Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

OPONENTSKÝ POSUDEK BAKALÁŘSKÉ PRÁCE

Student: **Vašinka Daniel** **Oponent:** **Ing. David Malaník, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2017/2018**

Téma bakalářské práce: **Bezpečnost dat ve firemní síti**

Hodnocení práce:

		A	B	C	D	E	F
	Hodnocení: A – nejlepší; F - nevyhovující						
1.	Obtížnost zadaného úkolu	☐	☒	☐	☐	☐	☐
2.	Splnění všech bodů zadání	☐	☐	☐	☐	☐	☒
3.	Práce s literaturou a její citace	☐	☐	☒	☐	☐	☐
4.	Úroveň jazykového zpracování	☐	☐	☒	☐	☐	☐
5.	Formální zpracování – celkový dojem	☐	☐	☐	☒	☐	☐
6.	Logické členění práce	☐	☒	☐	☐	☐	☐
7.	Vhodnost zvolené metody řešení	☐	☐	☐	☐	☐	☒
8.	Kvalita zpracování praktické části	☐	☐	☐	☐	☐	☒
9.	Výsledky a jejich prezentace	☐	☐	☐	☐	☐	☒
10.	Závěry práce a jejich formulace	☐	☐	☐	☐	☐	☒
11.	Přínos práce a její využití	☐	☐	☐	☐	☐	☒

Celkové hodnocení práce:
Výsledná známka není průměrem výše uvedených hodnocení. Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:
A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně , F – nedostatečně.
Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou bakalářskou práci nedoporučuji k obhajobě a navrhuji hodnocení

F - nedostatečně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Otázky k obhajobě:
1. "Bezpečnost RSA je dneska velice diskutabilní, jiţ v roce 2017 bylo zveřejněn potřebný výkon k prolomení RSA šifer na čipových kartách s délkou klíče 1024 bitů a to pomocí výkonného výpočetního výkonu. " Myslíte tím zranitelnost ROCA? Jedná se skutečně o problém šifry RSA?
2. Lze používat kvalifikovaný elektronický podpis i bez čipové karty, či tokenu?
3. Je vhodné mít citlivá firemní data na cloudu? Jaký cloud byste vybral pro uložení záloh obsahující data z personálního oddělení firmy?
4. Co myslíte bezpečnostní prověrkou zaměstnanců? strana 27.
5. Bod 5.2.1 Pokud volíte WPA2-PSK tak jiná možnost než zadatheslo k sítí není, navíc Vámi navrhované řešení s formulářem a ručním přidáním MAC adresy do AP je naprosto nereálné. Jaká je kapacita MAC adres na AP? A jak byste ten formulář řešil? Nebylo by vhodnější řešení WPA2-EAP?

6. Bod 5.2.1 jak si představujete sledování aktivit na sítí? Jak budete sledovat https provoz?
7. Bod 5.2.2 odkud čerpáte, že je doporučená délka hesla 8 znaků? Už mnoho let to neplatí.
8. "Uchování hesla je jedním z pravidel, které doporučuje nikomu heslo nesdělovat, zaznamenávat v písemné formě (na papírek u monitoru, v bloku, atd.), " - takže je v pořádku heslo zaznamenávat v písemné formě?
9. "Avšak bezpečnostní odborníci doporučují měnit heslo jednou za 14 dní či jednou za měsíc. V praxi se potkáme s obměnou hesla jednou za půl roku. " můžete uvédst zdroj?
10. Bod zadání 3. myslíte, že je vhodné pro hodnocení současného stavu na poli nástrojů pro ochranu dat použít dotazníkový průzkum kterým oslovíte firmy? Já ten bod chápu jako zhodnocení současné nabídky nástrojů, nikoliv průzkum ve firmách co a jak používají.
11. Myslíte, že bod zadání č. 4 je v práci řešen (dle jeho znění v zadání)?
12. Jak se stavíte k odpovědi v přiloženém dotazníku na otázku, zda si mohou brát zaměstnanci práci domů. U jednoho dotazníku máte zaškrtnuté jak ANO tak i NE.

