Posudek oponenta diplomové práce

Autor práce: **Milan Široký**

Název práce: **Příprava bezpečnostní dokumentace vyhovující zákonu o kybernetické bezpečnosti**

Obsah práce

Cílem práce je příprava bezpečnostní dokumentace pro systém HelpDesk firmy CCA tak, aby byly splněny požadavky zákona 181/2014 Sb. o kybernetické bezpečnosti.

Kvalita řešení a dosažených výsledků

V rámci práce vznikl dokument, který stručně přibližuje zákon o kybernetické bezpečnosti z roku 2014, dále jsou popsány systémy HelpDesk a ISZA, na kterých se budou bezpečnostní opatření demonstrovat. Následuje návrh bezpečnostní dokumentace, kde jsou přehledně popsané hlavní problémy z oblasti bezpečnosti v souvislosti s firmou CCA. Tato část poskytuje celkem hezký přehled z oblasti IT bezpečnosti.

Jádrem práce považuji analýzu a ohodnocení rizik spolu s návrhy řešení. Zde autor v součinnosti se zadavatelem práce popisuje jednotlivá rizika a navrhuje jednoduché vzorce pro výpočet celkového rizika, tj. míry dopadu pro firmu CCA. Autor vytvořil několik tabulek, kde uvádí hodnoty jednotlivých hrozeb. Tato práce je zajímavá, nicméně přiřazení hodnot jednotlivým rizikům, váhám (zřejmě „expertní" odhad autora, někde ve spolupráci se zadavatelem) i celkové vzorce se mi zdají „silně na vodě". Není zde uveden žádný výpočet ani zdůvodnění jednotlivých hodnot. Rozsah parametrů si také volil sám autor – někde popsáno stupnicí 1-3 (hrozby), jinde 1-4 (aktiva), dále 1-16 (závažnost rizik), atp. Název některých parametrů se mi zdá také jako silně zavádějící, např. „Pravděpodobnost hrozby" v intervalu <1;3>. Jak může být hodnota pravděpodobnosti větší než 1?

Dále se autor snaží navrhnout postupy tak, aby se eliminoval/minimalizoval dopad při vzniku incidentů.

Formální úroveň

Práce je vytvořena v systému LaTeX a je z formálního hlediska celkem v pořádku. Na přiloženém CD bych uvítal readme soubor s popisem jeho obsahu, jinak nemám výhrady.

Práce s literaturou

Práce obsahuje celkem 24 publikací, což je zcela postačující.

Splnění zadání

Zadání bylo splněno s připomínkami (viz výše).

Připomínky a dotazy k práci

1. V práci zmiňujete hešovací funkci MD5 – vysvětlete, zda je tato funkce dnes bezpečná?
2. V případě krádeže zařízení / dat neuvádíte jako problém možnost zneužití těchto dat. Vysvětlete prosím.
3. Jako možné riziko jsem nikde nenašel manipulace s daty v systému v rámci nepovoleného přístupu. Myslíte si, že se to nemůže stát? Proč jste se tímto nezabýval?

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky

4. V tabulce `DP_Siroky_Vyhodnocena_Rizika.xlsx` na CD na záložce Rizika Vám vyšlo, že výpadek komunikační linky je více závažný, než porucha serveru nebo krádež zařízení. To se mně zdá celkem zavádějící. Vysvětlete prosím.

Vzhledem k uvedeným připomínkám navrhuji hodnocení známkou **velmi dobře** a práci doporučuji k obhajobě.

V Plzni 7.6.2017

doc. Ing. Pavel Král, Ph.D.

SOUHLASÍ
S ORIGINÁLEM

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky
①