

Microsoft®
Exchange Server 2007

NASTAVENÍ ANTISPAMU
STRUČNÝ A NÁZORNÝ PRŮVODCE

Publikováno: červen 2009

Autor:

Miroslav Knotek - Microsoft MVP, IT Senior konzultant KPCS CZ, s.r.o.



Shrnutí: Průvodce obsahuje návod jak nastavit AntiSpam v Microsoft Exchange 2007. Návod je určen pro IT administratorům a partnerům společnosti Microsoft, kteří instalují Exchange 2007.

Upozornění

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user.

Obsah

1. Úvod	4
2. Podmínky pro využití antispamových funkcí	5
3. Filtrování dle připojení (Connection filtering).....	6
3.1. Konfigurace IP adres interních SMTP serverů	6
3.2. Konfigurace RBL (real-time block list)	6
3.3. Konfigurace IP Allow List	7
3.4. Služba Sender Reputation	7
4. Filtrování dle odesílatele (Sender filtering)	8
5. Filtrování dle příjemce (Recipient filtering)	9
6. Filtrování dle Sender ID (SenderID filtering)	9
7. Filtrování dle obsahu (Content filtering)	10
7.1. Nastavení akce	10
7.2. Konfigurace povolených a blokových slov	11
7.3. Specifikace výjimek pro konkrétní uživatele	11
7.4. Nastavení vlastního textu NDR při zamítnutí zprávy	11
8. Vybrané tipy pro optimalizaci antispamu.....	12
8.1. Premium Antispam	12
8.2. SafeList Aggregation	13
8.3. Individuální nastavení SCL akcí pro konkrétní schránku	13
8.4. Whitelisting domény nebo adresy odesílatele	13
9. Závěr	14
10. Dodatečné zdroje informací.....	15

1. Úvod

Microsoft Exchange Server 2007 obsahuje širokou škálu antispamových funkcí. Správným nastavením těchto technologií organizace všech velikostí získávají v rámci Exchange Serveru 2007 velmi mocný nástroj v boji s nevyžádanou poštou, což se odráží ve vyšší produktivitě práce uživatelů elektronické pošty. Cílem tohoto článku je popsat konfigurační kroky nutné pro optimální nastavení této antispamové ochrany.

2. Podmínky pro využití antispamových funkcí

Ochrana proti nevyžádané poště je rozdělena podle způsobu fungování do jednotlivých tzv. antispam agentů. Každý agent má své vlastní unikátní nastavení, každý antispamový agent může být také bez ohledu na stav ostatních agentů vypnut či naopak zapnut.

Antispamová agenti jsou ve výchozím nastavení automaticky instalováni pouze v rámci volitelné role Edge. Pokud v Exchange organizaci tato role chybí, je možné a podporované doinstalování agentů na serveru v roli Hub Transport pomocí následujícího postupu:

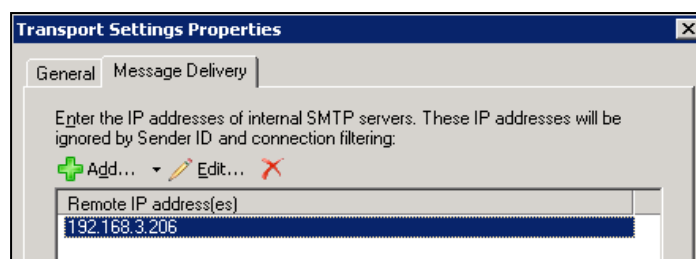
Přihlásíme se na Hub Transport server
Start -> Programy -> Microsoft Exchange Server 2007 -> Exchange Management Shell (EMS)
Spustíme příkaz Install-AntispamAgents.ps1
Provedeme restart služby "Microsoft Exchange Transport"

3. Filtrování dle připojení (Connection filtering)

Tento způsob ochrany je založen na důvěryhodnosti IP adresy serveru, který elektronickou poštu odesílá. Nastavení se skládá z následujících kroků:

3.1. Konfigurace IP adres interních SMTP serverů

V případě, že před Exchange serverem s instalovaným Connection filtering nebo Sender ID agentem existují další interní SMTP servery, je potřeba IP adresy těchto serverů uvést v EMC (Exchange Management Console): Organization Configuration -> Hub Transport -> Global Settings -> Transport Settings -> Message Delivery

