Análise de Riscos

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

Riscos Identificados:

Ataques de Phishing via e-mail ou mensagens de texto: Tentativas de enganar os clientes para revelar informações pessoais ou financeiras

Vazamento de dados dos clientes: Roubo de informações pessoais, como nomes, endereços e números de cartão de crédito

Ataque De DDoS: Tentativas de sobrecarregar o site da loja online, tornando-o inacessível aos clientes

Fraudes de cartão de crédito: Uso fraudulento de informações de cartão de crédito para realizar compras online

Fraudes na entrega de dispositivos: Cliente afirma não ter recebido um dispositivo ou o dispositivo foi entregue danificado

Ataque de aplicativos móveis: Se a empresa possui um aplicativo móvel, ele pode ser alvo de várias ameaças, incluindo malware e engenharia reversa

Falsificação de dispositivos: Venda de dispositivos falsificados ou alduterados como se fossem genuínos

Falhas no processo de verificação de identidade: Possibilidade de clientes utilizarem identidades falsas ou roubadas para fazer compras

Vulnerabilidades de segurança nos sistemas de pagamento: Brechas nos sistemas de pagamento online que podem ser exploradas por criminosos

Problemas de estoque: Estoques desatualizados ou mal gerenciados que podem levar a vendas de produtos que não estão mais disponíveis

Falhas na segurança física das instalações: Acesso não autorizado ás instalações onde os dispositivos são armazenados ou processados

Ataques de insider: Funcionários mal-intencionados que abusam dos seu privilégios para roubar dados ou causar danos

Roubo de dispositivos: Risco de roubo físico de estoque de celulares,Seja durante o transporte ou armazenamento

Ataques de ransomware nos sistemas de TI: Criptografia de dados da loja de celular por um atacante, exigindo resgate para restaurar o acesso

Ataques de engenharia reversa em dispositivos: Tentativas de desmontar ou modificar dispositivos para acessar dados sensíveis ou instalar software malicioso

Vulnerabilidades no software de e-commerce: Falhas de segurança em plataformas do comércio eletrônicos e WooCommerce

Ataque de negação de estoque: Ataques que esgotam artificialmente os estoques de produtos populares, prejudicando as vendas e a reputação da empresa

Falta de backups adequados: Se os dados da empresa não forem regularmente salvos e protegidos, eles podem ser perdidos permanentemente em caso de falha do sistema ou ataque

Falhas de segurança na cadeia de fornecimento: Vulnerabilidades nos sistemas de parceiros ou fornecedores que podem afetar indiretamente a empresa

Falhas de segurança em provedores de serviços terceirizados: Se os serviços de hospedagem, pagamento ou logística forem comprometidos, a empresa pode ser afetada

Análise de vulnerabilidades e ameaças potenciais:

1 - Ataques de Phishing via e-mail ou mensagens de texto:

- Impacto: Média (Pode resultar em divulgação de informações pessoais ou financeiras dos clientes)
- Probabilidade: Alta (Os ataques phishing são comuns e podem afetar qualquer empresa)

2 - Vazamento de dados dos clientes:

- Impacto: Muito alto (Violação grave da privacidade dos clientes, danos significativos á reputação)
- Probabilidade: Média (as empresas de e-commerce são frequentemente alvos devidos ás informações valiosas que possuem

3 - Ataque De DDoS:

- Impacto: Médio a alto (pode resultar em interrupção do serviço e perda de vendas)

- Probabilidade: Média (depende da visibilidade e do tamanho da empresa)

4 - Fraudes de cartão de crédito:

- Impacto: Alto (pode resultar em perdas financeiras significativas e danos á reputação)
- Probabilidade: Média a Alta (as transações online são frequentemente alvo de fraudes com cartão de crédito)

5 - Fraudes na entrega de dispositivos:

- Impacto: Médio (pode resultar em perda financeira e danos á reputação)
- Probabilidade: Baixa a Média (depende da eficácia dps sistemas de entrega e da honestidade dos clientes)

6 - Ataque de aplicativo móveis:

- Impacto: Médio (pode resultar em comprometimento de dados do cliente ou a interrupção do serviço)
- Probabilidade: Média (depende da segurança do aplicativo e da popularidade da empresa)

7 - Falsificação dos dispositivos:

- Impacto: Médio (pode resultar em perdas)
- Probabilidade: Média (depende da popularidade dos dispositivos e do mercado onde são vendidos)

8 - Falhas no processo de verificação de identidade:

- Impacto: Médio (pode resultar em fraudes)
- Probabilidade: Baixa a Média (depende da eficácia dos sistemas de verificação de identidade)

9 – Vulnerabilidades de segurança nos sistemas de pagamento:

- Impacto: Alto (pode resultar em perdas financeiras significativas)
- Probabilidade: Média a Alta (as transações financeiras são alvoes comunus para criminosos online)

10 – Problemas de estoque:

- Impacto: Médio (pode resultar em insatisfação do cliente)

