Segurança da informação

1. **Entrega 1: Análise de Riscos**
   Identificação e avaliação dos riscos de segurança para a empresa.

   Roubou ou perda de dados: Dados de clientes, como fotos e informações pessoais, podem ser perdidos ou roubados.

   Acesso não autorizado: Pessoas não autorizadas podem acessar as instalações ou sistemas da empresa.

   Ataques Cibernéticos: Ataques como ransomware, phishing e malware podem comprometer os sistemas da empresa.

   Vazamento de informações: Informações sensíveis podem ser divulgadas inadvertidamente.

   Danos físicos: Danos aos equipamentos ou instalações podem interromper as operações.

   Fraudo ou uso indevido de informações: Funcionários podem usar informações dos clientes de forma inadequada.

   Análise de vulnerabilidades e ameaças potenciais.

   Infraestrutura de TI desatualizada: Equipamentos e softwares desatualizados podem ter vulnerabilidades conhecidas que não foram corrigidas.

   Falta de controle e de acesso: Sistemas que não implementam controle de acesso adequado podem permitir que pessoas não autorizadas obtenham informações sensíveis.

   Ausência de políticas de segurança: A falta de políticas claras de segurança pode resultar em práticas inconsistentes e descuidadas por parte dos funcionários.

   Backup insuficiente: Falta de backups regulares e confiáveis pode resultar na perda permanente de dados.

   Uso de redes Wi-Fi inseguras: Conexões Wi-Fi não seguras podem ser exploradas por atacantes para interceptar dados

   Falta de treinamento em segurança: Funcionários mal informados são mais suscetíveis a erros que podem levar a brechas de segurança.

Ataques ransomware: Atacantes podem bloquear o acesso aos dados e exigir um resgate para restaurá-los.

Ataques de engenharia social: Emails ou mensagens falsas que tentam enganar os funcionários para revelar informações sensíveis ou instalar malware.

Ataques de negação de serviço: Atacantes sobrecarregam os sistemas da empresa, tornando-os inacessíveis para usuários legítimos.

Roubo ou perda de dispositivo: Dispositivos como laptops ou smartphones contendo informações sensíveis podem ser perdidos ou roubados.

Insider threats: Funcionários descontentes ou mal-intencionados podem comprometer a segurança intencionalmente.

Vazamento de informações: Informações sensíveis podem ser divulgadas inadvertidamente ou intencionalmente

2. **Entrega 2: Implementação de Medidas de Segurança**
   Implementação de políticas de controle de acesso aos sistemas e dados.

   Avaliação de necessidades: Identifique quais dados e sistemas são críticos para o negócio e quem precisa de acesso a eles.

   Definição de níveis de acesso: Estabeleça diferentes níveis de acesso baseados nas funções dos usuários, como administrador, funcionário regular, etc.

   Seleção de tecnologias: Escolha as ferramentas e tecnologias adequadas para implementar o controle de acesso, como sistemas de gerenciamento de identidade e acesso.

   Desenvolvimento de políticas: Crie políticas claras que definam quem pode acessar o quê, quando e como.

   Treinamento dos funcionários: Eduque os funcionários sobre as novas políticas de controle de acesso e por que elas são importantes.

   Implementação técnica: Configure as ferramentas e tecnologias escolhidas de acordo com as políticas definidas.

   Monitoramento e auditoria: Monitore regularmente o acesso aos sistemas e dados e realize auditorias para garantir conformidade com as políticas.

   Senha forte: Exigir senhas fortes e a alteração regular das mesmas.

Procedimentos de acesso: Definir como os usuários devem solicitar acesso, como ele será concedido e revogado.

Registros e auditoria: Registrar todas as tentativas e atividades de acesso para fins de auditoria e conformidade.

Políticas de saída: Estabelecer procedimentos para revogar o acesso quando um funcionário deixa a empresa ou muda de função.

Configuração de sistemas de detecção de intrusão e prevenção de ataques.

Avaliação de requisitos: Identifique as necessidades específicas da empresa, como tipos de tráfego, sistemas e aplicações que precisam ser monitorados.

Seleção de tecnologia: Escolha a solução de IDS/IPS adequada às necessidades da empresa, considerando fatores como escalabilidade, compatibilidade e recursos.

Planejamento de implementação: Defina a arquitetura do sistema, incluindo a localização dos sensores, configuração de políticas e procedimentos de resposta a incidentes.

Configuração e tuning: Configure as regras e políticas de detecção/prevenção para se alinhar com o perfil de risco da empresa e minimizar falsos positivos.

Interação com outros sistemas: Integre o IDS/IPS com outros sistemas de segurança, como firewalls, sistemas de gerenciamento de eventos e informações de segurança (SIEM) e sistemas de gerenciamento de vulnerabilidades.

Testes e validação: Realize testes de validação para garantir que o IDS/IPS esteja funcionando conforme esperado e detectando/prevenindo ataques de forma eficaz.

Monitoramento e manutenção: Monitore continuamente o desempenho do IDS/IPS, aplique atualizações de segurança e realize manutenções regulares.

Atualização regular: Mantenha as assinaturas de ameaças e regras de detecção atualizadas para garantir a eficácia contra as ameaças mais recentes.

Segmentação de rede: Separe a rede em segmentos para limitar o tráfego entre diferentes partes da rede e reduzir a superfície de ataque.

Logging e armazenamento de dados: Configure o armazenamento de logs de maneira adequada para suportar a análise forense e conformidade com regulamentações.

Resposta automatizada: Configure ações automáticas para bloquear tráfego malicioso em tempo real, conforme as políticas de prevenção configuradas.

Formação de equipe: Treine a equipe de segurança e operações para interpretar os alertas do IDS/IPS, investigar incidentes e responder adequadamente.

Auditoria e revisão: Realize auditorias regulares e revisões de desempenho para garantir a conformidade com as políticas e identificar áreas de melhoria.

Backup e recuperação: Estabeleça procedimentos de backup e recuperação para os sistemas de IDS/IPS para garantir a continuidade das operações em caso de falhas ou incidentes.