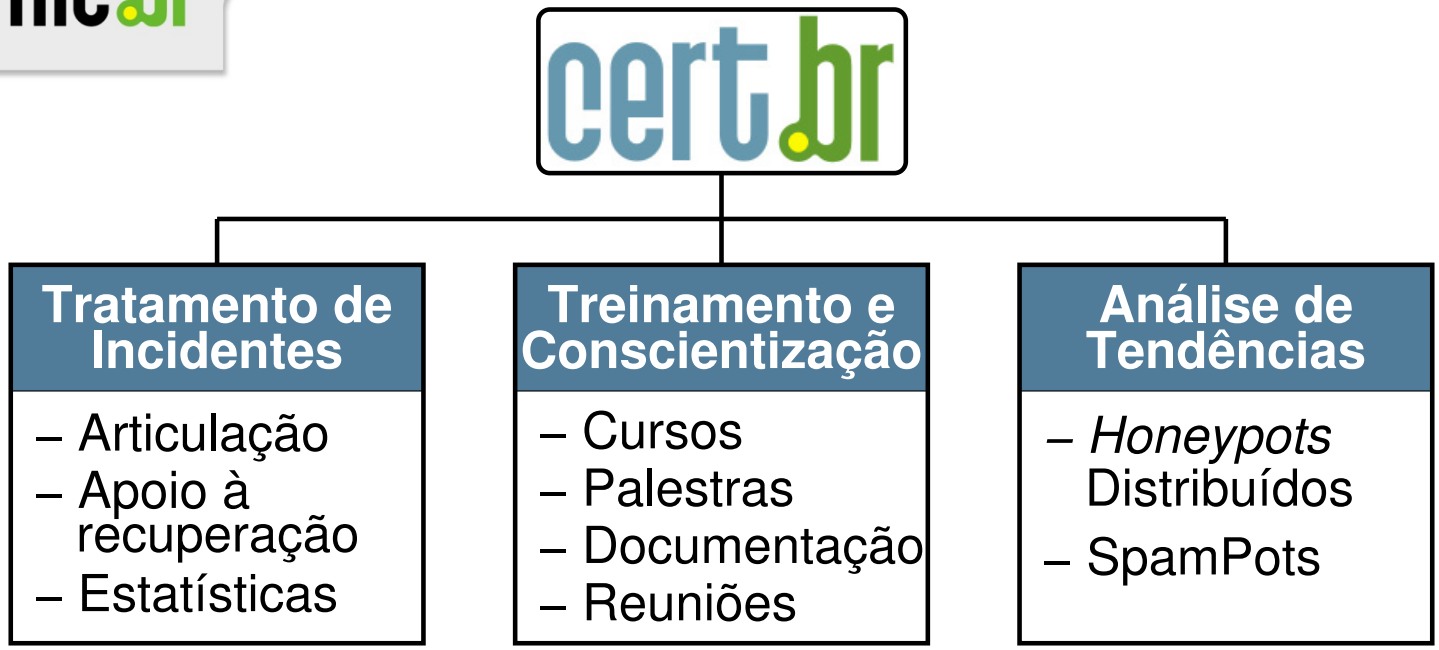
Privacidade na Web

Cristine Hoepers

cristine@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



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**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Privacidade e Confidencialidade

- **Privacidade – habilidade e/ou direito de proteger suas informações pessoais, extende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal.**

- **Confidencialidade – envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles.**

Fonte: **Security Engineering, 2nd Edition, 2008, Ross Anderson**
http://www.cl.cam.ac.uk/~rja14/book.html