- Probabilidade: Média (depende da eficácia dos sistemas de gestão de estoque e previsão de demanda)

11 – Falhas na segurança física das instalações:

- Impacto: Alto (pode resultar em roubo de mercadorias e interrupções das operações)
- Probabilidade: Baixa a Média (depende da localização e da eficácia das medidas de segurança física)

12 – Ataques de insider:

- Impacto: Alto (um insider pode ter acesso a dados sensíveis e causar danos significativos)
- Probabilidade: Baixa a Média (depende do controle de acesso e da confiança nos funcionários)

13 – Roubo de dispositivos:

- Impacto: Médio (pode resultar em perdas financeiras)
- Probabilidade: Baixa a Média (depende das medidas de segurança durante o transporte e armazenamento)

14 – Ataques de ransomware nos sistemas de TI:

- Impacto: Muito Alto (pode resultar em perdas de dados e interrupção das operações)
- Probabilidade: Baixa a Média (depende da segurança dos sistemas de TI e da conscientização dos funcionários)

15 – Ataques de engenharia reversa em dispositivos:

- Impacto: Alto (pode resultar em acesso não autorizado a dados sensíveis ou instalação de software malicioso)
- Probabilidade: Baixa a Média: (depende da natureza dos dispositivos e do interesse dos invasores)

16 – Vulnerabilidades no software de e-commerce:

- Impacto: Alto (pode resultar em acesso não autorizado a dados do cliente ou interrupção do serviço)
- Probabilidade: Média (depende da qualidade do software e da visibilidade da empresa)

17 – Ataque de negação de estoque:

- Impacto: Alto (pode acabar resultando em perdas de vendas)

- Probabilidade: Média (depende da popularidade dos produtos e da visibilidade da empresa)

18 – Falta de backups adequados:

- Impacto: Alto (perda potencial de dados críticos)]
- Probabilidade: Média: (depende da implementação e manutenção adequadas dos backups)

19 – Falhas de segurança na cadeia de fornecimento:

- Impacto: Alto (pode resultar em interrupção das operações)
- Probabilidade: Média a Alta (depende da segurança dos parceiros e fornecedores)

20 – Falhas de segurança em provedores de serviços terceirizados:

- Impacto: Alto (pode resultar em interrupção das operações)
- Probabilidade: Média a Alta (depende da segurança dos serviços terceirizados e da confiaça nas empresas fornecedoras)

Entrega 2: Implementação de Medidas de Segurança

Políticas de Controle de Acesso:

1 - Princípio do Privilégio Mínimo: Conceder acesso apenas ás informações e recursos necessários para que os funcionários desempenhem suas funções. Reduzir o acesso excessivo que pode limitar o potencial de danos em caso de comprometimento

2 - Autenticação de Múltiplos Fatores: Exigir Mais de uma forma de verificação de identidade antes de conceder acesso a sistemas ou dados invisíveis. Isso pode incluir combinações de senha, token, biometria, ou outros métodos de autenticação

3 – Controle de acesso Baseado em Funções: Atribuir permissões de acesso com base nas funções e responsabilidades dos usuários na organização. Isso simplifica a administração de acessos e reduz o risco de acesso não autorizado

4 - Políticas de Senhas Fortes: Estabelecer diretrizes claras para a criação e gerenciamento de senhas, exigindo comprimento mínimo, uso de caracteres, letras maiúsculas e minúsculas, e atualização regular das senhas

5 - Revisão e Auditoria de Acesso: Realizar revisões regulares dos acessos concedidos aos funcionários para garantir que estejam alinhados com suas funções

e responsabilidades. Registrar e auditar as atividades de acesso para identificar comportamentos suspeitos

6 – Monitoramento de Acesso em Tempo Real: Implementar sistemas de monitoramento que identifiquem e alertem sobre acessos não autorizados ou atividades incomuns. Isso permite uma resposta rápida a potenciais ameaças

7 – Treinamento de Conscientização em Segurança: Educar os funcionários sobre práticas de segurança de acesso, incluindo a importância de manter senhas seguras, identificar tentativas de phishing e relatar atividades suspeitas

8 – Restrição de Acesso a Dados Sensíveis: Implementar políticas de acesso restrito para dados sensíveis, como informações de pagamento e dados pessoais dos clientes. Garantir que apenas funcionários autorizados tenham acesso a esses dados e que o acesso seja estritamente controlado e monitorado

9 – Controle de Acesso Baseado em Horário: Limitar o acesso a certos sistemas ou recursos durante horários específicos, como fora do horário comercial. Isso reduz o risco de acesso não autorizado durante períodos de menor supervisão

10 - Revisão Regular de Privilégios de acesso: Estabelecer um processo regular de revisão dos privilégios de acessos concedidos a funcionários, contratados e outras partes autorizadas. Isso envolve a análise periódica das permissões de acesso para garantir que estejam alinhadas com as funções e responsabilidades atuais dos usuários.