Segurança em Redes Sociais

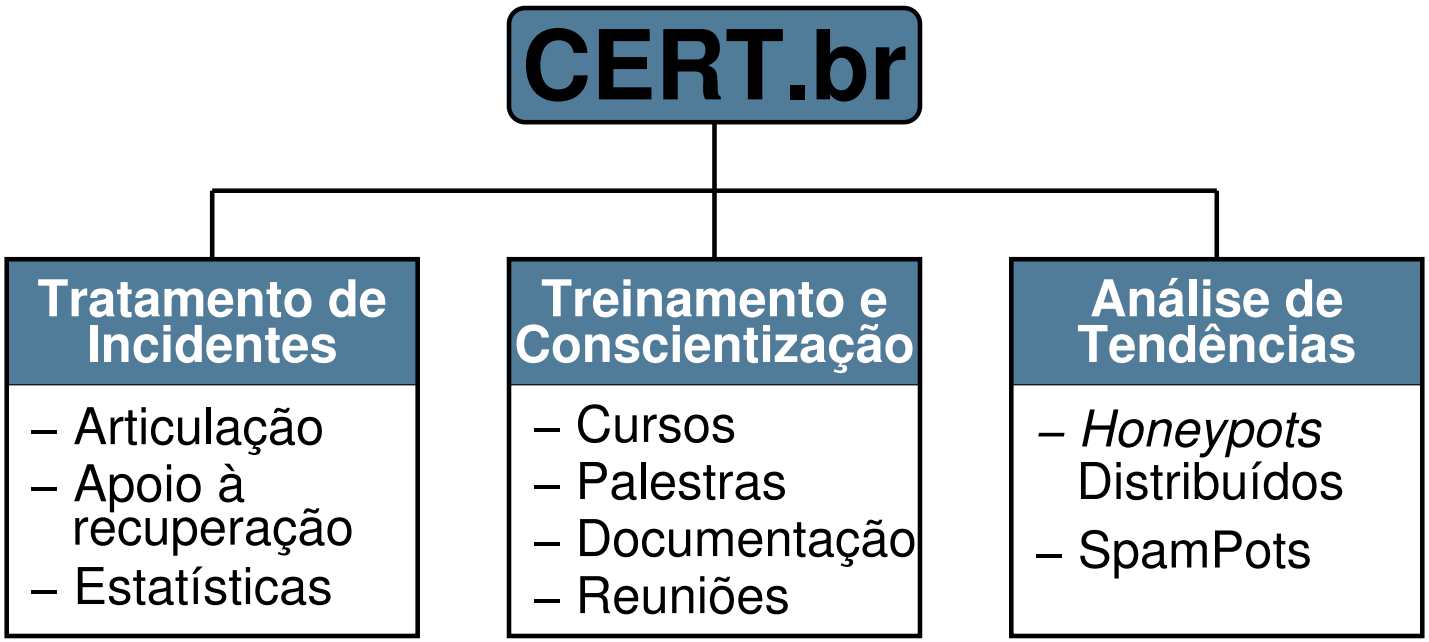
Luiz Eduardo Roncato Cordeiro
cordeiro@cert.br

Miriam von Zuben
miriam@cert.br

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 segurançaa relacionados com as redes conectadas à Internet no Brasil



