Rozšírené zadanie diplomovej práce

Názov práce: Manažment bezpečnostných informácií a udalosti pre akademický informačný systém

Autor práce: Bc. Eva Marková

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

Ciele:

(1) Analýza aktuálnych prístupov k manažmentu bezpečnostných informácií a udalosti (SIEM).
(2) Návrh dátového modelu a pravidiel detekcie bezpečnostných hrozieb pre akademický informačný systém zohľadňujúc bezpečnostné riziká podľa ISO/IEC 27000 a MITRE ATT&CK rámec.
(3) Návrh, implementácia a optimalizácia SIEM systému pre akademický informačný systém.

Popis:

Informačné systémy sú v organizáciách častokrát kritickými infraštruktúrami, ktoré je potrebné zabezpečiť a zabúda sa na nich, až do chvíle kým nie je zaznamenaný bezpečnostný incident. Ide o infraštruktúru (informačné a komunikačné prostriedky), ktorých znefunkčnenie, resp. ochromenie má za následok negatívny vplyv na organizáciu a jej procesy. V akademickom prostredí sú najdôležitejšími procesmi zabezpečenie výučby a výskumnej činnosti. Z tohto dôvodu môžeme okrem iných zaradiť medzi kritickú infraštruktúru akademických inštitúcií aj akademický informačný systém. V rámci tohto systému sa kumuluje veľké množstvo osobných, citlivých údajov, ktoré je potrebné chrániť a zabrániť ich narušeniu.

Z pohľadu minimalizácie dopadov bezpečnostných incidentov je elementárne dôležitá detekcia bezpečnostných útokov nevynímajúc vyhodnotenie bezpečnostných udalostí a informácií. K tomuto účelu využívame systémy na manažment bezpečnostných informácií a udalostí (SIEM). Spustenie úspešného systému SIEM vyžaduje, aby boli identifikované aktíva, siete, nepoužívané siete, aplikácie a privilegované účty. Potom musí centrum

bezpečnostných operácií (Security operations center, SOC) pochopiť, ktoré aktíva ovplyvňujú ktoré procesy a aplikácie, implementovať monitorovanie a pochopiť, ako útočník myslí a následne implementovať pravidlá, pomocou ktorých ich identifikuje [1]. SIEM systém v sebe predstavuje kombináciu štyroch prvkov [3]:

- Manažment bezpečnostných informácií (Security information management, SIM) ukladá, analyzuje, manipuluje a podáva správy o bezpečnostných záznamoch.
- Manažment bezpečnostných udalostí (Security event management, SEM) monitoruje systémy v reálnom čase a je zameraný na záznamy udalostí, ktoré sú generované z rôznych zariadení.
- Systém manažovania logov (Log Management System, LMS) zhromažďuje a ukladá logy z rôznych systémov a hostiteľov.
- Korelácia bezpečnostných udalostí (Security Event Correlation, SEC) je prístup, ktorý sleduje sled udalostí, ktoré naznačujú potenciálnu hrozbu a upozorňuje správcov.

Hlavným cieľom práce je navrhnúť vhodný SIEM systém, ktorý by zohľadňoval akademické prostredie a aktíva, zraniteľnosti, hrozby a typy útočníkov akademických informačných systémov. Z logov systému by tento systém mal byť schopný detegovať relevantnú množinu hrozieb, ktorým by mohol v budúcnosti čeliť práve akademický informačný systém. Plánujeme, aby implementovaný SIEM bol ľahko prispôsobiteľný pre rôzne akademické informačné systémy.

Tento hlavný cieľ práce je bližšie konkretizovaný v troch podcieľoch. V prvom cieli práce sa zameriame na analýzu a porovnanie aktuálnych prístupov k manažmentu bezpečnostných informácií a udalosti (SIEM). Jednou z možností je porovnanie implementácií rôznych SIEM systémov ako napríklad Splunk [4], Elastic Siem [5], AlienVault [6], IBM QRadar [7] atď. Tiež chceme SIEM systémy porovnať podľa toho, aký princíp modelovania bezpečnostných hrozieb využívajú. Na základe vykonanej analýzy sa rozhodneme, aký SIEM systém je pre riešenie nášho problému najvhodnejší.

Súčasťou druhého cieľa je pripraviť podrobnú analýzu bezpečnostných rizík pre akademický informačný systém na našej univerzite podľa noriem ISO/IEC 27000 vrátane zohľadnenia MITRE ATT&CK rámca. Tento rámec nám primárne poslúži na špecifikáciu relevantných bezpečnostných hrozieb a zraniteľností.. MITRE ATT&CK [8] je

celosvetovo dostupná vedomostná základňa protichodných taktík a techník založená na pozorovaniach v reálnom svete. Používa sa ako základ na vývoj špecifických modelov a metodológií bezpečnostných hrozieb. MITRE prístup je založený na piatich princípoch [9]:

- zahŕňa „Post-Compromise“ detekciu,
- zameriava sa na správanie,
- používa model založený na hrozbách,
- iteruje podľa návrhu a
- vyvíja a testuje sa v realistickom prostredí.

Vybrané hrozby odsimulujeme na testovacom serveri, aby sme následne boli schopní vytvoriť pravidlá pre detekciu útokov na akademickom informačnom systéme. Tiež bude potrebné navrhnúť dátový model, s ktorým budeme pracovať.

Posledným cieľom je návrh a implementácia samotného SIEM systému pre akademický informačný systém. Aby bol systém efektívny, je potrebné zamerať sa aj na optimalizáciu nami zadefinovaných pravidiel na detekciu.

Literatúra:

(1) MURDOCH, D. W. SOC, SIEM, and Threat Hunting (V1.02): A Condensed Guide for the Security Operations Team and Threat Hunter. Independent Publishing, 2019.
(2) COLLINS, Michael. Network Security Through Data Analysis: From Data to Action. O'Reilly Media, Inc., 2017.
(3) SIEM [online]. [cit. 2019-12-02]. Dostupné z: https://logdna.com/what-is-siem/
(4) Splunk [online]. [cit. 2019-12-02]. Dostupné z: https://www.splunk.com/en_us/siem-security-information-and-event-management.html
(5) Elastic [online]. [cit. 2019-12-02]. Dostupné z: https://www.elastic.co/products/siem
(6) AlienVault [online]. [cit. 2019-12-02]. Dostupné z: https://www.alienvault.com/solutions/siem-log-management
(7) IBM QRadar [online]. [cit. 2019-12-02]. Dostupné z: https://www.ibm.com/us-en/marketplace/ibm-qradar-siem
(8) Rámec Mitre Attack [online]. [cit. 2019-12-02]. Dostupné z: https://attack.mitre.org/
(9) STROM, Blake E., et al. Finding cyber threats with ATT&CK-based analytics. Technical Report MTR170202, MITRE, 2017.