1.Análise de vulnerabilidades

Um dos desafios ao analisar arquivos de log ou receber relatórios de varreduras de vulnerabilidades é que muitas vezes você precisa filtrar informações que simplesmente não são corretas. **Chamamos essa informação incorreta de falso positivo**. Recebemos um alerta informando que uma determinada vulnerabilidade existe em um sistema operacional específico, mas, após investigação, percebemos que essa vulnerabilidade na verdade não está presente nesse sistema. Nesse caso, recebemos um resultado positivo, **mas esse positivo é falso**.

Ao analisar um relatório com todas as vulnerabilidades que podem existir em um sistema, elas geralmente são organizadas por nível de gravidade. Algumas podem ser classificadas como vulnerabilidades críticas ou de alta severidade, enquanto outras podem ser consideradas de baixo risco ou meramente informativas. Às vezes, essas vulnerabilidades de baixo risco ou informativas são erroneamente chamadas de **falsos positivos**. No entanto, mesmo sendo de menor prioridade, elas ainda são vulnerabilidades reais e não devem ser classificadas como falsos positivos.

O oposto de um falso positivo é um falso negativo, e, em muitos casos, um falso negativo é muito pior. **Um falso negativo significa que uma vulnerabilidade realmente existe em um sistema operacional, mas a ferramenta de varredura não conseguiu detectá-la**. Isso significa que, no relatório de vulnerabilidades conhecidas, essa falha não será listada em lugar nenhum. Se um invasor encontrar esse sistema, ele pode explorar essa vulnerabilidade sem que você sequer soubesse da sua existência.

Se você pretende realizar uma varredura de vulnerabilidades, é sempre uma boa prática manter as assinaturas de detecção atualizadas. Isso ajuda a minimizar o número de falsos positivos e, idealmente, evita que ocorra um falso negativo. Se houver dúvidas sobre se uma vulnerabilidade detectada é real ou não, você pode entrar em contato diretamente com o fabricante da ferramenta de varredura para verificar se há uma atualização mais recente das assinaturas.

A categorização das vulnerabilidades por gravidade é muito importante, pois as falhas críticas geralmente precisam ser tratadas primeiro, enquanto as de menor impacto podem ser corrigidas depois. Sem um contexto adequado, pode ser difícil determinar a prioridade de uma vulnerabilidade isolada. Felizmente, existem várias listas públicas de vulnerabilidades que já classificam essas falhas conforme sua criticidade. Isso permite que você organize as vulnerabilidades encontradas, priorizando aquelas que representam o maior risco.

Um dos sistemas de pontuação utilizados para isso está disponível no **National Vulnerability Database (NVD)**, acessível pelo site **nvd.nist.gov**. Essa base de dados é sincronizada com a lista principal de **Common Vulnerabilities and Exposures (CVE)**. Cada vulnerabilidade listada recebe uma pontuação baseada no **Common Vulnerability Scoring System (CVSS)**, que varia de 0 a 10, sendo 10 a mais crítica.

Como o sistema de pontuação evoluiu ao longo do tempo, é possível encontrar múltiplas classificações para a mesma vulnerabilidade, dependendo da versão do CVSS utilizada.

As listas de vulnerabilidades são ferramentas essenciais e devem ser consultadas sempre que uma nova vulnerabilidade desconhecida for identificada em uma varredura. Muitas ferramentas de análise de vulnerabilidades já fornecem a referência do CVE associado a cada falha detectada, permitindo que o usuário consulte mais detalhes na base de dados do **NVD** ou diretamente na página do **CVE** no site **cve.mitre.org**. Se a vulnerabilidade estiver relacionada a um software da Microsoft, também pode ser útil verificar os boletins de segurança disponíveis no site da empresa.

Além da identificação das vulnerabilidades, um bom scanner de segurança também pode fornecer um contexto mais detalhado sobre a gravidade de cada falha. O elemento central de qualquer ferramenta de análise de vulnerabilidades é seu banco de dados de assinaturas, por isso é fundamental garantir que ele esteja sempre atualizado antes de iniciar qualquer varredura.

