Objetivo da Aula (Criação de um Plano de Ação)

- Entender os conceitos de ameaças e vulnerabilidades no contexto da segurança da informação.
- Identificar diferentes tipos de ameaças e vulnerabilidades e suas possíveis consequências.
- Aprender sobre estratégias e ferramentas para proteger informações contra essas ameaças e vulnerabilidades.

Parte 1: Introdução (30 minutos)

- Breve revisão teórica sobre ameaças e vulnerabilidades à segurança da informação.
- Discussão em grupo sobre notícias recentes envolvendo quebras de segurança e vazamento de dados.

Parte 2: Identificação de Ameaças e Vulnerabilidades (45 minutos)

- **Atividade Prática:** Divida os alunos em pequenos grupos e distribua descrições de cenários reais (sem identificação) de quebras de segurança em empresas. Peça para cada grupo identificar as possíveis ameaças e vulnerabilidades apresentadas nos cenários.
- Discussão em grupo sobre as ameaças e vulnerabilidades identificadas, complementando com exemplos reais de como essas questões foram ou poderiam ser mitigadas.

Parte 3: Estratégias de Proteção (45 minutos)

- **Atividade Prática:** Utilizando softwares de simulação de segurança (como o GNS3 com appliances de segurança) ou ferramentas de análise de vulnerabilidade (como o Nessus, em um ambiente controlado), permita que os alunos executem uma análise básica de vulnerabilidade em uma rede simulada.
- Discussão sobre as vulnerabilidades encontradas e quais medidas de segurança (tais como firewalls, antivírus, atualizações de software) poderiam ser aplicadas para mitigar os riscos.

Parte 4: Criação de um Plano de Ação (30 minutos)

- **Atividade Prática:** Com base nas discussões e nas atividades práticas anteriores, peça aos grupos para elaborar um plano de ação simples para aumentar a segurança da informação em um dos cenários apresentados. O plano deve incluir ações preventivas, detecção de ameaças e respostas a incidentes.
- Apresentações dos planos de ação por cada grupo, com feedback dos colegas e do professor.

Conclusão e Feedback (20 minutos)

- Recapitulação dos pontos principais discutidos durante a aula.
- Sessão aberta de perguntas e respostas para esclarecer dúvidas.

- Solicitação de feedback aos alunos sobre a aula prática, incluindo o que aprenderam e o que poderia ser melhorado em futuras sessões.

Materiais e Recursos Necessários

- Descrições de cenários de quebras de segurança.
- Acesso a computadores com internet e software de simulação de rede ou ferramentas de análise de vulnerabilidade.
- Materiais de leitura complementar sobre estratégias de proteção e resposta a incidentes.

Parte 2: Identificação de Ameaças e Vulnerabilidades (45 minutos)

Cenário 1 (Grupo 1): Ataque de Ransomware

- ✓ Uma empresa de contabilidade teve seus sistemas críticos criptografados por um ataque de ransomware, resultando na perda de acesso a dados financeiros vitais. O ataque foi lançado por meio de um e-mail de phishing que um funcionário inadvertidamente abriu.

Cenário 2 (Grupo 2): Vazamento de Dados de Clientes

- ✓ Um varejista online sofreu um vazamento de dados, expondo informações de cartão de crédito de milhares de clientes. Uma configuração incorreta em um servidor de banco de dados permitiu o acesso não autorizado.

Cenário 3 (Grupo 3): Ataque de Negação de Serviço (DDoS)

- ✓ Uma plataforma de mídia social experimentou vários ataques DDoS, tornando o serviço indisponível por períodos prolongados. Os ataques foram coordenados através de uma rede de botnets.

Cenário 4 (Grupo 4): Ameaça Interna

- ✓ Um ex-funcionário de uma empresa de tecnologia utilizou credenciais ainda ativas para acessar e excluir importantes projetos de software, demonstrando a falta de políticas eficazes de gerenciamento de acessos e saída de funcionários.

Cenário 5 (Grupo 5): Injeção de SQL

- ✓ Um site de notícias foi comprometido por meio de uma vulnerabilidade de injeção de SQL, permitindo que invasores acessassem e divulgassem informações confidenciais armazenadas no banco de dados.

Cenário 6 (Grupo 6): Phishing Direcionado (Spear Phishing)

- ✓ Diretores de uma empresa de investimentos foram alvo de uma campanha de spear phishing, levando ao comprometimento de informações financeiras sensíveis. Os e-mails maliciosos foram cuidadosamente personalizados para parecerem legítimos.

Cenário 7 (Grupo 7): Falha de Segurança em Terceiros

- ✓ Dados de clientes de um banco foram expostos após um ataque cibernético a um fornecedor terceirizado responsável pelo processamento de dados. O fornecedor não tinha medidas de segurança adequadas.

Cenário 8 (Grupo 8): Vulnerabilidade de Software Não Corrigida

- ✓ Uma empresa de software não aplicou uma atualização de segurança crítica, resultando na exploração de uma vulnerabilidade conhecida. Isso permitiu que atacantes acessassem remotamente o sistema.

Cenário 9 (Grupo 9): Engenharia Social

- ✓ Através de técnicas de engenharia social, invasores convenceram um funcionário de atendimento ao cliente a fornecer acesso a contas de clientes, comprometendo dados pessoais e financeiros.

Cenário 10 (Grupo 10): Ataque via Dispositivo IoT Inseguro

- ✓ Dispositivos IoT inseguros em uma rede corporativa foram explorados para estabelecer uma base de operações para ataques mais amplos dentro da rede, expondo dados confidenciais de negócios.