EFEKTIVITA NÁSTROJŮ PRO ELIMINACI NEVYŽÁDANÝCH ZPRÁV

Alžběta Davidová[1]
[1]*Přírodovědecká fakulta,*
Ostravská univerzita v Ostravě, 30. dubna 22
701 03 Ostrava, 732114889, R09265@student.osu.cz

Abstrakt

Úvod

Rostoucí objem nevyžádané elektronické pošty a vývoj spamovacích nástrojů vyvolává nutnost přijmout opatření, jak doručování nevyžádaných zpráv zamezit. Tato práce se věnuje problematice filtrování nevyžádané elektronické pošty na úrovni poštovního serveru.

V současnosti nejsou dostupné nezávislé studie, které by zkoumaly reálnou efektivitu nástrojů pro obsahovou kontrolu příchozích zpráv, či úspěšnost nasazení takovýchto opatření v kombinaci se systémy implementujícími principy greylistingu.

Cílem práce je prostudovat principy a nástroje pro eliminaci nevyžádané pošty, které jsou v současné době využívány na poštovních serverech Ostravské univerzity, a analyzovat vývoj jejich účinnosti v delší časové řadě, s důrazem na systém filtrování nevyžádaných zpráv pomocí obsahové kontroly.

Metody

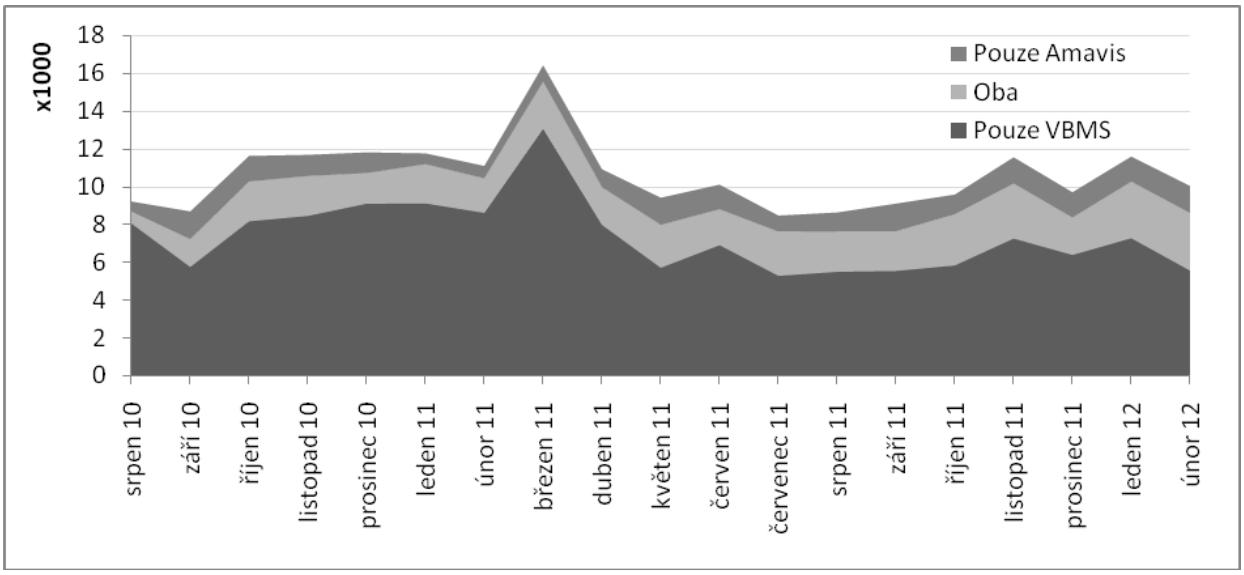
Součástí práce bylo vytvoření aplikace, která načítá a zpracovává logy programů zajišťujících obsahovou kontrolu příchozích zpráv. Aplikace pak záznamy extrahované z logů ukládá do databáze. Pro realizaci aplikace byl využit .NET Framework 4 a jako systém řízení báze dat pak Microsoft SQL Server 2008 R2 Express Edition. Takto získaná data byla podrobena statistické analýze, která se zaměřila n a prozkoumání dlouhodobých trendů v počtu a struktuře odhaleného spamu. Pro statistickou analýzu byl využit tabulkový procesor Microsoft Excel a statistický nástroj NCSS 2007.

Výsledky

Počet nevyžádaných zpráv odhalených obsahovou kontrolou dosahuje stabilně velmi nízkých hodnot, v řádech jednotek procent celkového objemu zpracovaných zpráv.

Bylo zjištěno, že systém Amavis má jen minimální podíl na celkovém množství nevyžádaných zpráv odhalených obsahovou kontrolou. Blíže podíl jednotlivých systémů na počtu odhalených nevyžádaných elektronických zpráv ilustruje obrázek 1. Průměrně je pouze systémem Amavis označeno za nevyžádanou poštu 10,8 % zpráv z celkového objemu spamu zachyceného obsahovou kontrolou.

Z dat byly také vypočteny odhady, kolik zpráv by mohlo být odhaleno ještě před doručením na server, pokud by byl nasazen skript pro mazání IP adres z automatického whitelistu, u kterého existovalo podezření, že právě přes něj dochází k propouštění většího množství nevyžádané pošty. U systému VBMS dosahoval podíl takto eliminovaných zpráv průměrně 33 %, u systému Amavis pak 32,5 %.



Obrázek 1 – srovnání podílu odhaleného spamu mezi systémy VBMS a Amavis

Diskuze

Ze získaných dat jsem zjistila, že účinnost v současnosti používaných systémů lze považovat za stabilní. Z dat získaných ze systému Postgrey, jenž aplikuje principy greylistingu, bylo stanoveno, že se nepotvrdily obavy, které provázely nasazení tohoto systému, tj. obavy, že tento jednoduchý princip bude v budoucnu masovými producenty spamu ve velkém obcházen.

Ze srovnání obou systémů obsahové kontroly vyplynulo, že jeden z nich, původem slovinský Amavis, vykazuje několika-násobně nižší účinnost, a to pravděpodobně z důvodu špatné konfigurace učení bayesovských filtrů.

Z vypracovaných odhadů účinnosti jednoho z plánovaných opatření – skriptu pro mazání záznamů z automatického whitelistu – vyplynulo, že toto opatření může v budoucnu dopomoci odhalit až třetinu spamu, který byl doposud odhalen obsahovou kontrolou, již před přijetím těchto zpráv na server, a to za relativně nízkých nároků na systémové zdroje. U obou systémů by mělo toto opatření pravděpodobně srovnatelnou účinnost. Navrhované opatření tedy vykazuje velký potenciál a mohlo by vést k významnému omezení nákladů na zpracování nevyžádaných zpráv.

Závěr

Cíle práce lze považovat za naplněné. Ukázalo se, že většina nevyžádaných zpráv je identifikována a blokována ještě před doručením na server, což lze považovat za úspěšné. Reálná efektivita systémů obsahové kontroly se ukázala být nevyrovnaná a jako účinnější se projevil systém VirusBuster.

Klíčová slova: *Spam, greylisting, e-mail, obsahová kontrola.*

Poděkování

Velice děkuji RNDr. Tomáši Sochorovi, CSc. za jeho cenné rady a výborné vedení při vytváření této práce. Také velmi děkuji Františku Zemanovi za pomoc se zpracováním části dat.