As varreduras de vulnerabilidades podem ser utilizadas para detectar diversos tipos de falhas, desde aplicações de desktop até sistemas de redes. Algumas ferramentas especializadas conseguem identificar vulnerabilidades dentro de aplicativos móveis e softwares populares, como, por exemplo, a vulnerabilidade **CVE-2020-1889**, que permitia um ataque no aplicativo de desktop do WhatsApp. Além disso, scanners também podem analisar servidores web, identificando falhas em aplicações hospedadas na internet, como a vulnerabilidade **CVE-2020-24981**, que afetava um sistema de gerenciamento de conteúdo web chamado **UCMS**.

Outros tipos de varredura podem detectar falhas em firewalls, switches, roteadores e outros dispositivos de rede. Um exemplo disso é a vulnerabilidade **CVE-2020-2579**, encontrada em softwares da **D-Link**, que exigiu a implementação de correções para evitar ataques.

Após identificar uma vulnerabilidade dentro de uma rede, é essencial avaliar o nível de risco associado a essa falha. Um dos métodos usados para medir esse risco é o **fator de exposição**, **geralmente representado em porcentagem. Por exemplo, se uma vulnerabilidade pode fazer com que um serviço fique indisponível metade do tempo, seu fator de exposição pode ser considerado 50%**. Se essa falha não tiver correções disponíveis e puder ser explorada por qualquer atacante externo, pode ser classificada como um **fator de exposição de 100%**.

A combinação das pontuações do CVSS com o fator de exposição ajuda as empresas a determinar quais vulnerabilidades devem ser corrigidas primeiro, especialmente quando há recursos limitados para aplicar atualizações. A criticidade de uma falha também pode depender do ambiente em que ela está presente.

Por exemplo, um servidor em uma **nuvem pública** acessível pela internet requer uma correção muito mais urgente do que um servidor isolado dentro de um ambiente de testes sem conexão externa.

Cada organização define seus próprios critérios para classificar vulnerabilidades como prioritárias ou não. Normalmente, a decisão leva em conta o número de usuários impactados, se o sistema é interno ou exposto ao público e se ele é crítico para a operação da empresa. Também pode ser relevante verificar se o sistema afetado é gerador de receita ou se a falha pode ser explorada com facilidade por invasores.

O impacto de um ataque varia conforme o tipo de organização. Um hospital, por exemplo, pode sofrer danos severos com um ataque cibernético. Em fevereiro de 2023, o hospital **Tallahassee Memorial Health** foi alvo de um ransomware, resultando no fechamento da unidade por **duas semanas**. Durante esse período, todas as emergências precisaram ser encaminhadas para outros hospitais e várias cirurgias foram canceladas.

Outros exemplos de impacto ocorreram em março de 2019, quando ataques de **negação de serviço distribuído (DDoS)** atingiram empresas de energia em **Salt Lake City, Utah** e **Los Angeles County, Califórnia**, interrompendo serviços críticos. Dependendo do tipo de organização, uma única falha pode ter consequências muito diferentes.

Gerenciar patches de segurança é um desafio, pois nem sempre é possível aplicar todas as correções ao mesmo tempo. **É necessário definir prioridades sobre quais dispositivos e sistemas devem ser corrigidos primeiro. Esse processo é conhecido como tolerância ao risco**, que representa o nível de risco que uma organização está disposta a aceitar enquanto a vulnerabilidade ainda não foi corrigida.

Embora o ideal seja aplicar patches assim que forem disponibilizados, isso nem sempre é possível. Muitas vezes, é necessário realizar testes para garantir que a atualização não causará problemas no ambiente. Durante esse período de testes, os sistemas ainda estarão vulneráveis, e a empresa precisa decidir entre acelerar a implementação da correção ou realizar mais testes antes da implantação.

Na maioria das empresas, busca-se um equilíbrio entre segurança e operação. Quando uma vulnerabilidade é crítica, fácil de ser explorada e afeta muitos sistemas, a tolerância ao risco é muito baixa, e a correção precisa ser feita o mais rápido possível para minimizar as chances de um ataque bem-sucedido.