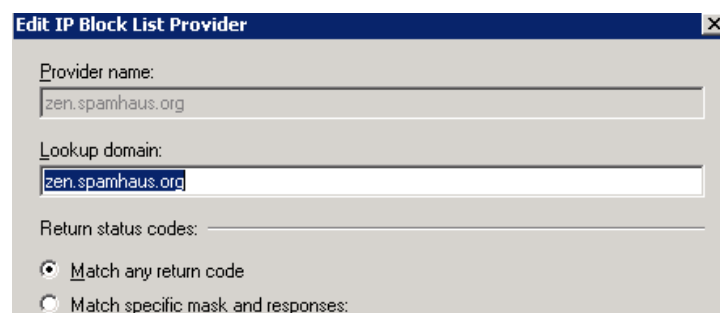


Obrázek 1 Konfigurace interních SMTP serverů

3.2. Konfigurace RBL (real-time block list)

Na Internetu existuje celá řada placených i neplacených služeb, které vedou evidenci důvěryhodných či naopak rizikových IP adres z hlediska rozesílání spamu. Tuto službu může náš Exchange Server dotazovat pro ověření IP adresy příchozího SMTP připojení. Je doporučeno vybrat 2-3 poskytovatele s vysokou reputací a garantovaným SLA. Pokud počet dotazů nepřesáhne 300 000 dotazů denně, je možné pro úvodní nastavení použít například široce využívaný RBL zen.spamhaus.org.

Vlastní nastavení pak provedeme v EMC: Organization Configuration -> Hub Transport -> Anti-Spam -> IP Block List Providers dle následujícího obrázku:

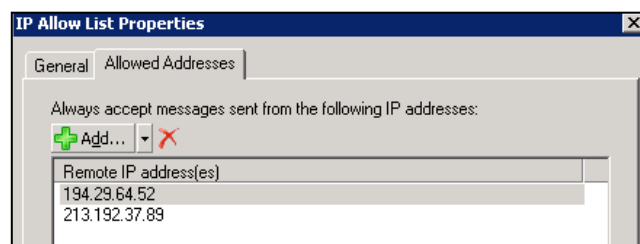


Obrázek 2 Nastavení RBL

3.3. Konfigurace IP Allow List

Pro snížení rizika zablokování pošty v případě, že se například obchodní partner ocitne se svým poštovním serverem na některém z RBL, je doporučeno IP adresy SMTP serverů klíčových partnerů přidat do IP allow listu dle následujícího návodu:

EMC: Server Configuration -> Hub transport -> ServerName -> Anti-spam -> IP Allow List



Obrázek 3 Konfigurace IP Allow List

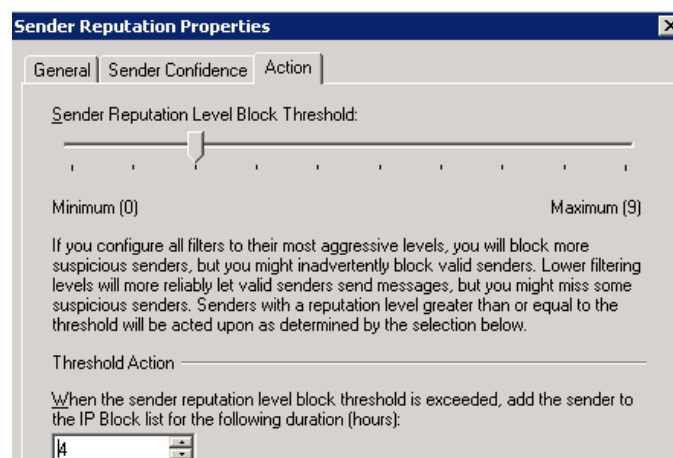
3.4. Služba Sender Reputation

Tato kontrola IP adres má 2 zdroje dat:

Pomocí MU/WSUS získáváme aktuální seznam IP a jejich reputací na základě dat ze služby Hotmail

Server vytváří vlastní hodnocení IP na základě průměrného SCL zpráv přijatých z této IP, sledování anomálií v rámci SMTP relace atd.

Můžeme nastavit jak hodně restriktivně se má tato ochrana chovat a na jak dlouho zablokovat IP adresu se špatnou reputací. Protože například freemaily mívají běžně vysoké průměrné SCL, doporučuji nastavit tento typ ochrany ze začátku málo restriktivně a blokovat IP třeba jen na 4h. Pokud je vše v pořádku, můžete zkusit postupné zpřísnění nastavení.



