Principais Ameaças na Internet e Recomendações para Prevenção

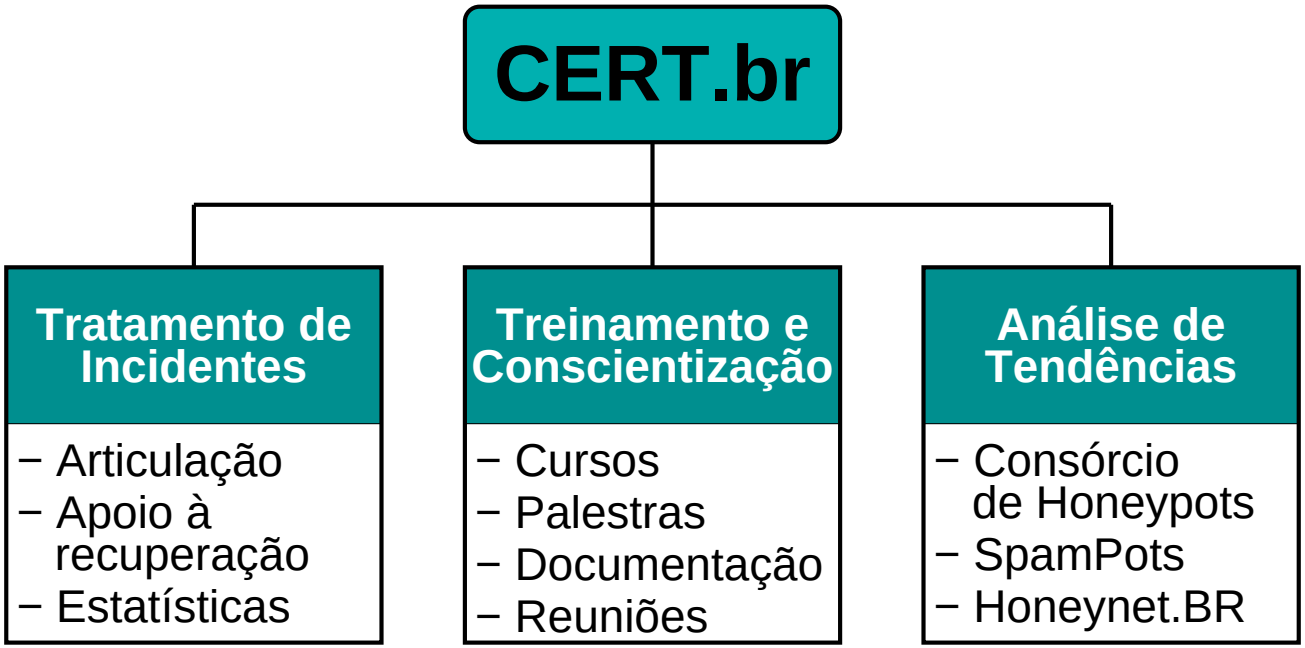
Cristine Hoepers
cristine@cert.br
Klaus Steding-Jessen
jessen@cert.br

Esta Apresentação:
http://www.cert.br/docs/palestras/

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

Sobre o CERT.br

Criado em 1997 como ponto focal nacional para tratar incidentes de segurança relacionados com as redes conectadas à Internet no Brasil



