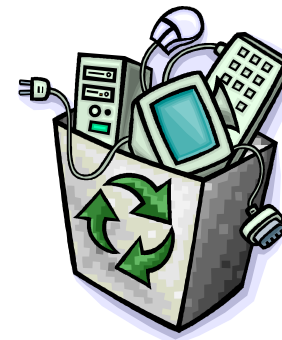


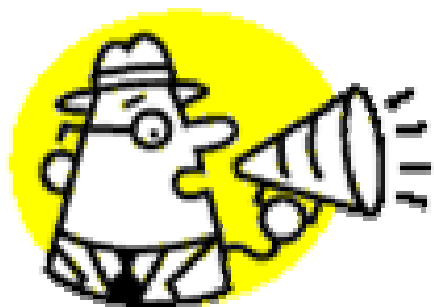
O Lixo eletrônico vem gerando tanto incomodo e prejuízo que tem administrador de rede ficando
neurótico



Alguns estão tomando atitudes radicais e muitas vezes... erradas...

Ações:

- Prover SMTP autenticado em porta diferente da 25, tal como a 587;
- Controlar vazão do envio de e-mails de um mesmo remetente a múltiplos destinatários em determinado espaço de tempo;
- Servidores com relay aberto: checar, orientar e se necessário auxiliar os clientes;
- O Draft do SPF foi aprovado e publicado em 06/06/05, em breve teremos uma RFC sobre SPF;
- SPF no domínio do cliente: respeitando seu modo de utilização;
- Orientar clientes sobre RFC 2142 – abuse e security@dominio;
- Reverso de DNS devidamente configurados;
- O nome do host do Servidor de Envio usado no VERBO HELO ou EHLO da comunicação SMTP deve ser válido.



Socorro...

Precisamos de ajuda !

Precisamos de ajuda:

- **DNS Reverso:** Teles e provedores precisam assumir um compromisso de orientar os clientes da necessidade do IP Reverso, principalmente se estes forem utilizar um servidor de correio;
- **RFC 2142:** Provedores devem fazer ampla divulgação aos seus clientes da necessidade dos endereços abuse e security;

O **registro.br** pode e precisa nos ajudar divulgando a RFC 2142 no corpo dos e-mails que envia aos contatos no momento do registro;

Recomendações já existem...

<http://www.cg.org.br/infoteca/documentacao/desenvolvimento.htm>

1.4 Serviços DNS Configurados Corretamente

Visando prover identificação imediata dos computadores ligados à Internet brasileira, seguindo um padrão mundial de operação com registros direto e reverso de "Domain Name System" (DNS), faz-se necessário que todas as redes conectadas à Internet/Br implementem tais serviços.

Recomendação: Todas as redes conectadas à Internet brasileira devem operar com registros direto e reverso de DNS corretamente configurados.

Recomendações já existem...

<http://www.nbso.nic.br/docs/seg-adm-redes/seg-adm-redes.html>

4.5.5. DNS Reverso

O uso mais freqüente do DNS é a tradução de nomes em endereços IP. Entretanto, ele também permite descobrir o nome associado a um determinado endereço IP. Isso é chamado DNS reverso, e possibilita a identificação do domínio de origem de um endereço IP.

Um DNS reverso mal configurado ou inexistente pode causar alguns transtornos. O primeiro deles é que muitos sites negam o acesso a usuários com endereços sem DNS reverso ou com o reverso incorreto. Em segundo lugar, erros na configuração do DNS depõem contra a competência técnica da equipe de administração de redes responsável pelo domínio, e isso pode vir a causar dificuldades quando for necessário interagir com equipes de outras redes.

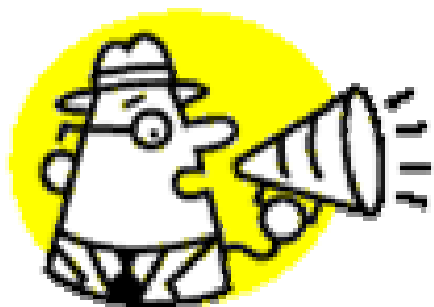
É recomendável que você mantenha atualizado o DNS reverso dos endereços sob sua responsabilidade. Em alguns casos a administração do DNS reverso dos seus blocos pode ser delegada à sua rede, enquanto em outros o seu provedor de backbone é quem é responsável pelo DNS reverso dos seus endereços. Entre em contato com o seu provedor de backbone para obter informações sobre como atualizar o seu DNS reverso.