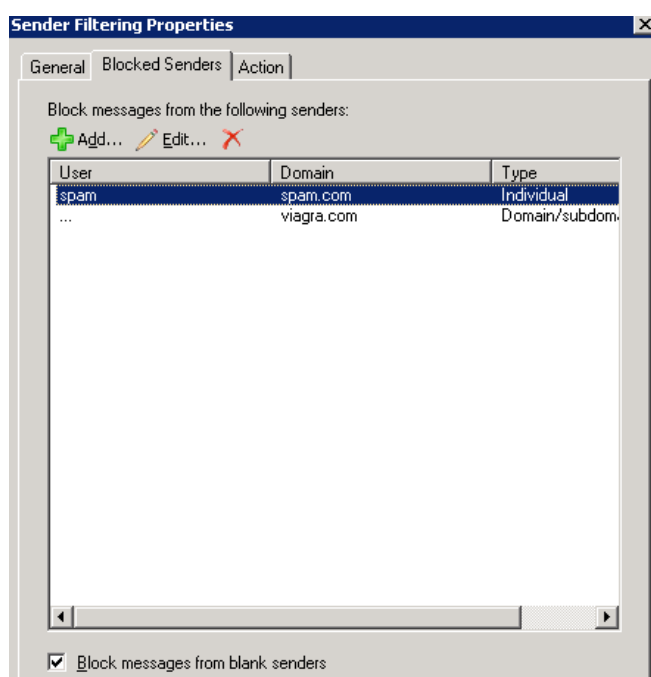
Obrázek 4 Nastavení Sender Reputation

4. Filtrování dle odesílatele (Sender filtering)

Tato ochrana je založena na testování e-mailové adresy odesílatele uvedené v hlavičce zprávy. Pokud chci globálně zakázat příjem zpráv z konkrétních e-mailových adres či celých domén, mohu je uvést zde:

EMC: Organization Configuration -> Hub transport -> Anti-spam -> Sender Filtering

Minimálně je doporučeno filtrovat zprávy, které nemají uvedenou adresu odesílatele vůbec.



Obrázek 5 Konfigurace Sender Filteringu

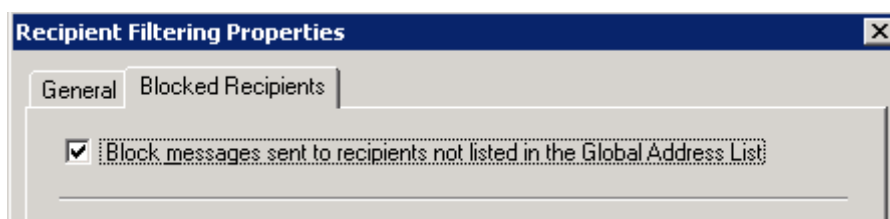
5. Filtrování dle příjemce (Recipient filtering)

Tato ochrana je založena na testování e-mailové adresy příjemce uvedené v hlavičce zprávy. Pokud je požadováno zakázat příjem zpráv z Internetu pro konkrétní e-mailové adresy interních uživatelů, mohou je uvést zde:

EMC: Organization Configuration -> Hub transport -> Antispam -> Recipient Filtering

Velmi důležitou volbou je zde "Block messages sent to recipients not listed in the Global Address List". Rozesílatelé spamu se totiž často pokouší posílat poštu na sice existující doménu, ale neexistující e-mailové adresy. Exchange server samozřejmě takovou zprávu nedoručí, ale přesto je jejím zpracováním zbytečně zatěžován včetně zodpovědnosti za odeslání NDR.

Řešením je kontrola existujících e-mailových adres ještě před vlastním přijetím zprávy. Tuto volbu tedy rozhodně nastavíme.



Obrázek 6 Blokování zpráv na neexistující adresy

6. Filtrování dle Sender ID (SenderID filtering)

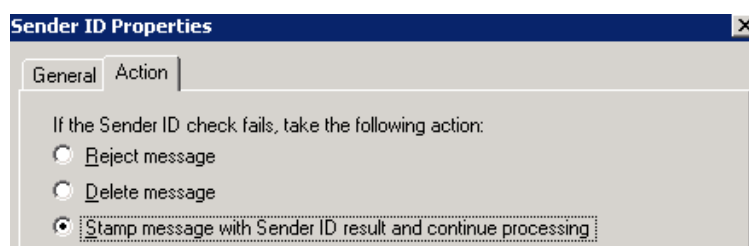
Sender ID filtering kontroluje odchozí IP adresu SMTP serveru oproti seznamu schválených IP adres pro odesílání v doméně odesílatele. Tyto adresy jsou volitelně zveřejněny v DNS pomocí tzv. Sender ID TXT záznamu.

