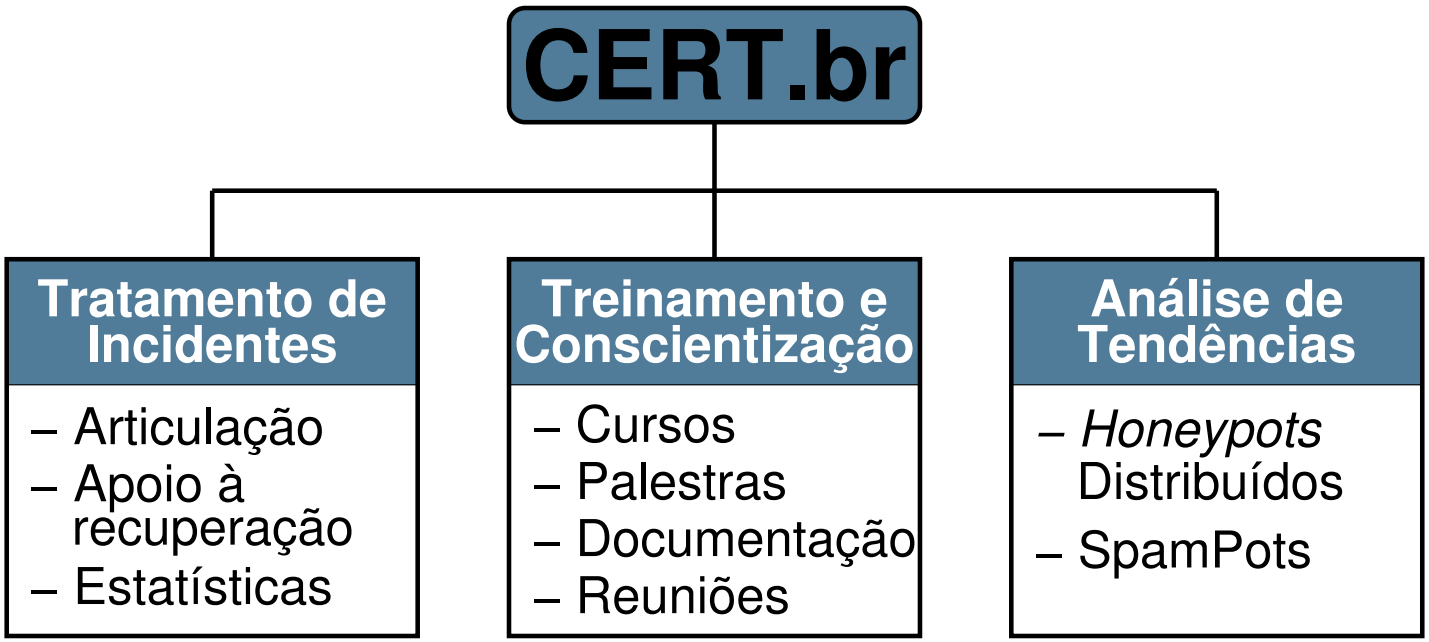
Segurança em Redes Sociais

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 segurança relacionados com as redes conectadas à Internet no Brasil



