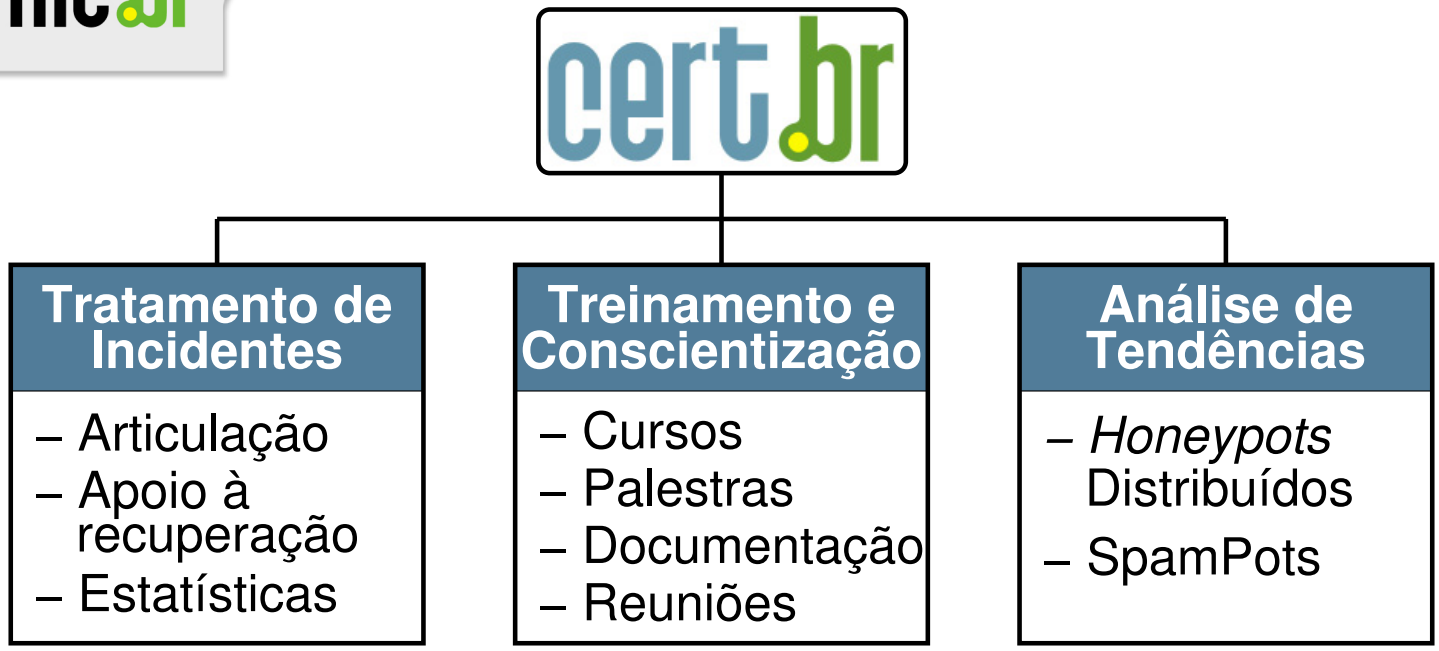
Evolução Tecnológica e a Segurança na Rede

Miriam von Zuben

miriam@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasill
Núcleo de Informação e Coordenação do Ponto br
Comitê Gestor da Internet no Brasil



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

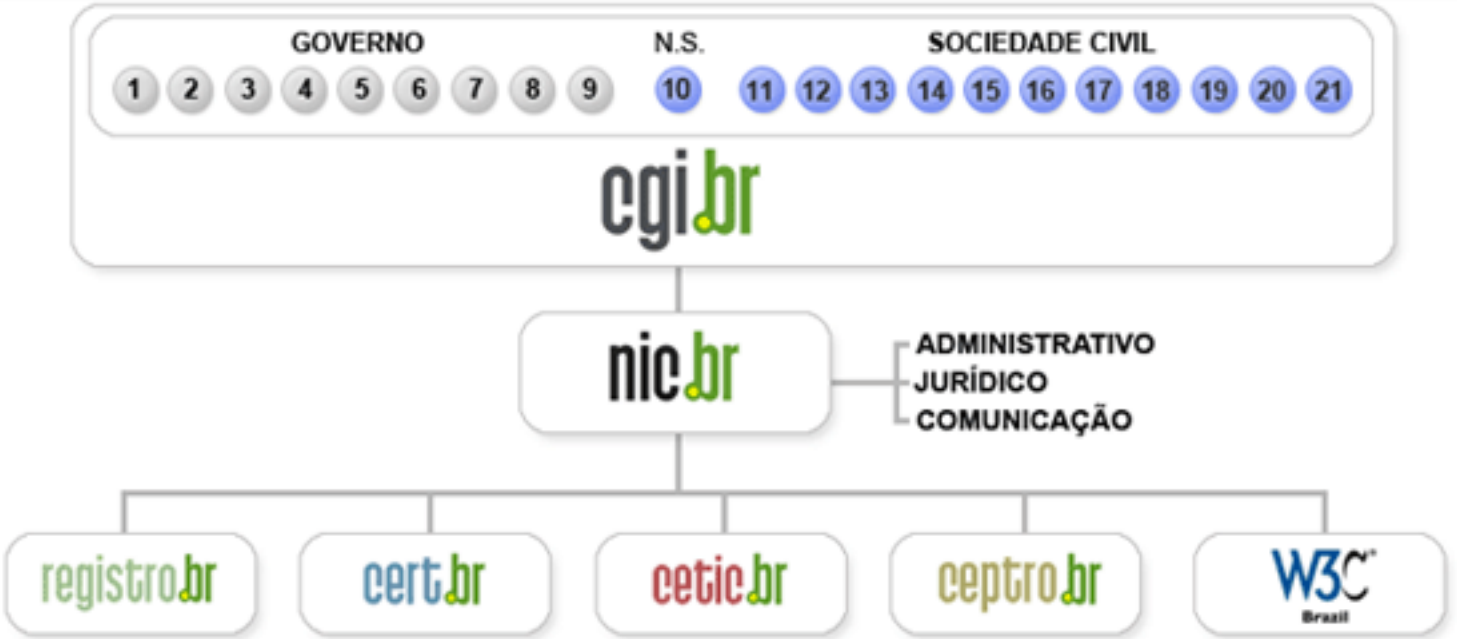
The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

