



Enterprise Computing Solutions - Education Services

NABÍDKA ŠKOLENÍ

Prosím kontaktujte nás zde

Arrow ECS, a.s., 28. října 3390/111a, 702 00 Ostrava

Email: training.ecs.cz@arrow.com
Phone: +420 597 488 811

Kód:	DÉLKA:	CENA:
OTH_KYB	8 Hours (1 den)	Kč bez DPH 5,900.00

Description

Cílem kybernetického školení ve virtuální realitě je zvýšit povědomí o kybernetické bezpečnosti a ochraně dat prostřednictvím vlastního zážitku.

Nasadíte si brýle a zažijete útoky na vlastní kůži – naučíte se jim čelit dříve, než nastanou.

Vžijete se do kůže hackera, který má za úkol oklamat oběti v různých organizacích, na odlišných pracovních pozicích a za použití většiny známých technik.

Aktuálně je připraveno 10 scénářů po 15 minutách.

Školení je pořádáno ve spolupráci s firmou ZEBRA SYSTEMS, s.r.o.

Určeno pro

Kurz je určen:

- zaměstnancům různých oddělení, kteří přicházejí do styku s citlivými informacemi nebo využívají podnikové IT infrastruktury — například v technických, administrativních či obchodních rolích,
- pro manažery a lídry týmů: TI, kteří mají odpovědnost za ochranu dat ve firmě, získají přehled o aktuálních kybernetických hrozbách a metodách prevence, což jim umožní efektivně nastavovat bezpečnostní politiku,
- všechny, kdo chtějí posílit svou odolnost vůči kybernetickým hrozbám.

Program

Školením Vás bude provázet lektor a každý účastník si vyzkouší minimálně jeden scénář s headsetem. Ostatní sledují jeho kroky na velké obrazovce. Po ukončení scénáře probíhá diskuse.

Scénář č. 1

Hackněte firmu prostřednictvím instalace viru do počítače zaměstnance.

- Sociální sítě
- Sociální inženýrství
- OSINT (Open Source INTelligence)
- Podezřelé webové stránky
- Phishing
- Trojský kůň

Scénář č. 2

Provedte phishingový útok, abyste vytvořili zombie počítače.

- Zombie farm (Botnet)
- Exploit
- 0 day virus

Scénář č. 3

S pomocí dronu přepravte flash disk obsahující malware.

- Připojování neautorizovaných médií (např. USB) k firemním počítačům

Scénář č. 4

Zašifrujte servery ransomwarem.

- Ransomware
- Silná hesla
- Veřejně dostupné adresy
- Emaily se zašifrovanými soubory

Scénář č. 5

Získejte finanční zprávy prostřednictvím telefonního rozhovoru.

- Telefonní scam
- Fake webs - falešné stránky

- 2FA - dvoufaktorové ověřování

Scénář č. 6

Pošlete dron, aby narušil GSM síť a zřídil veřejně přístupnou WiFi.

- Narušení sítí GSM
- Veřejné WiFi sítě
- Pravidla pro používání veřejných WiFi
- Platby online
- Falešné stránky a platby online

Scénář č. 7

Provedte scam a získejte peníze z bankovních účtů.

- SMS phishing (smishing)
- Využití umělé inteligence

Scénář č. 8

Nastavte filtry v poště a zaměňte firemní fakturu.

- Aplikace na prolomení hesla
- UDF FILE (Uživatelsky Definovaná Funkce)
- E-mailové filtry
- Falešná IP adresa
- Falešné faktury

Scénář č. 9

Hackněte veřejně přístupné kamery a vytvořte efektivní zálohu souborů.

- Zálohování dat
- Archivace šifrovaných dat
- Bezpečné mazání a ochrana citlivých dat
- Internet věcí (IOT)

Scénář č. 10

Zatímco scénáře 1 - 9 osvětlují rizika reálných situací, ke kterým může v pracovním i domácím prostředí dojít, scénář č. 10 představuje imaginární hackerskou techniku, jejímž cílem je uzavřít trénink v pozitivním duchu a po náročném školení se trochu rozhybat.

Termíny školení

Termíny školení na vyžádání, [kontaktujte nás prosím](#)

Dodatečné informace

Školení je možné zajistit na míru. [Kontaktujte nás pro bližší informace.](#)