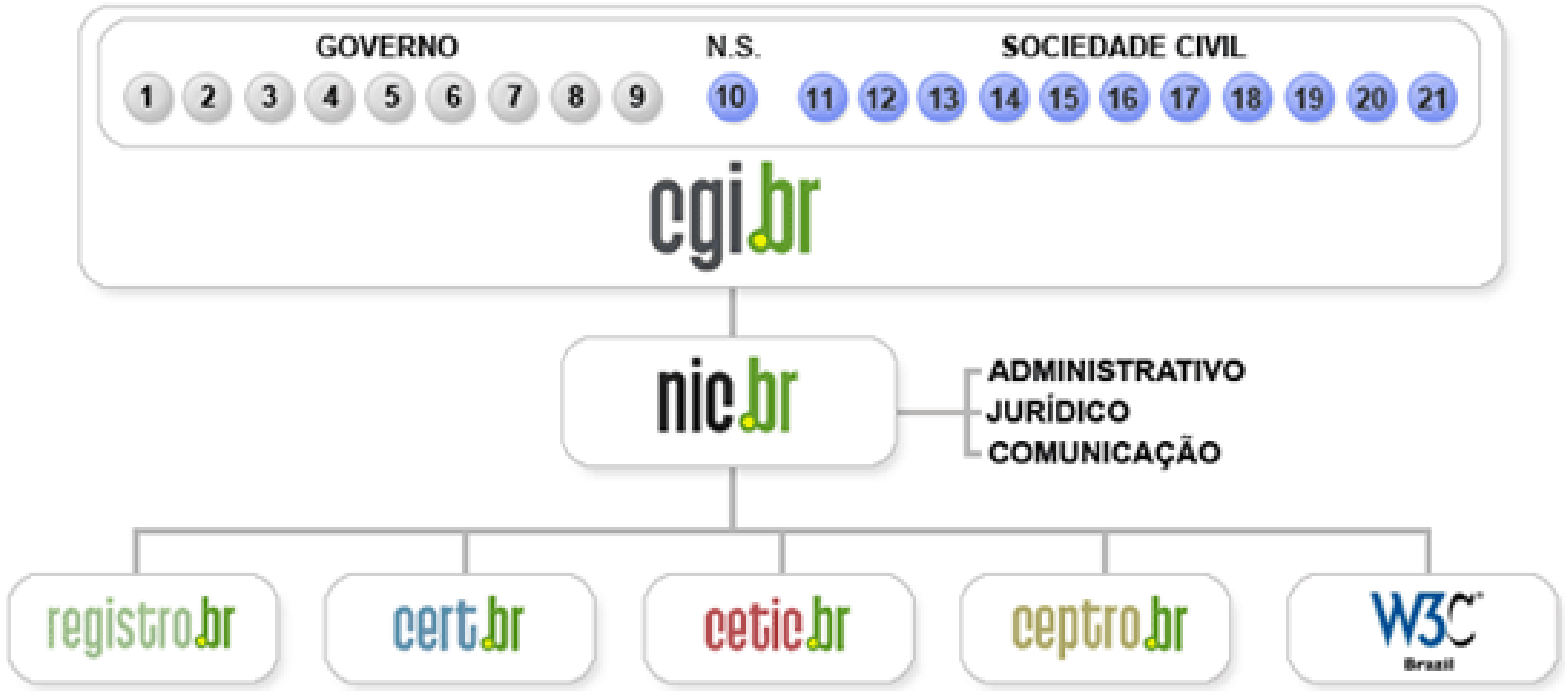
FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon

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

Estrutura do CGI.br



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

10- Notório Saber
11- Provedores de Acesso e Conteúdo
12- Provedores de Infra-estrutura de Telecomunicações
13- Indústria TICs (Tecnologia da Informação e Comunicação) e Software
14- Empresas Usuárias
15-18- Terceiro Setor
19-21- Academia

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

Redes Sociais

Principais Riscos

Prevenção

Referências

Redes Sociais

Permitem que os usuários:

- criem perfis
- interajam entre si
- se agrupem em comunidades, de acordo com afinidades, interesses, características e objetivos em comum

Algumas características:

- rápida disseminação de informações
- facilidade de uso em telefones celulares, *smartphones* e *tablets*
- grande utilização de *links* curtos
- tendência em confiar em mensagens de conhecidos

Principais Riscos

- Disseminação de códigos maliciosos
- Furto de identidade
  - *phishing*
  - perfis falsos
  - ataques de força bruta
  - reutilização de senhas
- Uso indevido de perfil oficial
- Vazamento de informações
- Outros riscos

Disseminação de Códigos Maliciosos

- 2005: Sammy *Worm*
  - alvo: usuários do Myspace
  - exploração de vulnerabilidade de *Cross Site Scripting* (XSS)
- 2008: Koobface *Worm* (anagrama de Facebook)
  - alvo: usuários do Facebook e do MysSpace
  - envio de mensagens, através de conta comprometida, informando a necessidade da atualização do programa *flash*
- 2009: Stalkdaily *Worm*
  - alvo: usuários do Twitter
  - envio de mensagem solicitando o acesso ao *site* stalkdaily.com
  - infecção ocorria quando este *site* era acessado

Furto de Identidade (1/2)

Ataques de força bruta:

