

Posudek vedoucího bakalářské práce

1. Identifikační údaje

Název práce: **Bezpečný přenos dat ve firmě a ve státní správě**

Autor práce: **Věra DŽBÁNKOVÁ, DiS.**

2. Cíl práce a jeho naplnění

Cílem práce bylo zjistit, jak lze v současné době dostatečně bezpečným způsobem přenášet data v rámci firmy, mezi firmami a při komunikaci se státní správou. Zaměřit se na různé úrovně utajovaných skutečností. Možnosti napadení přenášených dat a vhodná obrana proti takovýmto útokům. Pořizovací a provozní náklady na zvolená řešení. Úkolem bylo také sestavit několik vhodných případových studií autorkou zvolených různých typů firem.

Autorka ve své práci naplnila stanovený cíl a až na několik drobnějších nedostatků dodržela zásady pro zpracování bakalářské práce.

3. Obsahové zpracování a přístup k řešení

Autorka si v anotaci stanovila jako cílovou skupinu této práce studenty, kteří mohou této práci využít jako návod pro zabezpečení své firmy. Návodem je však tato práce velice orientačním a téměř v žádném svém bodu nejde příliš do hloubky potřebné pro plné pochopení problematiky, nebo alespoň zabezpečující dostatečné zabezpečení firmy. Pomocí tohoto návodu tedy bohužel nelze dosáhnout autorkou slibované "správné a účelné zabezpečení firmy".

Například na straně 41 autorka navrhuje zabezpečit webový server SSL certifikátem, který však slouží pouze k zabezpečení komunikace mezi webovým serverem a návštěvníkem webových stránek. Tudíž SSL certifikát ve výsledku k zabezpečení samotného webového serveru vůbec nepřispívá.

Autorka, od konce května 2015 do prodlouženého termínu odevzdání, tj. poloviny srpna 2015, zpracovala bakalářskou práci naprosto samostatně a často i bez zapracování doporučení vedoucího práce (např. nevhodné využití Google Apps pro firemní e-mailové schránky). Možnosti konzultace a kontrolu práce do 1. července 2015 autorka využila pouze na žádost vedoucího práce.

Jednotlivé kapitoly bakalářské práce v podstatě pokrývají zadané téma. Autorka v podstatné části bakalářské práce sestavila orientační přehled základního zabezpečení dat proti ztrátě dat a proti odcizení dat. Od strany 37 se pak věnuje návrhu ochrany dvou autorkou navržených fiktivních firem. Toto rozdělení považuji za vhodné, ačkoliv by samotnému návrhu mohlo být věnováno více prostoru.

4. Formální náležitosti a úprava

Práce je zpracována pouze s drobnými typografickými nedostatky, avšak na některých místech došlo i k závažnějším nedostatkům. Například u kapitoly 4.4 došlo k nesprávnému číslování podkapitol v pořadí 1, 2, 3, 1, 1 a 2. Nebo také nedokončená věta na konci třetího odstavce na straně 42, kde chybí celkem zásadní informace, jaký externí server firma využívá, jak velký je tento úložný prostor atd.

5. Připomínky

- Poděkování je napsáno nevhodným způsobem, který může navodit myšlenku, že autorka práci nenapsala sama.
- V práci je citováno několika stran textu z jednoho zdroje (např. str. 12 až 14 z [1]).
- Některé navrhované postupy jsou diskutabilní a často i nedoporučované, jako například okamžitá instalace vydaných záplat pro OS a SW (kapitola 4.4.1 Patch management, str. 32, nebo v tabulce 5, str. 40).
- Na straně 41 autorka jako ochranu před XSS doporučuje použít pouze funkci htmlspecialchars() v PHP. Což lze považovat jako vhodný základ, ale nikoliv dostatečné zabezpečení, protože i tuto funkci lze relativně snadno překonat a obejít bez použití dalších kontrol uživatelských vstupů. Navržený blacklist je stále nedostatečnou ochranou.
- Na straně 42 autorka navrhuje, že firemní e-mailovou schránku budou mít pouze interní zaměstnanci a externí lektoři budou využívat svoji soukromou e-mailovou schránku. Vzhledem k tomu, že i externí lektor může komunikovat s účastníkem kurzu, tak tento návrh nelze z marketingového hlediska považovat za vhodný.
- "Administrátorská práva ke všem počítačům má pouze správce sítě" (str. 43). Není ovšem zřejmé, jak je ve firmě řešena zastupitelnost.
- Došlo k posunutí číslování stránek v tištěné a elektronické verzi bakalářské práce. Číslo stránek v tomto posudku jsou podle tištěné verze.
- U tabulky 6 (str. 44) autorka uvádí celkové provozní náklady na firemní e-mail při použití Google Apps 40 € za rok (bez darů). Tato částka je podle licenčních podmínek firmy Google však pouze za jednu schránku se jménem zaměstnance (např. jiri.novak@firma.cz, obecné e-mailové schránky jsou zdarma, např. info@firma.cz). Při 5 zaměstnancích se pak tedy jedná o částku 200 €, případně pro všechny zaměstnance by byly nutné náklady 800 € za rok.
- Stejný problém s výpočtem ceny za e-mailovou schránku (40 €/rok/uživatel) má i tabulka 7 na straně 45.
- Autorka vůbec nezdůvodňuje výběr řešení e-mailových schránek pomocí Google Apps, které sice nabízí mnoho dalších služeb, ale autorkou zůstávají nevyužity a ani nezmněny. Přičemž existují webhostingové firmy, které nabízí autorkou požadované řešení za cenu jedné uživatelské licence pro Google Apps, tj. přibližně 1000 Kč za rok (např. firmy WEDOS, FORPSI, Czechia,...).
- Autorka navrhuje v tabulce 6 (str. 44) využití programu TeamViewer pro vzdálenou správu počítačů ve firmě Kurzy. Také zde není proveden výběr z dostupných řešení, jako například Vzdálená plocha přímo vestavěná v OS Windows (tj. nulové pořizovací náklady navíc), nebo možnost, že si správce jednoduše obejde všechny počítače ve firmě, tj. 2 stolní počítače a 20 notebooků (všechny počítače jsou připojeny do LAN).

Práci **doporučuji k obhajobě** a hodnotím ji stupněm
dobře

Pardubice, 25. srpna 2015

Ing. Martin Novák