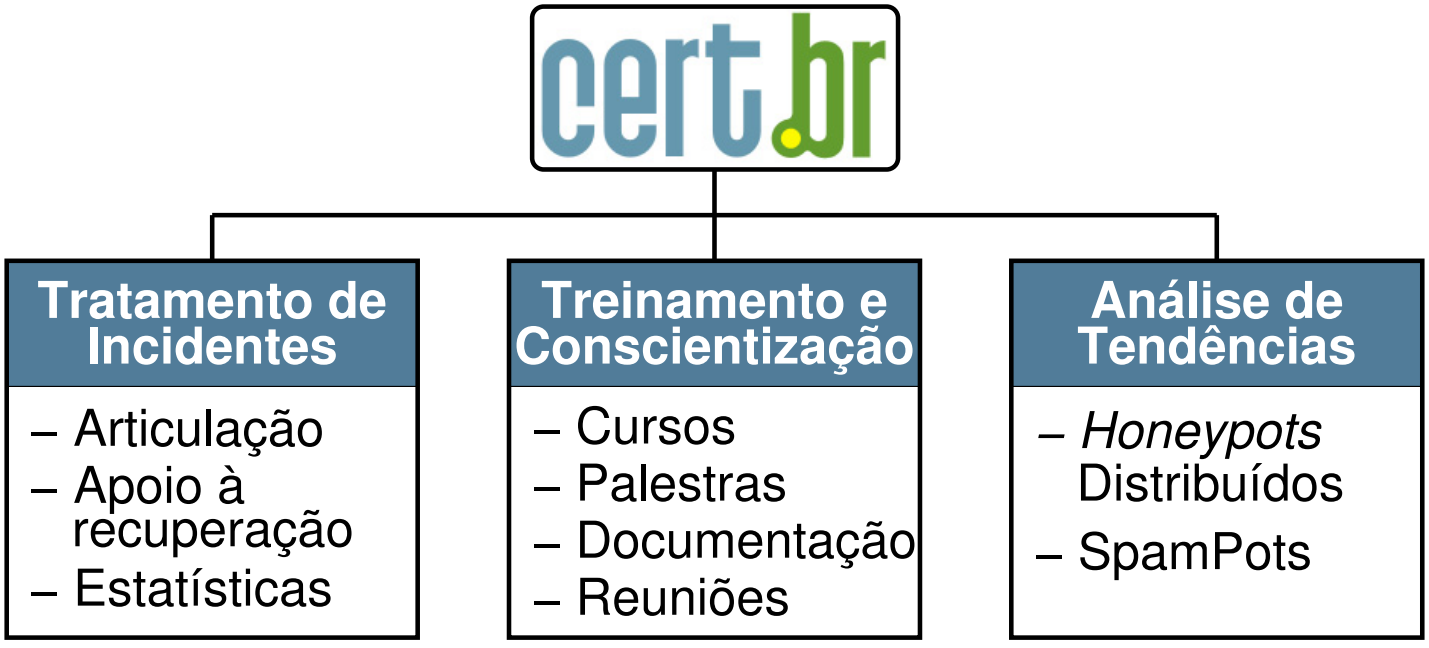
Segurança em Redes Sociais

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

