

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: Bc. Ján Štofán

Oponent: doc. Ing. Petr Hruža, Ph.D.

Studijní program: **Inženýrská informatika**

Studijní obor: **Bezpečnostní technologie, systémy a management**

Akademický rok: **2019/2020**

Téma diplomové práce: **Dopady kybernetických hrozeb na vybranou organizaci**

Hodnocení práce:

Cílem diplomové práce Bc. Jána ŠTOFANA na téma „*Dopady kybernetických hrozeb na vybranou organizaci*“ bylo analyzovat organizace, jejich účel, cílovou funkci, strukturu a aktiva. Vytvořit jejich vhodnou typologii, použitelnou k řešení dopadů kybernetických hrozeb. Pojednat o kybernetické bezpečnosti v podmínkách organizace. Zaměřit se na hrozby, scénář průběhu bezpečnostní situace a jejich dopady na aktiva a organizaci. Analyzovat možné způsoby oceňování hmotných a nehmotných aktiv. Zaměřit se na oceňování výpadků, způsobených kybernetickými hrozbami.. Hlavním cílem bylo vytvořit model dvou hypotetických organizací, na nichž měl hodnotit dopady kybernetických hrozeb. Na základě analýzy rizik následně stanovit pořadí nebezpečnosti kybernetických hrozeb. Pro tři nejhorší hrozby měl zpracovat scénář vývoje bezpečnostní situace a dopadů na hypotetické organizace. S pomocí vhodného postupu pak ocenit výši dopadů jednotlivých narušení bezpečnosti, způsobených třemi nejhoršími kybernetickými hrozbami. Ocenění měl provést po jednotlivých fázích vývoje.

Autor diplomové práce v teoretické části v první kapitole popsal organizace, jejich účel, cílovou funkci, strukturu a aktiva. Ve druhé kapitole se zabýval obecně kybernetickou bezpečností. Ve třetí kapitole popsal základní pojmy a přístupy v oblasti oceňování hmotných a nehmotných aktiv.

Teoretické poznatky autor využil v praktické části práce. Ve čtvrté kapitole popsal kybernetickou bezpečnost ve vybraných organizacích. První z nich si vybral zdravotnické zařízení (okresní nemocnice s poliklinikou) a druhým je soukromá strojírenská firma. U každé organizace provedl identifikaci aktiv, hrozeb a analýzu rizik. Výpočet míry rizika a přehled útoků autor uvedl do tabulek. V páté kapitole provedl ocenění dopadů kybernetických hrozeb na obě organizace v jednotlivých fázích na tři nejhorší kybernetické hrozby u každé organizace. Všechny výpočty jsou logické a stručně objasněny.

Základní struktura diplomové práce je logická a jednotlivé kapitoly práce na sebe navazují. V závěru práce autor sumarizuje zjištěné poznatky. Seznam literatury zahrnuje adekvátní množství relevantních zdrojů. Seznam použitých symbolů a zkratk je úplný. Autor splnil zadaný cíl a práci je možné charakterizovat jako původní. Postup řešení, který si autor zvolil, byl správný a logický.

Při obhajobě prosím o zodpovězení následujících otázek:

1. **Jaká opatření je potřeba přijmout, aby se minimalizovalo zašifrování dat na pevných discích serverů a počítačů?**
2. **Který software je pro strojírenskou firmu nejdůležitější a proč?**
3. **Není přístup do internetu z vnitřní sítě z počítačů v ordinacích lékařů a sester velkou hrozbou?**

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
B - velmi dobře.**

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

Datum 30. 8. 2020

Podpis oponenta diplomové práce