

Anti-Spam em um provedor Você X Clientes

Safe Defense
andre.ramoni@gmail.com
L - Series

André Guimarães
“Ramoni”

Encontro Nacional LinuxChix-BR 2007

Anti-Spam em um provedor

Você X Clientes

Administrar um servidor de email em um provedor:

- Ambientação
- Medidas anti-spam: focos e falsos positivos

Administrador X Usuários X Administrador

FIGHT !!!

Anti-Spam em um provedor

Você X Clientes

Realidade da Internet:

- Ambiente totalmente hostil
- Administradores que não protegem suas redes
- Administradores que montam servidores de email de qualquer jeito
- Muitos provedores facilitam o envio de spam
- Muitos administradores dizem: “Mas só pra você que eu não consigo enviar email”

Anti-Spam em um provedor

Você X Clientes

Necessidades dos clientes:

“Mas eu **preciso** receber esse email !!!”

- Não te pagam por uma solução de “segurança”
- Não querem receber spams nem vírus
- **Precisam** enviar e receber quaisquer tipos de arquivos anexados
- Precisam enviar e receber emails com links para arquivos
- Não querem usar anti-vírus nem antispam na estação
- Não querem mais receber emails de listas **que se cadastraram**
- **Não podem** deixar de receber emails “importantes”
- Querem que você resolva os problemas de destinatários externos

Anti-Spam em um provedor

Você X Clientes

Realidade dos clientes:

- Esquecem a senha
- Recebem emails duplicados
- Envia arquivos com dupla extensão
- Referenciam links para executáveis
- Escrevem assunto e corpo COM LETRAS MAIÚSCULAS
- Envia fotos em arquivo .doc em email vazio no formato HTML
- Erram o destinatário (ex: andré@yaho.com)
- Mensagens de erro: algum usuário lê ?
- Repassam spams
- Divulgam e cadastram seu email sem critérios

O administrador entende:

- “Não quero receber spams, mas quero enviar e receber spams”
- Percepção do cliente sobre spam: emails que ele não quer receber
- Percepção do administrador sobre spam: características

Anti-Spam em um provedor

Você X Clientes

Bloqueando "spam"

- MTA (Compliance – Sem falsos positivos (?))
 - Policy Enforcement – RFCs e BCPs (Best Current Practices)
 - Complexidade de customização
 - Sem buraco negro: erro reportado ao cliente MTA
 - Performance. Economia de recursos de processamento e banda
- Filtro de conteúdo
 - Anti-spam, anti-vírus, regras customizadas
 - Alto consumo de recursos
 - Controle total sobre o conteúdo do email
 - Flexibilidade de configuração
 - Regras customizadas de tamanho, anexos, whitelists e blacklists
 - Quarentena: buraco negro ?

Anti-Spam em um provedor

Você X Clientes

Evitando o envio de “spam”

- Adequação às boas práticas e RFCs
 - Existem normas para o email na Internet
 - Configuração correta do SMTP
 - Envio de email somente autenticado
- Rede
 - IP de saída do servidor SMTP ser exclusivo
 - Bloqueio de saída para porta 25/TCP quando possível

Anti-Spam em um provedor

Você X Clientes

Bloqueios no MTA IP reverso

Resolver IP => nome
Resolver IP => nome => IP

Prós:

- Usado por muitos provedores (terra, ig, uol, bol etc)

Problemas:

- Muitos provedores provém o registro PTR aos IPs dinâmicos
- Alguns administradores não configuram PTR

Anti-Spam em um provedor Você X Clientes

Bloqueios no MTA Validação do HELO/EHLO

Resolver hostname => IP origem => hostname

Prós:

- Interligação da administração do DNS e do email.

Problemas:

- Alguns administradores não configuram direito DNS e SMTP

Anti-Spam em um provedor

Você X Clientes

Bloqueios no MTA

Validação do domínio do remetente

Prós:

- Negar emails de domínios que não existem
- Negar emails de domínios que não possuem MX ou registro A

Problemas:

- Scripts automatizados [em ambientes] mal configurados

Anti-Spam em um provedor

Você X Clientes

Bloqueios no MTA Checagem de SPF

Autorização do cliente pelo domínio

Prós:

- Interligação da administração do DNS e do email.

Problemas:

- Alguns administradores podem configurar mal o SPF em um ambiente complexo
- Relays internos – filtros de email
- Encaminhamentos cross-domain

Anti-Spam em um provedor

Você X Clientes

Bloqueios no MTA
Checagem de DNSBLs

“Reputação” do IP

Prós:

- Listagem de IPs que comprovadamente mandam spam

Problemas:

- Algumas listas não oferecem bom mecanismo para de-listing
- Alguns administradores não tomam conta da sua rede
- Alguns administradores não procuram saber se estão em DNSBLs

Uso ideal:

- Checar 3 ou 4 DNSBLs
- Pesos diferentes de acordo com a DNSBL

Anti-Spam em um provedor

Você X Clientes

Bloqueios no MTA Validação do destinatário

Prós:

- Somente os emails que podem ser entregues entram na fila
- Evita consumo de recursos e geração de bounces

Problemas:

- ?