Nossa privacidade está cada vez mais nas mãos de terceiros

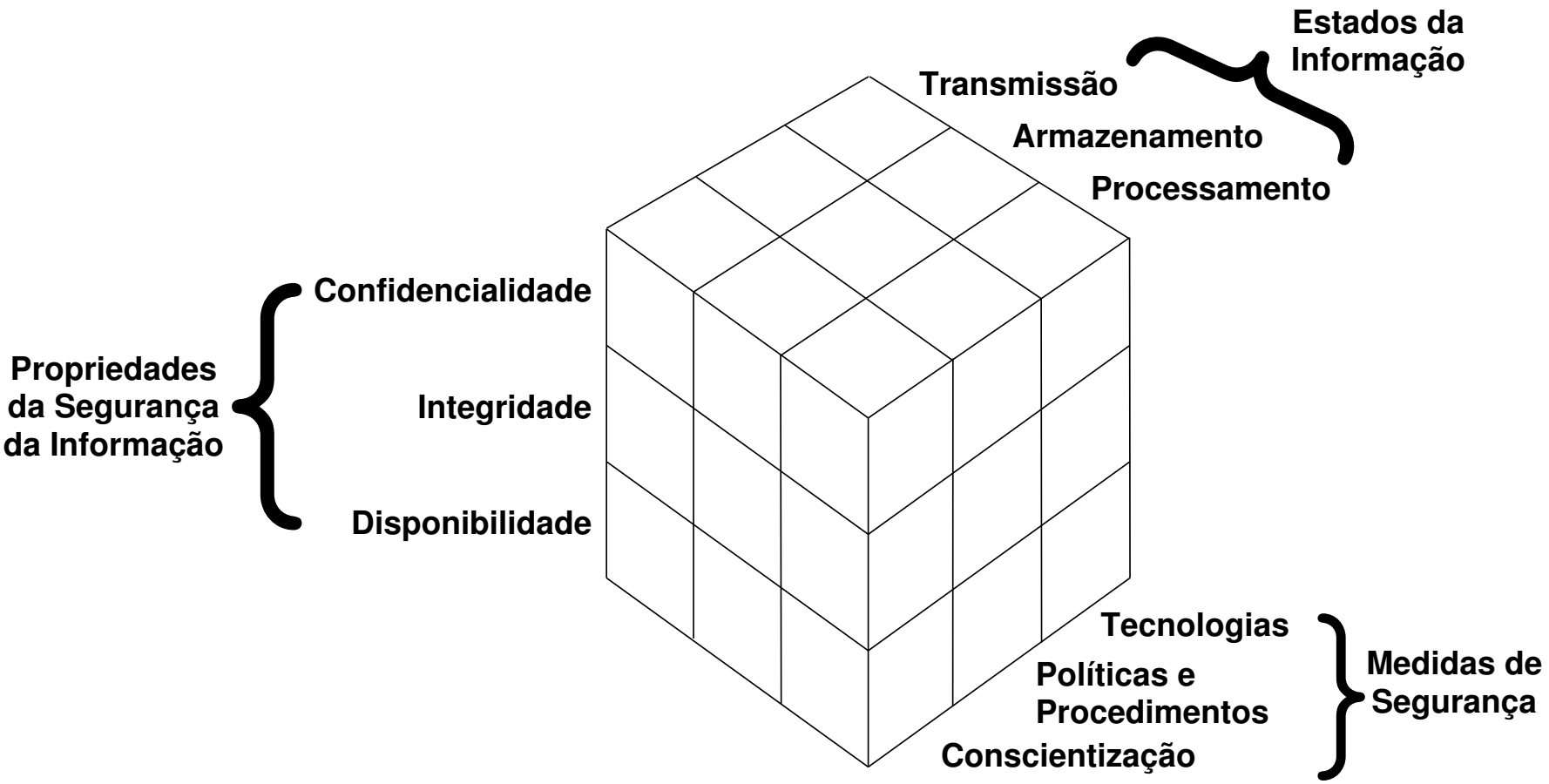
Privacidade com relação ao que está no computador e ao que se faz na Internet

- dados armazenados
- acessos a sites e conteúdos
  - gostos, hábitos, opiniões

Privacidade com relação a dados que precisam estar nos computadores de terceiros ou trafegar pela rede

- depende destes terceiros manterem a confidencialidade
- serviços de e-gov, e-health, e-commerce
  - resultados online de exames, serviços de previdência,
- exemplos recentes de problemas nessa área:
  - Adobe
  - PlayStation
  - Subway

As Informações Estão em Diversos Locais e a Segurança Depende de Múltiplos Fatores



Cenário atual na Web

Crescentes Serviços *Online*

- Grande demanda por *e-services*
- Dados sensíveis estão mais expostos
  - por necessidade, comodidade ou descuido