Pokud se zjistí, že e-mail je odeslán z neautorizované IP adresy, jedná se s vysokou pravděpodobností o nevyžádanou poštu a mohou s ní tak provést dvě akce:

Odmítnout (není doporučeno)

Smazat (není doporučeno)

Označit a znevýhodnit v rámci content filteringu a výsledného skóre SCL



Obrázek 7 Nastavení reakce na Sender ID kontrolu

7. Filtrování dle obsahu (Content filtering)

Filtrování dle vlastního obsahu zprávy je velmi důležitou součástí ochrany proti nevyžádané poště. Pokročilý algoritmus se snaží ohodnotit na základě rozpoznávaných charakteristických znaků nevyžádané pošty nebo známých spamových kampaní číslem SCL (Spam Confidence Level) pravděpodobnost toho, zda se jedná o korektní e-mailovou zprávu či naopak spam. SCL = 0 znamená korektní zprávu, SCL = 9 naopak značí v podstatě 100% pravděpodobnost, že se jedná o zprávu nevyžádanou.

Správce pak pro jednotlivé úrovně SCL určuje akci, která se má provést. Na výběr je z následujících možností:

- Zprávu smazat bez NDR
- Zprávu odmítnout
- Zprávu umístit do karantény
- Zprávu doručit uživateli, ale do zvláštní složky „Nevyžádaná pošta“

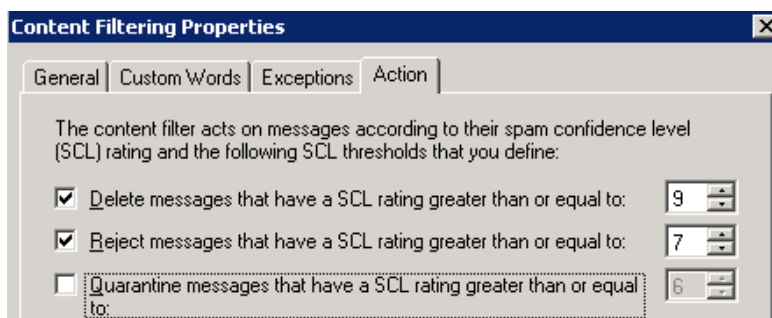
7.1. Nastavení akce

Dle praktických zkušeností je pro většinu firem nejvýhodnější následující seznam akcí, které uvádím včetně doporučených úrovní SCL:

- Zprávu smazat bez NDR – SCL = 9
- Zprávu odmítnout – SCL = 7, 8
- Zprávu doručit uživateli, ale do zvláštní složky „Nevyžádaná pošta“ – SCL = 4, 5, 6

Karanténu je doporučeno nepoužívat, pokud to není nezbytně nutné. Používání karantény totiž značně zatěžuje správce systému údržbou karanténní schránky, kterou je nutné pravidelně kontrolovat a také čistit.

První dvě akce nastavíme v EMC: Organization Configuration -> Hub transport -> Anti-spam -> Content Filtering.



Obrázek 8 Reakce filtrování obsahu dle SCL

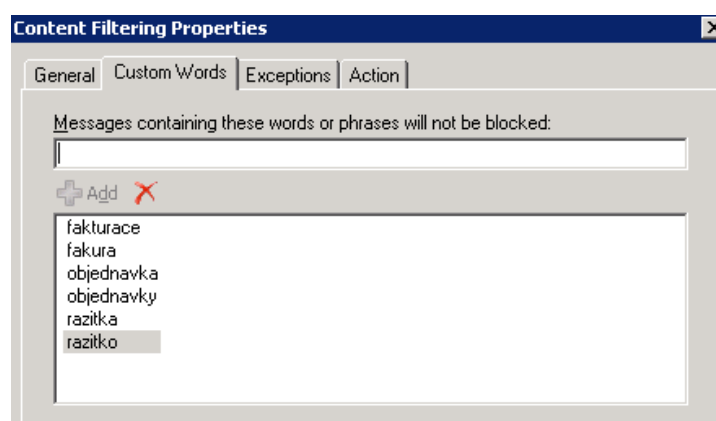
SCL pro doručování do složky Nevyžádaná pošta se pak nastavuje pomocí EMS příkazem:
Set-OrganizationConfig -SCLJunkThreshold 4

7.2. Konfigurace povolených a blokových slov

Pomocí nastavení povolených slov je možné dramaticky snížit tzv. false-positive (chybné zablokování korektní zprávy). Každá organizace by se měla zamyslet s ohledem na její předmět podnikání a vydefinovat si často používaná povolená slova. Pro firmu prodávající razítka to může být: razítko, razítka, objednávka atp.