FIRST Improving Security Together MEMBER

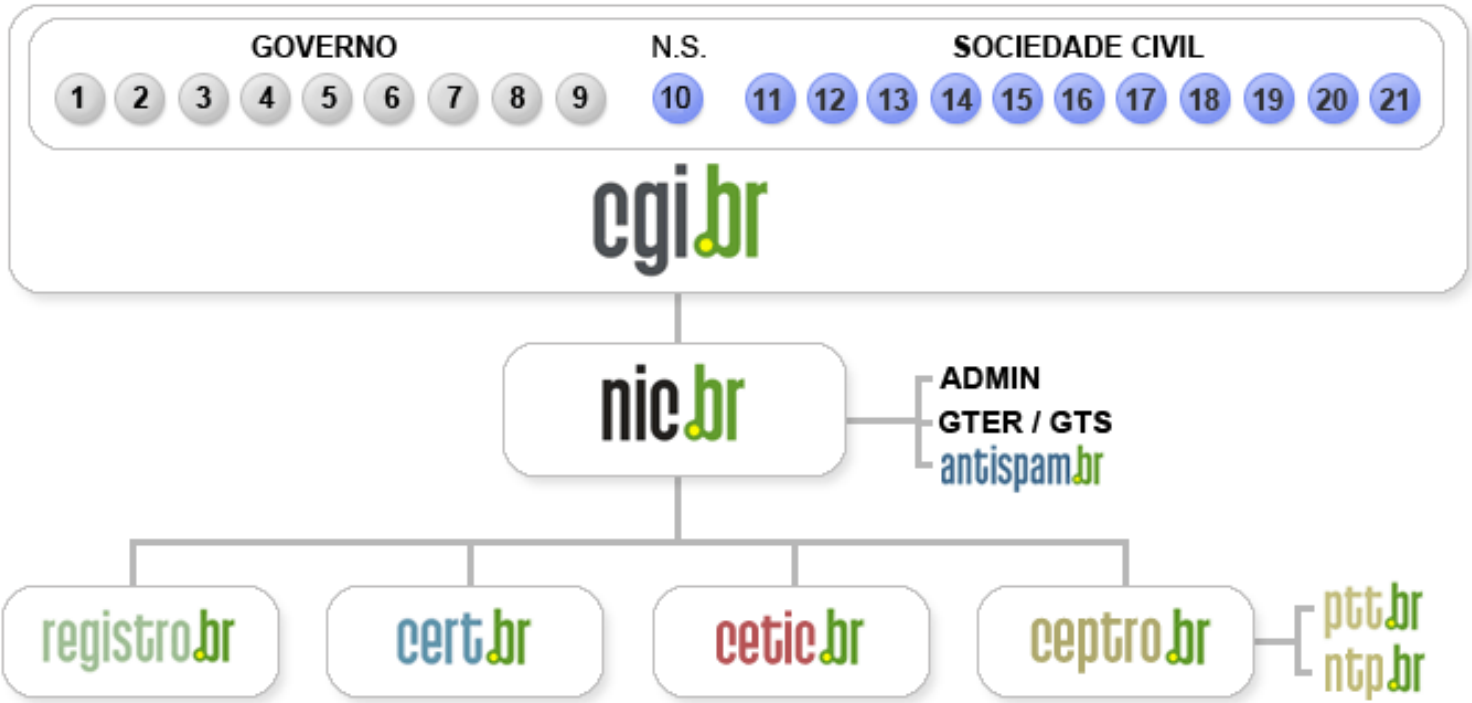
APWG

SEIPartner CERT Courses

The Honeynet PROJECT®

http://www.cert.br/missao.html

Estrutura do CGI.br



01- Ministério da Ciência e Tecnologia
02- Ministério das Comunicações
03- Casa Civil da Presidência da República
04- Ministério da Defesa
05- Ministério do Desenvolvimento, Indústria e Comércio Exterior
06- Ministério do Planejamento, Orçamento e Gestão
07- Agência Nacional de Telecomunicações (Anatel)
08- Conselho Nacional de Desenvolvimento Científico e Tecnológico
09- Fórum Nacional 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

Atribuições do CGI.br

Entre as diversas atribuições e responsabilidades definidas no Decreto Presidencial nº 4.829, 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**