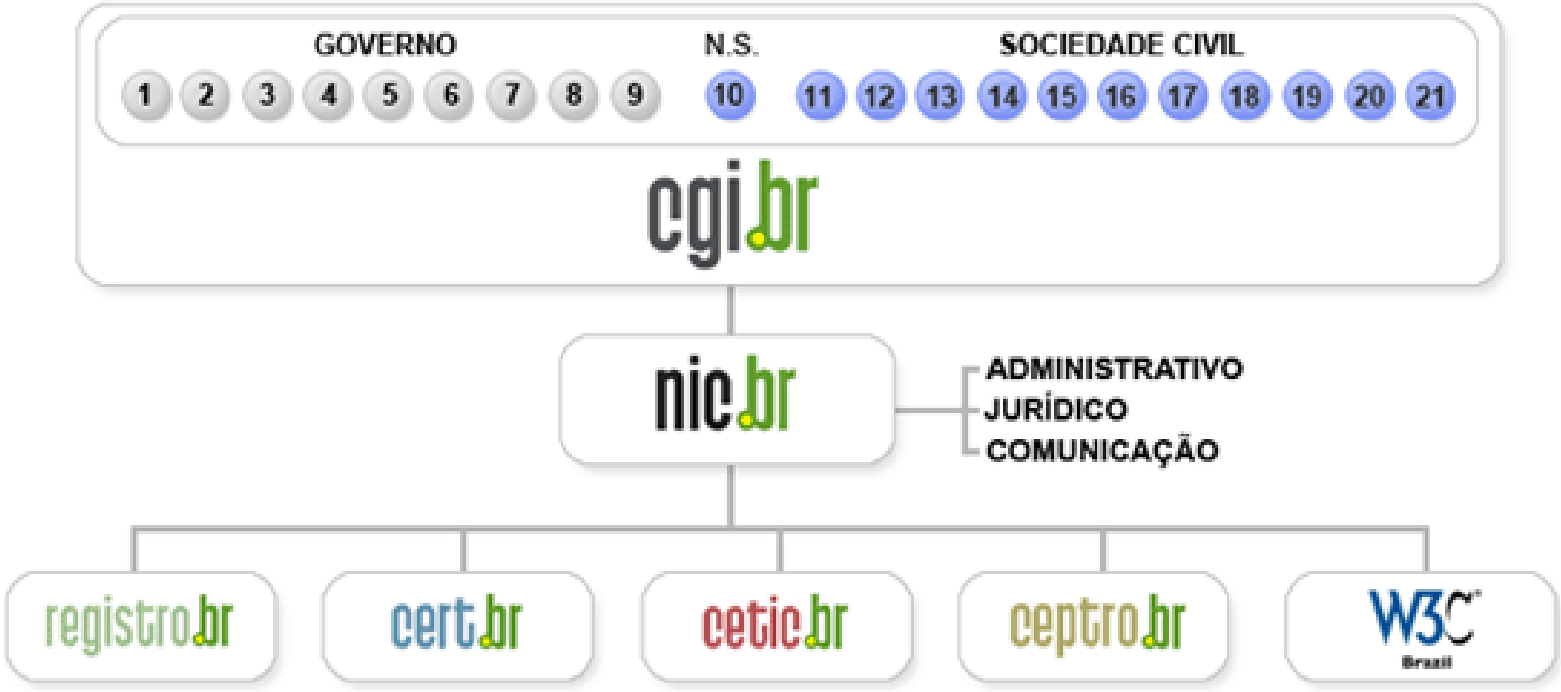
APWG RESEARCH PARTNER www.antiphishing.org

