Jak se dívá MKB na umělou inteligenci

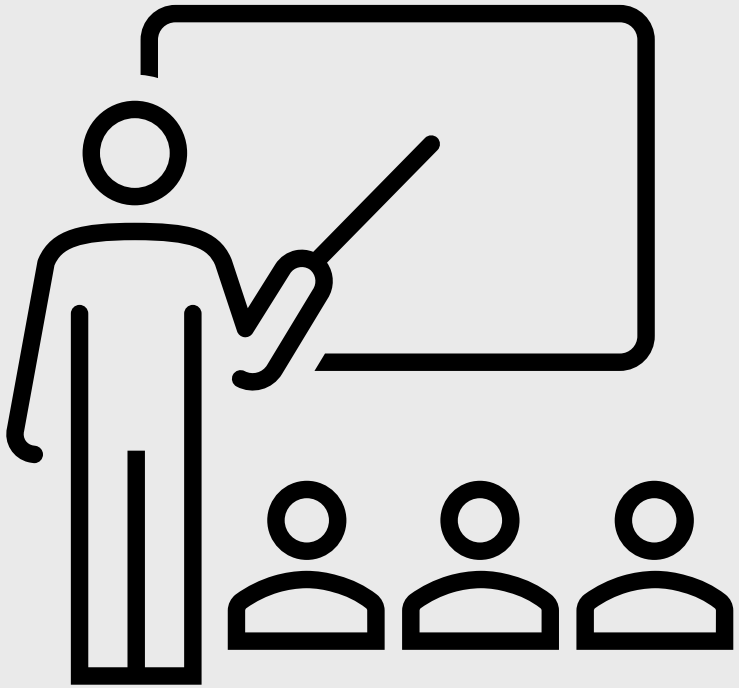
Jiří Kašpar

Manažer kybernetické bezpečnosti

Jihočeské centrum kybernetické bezpečnosti, s.r.o.

Jihočeské centrum kybernetické bezpečnosti

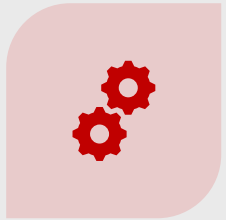
Role manažera kybernetické bezpečnosti



- Řízení rizik
- Nastavování bezpečnostních politik
- Ochrana dat, systémů a infrastruktury
- Nastavení pravidel reakcí na bezpečnostní incidenty

Přínosy AI v kybernetické bezpečnosti

DETEKCE HROZEB V REÁLNÉM ČASE



AUTOMATIZACE BEZPEČNOSTNÍCH PROCESŮ

ANALÝZA VELKÉHO MNOŽSTVÍ DAT (LOGY, SÍŤOVÝ PROVOZ)

ZVÝŠENÍ EFEKTIVITY

RYCHLEJŠÍ REAKCE

SNÍŽENÍ LIDSKÉ CHYBY

AI jako útočný nástroj

- Sociální inženýrství
- Deepfake
- Pomoc při hackování
- Přesvědčivější a efektivnější útoky

AI jako lovec zranitelností

- Tým Anthropic nasadil na Firefox svůj AI model s cílem prověřit, jak si AI poradí s vyhledáváním zranitelností v reálném, dobře zabezpečeném softwaru.

AI jako lovec zranitelností

- Prohlížeč Firefox byl mnohokrát testován a prověřován. Přesto v něm umělá inteligence Claude našla řadu chyb.
- Dvacet minut, první závažná chyba!

Reakce přišla rychle: chyba je reálná. „Co dalšího máte? Pošlete nám víc," reagoval inženýr Mozilly Brian Grinstead.

✓ 112 hlášení

✓ 22 bezpečnostních zranitelností

✓ 14 závažných

Zdroj: https://www.chip.cz/bezpecnost/ai-claude-firefox-chyby

Rizika spojená s AI

- Únik citlivých dat (např. zadání do AI nástrojů)
- Nedostatečná kontrola zdrojových dat pro trénování a validace výsledků
- Nedostatečná kontrola AI systémů
- Šedá zóna AI
- Určení odpovědnosti

M365 Copilot Information Disclosure Vulnerability

- Publikováno: 16. 3. 2026
- CVE: CVE-2026-26133
- Závažnost: 7.4 (HIGH)

Popis zranitelnosti

Zranitelnost umožňuje útočníkovi zneužít MS 365 Copilot tak, že dokáže zjistit citlivé firemní informace. Útočník vytvoří škodlivý obsah (např.: pdf nebo webovou stránku), který obsahuje pro uživatele neviditelné instrukce pro AI asistenta. Pokud Copilot tento obsah zpracuje, vykoná neviditelné instrukce a umožní přístup k citlivým interním informacím. Pro zneužití zranitelnosti je potřeba interakce s uživatelem, který nechá Copilot zpracovat škodlivý obsah.

Zdroj: https://nvd.nist.gov/vuln/detail/cve-2026-26133

Mitigace rizik spojených s AI

- Analýza rizik v procesu implementace AI
- Pravidla pro používání AI (organizační předpisy a směrnice, soulad s EU AI Act, GDPR)
- Školení uživatelů
- Evidence a klasifikace schválených AI systémů
- Monitoring a audit AI systémů
- Zabezpečení AI systémů (MFA)

Závěr

- AI přináší velké výhody, ale i rizika
- Využití AI bude stále rozšířenější
- Vysoký důraz na rovnováhu mezi inovací a bezpečností
- Odpovědné používání AI systémů
- Rostoucí důležitost kybernetické ochrany

Děkuji za pozornost