Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta
Katedra informačních technologií

Diplomová práce

Bezpečnostní infrastruktura informačního systému v MSP

Autor: Bc. Jan Drmla
Vedoucí práce: Doc. Ing. Zdeněk Havlíček, CSc.

Bezpečnostní infrastruktura informačního systému v MSP

Souhrn

Obsah celé diplomové práce lze rozdělit do dvou hlavních částí, kdy se jedná o návrh bezpečnostní politiky pro vybraný MSP a druhá část zabývající se samotnou realizací bezpečnostní infrastruktury. Popsány jsou jednotlivé postupy tvorby bezpečnostní politiky vycházející z jednotlivých bezpečnostních ISO norem. Uplatnění této politiky lze zobecnit na firemní prostředí podobného rozsahu a zaměření. Praktická část diplomové práce je rozčleněna do jednotlivých dílčích projektů a postavena na reálném firemním prostředí. Kde byly aplikovány současné postupy podloženy odbornými materiály. Dílčí části této práce jsou zaměřeny na vybudování centrální místnosti, propojení vzdálených lokalit a vytvoření interního dokumentu bezpečnostní politiky.

Klíčová slova: bezpečnost IS, počítačová síť, zálohování, hardware, software, firewall, ACL, bezpečnostní politika, simulace sítě

1. Úvod

Bezpečnost přenášených a uchovávaných informací je dnes bezpochybně celosvětově nejdiskutovanější tématem. Nejen ve firemním prostředí, ale i v osobním světě jsou informace v podstatě nejcennějším vlastněným aktivem. Zároveň ale v mnoha případech jsou vystaveny vnějším i vnitřním rizikům v podobě hackerských útoků, nebo ztráty, popřípadě poškození vlastními zaměstnanci apod., Těmto rizikům, která nás ohrožují lze včas předcházet a adekvátně na ně reagovat.

„Pod nátlakem narůstajících okolních hrozeb si sami firmy velice dobře uvědomují skutečnost, že důležitá interní data musejí chránit před vnějším světem mnohem důsledněji, než tomu bylo doposud.“ Tento výrok pronesl uznávaný zahraniční odborník na bezpečnost Borek Boissy, který byl pozván na akademickou půdu ČZU, aby zde vedle cyklus přednášek o současné problematice ICT[1] a její bezpečnosti. Proto jsou firmy ochotny na zvýšení bezpečnosti dle doporučených ISO norem a standardů vyčlenit finanční prostředky a změnit i vlastní postoje k ochraně dat. V lepších případech dochází pouze k aktualizaci stávajících řešení. Jinde musí dojít k restrukturalizaci nebo úplnému zřízení nové infrastruktury a uzpůsobení k bezpečnému chování všech zúčastněných osob ve firemním prostředí. Pokud firma učiní kroky ke zřízení bezpečnostní politiky a zaručí se k jejímu striktnímu plnění, musí při porušení pravidel dodržet sankční limity i pro nejvýše postavené. Protože integrita vnitřní bezpečnosti je neméně důležitou stránkou pro uchránění firemních informací, před vynášením nebo špionáží z vlastních řad, s jakýmkoliv úmyslem.

V diplomové práci budou navrženy konkrétní kroky a doporučeny kontrolní mechanismy, jak zlepšit vnitřní i vnější bezpečnostní situaci v dané organizaci. Jelikož většina těchto kroků je používána jako standardizovaný postup, lze navrhovaná řešení zobecnit na podobné typy objektů. Popřípadě znásobit jednotlivé oblasti dle velikosti rekonstruovaného objektu v návaznosti na potřeby a požadavky konkrétní organizace.

[1] Information & Comunication Technologies

2. Cíl práce

Hlavním cílem předkládané diplomové práce je zanalyzovat informační systémy z bezpečnostního hlediska a navrhnout bezpečnostní infrastrukturu aplikovatelnou do vybraného podniku.

Tento hlavní cíl práce se sestává z mnoha důležitých dílčích cílů, mezi něž jsou zahrnuty především tyto následující, které kopírují obecně definovanou strukturu takto zaměřeného odborného textu.

- *Teoretické zkoumání bezpečnostních technik, postupů a opatření*
- *Analyzovat současný stav ve zvoleném podniku z bezpečnostního hlediska*
- *Navrhnout patřičná bezpečnostní opatření pro zvýšení stability celého informačního systému*
- *Připravit dokument bezpečnostní politiky*
- *Formulovat obecné a specifické závěry dané problematiky*

3. Metodika

Nejdříve budeme analyzovat teoretické přístupy při zajišťování bezpečnosti informačního systémů a poté charakterizovat dílčí bezpečnostní oblasti, v praxi využívané pro návrh a realizaci. Teoretické poznatky budou čerpány z odborné literatury, řádně zacitovány a v textu označeny. Za další zdroje lze považovat samostudium problematiky a také již nabyté praktické zkušenosti v oboru.

Praktická část, tvořící jádro práce, vychází z načerpaných teoretických podkladů a povede k aplikaci jednotlivých postupů tvorby bezpečnostní infrastruktury. V prvních fázích bude představena a interně analyzována společnost Dahl-tok s.r.o. na níž budou provedena jednotlivá nápravná opatření pro zlepšení bezpečnosti systému. Počínaje vybudováním zabezpečené a klimatizované centrální místnosti, následováno propojením poboček do centrálního uzlu až po nastavení jednotlivých lokalit, jak z pohledu aplikačního prostředí, tak síťového rozhraní. Posledním krokem ke kompletizaci dílčích projektů bude vytvoření interního dokumentu bezpečnostní politiky v návaznosti na nově budovaný stav infrastruktury.

