Boas Práticas para Mitigação de Spams e de Fraudes via E-mail

Klaus Steding-Jessen
jessen@cert.br

Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil – CERT.br
http://www.cert.br/
cert@cert.br

Comitê Gestor da Internet no Brasil – CGI.br
http://www.cgi.br/

Roteiro

- Motivação
- Formas de mitigação
- Educação dos usuários
  - site antispam.br
- Referências

Motivação

- número grande de spams circulando na Internet
- abuso dos computadores de usuários finais
  - instalação de bots, utilizados para DDoS e envio de spam
  - utilização de proxies abertos para anonimato
- e-mail como vetor de progagação de vírus/worms
- spam como meio para a prática de fraudes
- bloqueio de spam apenas no destino não é ideal
  - consumo de banda, disco, processamento
  - contínuo esforço de configuração e de implantação de novas tecnologias

Dificultando o Abuso de Sua Rede

Spammers, bots, worms e vírus usam o envio direto de e-mails de um cliente para um MTA destino para se propagar.

- fechar *proxies* e *relays* abertos
- impedir o envio direto de e-mail a partir de estações clientes
  - bloquear a porta 25/TCP para conexões de saída
  - utilizar a porta 587/TCP (*mail submission port*)
- implementar SMTP autenticado

Combatendo a Falsificação de E-mails

Fraudadores e códigos maliciosos costumam forjar os remetentes das mensagens.

- DKIM (*Domain Keys Identified Mail*)
  - técnica que permite checar o **cabeçalho** de uma mensagem (campo `From:`)
  - consiste em assinar as mensagens para garantir a autenticidade do remetente
- SPF (*Sender Policy Framework*)
  - técnica que permite checar o campo `MAIL FROM` do **envelope** de uma mensagem

SPF

- permite anunciar quais servidores podem enviar e-mail em nome de um domínio
  - anúncio feito via registro `TXT` do DNS

```
example.com.    IN   TXT   "v=spf1 a mx ip4:192.0.2.32/27 -all"
```

- permite checar se um e-mail foi enviado a partir de um servidor autorizado
- o anúncio e a checagem são operações independentes
- diversas redes já estão utilizando SPF

SPF (cont)

```
planalto.gov.br.        3600    IN      TXT     "v=spf1 ip4:200.181.15.0/24
ip4:200.198.192.192/27 ~all"

stj.gov.br.             10800   IN      TXT     "v=spf1 mx -all"

ctir.gov.br.            86400   IN      TXT     "v=spf1 mx -all"

caixa.gov.br.           3600    IN      TXT     "v=spf1 mx a:200.201.164.40
a:200.201.164.41 a:200.201.164.42 a:200.201.164.43 mx:200.201.166.143
mx:200.201.166.204 ~all"

cert.br.                86400   IN      TXT     "v=spf1 mx a:listas.cert.br
-all"

uol.com.br.             2108    IN      TXT     "v=spf1 ip4:200.221.11.0/24
ip4:200.221.29.0/24 ip4:200.221.4.0/24 -all"

terra.com.br.           6159    IN      TXT     "v=spf1 ip4:200.154.55.0/24
ip4:200.176.2.0/23 ip4:200.176.10.0/23 include:tmp-spf.terra.com.br
include:ti-spf.terra.com.br include:te-spf.terra.com.br -all"
```

Acompanhamento de notificações de abuso

- criar emails da RFC 2142 (`security@`, `abuse@`)
- manter os contatos de Whois atualizados
- o contato técnico do domínio deve ser um profissional que tenha contato com as equipes de abuso
- redes com grupos de resposta a incidentes de segurança devem anunciar o endereço do grupo junto à comunidade
- os endereços de contato não podem ter as mesmas regras anti-spam que o resto da organização

