Rozšírené zadanie diplomovej práce

Názov práce: Predikcia situačného povedomia v kybernetickej bezpečnosti pomocou metód neurónových sietí

Autor práce: Bc. Jakub Mohler

Vedúci práce: doc. RNDr. JUDr. Pavol Sokol, PhD.

Konzultant: RNDr. Richard Staňa

Ciele:

1. Vytvoriť dátovú sadu časových radov pre analýzu situačného povedomia v kybernetickej bezpečnosti.
2. Preskúmať existujúce metódy neurónových sietí na predikciu situačného povedomia v kybernetickej bezpečnosti.
3. Navrhnúť model pre predikciu situačného povedomia v kybernetickej bezpečnosti a vyhodnotiť úspešnosť tohto modelu s existujúcimi výsledkami.
4. Navrhnúť a implementovať systém na interaktívnu grafickú reprezentáciu jednokrokových a viackrokových predikcií.

Popis:

Využitie nových technológií so sebou prináša nové typy bezpečnostných hrozieb a bezpečnostných incidentov. Ich počet neustále rastie Z tohto dôvodu sa im musíme vedieť efektívne brániť. Kybernetická bezpečnosť sa stáva stále viac dôležitou, a preto organizácie investujú peniaze na ochranu svojej infraštruktúry.

Klasický prístup k tejto problematike bol postavený na základe reaktívnych činností. Súčasným trendom je prechod od reaktívnych činností (riešenie, resp. koordinovanie bezpečnostného incidentu) k proaktívnym činnostiam (aktívne vyhľadávanie zraniteľností, tzv. threat hunting). Teda snažiť sa už vopred pripraviť na bezpečnostné hrozby, ktorým čelíme a v najlepšom prípade úplne zabrániť vzniku bezpečnostného incidentu [1].

Hlavným cieľom práce je navrhnúť model, ktorý by dokázal úspešne predikovať situačné povedomie v kybernetickej bezpečnosti. Následne sa tento model bude implementovať do systému na grafickú reprezentáciu predikcií. Vďaka tomu by sme vedeli automatizovane porovnávať predikciu s aktuálnym stavom a vyhľadávať anomálie v týchto rozdieloch. Nájdenie anomálie môže generovať upozornenia (napr. SIEM), na základe ktorých sa môžu vykonať ďalšie činnosti [2].

Tento hlavný cieľ je bližšie konkretizovaný v štyroch podcieľoch. Súčasťou prvého cieľa práce je zameriame sa na vytvorenie dátovej sady časových radov pre analýzu situačného povedomia v kybernetickej bezpečnosti. Dáta, ktoré bude treba pripraviť a preskúmať rôzne korelácie týchto dát, sú zozbierané z honeypotov rozmiestnených na univerzite.

Súčasťou druhého cieľa bude preskúmať existujúce metódy neurónových sietí na predikciu situačného povedomia v kybernetickej bezpečnosti. V tejto časti bude potrebné preštudovať viaceré výskumné články, ktoré sa venujú danej problematike. Vychádzať budeme z predošlého výskumu uvedeného v článku [3].

Na základe zistení z preskúmania existujúcich metód sa v cieli tri zameriame na navrhnutie modelu pre predikciu situačného povedomia v kybernetickej bezpečnosti. Následne tento model otestujeme a vyhodnotíme jeho úspešnosť s výsledkami existujúcich prístupov.

V poslednom cieli je potrebné navrhnúť a implementovať riešenie na interaktívnu grafickú reprezentáciu predikcie sieťového bezpečnostného povedomia. Ako základ chceme využiť technológie použité v systéme T-pot – honeynete[1]. Tento systém nám umožní zbierať dáta z rôznych typov honeypotov (pascí na útočníkov) a ukladať do nosql databázy Elastic [4]. Tieto údaje budú tvoriť základ pre samotnú predikciu. Súčasne T-pot obsahuje systém Kibana, v rámci ktorého je možné implementovať časť, ktorá bude predikovať situačného povedomia a informovania správcov o vývoji.

Literatúra:

1. Husák, M., Jirsík, T., & Yang, S. J. (2020, August). SoK: contemporary issues and challenges to enable cyber situational awareness for network security. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-10).

[1] https://github.com/telekom-security/tpotce

2. Husák M, Komárková J, Bou-Harb E, Čeleda P. Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials. 2018 Sep 24;21(1):640-60.
3. Stana, R., Patrik, P., Gajdos, A., Pavol, S.: Network security situation awareness forecasting based on neural networks. 8th International conference on Time Series and Forecasting.
4. Elastic. [online] Dostupné z: https://www.elastic.co/