Um e-mail não chega...

A culpa é do remetente que tem um servidor mal configurado (sem reverso, host name inválido, etc ...) ?

OU

Do destinatário que tem filtros e controles para evitar o lixo eletrônico ?



Socorro... Novamente precisamos de ajuda !

Precisamos novamente de ajuda:

- Estamos tentando fazer a coisa certa mas os usuários não entendem desta forma, principalmente quando um pedido ou informação importante não chega...
- O e-mail não chegou... a culpa é do Provedor ou do administrador da rede... De quem estiver mais perto...
- Precisamos ter estas “**recomendações**” compiladas, centralizadas num único documento e publicadas com destaque nos sites das entidades que REGULAM e tem o respeito da comunidade Internet Brasileira:



Convocar outros “exércitos” para esta guerra:

- FEBRABAN e SERASA
- Governo
- Os grandes sites de comércio eletrônico
- Portais de Humor e Cartões Virtuais

Resultado do filtro (dados reais):

DOMINIO: vecombrasil.com.br DATA:2005-08-19

```
*****  
*   MENSAGENS REBECIDAS E ENCAMINHADAS   *  
*****  
Total de Mensagens:      8339 msg(s)  
Total Recebidas:        295 msg(s)  
MBytes Processados:     11,89 MBytes
```

**8.044 msgs.
bloqueadas**

```
*****  
*   MENSAGENS REJEITADAS   *  
*****  
RECUSA:450 :      19 msg(s)  
RECUSA:457 :     223 msg(s)  
RECUSA:458 :    1104 msg(s)  
RECUSA:501 :      12 msg(s)  
RECUSA:504 :    1214 msg(s)  
RECUSA:558 :     331 msg(s)  
RECUSA:559 :    5118 msg(s)  
RECUSA:562 :      23 msg(s)
```

458 SoftFail

**504 HELO ou
EHLO
inválido**

559 SPF-Fail

Resultado do filtro (dados reais):

DOMINIO: cti.com.br DATA:2005-08-19

```
*****  
*   MENSAGENS REBECIDAS E ENCAMINHADAS   *  
*****  
Total de Mensagens:      32979 msg(s)  
Total Recebidas:         2310 msg(s)  
MBytes Processados:      153,88 MBytes
```

**30.669 msg.s.
bloqueadas**

```
*****  
*   MENSAGENS REJEITADAS   *  
*****  
RECUSA:450 :      212 msg(s)  
RECUSA:457 :     5426 msg(s)  
RECUSA:458 :     2934 msg(s)  
RECUSA:501 :      319 msg(s)  
RECUSA:504 :    11456 msg(s)  
RECUSA:558 :     1287 msg(s)  
RECUSA:559 :     8847 msg(s)  
RECUSA:561 :       12 msg(s)  
RECUSA:562 :      170 msg(s)  
VIRUS :          6 msg(s)
```

457 Neutral

458 SoftFail

**504 HELO ou
EHLO
inválido**

559 SPF-Fail

Respostas a Incidentes e SPAM

- Conscientização dos Provedores, TELES (SPEEDY, VELOX, BRTURBO, NET) de que o acompanhamento e **rápida ação e resposta** sobre incidentes de segurança e SPAM darão maior credibilidade às nossas empresas;
- Telefone IP para os Provedores, visando agilizar a comunicação em caso de incidente de segurança e/ou tratamento de casos graves necessitem de ação imediata.

Nossa responsabilidade é grande:
Enquanto destino, precisamos implementar
filtros e regras para proteger nossos
usuários

Quando origem, nos cabe fiscalizar e
controlar a ação de nossos usuários para
que não cometam abusos



Evento: CT SPAM
Rio de Janeiro - Marina da Glória



Obrigado

Carlos A. Bernardi

bernardi@cti.com.br



Soluções Corporativas em
Conectividade



Carlos A. Bernardi
bernardi@cti.com.br