Pokud je ve zprávě nalezené povolené slovo, SCL je automaticky nastaveno na hodnotu 0. Naopak pokud zpráva obsahuje blokové slovo, SCL bude stanoveno na úrovni 9.

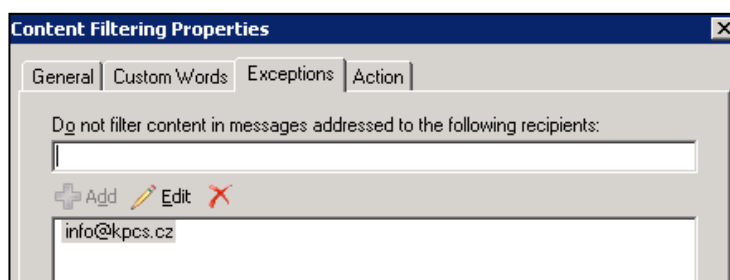
Vše nastavíme v EMC: Organization Configuration -> Hub transport -> Antispam -> Content Filtering -> Custom Words



Obrázek 9 Určení povolených slov

7.3. Specifikace výjimek pro konkrétní uživatele

V případě potřeby mohou také nastavit seznam příjemců pošty, pro které se bude filtrování obsahu zcela ignorovat.



Obrázek 10 Výjimky pro filtrování obsahu

7.4. Nastavení vlastního textu NDR při zamítnutí zprávy

Zajímavou možností je také nastavení vlastního textu pro NDR, který se posílá odesílateli při zamítnutí na základě obsahu. Vlastní text nastavíme pomocí EMS příkazem:

```
Set-ContentFilterConfig -RejectionResponse "Zprava byla vyhodnocena díky svemu obsahu jako spam"
```

8. Vybrané tipy pro optimalizaci antispamu

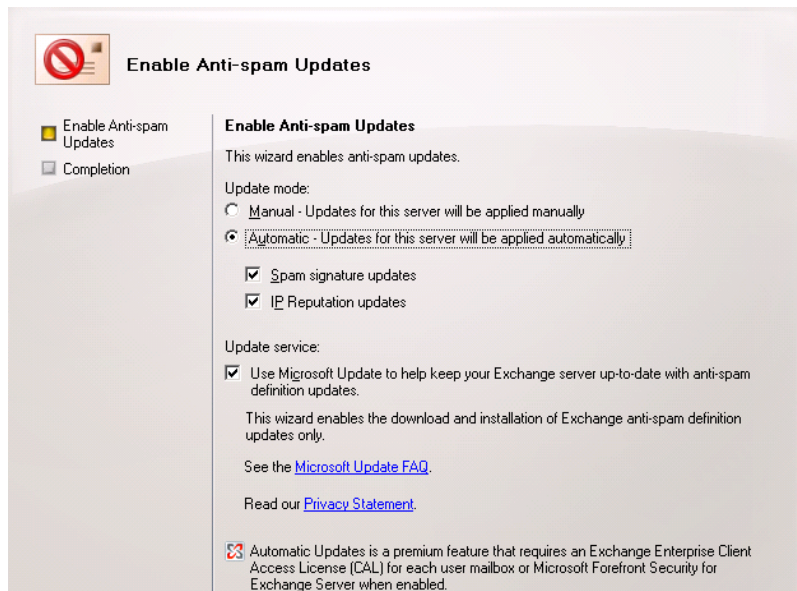
V předcházejících kapitolkách jsme popsali základní nastavení antispamu, které je nutné provést víceméně vždy. V závěrečné části se zaměříme na rozšiřující nastavení, která nám pomohou využít všechny výhody Exchange 2007 antispamu opravdu na maximum.

