16 SCI

Seminário RNP de Capacitação e Inovação

Escola Superior de Redes RNP

redeIpê

RNP

Ministério da Cultura

Ministério da Educação

Ministério da Ciência e Tecnologia

Bate-papo de segurança

Equipe do CAIS

Escola Superior de Redes RNP
redeIpê
RNP
Ministério da Cultura
Ministério da Educação
Ministério da Ciência e Tecnologia

Introdução

Sobre o CAIS

Liliana Solha (CAIS/RNP)

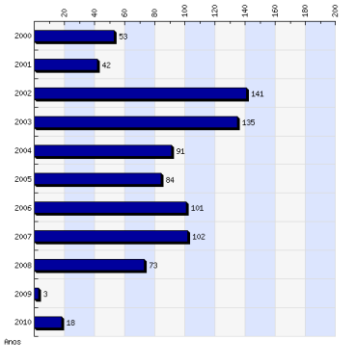
Sobre o CAIS

- Criado em maio de 1997
- Missão

"O CAIS – Centro de Atendimento a Incidentes de Segurança atua na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes."

http://www.rnp.br/cais/sobre.html

Resposta a Incidentes de Segurança



encsirts

'09 DISI
DIA INTERNACIONAL DE SEGURANÇA EM INFORMÁTICA
02.DEZ.2009 | UFBA

http://www.rnp.br/cais/alertas/

CAIS

www.rnp.br/keyserver.php

FIRST
Forum of Incident Response and Security Teams
FIRST Technical Colloquium
- Security Workshop
- FIRST/TRANSITS Course

October 7-12, 2006
Rio de Janeiro Brazil

Organized by www.rnp.br/cais
CAIS RNP
In cooperation with Latin American FIRST member teams

tipo	Promoção GOL R$ 0,99	ID: 2516
data	15/10/2009	
de	Promocoes@gol.com.br	
assunto	A promocao esta de volta aproveite.	
tag	gol, promocoes	
informações	Imagem 1 - Imagem 2 Texto da mensagem	
arquivo malicioso	Formulario.exe	
comentário	Mensagem falsa se passando pela GOL divulgando suposta promoção com passagens aéreas a R$ 0,99. A fraude fornece um link para visualização de mais detalhes sobre a promoção. Tal link, na verdade, leva a vítima a uma página falsa tentando se passar pela página... (leia mais)	

www.rnp.br/cais/fraudes.php

Estrutura Organizacional

- Alocado na Diretoria de Soluções e Serviços (DSS)
- Modelo interno

Equipe Interna

- Liliana Solha (Gerente)
- André Landim
- Atanai Ticianelli
- Carla Freitas
- Frederico Costa
- Leiseane Lopes
- Rildo Sousa

+ 02 sendo contratados

Agenda

- O CAIS em 2010: Algumas ações em foco
  - Monitoramento de atividade maliciosa na rede Ipê
    Frederico Costa, CAIS
  - GENICS: Nova ferramenta de envio de incidentes
    Atanai Ticianelli, CAIS
  - Panorama sobre o PL de Cibercrimes e Marco Civil
    Omar Kaminski, Consultor Júridico do CAIS
- Palestras convidadas
  - Iniciativas do governo na área de SIC
    Eduardo Wallier (CTIR.Gov/DSIC/GSI)
    Gerson Charbel (Consultor Júridico do DSIC/GSI)

Monitoramento de atividade maliciosa nas redes acadêmicas e de pesquisa

Ações do CAIS em andamento

Frederico Costa (CAIS/RNP)

O “problema”

- Monitorar e reportar atividades maliciosas na redeIpê
  - centenas de instituições conectadas
  - milhares de clientes conectados
  - centenas de Gbps de tráfego
  - dezenas de pontos de troca de tráfego
  - milhares de incidentes reportados

A “solução” atual

- Monitoramento por amostragem
  - Poucos sensores rodando darknets
    - Monitoramento do espaço de IPs não alocados
  - Parcerias com grupos de segurança nacionais e internacionais
    - Obtenção de fontes de ataques
  - Capacidade limitada de processamento de fluxos de dados

A “nova solução” em implantação

- Monitoramento com taxa de amostragem mais alta
  - Sensores distribuídos (1 por PoP – novas máquinas de serviço)
    - Maior abrangência de monitoramento nos sensores
      - Darknets
      - Malwares
      - SPAM
      - Botnets
  - Parcerias formalizadas com diversos colaboradores para obtenção de fontes de ataques
  - Melhoria na capacidade de processamento (correlacionamento) de fluxos de dados