http://www.cert.br/sobre/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica

Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**

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

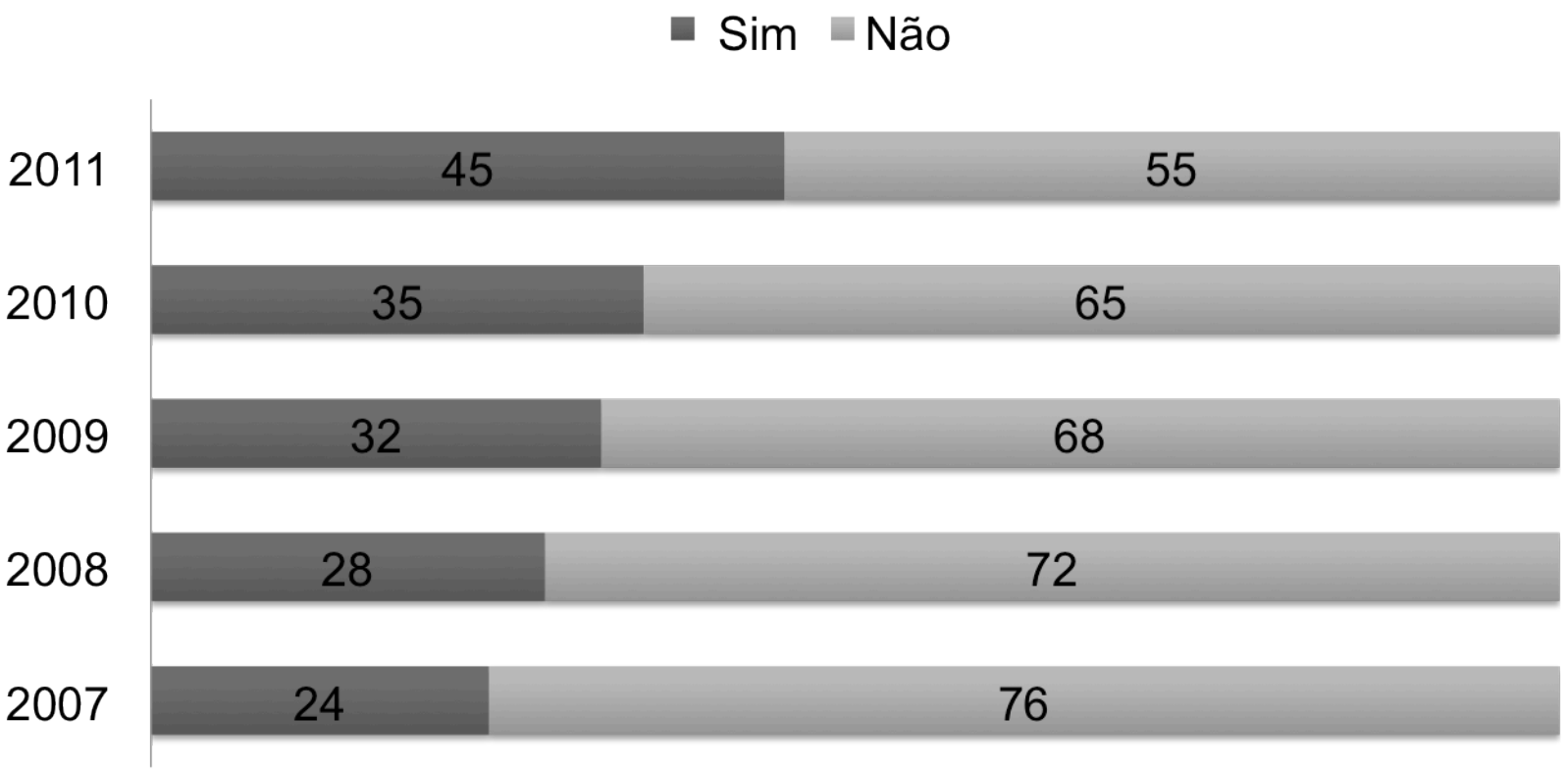
Agenda

- **Evolução Tecnológica**
  - **Domicílios**
  - **Empresas**
  - **Empresas X Segurança**
- **Evolução dos Incidentes de Segurança**
- **Considerações Gerais**
- **Prevenção**

