1.As diferentes maneiras de mitigação de ataques

As fontes de ameaça são as origens ou os pontos de onde as ameaças à segurança da informação podem surgir. Elas representam os locais, atores ou entidades que têm o potencial de causar danos, roubar informações, realizar atividades maliciosas ou comprometer a segurança de sistemas, redes e dados. Essas fontes incluem fontes internas e externas. Identificar e avaliar as ameaças internas e externas permite às organizações desenvolver estratégias de proteção mais eficazes e se preparar para possíveis incidentes de segurança.

1.1 Ameaças internas

As ameaças internas são um dos principais desafios de segurança da informação que as organizações enfrentam. Elas se originam dentro da própria organização, e são representadas por atores internos, ou seja, pessoas que têm acesso legítimo aos recursos e sistemas da empresa. A linha que separa atores internos de atores externos pode ser tênue em alguns casos.

A prevenção, detecção e resposta a ameaças internas requerem uma abordagem holística que inclui educação em segurança, monitoramento contínuo e acesso controlado a sistemas e informações críticas. A conscientização e a vigilância são elementos-chave na mitigação desse tipo de ameaça.

- **Atores internos acidentais:** Essas ameaças não têm a intenção de prejudicar a organização, mas podem inadvertidamente colocar em risco a segurança da informação. Isso inclui funcionários que cometem erros não intencionais, como clicar em links de phishing, compartilhar informações sensíveis acidentalmente ou perder dispositivos que contenham dados confidenciais.
- **Atores internos maliciosos:** Nessa categoria, incluímos pessoas que têm a intenção de causar danos ou agir contra os interesses da organização. Isso pode envolver funcionários descontentes, ex-funcionários com ressentimento, colaboradores coagidos ou qualquer pessoa que abuse de seu acesso privilegiado para cometer ações maliciosas.

1.2 Atributos dos atores internos

Para entender as ameaças internas com mais profundidade, é crucial analisar os atributos dos atores envolvidos:

- **Motivação:** A motivação dos atores internos pode variar consideravelmente. Alguns podem ser motivados por razões financeiras, buscando ganho pessoal, enquanto outros podem ser motivados por vingança, descontentamento no trabalho ou coerção por terceiros. Compreender as motivações é essencial para prever e prevenir possíveis ameaças.
- **Nível de sofisticação:** O nível de sofisticação e capacidade dos atores internos é um fator a ser considerado na avaliação de riscos de ameaça. Funcionários que têm conhecimento profundo dos sistemas e processos da organização podem ser capazes de

realizar ações mais elaboradas, como a criação de malware personalizado ou a exploração de vulnerabilidades complexas.

- **Recursos:** Os recursos disponíveis para os atores internos vão determinar suas capacidades. Alguns podem depender de recursos internos da organização, como acesso a sistemas ou informações, enquanto outros podem obter apoio de fontes externas, o que pode aumentar sua capacidade de causar danos.

1.3 Estratégias comuns usadas nas ameaças internas

As estratégias adotadas por ameaças internas podem ser diversas e evoluir com o tempo. Algumas das estratégias comuns incluem

- **Abuso de privilégios de acesso:** Ameaças internas muitas vezes exploram seu acesso privilegiado para realizar atividades não autorizadas, como a exfiltração de dados confidenciais, a modificação de registros ou a criação de contas falsas.
- **Roubo de informações confidenciais:** Funcionários podem roubar informações sensíveis, como propriedade intelectual, listas de clientes, planos estratégicos ou informações financeiras para uso pessoal ou para benefício de concorrentes.
- **Destruição de dados ou ativos:** Alguns atores internos podem buscar causar danos deliberados, destruindo dados ou ativos críticos para a operação da organização.
- **Divulgação de informações confidenciais:** Ameaças internas podem deliberadamente divulgar informações confidenciais para prejudicar a reputação da organização ou causar outros tipos de danos.
- **Vazamento de dados:** Isso pode envolver a divulgação de informações confidenciais ou a venda dessas informações a terceiros, frequentemente para ganho pessoal.

1.4 Ameaças externas

As ameaças externas constituem um grande desafio para a segurança da informação. Essas ameaças se originam de fora da organização e são representadas por atores externos incluindo hackers, grupos criminosos, concorrentes, governos ou qualquer outra entidade que não têm uma filiação direta com a organização e busque explorar vulnerabilidades em sistemas e redes. Tais ameaças geralmente não têm conhecimento interno e, frequentemente, buscam ganhos financeiros, acesso a informações confidenciais ou causar danos à reputação da organização. Podem ser de várias categorias como: hackers individuais; grupos criminosos; concorrentes; hacktivistas; governos estrangeiros.

