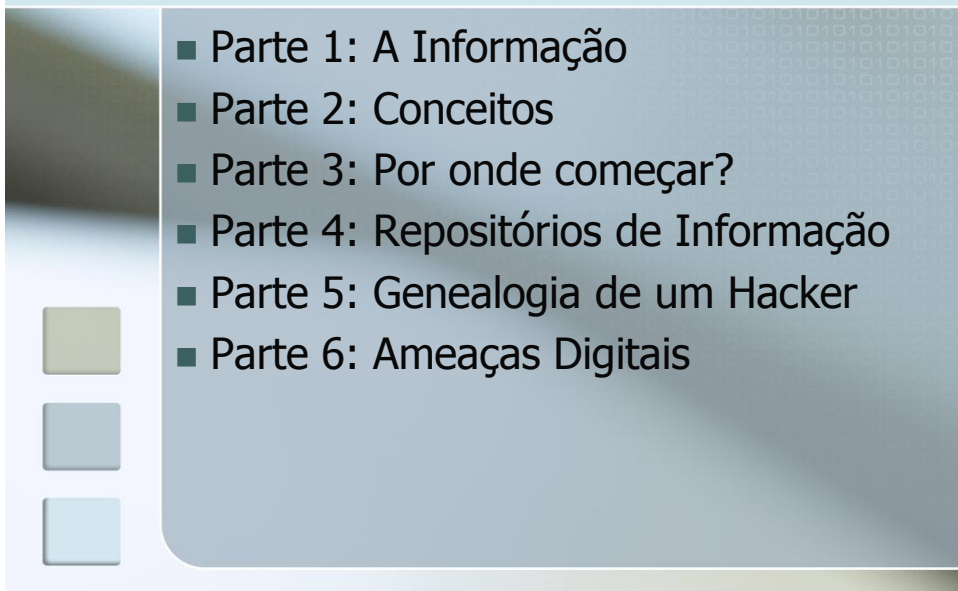




Introdução a Segurança da Informação

Conteúdo Programático

- Parte 1: A Informação
- Parte 2: Conceitos
- Parte 3: Por onde começar?
- Parte 4: Repositórios de Informação
- Parte 5: Genealogia de um Hacker
- Parte 6: Ameaças Digitais



PARTE 1

■ A Informação

Informação (Michaelis)

■ do Lat. *informatione*

s. f.,

Ato ou efeito de informar ou informar-se;

Comunicação;

Conjunto de conhecimentos sobre alguém ou alguma coisa;

Conhecimentos obtidos por alguém;

Fato ou acontecimento que é levado ao conhecimento de alguém ou de um público através de palavras, sons ou imagens;

Elemento de conhecimento susceptível de ser transmitido e conservado graças a um suporte e um código.

Propriedade (Michealis)

- do Lat. *proprietate*

s. f.,

Aquilo que pertença legitimamente a alguém ou sobre o qual alguém tenha direito pleno;

Bens, posses;

Patrimônio físico(tangível) e imaterial(intangível).

Consideração

- E quando o patrimônio é a informação?

Considerações

- Segundo a Universidade da Califórnia em Berkeley⁽²⁰⁰⁵⁾:
 - Existe aproximadamente 2.5 Bilhões de documentos acessíveis na WEB;
 - Este número cresce em cerca de 700 mil páginas por dia.
- Velhos jargões
 - “O segredo é a alma do negócio”;
- Novas tendências
 - Mundo Globalizado, Ubiquidade, Acesso a Informação.

PARTE 2

- Conceitos

Axioma de Segurança

“Uma corrente não é mais forte que o seu elo mais fraco”

