Centrum kybernetické bezpečnosti

Bezpečnostní seminář

Kybernetická bezpečnost & umělá inteligence

Připravil: Petr Jirásek

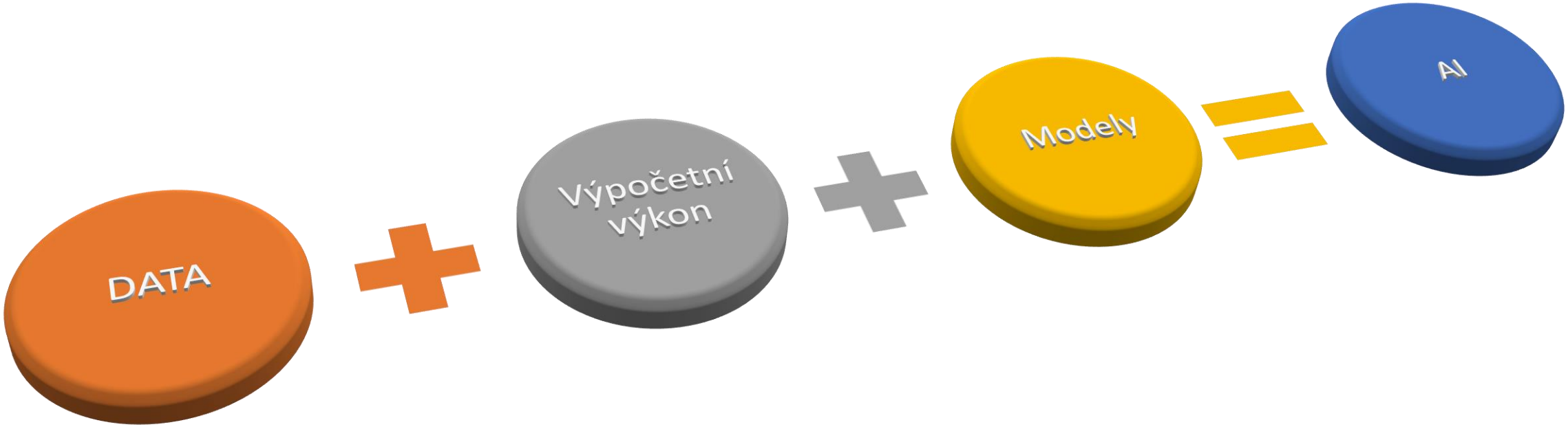
Umělá inteligence

- **Superinteligence** – schopnost počítače překonat člověka ve všech oblastech
- **Umělá obecná inteligence** – představuje schopnost systému na inteligenční úrovni člověka se stejnými schopnostmi zvládání problémů vyžadujícími učení a uvažování.
- **Umělá úzká inteligence** – představuje schopnost systému zpracovávat široký rozsah dat a detekovat v nich vzorce a vztahy, které by byly pro člověka obtížné nebo nemožné
  - **Generativní umělá inteligence** využívá techniky strojového učení k učení a vytváření nových dat (pomáhá vytvořit obsah).
  - **Konverzační umělá inteligence** umožňuje strojům porozumět lidskému jazyku a reagovat na něj „lidským způsobem“.

Strojové učení

- **Strojové učení** je nejen podmnožinou umělé inteligence, ale i nástrojem k dosažení všech výše uvedených kategorií.
- Systémy využívající algoritmy strojového učení nemusí být vždy v učení efektivnější než člověk, ale jsou rychlejší ve zpracování velkého objemu dat.
- Jedná se o techniku umožňující počítačovým systémům pomocí množiny algoritmů analýzu dat za účelem rozeznání zájmových informací bez lidské interakce.

Proč to dnes funguje?



Kybernetická bezpečnost versus Umělá inteligence

- Jak může umělá inteligence pomoci v oblasti kybernetické bezpečnosti
  - Široká automatizace analýzy, detekce a další procesů
    - Analýza zranitelností
    - Detekce hrozeb
    - Odhadování útoků
    - Zvyšování bezpečnosti hesel
- Jak může kybernetická bezpečnost chránit systémy založené na umělé inteligenci
  - Rizika plynoucí z chybné implementace
  - Rizika plynoucí ze zneužití

Nejčastěji požadované dovednosti v KB

- Cloud Computing Security
- Risk Assessment, Analysis, Management
- Security Analysis
- Governance, Risk Management, Compliance
- Threat Intelligence Analysis
- Application Security
- Security Administration
- Penetration Testing
- Data Management Protection

Zdroj: CISA, ENISA

Jak by Vás pozdravila umělá inteligence

Vážení kolegové, rád bych vás přivítal na dnešním setkání, které se zaměřuje na fascinující téma umělé inteligence. V dnešní době umělá inteligence ovlivňuje téměř každý aspekt našich životů a přináší nové možnosti i výzvy. Je důležité, abychom si uvědomili potenciál, ale i rizika spojená s tímto technologickým pokrokem. Během našeho setkání se zaměříme na aktuální trendy, výzkum a aplikace umělé inteligence a společně prozkoumáme, jak můžeme využít její sílu k pozitivnímu posunu naší společnosti. Děkuji vám za vaši účast a aktivní zapojení do diskuse.