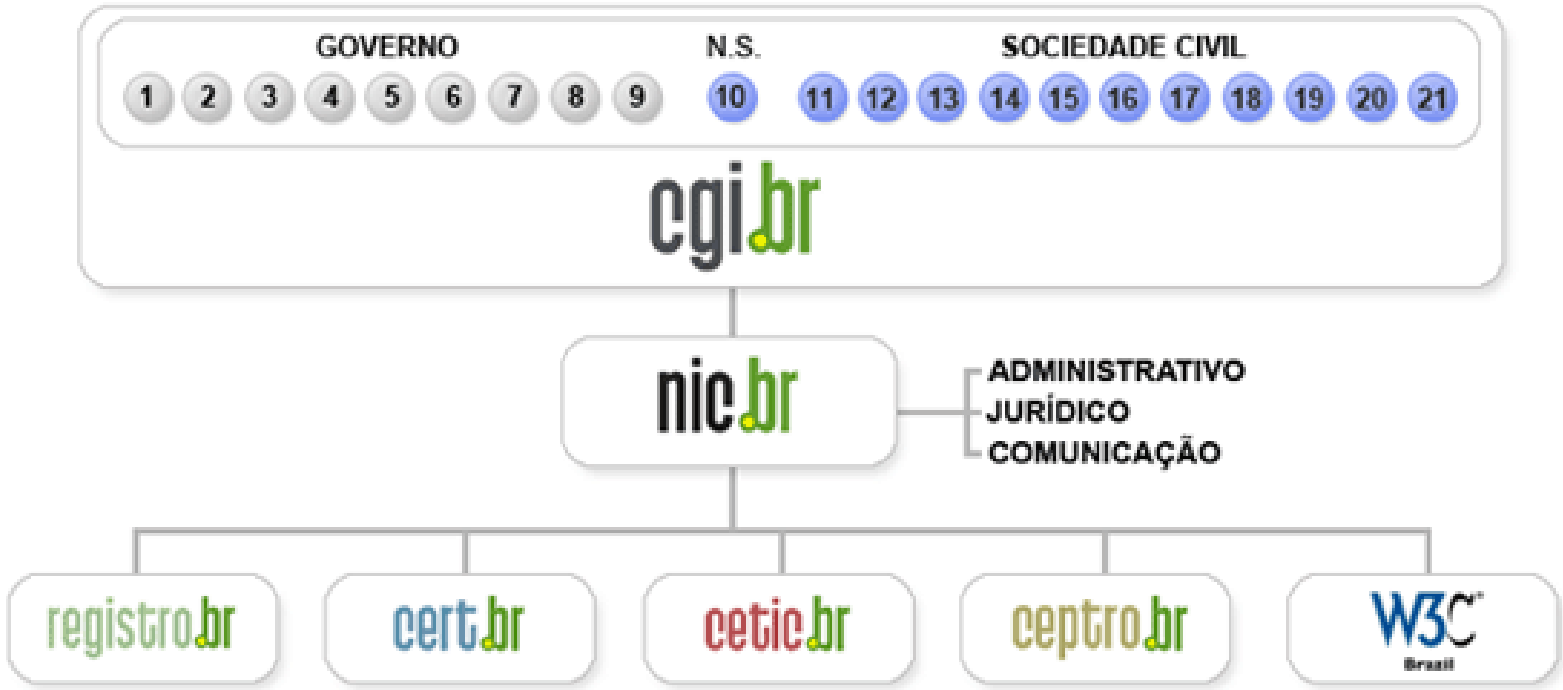
FIRST Improving Security Together MEMBER

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

Redes Sociais no Brasil

Principais Riscos

Prevenção

Referências

Redes Sociais

Permitem que os usuários:

- forneçam informações sobre si
- acessem informações sobre os demais usuários
- utilizem mecanismos de comunicação (*e-mails*, IM, chat...)
- se agrupem, de acordo com afinidades, interesses, características e objetivos em comum

Algumas características:

- conteúdo totalmente gerado pelos usuários
- rápida disseminação de informação
- informações não podem ser excluídas ou controladas
- acessíveis de *websites*, celulares, *smartphones*, etc.

Redes Sociais no Brasil

- Utilização elevada e diversificada

- Pesquisas divulgadas em agosto/2011
  - IBOPE Nielsen Online:
    - **Facebook**: 30,9 milhões
    - **Orkut**: 29 milhões
    - Twitter: 14,2 milhões
  - comScore:
    - **Orkut**: 37,1 milhões - cresc. mensal(2%)/anual(20%)
    - **Facebook**: 28,5 milhões - cresc. mensal(10%)/anual(214%)
    - Twitter: 13,42 milhões
    - Google+: 620 mil - sexto mercado no mundo (20 milhões)

Principais Riscos

- Furto de identidade
- *Phishing* e códigos maliciosos
- Invasão de privacidade
- Danos a imagem e a reputação
- Uso indevido do perfil oficial
- Vazamento de informações
- Sequestro
- Outros riscos

Furto de Identidade (1/2)