8.1. Premium Antispam

Pokud má firma k dispozici pro své uživatele Exchange Enterprise CAL nebo Forefront Security for Exchange Server, může využívat tzv. Premium Antispam, což zahrnuje následující výhody:

- Denní aktualizace IMF content filteru (standardně jen 1x za 14 dní)
- Několikrát denně IP reputation aktualizace
- Několikrát denně aktualizace spamových kampaní

Jak premium antispam zapnout? V EMC najdeme v sekci Server Configuration -> Hub transport -> ServerName příkaz kontextového menu: Enable Anti-spam Updates. Dále nás již vede průvodce viz obrázek.



Obrázek 11 Aktivace Premium antispamu

8.2. SafeList Aggregation

Uživatel rozhraní Outlook Web Acces či MS Outlook má možnost vytvořit si seznamy důvěryhodných odesílatelů (Safe Senders). Klient pak zprávy z těchto adres uživateli doručí vždy přímo do Doručené pošty. Ve výchozím nastavení se tím ale řídí pouze klient a nikoliv serverový antispam. Nastavením funkce SafeList Aggregation ale dojde k vy publikování seznamu bezpečných odesílatelů do Active Directory a odtud si je načítá i serverový antispam.

Jako uživatel tak mám možnost razantně ovlivňovat, jaké zprávy dojdou do Doručené pošty a jaké ne. Důležité je také vysvětlit, že bezpeční odesílatelé Uživatele A nejsou bezpečnými odesílateli pro uživatele B.

Postup pro nastavení je v kostce následující (přesný postup je [zde](#)):

```
Vytvoříme dávku např. Safelist.bat s příkazem "d:\Program Files\Microsoft
Command Shell\v1.0\Powershell.exe" -psconsolefile "d:\Program
Files\Microsoft\Exchange Server\bin\exshell.psc1" -command "get-mailbox |
where {$_.RecipientType -eq
[Microsoft.Exchange.Data.Directory.Recipient.RecipientType]::UserMailbox } |
update-safelist"
Dávku budeme pomocí plánovače úloh spouštět ideálně 1x denně
```

8.3. Individuální nastavení SCL akcí pro konkrétní schránku

V některých případech je požadováno nastavit jiné hranice SCL pro určené schránky. Nejen, že to je možné, ale dokonce můžeme pro konkrétního uživatele i jednotlivé typy filtrování zapnout/vypnout. Nastavení se provádí výhradně pomocí EMS. Uvedeme si 2 příklady:

```
Set-mailbox id "Miroslav Knotek" -SCLRejectEnabled $false -
SCLQuarantineEnabled $false -SCLDeleteEnabled $false - žádná zpráva pro
Miroslava Knotka nebude ani smazána, ani odmítnuta ani předána do karantény
Set-mailbox id "Miroslav Knotek" -SCLRejectThreshold 5 - zprávy pro Miroslava
Knotka se budou odmítat již proSCL = 5
```

8.4. Whitelisting domény nebo adresy odesílatele

Pokud chci vynechat z filtrování obsahu konkrétní e-mailové adresy odesílatele či celé domény, mohu toto nastavit v EMS pomocí příkazů

```
Set-contentfilterconfig -BypassedSenderDomains microsoft.com
Set-contentfilterconfig -BypassedSenders knotek@kpcs.cz
```

9. Závěr

Antispam v rámci Exchange 2007 je opravdu jeho vysoce výkonnou a spolehlivou součástí. Je však nutné alespoň základně porozumět principům fungování a vědět co, kdy, kde a jak správně nastavit. Věřím, že se v tomto článku podařilo antispam funkcionalitu a kroky pro nastavení alespoň stručně popsat a tak nasazení bude nyní pro každého již snadnou záležitostí.

10. Dodatečné zdroje informací

Technické odkazy:

Exchange server Community (anglicky)

<http://technet.microsoft.com/en-us/exchange/bb341336.aspx>

TechNet Webcast: Protecting Your Exchange Server 2007 Network from Viruses and Spam (Level 300) (anglicky)

<http://www.microsoft.com/events/series/tnexchangeserver.aspx?tab=Webcasts&seriesid=21&webcastid=2073>

Webové stránky Technet (anglicky)

<http://technet.microsoft.com/en-us/exchange/default.aspx>

Webové stránky Exchange (česky):

<http://www.microsoft.com/cze/servers/exchange/default.mspx>

Další odkazy:

Webové stránky o konceptu Sjednocené komunikace (česky)

www.microsoft.cz/uc

Webové stránky podnikových řešení (česky)

www.microsoft.com/cze/podnikovareseni

Microsoft[®]
Exchange Server 2007
