INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução a Segurança de Redes

Segurança da Informação

Filipe Raulino
filipe.raulino@ifrn.edu.br

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Objetivos

- Entender a necessidade de segurança da informação no contexto atual de redes de computadores;
- Conhecer conceitos básicos e a terminologia usada;
- Apresentar mecanismos de defesa.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

O que é segurança da Informação?

É a proteção da informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidade de negócios" [ISO 27002].

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

- A expansão da **Internet** gerou novos aspectos de negócios, **ampliando a atuação das empresas** e atingindo novos segmentos e mercados.

- A evolução dos ambientes informatizados levou as informações empresariais para o **formato digital.**

- Se isso abriu as portas da empresa para o mundo, **as informações devem ser protegidas.**

Introdução

O que devemos proteger?

- Registo de negócios;
- Bases de dados dos clientes;
- Informações Pessoais;
- Registros financeiros e transações;
- Base de dados de informações.

Para a política de segurança da informação é importante a proteção das informações, independente de onde estejam (Papel, memória do computador, trafegando na rede...).

Introdução

Um ataque bem sucedido pode resultar em:

- Prejuízo à imagem da empresa;
- Diminuição na produtividade;
- Perda de mercado;
- Vazamento de informações confidenciais;
- Prejuízo financeiro.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança da informação

- **A segurança da informação é baseada em 3 pilares (CID).**
  - Confidencialidade
  - Integridade
  - Disponibilidade
- **E envolve:**
  - Tecnologias
  - Processos
  - Pessoas

As pessoas são, normalmente, o elo mais fraco, portanto o mais explorado por atacantes.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Engenharia Social

- Práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas.
- Ataca o elemento mais vulnerável de qualquer sistema de segurança da informação: o ser humano.
- Ao realizar o ataque, o “Engenheiro social” pode fazer uso de qualquer meio de comunicação.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Vulnerabilidades X Ameaças x Riscos

Vulnerabilidade - falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema;

Ameaça - possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade específica;

Risco - probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Vulnerabilidades Tecnologicas

- Protocolos
- Sistema Operacional
- Equipamentos de Rede

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Vulnerabilidades de Configuração

- Manter configurações default inseguras
- Contas de sistemas com senhas previsíveis
- Configuração equivocada de equipamentos ou serviços.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Vulnerabilidades da Política de Segurança

- Falta de uma politica escrita;
- Falta de controle de acesso;
- Administração de segurança negligente;
- Alterações ou instalações de software ou hardware não seguem a política;
- Falta de conhecimentos sobre ataques;
- Falta de Planejamento de contingência.

Ameaças Acidentais

- Falhas de equipamentos
- Erros humanos
- Falhas de software
- Problemas causados por forças da natureza

Ameaças Propositais

- Espionagem;
- Crimes;
- Empregados insatisfeitos;
- Empregados desonestos;
- Vandalismo;
- Terrorismo.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Ataques na Internet

- Exploração de vulnerabilidades
- Varredura em redes (Scan)
- Falsificação de e-mail (E-mail spoofing)
- Interceptação de tráfego (Sniffing)
- Força bruta (Brute force)
- Desfiguração de página (Defacement)
- Negação de serviço (DoS e DDoS)

Os motivos que levam os atacantes a desferir ataques na Internet são bastante diversos, entre eles: demonstração de poder, busca de prestígio, motivações financeiras, ideológicas ou comerciais

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Golpes na Internet

- Furto de identidade (Identity theft)
- Fraude de antecipação de recursos (Advance fee fraud)
- Phishing
- Pharming
- Golpes de comércio eletrônico
- Boato (Hoax)

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Códigos Maliciosos

- Vírus;
- Worm;
- Bot e botnet;
- Spyware;
- Backdoor;
- Cavalo de troia (Trojan);
- Rootkit.

Perfil do Invasor

Lammer

- Menino ou adolescente
- Obter acesso gratuitamente a sites na Internet
- Brincar de “pichação virtual”
- Derrubar pessoas em salas de chat

Hacker

- Estudante de computação
- Motivos ideológicos
- Motivos psicológicos

Cracker

- Profissional motivado financeiramente
- Objetiva fraude e furto
- Pode ter o suporte do crime organizado em um futuro próximo

Mecanismos de Segurança

Para **minimizar** os riscos deve-se garantir alguns requisitos básicos de segurança, como:

- Identificação;
- Autenticação;
- Autorização;
- Integridade;
- Confidencialidade ou sigilo;
- Não repúdio;
- Disponibilidade.

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Mecanismos de Segurança

- Política de segurança;
- Notificação de incidentes e abusos;
- Contas e senhas;
- Criptografia;
- Cópias de segurança (Backups);
- Registro de eventos (Logs);
- Ferramentas antimalware;
- Firewall.