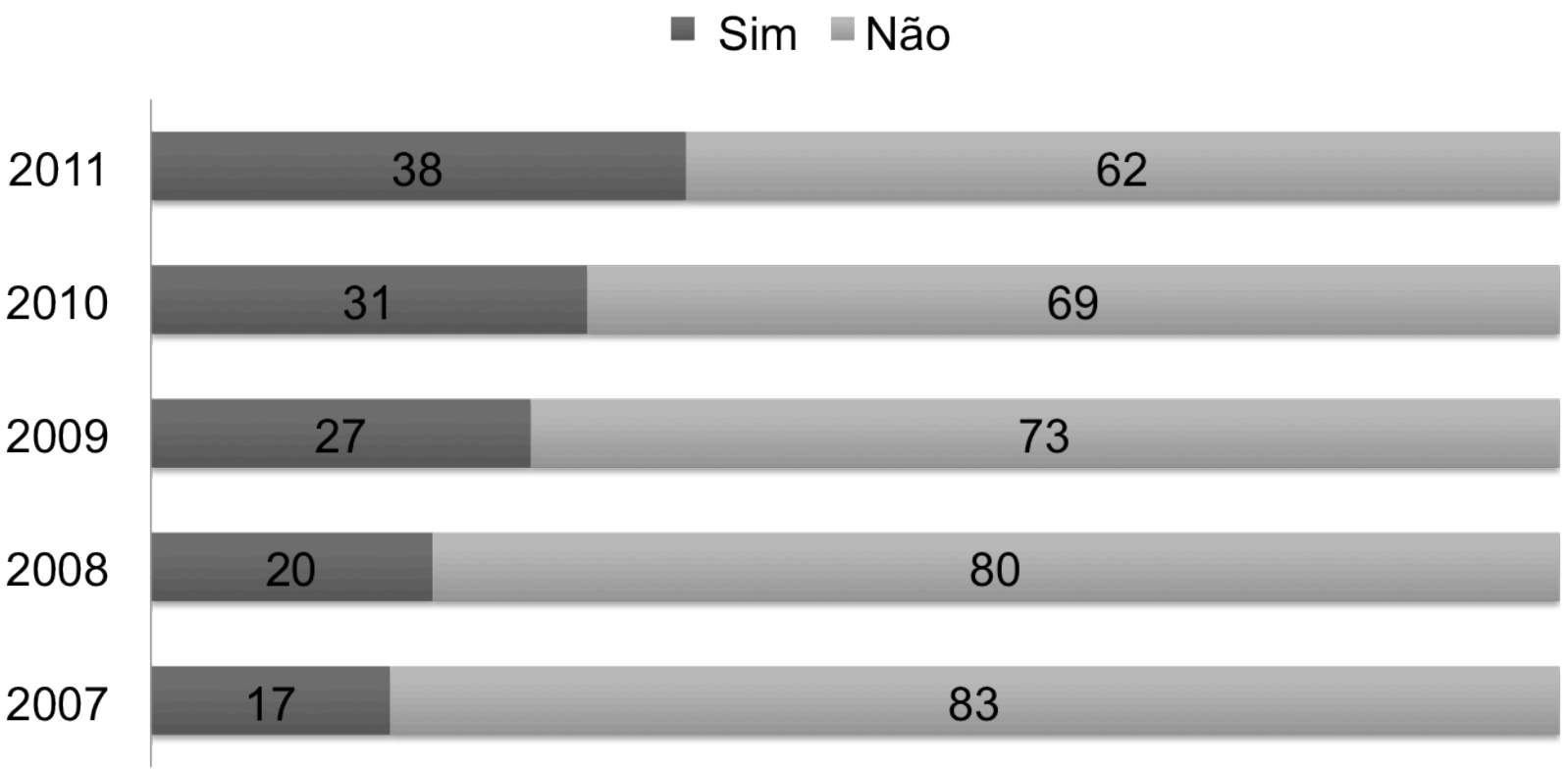
Evolução Tecnológica

Fonte: Pesquisas TIC
http://cetic.br/

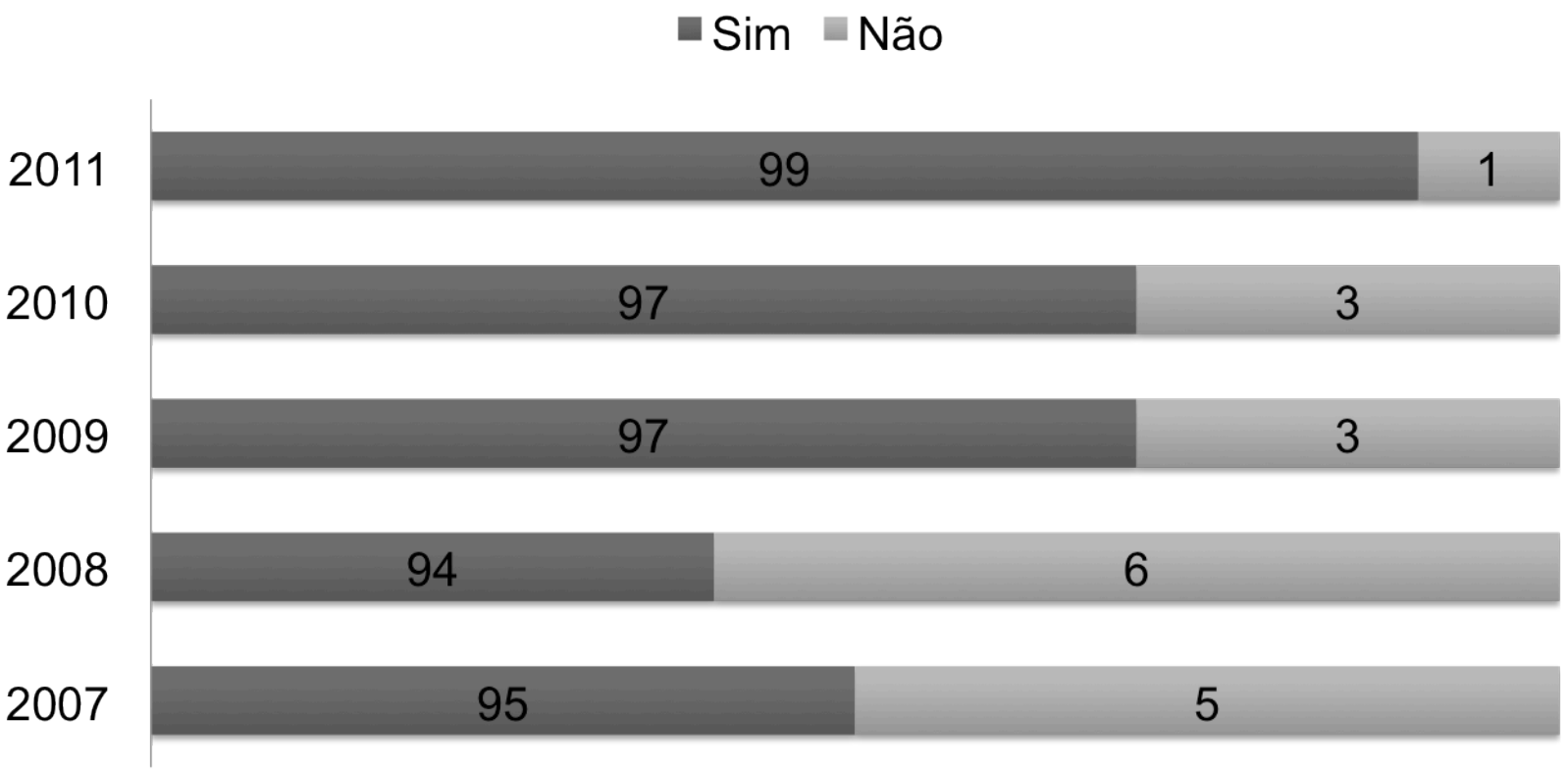
Domicílios com Computador



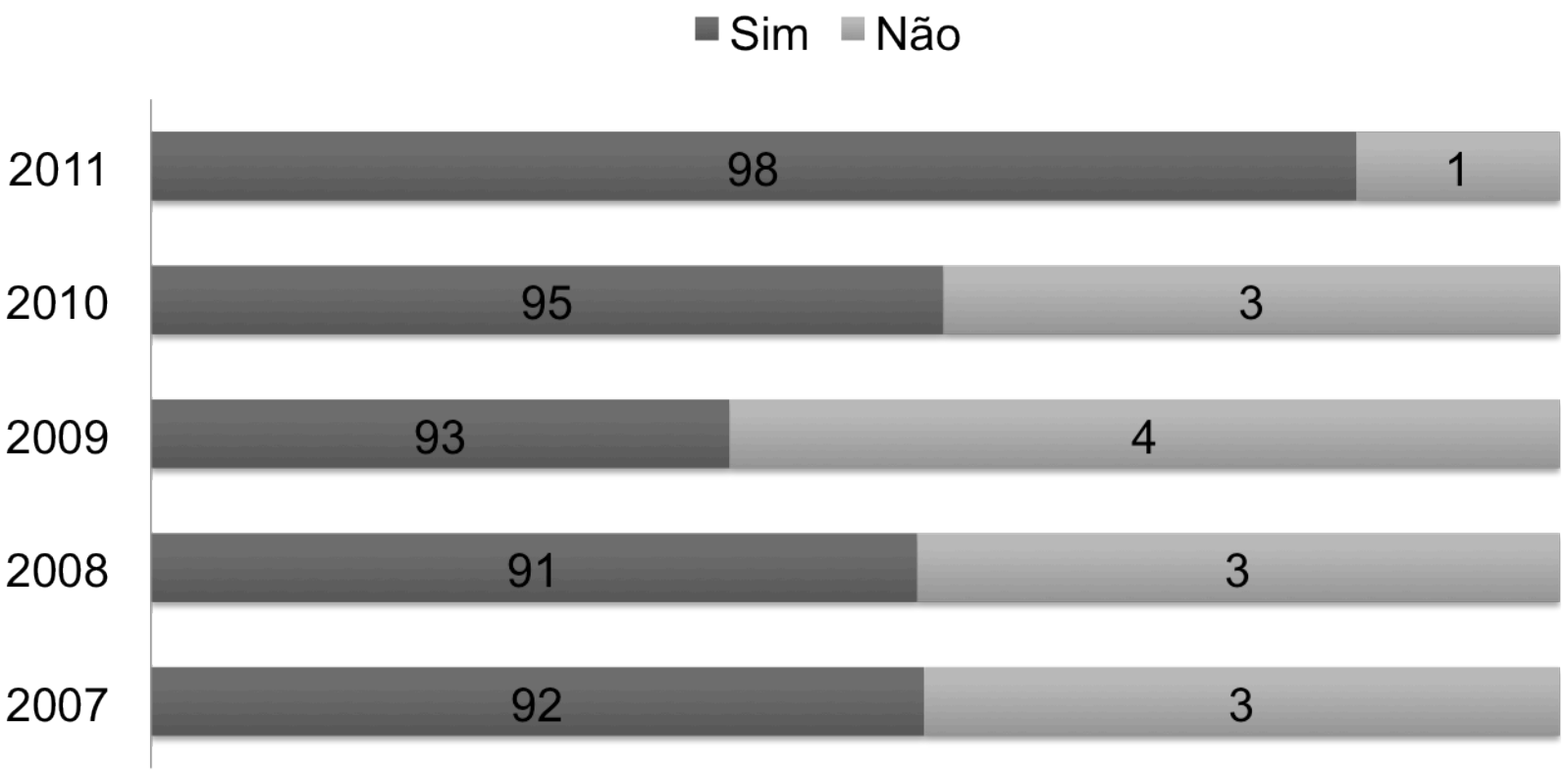
Domicílios com Acesso à Internet



Empresas - Uso de Computadores



Empresas - Uso da Internet



Segurança X Empresas (1/5)

Problemas de Segurança Identificados	
Vírus	59 %
Trojan	50 %
Worms ou *bots*	19 %
Ataque ao servidor Web	10 %
Furto de *notebooks*, PDAs ou outros dispositivos móveis	8 %
Ataque de negação de serviço (DoS)	6 %
