Univerzita Hradec Králové
Fakulta informatiky a managementu

POSUDEK OPONENTA DIZERTAČNÍ PRÁCE

Název práce: Návrh metodiky zaznamenávání činnosti na prvcích kritické informační infrastruktury v prostředí energetických systémů

Autor: Ing. Tomáš Svoboda

Studijní obor: Informační, komunikační a řídicí technologie

Školitel: prof. Ing. Simeon Karamazov, Dr.

Školitel specialista: Mgr. Josef Jan Horálek, Ph.D.

Oponent: doc. Ing. Vladimír Soběslav, Ph.D.

Celkové posouzení práce:

Tato práce zaměřuje na problematiku kybernetické bezpečnosti v energetických systémech. Jedná se o etablované téma, přičemž existuje dostatečné množství zdrojů a zároveň se oblastí kybernetické bezpečnosti v oblasti průmyslových systémů zabývají různé vědecké týmy. Téma je velmi aktuální i díky neustále rostoucímu počtu kybernetických útoků, které můžeme vysledovat nejen v indexech kybernetické bezpečnosti zveřejněných specializovanými agenturami, ale také i množství úspěšných pokusů, připomeňme si například kauzu nemocnic. Úspěšný hackerský zásah do energetických systémů a distribuční soustavy by ale neměl jen omezený lokální dopad na jednu nemocnici.

Z výše uvedených důvodů považuji téma za dizertabilní a velmi aktuální, které skrývá velký potenciál pro teoretické metody, ale i praktické ověření daných poznatků. Název disertační práce *„Návrh metodiky zaznamenávání činnosti na prvcích kritické informační infrastruktury v prostředí energetických systémů"* nevystihuje, dle mého názoru, komplexnost a obsah disertační práce neb zaznamenávání činností je pouze jednou z částí opatření pro řešení kybernetické bezpečnosti, jak je patrné z předložené práce.

Hlavním cílem disertační práce je *„Vytvoření nové metodiky SEC-MON, která vytváří průnik mezi rámci pro návrh a implementaci rozsáhlých architektonických řešení v rámci enterprise architektury a specifickou oblastí problematiky bezpečnostních monitorovacích systémů sloužících pro zaznamenávání činnosti na prvcích kritické informační infrastruktury v prostředí energetických systémů"*. Cíle disertační práce spatřuji jako adekvátní. Autor vhodně specifikoval dílčí cíle a celkovou metodiku práce pro jejich dosažení od úvodních fází přes dekompozici problémů, analýzy současné situace a možných přístupů až po návrh výsledné metodiky a její ověření. Jak již bylo řečeno, tato oblast je velmi široká a je nutné pečlivě abstrahovat a zahrnout oblasti, které se práce dotýkají. Jedná se dále o téma, které kombinuje různé vědecké přístupy. Tomu také odpovídá relativně velký rozsah disertační práce.

Obsah dizertační práce je rozdělen do několika částí. První část zaměřující se popis energetických řídicích systémů a související oblast bezpečnosti. V této části autor vhodně analyzoval současný stav z technologického, ale i bezpečnostního pohledu. Místy jsou však grafy, vzhledem k dynamičnosti této oblasti, tři až čtyři roky staré a bylo je možné aktualizovat. Následující část tvoří kapitoly čtyři a pět, zde se autor uvedl klíčové pohledy na správu IT infrastruktury a standardy, které jsou v této oblasti využívány. Závěrem pak představil rámcové koncepty podnikové architektury neboli enterprise architecture frameworks. Jedná se fakticky o rozbor existujících řešení, který opět částečně nekoresponduje s názvem kapitoly.

Z hlediska autorského přínosu jsou klíčové poslední tři kapitoly, které ústí v samotný návrh metodiky SEC-MON. V první části autor přehledně provedl komparativní analýzu rámců enterprise architektury, definoval jednotlivé pohledy a hlediska a následně zvolil rámec TOGAF. S touto volbou se, v daných podmínkách ztotožňuji, jedná se o uznávaný iterativní rámec, který je optimální právě pro návrhy rozsáhlých IT architektur. Návrh metodiky SEC-MON pak vychází z jednotlivých fází rámce TOGAF, který byl uzpůsoben na problematiku energetických systémů a je vhodně navázán na předchozí analýzu současného stavu. Opět je zde vidět iterativita a agilita metodiky díky zvolenému rámci. Ověření jakékoliv navržené metodiky je zpravidla jejím omezujícím faktorem. Vítám rozdělení na přímé a nepřímé ověření, co se týče ověření přímých ověření a srovnání s jinými metodami, je logicky vcelku omezené. Pokud v případě komplexních architektur, či obecně stochastických systémech, využiji jednu metodiku, pravděpodobně se nepodaří nasimulovat stejný průběh a zpracovat řešení jinou metodikou, které by pak bylo srovnatelné. V takovýchto případech narůstá vliv hodnocení nepřímého nebo statistické zhodnocení a jeho interpretace.

Celkově se jedná o zajímavou disertační práci prokazující erudici autora v dané oblasti. Dosažené výsledky považuji za inovativní a slibné pro budoucí práci či vědecké projekty.

Autor prezentoval celkově 13 publikací a 3 projekty, kterých se jako doktorand účastnil. 8 publikací souvisí s tematikou dizertační práce. Výstupy reprezentují zejména konferenční články IEEE či Scopus SJR, které jsou uvedeny ve známých vědeckých databázích a jsou doprovázeny nezávislými oponentními řízeními ve vědecké komunitě.

Výsledky považuji za adekvátní a doporučuji, aby tato práce byla přijata k obhajobě pro udělení doktorského titulu Ph.D.

Otázky pro diskuzi:

1) Popište aktuální trendy a hrozby v oblasti energetických systémů.
2) Jaké mohou být dopady úspěšného útoky na distribuční soustavu ČR.

V Hradci Králové 14. 9. 2020

[redacted]

.....

doc. Ing. Vladimír Soběslav, Ph.D.