Příloha k protokolu o SZZ č.

Vysoká škola: JU Pedagogická fakulta

Katedra: informatiky

Datum odevzdání posudku: 26. 1. 2010

Diplomant: Miloš BUČINSKÝ

Aprobace: VTI

Vedoucí bakalářské práce:

Ing. Ladislav Beránek, CSc., MBA

POSUDEK BAKALÁŘSKÉ PRÁCE

Analýza rizik bezpečnosti IS STAG

(téma)

Předkládaná bakalářská práce se věnuje problematice analýze rizik bezpečnosti IS s aplikací na informační systém používaný na universitách STAG. Práce je rozdělena do 5 kapitol. Ve druhé kapitole se autor věnuje popisu co je to riziko, uvádí základní pojmy týkající se analýzy rizik, uvádí obecný postup analýzy rizik. Zde také autor popisuje standardy vztahující se k analýze rizik a standard ISO 27001 pro zavedení ISMS v organizaci. Třetí kapitola je věnována metodikám analýzy rizik jako jsou CRAMM, RA2 a další. Zde také navrhuje vlastní metodiku, která vychází z obecného přístupu k analýze rizik a poznatků jiných komerčních metodik. Vlastní analýze rizik, vlastní praktické práci je věnována kapitola čtyři. Kde je proveden podrobný popis, jak autor postupoval při provádění analýzy rizik systému STAG.

Celkově je práce formálně velmi dobře zpracována, včetně struktury. Obsahuje řadu ilustrativních obrázků a tabulek, které zpřehledňují čtení práce. Vyskytuje se zde několik překlepů, kterých ale není mnoho. Také literatura je zpracována podle normy, výhradu bych měl k literatuře pod číslem 12, kde je u odkazu na zdroj z firmy AEC uveden odkaz na Google. Ani odkaz pod číslem 11 nepůsobí graficky příliš dobře, v době pravopisných korektorů by se ale ani tyto chyby nemusely vyskytovat.

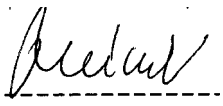
Analýza rizik se provádí standardně ve větších organizacích. Zde se většinou používají různé komerční metodiky, které jsou podporovány komerčním software, jako je CRAMM, RA2 a další. Analýza rizik není složitým problémem, její provádění ale klade požadavky na poměrně široké znalosti hodnotícího, včetně nutnosti jednání s lidmi (součástí je i provedení řady interview s cílem zjistit stav bezpečnosti IS z různých hledisek.

První teoretická kapitola (Riziko, analýza rizik) je zpracována velmi dobře. Uvádí obsáhlý přehled standardů a je doprovázena řadou tabulek a obrázků. Autor se soustředil na standard ISO 27001, který je také v praxi nejpoužívanější. COBIT je používán spíše v bankách a ITIL ve větších organizacích. V kapitole 3 (Metody analýzy rizik) je uveden přehled některých metod pro analýzu rizik. Je třeba poznamenat, že např. Octave není komerční metodou. Metodika je volně dostupná, dokumentace je však poměrně rozsáhlá. V kapitole 3.2 bych očekával podrobnější popis vlastní metody. Autor uvádí, že je možnost vytvořit si vlastní metodu, ale měl by uvést alespoň odkaz na kapitolu 4.2, kde je tato metoda použita apod. Praktická část práce je obsahem kapitoly 4 (Analýza rizik IS STAG). K této kapitole nemám připomínky. Autor si dal dost práce s provedením této analýzy rizik, a je to vidět i z této kapitoly. Pouze odstavec „Závěr a shrnutí zranitelností a výběry bezpečnostních protiopatření“ není dobře formulován, a tak určitým způsobem snižuje dojem z celé této kapitoly. Očekával bych zde shrnutí dosažených výsledků.

Přes tyto drobné nedostatky, které vyplývají z nedostatečné zkušenosti, hodnotím práci jako zdařilou. Pozitivně hodnotím fakt, že autor pracoval samostatně. Zvládl větší množství dokumentaci

a předvedl praktickou práci, jejíž výsledek bude použitelný i pro provozní IT oddělení university. Celkově hodnotím práci známkou **výborně**.

Návrh na klasifikaci bakalářské práce: výborně



Podpis vedoucího bakalářské práce

V Č. Budějovicích dne 26. 1. 2010

Stupeň klasifikace	výborně	velmi dobře	dobře	nevyhověl