Fraude facilitada pelas TIC (como furto de identidade, *phishing* ou outras fraudes financeiras pela Internet)	5 %
Declarou não ter identificado problemas de segurança	**29 %**
Não sabe/ Não respondeu	2 %

Segurança X Empresas (2/5)

Medidas de Apoio à Segurança Adotadas	
Política de segurança ou de uso aceitável dos recursos de TIC	37 %
Programa de treinamento para funcionário em seg. da informação	21 %
Não adotou nenhuma medida de apoio à segurança	**54 %**
Não sabe/ Não respondeu	3 %

Segurança X Empresas (3/5)

Tecnologias de Segurança Adotadas	
Antivírus	97 %
Antispam	73 %
Antispyware	65 %
Firewall	**62 %**
IDS	**35 %**
Outros	1 %
Nenhum desses	2 %
Não sabe/ Não respondeu	-

Segurança X Empresas (4/5)

Tecnologias Adotadas para Proteção de Dados	
Backup interno de dados sobre as operações da empresa	79 %
Uso de criptografia de dados armazenados em servidores ou *desktops*	27 %
Backup de dados *offsite*	27 %
Uso de criptografia para proteção de dados em mídias externas, *notebooks*, PDAs ou outros dispositivos móveis	**20 %**
Outros	-
Nenhum desses	15 %

