Plano de Ação de Segurança da Informação

Introdução

Este plano de ação tem como objetivo aumentar a segurança da informação de uma organização, baseado na Norma ISO/IEC 27001, boas práticas em segurança da informação e gestão de risco. Ele inclui ações preventivas, detecção de ameaças e respostas a incidentes para diferentes cenários de ameaças e vulnerabilidades.

Estrutura do Plano de Ação

1. Identificação dos Ativos e Riscos

- **Ativos:** Identificar os ativos de informação críticos, como sistemas, dados financeiros, dados de clientes, etc.
- **Ameaças e Vulnerabilidades:** Mapear as ameaças e vulnerabilidades relacionadas a esses ativos.

2. Análise e Avaliação de Riscos

- **Impacto:** Avaliar o impacto potencial de cada ameaça e vulnerabilidade.
- **Probabilidade:** Determinar a probabilidade de ocorrência de cada risco.

3. Controles de Segurança (Baseados na ISO/IEC 27001)

- **Políticas de Segurança da Informação:** Definir e implementar políticas de segurança abrangentes.
- **Organização da Segurança da Informação:** Estabelecer uma estrutura organizacional clara para a gestão da segurança da informação.
- **Segurança dos Recursos Humanos:** Implementar medidas de segurança desde a contratação até a saída dos funcionários.
- **Gestão de Ativos:** Assegurar que os ativos de informação são devidamente gerenciados e protegidos.
- **Controle de Acesso:** Implementar controles de acesso apropriados para proteger a informação.
- **Criptografia:** Usar criptografia para proteger a confidencialidade e integridade das informações.
- **Segurança Física e Ambiental:** Proteger fisicamente os locais onde os ativos de informação são armazenados.
- **Segurança Operacional:** Implementar procedimentos de segurança para a operação dos sistemas de informação.
- **Segurança nas Comunicações:** Garantir a segurança das informações em trânsito.

- **Aquisição, Desenvolvimento e Manutenção de Sistemas:** Integrar a segurança da informação no ciclo de vida dos sistemas.
- **Relacionamento com Fornecedores:** Assegurar que os fornecedores cumpram com os requisitos de segurança.
- **Gestão de Incidentes de Segurança:** Estabelecer procedimentos para a gestão de incidentes de segurança da informação.
- **Continuidade dos Negócios:** Implementar medidas para assegurar a continuidade dos negócios.
- **Conformidade:** Garantir que a organização está em conformidade com as exigências legais e regulamentares.

4. Implementação do Plano de Ação

Cada cenário identificado será tratado de acordo com a metodologia descrita acima. Abaixo está a implementação detalhada para cada cenário prático:

Cenário 1: Ataque de Ransomware

1. **Ações Preventivas**
    - **Treinamento de Conscientização:** Realizar treinamentos regulares de conscientização sobre segurança da informação e phishing para os funcionários.
    - **Implementação de Antivírus:** Instalar e manter atualizados softwares antivírus e anti-malware em todos os sistemas.
    - **Backup Regular:** Implementar uma política de backup regular e assegurar que os backups sejam armazenados de forma segura.
2. **Detecção de Ameaças**
    - **Monitoramento Contínuo:** Implementar sistemas de monitoramento contínuo para detectar atividades suspeitas.
    - **Alertas e Notificações:** Configurar alertas para atividades anômalas que possam indicar um ataque de ransomware.
3. **Resposta a Incidentes**
    - **Plano de Resposta a Incidentes:** Desenvolver e testar regularmente um plano de resposta a incidentes específico para ataques de ransomware.
    - **Isolamento de Sistemas:** Em caso de detecção de ransomware, isolar os sistemas afetados imediatamente para prevenir a propagação.
    - **Recuperação de Dados:** Utilizar backups seguros para restaurar dados e sistemas afetados.

Cenário 2: Vazamento de Dados de Clientes

4. **Ações Preventivas**
    - **Configuração Segura de Servidores:** Revisar e corrigir configurações de segurança em servidores de banco de dados.
    - **Criptografia de Dados:** Implementar criptografia para dados sensíveis, tanto em repouso quanto em trânsito.

- **Controle de Acesso:** Implementar controles rigorosos de acesso aos sistemas de banco de dados.

5. **Detecção de Ameaças**
   - **Monitoramento de Acesso:** Monitorar e registrar acessos aos dados sensíveis.
   - **Auditoria de Segurança:** Realizar auditorias de segurança periódicas para identificar possíveis vulnerabilidades.
6. **Resposta a Incidentes**
   - **Notificação de Incidentes:** Estabelecer um processo de notificação rápida para informar partes interessadas e reguladores sobre vazamentos de dados.
   - **Análise Forense:** Realizar análises forenses para entender a origem do vazamento e evitar recorrências.
   - **Remediação:** Corrigir as falhas de segurança identificadas e reforçar as medidas de proteção.

