ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

PROVOZNĚ EKONOMICKÁ FAKULTA

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

TEZE DIPLOMOVÉ PRÁCE

ZABEZPEČENÍ IT INFRASTRUKTURY A ZÁLOHA DAT V MALÝCH A STŘEDNÍCH PODNICÍCH

(Bc.) Radek ČERŇANSKÝ

vedoucí: Mgr. Ing. Vladimír Očenášek

1 SOUHRN

Diplomová práce je zaměřena na zabezpečení firemní infrastruktury a zálohu dat v malých a středně velkých podnicích. Teoretická část je rešerší odborné literatury a elektronických zdrojů. V praktické části autor analyzuje současný stav zabezpečení firemní IT infrastruktury malého a středně velkého podniku, včetně systémů pro zálohu dat. Analýza je provedena formou bezpečnostního auditu, který je cílený na komplexní přehled, reflektující současný stav zabezpečení a zálohy dat. Výsledky auditu jsou východiskem pro formulaci nápravných opatření a doporučení, která zajistí vyšší úroveň zabezpečení infrastruktury a zajistí cenná podniková data. Autor předkládá bezpečnostní řešení v několika variantách a jednotlivé návrhy kalkuluje dle aktuálních tržních cen.

Klíčová slova: IT infrastruktura, síťová architektura, bezpečnost, záloha dat, archivace

2 ÚVOD DO PROBLEMATIKY

Zabezpečení firemní infrastruktury a záloha podnikových dat je oblast, bedlivě sledovaná zejména u velkých a nadnárodních organizací a podniků. Na úrovni malých a středních podniků je téma bezpečnosti upozaděno, oproti jiným hrozbám, které jsou pro podniky zjevnější a snáze uchopitelné. U malých podniků, napojených na městské rozpočty, jsou klíčovým mezníkem finance, které nepřímo ovlivňují investice do modernějších technologií a konceptů pro nakládání s podnikovými daty.

Autor se zabývá uvedenou problematikou, neboť je přesvědčen o hloubce a vážnosti významu bezpečnosti firemní infrastruktury i na úrovni malých a středních podniků. V regionálním rozvoji, stejně tak jako ve veřejné správě, plní pracovní stanice, přenosný počítač či smartphone, důležitou úlohu – jsou základním pracovním nástrojem úředníků, manažerů a inovátorů. Výstupy a výsledky pracovní činnosti úředníka či manažera mikroregionu, jsou ve valné většině zpracovány, některým z výše zmíněných prostředků, které propojeny sítěmi různého typu, kvality a charakteru, tvoří IT infrastrukturu organizací všech úrovní a velikostí. Cenné výsledky výzkumů, analýz, bádání a kvalifikované práce, putující infrastrukturou, lze souhrnně označit, jako produkční data. Způsoby, jakými data (výsledky svých činností) chráníme proti poškození, zcizení, ztrátě a nenávratnému zničení, determinují systémy pro jejich zálohu a archivaci.

Aktuálnost zmíněné problematiky reflektují útoky a průniky do firemních infrastruktur organizací, všech velikostí i zaměření, které byly zaznamenány v nedávné době.

Diplomová práce je strukturována do teoretické a praktické části. Teoretickou část práce tvoří rešerše odborné literatury, odborný tiskovin a elektronických zdrojů. Praktická část je členěna do pěti úseků. Autor provádí analýzu zabezpečení podnikové infrastruktury v malém (Ašské lesy, s.r.o.) a středně velkém (Ašské služby, s.r.o.) podniku. Výsledky z provedených šetření jsou následně formulovány do řady nápravných opatření, doporučení a návrhů, které zajistí vyšší úroveň zabezpečení infrastruktury zkoumaných podniků a vyšší stupeň ochrany podnikových dat. Návrhy a doporučení autor následně kalkuluje dle aktuálních tržních cen. Pro jednotlivá nápravná opatření jsou autorem připravena variantní řešení, které podnikům umožní alokovat dodatečnou úroveň zabezpečení s ohledem na limitní rozpočet organizace.

3 CÍLE PRÁCE

Autorovým záměrem je posoudit a vyhodnotit současný stav zabezpečení IT infrastruktury a systémů pro zálohování a archivaci dat v malých a středních podnicích. Úroveň zabezpečení bude podrobena důkladnému testování a přezkoumávána ve vrstvách.

Dílčími cíli je konkrétní analýza stavu zabezpečení perimetrů lokálních sítí a bezdrátových sítí v malém a středně velkém podniku na regionální úrovni.

Následným dílčím cílem je prověřit aktuální stav systémů pro zálohování a archivaci dat v podnicích s regionální působností. Dále vyšetřit, jak je nakládáno s podnikovými daty a jakým způsobem jsou data archivována.

Výsledky z provedených šetření, uvažuje autor využít při formulaci nápravných opatření a doporučení pro posílení zabezpečení infrastruktury podniků a bezpečnějšímu systému pro zálohování a archivaci dat, která budou třetím dílčím cílem.