Další připomínky, vyjádření, náměty k obhajobě práce (možno pokračovat i na další stránce):
1. Kapitola 2.1.1 - na uvedeném zdroji se informace uvedené v BP nevyskytují.
2. kapitola 2.1.2 - na uvedeném zdroji se informace uvedené v BP nevyskytují.
3. s. 13 "Je obdobou Phishingu s rozdílem toho, ţe útočník v Domain Name System (DNS) tabulce uţivatele změní adresu webové stránky např. elektronického bankovnictví " - to není pravda a ani ve vámi uvedeném zdroji taková informace není.
4. s. 14 kapitola "Sociální inženýrství" - toto ve Vámi uvedeném zdroji vůbec není.
5. s 17. "Jsou to šifry, které pro zašifrování a odšifrování vyuţívají totožné klíče. Už z principu vypovídá o výhodě těchto šifer a tím je velmi nízká náročnost na výpočetní výkon, tato výhoda vyplývá z jednoduchosti šifrovacích a dešifrovacích algoritmů daných šifer. " jak můžeme na základě toho, že je stejný klíč použit pro šifrování a dešifrování usuzovat o výpočetní složitosti šifry?
6. kapitola 3.2.4.2 uvádíte nepravdivé informace "Zaručený elektronický podpis = Jedná se o elektronický podpis, který nezaručuje identitu podepsané osoby, a tudíž se za podepisovanou osobu může vydávat kdokoliv jiný nebo dokonce někdo, kdo vůbec neexistuje. " Dle zákona 227/2000sb. musí zaručený elektronický podpis splňovat: je jednoznačně spojen s podepisující osobou, umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě, byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou.
7. Co je Magnetický pevný disk a co elektronický pevný disk? (strana 24), jedná se paskvil. Je to nedokonale přepsaný zdroj ve kterém jsou Magnetická médi a Elektronická média. Student v práci popisuje neexistující terminologii a odvolává se na zdroj ve kterém nic takového není.
8. "Pro příchody a odchody z firmy by měl fungovat například nějaký elektronický docházkový systém, který by zabránil pohybu neoprávněných osob, které by chtěli například odcizit nebo poškodit firemní data." - velmi vágní formulace v podstatě nic neříkající.

Hodnocení F volín v důsledku:
Dle mého názoru práce nespňuje body zadání 3 a 4. Dotazníkový průzkum odpovídá stavu ve firmách a v žádném případě nereflektuje současnou nabídku nástrojů pro ochranu dat, která by byla vhodná pro malé a střední firmy. Pokud by byl bod zadání zhodnoťte současný stav nasazení nástrojů pro ochranu dat v malých a střeních firmách, bylo by řešení v pořádku.
Bod 4. opět řeší něco jiného než je v zadání práce: je to modelový příklad z pohledu firmy a opírající se o data z bodu 3. Samotný návrh v kapitole 7.3 vychází "ze vzduchu", jedná se o nepodložené doporučení několika nástrojů pro firmy - bohužel je navíc toto doporučení jen velmi obecné a jeho přínos je v podstatě nulový. Řešit vhodnost nasazení šiforvacího nástroje Veracrypt pouze na základě toho, že je zdarma "Je nástroj pro šifrování dat, který navazuje na historicky

oblíbený a dnes již nepoužívaný TrueCrypt. Velkou výhodou VeraCryptu je cena licence, která je naprosto zdarma. Licence je volně šiřitelná a proto je firmy Veracrypt optimálním řešením. V principu pracuje s datovými kontejnery, které zašifruje, tyto kontejnery se poté tváří jako běžný soubor a je možno je přesouvat, kopírovat, atd. " nepovažuji za vhodné. Doporučené nástroje pro zálohování jsou jen obecně popsané, nejsou řešeny žádné doporučení pro strategie zálohování. Čtenář se pouze dozví obecné informace o jaké programy se jedná a v konečném důsledku je asi "velmi překvapen" zjištěním, že slouží k zálohování.
Programy pro ukládání hesel jsou opět pouze obecně popsány a opět doporučeny "ze vzduchu". Není tu žádný relevantní důvod proč z portfolia možná desítek řešení vybrat zrovna tyto.
Jazykové zpracování odpovídá spíše velmi narychlo poskládané práci z různých zdrojů, v mnoha případech navíc chybně interpretovaných - student se pouští do závěrů, které jsou v rozporu s uvednými zdroji, než pečlivě připravené bakalářské práci.

Datum 1.6.2018 Podpis oponenta bakalářské práce