- Quanto mais informações um impostor possui, mais fácil é para ele furtar a identidade de uma pessoa

- Informações disponibilizadas podem ser usadas para:
  - criar contas de *e-mail* falsas
  - responder questões de segurança
  - emitir documentos falsos
  - realizar ataques de força bruta
  - criar perfis falsos

Furto de Identidade (2/2)

- Criação de perfil falso:
  - inevitável — contas são criadas em segundos
  - pode ser percebido como sendo um perfil oficial
  - informações de uma rede social podem ser usadas para a criação de perfil falso em outra rede
  - pode ser usado para coletar informações da rede de relacionamento do usuário
  - retirá-lo do ar pode ser difícil e demorado
- Ataques de força bruta:
  - muitos usuários ainda utilizam senhas:
    - curtas
    - baseadas em dados pessoais, palavras de dicionários e em sequências de teclado

Phishing e Códigos Maliciosos (1/2)

- Atacantes podem enviar mensagens contendo:
  - códigos maliciosos (*malware*)
  - links para páginas falsas (*phishing*)
- Procuram explorar a “confiança” que os seguidores/amigos depositam no usuário que teve a conta invadida
  - mensagens de conhecidos são tidas como confiáveis
- Grande uso de *links* reduzidos
- Uso de aplicações desenvolvidas por terceiros
- Reutilização de senhas

Phishing e Códigos Maliciosos (2/2)

- Contas invadidas:

Invasão de Privacidade (1/2)

- Síndrome da celebridade: quantidade X qualidade
  - quanto mais seguidores/amigos são aceitos mais pessoas têm acesso as informações disponibilizadas

- Pequenos pedaços de informação podem nada significar até serem juntados
  - Procura de emprego
    - pedidos de “recomendação”
    - funcionários de empresas competidoras na lista de amigos
    - *check-in* próximo a empresas concorrentes
  - Hábitos, rotina, estilo de vida e nível social
    - comunidades, grupos, planos de viagem

Invasão de Privacidade (2/2)

- Privacidade deixou de ser um conceito individual
  - não adianta um usuário restringir o acesso aos seus amigos se estes repassarem as informações adiante
    - fotos da época de colégio, viagens e confraternizações
    - planos de viagens, localização geográfica

- Informações divulgadas têm sido usadas em:
  - processos seletivos
  - investigações criminais
  - comprovação de união estável
  - divórcios: para comprovação de traição ou de renda

Danos a Imagem e a Reputação (1/2)

Para pessoas em geral:

- *Cyberbullying*
- Difamação, injúria e calúnia
  - podem colocar em risco a vida profissional
  - podem trazer danos psicológicos e de convívio social
- Frases fora de contexto podem ficar ofensivas/sem sentido
  - podem futuramente ser usadas contra o usuário
- Difícil diferenciar assuntos pessoais de profissionais
  - opiniões
  - imagens compartilhadas
  - tipo de linguagem utilizada

Danos a Imagem e a Reputação (2/2)

Para empresas:

- Funcionários e usuários insatisfeitos
- Difamações em redes sociais podem:
  - trazer prejuízos financeiros
  - gerar dúvidas nos consumidores
  - dificultar o recrutamento de funcionários
  - provocar a queda no moral da instituição

Exemplos: Brastemp, Renault, Arezzo, Twix e Zara

Uso Indevido do 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 e impossibilidade de exclusão

- Exemplos:
  - Supremo Tribunal Federal (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 do Perfil Oficial (2/3)

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

Uso Indevido do Perfil Oficial (3/3)

- Chrysler (03/2011)

Vazamento de Informações (1/2)

- Vazamento de notícias
- Discussões em reuniões
- Abertura ou fechamento de *sites*
- Informações sobre batidas policiais
- Lançamento de programas/serviços/produtos
- Detalhes técnicos de produtos, processos ou rede

Vazamento de Informações (2/2)

Exemplos:

- Ataque em Israel (03/2010)
  - "On Wednesday we clean up Qatanah, and on Thursday, God willing, we come home"

- Morte de Osama Bin Laden (05/2011)