Nápravná opatření a doporučení, které autor hodlá předložit, budou kalkulována dle aktuálních tržních cen.

4 METODIKA

Uchopit obsáhlé téma bezpečnosti, uvažuje autor pojmout skrze škálu testů a analýz, realizovaných v produkčním prostředí, zkoumaných podniků.

Sběr dat

Informace a data nezbytná k provedení podrobného přezkumu současné úrovně zabezpečení v podnicích, byla čerpána ze široké škály zdrojů a šetření.

Primární data – byla získána skrze vlastní výzkumná šetření, analýzy a realizovaná testování přímo v produkčním prostředí u obou podniků. Využity byly rovněž konzultace se systémovými administrátory, zodpovědnými za provoz a údržbu stávající infrastruktury a dodavatelem hardwarového vybavení.

Sekundární data – Interním zdrojem byla podniková dokumentace podniku Ašské lesy, s.r.o a Ašské služby, s.r.o. Jako externích zdrojů, autor využil dokumenty, příručky, doporučení a webináře společností Cisco, Autocont, Kaspersky, Sophos, Symantec, Fortinet, Kerio a TrendMicro.

Nástroje

Fáze sběru dat představovala samotné testování dílčích prvků infrastruktury. Dále rozhovory se zaměstnanci, studium podnikové dokumentace a směrnic. V neposlední řadě byly provedeny operativní testy na aktivních částech ekosystému.

Ve fázi analýzy dat, jsou zpracovány výsledky dílčích šetření, rozhovorů a rozborů podnikové dokumentace a směrnic bezpečnostní politiky. Zjištěná rizika jsou kategorizována. Následně jsou formulována opatření a doporučení, která umožní nápravu v problémových oblastech a zeštíhlí slabá místa systémů.

Analýza zabezpečení IT infrastruktury v podnicích

Analýza je cílena na objevení slabých míst a ohrožení, která vyplívají z nedostatečného zabezpečení perimetrů firemního prostředí. Pro komplexní testování infrastruktury podniku je nutno zvolit takové řešení, které obsáhne všechny parametry a atributy, které jsou součástí aktivit a prostředků, s přímým vlivem na funkčnost a stabilitu infrastruktury.

Bezpečnostní audit

Bezpečnostní audit firemní infrastruktury zkoumaných podniků, je zvolen jako testovací nástroj, který poskytne kompletní přehled o všech slabinách a nedostatcích uvnitř infrastruktury.

Finálním výstupem auditu je výsledná zpráva, která poskytuje kompletní přehled o současném stavu infrastruktury, zjištěné hrozby a nedostatky, včetně nápravných opatření a řešení ve formě návrhů a připomínek.

5 ZÁVĚRY A DOPORUČENÍ

Problematika bezpečnosti firemní infrastruktury a ochrana dat v malých a středních podnicích patří k důležitým, avšak opomíjeným tématům. Vedení organizací, problematiku bezpečnosti infrastruktury upozaďuje, oproti zřetelnějším a obvyklejším formám nebezpečí, které organizacím hrozí. Autor považuje za nezbytné upozornit na klíčový atribut, kterým nedostatečné zabezpečení perimetrů podniku a slabá ochrana dat, převyšuje ostatní rizika ohrožující organizace, činné ve veřejné správě a rozvoji regionů – bezprostřednost a okamžitost. Zatímco čerpání omezeného rozpočtu, odliv kvalifikovaných pracovníků a nevalná opora v zákonech, jsou problémem pozvolným a plíživým (organizace disponuje solidními reakčními časy, v řádech týdnu až měsíců), v případě útoku na podnikovou síť, převzetí kontroly nad klíčovým serverem infrastruktury, či ztrátě a úniku zásadních podnikových dat, je čas nutný pro obnovení původního stavu, otázkou několika hodin.

Provedené analýzy současného stavu zabezpečení perimetrů, odhalily závažná bezpečnostní rizika a nedostatky. Rizika jsou, vzhledem ke své závažnosti, hodnocena jako kritické slabiny, s působností na funkčnost a provoz, napříč podnikovými ekosystémy.

Bezpečnostní audit realizovaný autorem v podnicích, poskytl komplexní přehled o všech hrozbách a slabých místech infrastruktury v podnicích. Závažné hrozby nalezl autor v architektuře bezdrátové sítě, kdy nevhodné umístění jednoho z hardwarových prvků a způsob jeho konfigurace, představuje snadný cíl ze strany útočníka.

Nedostatky a rizika byla identifikována ve třinácti z patnácti analyzovaných bezpečnostních vrstev infrastruktury podniku Ašské služby a devíti z jedenácti vrstev společnosti Ašské lesy. Uspokojivé výsledky byly zaznamenány, u obou společností, v oblastech rozvodů a kvalitě metalické kabeláže, tvořící páteřní komunikační síť v podnicích.

