Você sabe o que é um registro SPF?

Não?

Nem eu, até que os usuários do meu site começaram a não receber os e-mails com suas senhas e respostas do fórum. O fato é que já havia algum tempo que usuários do Hotmail.com, Msn.com e Live.com não recebiam os e-mails de meu site, nem mesmo em suas caixas de spam, estes e-mails simplesmente sumiam, ou melhor, eram deletados sem qualquer aviso pelos filtros da Microsoft.
No início desta semana comecei a receber e-mails devolvidos pelo Hotmail.com, Msn.com e Live.com com mensagens de erro semelhantes a “550 SC-001 Mail rejected by Windows Live Hotmail for policy reasons...” e então tive de correr para encontrar uma solução. Para resumir, eles estavam classificando meus e-mails como prováveis SPAMs.
Se você ler sobre este assunto aqui poderá salvar-se de perder vários dias de sua vida em pesquisas e testes para tentar implementar uma solução para este problema.

Todos sabemos o stress de fazer a triagem de e-mails entre bons e spam, e temos de agradecer às pessoas que trabalham em soluções para filtrar ou simplesmente estancar este problema. No entanto, tenho a certeza que você vai entender o meu incômodo ao descobrir que, graças à configuração do meu servidor, fui classificado como "spammer" pela Microsoft e como resultado eles parecem mandar para um buraco negro qualquer e-mail enviado para uma conta do Hotmail.com, Msn.com ou Live.com a partir do meu servidor.

Antes de continuar gostaria apenas de esclarecer que isto de fato nada tem a ver com o servidor como um produto ou serviço, mas sim com a maneira pela qual um ambiente de servidor virtual funciona. Há dezenas de referências encontradas através do Google de pessoas reclamando dos mesmos problemas, e curiosamente vêem-se mais referências a pessoas rodando em ambientes VPS (Virtual Private Server) e utilizando Plesk. No meu caso específico uso cPanel/WHM em um servidor compartilhado.

Como ocorre com todas as coisas, quando algo dá errado, você tem que aprender como ela funciona para poder corrigi-la, e assim eu tive de aprender muito sobre as entradas e saidas do funcionamento de servidores de correio e do sistema de DNS.

Isenção de responsabilidade: Neste momento gostaria apenas de dizer que eu tenho uma idéia muito básica de como isto funciona, por isso não tome nenhuma destas informações como um evangelho, mas sim use-as como um guia e referência para onde você pode encontrar ajuda adicional.

Onde está indo o meu e-mail!?

Depois de entrar em contato com o suporte do meu provedor, decidi que eu precisava descobrir para onde os meus e-mails estavam indo. Eu não estava recebendo um retorno dos servidores de correio do Hotmail.com, Msn.com ou Live.com e o meu programa de envio de e-mails (Outlook Express, Windows Live Mail, etc.) dizia-me que o e-mail foi entregue. Felizmente, no meu caso, no início desta semana recebi alguns e-mails de retorno dos servidores de correio do Hotmail.com, Msn.com e Live.com indicando os prováveis motivos pelos quais os e-mails não estavam sendo aceitos. Abaixo temos um exemplo das mensagens que recebi:

" ...
e-mail_destino@hotmail.com
SMTP error from remote mail server after MAIL FROM:<e-mail_origem@meudominio.com.br> SIZE=2269:
host mx2.hotmail.com [65.54.244.40]: 550 SC-001 Mail rejected by Windows Live Hotmail for policy reasons. Reasons for rejection may be related to content with spam-like characteristics or IP/domain reputation problems. If you are not an email/network admin please contact your E-mail/Internet Service Provider for help. Email/network admins, please visit http://postmaster.live.com for email delivery information and support
------ This is a copy of the message, including all the headers. ------
... "

Alguns provedores permitem que você se aprofunde no sistema operacional para ver o que está acontecendo fora, assim você pode tentar pesquisar os registros do servidor SMTP para ver o que se passa fora. Alguns usuários do Plesk cujo servidor SMTP é o Qmail relataram que conseguiram localizar registros como o a seguir:

Mar 22 17:32:23 as qmail: 1174584743.517414 delivery 437: success: 65.54.244.168_accepted_message./Remote_host_said:_250_ <4602BEEF.1080905@helloian.com>_Queued_mail_for_delivery/

Assim parece que os servidores do Hotmail.com, Msn.com e Live.com estão aceitando os e-mails, colocando-os na fila, mas nunca realmente entregando-os, devido à sua tecnologia filtragem de spam. Uma rápida pesquisa no Google mostrou que muita gente parece ter experimentado ou ainda continua experimentando o mesmo problema.
Percebi que haviam poucos comentários sobre soluções concretas, e menos ainda em português, mas muitas referências à sigla SPF, assim como em http://postmaster.live.com , e mais específicamente nas diretrizes do Hotmail.com, Msn.com e Live.com em http://postmaster.live.com/Guidelines.aspx
, por isso, decidi que valia a pena pesquisar mais, testar e então escrever este artigo.

