Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

TEZE DIPLOMOVÉ PRÁCE

Network Intelligence

Marek MIKEL

Network Intelligence

Souhrn

Diplomová práce se zabývá problematikou Network Intelligence, skládající se z odchytávání paketů, hloubkové inspekce paketů a Business Intelligence. V empirické části je tato problematika aplikována na návrh multidimenzionálního modelu Network Intelligence.

Jejím cílem je vysvětlit obsáhlý pojem Network Intelligence, skládající se ze tří hlavních částí, a postup při jeho tvorbě. Dalším cílem je tyto poznatky aplikovat na tvorbu návrhu multidimenzionálního modelu.

Práci tvoří dvě stěžejní oblasti. Část teoretická, která objasňuje zpracování odborných pramenů, znalost počítačových sítí a definici Network Intelligence. Dále teoretická část objasňuje jednotlivé částí Network Intelligence a to hloubkovou inspekci paketů, odchytávání paketů a detailní vysvětlení Business Intelligence a jeho tvorby.

Empirická část předkládá postup návrhu funkčního multidimenzionálního modelu. V první části je popsán odchyt paketů pomocí sniffovacího programu a jejich export do souboru čtivého pro model. Ve druhé části je vytvořen samotný návrh multidimenzionálního modelu a v poslední části je vytvořen analytický výstup.

Klíčová slova

Network intelligence, Business Intelligence, deep packet inspection, packet capture, communications networks, protocols, metadata

ÚVOD

V současnosti řada společností zavádí systémy typu Business Intelligence k podpoře jejich řízení a rozhodování. Firmy, které pracují s daty, tento nástroj v rámci úspor a zkvalitnění působení na trhu rády zavádějí. Celý proces Business Intelligence je dosud zaměřován zejména na ekonomický směr, tedy zjednodušeně řečeno, na výnosy, náklady na jejich výrobky či služby a na jejich odbyt.

Téma diplomové práce bylo zvoleno z toho důvodu, že Business Intelligence dosud není zaměřen na kontrolu počítačové sítě, a proto se tato práce zabývá rozšířením technik Business Intelligence i do IT sféry. Ve větších firmách bývá problém s kontrolou síťové komunikace. Je možné zpětně ručně zkontrolovat konkrétní počítač, k jakým službám z něj bylo přistupováno, jaká data si ukládal z Internetu, či jaká data kopíroval na externí disky. Vše má ale časově zdlouhavý proces. Tato práce celý proces zjednodušuje na základě vytvoření tzv. Network Intelligence, neboli aplikace pro kontrolu síťové komunikace, která není dosud v české literatuře zavedena. Využívá analytické principy Business Intelligence v oblasti počítačových sítí. Tato aplikace je navržena zejména manažerům, správcům sítě, ale i zaměstnancům z oblasti bezpečnosti, která přináší přístup k těmto informacím z jedné aplikace. Z této aplikace mohou ve firmě kontrolovat pohyby na počítačové síti, zatížení této sítě i případné porušení bezpečnostních interních předpisů.

Nově zavedený model Network Intelligence je rozšířením Business Intelligence na počítačové sítě. Skládá se z Deep Packet Inspection, neboli z hloubkové inspekce paketů, z Packet Capture, odchytávání paketů a z Business Intelligence.

První část práce se zabývá vysvětlením jednotlivých pojmů Network Intelligence. V empirické části jsou tyto poznatky prakticky aplikovány. Nejprve je provedeno odchycení paketů, které poslouží k analýze síti a poté je vytvořen multidimenzionální model. Je navržen jak konceptuální a logický model, tak i fyzický model v programu MS Pivot. Na základě těchto skutečností je vytvořen jednoduchý report pro management podniku v nástroji PowerView, který informuje o síťové komunikaci.

CÍL PRÁCE A METODIKA

Cílem diplomové práce je přehledně popsat jednotlivé části týkající se technologie Network Intelligence. Práce se věnuje problematice zachycení paketů, hloubkové inspekci paketů a Business Intelligence. V rámci literární rešerše je jednotlivě popsána každá technologie. V empirické části jsou tyto poznatky využity k tvorbě návrhu multidimenzionálního modelu.

V teoretické části jsou nejprve vysvětleny základní definice Network Intelligence. Pro tvorbu kritické rešerše jsou použity obecné vědecké metody jako analýza a syntéza. Popsány jsou jednotlivé komponenty Network Intelligence, tzv. hloubková inspekce paketů, zachycení paketů a Business Intelligence. V empirické studii jsou použity metody pro tvorbu sledovaných ukazatelů (podle Poura, 2012) a metody pro návrh multidimenzionálních databází (Novotný, 2005).

