ProID

Kyberbezpečnost: Trendy a výzvy 2026

Ivo Vrána

Top témata pro rok 2026:

- **Autonomní AI:** Útoky generované AI v reálném čase.
- **Agentic AI:** AI, která nejen radí, ale sama jedná (v útoku i obraně).
- **Post-Quantum Cryptography (PQC) / Crypto-Agility:** Hrozba kvantových počítačů a schopnost rychle měnit šifrovací algoritmy.
- **Digital Provenance:** Ověřování původu digitálního obsahu (boj proti deepfakes).
- **IoT a OT Security:** Zabezpečení technických prvků, ochrana proti odposlechu či falzifikaci dat.
- **Legislativa:** Nastavení interních procesů, dokumentací, splnění norem...

Poznáme ještě realitu?

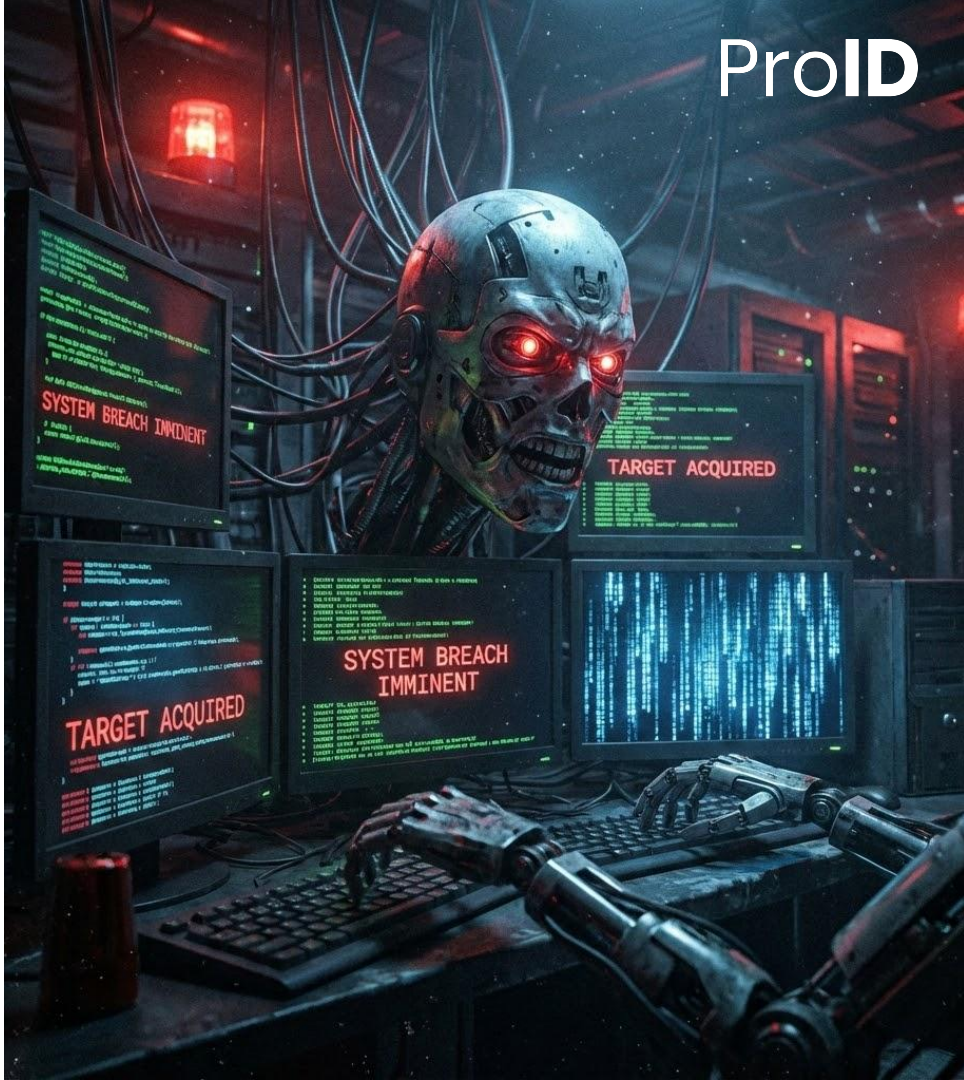
Ukázka Deepfake videa - vygenerované z náhodné fotografie
(https://youtube.com/shorts/ul0HuoPh1lM?si=ilqAFJDuJuUohwrD)


Rok 2026 přinese velké útoky
kompletně řízené AI.