SEI Partner Carnegie Mellon

The Honeynet PROJECT

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

Riscos para os Usuários em Geral

Riscos para as Instituições

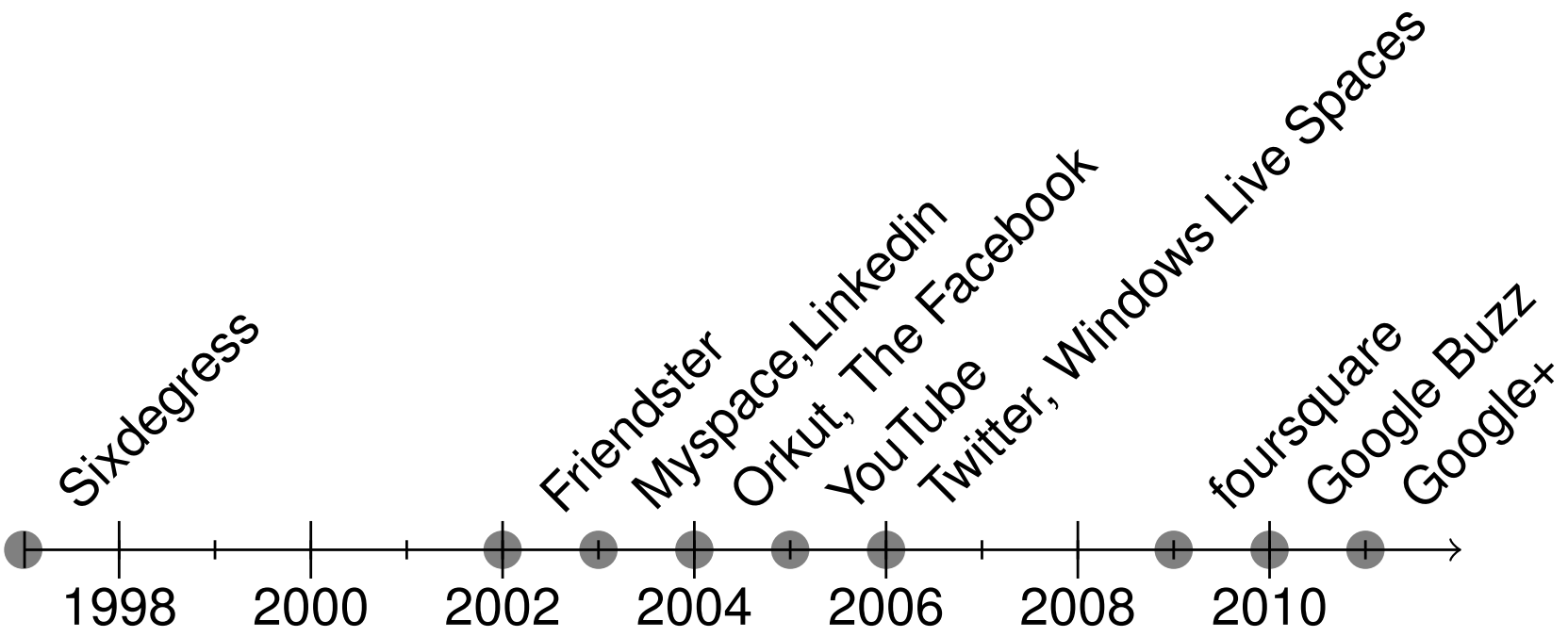
Prevenção

Referências

Redes Sociais

Diário público:

- "Quem você é?"
- "Onde você está?"
- "O que você curte?"
- "Quem você conhece?"
- "O que está acontecendo?"
- "No que você está pensando?"
- "O que seus amigos dizem sobre você?"
- "Em que lugares do mundo você tem estado?"



Redes Sociais no Brasil

- Utilização elevada e diversificada
- IBOPE Nielsen Online (agosto/2011):
  - **Facebook**: 30,9 milhões
  - **Orkut**: 29 milhões
  - Twitter: 14,2 milhões
- comScore (agosto/2011):
  - **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 (26 milhões)
- Linkedin (novembro/2011):
  - 6 milhões - quarto mercado no mundo (135 milhões)
  - país com maior taxa de crescimento (428%)

Riscos para os usuários em geral

Invasão de Privacidade (1/2)

- Síndrome da celebridade: quantidade X qualidade
  - quanto mais seguidores/amigos maior o número de pessoas com 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
- Mudanças nas políticas de privacidade dos *sites*
  - novos recursos (Ticker, Timeline)
- Informações divulgadas têm sido usadas em:
  - processos seletivos
  - investigações criminais
  - comprovação de união estável
  - divórcios (comprovação de traição ou renda)