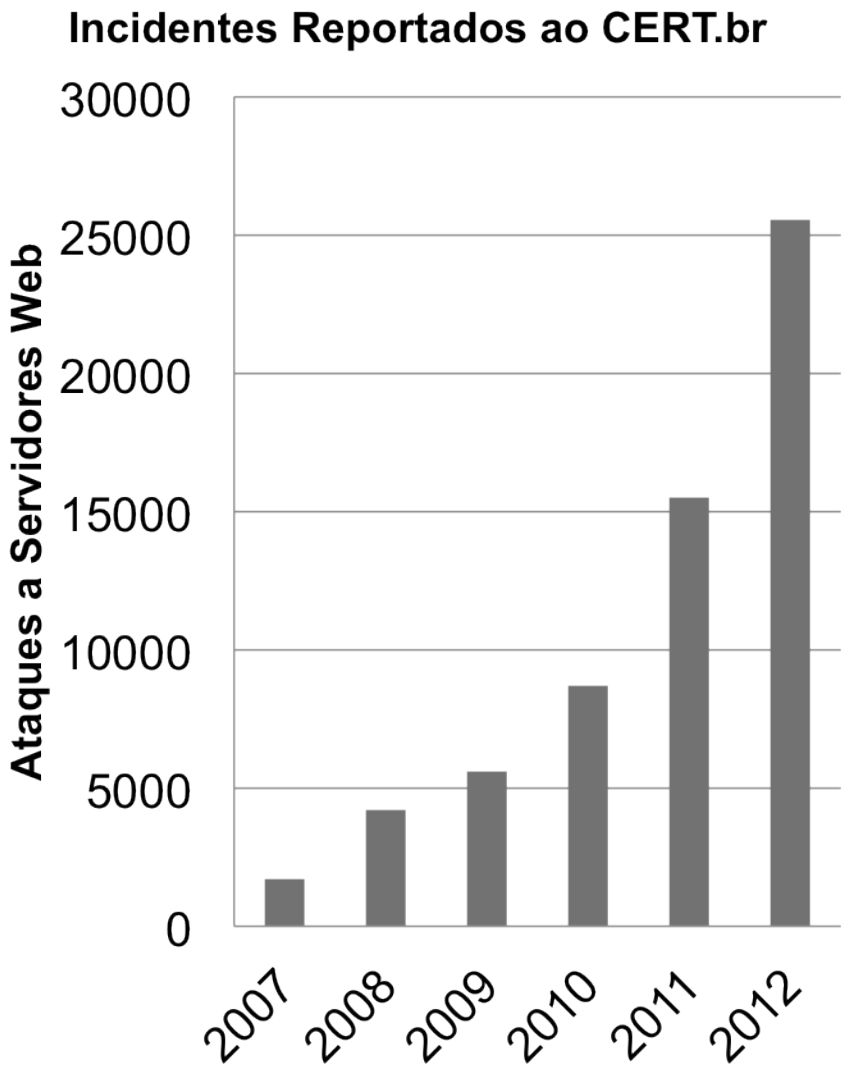
Segurança não é prioridade

- Impactos não são compreendidos
- Segurança não é parte do "*mindset*"
  - "alguém outro vai implementar"
- Sistemas críticos são conectados à Internet
  - controle de infraestruturas críticas
  - sistemas de e-gov
  - bases de dados ("*big data*")
  - dados médicos

Ataques a servidores Web tem crescido rapidamente

Causas mais frequentes

- senhas fracas
- *softwares* de CMS desatualizados
- uso de pacotes e módulos vulneráveis
- falta de atualização dos sistemas operacionais
- muitas falhas de programação:
  - falta de validação de entrada
  - falta de checagem de erros
- exploração automatizada
- Ex.: *botnet* Brobot, usada para negação de serviço



Desafios em aberto

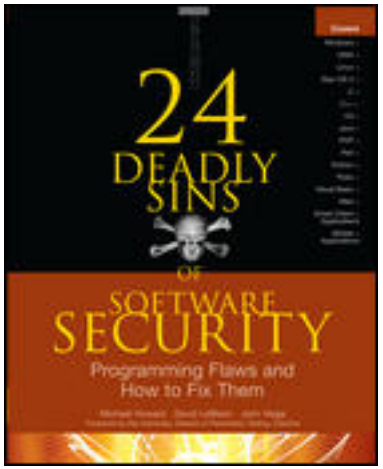
- Não é só uma questão de evitar rastreamento
  - não são só hábitos de navegação que podem afetar a privacidade
  - não são só em *cookies* que estão informações que interessam à privacidade dos cidadãos
- Mecanismos sendo propostos pressupõem que todos na Internet vão honrar os padrões e a vontade do usuário
  - ex. "*do not track*"
  - e os *sites* maliciosos e comprometidos?
- Informações enviadas pelos *browsers* são mais preocupantes que IPs fixos ou *cookies*
  - https://panopticlick.eff.org
- Serviços Web estão construindo bases de dados massivas que já são alvo para
  - venda, espionagem, crime organizado

Considerações Finais

- **Todos tem que fazer parte da solução para termos segurança e privacidade**
- **Não há "ferramenta de segurança" que consiga resolver os problemas de sistemas Web**
  - **os sistemas precisam ficar online 100% do tempo**
  - **o tráfego com destino a eles não pode ser barrado**
  - **ferramentas de detecção de assinaturas, em geral, não atuam em tráfego cifrado (HTTPS)**
- **Desenvolvimento seguro de *software* deve se tornar parte da formação de projetistas e programadores**
  - **Desde a primeira disciplina de programação e permeado em todas as disciplinas**
- **Temos que vencer a cultura de que é melhor investir em tecnologia do que em treinamento e implantação de boas práticas**

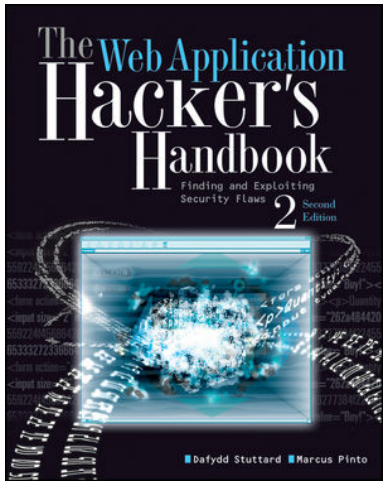
Leituras recomendadas

The Open Web Application Security Project (OWASP) Top Ten Project
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project



ISBN: 978-0071626750

ISBN: 978-0596514839



ISBN: 978-1118026472

Perguntas?

Cristine Hoepers
cristine@cert.br

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