Tratamento de Incidentes de Segurança na Rede-Rio

Marita Maestrelli

mm@rederio.br

Coordenação de Engenharia e Operações Rede-Rio

Centro Brasileiro de Pesquisas Físicas – CBPF

Coordenação de Engenharia Operacional da Rede Rio

CBPF

Rede Rio 2

Workshop de Tratamento de Incidentes

SSI 2003 - 5° Simpósio de Segurança em Informática

Índice da Apresentação

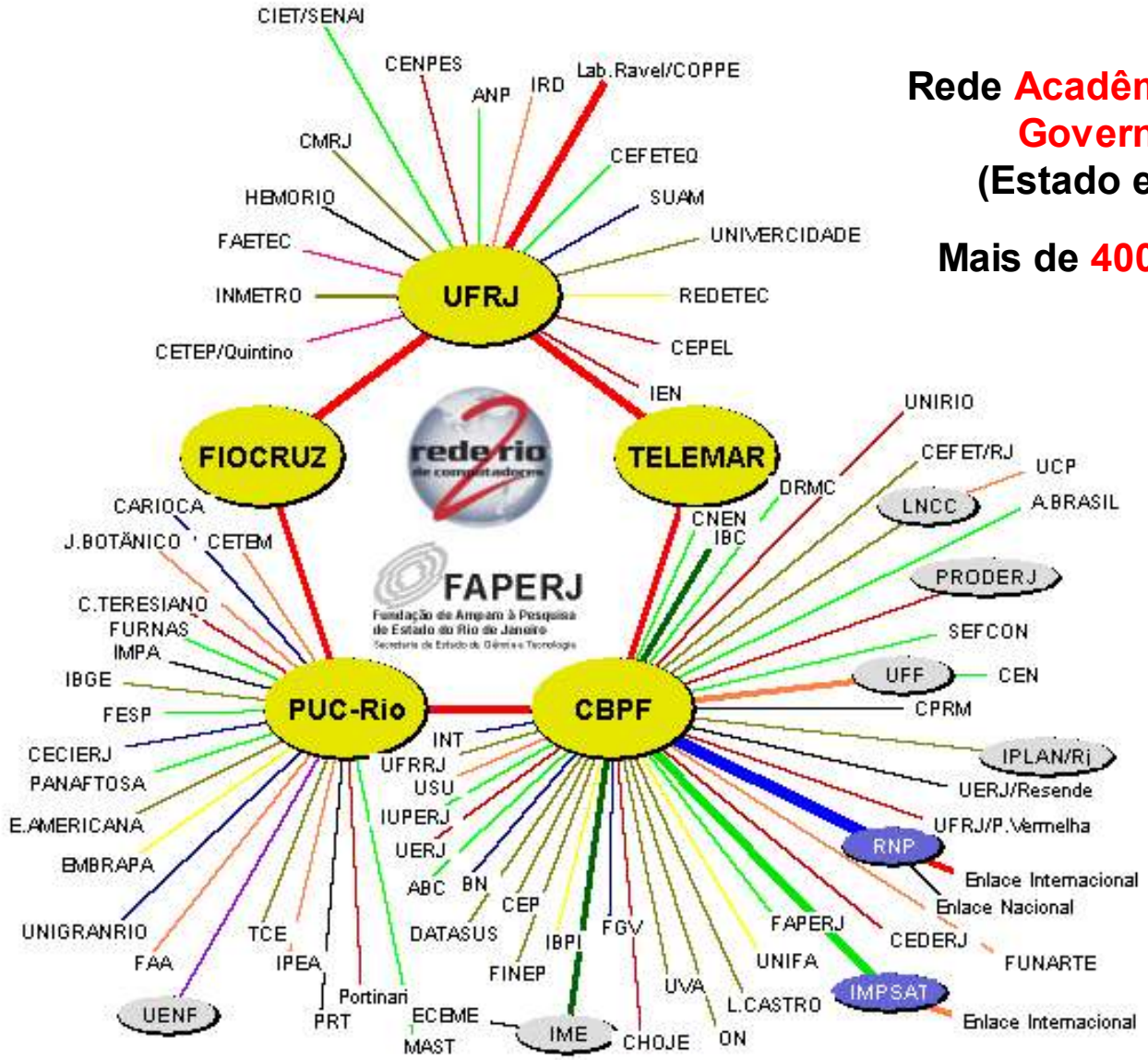
- Apresentação da RR
- Infra-estrutura da RR
- A segurança na RR
- Incidentes de Segurança na RR
- Conclusão

A Rede Rio é uma rede de computadores, integrada por universidades, centros de pesquisa e entidades governamentais (municipais, estaduais e federais) localizados no Estado do Rio de Janeiro.

É um dos principais instrumentos de desenvolvimento científico e tecnológico, alem de oferecer serviços do governo ao cidadão do Estado do Rio de Janeiro.

A SECTI é o órgão responsável pela sua coordenação, e a FAPERJ pelo seu financiamento.