A “solução futura”

- EWS
  - Obtenção de dados de fontes diversas
    - Sensores distribuídos especialistas
  - Maior correlação de dados
    - Necessidade de melhoramento nas técnicas para processamento de grande quantidade de dados
  - Possibilidade de previsão de ataques
    - Análise de comportamento das redes

GENICS:
Gerenciador de Envio de Incidentes e Contatos de Segurança

Nova ferramenta de envio de incidentes

Atanai Ticianelli (CAIS/RNP)

Motivação/Realidade enfrentada

- Grande quantidade de incidentes recebidos e com logs agrupados, a serem repassados aos clientes da RNP
- Diversos incidentes seguem um padrão nas mensagens, mas eram enviados manualmente
  - Spam
  - Bots
  - Download de filmes/músicas/etc
  - URLs maliciosas
- Criação de programas (scripts) não padronizados para o tratamento destas mensagens
  - Dificuldade de atualização de scripts
  - Dificuldade de manutenção de base de contatos pré-existente

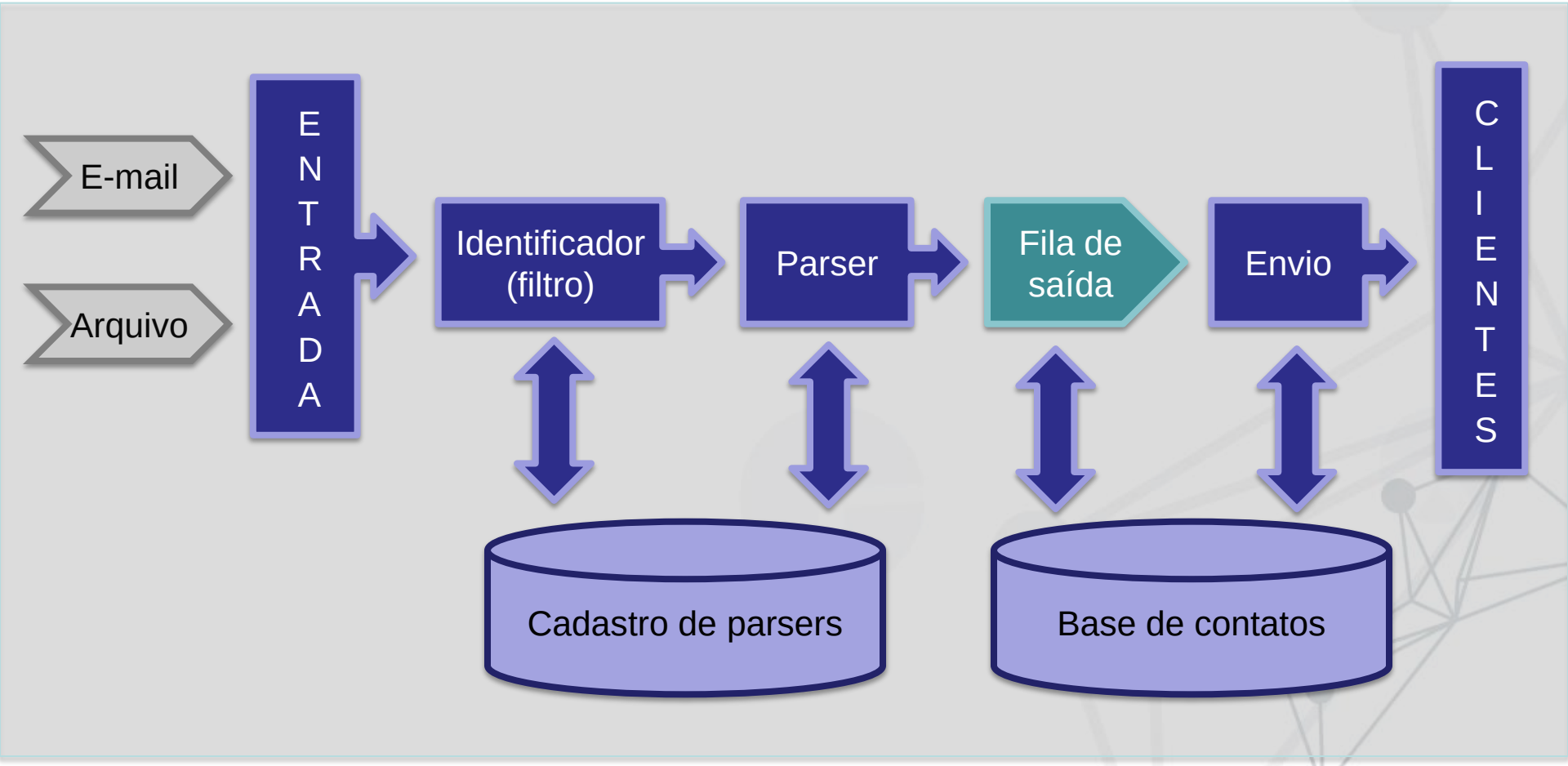
Necessidade de uma ferramenta que:

