KATEDRA INFORMATIKY
A VÝPOČETNÍ TECHNIKY

Martin Šebela

Diplomová práce

Inženýrská informatika
Softwarové inženýrství
2020/2021

Vedoucí práce:
Ing. Jiří Čepák
WEBnet Incident Response Team (WIRT)
CIV ZČU

FAKULTA
APLIKOVANÝCH VĚD
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

Systém pro správu bezpečnostních incidentů v síti WEBnet

Abstrakt

Diplomová práce se zabývá problematikou kyberbezpečnosti, a to konkrétně popisem bezpečnostních týmů typu CERT/CSIRT a popisem postupů a metod používaných při řešení bezpečnostních incidentů. Následuje analýza nejčastějších a nejzávažnějších bezpečnostních incidentů, které jsou řešeny univerzitním bezpečnostním týmem na ZČU. Na základě analýzy a současného stavu jsou specifikovány požadavky na software, který je výstupem diplomové práce. Implementovaný systém typu CAIH (Computer-aided Incident Handling) je navržen jako intuitivní a modulární a integruje několik existujících informačních systémů. Systém umožňuje po zadání data a času a libovolné IP adresy z rozsahu ZČU, vyhledat související záznamy v logu a provést blokaci, či následné odblokování konkrétního uživatele nebo zařízení v síti ZČU. Výsledky diplomové práce ukazují, že po nasazení implementovaného systému do ostrého provozu byla snížena doba nutná k vyřešení bezpečnostního incidentu v průměru až pětinásobně oproti manuálnímu postupu a až trojnásobně oproti dosud používanému nástroji.

Úvod

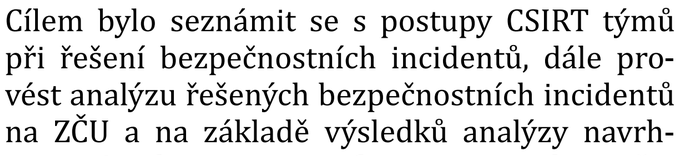
Cílem bylo seznámit se s postupy CSIRT týmů při řešení bezpečnostních incidentů, dále provést analýzu řešených bezpečnostních incidentů na ZČU a na základě výsledků analýzy navrhnout a implementovat software pro podporu řešení bezpečnostních incidentů, který proces řešení incidentu usnadní, zefektivní a automatizuje. Implementovaný systém bylo cílem otestovat v reálném provozu na ZČU.

Východiska, analytická část

Na základě provedené analýzy incidentů řešených na ZČU bylo zjištěno, že existuje množina incidentů, u nichž je shodný postup u analytických a komunikačních kroků. V podstatě se jedná o posloupnost kroků viditelných na obr. 1.

V každém z kroků se navíc řeší několik dalších činností, jako např. komunikace s původcem incidentu, se stěžovatelem nebo obsluha systémů, které umožní původce incidentu (od)blokovat.

Protože se ale vždy jedná o shodný postup, na jehož vstupu je IP adresa a datum a čas výskytu incidentu, bylo by vhodné mít nástroj, který činnosti v jednotlivých krocích automatizuje a celý proces řešení incidentu zrychlí a zefektivní.



Obr. 1: Kroky při řešení bezpečnostního incidentu.

Hlavní aspekty realizace

Vytvořený CAIH systém byl realizován jako webová aplikace, jejímž cílem bylo proces řešení incidentu co nejvíce zjednodušit a zefektivnit.

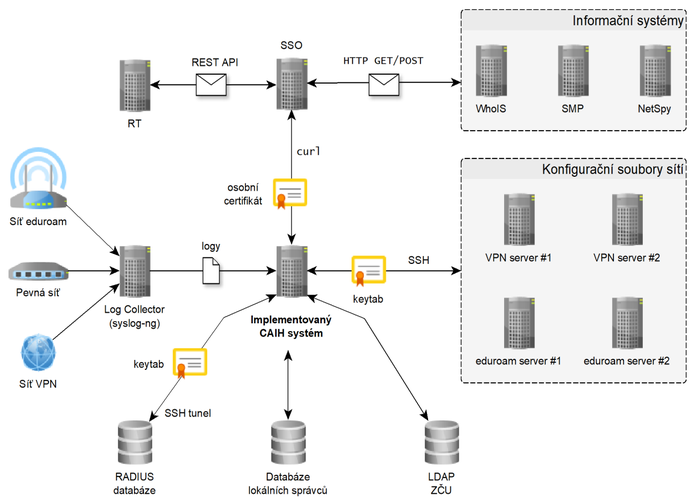
Klíčovou součástí aplikace jsou především moduly obsluhující jednotlivé části univerzitní sítě *WEBnet* (*eduroam*, VPN a pevná síť). Každý modul musí dle navrženého rozhraní umožňovat:

- vyhledat záznamy o libovolné IP adrese z IP rozsahu ZČU (147.228.0.0/16) v libovolný datum a čas,
- zablokovat původce incidentu (uživatele nebo zařízení), který měl danou IP adresu ve zvolený datum a čas přidělenou,
- odblokovat původce incidentu.

Díky jednotnému rozhraní nezávislého na typu sítě je možné systém dále rozšiřovat o nové moduly, které budou spravovat další oblasti sítě.

Integrace s univerzitními systémy

Klíčovou částí práce byla integrace s již existujícími systémy na ZČU (viz obr. 2). Každý z integrovaných systémů má navíc jiný účel nebo je určen pro jiný typ sítě. Zatímco současný stav vyžadoval manuální obsluhu většiny systémů (nebo serverů a databází), implementovaný CAIH systém tuto činnost automatizuje.



Obr. 2: Schéma zachycující integraci s již existujícími univerzitními systémy, servery, databázemi, a to včetně způsobu autentizace a komunikace.

Dosažené výsledky

Implementovaný CAIH systém byl nasazen do ostrého provozu na ZČU a je využíván pracovníky bezpečnostního týmu WIRT k řešení bezpečnostních incidentů v univerzitní síti *WEBnet*.

Výsledky porovnávající stav před a po nasazení vytvořeného CAIH systému ukazují, že řešení incidentu je po nasazení systému v průměru až:

- 5× rychlejší oproti manuálnímu postupu,
- 3× rychlejší oproti dosud používanému nástroji.

Maximální doba řešení incidentu v CAIH systému byla 2:50, a to včetně režijních činností.

Závěr

Výstupem diplomové práce je přehled postupů používaných CSIRT týmy při řešení incidentů, ale především implementovaný CAIH systém.

Systém univerzitnímu bezpečnostnímu týmu usnadnil, sjednotil a zefektivnil proces řešení bezpečnostních incidentů nezávisle na tom, v jakém typu sítě k incidentu došlo. Reakce na incident je tak maximálně v jednotkách minut.

Díky CAIH systému odpadne i dlouhé školení nových pracovníků, snížení nutné kvalifikace a přidělování oprávnění k přístupu k serverům.