Versão da Base de Dados: 30/05/2003



Rede Acadêmica / Cientifica Governamental
(Estado e Município)

Mais de 400 mil usuários

Atuação do Grupo de Segurança da RedeRio

- **Política de utilização do backbone**

  http://www.rederio.br/como_se_associar/regras/regras.htm

- **Práticas de Segurança**

  Incentivo aos administradores das afiliadas – base na do NBSO

- **Monitoramento constante**
- **Emissão de Alertas**
- **Repasse de incidentes aos afiliados**

  Envolve análise, orientação e acompanhamento

Gerência da Rede via Web

Gerência Pró-Ativa - problemas podem ser detectados em ≈ 2 ½ minutos

- Gerencia da Rede é integrada à Web.
- Gerenciamento Descentralizado e eficiente.
- Banco de Dados: informações de todas as Instituições afiliadas.
- Monitoramento do tráfego on-line
- Monitoramento de missão crítica
- Monitoramento Remoto (WAP)
- Previsão de Tráfego
- Redundância dos Serviços

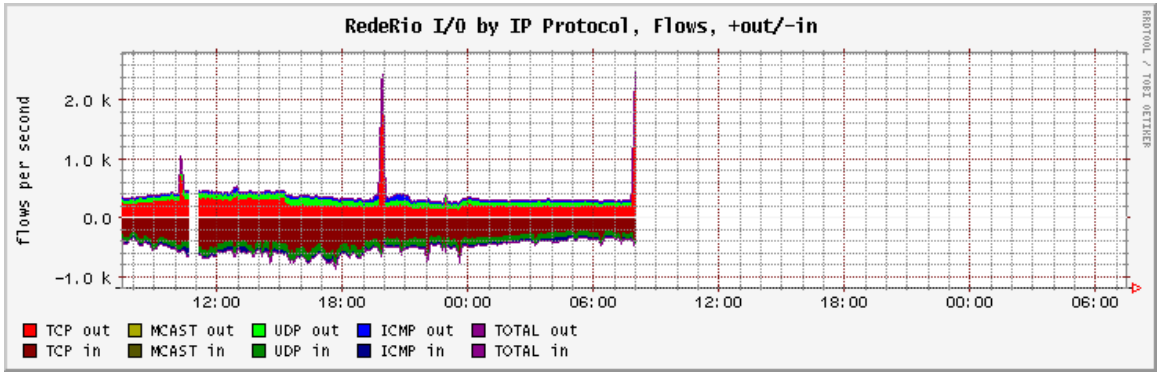
Gerência de Fluxo do Tráfego no backbone

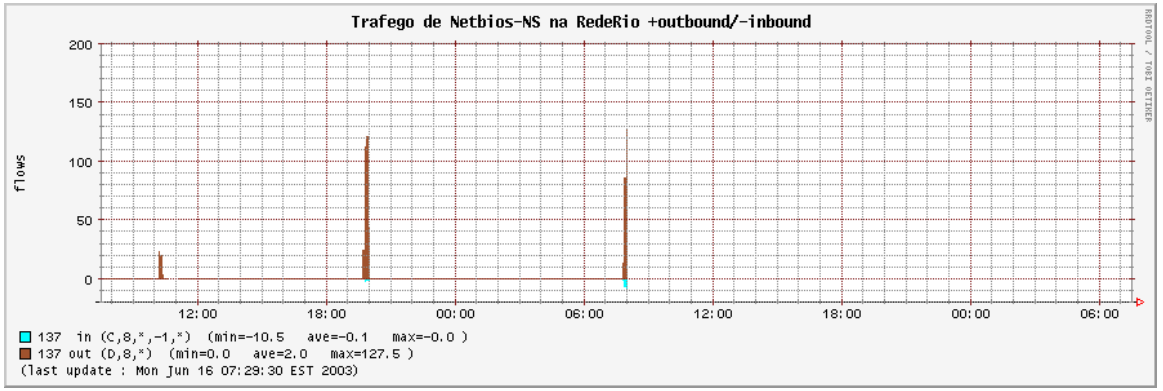
Facilidade em detectar incidentes visualmente

