Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

Teze diplomové práce
Zabezpečení IT infrastruktury firem v ČR

Stára František
Vedoucí: Ing. Čestmír Halbich, CSc.

© 2015 ČZU v Praze

Souhrn

Diplomová práce se zabývá problematikou IT bezpečnosti s důrazem na firemní prostředí. V první části jsou vysvětleny pojmy, které je nutné znát pro bližší porozumění oblasti IT bezpečnosti například charakteristika IT bezpečnosti, bezpečnostních nástrojů jako je firewall, antivir, DMZ, charakterizování útočníků a používaných metod pro útok. Pro realizaci praktické části byla použita reálná firma, z které vycházely další části. Nejprve je společnost představena, poté proveden bezpečnostní audit na základě normy ISO 27001. Po definování bezpečnostních hrozeb ohrožující firemní prostředí a aktiv ve firemní infrastruktuře, provedena analýza rizik na základě, které jsou navrhnuty bezpečnostní opatření pro eliminování zjištěných hrozeb. Práci uzavírá finanční kalkulace navrhovaných opatření.

Klíčová slova

Informační bezpečnost, hrozby, rizika, bezpečnostní incident, analýza rizik, bezpečnostní audit, hacker, bezpečnostní politika, standardy, firewall, počítačový útok.

Cíl práce

Cílem literární rešerše je definovat IT bezpečnost, popsat jednotlivé hrozby, rizika, bezpečnostní politiky, standardy a bezpečnostní incidenty.

Cílem praktické části je na základě teoretických východisek a analýzy výchozího stavu zhodnotit a doporučit nastavení zabezpečení.

Metodika

První část práce obsahuje teoretické informace. K jejich dosažení byly nastudována odborná literatura a odborné texty dostupné na internetu. V první kapitole jsou popsány pojmy související se zabezpečením IT infrastruktury.

V druhé části je představena analyzovaná společnost. Zabezpečení společnosti je analyzováno, na základě normy ISO 27001, kdy je postupováno podle metodických oblastí použité normy. Analýza není provedena do takové hloubky, aby sloužila jako podklad pro provedení certifikace. Slouží jako pomocný nástroj pro zaměření se na kritické oblasti informačních systémů.

Následně je provedena analýza rizik. Vycházející z definovaných hrozeb a aktiv společnosti. Analýza monitoruje pravděpodobnost vzniku rizika, kde vychází z aktuální možnosti aktivace hrozby. Ohodnocení následků specifikuje rizika ohodnoceny mírou

závažnosti následků. Celková analýza rizik se skládá ze součtu ohodnocení následků a pravděpodobnosti vzniku rizika.

Na základě výsledků analýzy rizik a provedeného auditu zabezpečení jsou navrženy možné způsoby pro eliminaci definovaných rizik. Součástí návrhu je konečná finanční kalkulace navrhovaných změn.

Závěr

Bezpečnost informačních systémů je důležitou otázkou, kterou by se měla zabývat každá firma od malých až po velké firmy.

Vedlejším cílem práce bylo definovat pojmy, které jsou používány v oblasti IT bezpečnosti. V praktické části jsou vysvětleny pojmy IT bezpečnost, popsání jednotlivých hrozeb, rizik, bezpečnostní politiky, standardů, bezpečnostních incidentů a dalších termínů, které pomohou lépe pochopit a porozumět dané problematice.

Hlavním cílem praktické části bylo na základě teoretických východisek a analýzy výchozího stavu zhodnotit a doporučit nastavení zabezpečení. Nejprve byla představena analyzovaná společnost včetně přiblížení, jakým disponuje IT vybavením. Poté byl proveden bezpečnostní audit, který vycházel z metodiky normy ISO 27001. Provedený audit byl zjednodušen a v případě rozhodnutí společnosti pro provedení certifikace ISO 27001 je nutné provést bezpečnostní audit více podrobně. Zde byl audit použit pro přiblížení aktuálního stavu, jako návod pro metodický postup a definování kritických oblastí.

Po provedení bezpečnostního auditu a přiblížení společnosti byla provedena analýza rizik. Analýza rizik určuje kritická aktiva umístěna ve společnosti a dává je do vztahu s aktuálními hrozbami, které mohou aktiva postihnout. Mezi nejkritičtější hrozby se řadí chyba administrátora, krádež nebo ztráta zařízení, zkoušení uhádnutí hesel a počítačový virus. Tedy hrozby hrozí spíše z vnitřního prostředí a je potřeba je ošetřit. Mezi nejohroženější aktiva patří emailový server a klientská aplikace.

Na základě analýzy rizik a zjištění bezpečnostních nedostatků v provedeném bezpečnostním auditu byly navrženy způsoby jak hrozby eliminovat a lépe zabezpečit aktiva. Zlepšení bylo navrženo pro všechny kritické hrozby. Jedná se například o zakoupení nového firewallu, switche implementování nového antivirového řešení. Zlepšení pro oblasti, které nejsou takovou mírou ohroženy, byly navrženy jen bodově. Pro správný chod IT, je

zapotřebí definovat pravidelné činnosti administrátorů a evidování v administrátorském deníku.

V závěru práce je souhrn časové náročnosti uvedených prací pracovníky IT a cen použitých technologií. Souhrn je k dispozici vedení společnosti pro dodatečné vyčíslení celkových nákladů na implementované bezpečnostní mechanismy. Pro práci nebyla získána informace o hodnotě práce jednotlivých IT pracovníků z toho důvodu, je vyčíslena pouze časová náročnost. Ceny použitých technologií jsou uvedeny bez DPH. Náklad na implementaci produktu ESET je vysoký, ale pro vypovídající hodnotu jako změny oproti stávajícímu řešení, je nutné od tohoto nákladu odečíst náklady na stávající řešení.

Cíle práce byly dosaženy. Práce může být použita jako podklad vedení společnosti pro schválení navrhovaných změn a jako podklad pro IT manažera, který získá určitý návod jak navrhované změny v infrastruktuře provést, časovou náročnost pro vytváření plánu implementace a ohrožená aktiva a seznam nedostatků.

Seznam vybraných zdrojů:

1) JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Hacking. ISBN 9788024715612.

2) LOCKHART, Andrew. *Bezpečnost sítí na maximum*. Vyd. 1. Překlad Jiří Veselský. Brno: CP Books, 2005, 276 s. ISBN 8025108058.

5) SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.

7) DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno: Computer Press, a.s., 2004. 190 s. ISBN 80-251-0106-1

9) ERNST & YOUNG. Průzkum stavu informační bezpečnosti v ČR 2009. Ernst & Young, NBÚ, DSM data security management a Národní bezpečnostní úřad, 2009. 40 s. ISBN 978-80-86813-19-6