HODNOCENÍ OPONENTA DIPLOMOVÉ PRÁCE

Autor práce	**Bc. Nikola Rebhanová**
Studijní program	**Bezpečnost společnosti**
Specializace	**Ochrana obyvatelstva**
Forma studia	**prezenční**
Akademický rok	**2023/2024**
Téma práce	**Kybernetické hrozby a jejich dopady na společnost v době světových krizí**
Autor posudku	**Ing. Petr Svoboda, Ph.D.**

	Kritéria hodnocení	**Váha**	**Hodnocení**
1	Formulace cílů práce a použité metody	0,07	B
2	Úroveň teoretické části práce	0,15	B
3	Úroveň analyticko-empirické části práce	0,25	B
4	Úroveň aplikační části práce	0,10	B
5	Výstavba textu a jeho logická provázanost, kvalitativní a kvantitativní parametry práce	0,08	A
6	Splnění cílů práce a relevance závěrů	0,15	B
7	Odborný přínos práce a její praktické využití	0,10	B
8	Jazyková úroveň práce	0,05	C
9	Formální náležitosti práce (včetně citací a užití šablony)	0,05	A
	Návrh hodnocení dle váženého průměru	1,00	**B (1,46)**

Předložená diplomová práce se zabývá kybernetickými hrozbami a jejich dopady na společnost v době světových krizí. Cíle jsou strukturovány specificky, nejsou děleny na cíl hlavní a dílčí cíle – hlavní je uveden v kapitole Úvod, v kapitole Cíle práce a použité metody jsou pak dva „cíle práce“. Cíle práce autorka v průběhu zpracování úspěšně naplnila za dodržení zásad pro zpracování a na základě doporučené literatury s využitím vyjmenovaných vědeckých metod. Vyjmenované metody jsou však zřejmě nekompletní, oponentem bylo v práci identifikováno využití dalších, např. deskripce, dedukce, indukce, syntéza a komparace.
Dělení malwaru uvedené v kapitolách 2.1 není šťastné, staví vedle sebe pojmy jako adware a virus, kdy první hovoří o projevech malwaru a druhý o způsobu jeho šíření. Ve výčtu typů phishingových útoků, kde jsou opět smíchány nesourodé pojmy jako whaling (definuje, na koho je útočeno) a vishing (definuje, užitou technologii) chybí moderní quishing.
Dílčí závěr (shodně jako celkový Závěr) je koncipován jako Abstrakt, autorka v něm popisuje obsah dosavadních kapitol práce. Pátá kapitola práce obsahuje přehled zásadních kybernetických útoků v České republice v době jednotlivých krizí. Na ni navazuje kapitola, kde autorka přehledně sumarizovala důsledky jednotlivých hrozeb v kontextu jednotlivých krizí. Pro větší přehlednost bylo vhodné opakovat řádky záhlaví jednotlivých tabulek. Scénář na Obrázku 8 bylo vhodné doplnit o variantu, kdy bylo výkupné zaplaceno, ale útočník data

neobnovil. Rovněž bylo vhodné vymezit, že se tento nezabývá double extortion ransomwarem. Celkově práci hodnotím jako zdařilou a doporučuji ji k obhajobě.

Otázky k obhajobě:

1. O čem hovoří pojem double extortion v souvislosti s ransomwarem? Jaká opatření (kroky) byste doporučila v případě úspěšného útoku tohoto typu?
2. Jak se vyvíjí legislativní proces ve smyslu přijetí nového Zákona o kybernetické bezpečnosti (v kontextu str. 25: „…ČR musí implementovat tuto směrnici formou novelizace zákona o kybernetické bezpečnosti, do 18. října 2024.)?

V Uherském Hradišti dne 09.05.2024 **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-…