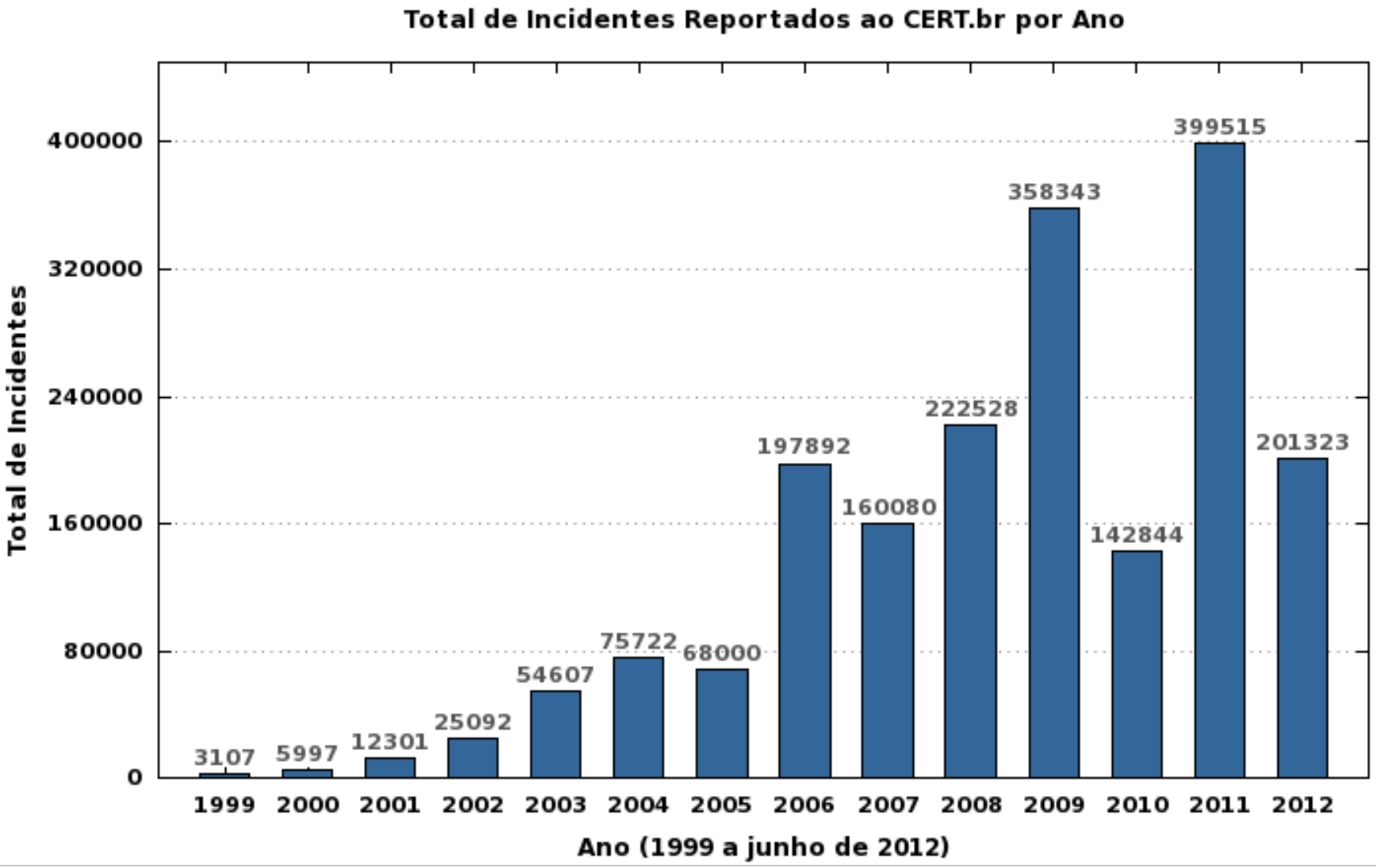
Segurança X Empresas (5/5)

Empresas que Ofereceram Treinamento em TIC para Funcionários	
Treinamento para usuários de computador e Internet	32%
Treinamento para especialistas em TI	17%
Nenhum desses	**64%**
Não sabe / Não respondeu	1%

Evolução dos Incidentes de Segurança

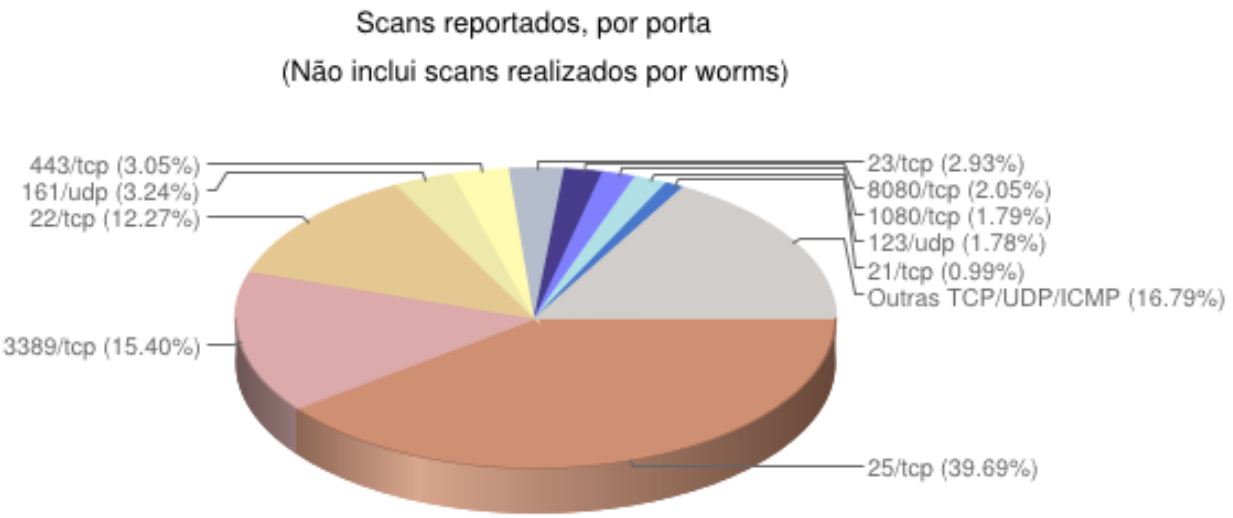
Fonte: Estatísticas CERT.br
http://www.cert.br/stats/incidentes/

