POSUDEK OPONENTA DOKTORSKÉ DISERTAČNÍ PRÁCE

Doktorand: Ing. Libor Sarga

Oponent: Prof. Ing. Said Krayem, CSc.

Název práce: Organizational Security Processes and Crisis Management in the Knowledge Society

Hodnocení práce:

Uvedeným cílem této disertační práce je sestavení modelu řízení informační a komunikační bezpečnosti podniku.

V první kapitole disertační práce je vymezena terminologie používaná v oblasti informační bezpečnosti.

Druhá kapitola je věnována základním principům informační bezpečnosti, sledujícím tři základní atributy: důvěrnost, integritu a dostupnost dat a funkcí ICT systémů organizace.

Ve třetí kapitole je popsán fenomén BYOD (Bring Your Own Device), kterým se firmy vyrovnávají s potřebou umožnit svým zaměstnancům, partnerům a často též dodavatelům a zákazníkům přístup do své ICT infrastruktury pomocí notebooků, tabletů a mobilních telefonů, jejichž nastavení a zabezpečení není plně v pravomoci organizace.

Ve čtvrté kapitole jsou popsány některé typy útoků, kterými je útočník schopen prolomit systém řízení přístupu k citlivým datům a funkcím ICT infrastruktury a získat k nim neoprávněný přístup. Kapitola číslo čtyři se dále zabývá dotazníky pro vybrané oblasti rizikové analýzy a zpracováním výsledků provedené analýzy s jejich použitím.

V páté kapitole jsou uvedeny dvě případové studie popisující jednak hrozbu prolomení hesel metodou reverse engineering, jednak testování možnosti průniku do interní ICT infrastruktury z internetu.

Šestá kapitola obsahuje popis modelu ICT bezpečnosti a ekonomických ukazatelů pro vyhodnocení ekonomických přínosů implementace opatření ICT bezpečnosti.

V sedmé kapitole jsou shrnuty výsledky disertační práce. Kapitola kromě vlastního rozboru výsledků práce obsahuje řadu velmi cenných poznatků převzatých (a citovaných) z odborné literatury a využitých pro hlubší vyhodnocení vlastních výsledků práce. Příkladem je velmi aktuální riziko rozlomení hesel (a klíčů) a obrana použitím nástrojů "password manager".

Osmá, devátá a desátá kapitola popisují možnosti využití výsledků disertační práce v budoucím navazujícím výzkumu v praxi a ve výuce.

Předložená práce **zahrnuje podstatně širší oblast ICT bezpečnosti, než by naznačoval její název**. Kromě oblasti podnikové bezpečnosti obsahuje rozsáhlé a odborně fundované části textu věnující se

poměrně detailním technickým aspektům různých typů bezpečnostních rizik a útoků zaměřených přímo na slabé články hardwarových a softwarových bloků ICT infrastruktury. Tato **šířka záběru prokazuje rozsáhlé znalosti autora v těchto ryze technických oblastech ICT bezpečnosti**. Ne příliš šťastným důsledkem je pak značný rozsah textu, jehož důkladné přečtení a posouzení vyžaduje mnoho času.

K předložené práci mám pouze jeden podstatnější komentář a několik drobných dotazů:

1) V navrženém modelu ICT bezpečnosti je zmíněn proces „Incident Managementu", ale v mém porozumění textu je omezen jednak v souvislosti s Business Continuity (str. 200, poslední odst.), jednak v 6.2.3 - Incident Response, ICT Infrastructure Hardening.

Vlastní struktura kapitoly 6, viz níže, též podporuje dojem, že **incident management je v práci vnímán jako proces redukovaný pouze na incidenty vzniklé na straně ICT infrastruktury a není chápán jako klíčový proces ICT security modelu zahrnující všechny typy incidentů a zajišťující poučení ze vzniklých incidentů a zpětnou vazbu zaručující opravu bezpečnostní politiky a dalších bezpečnostních procesů a ověření, že riziko opakování incidentu je redukováno na přijatelnou míru.**

6 THE ICT SECURITY GOVERNANCE MODEL
- *6.1 User-Side Security*
- *6.2 ICT-Side Security*
  - *6.2.1 BYOD Management*
  - *6.2.2 Internal Network Segmentation*
  - *6.2.3 Incident Response, ICT Infrastructure Hardening*
  - *6.2.4 Password Composition Requirements*
- *6.3 Model Metrics*
- *6.4 Conclusion*

Při pohledu na incident management v tomto širším kontextu může významně pomoci ke zvýšení celkové úrovně ICT bezpečnosti v jednom velmi závažném riziku – riziku chyby či neznalosti ICT administrátorů. Kapři si neradi vypouštějí vlastní rybník a proto velmi důležitou položkou incident managementu je pravidelný externí security audit.

2) Str. 42: "No suitable policies have usually been set for this class of devices as a result of low flexibility and reactive approach to new trends, creating a window of opportunity with no countermeasures put in place. "
Dotaz: Pokud jsou třídou zařízení míněny servery a pracovní stanice, nepřipadá mi formulace šťastná. Bezpečnostní politika pro tato zařízení je podle mne jedna z nejdůležitějších.

3) Str. 66, 2. odst: "SQL has become widely deployed as a back-end solution for web applications, accompanied by additional software tools. " Nepříliš šťastná formulace. SQL plní roli databáze pro rychlé uložení a výběr dat aplikace včetně dat pro webovou prezentaci. Back-end solution bývá používáno dost odlišným způsobem.

4) Str. 247 – není výtka, jen poznámka: opakující se argument rychlého zastarávání poznatků v IT security a množství nových typů útoků a obecně bezpečnostních incidentů. Velmi častý v odborné literatuře a v jistém smyslu pravdivý. Avšak při hlubším rozboru nových typů útoků lze poznat, že převážně využívají již známé slabiny ICT technologií a opakující se chyby v chování uživatelů. Mohou být úspěšné hlavně proto, že současná protiopatření nebyla dostatečná nebo/a důsledná a

parametry ICT systémů se rapidně zvyšují a umožňují vývoj výkonnějších hackerských nástrojů. Přílišná koncentrace na fenomén rychlých změn může mít za následek nižší efektivnost a účinnost řízení ICT bezpečnosti a přehlédnutí důležitosti posílení již známých forem obrany.

Závěr:

Hlavní výsledky disertační práce byly publikovány v jedenácti samostatných publikacích ve významných mezinárodních časopisech.
Práce svou náplní a kvalitou splňuje požadavky kladené na doktorskou disertační práci.
Doporučuji proto práci k obhajobě a věřím, že po její úspěšné obhajobě bude autorovi udělena vědecká hodnost doktor.

Prof. Dr. Eng. Said Krayem, CSc.
University of Aleppo - Syria