Nápravným opatřením a doporučeními jsou v případě podniku Ašských služeb, změny v konfiguracích serverů a uspořádání síťových hardwarových prvků. Rekonfigurace sběrnicové ústředny systému elektronického zabezpečení. Instalace nové jednotky záložního napájení do serverovny číslo 2. Výstavba dohledového systému v ústředí podniku. Integrace antivirového řešení Kaspersky Endpoint Security na všechny pracovní stanice, včetně

mobilních zařízení. Změny v hardwarové konfiguraci databázového serveru. Investice do nového nárazníkového firewallu, případně výměna operačního systému pod softwarovou nadstavbou. Změna systému zálohování, spočívající v integraci zařízení typu NAS do infrastruktury a pronájem cloudového úložiště, určeného pro archivaci a duplikaci podnikových dat. V podniku Ašských lesů, je nutno rekonfigurovat nastavení přístupového bodu bezdrátové sítě. Zavést systém pro zálohu produkčních dat na externí diskové pole, případně zařízení typu NAS, pronajmout cloudový prostor. Doporučuji úpravu nastavení, restrikce oprávnění lokální správy, všech pracovních stanic.

Při sestavování variantních, nápravných opatření pro oba podniky, autor respektuje omezené rozpočty malého a středně velkého podniku. Každá varianta je kalkulována s cenovým rozpětím, které lze aplikovat, při zachování přidané hodnoty v podobě posílení stávajícího zabezpečení. Některá nápravná opatření jsou realizovatelná, bez nutnosti dalších investic. Jsou spojeny pouze s částečnou, u některých opatření kompletní, odstávkou systémů a serverů. Varianty jsou vymezeny v časových harmonogramech, které pokrývají, dobu nezbytně potřebnou, pro aplikaci nápravných kroků.

V prostředí zkoumaných podniků, autor doporučuje konzultovat nápravu současného stavu podnikové infrastruktury, se specialistou na bezpečnost. Identifikované hrozby klasifikuje jako závažné a hrozící výpadek či nevratná ztráta dat, je více než pravděpodobná.

Autor předložil výsledky šetření jednatelům obou podniků, kteří připomínkovali zkoumané oblasti auditu a vzhledem k neuspokojivému stavu současného stavu infrastruktury u obou organizací, požádali autora o další spolupráci.

Zaměření autorova výzkumu v oblasti zabezpečení a zálohy dat v malých a středních podnicích, je cíleno na technické aspekty infrastruktury. Pro svou další činnost a spolupráci s podniky, autor hodlá zpracovat bezpečnostní audit procesního charakteru, který bude cílen na vzájemnou provázanost bezpečnostní politiky s nasazenými technologiemi.

SEZNAM POUŽITÝCH ZDROJŮ

Tištěné zdroje

BEJTLICH, Richard. *The practice of network security monitoring: understanding incident detection and response*. San Francisco: No Starch Press, 2013, 1 online zdroj (379 pages). ISBN 978-1-59327-534-1.

BIGELOW, Stephen J. Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů. Vyd. 1. Překlad Petr Matějů. Brno: ComputerPress, 2004, 990 s. ISBN 80-251-0178-9.

DONAHUE, Gary A. Network warrior. 2nd ed. Beijing: O'Reilly, 2011, xxiii, 757 s. ISBN 978-1-449-38786-0.

ENGEBRETSON, Pat a James BROAD. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Waltham, MA: Syngress, c2011, xvii, 159 p. ISBN 1597496553.

KENNEDY, David. Metasploit: the penetration tester's guide. 1st ed. San Francisco: No Starch Press, c2011, xxiv, 299 s. ISBN 9781593272883.

NEMETH, Evi, Garth SNYDER a Trent R HEIN. Linux: kompletní příručka administrátora: 2. aktualizované vydání. Vyd. 1. Brno: ComputerPress, 2008, 984 s. ISBN 978-80-251-2410-9.

SOSINSKY, Barrie A. Mistrovství – počítačové sítě. Vyd. 1. Brno: ComputerPress, 2010, 840 s. Mistrovství (ComputerPress). ISBN 978-80-251-3363-7.

TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.

Elektronické zdroje

Access Communications. ACCESS COMMUNICATIONS PTY LTD. *Www.accesscomms.com* [online]. 2014 [cit. 2014-11-04]. Dostupné z: https://www.accesscomms.com.au/reference/coax.htm
Best cloud storage [online]. 2015 [cit. 2015-03-10]. Dostupné z: http://www.bestcloudstorage.net/

Edraw Visualization Solutions. *Active Directory Diagramming Software* [online]. 2013 [cit. 2014-11-04]. Dostupné z: http://www.edrawsoft.com/Active-Directory.php

SURAPATI, Taufan. How Antivirus Works: SignatureBasedDetection, HeuristicScanning and BehaviorBlocker [online]. 13. 8. 2011. [cit. 30-10-2014]. Dostupné z: http://www.articlesbase.com/security-articles/how-antivirusworks-signature-based-detection-heuristic-scanning-and-behavior-blocker-5124641.html.

THE OPEN GROUP. *The UNIX System* [online]. 1. vyd. Londýn, 2012 [cit. 2014-11-03]. Dostupné z: http://www.unix.org/what_is_unix/history_timeline.html