Incidentes reportados ao CERT.br – até junho/2012



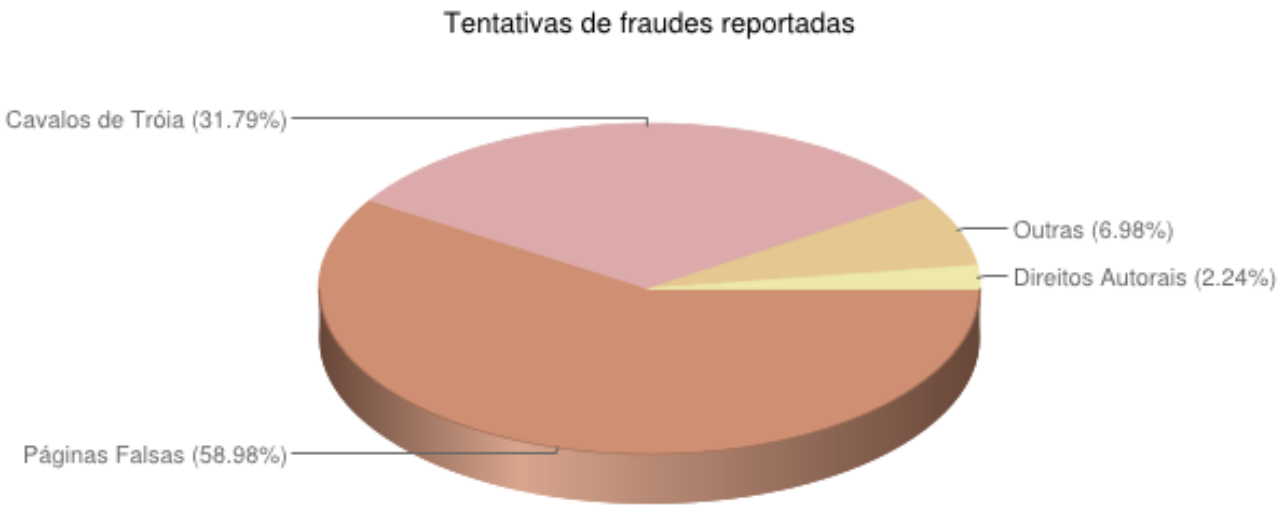
Tipos de ataque – abril a junho de 2012

Scans reportados – abril a junho de 2012



- **Força bruta:**
  - **SSH, TELNET, FTP, VNC, etc**
  - **Alvos:**
    - **senhas fracas, senhas padrão, contas temporárias**
  - **Pouca monitoração permite ao ataque perdurar por horas/dias**

Tentativas de fraudes – abril a junho de 2012



- ***Spams*** **em nome de diversas entidades/temas variados**
  - ***Links*** **para** ***trojans*** **hospedados em diversos** ***sites***
  - **Vítima raramente associa o** ***spam*** **com a fraude**
- **Retorno de páginas falsas**
  - **via** ***spams*** **em nome das instituições financeiras e/ou de comércio eletrônico**
  - **muitas envolvem alteração do arquivo hosts das máquinas**

Considerações Gerais

Considerações Gerais (1/3)

- **Grande quantidade de computadores e serviços vulneráveis**
  - **serviços sendo disponibilizados sem proteção**
  - **pressão para lançamento de novos produtos**
    - **sem os devidos testes**

- **Criminosos:**
  - **com pouco conhecimento**
    - **uso de *kits* prontos**
  - **migrando para onde estão os negócios**
  - **motivação financeira**

