Atividade 1 - Segurança e Auditoria de Sistemas

Aluno: João Victor Póvoa França

Problema 1.1: Caixa Eletrônico (ATM)

- **Confidencialidade:** O sistema deve garantir que o número de identificação pessoal (senha/PIN) inserido pelo usuário e os dados do saldo da conta não sejam vistos por terceiros ou interceptados na rede.
  - *Grau de importância:* **Alto**. O comprometimento da senha leva à fraude financeira direta.
- **Integridade:** O sistema deve assegurar que o valor solicitado para saque seja exatamente o valor debitado da conta do usuário. Nenhuma alteração pode ocorrer na transação durante a comunicação entre o caixa e o banco.
  - *Grau de importância:* **Alto**. Alterações nos valores das transações causam perdas severas para o banco ou para o cliente, destruindo a confiança no sistema.
- **Disponibilidade:** O caixa eletrônico e a rede de comunicação com o banco devem estar operacionais e acessíveis quando o usuário precisar realizar um saque ou consulta.
  - *Grau de importância:* **Moderado a Alto**. Embora a indisponibilidade cause transtornos e afete a imagem da instituição (e a receita com taxas), ela geralmente não resulta em fraude direta ou roubo de fundos, diferentemente da falha nos dois anteriores.

Problema 1.2: Sistema de Comutação de Telefonia

- **Confidencialidade:** O conteúdo das chamadas de voz e os metadados (quem está ligando para quem, duração da chamada) não devem ser acessíveis a partes não autorizadas.
  - *Grau de importância:* **Alto**. A quebra desse requisito fere leis de privacidade e sigilo das telecomunicações.
- **Integridade:** O sistema não deve permitir que o número discado pelo usuário seja alterado em trânsito, garantindo que a chamada seja roteada para o destino correto. Também deve garantir que a comunicação não sofra interferências ou injeções.
  - *Grau de importância:* **Alto**. Falhas de integridade levariam ao caos no roteamento e faturamento incorreto.
- **Disponibilidade:** O serviço de telefonia deve estar ativo para completar chamadas sempre que solicitado, com capacidade para lidar com o volume de tráfego.
  - *Grau de importância:* **Alto**. A indisponibilidade de telefonia é crítica, especialmente por bloquear o acesso a serviços de emergência (polícia, bombeiros, ambulâncias).

Problema 1.3: Sistema de Editoração Eletrônica

- **a. Confidencialidade mais importante:** Um sistema usado para preparar relatórios financeiros trimestrais (balanços) de uma empresa de capital aberto antes de sua divulgação oficial ao mercado. O vazamento prévio configuraria crime de *insider trading*. Outro exemplo seria a editoração de provas de concursos públicos.
- **b. Integridade mais importante:** Um sistema de publicação do "Diário Oficial" do governo. Se uma lei, decreto ou valor de edital for alterado de forma não autorizada antes de ser publicado, o impacto legal e financeiro é imenso.
- **c. Disponibilidade mais importante:** Um sistema de portal de notícias diário (jornalismo de última hora). Se o sistema ficar fora do ar, a organização perde publicidade, acessos e furos de reportagem para os concorrentes.

Problema 1.4: Níveis de Impacto FIPS 199

- **a. Servidor web público:**
  - *Confidencialidade:* **Baixo**. Os dados são destinados ao público.
  - *Integridade:* **Moderado**. Uma alteração não autorizada (ex: *defacement* ou publicação de notícias falsas em nome da empresa) pode causar danos à reputação e perda de confiança.
  - *Disponibilidade:* **Moderado**. A indisponibilidade afeta a imagem pública e pode interromper serviços de atendimento primário.
- **b. Investigação policial sensível:**
  - *Confidencialidade:* **Alto**. O vazamento pode alertar suspeitos, arruinar investigações ou colocar vidas em risco.
  - *Integridade:* **Alto**. A alteração de evidências digitais ou registros pode invalidar um processo judicial.
  - *Disponibilidade:* **Moderado**. A perda temporária de acesso atrapalha, mas o foco primário é evitar que os dados vazem ou sejam corrompidos.
- **c. Organização financeira (administrativo rotineiro, sem privacidade):**
  - *Confidencialidade:* **Baixo**. Não há dados de clientes ou segredos de negócios envolvidos.
  - *Integridade:* **Baixo**. Informações de rotina administrativa (ex: reserva de salas, cardápio do refeitório) podem ser corrigidas facilmente se alteradas.
  - *Disponibilidade:* **Baixo**. O sistema não afeta o *core business* financeiro.
- **d. Aquisições (dados sensíveis de pré-solicitação + administrativos):**
  - *Separadamente:* Dados de pré-solicitação exigiriam Confidencialidade e Integridade **Altas**, enquanto os dados administrativos exigiriam níveis **Baixos**.
  - *Sistema Único (Impacto):* Se combinados, aplica-se o conceito de "marca d'água

elevada" (*high-water mark*). Todo o sistema herdaria as exigências mais rigorosas (Alto para C e I). Isso tornaria o gerenciamento do sistema rotineiro desnecessariamente caro, restritivo e complexo.

- **e. Indústria de energia (SCADA + administrativo):**
  - *Separadamente:* O SCADA exige Integridade e Disponibilidade **Altas** (falhas causam blecautes, riscos físicos ou interrupção de base militar). O administrativo exige níveis **Baixos**.
  - *Sistema Único (Impacto):* Mesclar o SCADA com a rede administrativa expõe o sistema de controle industrial (crítico) às mesmas vulnerabilidades da rede corporativa (e-mails, internet). Isso eleva drasticamente o risco de invasão ao SCADA via vetores administrativos, exigindo que o sistema inteiro seja classificado e isolado com níveis máximos de segurança, o que é ineficiente e perigoso.

Problema 1.5: Matriz de Serviços de Segurança vs. Ataques

Relacionamento (baseado na arquitetura OSI X.800) mostrando quais serviços protegem contra quais ataques:

Serviços de Segurança (X.800)	**Vazamento de Conteúdo (P)**	**Análise de Tráfego (P)**	**Disfarce (A)**	**Repasse (A)**	**Modificação (A)**	**Negação de Serviço (A)**
Autenticação de Entidade Par			X	X		
Autenticação de Origem de Dados			X		X	

Controle de Acesso			X			
Confidencialidade de Dados	X					
Confidencialidade de Fluxo		X				
Integridade de Dados				X	X	
Irretratabilidade			X			
Disponibilidade						X

(P = Ataque Passivo; A = Ataque Ativo)

Problema 1.6: Matriz de Mecanismos de Segurança vs. Ataques

Relacionamento entre os mecanismos específicos da X.800 e as ameaças que eles ajudam a mitigar:

Mecanismos de Segurança	Vazamento de Conteúdo (P)	Análise de Tráfego (P)	Disfarce (A)	Repasse (A)	Modificação (A)	Negação de Serviço (A)
Encriptação (Cifragem)	X					
Assinatura Digital			X		X	
Controle de Acesso	X		X			X
Integridade de Dados				X	X	
Troca de Autenticação			X	X		
Preenchimento de Tráfego		X				

Controle de Roteamento	X	X				X
Notarização			X		X	