Princípios Fundamentais de Segurança da Informação

1. Introdução

A segurança da informação tornou-se um aspecto central para qualquer organização. Antes de implementar mecanismos de proteção, é essencial entender o **adversário** e os **riscos** envolvidos. A segurança não é absoluta; seu objetivo é **minimizar vulnerabilidades e dificultar os ataques**, nunca eliminá-los totalmente.

---

2. Tríade CIA – Confidencialidade, Integridade e Disponibilidade

A **tríade CIA** representa as três funções básicas da segurança da informação:

- **Confidencialidade**: Garantia de que apenas pessoas autorizadas tenham acesso à informação.
- **Integridade**: Assegura que a informação não foi modificada de forma não autorizada.
- **Disponibilidade**: Assegura que a informação e os sistemas estejam acessíveis quando necessário.

Exemplos:

- **E-commerce**:
    - Confidencialidade: proteção dos dados do cartão.
    - Integridade: manter o endereço de entrega correto.
    - Disponibilidade: acesso ao site para efetuar compras.
- **Registros Médicos**:
    - Confidencialidade: proteção dos dados dos pacientes.
    - Integridade: diagnóstico correto com base em dados precisos.
    - Disponibilidade: acesso do médico aos registros em consultas.

Equilíbrio é essencial: Focar demais em um pilar pode comprometer os outros dois.

---

3. Extensões da Tríade CIA

Além da CIA, outros dois princípios são fundamentais:

- **Autenticidade**: Garante que os dados sejam genuínos e provenientes de uma fonte confiável.
- **Não-repúdio**: Impede que a origem de uma informação negue sua autoria.

Esses princípios são críticos em sistemas de transações, registros médicos e comunicações empresariais.

---

4. Hexade Parkerian

Proposto por Donn Parker, este modelo amplia a CIA para seis elementos:

1. **Confidencialidade**
2. **Integridade**
3. **Disponibilidade**
4. **Autenticidade**
5. **Utilidade**: A informação deve estar em uma forma útil.
6. **Posse**: Propriedade e controle legítimo sobre a informação.

Exemplo: Dados criptografados sem chave de decriptação têm **disponibilidade**, mas não têm **utilidade**.

---

5. Tríade DAD – Divulgação, Alteração e Destruição

Oposto à CIA, a tríade **DAD** representa os principais ataques à segurança:

- **Divulgação**: Viola a confidencialidade.
- **Alteração**: Viola a integridade.
- **Destruição/Negação**: Viola a disponibilidade.

---

6. Modelos de Segurança

Bell-LaPadula (Foco: Confidencialidade)

- **Sem leitura acima**: usuários de baixo nível não podem acessar dados de nível superior.
- **Sem escrita abaixo**: usuários de alto nível não podem gravar em níveis inferiores.

Regras: “escrever para cima, ler para baixo”.

Biba (Foco: Integridade)

- **Sem leitura abaixo**: impedir contaminação de dados por informações de menor integridade.
- **Sem escrita acima**: impedir que dados de baixa integridade afetem informações confiáveis.

Regras: “ler para cima, escrever para baixo”.

Clark-Wilson (Foco: Integridade Transacional)

- **CDIs**: Dados sensíveis que devem manter integridade.
- **UDIs**: Dados não controlados (como entradas de usuários).
- **TPs**: Operações seguras autorizadas.
- **IVPs**: Verificações periódicas de integridade.

---

7. Conceitos Relacionados

- **Vulnerabilidade**: Fraqueza no sistema que pode ser explorada.
- **Ameaça**: Potencial agente malicioso ou evento que tenta explorar uma vulnerabilidade.
- **Risco**: Possibilidade de que uma ameaça explore uma vulnerabilidade causando dano.

---

8. Princípios Estratégicos de Segurança

- **Defesa em profundidade**: Uso de múltiplas camadas de segurança.
- **Zero confiança**: Nenhuma entidade é confiável por padrão, mesmo dentro da rede.
- **Confiança, mas verifique**: Confiança condicional, baseada em validação contínua.

---

9. Normas e Padrões

- **ISO/IEC 19249**: Define mecanismos e estruturas de segurança para produtos de TI.

---

10. Conclusão

A segurança da informação é multifacetada e requer compreensão clara de:

- Quais ativos estão sendo protegidos,
- Contra quem,
- E com quais mecanismos.

Adotar modelos como CIA, Hexad Parkerian e os modelos Bell-LaPadula, Biba e Clark-Wilson permite estruturar soluções eficazes e equilibradas, ajustadas ao contexto e à criticidade de cada sistema.

Conceito de Defesa em Profundidade

- Estratégia de segurança com **múltiplas camadas de proteção**.
- Analogamente: trancar gaveta, sala, porta do apartamento, portão e usar câmeras.
- Objetivo: **retardar ou impedir** ataques, mesmo que uma camada seja violada.

📘 **Norma ISO/IEC 19249:2017**

- Estabelece princípios para **arquitetura e design de segurança** de sistemas, produtos e aplicações.

🏛️ **Cinco Princípios Arquiteturais (Architecture Principles)**

1. **Separação de Domínio**
    - Agrupamento de componentes com atributos de segurança comuns.
    - Ex: níveis de privilégio do processador (anel 0, anel 3).
2. **Camadas (Layering)**
    - Segurança aplicada em diferentes níveis (ex: modelo OSI).
    - Ajuda na validação do funcionamento e na aplicação de políticas.
3. **Encapsulamento**
    - Ocultação de detalhes de implementação.
    - Uso de APIs e métodos para evitar acesso direto a dados internos.
4. **Redundância**
    - Garante **disponibilidade e integridade**.
    - Ex: RAID 5, fontes de alimentação duplicadas.
5. **Virtualização**
    - Compartilhamento de hardware entre sistemas.
    - Fornece isolamento (sandbox), detonação segura e controle de ameaças.

🛠️ **Cinco Princípios de Design (Design Principles)**

1. **Menor Privilégio (Least Privilege)**
    - Conceder apenas as permissões mínimas necessárias.
2. **Minimização da Superfície de Ataque**
    - Reduzir pontos de entrada e serviços desnecessários.
3. **Validação Centralizada de Parâmetros**
    - Entrada de dados deve ser validada centralmente para prevenir abusos.
4. **Serviços de Segurança Centralizados**
    - Ex: servidor único de autenticação.
    - Deve-se mitigar risco de ponto único de falha.
5. **Tratamento de Erros e Exceções**
    - Sistemas devem **falhar de maneira segura**.
    - Mensagens de erro não devem expor dados sensíveis.

Princípios de Confiança

1. **Confie, mas Verifique**
    - Auditar e monitorar atividades, mesmo de fontes confiáveis.
    - Uso de proxies, IDS/IPS, logs.
2. **Confiança Zero (Zero Trust)**
    - **“Nunca confie, sempre verifique.”**
    - Nenhuma confiança implícita com base em localização ou propriedade.
    - Requer autenticação e autorização rigorosas.
    - **Microsegmentação** como técnica para isolar comunicações por host.

Conceitos Complementares

- CIA: Confidencialidade, Integridade, Disponibilidade.
- DAD: Divulgação, Alteração, Destruição.
- Termos adicionais: autenticidade, repúdio, vulnerabilidade, ameaça, risco.