Cenário 3: Ataque de Negação de Serviço (DDoS)

7. **Ações Preventivas**
   - **Serviços de Mitigação DDoS:** Utilizar serviços de mitigação de DDoS oferecidos por provedores de hospedagem ou empresas especializadas.
   - **Capacidade de Redundância:** Implementar redundância de capacidade para absorver picos de tráfego.
   - **Regras de Firewall:** Configurar firewalls para bloquear tráfego malicioso identificado.
8. **Detecção de Ameaças**
   - **Monitoramento de Tráfego:** Utilizar sistemas de monitoramento de rede para detectar padrões de tráfego incomuns que podem indicar um ataque DDoS.
   - **Alertas Automáticos:** Configurar alertas automáticos para picos de tráfego que correspondam a ataques DDoS.
9. **Resposta a Incidentes**
   - **Isolamento de Tráfego:** Redirecionar ou isolar tráfego malicioso para proteger a infraestrutura principal.
   - **Contato com Provedores:** Trabalhar com provedores de serviços de internet para mitigar o ataque.
   - **Recuperação do Serviço:** Restaurar o serviço normal o mais rápido possível e implementar medidas adicionais para prevenir futuros ataques.

Cenário 4: Ameaça Interna

10. **Ações Preventivas**

- **Políticas de Acesso:** Implementar políticas rigorosas de gerenciamento de acessos, garantindo que ex-funcionários tenham suas credenciais desativadas imediatamente após a saída.
- **Monitoramento de Atividades:** Monitorar atividades dos usuários para detectar comportamentos anômalos.
- **Conscientização e Treinamento:** Treinar funcionários sobre os riscos de ameaças internas e como preveni-las.

11. **Detecção de Ameaças**
    - **Sistema de Detecção de Intrusões (IDS):** Utilizar IDS para monitorar e alertar sobre atividades suspeitas.
    - **Análise de Logs:** Realizar análise regular de logs de sistema para identificar acessos não autorizados.
12. **Resposta a Incidentes**
    - **Revogação de Acessos:** Revogar imediatamente qualquer acesso detectado como não autorizado.
    - **Investigação Interna:** Conduzir uma investigação interna para identificar a origem da ameaça e tomar medidas disciplinares se necessário.
    - **Reforço de Políticas:** Atualizar políticas de segurança com base nas lições aprendidas.

Cenário 5: Injeção de SQL

13. **Ações Preventivas**
    - **Sanitização de Entradas:** Implementar práticas de codificação seguras, como sanitização de entradas e uso de consultas parametrizadas.
    - **Testes de Penetração:** Realizar testes de penetração regulares para identificar e corrigir vulnerabilidades.
    - **Atualizações de Software:** Manter sistemas e aplicativos atualizados com as últimas correções de segurança.
14. **Detecção de Ameaças**
    - **Ferramentas de Varredura:** Utilizar ferramentas de varredura de vulnerabilidades para identificar possíveis falhas de injeção de SQL.
    - **Monitoramento de Acessos:** Monitorar logs de acesso ao banco de dados para detectar padrões anômalos.
15. **Resposta a Incidentes**
    - **Bloqueio de Acessos:** Bloquear imediatamente os acessos suspeitos ao banco de dados.
    - **Correção de Vulnerabilidades:** Aplicar correções de segurança e reconfigurar o código vulnerável.
    - **Revisão de Código:** Realizar uma revisão completa do código para assegurar que todas as vulnerabilidades foram mitigadas.

Cenário 6: Phishing Direcionado (Spear Phishing)

16. **Ações Preventivas**
    - **Treinamento de Conscientização:** Realizar treinamentos regulares para educar os funcionários sobre spear phishing e como identificar e evitar tais ataques.
    - **Filtros de E-mail:** Implementar filtros avançados de e-mail para bloquear mensagens suspeitas.
    - **Autenticação Multifator (MFA):** Implementar MFA para aumentar a segurança de acessos.
17. **Detecção de Ameaças**
    - **Análise de E-mails:** Utilizar ferramentas de análise para detectar e-mails de phishing.
    - **Alertas de Phishing:** Configurar alertas para atividades que correspondam a padrões de phishing.
18. **Resposta a Incidentes**
    - **Isolamento de Contas Comprometidas:** Isolar contas comprometidas para evitar propagação de danos.
    - **Notificação e Mitigação:** Notificar imediatamente os funcionários e tomar medidas para mitigar o impacto.
    - **Revisão de Procedimentos:** Atualizar procedimentos de segurança para evitar futuras ocorrências.

