Program Slovensko

Newsletter
1/2026

Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom

cybersecurityresearch.sk

Spolufinancovaný Európskou úniou

PROGRAM SLOVENSKO

MINISTERSTVO ŠKOLSTVA, VÝSKUMU, VÝVOJA A MLÁDEŽE SLOVENSKEJ REPUBLIKY

Projekt: Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom

Projekt Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom reaguje na rastúcu sofistikovanosť kybernetických hrozieb , pri ktorých tradičné bezpečnostné riešenia založené na signatúrnej detekcii prestávajú byť účinné. Útočníci čoraz častejšie využívajú kombináciu automatizovaných techník, umelej inteligencie a behaviorálnej manipulácie, čo si vyžaduje prechod od reaktívnych prístupov k prediktívnym a adaptívnym modelom detekcie.

Hlavným cieľom projektu je výskum metód, postupov a nástrojov na efektívnu detekciu pokročilých kybernetických útokov využívajúcich konkrétne útočné taktiky, ako sú exploatácia, laterálny pohyb a eskalácia privilégií v súlade s rámcom MITRE ATT&CK. Dôraz sa kladie na analýzu techník, podtechník a procedúr (TPP), identifikáciu ich charakteristických znakov a odhalenie limitov existujúcich detekčných prístupov.

Projekt sa zároveň zameriava na behaviorálnu analýzu útokov, identifikáciu indikátorov kompromitácie (IoC) a indikátorov správania (IoB), ako aj na návrh pokročilých modelov využívajúcich strojové učenie a umelú inteligenciu pre detekciu anomálií v rôznych fázach útoku. Súčasťou riešenia je aj optimalizácia presnosti a efektivity detekčných modelov a ich testovanie v realistických podmienkach prostredníctvom simulácie kybernetických útokov.

Navrhované riešenie prispieva k zvýšeniu odolnosti digitálnej infraštruktúry, podpore rozvoja domácich výskumných kapacít, transferu znalostí medzi akademickou a priemyselnou sférou a posilnenie kybernetickej odolnosti Slovenska v európskom kontexte

Medzi hlavné výstupy projektu patrí výskumná správa o taktikách a technikách kybernetických útokov, simulačná platforma pre analýzu a detekciu hrozieb, pokročilé modely strojového učenia a štatistického učenia, ako aj správy o penetračných testoch a výkonnostné porovnania detekčných modelov.

Spolufinancované Európskou úniou prostredníctvom Programu Slovensko v rámci projektu č. NFP401101C360: Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom.

Spolufinancovaný Európskou úniou
PROGRAM SLOVENSKO
MINISTERSTVO ŠKOLSTVA, VÝSKUMU, VÝVOJA A MLÁDEŽE SLOVENSKEJ REPUBLIKY

Projekt vyvíja pokročilé AI riešenia pre detekciu kybernetických hrozieb

Výskumné aktivity projektu NFP401101C360: Výskum a vývoj pokročilých riešení umelej inteligencie na detekciu kybernetických hrozieb a obranu proti sofistikovaným útokom prinášajú nové prístupy k detekcii sofistikovaných kybernetických hrozieb s využitím strojového učenia a behaviorálnej analýzy útokov.

Projekt sa sústreďuje na vývoj metód a nástrojov umožňujúcich spoľahlivú detekciu sofistikovaných kybernetických útokov. Zameriava sa najmä na tie využívajúce exploatáciu, laterálny pohyb a eskaláciu privilégií podľa rámca MITRE ATT&CK. Výskum zároveň analyzuje limity súčasných detekčných prístupov a hľadá možnosti zvýšenia ich presnosti v reálnych podmienkach.

Dôležitou súčasťou riešenia je podrobná analýza techník, podtechník a procedúr (TTP). Pri týchto technikách je potrebné vykonať identifikáciu ich charakteristických prejavov a skúmanie nástrojov využívaných pri realizácii útokov. Súčasťou projektu je aj simulácia kybernetických incidentov v bezpečnom testovacom prostredí a overovanie rôznych scenárov detekcie.

Predmetom výskumu je aj behaviorálna analýza kybernetických útokov založená na skúmaní forenzných a sieťových dát. Cieľom je identifikácia indikátorov kompromitácie (IoC) a indikátorov správania (IoB), ako aj určenie parametrov operačných systémov a sieťovej komunikácie, ktoré prispejú k efektívnejšej detekcii kybernetických hrozieb.

Významnou časťou projektu je návrh nových modelov založených na strojovom učení, umelej inteligencii a matematických modeloch. Modely sa využívajú pre detekciu anomálií a útokov vo viacerých fázach kompromitácie systému. Pozornosť sa venuje aj optimalizácii výkonnosti detekčných modelov s dôrazom na presnosť, citlivosť a znižovanie výpočtových nárokov.

Projekt zároveň prispieva k rozvoju odborných kapacít v oblasti kybernetickej bezpečnosti. Výsledky výskumu budú postupne integrované do univerzitných predmetov zameraných na kybernetickú a informačnú bezpečnosť, ako aj dátovú analytiku.

Riešitelia projektu na konferencii o krízovom riadení

Riešitelia projektu prof. Ing. Milan Kubina, PhD. a prof. Ing. Pavel Segeč, PhD. sa zúčastnili konferencie *Riešenie krízových situácií v špecifickom prostredí*, ktorá sa konala pod záštitou Žilinskej univerzity v Žiline a Ministerstva vnútra SR.

Z pohľadu riešeného projektu ich najviac zaujala panelová diskusia na tému Aktuálne otázky regulácie informačnej a kybernetickej bezpečnosti na Slovensku, v rámci ktorej odzneli podnetné názory na súčasné výzvy a smerovanie kybernetickej bezpečnosti.

Spolufinancovaný Európskou úniou
PROGRAM SLOVENSKO
MINISTERSTVO ŠKOLSTVA, VÝSKUMU, VÝVOJA A MLÁDEŽE SLOVENSKEJ REPUBLIKY