Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Teze diplomové práce

Bezpečnostní prověrka IT zabezpečení finanční organizace

Bc. Filip Honč

Bezpečnostní prověrka IT zabezpečení finanční organizace

Souhrn

Tato diplomová práce se zabývá tématem bezpečnosti IT, které je velice aktuální a váže se s pojmy audit nebo systém řízení bezpečnosti informací. V teoretické části je nastíněna teorie auditu a s ním souvisejících procesů, jehož výsledky a analýzy pomáhají vedení sledované organizace efektivně zacílit a odstranit nalezené nedostatky. Praktická část se věnuje otázce možností bezpečnostních testů prověřujících ochranu cílových systémů ve vybrané konkrétní instituci.

Cílem práce je prověření a kritické zhodnocení stavu IT bezpečnosti ve vybrané finanční instituci nebankovního sektoru a vytvoření návrhu změn pro zlepšení jejího stavu, a zároveň představení hlavních metod a postupů, jak hodnotit stav IT zabezpečení, a zásad podle kterých by se mělo firemní IT řídit.

Klíčová slova:

Bezpečnost IT, bezpečnostní audit, bezpečnost finanční organizace, bezpečnostní prověrka, penetrační testy, řízení bezpečnosti informací

1 Úvod

Diplomová práce se zabývá bezpečnostní prověrkou IT zabezpečení ve smyslu auditu informačních systémů a technologií. Audit IT jako takový je poměrně mladá a rychle se rozvíjející disciplína. V této práci se proto věnuji možnostem auditu IS/IT v menším podniku ve spojení s testy bezpečnosti řízení informací.

Představím základní techniky a koncepce řízení IT oddělení a pokusím se je aplikovat na zkoumaný podnik. V průběhu studia norem a standardů jsem dospěl k závěru,

že většina norem a standardů je vytvořena pro využití ve velkých společnostech, a proto bude zajímavé, jak lze aplikovat zvolené metodiky při řešení auditu IT ve společnosti menší, případně střední.

Motto:

Bezpečnost je tak účinná, jak je silný její nejslabší článek.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem mé práce je zjistit současný stav bezpečnosti informačního systému v menším finančním podniku v nebankovní sféře. V současnosti je kritizována u menších podniků nedostatečná IT bezpečnost, což vede k přeorientování útočníků (hackerů) v posledních letech na malé a střední firmy. Jako základ pro srovnání bezpečnosti použiji standardy a metodiky pro auditování IS/IT.

Dále mám za cíl zjistit, jaké mají tyto podniky protiopatření proti útoku zvenčí i zevnitř sítě a vyzkoušet testovací útoky na průnik do vnitřní sítě z internetu, případně ohrozit stabilitu webových služeb.

Na základě těchto dat chci provést analýzu rizik a porovnat s očekáváním nižší úrovně zabezpečení. V poslední části je mým cílem vytvořit návrh na zlepšení stavu zabezpečení s konkrétním doporučením a výběrem technik nebo produktů, které jsou v současnosti na trhu nebo v souladu s mezinárodními normami.

Tato práce nemá za cíl do nejmenších podrobností rozebrat teorii auditu a samotný průběh, ale praktická část se věnuje otázce skutečných testů na zjištění ochrany cílových systémů. Jedním z dalších cílů je vytvořit komplexní přehled metod a nástrojů, jak by se mělo moderní IT řídit. Dále se hledá odpověď na otázku, jestli má smysl provádět na menších firmách kompletní audit IS/IT dle mezinárodních standardů. Celkově je práce na pomezí dvou větších informatických celků a těmi jsou audit IS/IT a řízení bezpečnosti informací.

2.2 Metodika

Analýza skutečného prostředí podniku, sběrem informací na místě a pomocí dotazování na vedoucího IT oddělení. Dalším krokem je vypracování analýzy rizik a SWOT analýzy. Pomocí dostupných zdrojů určit vhodné testování cílového podniku na základě metodik nebo jejich kombinací.

