Prípadová štúdia

Vývoj a implementácia štandardizovaného procesu kvalifikácie AI dodávateľov

---

Výzva:

Spoločnosť DÔVERA zdravotná poisťovňa, a.s. čelila výzve štandardizovať kvalifikačný proces hodnotenia dodávateľov umelej inteligencie (AI) a ich riešení. Cieľom bolo vytvoriť optimálnu kontrolnú metodiku, umožňujúcu identifikáciu potenciálnych rizík vyplývajúcich z obstarania a implementácie AI riešení. Metodika mala tiež zohľadňovať biznis prínos a inovatívnosť riešení v kontexte indentifikovaných rizík. Kľúčovým predpokladom bolo získať kompletný obraz o AI dodávateľoch, ich riešeniach, možných rizikách v dodávateľskom reťazci, zavedených bezpečnostných praktikách, vývojových procesoch a o súlade s legislatívnymi požiadavkami. To umožní kvalifikované posúdenie rizík a potenciálnych prínosov pre biznis procesy organizácie.

Výzvu sme riešili na viacerých úrovniach:

1. **Vytvorenie a implementácia štandardizovaného procesu hodnotenia dodávateľov AI riešení**, zahŕňajúci kvalitu AI riešení, kybernetickú bezpečnosť a realizovateľnosť riešení z pohľadu interných rizík
2. **Identifikácia právnych povinnosti** pre klienta vyplývajúcu z nových regulácií ako napr. nariadenie EÚ Akt o AI
3. **Posúdenie a príp. úprava organizačnej štruktúry** umožňujúcej implementáciu a správu životného cyklu AI riešení

Riešenie:

Na riešenie týchto výziev sme vyvinuli metodiku založenú na osvedčených postupoch z rámcov *NIST AI Risk Management Framework (RMF), NIST Cybersecurity Supply Chain Risk Management Framework* a v súlade s nariadením *EÚ Akt o AI*. Postupy a odporúčania boli konkretizované na základe vstupov zo strany viacerých tímov klienta a AI dodávateľov. Naše riešenie obsahovalo:

1. **Nástroj pre preverenie AI dodávateľov:** Dotazník, ktorý hodnotil pripravenosť AI dodávateľov z pohľadu:
    - Kvality AI systému/modelu a etických štandardov
    - Súladu s EÚ Aktom o AI a s tým spojenými právnymi normami
    - Kybernetickej bezpečnosti v organizácii dodávateľa
    - Realizovateľnosti riešenia v rámci ekosystému klienta
2. **Identifikáciu právnych požiadaviek:** Identifikovali sme kľúčové právne povinnosti, podľa EÚ Aktu o AI a v kombinácii s odporúčaniami z NIST rámcov sme zadefinovali konkrétne bezpečnostné a technické opatrenia, ktoré musia byť implementované
3. **RACI maticu pre organizačnú štruktúru:** Navrhli sme RACI maticu pre zefektívnenie internej štruktúry organizácie za účelom úspešnej adopcie AI v organizácii

---

Implementácia a výsledky:

V úzkej spolupráci s klientom sme úspešne vykonali niekoľko auditov AI dodávateľov pomocou vyvinutej štandardizovanej metodiky. Audity priniesli nasledujúce praktické výsledky:

- **Odporúčania a návody:** organizačným jednotkám sme poskytli informácie a odporúčania pre schválenie resp. zamietnutie AI dodávateľov a ich riešení
- **Realizácia PoC:** Schválení dodávatelia môžu realizovať Proof of Concept (PoC) v zabezpečenom prostredí cloudového sandboxu v Microsoft Azure. Sandboxy budú vybudované na základe osvedčených postupov a Microsoft Azure politík, ktoré budú kontinuálne vynucovať dodržiavanie vysokých bezpečnostných štandardov

Kľúčové zistenia:

- Vzhľadom na relatívne málo prebádanú oblasť AI riešení je nutné podrobiť AI dodávateľov dôslednej previerke s dôrazom na ich stabilitu, reputáciu, organizačné štruktúry, bezpečnostné postupy, znalosti využívaných AI modelov a legislatívnych noriem. Štandardizovaný proces a dotazník nám umožnili zistiť skutočnosti, ktoré vieme zohľadniť v budúcich zmluvných podmienkach
- Proces auditov odhalil aj dôležité informácie, ktoré neboli na prvý pohľad zrejmé ako napr. (ne)pripravenosť dodávateľov riešiť potenciálne technické, biznisové, etické či legislatívne problémy a celkovú realizovateľnosť riešení v kontexte integrácie do klientovho prostredia

Poučenia z procesu hodnotenia:

- Diskusie s AI dodávateľmi a hodnotenie ich pripravenosti z viacerých uhlov pohľadu vyžadovali značnú investíciu času a úsilia viacerých tímov, ale v konečnom dôsledku umožnili výrazne hlbšie pochopenie ich pripravenosti a potenciálnej hodnoty konkrétnych AI riešení pre klienta
- Investovaný čas umožnil priebežné zdokonaľovanie metodiky a tým aj vyššiu efektivitu a adresnosť diskusií, kvalitu výstupov a hodnotu prínosov do rozhodovacieho procesu

---

Záver:

Tento projekt jasne ukázal dôležitosť štruktúrovaného a komplexného prístupu k hodnoteniu AI dodávateľov. Implementácia metodiky založenej na uznávaných rámcoch, štandardoch a legislatívnych normách pomohla klientovi prijímať informované rozhodnutia a zabezpečiť, že len kvalifikovaní dodávatelia môžu pokračovať v realizácii v zabezpečnom prostredí. Súčasťou ďalších krokov bude dôsledná aplikácia identifikovaných bezpečnostných opatrení a governance princípov pre kontinuálnu adopciu inovatívnych AI riešení vrámci spoločnosti DÔVERA zdravotná poisťovňa, a.s.

DÔVERA zdravotná poisťovňa, a. s., je najväčšia súkromná zdravotná poisťovňa na Slovensku zabezpečujúca zdravotnú starostlivosť pre 1,7 milióna poistencov.