AI na straně útočníků: Éra autonomních hrozeb

V roce 2026 útočníci používají AI k automatizaci celého "životního cyklu" útoku.

- **Autonomní modely:** Nasazení AI agentů, kteří samostatně provádějí průzkum sítě, identifikují zranitelnosti a volí metody průniku bez lidského zásahu.
- **Malware generovaný v reálném čase:** AI neustále upravuje kód malwaru tak, aby se vyhnul detekci tradičními firewally a antiviry. Každá instance útoku je unikátní.
- **Hyper-personalizovaný Social Engineering:** Deepfake technologie v reálném čase napodobují hlas, vzhled či rétoriku konkrétních osob.
- **Shadow AI:** Nekontrolované používání AI nástrojů zaměstnanci.
- **Úniky citlivých dat:** Infikované či špatně nastavené AI nástroje odesílají chráněná data mimo organizaci.



IoT a OT Security – Fyzický svět pod palbou

- V roce 2026 připadá na jednoho zaměstnance průměrně **82 strojových identit**.
- Tisíce neevidovaných chytrých senzorů a kamer tvoří obrovský, neviditelný perimetr.
- Útočníci hrozí fyzickým **poškozením strojů** (např. přetížením turbín).
- Velkým nebezpečím je **ovládnutí přístrojů** na dálku a manipulace s nimi (dávkovače v chemičkách apod.).
- Hacknuté přístroje **odesílají citlivá data** mimo organizaci (GPS souřadnice, naměřené hodnoty atd.).
- Nezabezpečené přístroje jsou často **vstupní branou** do infrastruktury organizace.

Obrana proti hackerským útokům (Nástroje a strategie)

- **Zero Trust Architecture:** Princip "nikdy nevěř, vždy prověřuj". Každý uživatel i zařízení v síti musí být neustále autentizováno.
- **“Tvrdá” kryptografie:** Důsledné šifrování komunikace s využitím nejsilnějších algoritmů a prostředků.
- **Identity-First Security:** Správa identit jako hlavní perimetr. Hesla jsou mrtvá, nastupuje vícefaktorová autentizace (MFA) s biometrikou a hardwarovými klíči.
- **Zálohování a mikrosegmentace:** Zálohy, které nelze přepsat ani smazat (ochrana proti ransomwaru), vždy offline.
- **Nasazení systémů EDR/XDR**, které dokážou v milisekundách detekovat anomálie v chování sítě.
- **Monitoring darknetu:** úniky firemních přihlašovacích údajů, záplat atd.
- **Důsledná aktualizace** legacy systémů, sledování doporučení výrobců atd.

Nová výzva IROP č. 120 – Kybernetická bezpečnost

- **Území:** Středočeský, Jihočeský, Plzeňský, Jihomoravský kraj a Kraj Vysočina.
- **Detaily:** Alokace 2,2 MLD CZK, otevření výzvy březen 2026
- **Pro koho:** Státní organizace a státní podniky, kraje, obce a subjekty poskytující veřejnou službu v oblasti zdravotní péče.
- **Na co lze využít:** Fyzická bezpečnost, nástroje pro ověřování identity uživatelů, nástroje pro řízení přístupových oprávnění, bezpečnost průmyslových a řídicích systémů, atd.

Chcete vědět více? Registrujte se na naše Security Brunche: https://proid.cz/seminare-dotace-irop-2026/

Ivo Vrána

TProduct Marketing Manager

ivrana@monetplus.cz

proid.cz | monetplus.cz

Děkuji!