HODNOCENÍ OPONENTA BAKALÁŘSKÉ PRÁCE

Autor práce	**Šimon Kovalčík**
Studijní program	**Ochrana obyvatelstva**
Forma studia	**prezenční**
Akademický rok	**2023/2024**
Téma práce	**Identifikace a posouzení rizik informačního systému vybrané organizace**
Autor posudku	**Ing. Petr Svoboda, Ph.D.**

	Kritéria hodnocení	**Váha**	**Hodnocení**
1	Formulace cílů práce a použité metody	0,10	C
2	Úroveň teoretické části práce	0,30	E
3	Úroveň analyticko-empirické a návrhové části práce	0,20	E
4	Výstavba textu a jeho logická provázanost, kvalitativní a kvantitativní parametry práce	0,13	D
5	Splnění cílů práce a relevance závěrů	0,15	E
6	Jazyková úroveň práce	0,05	C
7	Formální náležitosti práce (včetně citací a užití šablony)	0,07	C
	Návrh hodnocení dle váženého průměru	1,00	**E (2,72)**

Student předložil bakalářskou práci zaměřenou v souladu s názvem na identifikaci a posouzení rizik informačního systému vybrané organizace. Cíle práce jsou vymezeny v části Úvod a nejsou děleny na hlavní a dílčí. Autor je naplnil za dodržení zásad zpracování a doporučené literatury a s využitím vyjmenovaných vědeckých metod. Některé metody v práci použité však byly autorem opomenuty, a to například syntéza, deskripce; rovněž by bylo vhodné doplnit, kde byly uvedené metody v práci využity.
Teoretická část práce je velmi přehledového charakteru a její obsah je v mnoha ohledech výrazně zjednodušen. Kapitoly nejsou zpracovány komplexně (viz např. kapitola 3.1, kde jsou vyjmenovány pouze některé na základě mně neznámého klíče vybrané typy kybernetických útoků). Zmíněná kapitola 3.1 dále obsahuje nešťastné dělení, kdy autor uvádí pojem malware na stejné úrovni jako adware (druhý zmíněný je přitom podmnožinou prvního). Ve stejném dělení pak figurují i viry, červi a trojské koně, tedy pojmy ze samostatné kategorie (dělení dle způsobu šíření). Stejný trend lze nalézt v kapitole 4., kde jsou opět vyjmenovány jen některé a velmi obecné způsoby zabezpečení. Přitom chybí některé zásadní, například nutnost aktualizací programového vybavení. Definice v kapitolách uvedené často odkazují na internetové zdroje, zde bylo vhodnější využít například Výkladového slovníku kybernetické bezpečnosti.
Praktická část je zaměřena na vlastní analýzu rizik organizace za pomoci What-if analýzy. Oponentovi není zřejmé, na základě jakého klíče byly zvoleny právě uvedené scénáře hrozeb. Rozpracováno jich je pouhých 8, rozhodně to tedy není kompletní výčet všech hrozeb pro

organizaci. U první zmíněné (phishing) rovněž vnímám oproti šíření virů v systému jako daleko pravděpodobnější (a nediskutovaný) dopad odcizení přihlašovacích údajů. Rovněž chybí v analýze logické provázání s teoretickou částí, kde bych, vzhledem k jejich zmínce, očekával, že budou uvedené hrozby jako adware, spyware a další. Na základě uvedeného rozhovoru a omezeného počtu a detailnosti otázek nemohu posoudit, zda bylo možno studentem kvalifikovaně koncipovat SWOT analýzu. Jako silnou stránku autor uvádí „důraz na zálohování“, přitom v opatřeních můžeme identifikovat doporučení metody 3-2-1. V souvislosti s tím chybí hlubší diskuze nad běžnou funkcionalitou moderních ransomwarů, které dokáží šifrovat i zálohy.
Celkově vnímám práci jako velice obecnou. Zvolené téma je aktuální a jeho zpracování může být přínosné pro řešený subjekt, v tomto případě však nejsem o přínosech kvalifikační práce přesvědčen.

Otázky k obhajobě:

1. V textu uvádíte, že Česká republika přijme v říjnu 2024 nový zákon o kybernetické bezpečnosti. V jakém stavu je aktuálně jeho schvalování?
2. Jak se propsala výsledná strategie identifikovaná na základě SWOT analýzy do navržených opatření?
3. Budou výsledky práce využity v praxi? Byly výstupy analýzy předloženy konzultantovi a pokud ano, jak jím byly oceněny?

V Uherském Hradišti dne 20.05.2024 **Podpis:**

Hodnocení odpovídá následující stupnici:
A = 1,00-1,24 B = 1,25-1,50 C = 1,51-2,00 D = 2,01-2,50 E = 2,51-3,00 F = 3,01-…