Agenda

Motivação

Incidentes de Segurança mais Comuns

Pesquisa TIC Domicílios

Evolução dos Problemas de Segurança

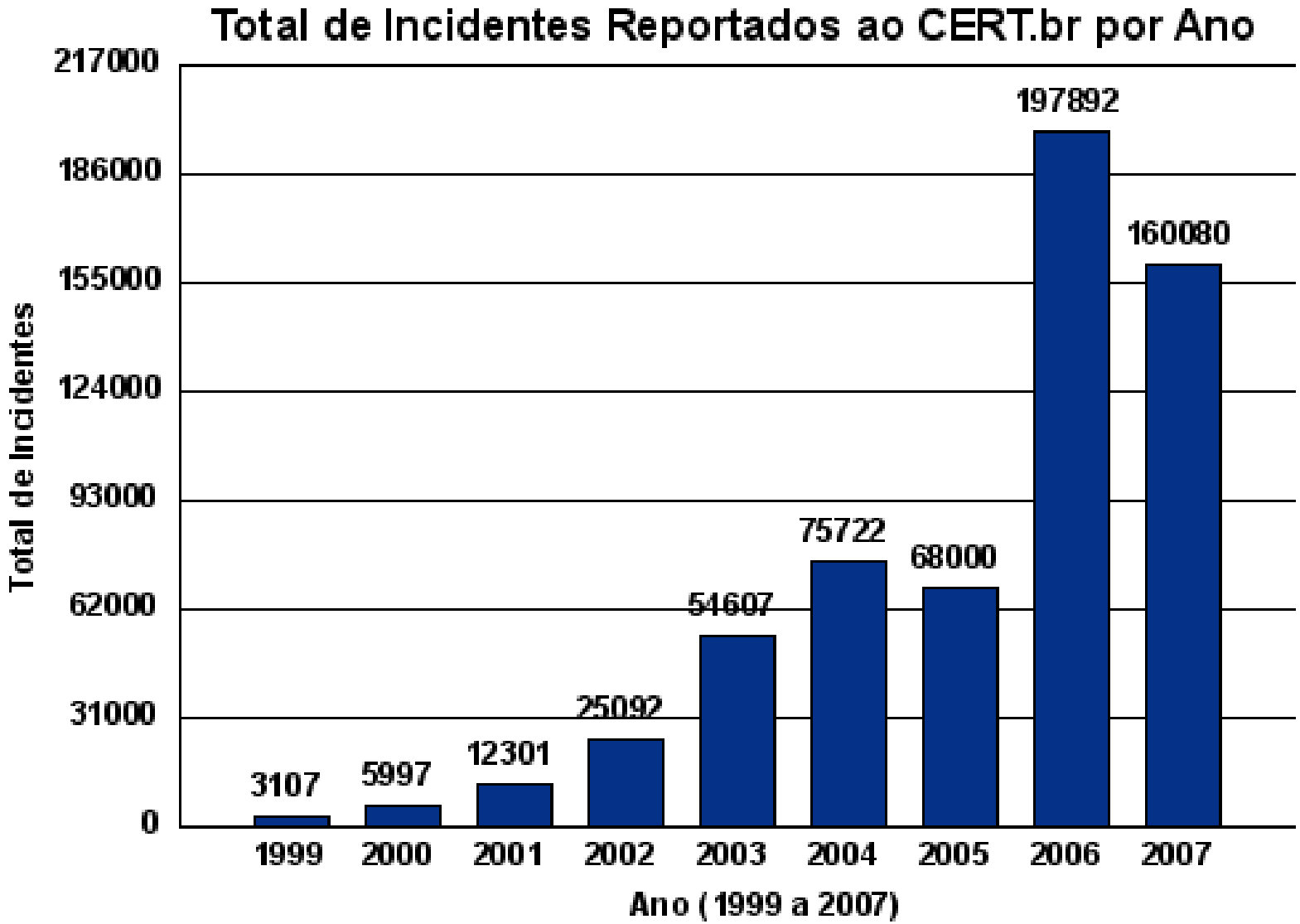
Prevenção

Referências

Motivação

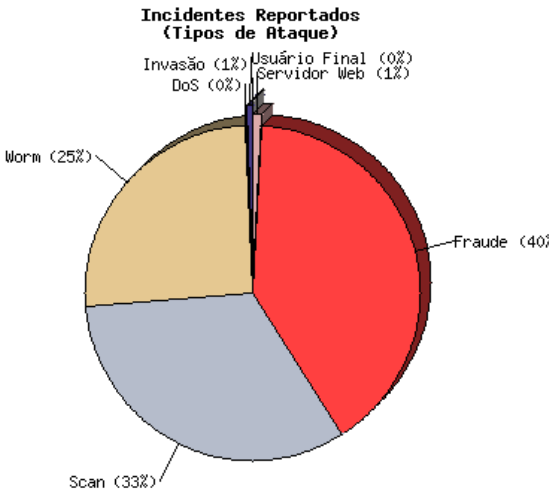
- Analisar dados sobre segurança na Internet, para entendermos o problema
- Discutir a evolução dos problemas de segurança desde a concepção da Internet até os dias atuais
- Discutir possíveis formas de proteção, isto é, o que podemos fazer para usar a Internet de modo mais seguro

Incidentes de Segurança: 1999–2007

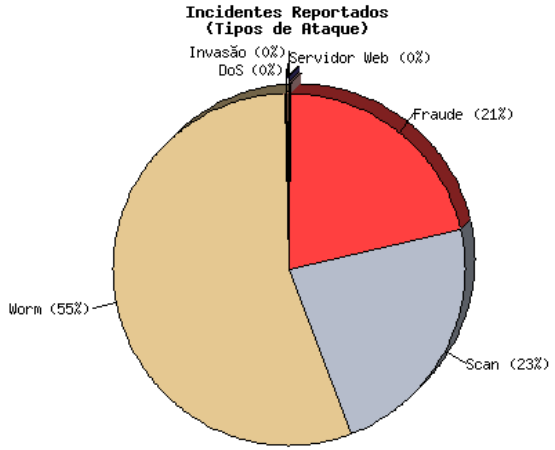


