BAKALÁŘSKÁ PRÁCE - posudek oponenta

Marek Uher: Zabezpečení podnikové sítě (Intranetu)

Bakalářská práce se zabývá popisem řešení zabezpečení vnitřní sítě Ústavu hematologie a krevní transfuze (ÚHKR) v Praze.

V rámci úvodní kapitoly jsou podrobně popsána rizika, které je nutné řešit při ochraně vnitřní sítě. Další kapitola popisuje základní bezpečnostní principy, provádí rizikovou analýzu z hlediska užitné hodnoty, četnosti útoků, typu útočníků i útoků. V závěru kapitoly jsou zhodnoceny typy a chování *firewallů*.

Třetí kapitola se zabývá hodnocením a výběrem vhodného *firewallu* pro ÚHKR. Autor zvolil variantu paketového *firewallu* nad operačním systémem *Linux* (distribuce Caldera OpenLinux). V kapitole je provedeno zhodnocení bezpečnosti jednotlivých vstupních míst do intranetu a důkladně zdokumentována politika přístupu do/z Internetu. Další část kapitoly se věnuje popisu a zhodnocení jednotlivých dostupných administrativních nástrojů a popisem funkce *firewallu* v Linuxu. Autor využil pro implementaci své pomocné nástroje napsané v rámci dávek *tcsh*.

Práce je velmi propracovaná, ale měl bych několik připomínek. Zajímalo by mě podle jaké metodiky dospěl autor k vysokým číslům v rámci prováděné rizikové analýzy (str.15-19) a proč nepoužil popis podle uvedené metodiky (str. 13-14). Dále bych rozhodně zvážil propouštění ICMP zpráv - *redirect* (obecně rizika s napadením IP-směrování i zahlcení zdrojů nejsou zvážena). Autor několikrát neoprávněně zpochybňuje odolnost systému X-Windows (síťová bezpečnost je zajištěna pomocí otevřených autorizačních systémů (např. MIT-cookie...)), ale na *firewall* bych také X-windows neinstaloval. Na straně 37 (na rozdíl od strany 40 v úvahách o IP+) je chybně uvedeno, že směrovače fy Cisco umožňují filtrovat pouze podle IP-adres. Pro testování odolnosti *firewallů* existuje zpracovaná metodika například od NCSA i celá řada programů (Satan, ISS...).

Autorovi bych dále doporučil zvážit, zda nepoužít uvnitř ÚHKR privátní číslovací plán a použít překladu adres na *firewallu* (Network/Port Address Translation). Zvýšila by se zajisté bezpečnost celého systému (před některými typy útoků nelze ochránit paketovým filtrem) a další výhodou je možnost připojení dalších počítačů. Autor by měl zvážit i výkonnostní aspekty řešení a použít *proxy-cache* pro www služby a třeba i řízení toků (upřednostnění služeb) na výstupní lince (např. CheckPoint/FloodGate).

Práci doporučuji k obhajobě a navrhuji známku **výborně**.

V Hradci Králové dne 4.9.1998 Martin Červený