Závěrem budou synteticky zhodnoceny přínosy a nedostatky navrhovaných řešení, osvětleny některé realizační postupy a jejich současné rozpracování.

4. Závěr

Hlavní cíl, analýza informačních systémů z bezpečnostního hlediska a návrh bezpečnostní infrastruktury byl splněn, na základě dílčích cílů předkládané diplomové práce, z kterých postupně vznikaly výsledné návrhy a závěry:

- *Teoretické zkoumání bezpečnostních technik, postupů a opatření*

Formulace úvodních teoretických podkladů jednotlivých bezpečnostních technologií a postupů byl plně využit pro vypracování praktické části diplomové práce. Obě hlavní kapitoly práce jsou úzce provázány a ve výsledku aplikovány do reálného firemního prostředí. Studiem a analýzou odborných materiálů zaměřených na standardy a normy bylo přispěno k vytvoření teoretického podkladu pro definování interního dokumentu bezpečnostní politiky.

- *Analyzovat současný stav ve zvoleném podniku z bezpečnostního hlediska*

Vlastní analýza vybraného podniku odhalila ukázkový příklad decentralizovaného a nezabezpečeného firemního prostředí, velice náchylného k výpadku služeb s velkým množstvím rizikových faktorů jako například chybějící záloha interních dat. Na těchto základních analýzách byla stanovena jednotlivá bezpečnostní opatření, která byla demonstrována v další kapitole práce.

- *Navrhnout patřičná bezpečnostní opatření*

Dílčí návrhy bezpečnostních opatření využívají celou množinu vnitřních a vnějších bezpečnostních prvků nabitých z teoretických a praktických podkladů a využité pro samotné aplikování do reálného prostředí. Především došlo k centralizaci infrastruktury a přechod na samosprávu prvků zajišťující bezpečný chod celého systému umístěného v nově vybudované zabezpečené centrální místnosti. Další opatření podpořila vznik nového bezpečného a šifrovaného propojení vzdálených lokalit nebo vytvoření stabilního zálohovacího systému, kterým bylo zcela eliminováno i kritické místo v podobě ztráty interních dat.

- *Připravit dokument bezpečnostní politiky*

Zavedení připravovaného dokumentu v budoucnu poslouží pro kontrolované řízení bezpečnosti informačního systému jako celku. Návrh bezpečnostního dokumentu je založen na doporučených ISO standardech a ostatních normách. Dokument se dotýká všech nově navrhovaných opatření bezpečnostní infrastruktury a určuje pravidla a povinnosti osobám pracujícím v systému. Návrh byl z hlediska správnosti postupů a norem ověřen nezávislým odborníkem zabývajícím se auditními bezpečnostními kontrolami. V důsledku toho byla doporučena každoroční revizní schůzka k provedení důležitých aktualizací dokumentu.

- *Formulovat obecné a specifické závěry dané problematiky*

Se závazným doporučením aktualizací a průběžných kontrol je samozřejmě svázána i celá bezpečnostní infrastruktura nevyjímaje ani povědomí o aktuální informační bezpečnosti svých zaměstnanců. Hlavně z důvodu dynamického rozvoje bezpečnostních technologií, které zejména reagují na propracovanost kybernetické kriminality, proto z pohledu firmy a ochrany jejich interních dat nelze podcenit žádnou část bezpečnostní infrastruktury. A vždy se zabývat každým incidentem i malého rozsahu, který ve firmě nastane a vyvodit z nich příslušná opatření.

Za specifikum takovýchto návrhů je považována finanční náročnost jednotlivých bezpečnostních opatření, která v oblasti IT nečiní malé náklady. Proto je vždy důležité myslet na případná rizika a ztráty plynoucí z nezabezpečeného systému. Náklady vložené do bezpečnostních opatření mohou narůstat do statisícových částek, jako je tomu v zde v diplomové práci, kde se vybudování centrální místnosti pohybuje okolo 800 000 Kč pro konkrétní řešení. Uvědomme se, že ztrátu dat nelze snadno vyčíslit nebo nahradit finančními prostředky, proto by měly být investice vložené do bezpečnosti chápány pouze pozitivně jako budoucí zisk.

5. Seznam vybraných použitých zdrojů

Bigelow Stephen J. Mistrovství v počítačových sítích [Kniha]. - Brno : Computer Press, 2004. - str. 992. - ISBN: 80-251-0178-9.

Donahue Gary A. Kompletní průvodce síťového experta [Kniha]. - Brno : Computer press, 2009. - ISBN: 978-80-251-2247-1.

NBÚ Metodický pokyn bezpečnostní dokumentace ver. 3.0 [Online] // NárodníBezpečnostníÚřad.cz. - 15. Září 2014. - 23. leden 2015. - http://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/certifikace-informacnich-systemu/metodicke-pokyny/.

Strebe Matthew a Perkins Charles Firewally a proxy-servery [Kniha]. - Brno : Computer press, 2003. - ISBN: 80-7226-983-6.

Chlup Marek Bezpečnost ICT a standardy ISO [Článek] // Computerworld. - Praha : IDG Czech, a.s., 2008. - Ročník 19.. - Číslo 2 : Sv. 1.-14.2.

Ohlhorst Frank [Online] // NetworkComputing. - 1. Březen 2013. - 3. Březen 2015. - http://www.networkcomputing.com/careers-and-certifications/next-generation-firewalls-101/a/d-id/1234097?.