Mám pro odborné publikum udělat úvodní slovo na téma umělá inteligence. Co bych jim měl říct? Navrhni mne pět vět.

K

Co by umělá inteligence řekla o svých rizicích?

Je nezbytné si uvědomit, že s pokrokem umělé inteligence přicházejí i nová rizika a etické dilemata, jako je potenciální zneužití osobních dat, ztráta pracovních míst v důsledku automatizace nebo možnost vzniku algoritmické diskriminace. Důsledné zvažování těchto rizik a implementace odpovídajících ochranných opatření je klíčové pro zajištění spravedlivého a bezpečného využívání umělé inteligence. Naše diskuse by měla zahrnovat strategie, jak minimalizovat tyto potenciální negativní dopady a směřovat k udržitelnému rozvoji technologií AI.

Měl bych rovněž říci něco o rizicích umělé inteligence. Poraď co publiku sdělit ve třech větách.

Ohrožené pracovní pozice dle AI

Umělá inteligence a strojové učení výrazně mění dynamiku pracovních pozic v oblasti kybernetické bezpečnosti. Některé typické pozice, které mohou být ohroženy, zahrnují:

1. **Analýza bezpečnostních událostí:** Pokročilé algoritmy AI mohou efektivně analyzovat velká množství dat a identifikovat anomálie nebo potenciální hrozby, což může snížit potřebu manuální analýzy.
2. **Monitorování sítě a detekce hrozeb:** AI může být využita k automatizaci procesu monitorování sítě a detekce hrozeb, což může ovlivnit potřebu lidí pro sledování a reakci na bezpečnostní incidenty.
3. **Zabezpečení aplikací a systémů:** S rostoucí automatizací a autonomií systémů AI mohou být některé pozice v oblasti ručního zabezpečení aplikací a systémů ohroženy.
4. **Testování zranitelností a penetrace:** Technologie AI mohou být využity k automatizaci procesu testování zranitelností a penetrace, což může mít dopad na potřebu manuálních testerů.
5. **Reakce na bezpečnostní incidenty:** AI může být využita k automatizaci procesu reakce na bezpečnostní incidenty, což může ovlivnit potřebu lidských operátorů pro rychlou reakci a řízení krizových situací.

Je důležité si uvědomit, že zatímco některé pracovní pozice mohou být ohroženy automatizací díky AI, zároveň vznikají nové příležitosti a pracovní role vyžadující odborné znalosti v oblasti umělé inteligence a kybernetické bezpečnosti.

Měl bych rovněž říci něco o rizicích umělé inteligence. Poraď co publiku sdělit ve třech větách.

K

Co je podstatné na AI?

Z dnešní akce by účastníci měli odnést následující klíčové poznatky:

1. **Rozvoj technologií AI v kybernetické bezpečnosti:** Porozumění tomu, jak umělá inteligence mění přístup k kybernetické bezpečnosti a jaké nové nástroje a metody jsou k dispozici pro identifikaci a řešení bezpečnostních hrozeb.
2. **Rizika a výzvy:** Pochopení rizik a výzev spojených s používáním umělé inteligence v kybernetické bezpečnosti, včetně otázek týkajících se ochrany dat, etiky a možných zranitelností.
3. **Strategie ochrany a prevence:** Získání znalostí o strategiích a postupech pro minimalizaci rizik spojených s využíváním umělé inteligence v oblasti kybernetické bezpečnosti a implementace odpovídajících opatření ochrany.
4. **Budoucnost kybernetické bezpečnosti:** Diskuse o budoucím směřování kybernetické bezpečnosti v kontextu rostoucí role umělé inteligence a možnostech, které tato technologie přináší pro zlepšení ochrany dat a sítí.
5. **Spolupráce a sdílení znalostí:** Podpora spolupráce a sdílení znalostí mezi účastníky s cílem posílit schopnost odolávat kybernetickým hrozbám v prostředí, kde umělá inteligence hraje stále větší roli.

Tyto poznatky by měly účastníkům poskytnout ucelený pohled na současný stav a budoucnost kybernetické bezpečnosti v kontextu rostoucí role umělé inteligence.

Jaké podstatné poznatky by si účastníci tohoto odborného fóra měli z dnešní akce odnést?