Guia de Implementação do Plano de Ação para os Alunos

Estrutura do Plano de Ação

1. **Introdução**
    - Definir o objetivo do plano de ação.
    - Descrever brevemente o cenário específico do grupo.
2. **Identificação dos Ativos e Riscos**
    - Listar os ativos de informação críticos relacionados ao cenário.
    - Identificar ameaças e vulnerabilidades específicas.
3. **Análise e Avaliação de Riscos**
    - Avaliar o impacto potencial de cada ameaça e vulnerabilidade.
    - Determinar a probabilidade de ocorrência de cada risco.
4. **Controles de Segurança (Baseados na ISO/IEC 27001)**
    - Descrever as políticas e medidas de segurança a serem implementadas.
    - Explicar como cada controle de segurança será aplicado ao cenário específico.
5. **Implementação do Plano de Ação**
    - Detalhar as ações preventivas, detecção de ameaças e respostas a incidentes para o cenário.
6. **Monitoramento e Revisão**
    - Definir como o grupo monitorará a eficácia das medidas implementadas.
    - Explicar o processo de revisão e atualização do plano.
7. **Documentação e Relatórios**
    - Descrever como os incidentes e ações serão documentados.
    - Explicar a importância da documentação para conformidade e melhorias contínuas.

Implementação para Cada Cenário

Cenário 1: Ataque de Ransomware (Grupo 1)

8. **Introdução**
    - Objetivo: Proteger os sistemas críticos de uma empresa de contabilidade contra ataques de ransomware.
    - Cenário: Sistema criptografado por ransomware via e-mail de phishing.
9. **Identificação dos Ativos e Riscos**
    - Ativos: Dados financeiros, sistemas de contabilidade.
    - Ameaças: Phishing, ransomware.
    - Vulnerabilidades: Falta de treinamento, ausência de antivírus atualizado.
10. **Análise e Avaliação de Riscos**
    - Impacto: Alto (perda de acesso a dados vitais).
    - Probabilidade: Alta (e-mails de phishing são comuns).
11. **Controles de Segurança**
    - Políticas de Conscientização: Treinamento regular sobre phishing e segurança da informação.
    - Antivírus: Instalar e atualizar software antivírus.
    - Backup: Realizar backups regulares e armazenar de forma segura.
12. **Implementação do Plano de Ação**
    - Ações Preventivas: Conscientização e treinamento, antivírus atualizado, política de backup.
    - Detecção: Monitoramento de e-mails, alertas de atividades suspeitas.
    - Resposta: Isolamento de sistemas afetados, restauração de dados de backups.
13. **Monitoramento e Revisão**
    - Monitoramento: Ferramentas de monitoramento de e-mails e sistemas.
    - Revisão: Revisão periódica de políticas e procedimentos de segurança.
14. **Documentação e Relatórios**
    - Relatórios de Incidentes: Documentar incidentes de ransomware e ações tomadas.
    - Registros de Treinamento: Manter registros de treinamentos de conscientização realizados.

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

15. **Introdução**
    - Objetivo: Proteger dados de clientes de um varejista online contra vazamentos.
    - Cenário: Vazamento de dados devido a configuração incorreta de servidor de banco de dados.
16. **Identificação dos Ativos e Riscos**
    - Ativos: Dados de clientes, informações de cartão de crédito.
    - Ameaças: Acesso não autorizado.

- Vulnerabilidades: Configuração incorreta do servidor.

17. **Análise e Avaliação de Riscos**
    - Impacto: Alto (exposição de dados de clientes).
    - Probabilidade: Média (erro de configuração).
18. **Controles de Segurança**
    - Configuração Segura: Revisar e corrigir configurações de segurança.
    - Criptografia: Implementar criptografia de dados.
    - Controle de Acesso: Controles rigorosos de acesso ao banco de dados.
19. **Implementação do Plano de Ação**
    - Ações Preventivas: Configuração segura, criptografia de dados, controles de acesso.
    - Detecção: Monitoramento de acessos, auditorias regulares.
    - Resposta: Notificação rápida de vazamentos, análise forense, remediação.
20. **Monitoramento e Revisão**
    - Monitoramento: Ferramentas de monitoramento de banco de dados.
    - Revisão: Auditorias de segurança periódicas.
21. **Documentação e Relatórios**
    - Relatórios de Incidentes: Documentar vazamentos de dados e ações corretivas.
    - Registros de Configuração: Manter registros de configurações de segurança.