Incidentes de Segurança: Categorias

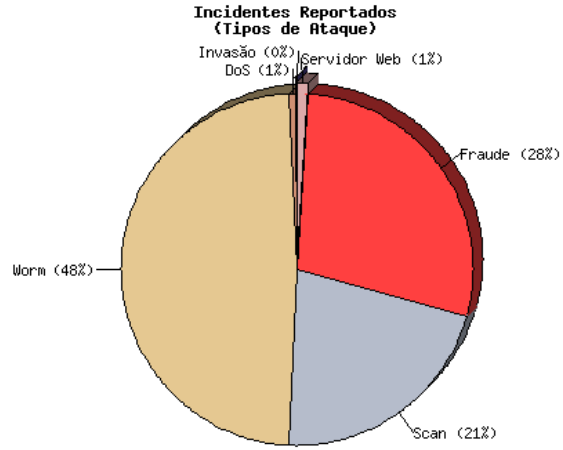
2005



2006



2007



Totais da categoria fraude:

2004	**4.015 (05%)**
2005	**27.292 (40%)**
2006	**41.776 (21%)**
2007	**45.298 (28%)**

Características das tentativas de fraude:

- **Em nome das mais variadas instituições e com tópicos diversos**
- **Com links para cavalos de tróia**

Totais da categoria *worm* (engloba *bots*):

2004	**42.267 (55%)**
2005	**17.332 (25%)**
2006	**109.676 (55%)**
2007	**77.473 (48%)**

Maior influência no aumento de 191% no total de 2005 para 2006 e na queda de 19% de 2006 para 2007.