- Recebesse e automaticamente manipulasse as notificações que chegam padronizadas ao CAIS
- Permitisse o cadastramento/edição/teste de scripts (mini-programas) para manipular as notificações recebidas
- Gerenciasse uma base de contatos de segurança vinculando instituições e endereços de rede
- Realizasse o envio de notificações aos clientes da RNP de forma automatizada

GENICS: Gerenciador de Envio de Incidentes e Contatos de Segurança

- Desenvolvimento terceirizado: 24/09/2009 a 24/09/2010
- Requisitos voltados ao envio automático de incidentes e à gerência de contatos de segurança
- Não é uma ferramenta para gestão dos incidentes (RTIR, AIRT, Jitterburg, outros)

Fluxo de funcionamento



Melhorias obtidas

- 22 parsers cadastrados (12 novos)
- Ambiente de teste de parsers, com funcionalidades refinadas
- Automação de parte do tratamento de incidentes: 1.465 incidentes enviados em 16/10/2010
- 781 endereços de rede cadastrados, agrupados em 378 instituições
- Controle de usuários, registros das modificações realizadas na ferramenta, registros de execução

Próximos passos

- Piloto de utilização com CSIRTs
- Distribuição da ferramenta aos CSIRTs para uso
- Levantamento de melhorias para implementação
- Sistema para gestão de incidentes de segurança ?

Vamos à ferramenta…

Panorama sobre o Projeto de Lei de Crimes Informáticos e o Marco Civil da Internet

Status atual

Omar Kaminski (CAIS/RNP)

PROJETO DE LEI Nº 84, DE 1999 – “Novos” crimes

• **Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado**
Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

• **Obtenção, transferência ou fornecimento não autorizado de dado ou informação**
Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

• **Divulgação ou utilização indevida de informações e dados pessoais**
Pena – detenção, de 1 (um) a 2 (dois) anos, e multa.

PROJETO DE LEI Nº 84, DE 1999 – “Novos” crimes

- **Dano**

Pena - detenção, de 1 (um) a 6 (seis) meses, ou multa.

- **Inserção ou difusão de código malicioso**

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

- **Inserção ou difusão de código malicioso seguido de dano**

Pena – reclusão de 1 (um) a 3 (três) anos, e multa.

- **Estelionato Eletrônico**

Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

PROJETO DE LEI Nº 84, DE 1999 – “Novos” crimes

• **Atentado contra a segurança de serviço de utilidade pública**
Pena - reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

• **Falsificação ou Alteração de dado informático ou documento público**
Pena - reclusão, de 2 (dois) a 6 (seis) anos, e multa.

• **Falsificação ou alteração de dado informático ou documento particular**
Pena - reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Art. 20. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a:

I – manter em ambiente controlado e de segurança, **pelo prazo de três anos**, com o objetivo de provimento de investigação pública formalizada, **os dados de endereçamento eletrônico da origem, destino, hora, data e a referência GMT da conexão** efetuada por meio de rede de computadores **e fornecê-los exclusivamente à autoridade policial e ao Ministério Público**, mediante requisição;

II – preservar imediatamente, após requisição, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;

III – Levar ao conhecimento, de maneira sigilosa, da autoridade policial ou judicial, informação em seu poder ou que tenha ciência e que contenha indícios da prática de crime sujeito a acionamento penal, **cuja prática haja ocorrido no âmbito da rede de computadores sob sua responsabilidade**, ressalvada a responsabilização administrativa, civil e penal da pessoa jurídica, sem exclusão das pessoas físicas autoras, co-autoras ou partícipes do mesmo fato.

