
ProID
Trendy v bezpečnosti pro firmy
Ivo Vrána

Top trendy pro rok 2026:

- Nastavení správných **procesů** a splnění nové legislativy
- **IoT a OT Security**: Zabezpečení technických prvků, ochrana proti odposlechu či falzifikaci dat.
- Obrana proti útokům řízeným **AI**
- **Zabezpečení přístupů** do systémů a sdílených dat
- Bezpečná **vzdálená práce**
- Obnova a výstavba bezpečné **infrastruktury**
- **Vzdělávání** a vytvoření kultury bezpečnosti


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.

Ivo Vrána

Product Marketing Manager

ivrana@monetplus.cz

proid.cz | monetplus.cz

Děkuji!