Empirická část popisuje postupnou tvorbu návrhu multidimenzionálního modelu, jehož výsledkem je konceptuální, logický a fyzický model. Následně je z tohoto modelu vytvořen analytický výstup. Nejprve je provedeno odchycení paketů v programu WireShark 1.12.4. a export balíku paketů do souboru .csv čtivého pro dále navržený model. Ve druhé části je vytvořen multidimenzionální model. Nejprve je vytvořen návrh dimenzí a ukazatelů, dále návrh charakteristik jednotlivých atributů dimenzionálních a faktových tabulek, identifikace vazeb mezi těmito tabulkami a poté návrh multidimenzionálního modelu z konceptuálního schématu a logického schématu. Schéma modelu je typu Hvězda, neboli každá dimenze je reprezentována právě jednou dimenzionální tabulkou. Jedná se o způsob, jak převést data z relační databáze do multidimenzionální struktury. Fyzické řešení multidimenzionálního pohledu na data je řešeno prostřednictvím programu MS PowerPivot. Jedná se o bezplatný doplněk k aplikaci tabulkového procesoru MS Excel pro tvorbu datových skladů a Business Intelligence a zobrazování dat. Z vytvořeného modelu je navržena kontingenční tabulka a nastaveny ukazatele. V konečné fázi je vytvořen jednoduchý report pro management podniku v nástroji PowerView, ve kterém je navržen analytický výstup (report).

ZÁVĚR

Diplomová práce se zabývala využitím a rozšířením technik Business Intelligence do IT sféry. Jejím cílem bylo pomocí znalostí získaných zpracováním odborné literatury zhotovit návrh multidimenzionálního modelu Network Intelligence, který není dosud v české literatuře zaveden. Cílem bylo zjistit, zda je možno Business Intelligence využít i v jiných částí sféry, než je dosud zatím využíváno. Bylo třeba pochopit odchytávání paketů, zpracování návrhů multidimenzionálních modelů a poté práci s nástrojem pro tvorbu Business Intelligence. Celá tato technika byla nazvaná jako Network Intelligence.

Zpracováním teoretické části byly vysvětleny základní pojmy týkající se počítačových sítí, odchytávání paketů, inspekce paketů a dosud využívaný pojem Network Intelligence. Dále byl charakterizován pojem Business Intelligence a postup tvorby multidimenzionálního modelu.

Na základě těchto zjištěných informací bylo v empirické části přistoupeno k návrhu aplikace Network Intelligence. V první části byl využit sniffovací program Wireshark pro odchycení paketů. Byl nainstalován na testovací počítač, který byl poté připojen na rozbočovač, ke kterému byly připojeny další počítače, ze kterých byla odchytávána jejich síťová komunikace. Vše bylo testováno v domácím prostředí, takže povolení k tomuto testu nebylo třeba získávat. Tato odchycená komunikace byla vyexportována do souboru .csv. V další části bylo přistoupeno k tvorbě multidimenzionálního modelu. Prvně bylo třeba navrhnout dimenze, ukazatele, jejich charakteristiky a tabulky faktů a dimenzí. Na základě tohoto bylo možno nastavit vazby mezi těmito tabulkami. Tvorba samotného multidimenzionálního modelu byla rozvržena do tří částí. V první bylo navrhnuto schéma konceptuálního modelu a následně konceptuální model podle metody STAR schéma. Ze STAR schéma byl dále navrhnut logický model, podle kterého byl dále navržen v programu PowerPivot fyzický model.

Z vytvořeného modelu byly navrženy kontingenční tabulky a nastavené ukazatele pro součet a průměr zatížení sítě. Na základě těchto vytvořených částí bylo přistoupeno k vytvoření jednoduchého reportu pro management podniku v nástroji PowerView. Report informuje o jednotlivé komunikaci počítačů za dobu probíhaného sniffování. Z výsledků je patrné, že report informuje o celkové velikosti stažených paketů, o jejich počtu a o maximální velikosti staženého paketu do počítače.

Přínosem této práce je aplikace, která může pomoci v kontrole síťové komunikace ve firmě. Odpovídá na otázky, jako jsou např. - Který uživatel zbytečně přetěžuje síť?, O který konkrétní počítač se jedná?, V jakém oddělení se nachází? a V jakém čase bylo ke které službě přistupováno? Dále je tato aplikace vhodná k ověření, zda někdo neporušuje bezpečností předpisy firmy.

VYBRANÉ POUŽITÉ ZDROJE

ABELSON, Hal, LEDEEN, Ken a LEWIS, Chris. 2009. *Just Deliver the Packets, in: "Essays on Deep Packet Inspection", Ottawa.* [Online] 2009. http://dpi.priv.gc.ca/index.php/essays/ just-deliver-the-packets/).

ANDERSON, Nate. 2007. *Deep Packet Inspection meets 'Net neutrality, CALEA'.* [Online] 25. 7 2007. http://arstechnica.com/gadgets/2007/07/deep-packet-inspection-meets-net-neutrality/.

B., Naachiz. 2011. *Window7themes.* [Online] 11. 9 2011. http://windows7themes.net/en-us/enable-promiscuous-mode-manually-in-windows-7/.

