Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **BC. KINCL JAN** **Oponent:** **Ing. Ladislav Vyskočil**

Studijní program: **Inženýrská informatika**
Studijní obor/Specializace: **Kybernetická bezpečnost**
Akademický rok: **2021/2022**

Téma diplomové práce: **Zabezpečení a monitoring rozsáhlých IT infrastruktur**

Hodnocení práce:

Cílem diplomové práce bylo popsat problematiku zabezpečení a monitoringu rozsáhlých IT infrastruktur, k jehož dosažení bylo třeba naplnit několik bodů, jejichž přesná specifikace byla součástí zásad uvedených v zadání práce. Všechny body zadání diplomové práce byly splněny v plném rozsahu. Diplomant popisované problematice rozumí. Náročnost a rozsah diplomové práce hodnotím velmi dobře.
Diplomová práce je přehledně strukturována a jednotlivé části na sebe logicky navazují. Text práce je zpracován srozumitelně. Po jazykové stránce nebyly nalezeny žádné pravopisné, nebo stylistické chyby. Po formální stránce je práce vhodným způsobem řazena do logických celků a doplněna upřesňujícími komentáři i odkazy na odpovídající literární či elektronické zdroje. V diplomové práci autor uvádí přiměřené množství obrázků, tabulek a příloh k objasnění popisované problematiky.

V teoretické části byla popsána problematika IT infrastruktur, jejich možnosti členění, proces tvorby zabezpečené infrastruktury s uvedením možných hrozeb a zranitelností, monitorování IT infrastruktur a charakter získaných dat. Dále byly popsány požadavky při návrhu monitorovacího systému a jeho přínosy. Poslední část teoretické části je zaměřena na přehled existujících monitorovacích systémů, popis vybraných řešení a jejich srovnání. Obsah teoretické části je přehledně popsán s ohledem na nejčastěji požívaná řešení a problémy v praxi.

Praktická část obsahuje rozsáhlý popis řešené infrastruktury a identifikace jejích kritických prvků, návrh a požadavky implementace monitorovacího systému, volbu řešení a možnosti integrace systému ZABBIX pro řešenou infrastrukturu. V další části je popsána implementace systému ZABBIX v testovací infrastruktuře, zahrnující instalaci systému ZABBIX, scénáře použití a možnosti využití ZABBIX agenta pro monitoring zařízení. Dále je popsáno získávání dat ze sledovaných zařízení, monitoring zařízení nepodporujících ZABBIX agenta a grafická vizualizace v systému ZABBIX.Na závěr praktické části byly popsány možnosti detekce provozních výpadků a kybernetických útoků, vyhodnocení provozních výpadků a identifikace bezpečnostních incidentů. Bylo rovněž popsáno rozšíření implementace o systém OSSIM AlienVault pro detekci a automatickou klasifikaci bezpečnostních incidentů.

Přínosem práce je přehledný a podrobný popis dané problematiky, kdy diplomová práce může sloužit jako vzorový návod pro mnohá řešení v praxi. Diplomová práce se jeví jako velmi zdařilá a splňující svůj cíl, a proto ji doporučuji předložit k obhajobě.

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Otázka k obhajobě:
Jaké by bylo ideální řešení pro zabezpečení a monitoring koncových zařízení, která nejsou majetkem společnosti, ale využívají firemní IT infrastrukturu? (např. soukromé notebooky studentů a podobně)

Celkové hodnocení práce:
Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum 1. 6. 2022 Podpis oponenta diplomové práce