O Sender Policy Framework (SPF)

O Sender Policy Framework permite a um proprietário de domínio especificar quais máquinas têm permissão para enviar e-mails em seu nome. Este tipo de mecanismo, infelizmente, não está presente no Simple Mail Transfer Protocol (SMTP), um fato que permite que aos spammers enviar e-mail de endereços forjados de forma relativamente fácil, uma vez que não existe inerente validação quando um e-mail é enviado e recebido em seguida.

Felizmente a solução é relativamente simples de implementar. O registro SPF é aplicado como uma entrada do tipo TXT no registro DNS do domínio, e é simples como isto. Agora, quando você envia um e-mail, o servidor de correio que o recebe pode usar este registro SPF para verificar se a origem do e-mail é legítima. Para ajudar a ilustrar o que está acontecendo temos a seguir um cabeçalho MIME de um e-mail que meu site enviou a partir do meu servidor (modifiquei os nomes por segurança) que permite um exemplo bem mais complexo.

Return-path: <email_origem@meudominio.com.br>
Received: from [174.132.122.200] (helo=www.meudominioprincipal.com.br)
by meu.webserver.com with esmtpa (Exim 4.69)
(envelope-from <email_origem@meudominio.com.br>)
id 1Kjzam-0007rD-KQ
for email_destino@hotmail.com; Sun, 28 Sep 2008 11:57:56 -0500
Date: Sun, 28 Sep 2008 11:57:56 -0500
To: email_destino@hotmail.com
From: Meu - Website <email_origem@meudominio.com.br>
Subject: Detalhes da conta
Message-ID: <2281561eae5280cc531577b47b669e53@www.meudominio.com.br>
X-Priority: 3
X-Mailer: PHPMailer [version 1.73]
MIME-Version: 1.0
Content-Transfer-Encoding: 8bit
Content-Type: text/plain; charset="iso-8859-1"

A explicação para este cabeçalho acima ter três (3) domínios envolvidos é que “meudominio.com.br” é um domínio estacionado junto a “meudominioprincipal.com.br”, que é meu domínio principal, e que por sua vez está hospedado em um servidor compartilhado cujo domínio é “meu.webserver.com”.

A confusão surge quando a máquina receptora lê que o e-mail alega ser do domínio “meudominio.com.br”, mas foi enviado pelo servidor de IP 174.132.122.200, o qual aponta para o domínio “meudominioprincipal.com.br”, através do servidor “meu.webserver.com” (IP 74.32.122.200). Tanto quanto a máquina, não há nenhuma ligação entre o remetente alegado no e-mail, a máquina que o originou e a que realmente enviou o e-mail. Não há nenhuma maneira de saber se esta informação é legítima ou não.

Minhas pesquisas iniciais no Google pareciam mostrar que na maioria são usuários de VPSs com vários domínios que haviam sido atingidos por este problema. Isso porque por sua própria natureza, um servidor VPS rodando múltiplos domínios (por exemplo, “meudominio.com.br”) irá enviar e-mails pelo servidor de correio de um determinado domínio (no meu caso “meudominioprincipal.com.br”), através do servidor SMTP do hospedeiro da plataforma VPS (“meu.webserver.com” no meu caso). Infelizmente e-mails enviados usando essa configuração são muito semelhantes à mensagens de “SPAM” e o filtro de spam do Hotmail.com, Msn.com e Live.com (conhecido como “SmartScreen”) é rápido em dar o próximo passo enviando os e-mails para um buraco negro, significando que eles nunca chegam a seu destino, apesar do servidor do Hotmail.com, Msn.com e Live.com notificar o remetente de que os e-mails foram recebidos e entregues.

Felizmente é aqui onde o registro SPF entra para tornar estas questões mais claras. O registro SPF narra à máquina receptora que o servidor “meu.webserver.com” envia e-mails em nome do servidor de correio do domínio “meudominioprincipal.com.br” e que este, por sua vez, envia e-mails em nome do servidor de correio do domínio “meudominio.com.br”. Este registro SPF é escrito como mostrado a seguir:

meudominio.com.br. IN TXT “v=spf1 a mx ip4:74.32.122.200 ip4:174.132.122.200 a:meu.webserver.com include:meudominioprincipal.com.br -all”

O registro SPF em si é a parte entre aspas e ele pode ser explicado da seguinte forma:

v=spf1 Isso identifica o registro TXT como uma string SPF.

a Esta opção indica que os endereços listados nas entradas A do DNS deste domínio estão autorizadas a enviar e-mails em seu nome. No meu caso o endereço IP de “meudominio.com.br” é 174.132.122.200 (mesmo IP de “meudominioprincipal.com.br”) e está listado nas entradas A do DNS de “meudominio.com.br”, estando autorizado a enviar e-mails.