Educação dos Usuários

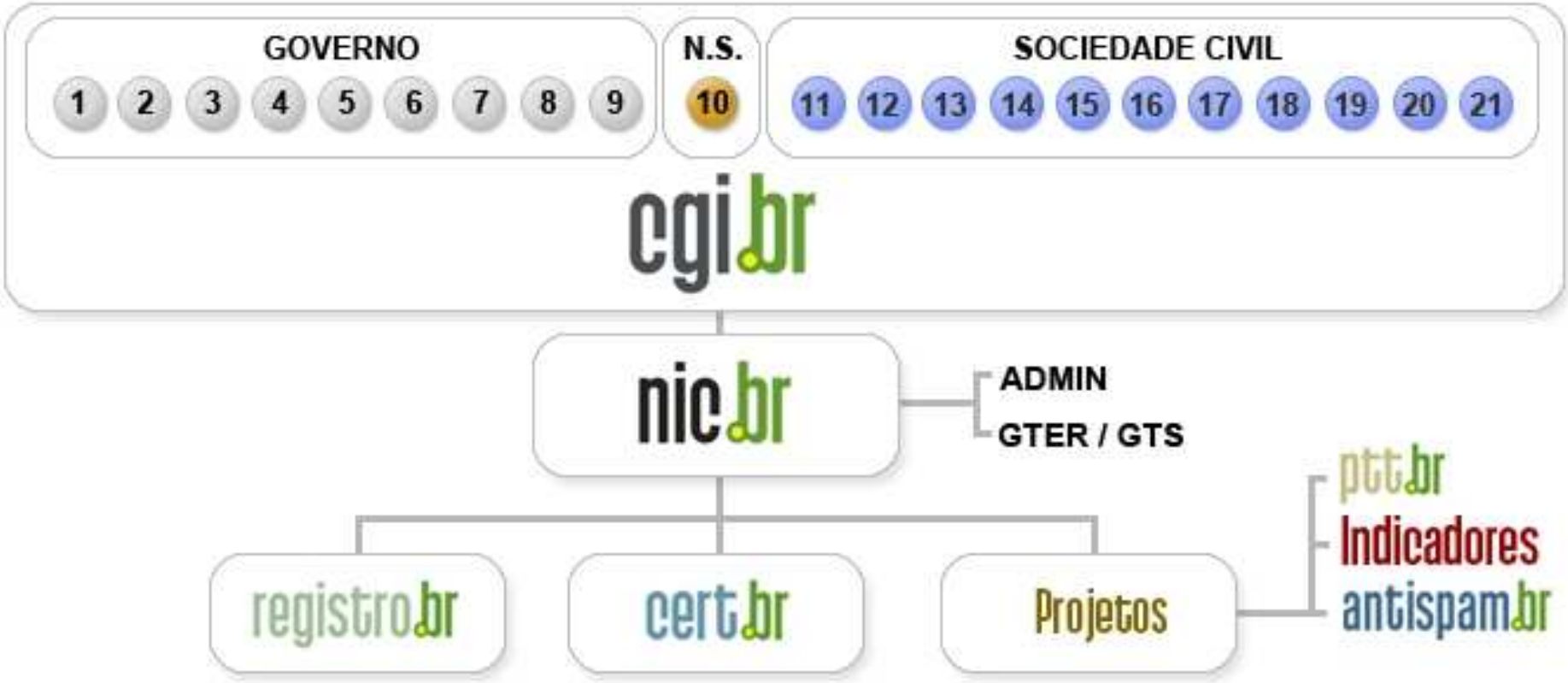
Antispam.br

- iniciativa da Comissão de Trabalho Anti-Spam do CGI.br

  http://www.cgi.br/sobre-cg/antispam.htm

- objetiva informar o usuário e o administrador de redes sobre o combate ao spam, suas implicações e formas de proteção