BENDRATH, Ralf. 2009. *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection, Paper presented at the International Studies Annual Convention, New York City, 15-18 February 2009.* [Online] 16. 3 2009. http://userpage.fu-berlin.de/~bendrath/Paper_Ralf-Bendrath_DPI_v1-5.pdf.

BIGELOW, Stephen J. a ODOM, Wendell. 2004. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů.* Brno : Computer Press, 2004. str. 990. 80-251-0178-9.

CLIPART. *cz.clipart.* [Online] http://cz.clipart.me/premium-animals-wildlife/the-donkey-carries-a-large-bag-vector-152184.

CLOMBS, Gerald. *Wireshark.* [Online] https://www.wireshark.org/about.html.

DUBRAWSKY, Ido. 2003. *FireWall Evolution - Deep Packet Inspection.* [Online] 29. 7 2003. http://www.securityfocus.com/infocus/1716.

GÁLA, Libor, POUR, Jan a TOMAN, Prokop. 2006. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi, technologie informačních systémů, čízení a rozvoj podnikové informatiky.* Praha : Grada, 2006. str. 482. 80-247-1278-4.

LABERGE, Robert. 2012. *Datové sklady: agilní metody a business intelligence.* Brno : Computer press, 2012. str. 350. ISBN 978-80-251-3729-1.

LACKO, Luboslav. 2005. *Business Intelligence v SQL Serveri 2005.* Praha : Microsoft, 2005. str. 103.

—. 2003. *Databáze: datové sklady, analýza OLAP a dolování dat s příklady v Microsoft SQL Serveru a Oracle.* Brno : Computer press, 2003. str. 486. ISBN 80-722-6969-0.

—. 2009. *Deep packet inspection engie goes open source.* [Online] 9. 9 2009. http://arstechnica.com/ open-source/news/2009/09/deep-packet-inspection-engine-goes-open-source.ars.

NOVOTNÝ, Ota, POUR, Jan a SLÁNSKÝ, David. 2005. *Business Intelligence: Jak využít bohatství ve vašich datech.* Praha : Grada Publishing, 2005. ISBN 80-247-1094-3.

ODOM, Wendell. 2005. *Počítačové sítě bez předchozích znalostí.* Brno : CP Books, 2005. str. 383. 80-251-0538-5.

OREBAUGH, Angela, a další. 2005. *Wireshark a Ethereal - Kompletní průvodce analýzou a diagnostikou sítí.* Brno : Computer Press, a.s., 2005. 978-80-251-2018-4.

P.V.A.Systems. 2010. *Pvasystems.* [Online] 2010. http://www.pvasystems.cz/cz/datovy-sklad-olap-business-inteligence/.

PARTRIDGE, Brian. 2010. *Network Intelligence is Key to Profiting from Anywhere Demand.* [Online] 17. 5 2010. http://www.yankeegroup.com/ResearchDocument.do?id=53513.

PORTER, Thomas. 2005. *The Perils of Deep Packet Inspection.* [Online] 1. 11 2005. www.securityfocus.com/infocus/1817.

POUR, Jan, MARYŠKA, Miloš a NOVOTNÝ, Ota. 2012. *Business intelligence v podnikové praxi.* Praha : Professional Publishing, 2012. str. 276. ISBN 978-80-7431-065-2.

REHBERGER, Ivo. 2002. *Lupa.cz.* [Online] 13. 02 2002. http://www.lupa.cz/clanky/kam-pakety-kam-jdete-aneb-odposlech-siti/.

RUSEK, Ondřej. Gymnázium Boženy Němcové v Hradci Králové. *www.gybon.cz.* [Online] http://www.gybon.cz/~rusek/vyuka/site/site003.html.

RUSELL, Jesse a COHN, Eonald. 2012. *Network intelligence.* USA : LENNEX Corp, 2012. 978-5-5121-5274-4.

SANDERS, Chris. 2012. *Analýza sítí a řešení problémů v programu Wireshark.* Brno : Computer Press, 2012. str. 288. 978-80-251-3718-5.

SHERRINGTON, Simon. 2010. *Deep Packet Inspection Semi-Annual Market Tracker.* [Online] 6 2010. http://www.heavyreading.com.

SCHWARTZ, Ephraim. 2008. *The dangers of cloud computing.* [Online] 7. 7 2008. http://www.infoworld.com/d/cloud-computing/dangers-cloud-computing-839.

SIENKIEWICZ, Henry. 2008. *DISA's Cloud Computing Initiatives.* [Online] 30. 4 2008. www.govinfosecurity.com/podcasts.php?podcastID=229.

SPURNÁ, Ivona. 2010. *Počítačové sítě.* Kralice na Hané : Computer Media, 2010. str. 180. 978-80-7402-036-0.

VIELER, Ric. 2007. *Professional Rootkits.* Indiapolis : Wiley Publishing, 2007. 978-0-470-10154-4.