Uso Indevido das Informações Disponibilizadas

- Quanto mais informações um usuário disponibiliza mais fácil se torna para um impostor furtar a sua identidade
- Criação de perfil falso
  - inevitável — contas são criadas em segundos
  - pode ser percebido como um perfil oficial
  - retirá-lo do ar pode ser difícil e demorado
  - usado para:
    - coletar informações dos amigos
    - aproximar-se de outras pessoas
- Criação de contas de *e-mail* falsas
- Invasão de contas
  - ataques de força bruta
  - resposta a questões de segurança

Spam, *Phishing* e *Malware*

- Atacantes procuram explorar:
  - rede de relacionamento
  - a “confiança” depositada pelo seguidores/amigos
  - necessidade de imediatismo
  - uso de *links* reduzidos
  - facilidade de disponibilização de aplicações
- *Spear-Phishing*
- Reutilização de senhas
- Dados CERT.br:
  - desde 2009: 430 URLs de *phishing* envolvendo *sites* de redes sociais

Danos à Imagem e à Reputação

- 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

Sequestro e Furto de Bens

- 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

- Perda de dados
- Uso excessivo
- Sentimento de exclusão social

Para crianças:

- Acesso a conteúdos impróprios ou ofensivos
- *Cyberbullying*
- Contato com pessoas estranhas
  - Uso de *Webcam*
  - pedófilos utilizando localização geográfica para criação de mapas de vítimas em potencial

Riscos para as instituições

Invasão do Perfil Oficial

Uso Indevido do Perfil Oficial

- 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

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

CulturaSP Secretaria Cultura

PQ foi o José Alencar e não o #Samey?

55 minutes ago

CulturaSP Secretaria Cultura

Mensagem postada indevidamente no nosso perfil não reflete a posição oficial da Secretaria. Lamentamos o ocorrido.

1 hour ago

Danos à Imagem e à Reputação

- Funcionários e consumidores insatisfeitos
  - Brastemp, Renault e Qantas
    - "#QantasLuxury- when the passengers arrive before the couriers delivering the lockout notices do"
    - "Getting from A to B without the plane being grounded or an engine catching fire. #qantasluxury"
- Falha de planejamento
  - Mars Brasil
- Envolvimento em escândalos
  - Arezzo e Zara

Vazamento de Informações

- Vazamento de informações
  - discussões em reuniões
  - informações sobre batidas policiais
  - detalhes técnicos e lançamento de serviços e produtos
- 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)

Prevenção

Manter a Privacidade

- **Utilizar ao máximo as opções de privacidade disponíveis**
- **Considerar que está em um local público**
  - Ser criterioso ao:
    - aceitar amigos/seguidores
    - se associar a comunidades
    - divulgar opiniões pessoais e profissionais
    - fornecer informações sobre localização geográfica
- Localização geográfica:
  - fazer *check-in* ao sair e não ao chegar
  - fazer *check-in* apenas em locais públicos e movimentados
  - utilizar opção “fora de cena”
  - restringir as informações (opção “Quem está aqui”)
- Criar círculos
- Apagar e restringir recados

Respeitar a Privacidade Alheia

- 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

Cuidados com a Imagem

Usuários em geral:

- Usar círculos/redes distintas para fins específicos
- Avaliar o impacto da mensagem postada sobre:
  - a própria imagem e de outras pessoas
  - a imagem da instituição onde trabalha

Empresas:

- Prender-se a fatos
- Treinar a pessoa responsável
- Envolver mais de uma pessoa, departamento
- Criar um código de conduta para os funcionários
- Ser pró-ativo, não esperar o problema aparecer
  - monitorar continuamente e responder pelo mesmo canal
  - garantir que artigos positivos sejam disseminados

Proteção contra *Phishing* e *Malware*

- 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*
- Não considerar que mensagens de conhecidos são sempre confiáveis, pois podem ter sido enviadas:
  - sem terem sido checadas
  - de perfis falsos, contas invadidas ou computadores infectados
- Ser cuidadoso ao:
  - instalar aplicações de terceiros
  - utilizar mídias removíveis e computadores de terceiros

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/