Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: **Bc. Černý, Libor** **Oponent:** **ing. Josef Kaderka, Ph.D.**

Studijní program: **Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**
Akademický rok: **2013/2014**

Téma diplomové práce: **Zajištění bezpečnosti datového centra**

Hodnocení práce:

Na základě podrobného prostudování diplomové práce Bc. Libora Černého (dále diplomanta) konstatuji: Předloženou diplomovou považuji za úplnou, velmi detailně řešící aktuální problematiku všestranného zabezpečení datového centra. Práce má celkový rozsah 150 stran včetně seznamů použité literatury, obrázků, zkratek apod., což je dle mne daleko více, než se od diplomové práce obvykle očekává. Nejsem si ale jist, zda je takovýto rozsah vůbec rozumný; na některých školách by byl nepřípustný.

Určitý problém vidím již ve formulaci zadání, kde je uváděno, že se má jednat o „bezpečnost datového centra“. Je zjevné, že takové zadání lze naplnit značně obtížně, neboť je velmi obecné. Vhodnější by bylo zvolit typovou situaci a nad ní se pak hlouběji zamýšlet. Jiné požadavky na bezpečnost datového centra budou u malé firmy, jiné u velké společnosti se značným obratem a zcela odlišné u pracoviště majícího na starosti protivzdušnou obranu státu.

S přihlédnutím k obsahu i formě hodnotím práci jako kvalitní, diplomant je rozhodně mimořádně pracovitý a má neobyčejně široký rozsah znalostí.

Vzhledem k zmíněnému rozsahu bych považoval za vhodnější text práce rozdělit do základní části, která by naplňovala požadavky zadání, a příloh, které by obsahovaly detailnější údaje. Po stránce vypracování je práce pěkná, počet formálních či jazykových chyb je minimální.

Z textu práce vidím diplomantovu (zdá se mi úspěšnou) snahu na nic nezapomenout, což ovšem vedlo ke zmíněnému značnému počtu stran. V teoretické části textu práce se lze setkat s popisem problematiky legislativy, fyzické bezpečnosti, prevence a detekce útoků a požadavky na návrh počítačové sítě, dále pak v praktické části s logickým návrhem, fyzickým návrhem a systémem kontroly (spíše řízení) bezpečnosti. Obě tyto části se však obsahem zčásti podobají, resp. praktická část působí dojmem zpřesnění a rozšíření údajů uváděných v části teoretické. Rozhodně od ní nelze očekávat vlastnosti projektové dokumentace nebo závazných interních předpisů.

Například problematika ochrany utajovaných informací má jasně daná pravidla, primárně zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, a dále vyhláškami NBÚ. Veškeré v práci uváděné návrhy ochrany přenášených dat prostřednictvím virtuálních privátních sítí či protokolu IPSec jsou irelevantní, jedinou možností je použít certifikovaný kryptografický prostředek se všemi efekty (kromě zabezpečení a také například potřeba řádně vyškolené obsluhy mající příslušnou bezpečnostní prověrku).

V textu práce jsem narazil na některé sporné pasáže, jejichž výběr uvádím dále.

Strana	Popis / odkazovaný text	Komentář
33		Jsou směšovány normy ČSN, metodické pokyny pojišťoven (obojí nezávazné) a vyhlášky NBÚ (legislativně závazné, včetně sankcí).