- muitos ainda utilizam senhas:
  - curtas
  - baseadas em dados pessoais
  - baseadas em palavras de dicionários
  - baseadas em sequências de teclado

Reutilização de senhas:

- uma única senha utilizada para acessar várias redes sociais ou serviços

Furto de senhas:

- programas maliciosos (*malware*)
- página falsa (*phishing*)

Furto de Identidade (2/2)

Criação de perfis falsos:

- inevitáveis — contas são criadas em segundos
- podem ser percebidos como perfis oficiais
- informações disponibilizadas em uma rede social podem ser utilizadas para a criação de perfil falso em outra rede
- perfil falso utilizado para obter informações da rede de relacionamento do usuário
- engenharia social
- retirá-los do ar pode ser difícil e demorado

Phishing:

- exploram a “confiança” que os seguidores/amigos depositam no usuário que teve a conta invadida
  - mensagens vindas de conhecidos são tidas como confiáveis

Pouca Proteção do Computador Pessoal

Problemas de Segurança Encontrados:

	Nenhum	Vírus ou outro programa malicioso	Uso indevido de informações	Fraude financeira	Outro	Não sabe
2008	68	28	1	1	ND	3
2009	63	35	1	1	ND	1

Medidas de Segurança Adotadas:

	Antivírus	*Firewall* pessoal	Outro programa	Nenhuma medida
2008	70	10	4	28
2009	75	9	4	22

Fonte: Pesquisa TIC Domícilios – CETIC.br (http://www.cetic.br/)

Problemas mais Frequentes nas Empresas

Problemas de Segurança Identificados:

	Vírus	*Trojans*	*Worms* ou *Bots*	Fraude	Não identificados	NS/NR
2008	55	48	19	6	33	1
2009	63	53	21	6	26	1

Tecnologias de Segurança Adotadas:

	Antivírus	*Antispam*	Anti-*spyware*	*Firewall*	Não possui	NS/NR
2008	98	74	68	64	1	1
2009	98	73	66	61	2	-

Medidas de Apoio à Segurança Adotadas:

	Política de segurança ou de uso aceitável dos recursos de TIC	Política de treinamento para funcionário em segurança da informação	Nenhuma medida de apoio adotada	NS/NR
2008	33	22	58	2
2009	38	21	54	3

Fonte: Pesquisa TIC Empresas – CETIC.br (http://www.cetic.br/)

Uso Indevido de Perfil Oficial (1/3)

- Perfil oficial utilizado para o envio de opiniões pessoais
  - problemas causados geralmente por imprudência ou distração
  - usuário acessando ao mesmo tempo perfil pessoal e oficial
  - pode denegrir a imagem da instituição
  - rápida disseminação
  - impossibilidade de exclusão

Exemplos:

- Supremo Tribunal Federal (15/02/2011)

STF_oficial Ouvi por aí: "agora que o Ronaldo se aposentou, quando será que o Sarney vai resolver pendurar as chuteiras?"

about 1 hour ago via web

Retweeted by you and 100+ others

Uso Indevido de Perfil Oficial (2/3)

- Secretaria de Estado de Cultura de São Paulo (29/03/2011)

Uso Indevido de Perfil Oficial (3/3)

- Chrysler

Vazamento de Informações

- Discussões em reuniões
- Detalhes técnicos de produtos, processos ou rede
- Abertura ou fechamento de *sites*
- Lançamento de novas versões de programas, serviços ou produtos
- Informações sobre batidas policiais
- Notícias: Morte de Osama Bin Laden

@keithurbahn
Keith Urbahn

So I'm told by a reputable person they have killed Osama Bin Laden. Hot damn.

6 hours ago via Twitter for BlackBerry® ☆ Favorite ↩ Retweet ↩ Reply

Outros Riscos

- Dificuldade de diferenciar opinião pessoal da profissional
- Riscos na segurança física devido ao excesso de informação disponíveis
  - furto de bens
  - sequestro
    - filho de Eugene Kaspersky, da Kaspersky Labs, foi sequestrado em abril/2011
- Usuários insatisfeitos
- SCAMs são muito efetivos quando usam a imagem de uma instituição
- Difamações em redes sociais podem:
  - gerar dúvidas nos consumidores ou usuários de serviços, fazendo com que percam a confiança
  - provocar a queda no moral da instituição
  - aumentar a dificuldade no recrutamento de funcionários

