tiskové prostředí – téma pro seminář o bezpečnosti?

Tiskárny a multifunkční zařízení jsou samozřejmě součástí Vaší IT infrastruktury, stejně jako síťové prvky, servery a počítače. Jsou však také součástí úvah o zabezpečení přístupu, dat a dokumentů? V rámci semináře se podíváme na to, zda tiskárny představují potenciální zdroj ohrožení a zda se dá tomuto ohrožení předcházet.

*Jan Honců, HP*

11:15 – 11:45

### SECaaS – Bezpečnost jako služba – v Security Expert Centru O2 IT Services

Bezpečnost jako služba, tzv. SECaaS, je aktuálním tématem současnosti. Proč by se zákazník měl pro tuto formu zajištění bezpečnosti rozhodnout? V podání O2 IT Services služba staví na třech základních pilířích: prevenci, detekci a odpovědnosti. Její neoddelitelnou součástí je bezpečnostní dohled, který je jedním z povinných technických a organizačních opatření dle zákona o kybernetické bezpečnosti č. 181/2014 Sb. Zverme vás na ukázkou typické implementace SECaaS a jak vypadá, když experti bezpečnostního dohledu detekují incident.

1. Proč volit SECaaS aneb výhody oproti tzv. green field a nulovému řešení bezpečnosti.
2. Bezpečnostní dohled jako součást SECaaS. Personální zajištění a režim provozu.
3. Implementace SECaaS a její jednotlivé fáze.
4. Princip detekce a reakce na bezpečnostní incident v Security Expert Centru O2 IT Services.

*Jiří Sedlák, O2 IT Services*

11:45 – 12:15

### Ochrana před DDoS v praxi

Množství DDoS útoků každoročně stoupá. Co dělat, když se na Vás zaměří a jak se proti těmto útokům bránit? Představíme Vám kompletní služby ochrany a ukážeme některé statistiky útoků, které jsme měli možnost nashromáždit za dva roky fungování čistícího centra ComSource FlowGuard.

*Jaroslav Cihelka, ComSource*

12:15 – 13:15

### Přestávka na oběd

13:15 – 13:45

### Ransomware již není hrozbou aneb REVOLUCE V OCHRANĚ ENDPOINTŮ

Stavět nové produkty proti každé nové hrozbě je nesmysl. Intel Security (s McAfee produkty) přichází s řešením, které obrací tradiční paradigma signatur a blacklistů. Nový ransomware a nové typy malware spojuje jedna zásadní vlastnost, ve chvíli útoku je nikdo nezná. A přesně sem míří i Intel Security (McAfee) a neznámé procesy inteligentně zapouzdřuje funkcí Dynamic Application Containment. Neškodné procesy dál nerušeně fungují, ale malware je omezen a nezpůsobuje žádné škody. Z pohledu ochrany koncových bodů se jedná o přelomový nástroj. Představíme si detailně jeho fungování a otestujeme jeho schopnosti i na reálném a aktuálním ransomwaru.

*Jakub Mazal, COMGUARD*

13:45 – 14:15

### Inteligentní Next Generation firewall aneb když obyčejný Next Generation firewall již nestačí

Seznámení s bezpečností platformou výrobce Hillstone pro účinnou ochranu proti neznámým hrozbám a kybernetickým útokům na informační systémy. Inteligentní Next Generation Firewall Hillstone poskytl špičkovou ochranu v reálném čase proti síťovým útokům – virům, spywaru, červům, botnetům, ARP spoofingu, DoS/DDoS útokům, trojským koním atp. Oproti NGFW používá řada iNGFWV kontinuální monitoring provozu a klíčové technologie pro nejvyšší možnou bezpečnost jako Behaviorální analýza, Kill Chain, Mitigace, Statistický clustering.

*Martin Ťupa, Proficomms*

14:15 – 14:45

### Panelová diskuze a tombola

15:00

### Ukončení akce



Seminář pořádá DCD Publishing

[www.dcd.cz](http://www.dcd.cz)

Změna programu vyhrazena.

GENERÁLNÍ PARTNER:



HLAVNÍ PARTNEŘI SEMINÁŘE:

COMGUARD  
communication security

Com Source

eset  
ENJOY SAFER TECHNOLOGY™



O<sub>2</sub> IT Services

PROFICOMMS  
value added distributor