RedeRio Tráfego Roteador de borda - 200.20.94.58 - Netscape

Exemplo 2

Tráfego: 137/UDP NetBios-NS



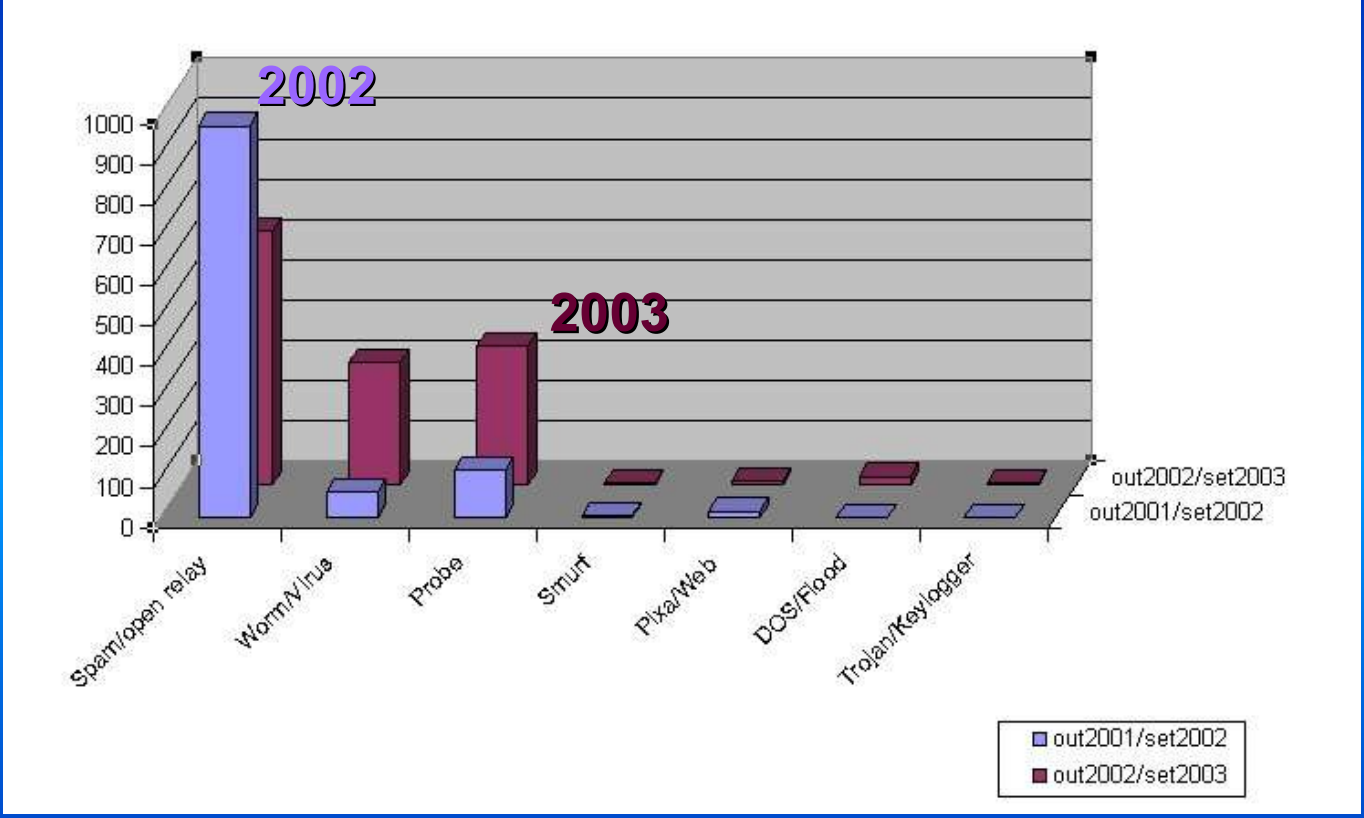


ise de Fluxo:

dows

Incidentes de Segurança nas instituições afiliadas da RedeRio

Comparativo para os anos de 2002 e 2003



- **Incidentes denunciados envolvendo instituições afiliadas.**

TIPO	2002	2003
Spam/OpenProxy/Relay: espalhamento de mensagens não solicitadas, utilizando máquinas mau configuradas	**971**	**629**
Worms: programas intrusos que se copiam e atualizam automaticamente pela rede	**65**	**303**
Probe: tentativas de invasões por procura de vulnerabilidades	**117**	**344**
Smurf: forja o endereço da vítima como origem (roteadores mau configurados)	**6**	**6**
Defaced: “pixações” de páginas Web de instituições afiliadas.	**16**	**9**
DOS: Negação de serviços	**1**	**20**
Trojan/keylogger: programas maliciosos com a finalidade de pegar senhas,e outros dados sigilosos.	**0**	**4**

Alertas sobre Incidentes de Segurança

Originado por insituições afiliadas

Total de Alertas enviados divididos por tipo de infecção	199
Worm Slapper	15
Virus Sobig	3
Worm MSBlaster/Welchia	30
Worm BugBear/Opaserv	145
Outros	6

Incidentes Acadêmicos

Rede-Rio é uma rede heterogênea com bastante flexibilidade
(característica do ambiente acadêmico)

Caso 1: Invasão nas máquinas de um laboratório de pesquisa.

Caso 2: Página de um banco numa instituição de pesquisa.

Caso 3: Re-incidência em Open-Relay.

Caso 4: Rede com Proxy de aplicação.

Caso : "Censura" num micro pessoal – (ignorância do usuário).

Conclusão

- Nesta apresentação falamos do tratamento à incidentes de segurança em um backbone acadêmico (Rede-Rio)
  - *Alertas, Repasse para responsáveis e acompanhamento (e ajuda se for o caso) , estatísitcas de ocorrência (histórico) e estudos de casos.*
- Normalmente a preocupação com segurança começa depois do incidente.
- É muito importante a definição de uma legislação específica no país.

"Cabe lembrar que o mais importante sempre será a informação. A área de segurança, para backbones acadêmicos, trabalha numa tênue linha que visa proteger a informação, porém sem bloquear ou censurar"

Grupo de Segurança da RedeRio

security@rederio.br

Workshop de Tratamento de Incidentes

SSI 2003 - 5° Simpósio de Segurança em Informática