Pesquisa TIC Domicílios

Problemas de Segurança Encontrados:

	Nenhum	Vírus	Vírus c/ Dano	Abuso de Informação	Fraude Bancária	Fraude c/ Cartão	Outro	Não Sabe
2005	40,99	19,64	7,13	1,67	0,94	—	1,10	0,24
2006	44,46	20,34	7,89	1,85	0,60	0,26	1,14	29,95

Medidas de Segurança Adotadas:

	Antivírus	*Firewall* Pessoal	Anti-*Spyware*	Nenhuma Medida	Não sabe
2005	69,76	19,33	22,09	—	—
2006	70,24	14,25	13,93	16,40	10,87

Freqüência de Atualização do Antivírus

	Diária	Semanal	Mensal	Trimestral	Não atualizou	Não sabe
2005	21,11	27,01	17,37	3,47	31,03	—
2006	25,99	23,69	12,77	3,66	14,50	19,38

Fonte: CETIC.br
http://www.cetic.br/

Evolução dos Problemas de Segurança

Final dos Anos 60

Internet

- Projeto não considera implicações de segurança
- Comunidade de pesquisadores
- Confiança

Anos 80

Invasores com

- Alto conhecimento
- Dedicação por longos períodos para realização de poucos ataques

"*Cookoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*", Cliff Stoll

- 30+ sistemas invadidos
- Contas/senhas óbvias
- Vulnerabilidades em *softwares*
- Tempo e persistência

Final dos Anos 80

- Primeiro *worm* com maiores implicações de segurança
  - Criado por Robert Morris Jr.
  - Explorava a combinação de vulnerabilidades no sendmail, finger e em configurações dos *"r" services*
  - Mais de 6000 computadores atingidos
- Aproximadamente 10% da Internet na época
- Mobilização em torno do tema segurança
- Criação do CERT/CC 15 dias após

ftp://coast.cs.purdue.edu/pub/doc/morris_worm/
http://www.cert.org/archive/pdf/03tr001.pdf
http://www.ietf.org/rfc/rfc1135.txt

Anos 1991–2001

- Início da utilização da “engenharia social” em grande escala
- Primeiros ataques remotos aos sistemas
- Popularização de: cavalos de tróia, furto de senhas, varreduras em busca de máquinas vulneráveis, captura de informações digitais (*sniffers*), ataques de negação de serviço, etc
- Primeiras ferramentas automatizadas para
  - Realizar invasões
  - Ocultar a presença dos invasores (*rootkits*)
- Sofisticação no processo de controle das ferramentas

Anos 2002–2005

- Explosão no número de códigos maliciosos com diversos fins
  - *worms*, *bots*, cavalos de tróia, vírus, *spyware*
- Códigos com múltiplas funcionalidades
  - Múltiplos vetores de ataque, código eficiente, aberto e facilmente adaptável
- Permitem controle remoto
- Praticamente não exigem interações por parte dos invasores

Situação Atual (1/3)

Características dos Ataques

- Crime organizado
  - Aliciando *spammers* e invasores
  - Injetando dinheiro na "economia *underground*"
- *Botnets*
  - Usadas para envio de *scams*, *phishing*, invasões, esquemas de extorsão
- Redes mal configuradas sendo abusadas para realização de todas estas atividades
  - sem o conhecimento dos donos
- **Alvo migrou para usuários finais**

Situação Atual (2/3)

Características dos Atacantes

- Em sua maioria pessoal com pouco conhecimento técnico que utiliza ferramentas prontas
- Trocam informações no *underground*
- Usam como moedas de troca
  - Senhas de administrador/`root`
  - Novos *exploits*
  - Contas/senhas de banco
  - Números de cartão de crédito
  - *bots*/*botnets*

Situação Atual (3/3)

Perfil dos Ataques / Principais Ameaças

- Sistemas operacionais e *softwares* desatualizados, vulnerabilidades freqüentes
- Códigos maliciosos explorando essas vulnerabilidades em curto espaço de tempo
- Ferramentas automatizadas de ataque
- Vírus / *worms* / *bots*
- Ataques de força bruta
- Atacantes + *spammers*
- Fraudes / *scams* / *phishing* / crime organizado

