AUTOCONT

AC seminář

2. dubna 2019 / 9.00 - 12.00 / JIC, Purkyňova 649/127, Brno, zasedací místnost „Veselý“, 3.NP.

Soudobé kybernetické hrozby a obrana proti nim

Znát útočníka, jeho motiv, techniky a postupy je základním krokem v obranné strategii proti kybernetickým hrozbám. Na našem semináři se zaměříme na motivy agresorů a slabá místa ve firemních IT. Přehledně si zrekapitulujeme typy útoků a také způsoby, jakými jsou prováděny.

Podrobněji se podíváme na oblast **Malware Defense** a vysvětlíme na konkrétním postupu moderního útoku pojmy jako je **Rootkit, Backdoor, Spyware, Botnet** a další a také jakou mají roli. Dále se zaměříme na to, jak podobným hrozbám čelit. Vysvětlíme si, co to je a jak vzniká **Threat Inteligence**, co je to bezpečnostní score a k čemu se využívá.

V poslední části semináře se budeme věnovat modelování kybernetických hrozeb, proč je důležité modely využívat a které, a v závěru nahlédneme do oblasti detekce bezpečnostních událostí a reakcí na ně.

Program

- 9:00 Registrace a občerstvení, zahájení semináře
- Typy kybernetických hrozeb
- Příklad moderního útoku
- Threat Inteligence
- Modelování kybernetických hrozeb a detekce bezpečnostních událostí
- 12:00 Prostor pro vaše dotazy, ukončení semináře

Za společnost AUTOCONT a.s. vás srdečně zve

Petr Konečný
ředitel regionálního obchodního centra

REGISTRACE:
http://akce.autocont.cz

Zaregistrujte se, prosím, co nejdříve.
Účast je bezplatná, ale kapacita semináře je omezená.

V případě zájmu o další informace k akci kontaktujte Petru Horňákovou
telefon: +420 607 829 584, email: petra.hornakova@autocont.cz