Anti-Spam em um provedor Você X Clientes

“Anti-spam do UOL”

Pedido de confirmação ao remetente

Prós:

- Remetentes precisam confirmar que enviaram um email

Problemas:

- Remetentes precisam confirmar que enviaram um email

Anti-Spam em um provedor

Você X Clientes

Bloqueios no MTA Greylisting

Comportamento do MTA (hash IP:From:To)

Prós:

- Evita scripts pobres de spammers

Problemas:

- Spammers rodam MTAs “completos” e tratam falhas temporárias
- Demora na entrega de mensagens
- Problemas com provedores com vários servidores SMTP

Anti-Spam em um provedor

Você X Clientes

Bloqueios no MTA Outras configurações

- **Limite de conexões simultâneas**
- **Limite de tempo idle**
- Limite de conexões por tempo
- Limite de emails por conexão
- Limite de destinatários por email
- Limite de tamanho de mensagem

Anti-Spam em um provedor

Você X Clientes

Filtro de conteúdo Anti-vírus / Anti-phishing

Prós:

- Proteção contra códigos e páginas maliciosas conhecidas

Problemas:

- ?

Anti-Spam em um provedor

Você X Clientes

Filtro de conteúdo Checagem de URLs

Prós:

- URIDNSBL: URLs conhecidas de vírus / phishing
- Baixar arquivos e checá-los contra vírus *
- Validação da URL *

* Problemas:

- DoS

Anti-Spam em um provedor

Você X Clientes

Filtro de conteúdo Regras via regex

Prós:

- Identificação dos padrões frequentemente encontrados em spams

Problemas:

- Regras ruins
- Usuários ruins

Uso ideal:

- Diversas regras de pouca pontuação

Anti-Spam em um provedor

Você X Clientes

Filtro de conteúdo Imagens

Prós:

- Reconhecimento de palavras em imagens
- Reconhecimento de imagens comuns

Problemas:

- Falsos negativos – erro de software
- Falsos positivos – erro de software, acasos extremos

Anti-Spam em um provedor

Você X Clientes

Filtro de conteúdo Decisões

Chance de ser spam: marcar assunto
Altíssima chance de ser spam: quarentena
(Ex: spamassassin score > 10)

Prós:

- Email não é perdido
- Possibilidade do usuário criar regras pela marcação no assunto
- Pode ser reportado como não spam e analisado

Problemas:

- Falsos positivos extremos e usuários não checam a quarentena

Anti-Spam em um provedor

Você X Clientes

Filtro de conteúdo Configuração pelo usuário

Usuário treinar seu filtro anti-spam

Prós:

- Sensação de controle da parte do cliente

Problemas:

- Base individual de spam – outros não usufruirão
- Reportarão emails de listas que se inscreveram
- Reportarão emails que depois irão querer receber

Solução:

- Sem aprendizagem comandada pelo usuário
- Email para reportar spam e falsos positivos e equipe de análise

Anti-Spam em um provedor

Você X Clientes

Recomendações

Conformidade:

- Exigência de conformidade RFC do protocolo SMTP (821, 2821)
- Credibilidade na relação DNS e email
- Problema: administradores “newbies”
- Spammers não são “new players” - obedecem normas que podem

Conteúdo:

- Não bloquear emails que o cliente quer receber
- Feedback para tratar falsos positivos e falsos negativos

Anti-Spam em um provedor

Você X Clientes

Solução

Flexibilidade (software)

- Conscientização dos clientes sobre as regras
- Análise de cada caso com transparência ao cliente
- Flexibilidade de escolher as medidas que cada cliente quiser

Resultado

- Clientes recebem mais spams
- Conscientização dos clientes sobre as regras
- Algumas medidas são novamente habilitadas
- Clientes querendo que os outros se conscientizem
- Clientes percebem o bom nível de serviço

Anti-Spam em um provedor

Você X Clientes

Estatísticas

(universo de 109.471 emails)

- Bloqueados por não ter IP reverso: 39.202 (35.6%)
- Bloqueados por HELO/EHLO: 27.891 (25.5%)
- Bloqueados por domínio do remetente: 3.115 (2.8%)
- Bloqueados por destinatário inválido: 4.123 (3.7%)
- Outras checagens: 17.641 (16%)
- Bloqueados por SPF: 896 (<1%)
- Bloqueados por DNSBLS: 5.239 (4.8%)

- Bloqueados por vírus: 33 (<1%)
- Quarentenados por spam: 3834 (3.5%)
- Entregues marcados como spam: 1452 (1.3%)
- Entregues não marcados: 6045 (5.5%)

Anti-Spam em um provedor

Você X Clientes

FIM

Conclusão:

- O maior problema está nos administradores de email (bloqueios no MTA)
- Os usuários precisam se reeducar (regras no filtro de conteúdo)

André Guimarães, “Ramoni”
andre.ramoni@gmail.com