Ip4:74.32.122.200 Esta opção indica que o endereço IP 74.32.122.200 tem permissão para enviar e-mails em nome de “meudominio.com.br”. Este é o endereço IP do servidor onde meus domínios estão hospedados e assim é através do servidor SMTP deste servidor que meus e-mails são enviados.

Ip4:174.132.122.200 Esta opção indica que o endereço IP 174.132.122.200 pertencente a “meudominioprincipal.com.br” também tem permissão para enviar e-mails em nome de “meudominio.com.br”. Nos testes esta opção se mostrou necessária para envio de e-mails para provedores como o UOL e o BOL apesar de “meudominioprincipal.com.br” já estar especificado na opção “include”.

a:meu.webserver.com Esta opção, neste caso, é similar a descrição do IP4 acima com a diferença de que se refere a um domínio o qual também possui permissão para enviar e-mails de “meudominio.com.br”. Na realidade, tecnicamente esta opção nem seria necessária porque este domínio “meu.webserver.com” possui o endereço IP 74.32.122.200 que já foi autorizado acima na opção IP4, contudo é interessante acrescentá-la pois alguns VPS's hospedados em datacenters não possuem um DNS reverso (rDNS) correto e assim o IP 74.32.122.200 não aponta para o domínio “meu.webserver.com” podendo causar problemas também.

include:meudominioprincipal.com.br Esta opção faz com que o teste seja reiniciado usando o domínio incluído, no caso "meudominioprincipal.com.br", no lugar do domínio do remetente.

-all Esta opção indica que nenhum outro servidor possui permissão ou deve enviar e-mails em nome de “meudominio.com.br” e caso isso ocorra deve ser devolvida uma mensagem de erro ao endereço de e-mail de retorno.

Este é um bom padrão para os sites particularmente preocupados com as fraudes e falsificações de modo que este registro SPF deve ser inserido nas entradas DNS de cada domínio, seja por você ou por seu provedor de hospedagem.

Um assistente bastante interessante e que me ajudou bastante a compreender como isso tudo funcionaria em meus domínios pode ser encontrado em http://www.spfwizard.com (em inglês).

O website do Open SPF (http://www.openspf.org) explica os dados acima com mais detalhes e também oferece uma ferramenta para ajudá-lo a criar seu registro SPF. A Microsoft também tem disponível uma ferramenta semelhante no endereço http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard , porém apesar de ter sido referida pelo suporte técnico do Hotmail.com, Msn.com e Live.com, revelou-se mais um entrave do que uma ajuda pois ela e muitas outras referências recomendam que um mecanismo PTR seja incluído no registro SPF. O registro PTR permite a pesquisa inversa de um endereço IP, que é identificar o domínio de um endereço IP. A pesquisa reversa é usada para verificar se o nome de domínio e o endereço IP no cabeçalho MIME do e-mail se correlacionam realmente e que não tenham sido falsificados. Embora isto soe como uma boa idéia, na realidade, uma pesquisa inversa toma uma quantidade considerável de tempo e não é geralmente um método empregado por grandes provedores de e-mail como o Hotmail.com, Msn.com ou Live.com. Descobri que na verdade o Hotmail.com, Msn.com e Live.com podem recusar seu registro SPF justamente por incluir este mecanismo PTR. Cito o prório suporte técnico do Hotmail.com, Msn.com e Live.com:

"... A especificação para registros SPF (RFC 4408) desencoraja o uso do "ptr" por razões de desempenho e confiabilidade. Isto é especialmente importante para o Windows Live Mail, para o Hotmail e para outros grandes provedores como resultado do volume muito grande de e-mails que recebemos diariamente. É altamente recomendável que você remova o mecanismo "ptr" de seu registro SPF e, se necessário, substitua-o por outros mecanismos SPF que não requeiram uma pesquisa de DNS inversa, como "a", "mx", "ip4" e "include" ..."

Solução de problemas

Feita inserção do registro SPF nas entradas DNS de seus domínios é hora de preencher um formulário informando aos servidores do Hotmail.com, Msn.com e Live.com alguns dados em https://support.msn.com/eform.aspx?productKey=edfsmsbl&mkt=pt-br
.
Após preencha também o formulário do SenderID da Microsoft disponível em https://support.msn.com/eform.aspx?productKey=senderid&mkt=en-us
(em inglês) e informe seus domínios para que sejam inseridos na base de dados da Microsoft.
Neste ponto, caso necessite de ajuda, contate seu provedor de hospedagem o qual terá melhores condições de fornecer estes dados ou mesmo fazer este preenchimento.

