Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Jméno studenta: Adam Hübner

Název práce: Testování zabezpečení počítačové sítě s využitím standardů pro bezpečnost

Autor posudku: Ing. Luboš Mercl

Cíl práce: Cílem práce je podrobně popsat normy, standardy a best parctice řešení pro zabezpečení počítačové sítě. Tyto metodiky porovnat a na jejich základě provést praktickou komparativní analýzy zavedení bezpečnosti a jejích praktického testování. V teoretické části autor představí zásadní normy, standardy a metodiky pro zavedení bezpečnostních opatření na úrovni zabezpečení dat a síťové komunikace. Autor provede komparativní analýzu relevantních řešení a matodik. V praktické části autor realizuje bezpečností opratření na ochranu dat a komunikace. Tato řeše otestuje na základě vybraých best practice řešení.

Povinná kritéria hodnocení práce	**Stupeň hodnocení** (známka)					
	A	**B**	**C**	**D**	**E**	**F**
Práce svým zaměřením odpovídá studovanému oboru	☐	☐	☒	☒	☐	☐
Vymezení cíle a jeho naplnění	☐	☐	☐	☒	☐	☐
Zpracování teoretických aspektů tématu	☐	☐	☒	☐	☐	☐
Zpracování praktických aspektů tématu	☐	☐	☐	☒	☐	☐
Adekvátnost použitých metod, způsob jejich použití	☐	☐	☒	☒	☐	☐
Hloubka a správnost provedené analýzy	☐	☐	☐	☒	☐	☐
Práce s literaturou	☐	☐	☒	☐	☐	☐
Logická stavba a členění práce	☐	☒	☒	☐	☐	☐
Jazyková a terminologická úroveň	☐	☒	☐	☐	☐	☐
Formální úprava a náležitosti práce	☐	☒	☒	☐	☐	☐
Vlastní přínos studenta	☐	☐	☒	☐	☐	☐
Využitelnost výsledků práce v teorii (v praxi)	☐	☐	☒	☐	☐	☐

Vyjádření k výsledku anti-plagiátorské kontroly

Celková podobnost 1% (pouze seznam použité literatury)

Dílčí připomínky a náměty:

Název práce „Testování zabezpečení počítačové sítě s využitím standardů pro bezpečnost“ je částečně zavádějící, protože autor práci nic netestuje – více celkové posouzení práce. Tato verze

diplomové práce je druhé odevzdání po neúspěšné obhajobě, nicméně významně se neliší od předchozí verze.

Celkové posouzení práce a zdůvodnění výsledné známky:

Student se ve své diplomové práci zabývá bezpečností v počítačových sítích, nicméně v teoretické části práce představuje převážně bezpečnostní normy a jak jsou definovány, jakou používají metodiku, princip a názvosloví, tedy spíše metodickou než fyzickou bezpečnost. V praktické části se pak student zaobírá obecnými přístupy a řešení pro bezpečnostní opatření a pokračuje tak spíše v metodickém popisu než reálnému řešení. Student zde pracuje s jednoznačně nedefinovaným prostředím, které se snaží zanalyzovat (alespoň na úrovni obecných rizik) a navrhnout metodické doporučení.
Co se týká realizování bezpečnostních opatření (kap. 4), tak student nejdříve definuje metodiku, kterou chce využít, následně ohodnotí v rámci vlastní metodiky jednotlivé hrozby bez zabezpečení (zranitelnost = 4), navrhne částečná opatření pro jednotlivé hrozby a pak hrozby ocení (zranitelnost = 1 nebo 2). Jednotlivé studentova ohodnocení (dopad, hrozba, riziko) mohou být diskutabilní, protože se jedná spíše o subjektivní zhodnocení.
Pro přehlednost by bylo dobré přidat tabulku, která by shrnula změny v ohodnoceních před opatřením a po opatřeních, čímž by se zvýšila čitelnost práce.

Každopádně teoretická část obsahuje dobře strukturovaný přehled jednotlivých norem a směrnic, ovšem co se týká komparativní analýzy jednotlivých norem, tak ta zde příliš není a jedná se (kap. 2 – Komparativní analýza) pouze o jakýsi souhrn všech možných doporučení. Doporučuji využít komparativní tabulku, čímž by se daná kapitola zpřehlednila (tato tabulka nejspíše existuje (příloha 2) nicméně nikde na ní není odkazováno v textu a dále by se student měl zaměřit hlavně na rozdíly mezi normami.

Další méně podstatné nedostatky:
- Kapitola 2, dále podkapitola 2.1 a následně 2.1.1 – bez dalších podkapitol s vyšším číslem (např. 2.1.2).

Otázky k obhajobě:

Kapitola 2 „Komparativní analýza“ obsahuje na první pohled spíše popis doporučení, které nejspíše vycházejí z jednotlivých norem. Prosím zdůvodněte, co v této kapitole je a jak jste jednotlivé bezpečnostní standardy a normy porovnával.

Výsledkem Vaší práce by dále mohl být i fakt, že toto prostředí by před Vašimi opatřeními certifikaci ISO 27001 nezískalo a po Vašich opatřeních získalo bez problémů (tedy prošlo auditem)?

V práci používáte testování hrozeb spíše jako subjektivní ohodnocení rizik, jaké jsou možnosti (pokud existují) pro objektivní zhodnocení jednotlivých hrozeb? Případně jak byste jednotlivá zabezpečení aktiv testoval?

Práci doporučuji k obhajobě.

Navržená výsledná známka: D

V Hradci Králové**, dne 2. ledna 2019**

podpis