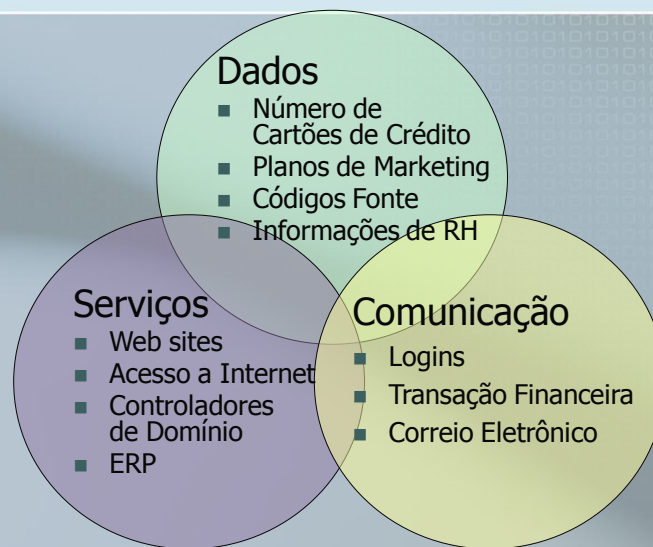
Segurança da Informação

- “A segurança da informação é um conjunto de medidas que se constituem basicamente de **controles** e **política de segurança**, tendo como objetivo a proteção das informações dos clientes e da empresa (**ativos/bens**), controlando o **risco** de revelação ou alteração por pessoas não autorizadas.”

Política de Segurança

- Trata-se um conjunto de diretrizes (**normas**) que definem formalmente as regras e os direitos dos usuários, visando à proteção adequada dos **ativos** da informação

Ativos (Bens)



Definições

- Ameaça
 - Evento ou atitude indesejável que potencialmente remove, desabilita, danifica ou destrói um **recurso**;
- Vulnerabilidade
 - Característica de fraqueza de um bem;
 - Características de modificação e de captação de que podem ser alvos os bens, ativos, ou recursos intangíveis de informática, respectivamente, software, ou programas de bancos de dados, ou informações, ou ainda a imagem corporativa.

Conceitos Básicos

- Risco
 - A **probabilidade** da ocorrência de uma ameaça em particular
 - A **probabilidade** que uma ameaça explore uma determinada vulnerabilidade de um recurso

Ameaça, Vulnerabilidade e Risco

- Ameaça (evento)
 - assalto a uma agência bancária
- Vulnerabilidade (ponto falho)
 - liberação manual das portas giratórias pelos vigilantes
- Risco
 - **baixo**, devido ao percentual de assaltos versus o universo de agências
 - **alto**, se comparando as tentativas frustradas versus as bem sucedidas

Conceitos Fundamentais

- Princípios da Segurança



CIA – Confidencialidade

- Propriedade de manter a informação a salvo de acesso e divulgação **não autorizados**;
- Proteger as informações contra acesso de qualquer pessoa não devidamente autorizada **pelo dono** da informação, ou seja, as informações e processos são liberados apenas a **pessoas autorizadas**.

CIA – Integridade

- Propriedade de manter a informação acurada, completa e atualizada
- Princípio de segurança da informação através do qual é garantida a **autenticidade** da informação
- O usuário que arquiva dados espera que o conteúdo de seus arquivos não seja alterado por erros de sistema no suporte físico ou lógico

CIA – Disponibilidade (Availability)

- Propriedade de manter a informação disponível para os usuários, quando estes dela necessitarem
- Relação ou percentagem de tempo, em que uma unidade do equipamento de processamento está funcionando corretamente

Princípios Auxiliares

Métodos

- DAC
- MAC
- RBAC

Controle de Acesso

Auditoria

Autorização

Sigilo
Identificação

Autenticação

Vias

- O que Sou
- O que Sei
- O que Tenho

Controle de Acesso

- Suporta os princípios da CIA
- São mecanismos que limitam o acesso a recursos, baseando-se na identidade do usuário, grupo que integra e função que assume.
- Em segurança, é suportado pela tríade AAA (definida na RFC 3127)

Auditoria (Accountability)

- É a capacidade que um sistema tem de determinar as ações e comportamentos de um único indivíduo no sistema, e de identificar este indivíduo;
- Trilha de auditoria, tentativas de acesso, problemas e erros de máquina, e outros eventos monitorados ou controlados.

Autenticação

- Propriedade de confirmar a identidade de uma pessoa ou entidade.
- Meio pelo qual a identidade de um usuário é confirmada, e garante que ele realmente é quem diz ser

Autorização

- São os direitos ou permissões, concedidos a um indivíduo ou processo, que permite acesso a um dado recurso.
- Após a identificação e autenticação de um usuário terem sido estabelecidas, os níveis de autorização irão determinar a extensão dos direitos que este usuário pode ter em um dado sistema.