A própria natureza do sistema DNS faz deste um problema muito frustrante de se enfrentar, porque você não vê resultados instantâneos, mas evidentemente tem que esperar até 48 horas para que as informações no DNS sejam propagadas pela internet.

A Microsoft também não ajuda muito pois após tudo cadastrado no SenderID você recebe um e-mail de confirmação com as informações abaixo reproduzidas parcialmente (em inglês):

"...
We have added your domains to the Sender ID program. This may take up to 2 business days to be fully replicated in our systems. If you have any questions regarding this please let me know.

If you should make any changes to your SPF record, you do not need to notify us when you make this or any revision to your SPF record since we will automatically pull the current record from the DNS daily.
..."

Este retorno informa que as alterações demorarão em torno de 2 dias úteis para entrar em

vigor nos servidores da Microsoft.
E, o mais importante, que qualquer alteração feita nos registros SPF não precisarão ser informadas a eles pois o sistema deles obtém automaticamente estes novos registros SPF do seu DNS diariamente, ou seja, depois de cadastrado lá se você alterar o seu registro SPF terá de esperar até o próximo dia para que veja algum resultado. Foi assim para mim.

Testando seu registro SPF

Você pode utilizar algumas das ferramentas para verificar se seu registro SPF está configurado corretamente, como as disponíveis em http://www.politemail.com/check-spf.aspx , http://www.kitterman.com/spf/validate.html
e em
http://www.openspf.org/Tools
.
Depois de ter confirmado que o seu registro está configurado corretamente você também pode enviar um e-mail em branco para check-auth@verifier.port25.com que irá testar o seu registro SPF e enviar de volta um e-mail com os resultados.
Também é interessante para testar sua configuração de DNS o intodns.com. Embora ele não verifique a funcionalidade do seu registro SPF, é uma ótima ferramenta para dar-lhe um retorno sobre quase todos os aspectos da sua configuração DNS e pode ser uma excelente ferramenta para a solução de problemas.

O SPF Funciona!

Finalmente posso mandar e-mails à utilizadores do Hotmail.com, Msn.com e Live.com sem me preocupar se ele vai passar, e se você estiver rodando um servidor ou configuração similar então eu sugiro fortemente que você use um registro SPF, mesmo se você não está tendo problemas no momento.
Meus e-mails atualmente estão sendo recebidos normalmente pelos usuários do Hotmail.com, Msn.com e Live.com sem que caiam na pasta de lixo/spam. Ah, não esqueçamos de Uol.com e Bol.com... lá também chegam meus e-mails apesar de eles serem bem rigorosos e de não responderem aos e-mails de pedido de ajuda e isso graças aos registros SPF.

Caso os passos acima não funcionem para você, entre em contato com seu provedor de

hospedagem e certifique-se de ter executado todos os testes mencionados. Há várias possíveis causas para que seus e-mails sejam recusados por algum provedor como, por exemplo, se seu servidor de e-mails estiver em uma lista negra. Verifique isto informando o IP de seu servidor em http://www.mxtoolbox.com/blacklists.aspx .

Infelizmente, no final, é necessário realmente compreender o que está errado, por isso sugiro-lhe familiarizar-se com a forma como o sistema DNS funciona. A Wikipédia possui um excelente artigo (http://en.wikipedia.org/wiki/Domain_name_system) que deve colocá-lo no caminho certo.

Você também encontrará fartas informações em português a repeito de spam, SPF, funcionamento de correio eletrônico e muitos outros assuntos no site http://www.antispam.br .

Registro SPF para usar Google APPs

Este ponto deste artigo está sendo adicionado após contato do leitor JC Lins que contribuiu com um link bastante interessante para quem usa o Google APPs pois mostra como configurar o registro SPF de modo que seus e-mails funcionem corretamente através deste serviço.

Basicamente basta incluir no registro SPF uma opção "include:aspmx.googlemail.com" e ao final do registro usar "~all" no lugar do "-all" para que os servidores do Google tenham autorização de envio dos e-mailsde seu domínio. Eles ressaltam que "*A publicação de um registro SPF sem* ***includ e:aspmx.googlemail.com*** *ou a especificação de* ***-all*** *, em vez de* ***~all*** *, pode resultar em problemas de entrega* ".

Você pode conferir a documentação completa a este respeito em http://www.google.com/support/a/bin/answer.py?hlrm=br&answer=33786 .

Fontes de pesquisa:

http://www.innovation-station.net/archives/2007/03/29/hotmail-and-my-spf-nightmare
http://www.openspf.org
http://www.spfwizard.com
http://www.forumcpanel.com.br/index.php?showtopic=1787
http://www.webhostingtalk.com/showthread.php?t=686676
http://support.msn.com
http://postmaster.live.com
http://www.antispam.br
http://www.google.com/support/a/bin/answer.py?hlrm=br&answer=33786