48	Programy Tcpdump nebo libpcap velmi efektivně slouží jako senzory.	Ovšem použitelné pouze pro nejjednodušší účely jako je rozpoznávání základních signatur.
48		Rozdíl mezi senzory a agenty není příliš zřejmý.
53	kabel kategorie 6e	kabel kategorie 6a.
54		Některá tvrzení o IPv6 jsou dosti diskutabilní: záhlaví paketu je sice jednodušší, ovšem téměř vždy se vyskytuje ještě rozšiřující záhlaví; flow label nebyl určen pro QoS, ale pro aplikace pracující v reálném čase (a prakticky se nepoužívá); (pod)sítě jsou řešeny stejně jako u IPv4 (s CIDR); i i IPv6 existuje NAT (viz např. RFC 6296 - IPv6-to-IPv6 Network Prefix Translation) a samozřejmě také DHCP (RFC 3315).
54	Identifikátory sítě a hostitele mají stejnou délku 64 bitů	Toto se týká pouze koncových systémů. Adresy sítí se institucím přidělují podobně jako v současnosti u IPv4, tj. adresou a prefixem (CESNET - 2001:0718::/35).
54		Uvedené dělení firewallů je spíše výčtem možností realizace, vhodnější by bylo zobecnění. Je například otázkou, zda řadit NAT k základní funkci firewallu; domnívám se, že nikoliv – NAT je NAT.
57		Typy zranitelností – jsou směšovány obecné typy a zcela konkrétní případy. Proti většině navíc existuje účinná ochrana.
ko 58	Autentizace – podvržení autentizačních údajů.	Autentizační mechanismy by měly být vůči tomuto odolné, bylo by vhodné bližší vysvětlení.
67	Graf 1, Graf 3	Zkratky na horizontální ose by zasloužily vysvětlení někde poblíž.
73	Systémová bezpečnostní politika	Některé body by bylo možné sloučit, zjednodušit, zobecnit. Řada z nich se týká jen správců. Určitá opatření by se dala prosadit automaticky, nastavením příslušných systémových parametrů.
74		Pasáž související s VPN je příslušná spíše pro správce.
75	Síťový prvek nesmí mít lokálně definovaný uživatelský účet	Pokud by síťový prvek neměl možnost lokálního přístupu, jak by se dal spravovat v nouzi, například při výpadku sítě nebo zásadních změnách?
75	invalidními adresami dle RFC1918	Nepříliš přesný popis. RFC1918 specifikuje adresy pro použití v privátních sítích, které jsou ovšem jinak naprosto plnohodnotné.
78	attack surface	Tuto frázi nelze překládat jako „útočný povrch“, nic takového přece v češtině nemáme.
80	v případě pozitivního průniku	Co je to? Existuje i negativní průnik?
81	X-Windows	X-Window.
86	nepoužívat automatickou konfiguraci VLAN (DTP)	Protokol DTP umožňuje dohodnout režim portu (přístupový nebo trunk), s VLAN nijak nesouvisí.
87	modifikovat priority STP pro preferované cesty	Toto ovšem vyžaduje důkladnou znalost topologie sítě a zejména řádnou analýzu potenciálních dopadů!
87		Diplomant v ukázkách výpisů směšuje problematiku L2 přepínačů a L3 přepínačů.

89		Diplomat provádí umělé kalkulace, vycházející z vágních pojmů jako je „organizace středního až většího rozsahu“ apod. Dosti záhadně používá termín CIDR – je si skutečně vědom jeho významu? Má dojem, že nikoliv, jinak by těžko napsal „Malé organizace si vystačí s IP rozsahem /16 s maximálním počtem 256 logických segmentů (VLAN), z nichž každý disponuje 256 adresami.“, nýbrž by věděl, že oněch 16 bitů lze rozdělit podle potřeby jinak (viz VLSM). Navíc adresní rozsah /16 skýtá dostatečný prostor i pro velké organizace, ovšem při promyšleném hospodaření s adresami.
95	kategorie je Tier III	Dosáhnout naplnění požadavků Tier III (s certifikací) je velmi náročné, v ČR si je může dovolit snad jen firma typu ČEZ. Řada institucí si na Tier III pouze hraje, viz poznatky z výpadků poskytovatelů cloudových, hostingových a jiných služeb (Casablanca, naposledy WEDOS).
133	IPS vyšle falšovaně nastavený reset bit na oba konce aktuálního spojení	Spíše vyšle na každý konec spojení TCP segment s nastaveným příznakem RST.

Dotazy na diplomanta: jím částečně popisovaný protokol Spanning Tree trpí zásadní nevýhodou, která je ale současně jeho fundamentální vlastností. Tím, že blokuje vybrané spoje, sice řeší problém cyklů, zablokovaný spoj ale leží ladem, přičemž při kvalitní síti bez výpadků tak tomu může být trvale. V extrémním případě, pokud by se fyzická topologie blížila úplné topologii, by tak byla nevyužita, resp. nevyužitelná až polovina existujících spojů (!).

Zná diplomant jiné, efektivnější řešení problému cyklů na druhé vrstvě referenčního modelu síťové architektury, nežli nabízí protokol Spanning Tree?

Byl by diplomant schopen navrhnout dvě nebo tři reálně použitelné varianty zabezpečení malého datového centra od základní po velmi dokonalou a porovnat jejich finanční náročnost se zohledněním veškerých relevantních nákladů?

Celkové hodnocení práce:
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 diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

B - velmi dobře.

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

Datum 25.5.2014 Podpis oponenta diplomové práce