§ 1º Os dados de que cuida o inciso I, deste artigo, as condições de segurança de sua guarda, a perícia à qual serão submetidos e a autoridade competente responsável por requisitar a perícia, bem como as condições para que sejam fornecidos e utilizados, **serão definidos nos termos de regulamento**, preservando-se sempre a agilidade na obtenção destas informações e o sigilo na sua manipulação.


Usuário de Web
IP: 201.163.0.248
Usuário: João José da Silva
Senha: 069000
repita: 069000
Nasc.: 22/09/2050
RG: 906.999.902
CPF 099.999.099
Filiação: Mariana Maria Silva
Endereço: Rua Silva Santos, 999


Diga NÃO
Diga Não ao
Projeto do
Senador Azeredo
Diga NÃO
ao projeto do
SENADOR AZEREDO
DIGA NÃO AO
Projeto do
Senador Azeredo
ao projeto do
SENADOR AZEREDO

Marco Civil da Internet

seus direitos e deveres em discussão

MARCO CIVIL DA INTERNET
http://culturadigital.br/marcocivil/

Art. 2º. A disciplina do uso da Internet no Brasil tem como fundamentos o reconhecimento da escala mundial da rede, o exercício da cidadania em meios digitais, os direitos humanos, a pluralidade, a diversidade, a abertura, a livre iniciativa, a livre concorrência e a colaboração, e observará os seguintes princípios:

I – garantia da liberdade de expressão, comunicação e manifestação de pensamento;

II – proteção da privacidade;

MARCO CIVIL DA INTERNET
http://culturadigital.br/marcocivil/

III – proteção aos dados pessoais, na forma da lei;

IV – preservação e garantia da neutralidade da rede;

V – preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; e

VI – preservação da natureza participativa da rede.

MARCO CIVIL DA INTERNET
http://culturadigital.br/marcocivil/

Art. 7º. O usuário de Internet tem direito:

I – à inviolabilidade e ao sigilo de suas comunicações, salvo por **ordem judicial**, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (...)

IV – à não divulgação ou uso de seus registros de conexão e registros de acesso a serviços de Internet**, salvo mediante seu consentimento expresso ou em decorrência de determinação judicial**.

MARCO CIVIL DA INTERNET
http://culturadigital.br/marcocivil/

Art. 9º. A provisão de conexão à Internet impõe a obrigação de guardar **apenas os registros de conexão**, nos termos da Subseção I da Seção III deste Capítulo, ficando **vedada a guarda de registros de acesso a serviços de Internet** pelo provedor.

Parágrafo único. O provedor de conexão a Internet fica impedido de monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, salvo para administração técnica de tráfego, nos termos do art 12.

MARCO CIVIL DA INTERNET
http://culturadigital.br/marcocivil/

Art. 10. A provisão de serviços de Internet, onerosa ou gratuita, não impõe ao provedor a obrigação de monitorar, filtrar, analisar ou fiscalizar o conteúdo dos pacotes de dados, tampouco de guardar registros de acesso a serviços de Internet, salvo, em qualquer dos casos, **por ordem judicial específica**, observado o disposto no art. 18.

Parágrafo único. Para efeitos deste dispositivo, os usuários que detenham poderes de moderação sobre o conteúdo de terceiros se equiparam aos provedores de serviços de Internet.

Do tráfego de dados

Art. 13. O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, conteúdo, serviço, terminal ou aplicativo, sendo vedado estabelecer qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos destinados a preservar a qualidade contratual do serviço.

Da guarda de registros de conexão

Art. 13. A **guarda e a disponibilização dos registros de conexão** a que esta lei faz referência devem atender à preservação da intimidade, vida privada, honra e imagem das partes direta ou indiretamente envolvidas.

Art. 14. A provisão de conexão à Internet impõe ao administrador do sistema autônomo respectivo o dever de manter os registros de conexão sob sigilo, em ambiente controlado e de segurança, pelo prazo máximo de 6 (seis) meses, nos termos do regulamento.

Art. 15. Na guarda de registros de conexão:

I – os registros de conexão somente poderão ser fornecidos a terceiros mediante **ordem judicial** ou por autorização prévia e expressa do respectivo usuário;

II – os dados cadastrais somente poderão ser disponibilizados de maneira vinculada aos registros de conexão mediante **ordem judicial**; e

III – **as medidas e procedimentos de segurança e sigilo dos registros de conexão e dos dados cadastrais devem ser informados de forma clara aos usuários**.

Parágrafo único. Os procedimentos de segurança necessários à preservação do sigilo e da integridade dos registros de conexão e dos dados cadastrais referidos neste artigo deverão atender a padrões adequados, a serem definidos por meio de regulamento.