Prevenção

Cuidados com a Imagem

- Perfil oficial:
  - prender-se a fatos
  - treinar a pessoa responsável
  - envolver mais de uma pessoa, departamento
  - ser pró-ativo, não esperar o problema aparecer
    - garantir que artigos positivos sejam disseminados, discutidos e referenciados
    - criar uma cadeia de “defensores”
    - monitorar continuamente
- Funcionários que representam a empresa devem ter cuidados especiais
  - incluindo os parceiros e terceirizados
- Como remover uma conta falsa?
  - cada rede social tem políticas e procedimentos próprios
  - listas de políticas atuais em:

    http://www.brandprotect.com/resources/Username-Policies.pdf

Manter a Privacidade

- Não divulgar informações pessoais, internas ou confidenciais
  - nome, endereço, número de telefone, etc.
- Restringir o acesso a perfil, mensagens, fotos e vídeos
- Ser seletivo ao aceitar amigos/seguidores
  - quanto maior a rede de contatos, maior o número de pessoas com acesso às informações
- Apagar e restringir recados

Dicas para perfis de executivos:

- Ser cuidadoso ao se associar a comunidades
  - comunidades permitem deduzir informações sobre rotina, hábitos e classe social
- Utilizar opções de navegar anonimamente
  - pode bloquear o histórico de acesso ao seu perfil
- Não fornecer informações sobre localização geográfica

Respeitar a Privacidade

- Não fornecer informações de outras fontes
- Não repassar mensagens de outras fontes, sem autorização
- Não divulgar dados em que pessoas apareçam sem autorização prévia
  - documentos, fotos, vídeos, etc
  - principalmente crianças
- Não disponibilizar dados copiados de perfis que restrinjam o acesso

Proteção contra *Phishing* e Códigos Maliciosos (1/2)

- Ser cuidado ao acessar *links* reduzidos
- Não acessar *sites* ou seguir *links*
  - recebidos através de mensagens eletrônicas
  - obtidos em páginas sobre as quais não se saiba a procedência
- Desligar a opção de recebimento de notificações via *e-mail*
  - para evitar a disseminação de códigos maliciosos
  - para facilitar a identificação de mensagens falsas

Proteção contra *Phishing* e Códigos Maliciosos (2/2)

- Não considerar que mensagens vindas de conhecidos são sempre confiáveis
  - fraudadores se fazem passar por instituições confiáveis
  - códigos maliciosos podem ser enviados de computadores infectados

- Ser cuidadoso ao utilizar computadores de terceiros
  - *lan houses*, *cyber cafes*, etc.

Proteção de Contas e Senhas

- Utilizar senhas diferentes para diferentes serviços/*sites*
- Evitar senhas fáceis de serem descobertas
  - nomes, números de documentos, placas de carros, números de telefones, qualquer tipo de data
  - palavras que façam parte de dicionários
- Utilizar senhas longas, com letras, números e símbolos

Proteção do Computador

- Manter o computador atualizado, com todos os programas:
  - com as versões mais recentes
  - com todas as atualizações aplicadas
- Utilizar e manter atualizadas ferramentas de segurança
  - *firewall* pessoal
  - antivírus
  - *antispam*
  - *antispyware*
  - complementos e *plugins* em navegadores
- Utilizar o usuário Administrador (*root*) somente quando for estritamente necessário
- Criar tantos usuários com privilégios normais, quantas forem as pessoas que utilizam o computador

Informar-se e Manter-se Atualizado (1/2)

http://cartilha.cert.br/

http://www.cert.br/rss/certbr-rss.xml

http://twitter.com/certbr

Informar-se e Manter-se Atualizado (2/2)

- **Site Antispam.br – Vídeos Educacionais no escopo das atividades da CT Anti-Spam do CGI.br**
  http://www.antispam.br/

Referências

- Esta apresentação pode ser encontrada em:
  http://www.cert.br/docs/palestras/
- Comitê Gestor da Internet no Brasil – CGI.br
  http://www.cgi.br/
- Núcleo de Informação e Coordenação do Ponto br – NIC.br
  http://www.nic.br/
- Centro de Estudo, Resposta e Tratamento de Incidentes no Brasil – CERT.br
  http://www.cert.br/