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

22. **Introdução**
    - Objetivo: Proteger uma plataforma de mídia social contra-ataques DDoS.
    - Cenário: Ataques DDoS coordenados por botnets.
23. **Identificação dos Ativos e Riscos**
    - Ativos: Serviços de plataforma de mídia social.
    - Ameaças: Ataques DDoS.
    - Vulnerabilidades: Insuficiência de medidas de mitigação.
24. **Análise e Avaliação de Riscos**
    - Impacto: Alto (indisponibilidade do serviço).
    - Probabilidade: Alta (ataques DDoS são comuns).
25. **Controles de Segurança**
    - Mitigação DDoS: Utilizar serviços de mitigação de DDoS.
    - Redundância: Implementar redundância de capacidade.
    - Regras de Firewall: Configurar firewalls para bloquear tráfego malicioso.
26. **Implementação do Plano de Ação**
    - Ações Preventivas: Serviços de mitigação DDoS, redundância, regras de firewall.
    - Detecção: Monitoramento de tráfego, alertas automáticos.

- Resposta: Isolamento de tráfego, contato com provedores, recuperação do serviço.

27. **Monitoramento e Revisão**
    - Monitoramento: Sistemas de monitoramento de rede.
    - Revisão: Revisão periódica de medidas de mitigação.
28. **Documentação e Relatórios**
    - Relatórios de Incidentes: Documentar ataques DDoS e respostas.
    - Registros de Configuração: Manter registros de configuração de firewall e redundância.

Cenário 4: Ameaça Interna (Grupo 4)

29. **Introdução**
    - Objetivo: Proteger uma empresa de tecnologia contra ameaças internas.
    - Cenário: Ex-funcionário utiliza credenciais ativas para acessar e excluir projetos.
30. **Identificação dos Ativos e Riscos**
    - Ativos: Projetos de software.
    - Ameaças: Acesso não autorizado por ex-funcionário.
    - Vulnerabilidades: Políticas de acesso inadequadas.
31. **Análise e Avaliação de Riscos**
    - Impacto: Alto (perda de projetos importantes).
    - Probabilidade: Média (acessos não desativados).
32. **Controles de Segurança**
    - Políticas de Acesso: Gerenciamento rigoroso de acessos.
    - Monitoramento de Atividades: Monitorar atividades dos usuários.
    - Conscientização: Treinamento sobre ameaças internas.
33. **Implementação do Plano de Ação**
    - Ações Preventivas: Políticas de acesso, monitoramento, treinamento.
    - Detecção: IDS, análise de logs.
    - Resposta: Revogação de acessos, investigação interna, reforço de políticas.
34. **Monitoramento e Revisão**
    - Monitoramento: IDS e análise de logs.
    - Revisão: Revisão de políticas de acesso.
35. **Documentação e Relatórios**
    - Relatórios de Incidentes: Documentar acessos não autorizados.
    - Registros de Treinamento: Manter registros de treinamento de conscientização.

Cenário 5: Injeção de SQL (Grupo 5)

36. **Introdução**
    - Objetivo: Proteger um site de notícias contra injeções de SQL.

- Cenário: Invasores exploram vulnerabilidade de SQL para acessar informações confidenciais.

37. **Identificação dos Ativos e Riscos**
    - Ativos: Banco de dados do site.
    - Ameaças: Injeção de SQL.
    - Vulnerabilidades: Falta de sanitização de entrada de dados.
38. **Análise e Avaliação de Riscos**
    - Impacto: Alto (exposição de informações confidenciais).
    - Probabilidade: Média (vulnerabilidade de SQL).
39. **Controles de Segurança**
    - Sanitização de Entradas: Práticas seguras de codificação.
    - Testes de Penetração: Realizar testes regulares.
    - Atualizações de Software: Manter sistemas atualizados.
40. **Implementação do Plano de Ação**
    - Ações Preventivas: Sanitização de entradas, testes de penetração, atualizações.
    - Detecção: Ferramentas de varredura, monitoramento de acessos.
    - Resposta: Bloqueio de acessos, correção de vulnerabilidades, revisão de código.
41. **Monitoramento e Revisão**
    - Monitoramento: Ferramentas de varredura e monitoramento de banco de dados.
    - Revisão: Revisão de políticas de atualização e práticas de codificação.
42. **Documentação e Relatórios**
    - Relatórios de Incidentes: Documentar injeções de SQL e correções.
    - Registros de Testes: Manter registros de testes de penetração realizados.