1.5 Atributos dos atores externos

Para entender as ameaças externas em maior profundidade, é fundamental analisar os atributos dos atores envolvidos

- **Motivação:** A motivação dos atores externos varia amplamente. Alguns são movidos por ganhos financeiros, enquanto outros buscam causas políticas, sociais ou até mesmo pessoais. Compreender as motivações auxilia a prever ações desses atores por meio de análise comportamental.
- **Nível de sofisticação:** O nível de sofisticação e capacidade dos atores externos pode variar significativamente. Alguns atores, como grupos criminosos altamente

organizados, possuem considerável expertise técnica, enquanto outros podem ser menos sofisticados, realizando ataques mais simples.

- **Recursos e financiamento:** A disponibilidade de recursos e financiamento é um fator crítico na determinação das capacidades dos atores externos. Grupos criminosos, por exemplo, podem ter acesso a financiamentos substanciais para conduzir suas operações, enquanto hackers individuais podem ter recursos limitados.

1.6 Risco

O ***risco*** é a probabilidade de que uma ameaça explore uma vulnerabilidade específica e cause danos. Ele é frequentemente expresso como uma combinação da probabilidade de ocorrência de uma ameaça e do impacto potencial dos danos. Para avaliar riscos, devemos identificar uma vulnerabilidade e então avaliar a probabilidade de que ela venha a ser explorada por uma ameaça e, assim, calcular o impacto que a exploração bem-sucedida poderia trazer.
risco = probabilidade * impacto

É importante ressaltar que a Segurança da Informação busca reduzir o risco identificado, vulnerabilidades, avaliando ameaças potenciais e implementando medidas de segurança adequadas para mitigar ou aceitar riscos a um nível considerado admissível. A gestão de riscos é o processo que equilibra os custos operacionais de provisão de medidas de proteção com os ganhos através da proteção do ativo.

Existem quatro maneiras de gerenciar o risco.

- **Aceitação de risco:** Ocorre quando o custo das operações de gerenciamento de risco supera o custo do próprio risco. O risco é aceito e nenhuma ação é tomada.
- **Prevenção de riscos:** Isto significa evitar qualquer exposição ao risco eliminando a atividade ou dispositivo que apresenta o risco. Ao eliminar uma atividade para evitar riscos, todos os benefícios possíveis da atividade também são perdidos.
- **Redução de riscos:** Isto reduz a exposição ao risco ou reduz o impacto do risco, tomando medidas para diminuir o risco. É a estratégia de mitigação de riscos mais utilizada e requer uma avaliação cuidadosa dos custos de perda, da estratégia de mitigação e dos benefícios obtidos com a operação ou atividade que está em risco.
- **Transferência de risco:** Parte ou todo o risco é transferido para um terceiro dispositivo como uma companhia de seguros
- **Contramedida:** As ações que são tomadas para proteger ativos, atenuando uma ameaça ou reduzindo o risco.
- **Impacto:** O dano potencial à organização causado pela ameaça.

Uma maneira de mitigar ataques de vírus e cavalos de Tróia é o próprio software antivírus. Ele ajuda a impedir que os hosts sejam infectados e espalhem código malicioso. Isso requer muito mais tempo para limpar computadores infectados do que para manter atualizações de software antivírus e definições de antivírus nas mesmas máquinas. Estes produtos possuem opções de automação de atualizações para que novas definições e novas atualizações possam ser baixadas automaticamente.

Os produtos antivírus baseados em host são instalados em computadores e servidores para detectar e eliminar vírus, porém, não impedem que vírus entrem na rede.

Outra maneira de mitigar ameaças de malware é evitar que arquivos de malware entrem na rede. Dispositivos de segurança no perímetro da rede podem identificar arquivos de malware conhecidos com base em seus indicadores de compromisso. Os arquivos podem ser removidos do fluxo de dados de entrada antes que eles possam causar um incidente.

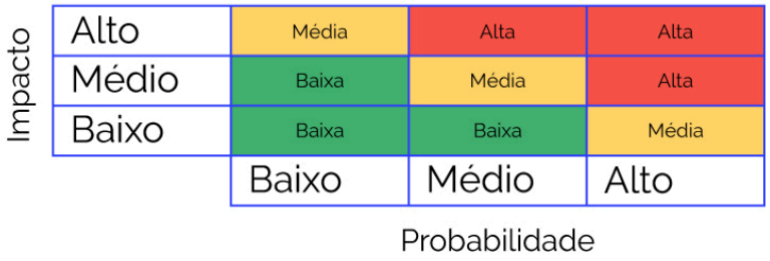
Os Worms são mais baseados em rede do que vírus. A mitigação de worm requer diligência e coordenação por parte dos profissionais de segurança da rede e seguir algumas fases.