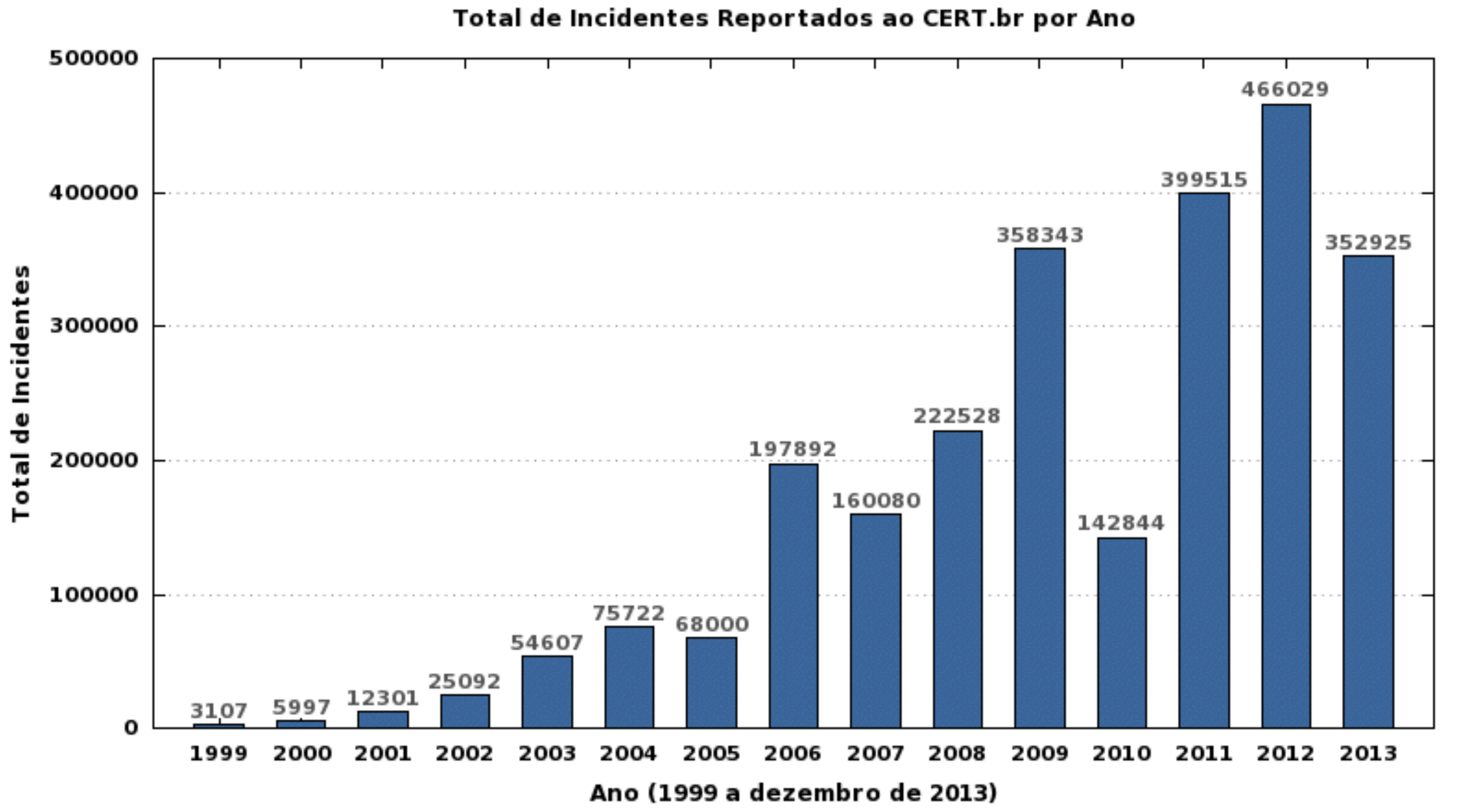
Normas

Existem algumas normas que orientam e padronizam boas práticas de gestão da segurança da informação

- ISO 27001;
- ISO 27002;
- BASILEIA II;
- PCI-DSS;
- ITIL;
- COBIT;

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Tendências



Tendências

Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2013

Estudo de Caso

Invasão da PSN

- Em 19 de abril de 2011 membros da equipe de ti da Sony encontraram vestigios de Atividades não autorizadas em sua rede.
- No dia seguinte foram descobertos evidências de invasão ao sistema e roubo de informações, eles então resolveram tirar o serviço do ar e contrataram empresas especializadas em análise forense para investigar o caso.
- No dia 26 de abril de 2011 a Sony informou que os dados de aproximadamente 77 milhões de usuários haviam sido roubados. O FBI foi acionado para investigar o caso.
- A rede so voltou ao ar no dia 15 de maio, causando um prejuízo estimado de 24 bilhões de dólares.