2.2.1 Audit IS/IT a systém pro řízení bezpečnosti informací

Předpokladem kvalitního auditu je využití existující metodiky, případně standardu, či normy, proto provedu porovnání nejznámějších metodik auditu, což jsou ITIL a COBIT. Následně provedu z pohledu zvolené metodiky hodnocení stavu IT v menším podniku. V další části diplomové práce popíšu návrh změn s cílem uzpůsobit fungování IT oddělení v souladu s moderním řízením IT a postup, jak zapracovat systém řízení bezpečnosti informací ISMS.

2.2.2 Penetrační testy

Největší důraz věnuji penetračním testům, které jsou metodou pro hodnocení počítačového a síťového zabezpečení. Jedná se o simulaci útoku na systém zevnitř nebo zvenčí. Jediným rozdílem oproti skutečnému útoku je, že nemá za cíl nějakým způsobem poškodit cílový subjekt, ale pouze zjistit nedostatky vycházející z chybného nastavení systému, případně chybějících bezpečnostních komponent. Vychází ze známých softwarových a hardwarových nedostatků. Analýza je provedena z pohledu potencionálních útočníků.

3 Závěr

V teoretické části této diplomové práce byly objasněny techniky a metody, které vedou k systematickému vedení IT oddělení. V obecné rovině byly představeny aktuální normy a zákony, které je dobré sledovat, a podle nich přizpůsobit řízení podnikového IT. Ve zkratce byl nastíněn vznik a význam auditu a institucí, jež umožňují rozvoj tohoto odvětví. Jako další zásadní bod byla prezentována nutnost řídit bezpečnost informací a

zapracovat ji do bezpečnostní politiky podniku. V teoretické rovině byly popsány metodiky provádění penetračních testů, které byly následně v praktické části použity společně s vybraným nástrojem.

Cílem praktických testů bylo dokázat možnost průniku zabezpečením organizace technikami používanými hackery k útokům na interní počítačové systémy. Bez problému bylo překonáno zabezpečení bezdrátové sítě a proveden průzkum sítě za ní. Povedlo se dokázat, že zabezpečení zvolené firmy je na velmi špatné úrovni.

Po provedení testů je možné objektivně prohlásit, že prověřovaná instituce je snadným terčem pro útok hackerů a celkové zabezpečení by mělo být zásadně posíleno, jinak bude bezpečnost systémů v permanentním ohrožení. Zároveň je nutné bezpečnostním problémům předcházet, nikoli řešit až naléhavé problémy. Provedená bezpečnostní prověrka odhalila několik zásadních nedostatků. Jako klíčový nedostatek byla označena absence promyšleného řízení IT a s tím spojená bezpečnostní politika. V závěru praktické části byl navržen plán změn s návrhem konkrétních protiopatření, včetně návrhu na přepracování systému řízení bezpečnosti do shody s normou ISO/IEC 27000 a doporučena následná certifikace. Přínosem pro testovaný podnik byl nový a nezaujatý náhled na stav bezpečnosti IT a představení nového směru, jak ji vnímat a zajišťovat.

4 Seznam použitých zdrojů

1) SVATÁ, Vlasta. Audit informačního systému. 2. vyd. Praha: Professional Publishing, 2012, 219 s. ISBN 9788074311062.

2) DOUCEK, Petr, Luděk NOVÁK a Vlasta SVATÁ. Řízení bezpečnosti informací. 1. vyd. Praha: Professional Publishing, 2008, 239 s. ISBN 9788086946887.

3) SENFT, Sandra. Information technology control and audit. 4th ed. Boca Raton, FL: CRC Press, 2013, 740 s. ISBN 9781439893203.

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

5) ISO.cz. [online]. [cit. 2015-03-04]. Dostupné z: http://www.iso.cz/?page_id=46