Resolução dos Cenários Práticos

Cenário 1: Ataque de Ransomware

- **Ameaças:** Phishing, malware.
- **Vulnerabilidades:** Falta de treinamento de funcionários, ausência de antivírus atualizado.
- **Plano de Ação:** Implementar treinamento de conscientização, instalar e atualizar antivírus, realizar backups regulares.

Cenário 2: Vazamento de Dados de Clientes

- **Ameaças:** Acesso não autorizado.
- **Vulnerabilidades:** Configuração incorreta do servidor.
- **Plano de Ação:** Revisar e corrigir configurações de segurança, implementar controles de acesso rígidos.

Cenário 3: Ataque de Negação de Serviço (DDoS)

- **Ameaças:** Botnets, tráfego malicioso.
- **Vulnerabilidades:** Insuficiência de medidas de mitigação DDoS.
- **Plano de Ação:** Utilizar serviços de mitigação DDoS, monitorar tráfego de rede.

Cenário 4: Ameaça Interna

- **Ameaças:** Acesso não autorizado por ex-funcionário.
- **Vulnerabilidades:** Políticas de acesso inadequadas.
- **Plano de Ação:** Implementar políticas de gerenciamento de acessos, desativar contas de ex-funcionários imediatamente.

Cenário 5: Injeção de SQL

- **Ameaças:** Invasores explorando falhas de software.
- **Vulnerabilidades:** Falta de sanitização de entrada de dados.
- **Plano de Ação:** Implementar práticas seguras de codificação, realizar testes de penetração.

Cenário 6: Phishing Direcionado (Spear Phishing)

- **Ameaças:** Emails maliciosos personalizados.
- **Vulnerabilidades:** Falta de treinamento de funcionários.
- **Plano de Ação:** Conscientização e treinamento em segurança, implementação de filtros de email avançados.

Cenário 7: Falha de Segurança em Terceiros

- **Ameaças:** Acesso não autorizado através de fornecedores.
- **Vulnerabilidades:** Medidas de segurança inadequadas de terceiros.

- **Plano de Ação:** Realizar auditorias de segurança em fornecedores, implementar contratos com requisitos de segurança.

Cenário 8: Vulnerabilidade de Software Não Corrigida

- **Ameaças:** Exploração de vulnerabilidades conhecidas.
- **Vulnerabilidades:** Falta de atualização de software.
- **Plano de Ação:** Aplicar atualizações de segurança regularmente, monitorar e gerenciar vulnerabilidades.

Cenário 9: Engenharia Social

- **Ameaças:** Manipulação de funcionários.
- **Vulnerabilidades:** Falta de conscientização.
- **Plano de Ação:** Treinamento em engenharia social, implementar políticas de verificação de identidade.

Cenário 10: Ataque via Dispositivo IoT Inseguro

- **Ameaças:** Exploração de dispositivos IoT.
- **Vulnerabilidades:** Falta de segurança em dispositivos IoT.
- **Plano de Ação:** Implementar segurança em dispositivos IoT, segmentar redes.