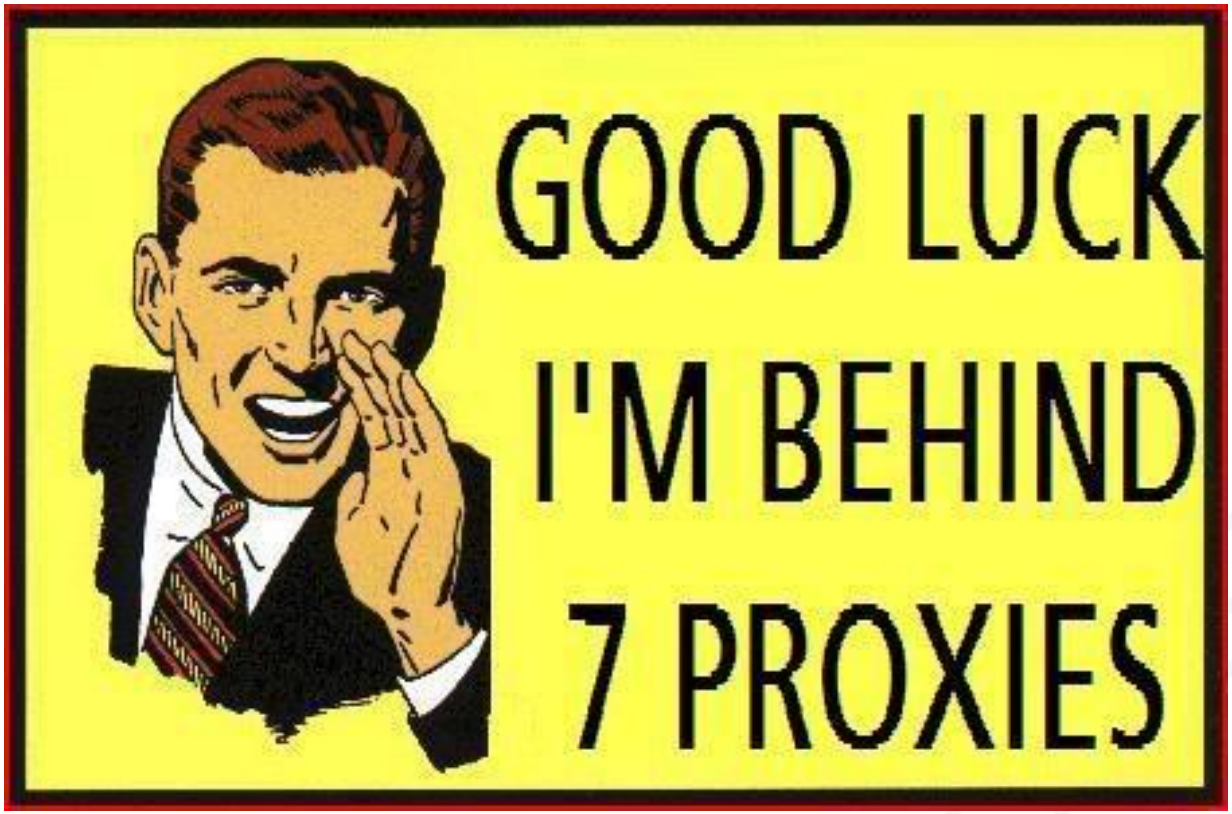
Da guarda de registros de acesso a serviços de Internet

Art. 16. A guarda de registros de acesso a serviços de Internet dependerá de autorização expressa do usuário e deverá obedecer ao que segue, sem prejuízo às demais normas e diretrizes relativas à proteção de dados pessoais:

I – informação prévia ao usuário sobre a natureza, finalidade, período de conservação, políticas de segurança e destinação das informações guardadas, facultando-lhe o acesso, retificação e atualização sempre que solicitado;

II – consentimento livre e informado do usuário previamente ao tratamento, à distribuição a terceiros ou à publicação das informações coletadas; e

III – os dados que permitam a identificação do usuário somente poderão ser disponibilizados de maneira vinculada aos registros de acesso a serviços de Internet mediante **ordem judicial**.


GOOD LUCK
I'M BEHIND
7 PROXIES

Escola Superior de Redes RNP

redeIpê

RNP

Ministério da Cultura

Ministério da Educação

Ministério da Ciência e Tecnologia