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

43. **Introdução**
    - Objetivo: Proteger uma empresa de investimentos contra spear phishing.
    - Cenário: Diretores são alvos de e-mails maliciosos personalizados.
44. **Identificação dos Ativos e Riscos**
    - Ativos: Informações financeiras sensíveis.
    - Ameaças: Spear phishing.
    - Vulnerabilidades: Falta de treinamento, ausência de filtros avançados.
45. **Análise e Avaliação de Riscos**
    - Impacto: Alto (comprometimento de informações financeiras).
    - Probabilidade: Alta (e-mails maliciosos personalizados).
46. **Controles de Segurança**
    - Treinamento de Conscientização: Educação sobre spear phishing.
    - Filtros de E-mail: Implementar filtros avançados.

- Autenticação Multifator (MFA): Implementar MFA.

47. Implementação do Plano de Ação

- Ações Preventivas: Treinamento, filtros de e-mail, MFA.
- Detecção: Análise de e-mails, alertas de phishing.
- Resposta: Isolamento de contas comprometidas, notificação e mitigação, revisão de procedimentos.

48. Monitoramento e Revisão

- Monitoramento: Ferramentas de análise de e-mails e alertas de phishing.
- Revisão: Revisão de procedimentos de segurança e treinamentos.

49. Documentação e Relatórios

- Relatórios de Incidentes: Documentar ataques de spear phishing e respostas.
- Registros de Treinamento: Manter registros de treinamentos de conscientização.

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

50. Introdução

- Objetivo: Proteger dados de clientes de um banco contra falhas de segurança de fornecedores.
- Cenário: Dados expostos devido a ataque cibernético a fornecedor terceirizado.

51. Identificação dos Ativos e Riscos

- Ativos: Dados de clientes.
- Ameaças: Acesso não autorizado através de fornecedores.
- Vulnerabilidades: Medidas de segurança inadequadas de terceiros.

52. Análise e Avaliação de Riscos

- Impacto: Alto (exposição de dados de clientes).
- Probabilidade: Média (segurança de terceiros).

53. Controles de Segurança

- Contratos de Segurança: Estabelecer contratos com requisitos de segurança.
- Auditorias de Segurança: Auditorias regulares em fornecedores.
- Avaliação de Riscos de Terceiros: Avaliação contínua dos riscos de segurança.

54. Implementação do Plano de Ação

- Ações Preventivas: Contratos de segurança, auditorias, avaliação de riscos.
- Detecção: Monitoramento de atividades de fornecedores, relatórios de conformidade.
- Resposta: Isolamento de sistemas afetados, investigação e remediação, revisão de contratos.

55. Monitoramento e Revisão

- Monitoramento: Atividades de fornecedores e conformidade.

- Revisão: Auditorias de segurança e contratos.

56. Documentação e Relatórios

- Relatórios de Incidentes: Documentar falhas de segurança e ações corretivas.
- Registros de Auditorias: Manter registros de auditorias realizadas.

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

57. Introdução

- Objetivo: Proteger uma empresa de software contra explorações de vulnerabilidades não corrigidas.
- Cenário: Exploração de vulnerabilidade devido à falta de atualização.

58. Identificação dos Ativos e Riscos

- Ativos: Sistemas de software.
- Ameaças: Exploração de vulnerabilidades.
- Vulnerabilidades: Falta de atualização de software.

59. Análise e Avaliação de Riscos

- Impacto: Alto (acesso remoto ao sistema).
- Probabilidade: Alta (vulnerabilidades conhecidas).

60. Controles de Segurança

- Atualizações Regulares: Aplicar atualizações de segurança regularmente.
- Gestão de Patches: Processo de gestão de patches.
- Verificação de Vulnerabilidades: Ferramentas de verificação de vulnerabilidades.