Histórico das Fraudes no Brasil

2001 *Keyloggers* enviados por *e-mail*, ataques de força bruta

2002–2003 Casos de *phishing* e uso disseminado de servidores DNS comprometidos

2003–2004 Aumento dos casos de *phishing* mais sofisticados

- Dados eram enviados dos *sites* falsificados para *sites* coletores
- *Sites* coletores processavam os dados e os enviavam para contas de *e-mail*

2005–2006 *Spams* usando nomes de diversas entidades e temas variados

- *Links* para cavalos de tróia hospedados em diversos *sites*
- Vítima raramente associa o *spam* recebido com a fraude financeira

2007–hoje *downloads* involuntários, via códigos JavaScript, ActiveX, etc, em máquinas vulneráveis

- continuidade das tendências de 2005–2006

Prevenção

Manter o Sistema Atualizado

Instalar a última versão e aplicar as correções de segurança (*patches*)

- Sistema operacional
  - o computador está ligado na hora da atualização automática?
- Aplicativos
  - navegador, processador de textos, leitor de *e-mails*, visualizador de imagens, PDFs e vídeos, etc
- *Hardware*
  - *firmware* de *switches*, bases *wireless*, etc

Utilizar Programas de Segurança

- *firewall* pessoal
- antivírus
  - atualizar as assinaturas diariamente
- anti-*spyware*
- anti-*spam*
- extensões em navegadores
  - gerência de JavaScript, *cookies*, etc

Melhorar a Postura On-line (1/3)

- Não acessar *sites* ou seguir *links*
  - recebidos por *e-mail*
  - recebidos por serviços de mensagem instantânea
  - presentes em páginas sobre as quais não se saiba a procedência
- Receber um *link* ou arquivo de pessoa ou instituição conhecida não é garantia de confiabilidade
  - códigos maliciosos se propagam a partir das contas de máquinas infectadas
  - fraudadores se fazem passar por instituições confiáveis

Melhorar a Postura On-line (2/3)

Não fornecer em páginas *Web*, *blogs* e *sites* de redes de relacionamentos:

- seus dados pessoais ou de familiares e amigos (*e-mail*, telefone, endereço, data de aniversário, etc)
- dados sobre o seu computador ou sobre os *softwares* que utiliza
- informações sobre o seu cotidiano
- informações sensíveis, como senhas e números de cartão de crédito

Melhorar a Postura On-line (3/3)

Precauções com contas e senhas

- utilizar uma senha diferente para cada serviço/*site*
- evitar senhas fáceis de adivinhar
  - nome, sobrenomes, números de documentos, placas de carros, números de telefones, datas que possam ser relacionadas com você ou palavras que façam parte de dicionários
- usar uma senha composta de letras, números e símbolos
- utilizar o usuário Administrador ou `root` somente quando for estritamente necessário
- criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam seu computador

Informar-se e Manter-se Atualizado – 1

http://cartilha.cert.br/

Núcleo de Informação e Coordenação do Ponto br

Início Dicas Download Checklist Glossário Livro

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

cgi.br NIC.br Registro

Cartilha de Segurança para Internet 3.1

Livro Completo

A partir da versão 3.1 a Cartilha de Segurança para Internet passou a ser editada também como livro. Nesta página você encontra o prefácio do Livro e o arquivo para download.

Prefácio

A Cartilha de Segurança para Internet é um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças.

Produzido pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br, com o apoio do Comitê Gestor da Internet no Brasil – CGI.br, o documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

Livro Completo para download (886 KB)

Cartilha de Segurança para Internet, versão 3.1 / CERT.br – São Paulo: Comitê Gestor da Internet no Brasil, 2006.

ISBN: 978-85-60062-06-5
ISBN: 85-60062-06-8

Informar-se e Manter-se Atualizado – 2

http://www.antispam.br/videos/

Referências

- Esta Apresentação
  http://www.cert.br/docs/palestras/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br
  http://www.cert.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Antispam.br
  http://www.antispam.br/
- Centro de Estudos sobre as Tecnologias da Informação e da Comunicação – CETIC.br
  http://www.cetic.br/