- Trata-se do nível de confidencialidade e garantia de privacidade de um usuário no sistema;
- Ex.: Garante a privacidade dos dados de um usuário em relação ao operador do sistema.

- Meio pelo qual o usuário apresenta sua identidade. Mais frequentemente utilizado para controle de acesso, é necessário para estabelecer Autenticação e Autorização.

PARTE 3

■ Onde Começar ?

Leis Imutáveis da Segurança

- Ninguém acredita que nada de mal possa acontecer até que acontece;
- Segurança só funciona se a forma de se manter seguro for uma forma simples;
- Se você não realiza as correções de segurança, sua rede não será sua por muito tempo;
- Vigilância eterna é o preço da segurança;
- Segurança por Obscuridade, não é segurança;
- LOGs, se não auditá-los, melhor não tê-los.

Leis Imutáveis da Segurança

- Existe realmente alguém tentando quebrar (adivinhar) sua senha;
- A rede mais segura é uma rede bem administrada;
- A dificuldade de defender uma rede é diretamente proporcional a sua complexidade;
- Segurança não se propõe a evitar os riscos, e sim gerenciá-los;
- Tecnologia não é tudo.

*By Scott Pulp – Security Program Manager at
Microsoft Security Response Center*

Responsabilidades da Empresa

- “Desde que uma empresa fornece acesso internet a seus funcionários, esta empresa torna-se responsável pelo que ele faz, a menos que possa provar que tomou as medidas cabíveis para evitar problemas”

*Corporate Politics on the Internet:
Connection with Controversy, 1996*

Segurança nas Organizações

- Segurança é um “processo” que tenta manter protegido um sistema complexo composto de muitas entidades:
 - Tecnologia (hardware, software, redes)
 - Processos (procedimentos, manuais)
 - Pessoas (cultura, conhecimento)
- Estas entidades interagem das formas mais variadas e imprevisíveis
- A Segurança falhará se focar apenas em parte do problema
- Tecnologia não é nem o problema inteiro, nem a solução inteira

Ciclo de Segurança

- Análise da Segurança (Risk Assessment)
- Definição e Atualização de Regras de Segurança (Política de Segurança)
- Implementação e Divulgação das Regras de Segurança (Implementação)
- Administração de Segurança (Monitoramento, Alertas e Respostas a Incidentes)
- Auditorias (Verificação do Cumprimento da Política)

Domínios de Conhecimento

- “The International Information Systems Security Certification Consortium, Inc. [(ISC)²]”

- <http://www.isc2.org>



- A (ISC)² define 10 domínios de conhecimento (CBK), para sua certificação introdutória CISSP

- Certified Information Systems Security Professional
 - Common Body of Knowledge

CBK – Common Body Of Knowledge

- Security Management Practices
- Access Control Systems
- Telecommunications and Network Security
- Cryptography
- Security Architecture and Models
- Operations Security
- Applications and Systems Development
- Business Continuity Planning and Disaster Recovery Planning
- Law, Investigation, and Ethics
- Physical Security




Outras Certificações



- GIAC - Global Information Assurance Certification (Sans.Org)
 - 3 Níveis de Expertise em 5 Áreas de Conhecimento
 - Níveis
 - GIAC Silver
 - 2 ou mais testes
 - GIAC Gold
 - Silver + Pesquisa e Publicação
 - GIAC Platinum
 - Gold em 2 ou mais AC's + testes(3 dias)
 - Áreas de Conhecimento
 - Administração de Segurança
 - Gerência de Segurança
 - Operações
 - Legislação
 - Auditoria

Outras Certificações



- CompTIA – Security+
 - 5 Domínios de Conhecimento
 - Communication Security
 - Infrastructure Security
 - Cryptography
 - Operational Security
 - General Security Concepts

Outras Certificações

■ MCSO – Módulo Certified Security Officer

■ 2 Módulos compreendendo:

■ Conceitos, Padrões e Aplicações

- Fundamentos de Segurança da Informação
- Organização de departamentos
- Gestão de pessoas
- Política de Segurança da Informação.

■ Gestão de Tecnologias

- Windows/Unix
- Segurança em redes e telecomunicações
- Controle de acesso
- Arquitetura e modelos de segurança
- Criptografia