Cenário 7: Falha de Segurança em Terceiros

19. **Ações Preventivas**
    - **Contratos de Segurança:** Estabelecer contratos de segurança com fornecedores que incluam requisitos rigorosos de segurança.
    - **Auditorias de Segurança:** Realizar auditorias de segurança regulares em fornecedores.
    - **Avaliação de Riscos de Terceiros:** Implementar uma avaliação contínua dos riscos de segurança associados aos fornecedores.
20. **Detecção de Ameaças**
    - **Monitoramento de Atividades de Fornecedores:** Monitorar as atividades dos fornecedores para detectar comportamentos anômalos.
    - **Relatórios de Conformidade:** Exigir relatórios regulares de conformidade de segurança dos fornecedores.
21. **Resposta a Incidentes**
    - **Isolamento de Sistemas:** Isolar sistemas afetados para evitar a propagação de danos.
    - **Investigação e Remediação:** Conduzir uma investigação para determinar a origem da falha de segurança e implementar medidas de remediação.

- **Revisão de Contratos:** Revisar e atualizar os contratos de segurança com base nas lições aprendidas.

Cenário 8: Vulnerabilidade de Software Não Corrigida

22. **Ações Preventivas**
    - **Atualizações Regulares:** Estabelecer um cronograma regular para aplicar atualizações de segurança.
    - **Gestão de Patches:** Implementar um processo de gestão de patches para assegurar que todas as atualizações críticas sejam aplicadas imediatamente.
    - **Verificação de Vulnerabilidades:** Utilizar ferramentas de verificação de vulnerabilidades para identificar e corrigir falhas de segurança.
23. **Detecção de Ameaças**
    - **Monitoramento de Atualizações:** Monitorar atualizações de segurança e alertas de fornecedores de software.
    - **Teste de Vulnerabilidades:** Realizar testes regulares para identificar vulnerabilidades em sistemas e aplicativos.
24. **Resposta a Incidentes**
    - **Aplicação de Patches:** Aplicar imediatamente patches de segurança disponíveis para corrigir vulnerabilidades.
    - **Reconfiguração de Sistemas:** Reconfigurar sistemas para eliminar a exposição a vulnerabilidades conhecidas.
    - **Revisão de Políticas de Atualização:** Atualizar políticas e procedimentos para assegurar uma resposta rápida a novas vulnerabilidades.

Cenário 9: Engenharia Social

25. **Ações Preventivas**
    - **Treinamento de Funcionários:** Implementar treinamentos regulares sobre os riscos e táticas de engenharia social.
    - **Políticas de Verificação:** Estabelecer políticas de verificação rigorosas para solicitações de informações sensíveis.
    - **Conscientização Continuada:** Promover uma cultura de conscientização sobre segurança entre todos os funcionários.
26. **Detecção de Ameaças**
    - **Monitoramento de Solicitações:** Monitorar solicitações de informações para identificar padrões de engenharia social.
    - **Alertas de Comportamento:** Configurar alertas para comportamentos que possam indicar tentativas de engenharia social.
27. **Resposta a Incidentes**
    - **Bloqueio de Acessos Indevidos:** Bloquear imediatamente acessos indevidos identificados através de engenharia social.

- **Investigação e Correção:** Conduzir uma investigação para entender como o ataque foi bem-sucedido e implementar medidas corretivas.
- **Reforço de Treinamento:** Reforçar o treinamento e conscientização entre os funcionários após um incidente.

Cenário 10: Ataque via Dispositivo IoT Inseguro

28. **Ações Preventivas**
    - **Segurança de Dispositivos IoT:** Implementar medidas de segurança em todos os dispositivos IoT, como senhas fortes e atualizações regulares de firmware.
    - **Segmentação de Rede:** Segmentar a rede para isolar dispositivos IoT de sistemas críticos.
    - **Monitoramento de IoT:** Utilizar sistemas de monitoramento específicos para dispositivos IoT.
29. **Detecção de Ameaças**
    - **Monitoramento de Dispositivos:** Monitorar dispositivos IoT para atividades anômalas.
    - **Alertas de Segurança IoT:** Configurar alertas para detectar comportamentos suspeitos em dispositivos IoT.
30. **Resposta a Incidentes**
    - **Isolamento de Dispositivos:** Isolar dispositivos IoT comprometidos para prevenir a propagação de ataques.
    - **Investigação de Brechas:** Conduzir uma investigação para identificar a vulnerabilidade explorada e corrigir a falha.
    - **Atualização de Políticas de IoT:** Revisar e atualizar políticas de segurança para dispositivos IoT com base nas lições aprendidas.

5. Monitoramento e Revisão

- **Avaliação Contínua:** Monitorar a eficácia das medidas de segurança implementadas e realizar avaliações contínuas.
- **Atualização do Plano:** Revisar e atualizar o plano de ação periodicamente para refletir mudanças no ambiente de ameaças e vulnerabilidades.

6. Documentação e Relatórios

- **Relatórios de Incidentes:** Documentar todos os incidentes de segurança e as ações tomadas em resposta.
- **Registros de Conformidade:** Manter registros detalhados para demonstrar conformidade com a ISO/IEC 27001 e outras regulamentações aplicáveis.