

# Posudek oponenta diplomové práce

Autor práce: **Bc. Martin Šebela**

Název práce: **Systém pro správu bezpečnostních incidentů v síti WEBnet**

## Obsah práce

Diplomová práce se zabývá problematikou kybernetické bezpečnosti a vytvoření systému, který bude usnadňovat řešení bezpečnostních incidentů a bude spolupracovat s dalšími systémy dané organizace.

V první části práce se diplomant zabývá důležitými tématy – strukturou bezpečnostních týmů, typy bezpečnostních incidentů, jejich řešením a dále konkrétními příklady bezpečnostních incidentů z univerzitního prostředí ZČU. Vše je podáno velmi srozumitelnou formou, domnívám se, že by daný text mohl dále sloužit jako vhodný výukový materiál pro lokální správce.

V druhé části práce je popsána tvorba systému navrženého diplomantem. V jednotlivých kapitolách je popsána implementace systému, struktura použité databáze a grafické rozhraní systému. Důraz je kladen i na zabezpečení celého systému (validace uživ. vstupu, CSRF a další). V rámci testování byla mj. otestována použitelnost systému, kdy uživatelé dosahovali lepších časů řešení incidentu oproti stávajícím řešením.

Diplomant se musel vypořádat s integrací vytvářeného řešení s již existujícími systémy na ZČU s různým přístupem (např. pro blokování problémových zařízení či konkrétních uživatelů). Oceňuji i možnost grafického odlišení významných informací v logových souborech pro snadnou identifikaci problémové aktivity. Systém je navržený tak, aby uživatele celým procesem řešení incidentu provedl a minimalizoval vynaložené úsilí.

## Kvalita řešení a dosažených výsledků

Diplomantovi se podařilo vyvinout a zprovoznit systém pro správu bezpečnostních incidentů v síti WEBnet. Výhodou systému je, že umožní blokování přístupu do různých částí sítě (VPN, eduroam, pevná síť) jednotným stylem i bez potřeby znalosti přihlašovacích údajů k četným dalším systémům. Vytvořený systém mi byl diplomatem předveden a je plně funkční. Systém je již nyní využitý v ostrém provozu při správě reálných bezpečnostních incidentů.

## Formální úroveň

Předložená diplomová práce má 96 stran včetně příloh. Struktura práce je logická. Práce obsahuje celou řadu diagramů a tabulek pro lepší pochopení dané problematiky. Drobnou výhradu bych měl jen k čitelnosti některých screenshotů z obrazové přílohy B v tištěné podobě.

## Práce s literaturou

Použitá literatura obsahuje celkem 25 záznamů relevantních k tématu diplomové práce. Vzhledem k povaze práce jsou použité zdroje převážně elektronické, uvedena je ale i knižní publikace.

### **Splnění zadání**

Zadání práce bylo splněno bez výhrad.

### **Doplňující informace k práci**

Nemám.

### **Dotazy k práci**

Je webové rozhraní systému využitelné i z mobilního zařízení?

Uvažuje se o nasazení systému i na dalších univerzitách?

Jakou mírou se IPv6 podílí na incidentech?

Navrhuji hodnocení známkou **výborně** a práci doporučuji k obhajobě.

V Plzni, 8. 6. 2021

Ing. Ladislav Pešička