CGI.br e o Antispam.br



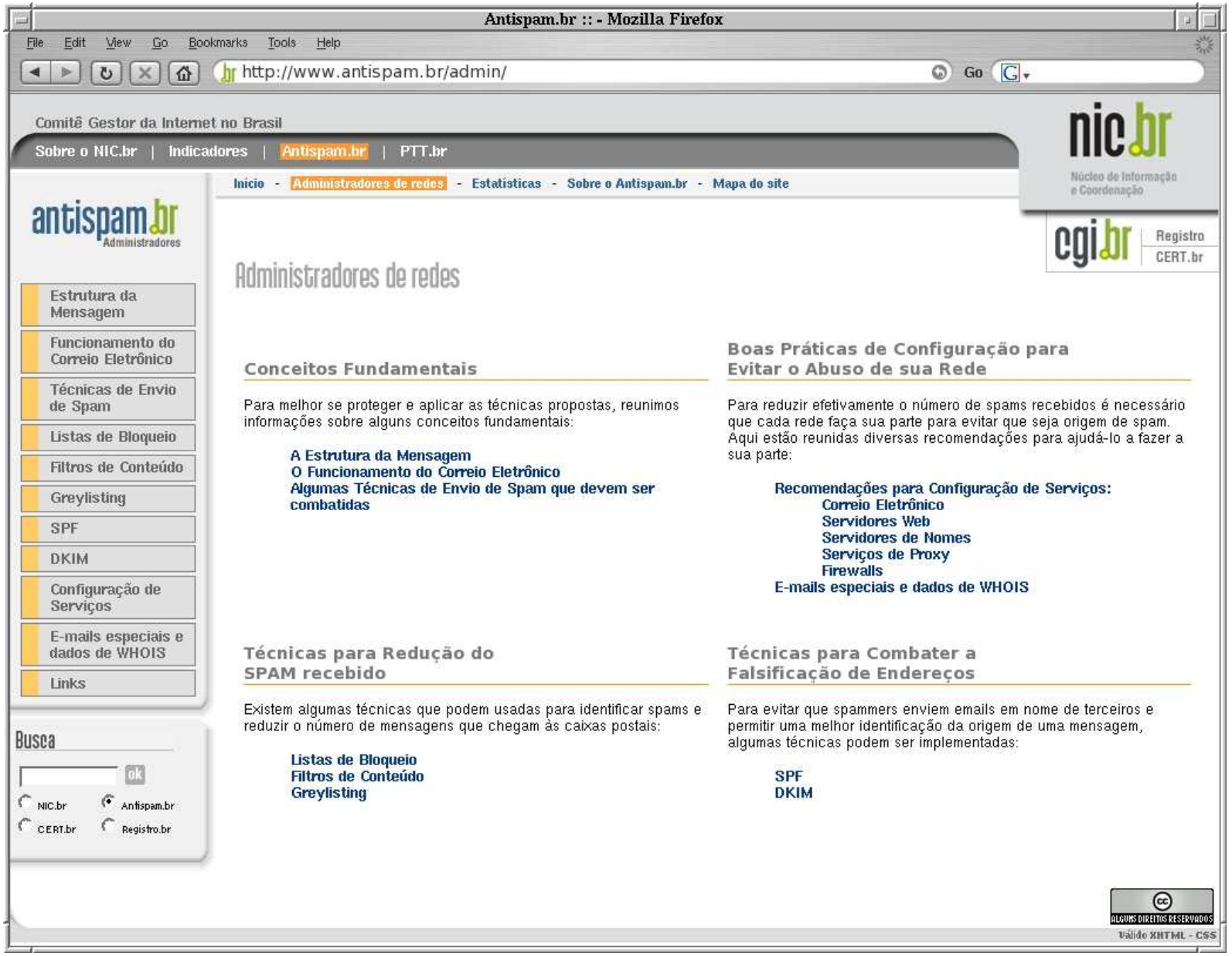
http://www.antispam.br/

Antispam.br (cont)

Material de apoio para a educação dos usuários:

- tipos de spam e como identificá-los
- fraudes e sua prevenção
- boas práticas e dicas para proteção
- origem e curiosidades
- links para ferramentas e outros documentos

http://www.antispam.br/admin/



Referências

- Esta Palestra
  http://www.cert.br/docs/palestras/
- Antispam.br
  http://www.antispam.br/
- Comitê Gestor da Internet no Brasil
  http://www.cgi.br/
- CERT.br
  http://www.cert.br/
- Cartilha de Segurança para Internet
  http://cartilha.cert.br/