- **Fase 1 - Custos:** A fase de contenção envolve limitar a propagação de uma infecção por vermes para áreas da rede que já estão afetadas. A contenção requer o uso de ACLs de saída e entrada em roteadores e firewalls em pontos de controle dentro da rede.
- **Fase 2 - Inoculação:** A fase de inoculação ocorre paralela ou subsequente à fase de contenção. Nela, todos os sistemas não infectados são corrigidos com o patch de fornecedor apropriado. O processo de inoculação privada ainda mais o worm de quaisquer alvos disponíveis.
- **Fase 3 - Quarentena:** Esta fase envolve rastrear e identificar máquinas infectadas dentro das áreas contidas e desconectá-las, bloquear ou removê-las. Isto isola estes sistemas adequadamente para a fase de tratamento.
- **Fase 4 - Tratamento:** Aqui se envolve a desinfecção ativa dos sistemas infectados, podendo se encerrar o processo do worm, remover arquivos modificados ou configurações do sistema introduzidos pelo worm e corrigir a vulnerabilidade que o worm usou para explorar o sistema. Alternativamente, em casos mais graves, o sistema pode precisar ser reinstalado para garantir que o worm e seus subprodutos sejam removidos.

1.7 Matriz de risco

A matriz de risco em Segurança da Informação é uma ferramenta que ajuda as organizações a avaliar e visualizar os riscos de segurança relacionados às suas operações, sistemas, ativos de informação e processos. A matriz de risco ajuda as organizações a priorizar os riscos com base em sua gravidade e probabilidade. Os riscos mais críticos e prováveis recebem maior atenção e recursos para a implementação de medidas de segurança. Ela é usada para classificar e priorizar os riscos com base em sua probabilidade de ocorrência e no impacto potencial.

A criação e manutenção de uma matriz de risco é uma prática importante em segurança da informação, e está intimamente ligada à gestão de riscos. À medida que os ambientes digitais evoluem e as ameaças mudam, a matriz de risco deve ser atualizada regularmente para refletir as condições atuais e garantir que as estratégias de segurança estejam alinhadas com os riscos mais relevantes.



Os ataques de reconhecimento são tipicamente o precursor de outros ataques que têm a intenção de obter acesso não autorizado a uma rede ou interromper a funcionalidade da rede. Estes alarmes são provocados quando determinados parâmetros são excedidos, tal como o número de pedidos ICMP por segundo.

Uma variedade de tecnologias e dispositivos podem ser usados para monitorar esse tipo de atividade e gerar um alarme. Para mitigar estes ataques, deve-se implementar a autenticação para garantir o acesso adequado, utilizar criptografia para tornar os ataques de sniffers de pacotes inúteis, utilizar ferramentas anti-sniffers para detectar ataques de sniffers de pacotes, usar um firewall e IPS além de implementar uma infraestrutura comutada.

É impossível mitigar a varredura de portas, mas **usar um IPS e firewall pode limitar as informações que podem ser descobertas com um scanner de porta**. As varreduras de ping podem ser paradas se o eco ICMP e a resposta de eco estiverem desligados nos roteadores de borda. As varreduras simplesmente levam mais tempo porque endereços IP inativos também são verificados.

Várias técnicas estão disponíveis para mitigar ataques de acesso, das quais incluem segurança de senha forte, princípio de confiança mínima, criptografia, aplicações de patches no sistema operacional e aplicativos. **Deve-se criar e impor uma política de autenticação forte** que inclua o uso de senhas fortes, o desativamento de contas após um número específico de logins malsucedidos ter ocorrido.

O uso de hash também reduz consideravelmente a probabilidade de ataques de acesso bem-sucedidos. A rede também deve ser projetada usando o princípio da confiança mínima. Por fim, eduque os funcionários sobre os riscos da engenharia social e desenvolva estratégias para validar identidades por telefone, e-mail ou pessoalmente. A autenticação multifator também é bem vinda. Estes ataques podem ser detectados através da revisão de logs, utilização da largura de banda e cargas de processo.

Um dos primeiros sinais de um ataque DoS é um grande número de reclamações de usuários sobre recursos indisponíveis ou desempenho de rede excepcionalmente lento. Para minimizar o número de ataques, um pacote de software de utilização de rede deve estar sempre em execução. A análise do comportamento da rede pode detectar padrões incomuns de uso que indicam que um ataque DoS está ocorrendo.

Outro meio de detectar um comportamento incomum de rede deve ser exigido pela política de segurança de rede da organização. Os ataques DoS podem ser um componente de uma ofensiva maior. Os ataques DoS podem levar a problemas nos segmentos de rede dos computadores que estão sendo atacados.

1.8 Relação entre vulnerabilidade, ameaça e risco

Os times de segurança devem identificar as formas pelas quais seus sistemas podem ser atacados. Essas avaliações envolvem mapear vulnerabilidades, ameaças e riscos. O entendimento dessas relações proporciona a tomada de decisões embasadas por informações sobre a segurança, permitindo que as organizações priorizem seus esforços e aloquem recursos de forma eficaz para proteger ativos críticos e reduzir os riscos a níveis aceitáveis.