Sequestro

- Ivan Kaspersky (abril/2011)
- Harold Wigginbottom (maio/2009)

Wiggy107 Amped for South America trip to fire up Colombian sales force! Landing Tues 5/12 around 4:10pm
10:13 AM May 10 from web

Wiggy107 Airport time = reading time. Briefcase locked & loaded w/ Q4 projections and R&D reports. Then Tetris!
7:01 AM May 12 from TwitterBerry

Wiggy107 Did I leave front door unlocked? Will find out when I'm back next week LOL! Preboarding 1st class now!
7:42 AM May 12 from TwitterBerry

Wiggy107 Wheels down! Bogota airport kinda sketchy. Hooray, admin musta remembered car service -- driver has sign for Wiggy107!
4:19 PM May 12 from TwitterBerry

Wiggy107 NO SE PREOCUPEN, TODO ESTA BIEN. POR FAVOR ENVIEN MUCHO $$$$ A ESTA OFICINA DE LA WESTERN UNION...
5:31 PM May 15 from TwitterBerry

Outros Riscos

- Furto de bens
- Queda de produtividade
- Uso excessivo
- Perda de dados
- Disseminação de boatos
- Recebimento de *spam*
- Plágio e violação de direitos autorais
- Acesso a conteúdos impróprios ou ofensivos

Prevenção

Manter a Privacidade (1/2)

- Considerar que está em um local público
- Não divulgar informações pessoais
  - nome, endereço, número de telefone, etc.
- Não divulgar informações profissionais
  - verifique, se existir, o código de conduta da empresa
- Ser criterioso ao:
  - aceitar amigos/seguidores
  - se associar a comunidades
  - divulgar opiniões pessoais

Manter a Privacidade (2/2)

- Utilizar ao máximo as opções de privacidade disponíveis
  - restringir o acesso a perfil, mensagens, fotos e vídeos
- Criar círculos
- Apagar e restringir recados
- Não fornecer informações sobre localização geográfica
- Utilizar opções de navegar anonimamente
  - podem bloquear o histórico de acesso ao seu perfil

Respeitar a Privacidade

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

Cuidados com a Imagem (1/2)

Empresas:

- Prender-se a fatos
- Treinar a pessoa responsável
- Envolver mais de uma pessoa, departamento
- Criar um código de conduta para os funcionários
  - funcionários que representam a empresa devem ter cuidados especiais (incluindo os parceiros e terceirizados)
- Ser pró-ativo, não esperar o problema aparecer
  - garantir que artigos positivos sejam disseminados, discutidos e referenciados
  - criar uma cadeia de “defensores”
  - monitorar continuamente
  - responder pelo mesmo canal

Cuidados com a Imagem (2/2)

Geral:

- Usar círculos/redes distintas para fins específicos (profissionais, pessoais, etc.)

- Avaliar o impacto da mensagem postada
  - sobre a própria imagem
  - sobre a imagem da empresa onde trabalha
  - sobre a imagem de outras pessoas

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

- Ser cuidadoso 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
- Desabilitar o 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
  - podem ter sido repassadas sem terem sido checadas
  - podem ter sido enviadas através de:
    - perfis falsos
    - contas invadidas
    - computadores infectados
- Ser cuidadoso ao:
  - instalar aplicações de terceiros
  - utilizar mídias removíveis
  - utilizar computadores de terceiros
    - *lan houses*, *cyber cafes*, etc.

Proteção de Contas e Senhas (1/2)

- Nunca compartilhar 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
  - informações disponíveis no perfil
  - palavras que façam parte de dicionários
- Utilizar senhas longas, com letras, números e símbolos
- Criar questões de segurança próprias
- Colocar senha em telefones celulares, *smartphones*, etc.
  - importante em caso de furto ou uso não autorizado

Proteção de Contas e Senhas (2/2)

- Utilizar conexões seguras (HTTPS)
- Habilitar, quando disponível, as notificações de *login*
- Utilizar sempre a opção de “Sair”
- Utilizar sempre as opções de “Denúncia”

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

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*, *anti-spyware*
  - 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://internetsegura.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/