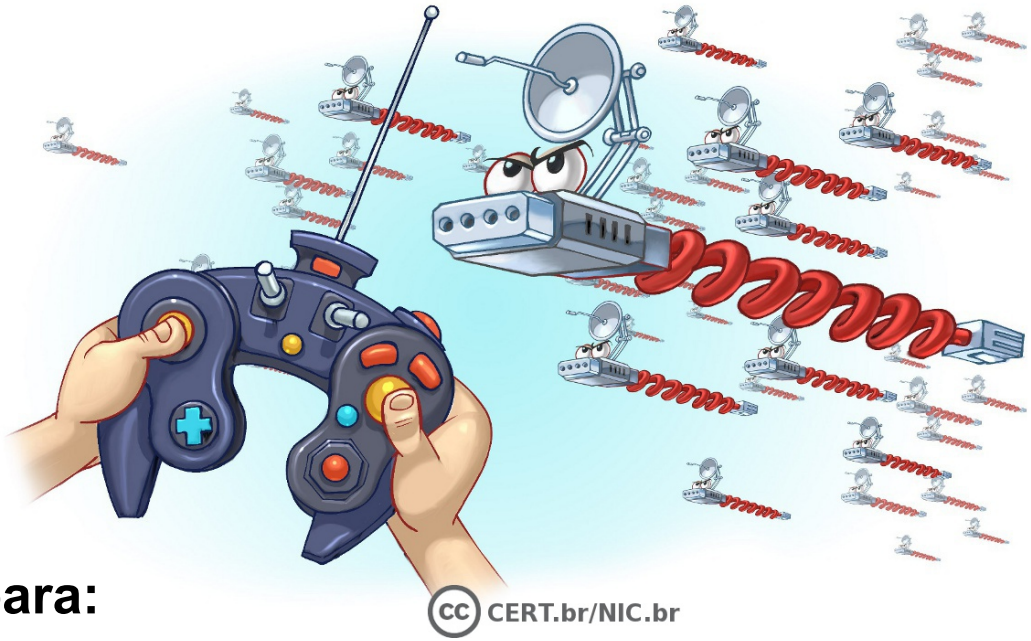
Considerações Gerais (2/3)

- **Internet cada vez mais faz parte do dia a dia das pessoas, principalmente por meio de:**
  - **acesso a serviços**
  - **redes sociais**
  - **dispositivos móveis**

- **Usuários:**
  - **não são especialistas**
  - **mais fáceis de serem atacados (engenharia social)**
  - **grande quantidade de informações:**
    - **pessoais: senhas, números de cartão de crédito**
    - **profissionais: segredos de mercado, documentos**
- **Uso errado do termo “virtual”**

Considerações Gerais (3/3)

- ***Botnets***



- **Computadores usados para:**
  - **ataques de negação de serviço (DoS)**
  - **disseminação de *spams***
  - **propagação de códigos maliciosos**
  - **repositório de dados fraudulentos**
  - **esconder a identidade do atacante**
  - **extorsão**

Prevenção

Proteger o Computador

- **Manter o computador seguro:**
  - **com todas as atualizações aplicadas**
  - **com todos os programas instalados com as versões mais recentes**
- **Usar mecanismos de segurança**
  - ***firewall* pessoal, *antimalware, antiphishing*, *antispam***
  - **complementos, extensões, *plugins***
- **Usar apenas programas originais**
- **Usar as configurações de segurança já disponíveis**
- **Ser cuidadoso ao instalar aplicativos desenvolvidos por terceiros**

Manter uma Postura Preventiva

- **Não acessar *sites* ou seguir *links***
  - **recebidos de mensagens eletrônicas**
  - **em páginas sobre as quais não se saiba a procedência**

- **Não confiar apenas no remetente da mensagem, pois ela pode ter sido enviada de:**
  - **máquinas infectadas**
  - **contas falsas ou invadidas**

- **Proteger a privacidade, evitando divulgar:**
  - **dados pessoais ou de familiares e amigos**
  - **informações sobre seu cotidiano**
  - **informações sensíveis, como:**
    - **senhas**
    - **números de cartão de crédito**

Proteger Contas e Senhas (1/2)

- **Utilizar senhas contendo:**
  - **grande quantidade de caracteres**
  - **diferentes tipos de caracteres**
  - **números aleatórios**

- **Não usar:**
  - **sequências de teclado**
  - **dados pessoais:**
    - **nome, sobrenome, contas de usuário, números de documentos, placas de carros, números de telefones**
    - **informações que possam ser coletadas em *blogs* e redes sociais**
  - **palavras que façam parte de listas**
    - **nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc.**

Proteger Contas e Senhas (2/2)

- **Dicas de elaboração**
  - **selecionar caracteres de uma frase**
    - **“O Cravo brigou com a Rosa debaixo de uma sacada” ➔ ”?OCbcaRddus”**
  - **utilizar uma frase longa**
    - **“1 dia ainda verei os aneis de Saturno!!!”**
  - **fazer substituições de caracteres:**
    - **“Sol, astro-rei do Sistema Solar” ➔ “SS0l, asstrr0-rrei d0 SSisstema SS0larr”**
- **Trocar regularmente as senhas**
- **Usar o usuário “administrador” o mínimo necessário**

Manter-se atualizado (1/2)

Cartilha de Segurança para Internet
http://cartilha.cert.br/

RSS
http://cartilha.cert.br/rss/cartilha-rss.xml

Twitter
http://twitter.com/certbr

Manter-se atualizado (2/2)

Portal Internet Segura

http://www.internetsegura.br/

INTERNET SEGURA.BR

Campanha Antispam.br

http://www.antispam.br/

Perguntas?

Miriam von Zuben
miriam@cert.br

- **CGI.br - Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do .br**
  http://www.nic.br/
- **CERT.br -Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/