61. Implementação do Plano de Ação

- Ações Preventivas: Atualizações regulares, gestão de patches, verificação de vulnerabilidades.
- Detecção: Monitoramento de atualizações e testes de vulnerabilidades.
- Resposta: Aplicação de patches, reconfiguração de sistemas, revisão de políticas de atualização.

62. Monitoramento e Revisão

- Monitoramento: Ferramentas de monitoramento de atualizações e vulnerabilidades.
- Revisão: Revisão de políticas e procedimentos de atualização.

63. Documentação e Relatórios

- Relatórios de Incidentes: Documentar explorações e correções.
- Registros de Atualizações: Manter registros de atualizações aplicadas.

Cenário 9: Engenharia Social (Grupo 9)

64. Introdução

- Objetivo: Proteger uma empresa contra ataques de engenharia social.
- Cenário: Invasores utilizam técnicas de engenharia social para acessar contas de clientes.

65. Identificação dos Ativos e Riscos

- Ativos: Dados pessoais e financeiros de clientes.
- Ameaças: Engenharia social.
- Vulnerabilidades: Falta de conscientização.

66. Análise e Avaliação de Riscos

- Impacto: Alto (comprometimento de dados pessoais e financeiros).
- Probabilidade: Alta (técnicas de engenharia social são comuns).

67. Controles de Segurança

- Treinamento de Funcionários: Educação sobre riscos e táticas de engenharia social.
- Políticas de Verificação: Verificação rigorosa de solicitações de informações sensíveis.
- Conscientização Continuada: Cultura de conscientização sobre segurança.

68. Implementação do Plano de Ação

- Ações Preventivas: Treinamento, políticas de verificação, conscientização continuada.
- Detecção: Monitoramento de solicitações e alertas de comportamento.
- Resposta: Bloqueio de acessos indevidos, investigação e correção, reforço de treinamento.

69. Monitoramento e Revisão

- Monitoramento: Solicitações e comportamentos suspeitos.
- Revisão: Procedimentos de segurança e treinamentos.

70. Documentação e Relatórios

- Relatórios de Incidentes: Documentar ataques de engenharia social e respostas.
- Registros de Treinamento: Manter registros de treinamentos realizados.

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

71. Introdução

- Objetivo: Proteger uma rede corporativa contra ataques via dispositivos IoT inseguros.
- Cenário: Dispositivos IoT explorados para ataques dentro da rede.

72. Identificação dos Ativos e Riscos

- Ativos: Dados confidenciais de negócios.
- Ameaças: Exploração de dispositivos IoT.
- Vulnerabilidades: Falta de segurança em dispositivos IoT.

73. Análise e Avaliação de Riscos

- Impacto: Alto (exposição de dados confidenciais).
- Probabilidade: Alta (dispositivos IoT inseguros).

74. Controles de Segurança

- Segurança de Dispositivos IoT: Senhas fortes, atualizações de firmware.
- Segmentação de Rede: Isolar dispositivos IoT de sistemas críticos.

- Monitoramento de IoT: Monitorar dispositivos IoT.

75. Implementação do Plano de Ação

- Ações Preventivas: Segurança de dispositivos IoT, segmentação de rede, monitoramento.
- Detecção: Monitoramento de dispositivos e alertas de segurança.
- Resposta: Isolamento de dispositivos comprometidos, investigação e correção, atualização de políticas de IoT.

76. Monitoramento e Revisão

- Monitoramento: Ferramentas de monitoramento de dispositivos IoT.
- Revisão: Políticas de segurança e práticas de monitoramento.

77. Documentação e Relatórios

- Relatórios de Incidentes: Documentar ataques via dispositivos IoT e respostas.
- Registros de Monitoramento: Manter registros de monitoramento de dispositivos IoT.

Conclusão e Feedback

78. Recapitulação

- Revisão dos principais pontos discutidos durante a aula.
- Reforçar o entendimento dos conceitos de ameaças, vulnerabilidades e medidas de mitigação.

79. Sessão de Perguntas e Respostas

- Abrir para perguntas e responder dúvidas dos alunos.
- Solicitar feedback sobre a aula prática, o que aprenderam e sugestões para melhorias.