Introdução a Segurança da Informação

Nome: *Gabriel Domingues Silva* ***Turma:*** *24E3-3*

Tema: TP2

Prof. Fabiano Alves Gisbert

Instituto Infnet

]

29 de novembro de 2024

1 O que é gestão de riscos em cibersegurança e qual a sua importância? Dê exemplos de situações práticas em que a gestão de riscos poderia ter evitado incidentes cibernéticos.

A **gestão de riscos em cibersegurança** é o processo de identificar, avaliar e mitigar os riscos relacionados à segurança digital de uma organização. Isso inclui proteger ativos como dados, sistemas e redes contra ameaças cibernéticas. Sua importância está na prevenção de danos financeiros, reputacionais e operacionais, garantindo a continuidade dos negócios.

1.1 Exemplo prático:

Imagine uma organização que não atualizou seus sistemas com patches de segurança. Um ataque ransomware explora uma vulnerabilidade conhecida, criptografando todos os dados da empresa. Com uma gestão de riscos eficiente, o seguinte poderia ter sido evitado:

- **Identificação**: Detectar a vulnerabilidade em sistemas desatualizados.
- **Mitigação**: Aplicar atualizações de segurança regularmente.
- **Prevenção**: Implementar backups automáticos e verificar sua integridade.

2 Defina com suas próprias palavras:

- **Vulnerabilidade:** Uma fraqueza ou falha em um sistema, software ou processo que pode ser explorada para causar danos.
- **Ameaça:** Um agente ou evento que pode explorar vulnerabilidades para causar prejuízos.
- **Risco:** A combinação da probabilidade de ocorrência de uma ameaça e o impacto potencial causado.
- **Ativo:** Qualquer recurso de valor para a organização, como dados, sistemas, equipamentos ou reputação.

3 Explique como é feita a análise de riscos em uma organização, listando as etapas principais. Forneça exemplos de ferramentas que podem ser utilizadas durante essas etapas (por exemplo, análise de vulnerabilidades, relatórios de auditoria).

1. **Identificação de ativos e ameaças:** Mapear recursos críticos e possíveis vetores de ataque.

2. **Avaliação de vulnerabilidades:** Realizar testes e auditorias para identificar fragilidades.
3. **Análise de impacto e probabilidade:** Determinar a severidade e a frequência de possíveis ataques.
4. **Definição de estratégias de mitigação:** Implementar medidas para reduzir riscos.

Ferramentas Utilizadas:

- *Nmap*: Para análise de vulnerabilidades.
- *Nessus*: Para realizar auditorias de segurança.
- *OWASP ZAP*: Para identificar falhas em aplicações web.

4 Quais são os principais métodos de mitigação de riscos e como podem ser aplicados na prática para reduzir o impacto de uma ameaça cibernética em uma organização? Cite exemplos concretos de medidas, como implementar firewalls, aplicar patches de segurança ou realizar backups frequentes.

- **Implementação de firewalls:** Bloqueio de tráfego não autorizado.
- **Patches de segurança:** Atualização de software para corrigir vulnerabilidades.
- **Backups frequentes:** Garantia de recuperação em caso de ataque.
- **Treinamento de funcionários:** Prevenção de ataques de engenharia social.

5 Explique a relação entre impacto e probabilidade na gestão de riscos em cibersegurança, ilustrando com exemplos práticos de decisões de mitigação baseadas nessa relação.

A matriz de impacto e probabilidade ajuda a priorizar riscos com base em dois critérios:

- **Impacto:** Consequências potenciais para a organização.
- **Probabilidade:** Chances de uma ameaça ocorrer.

Por exemplo, um ataque de phishing pode ter alta probabilidade, mas impacto médio, enquanto um ataque ransomware pode ter baixa probabilidade, mas impacto catastrófico.

6 Uma empresa de e-commerce identificou uma vulnerabilidade em seu sistema de pagamento online. O risco de exploração é médio, mas o impacto potencial é muito alto, já que pode comprometer informações financeiras de clientes.

Cenário: Uma vulnerabilidade foi identificada no sistema de pagamento online.

- **Risco:** Exploração de dados financeiros dos clientes.
- **Mitigação:** Implementar correções imediatas e fortalecer a segurança do sistema.

Matriz de Impacto x Probabilidade:

	Baixo Impacto	**Médio Impacto**	**Alto Impacto**
Alta Probabilidade	—	—	**Risco atual**
Média Probabilidade	—	—	—
Baixa Probabilidade	—	—	—

7 Descreva as principais camadas de uma estrutura de rede (por exemplo, camada de acesso, transporte, aplicação) e os tipos de vulnerabilidades associadas a cada uma delas. Cite exemplos de ferramentas ou práticas de segurança recomendadas para proteger cada camada.

- **Camada de Acesso:** Falhas em autenticação e dispositivos não gerenciados.
- **Camada de Transporte:** Interceptação de dados por meio de ataques *Man-in-the-Middle*.
- **Camada de Aplicação:** Exploração de vulnerabilidades em softwares.

Práticas de Proteção:

- Controle de acesso rigoroso.
- Criptografia de dados.
- Monitoramento de atividades anômalas.

8 Explique como o uso de dispositivos sem proteção adequada pode comprometer a segurança de uma rede. Dê exemplos práticos de falhas de segurança envolvendo dispositivos pessoais ou IoT mal configurados.

Exemplo: Um dispositivo IoT mal configurado pode permitir que invasores acessem a rede corporativa. Medidas de mitigação incluem segregação de redes e configuração segura.

9 Durante uma auditoria, foi descoberto que vários dispositivos na rede da sua empresa possuem firmware desatualizado, o que expõe a rede a potenciais exploits conhecidos.Qual seria sua estratégia para resolver essa vulnerabilidade sem causar grandes interrupções nas operações da empresa? Detalhe um plano de atualização escalonado que minimize o tempo de inatividade.

Plano de Ação Escalonado:

1. Identificar dispositivos críticos.
2. Atualizar dispositivos em horários de baixa utilização.
3. Verificar funcionalidade após cada etapa.

10 Explique de que maneira o monitoramento contínuo e detalhado da rede contribui para a identificação de vulnerabilidades, especificando como ele permite detectar padrões anômalos, comportamentos suspeitos e possíveis falhas de segurança que possam ser exploradas por agentes mal-intencionados.

O monitoramento contínuo permite:

- Detecção precoce de atividades suspeitas.
- Correção de falhas antes que sejam exploradas.
- Registro de logs para análise forense.

11 O que é um ataque de "MAC flooding"em um switch e como ele compromete a segurança da rede? Dê um exemplo de como esse tipo de ataque pode ser identificado e mitigado na prática.

Definição: Saturação da tabela de endereços de um switch com entradas falsas, forçando-o a agir como um *hub*. Isso permite o acesso a dados confidenciais. **Mitigação:** Configuração de segurança de portas e limite de endereços MAC.

12 Quais estratégias proativas de segurança são mais eficazes na prevenção de ataques de "MAC flooding"? Considere o uso de funcionalidades específicas de switches, como port security e VLANs, e explique como cada uma contribui para a proteção contra esse tipo de ameaça.

- **Port Security:** Limitação do número de endereços MAC por porta.
- **VLANs:** Segmentação de rede para isolar tráfego.