1.Remediações para vulnerabilidades

Na maioria dos casos em que uma vulnerabilidade é identificada, ela pode ser facilmente corrigida com a instalação de um patch de segurança. Muitas vezes, esses patches são disponibilizados em um cronograma fixo, podendo ser liberados semanalmente ou mensalmente, contendo todas as atualizações de segurança daquele período. No entanto, quando a vulnerabilidade é considerada crítica ou se trata de um ataque do tipo zero-day, onde há exploração ativa sendo realizada, um patch emergencial pode ser lançado fora do cronograma regular. Esse tipo de atualização busca eliminar a vulnerabilidade do sistema ou oferecer alguma forma alternativa de mitigação.

Para quem trabalha na área de TI, esse processo é contínuo. Fabricantes e desenvolvedores de software constantemente lançam novos patches, exigindo que as empresas realizem testes antes de implantá-los em ambientes de produção. Além da aplicação de patches, **uma outra estratégia de mitigação de riscos envolve o uso de seguros de segurança cibernética**. Essas apólices costumam ser acionadas após um incidente, cobrindo perdas financeiras devido a ataques, recuperação de dados ou até processos judiciais decorrentes de violações de segurança. Entretanto, assim como outros tipos de seguro, o seguro cibernético não cobre tudo. Algumas exclusões podem incluir ações intencionais de funcionários ou transferências de fundos que não sigam os procedimentos adequados.

O crescimento dos ataques de ransomware tem feito com que mais organizações busquem esse tipo de proteção. Entretanto, a melhor estratégia para reduzir o impacto de ataques é limitar seu alcance dentro da rede. Uma abordagem eficaz é a segmentação da infraestrutura de TI, separando dispositivos em redes distintas ou VLANs. Isso não impede que um invasor comprometa um sistema, mas pode impedir que ele se movimente lateralmente e obtenha acesso a outros recursos mais sensíveis. Em alguns casos, quando um patch não pode ser aplicado devido a incompatibilidades com outros softwares ou falhas na instalação, a melhor alternativa pode ser isolar completamente um segmento da rede, removendo-o da comunicação com o restante da infraestrutura.

Firewalls de próxima geração são particularmente úteis para monitorar o tráfego entre diferentes segmentos de rede, pois permitem identificar com precisão quais aplicativos estão sendo utilizados para a comunicação entre esses segmentos. Por exemplo, seria possível visualizar que um servidor web e um banco de dados estão interagindo normalmente, mas detectar tentativas de conexões não autorizadas via SSH.

Se for necessário criar um isolamento completo, um ***air gap*** **pode ser implementado utilizando dispositivos físicos separados, como switches distintos para redes diferentes**. Isso garante que não haja conectividade entre os segmentos,

evitando que um ataque se espalhe de um setor para outro. A segmentação também pode ser feita logicamente por meio do uso de VLANs dentro de um mesmo switch. Nesse caso, cada interface do switch é associada a uma VLAN específica, impedindo que dispositivos em VLANs diferentes se comuniquem sem a presença de um roteador configurado para intermediar essa comunicação.

Além da segmentação, outras estratégias podem ser adotadas para reduzir o impacto de vulnerabilidades quando um patch não pode ser aplicado. Uma delas é a desativação do serviço vulnerável, o que impede que ele seja explorado por atacantes, mas pode causar indisponibilidade para os usuários legítimos. Outra possibilidade é restringir o acesso ao serviço para um grupo específico de usuários confiáveis.

A maioria das organizações possui um firewall perimetral, que pode ser configurado para bloquear tentativas de acesso externo a serviços vulneráveis dentro da rede interna. Mesmo sem firewalls internos, algumas medidas podem ser adotadas para reforçar a segurança, como a implementação de listas de controle de acesso em roteadores ou o uso de firewalls baseados em software diretamente nos servidores afetados.

A melhor solução para uma vulnerabilidade sempre será a aplicação do patch adequado. No entanto, quando essa opção não está disponível, **o uso de controles compensatórios pode ser a melhor alternativa**. Em algumas situações, um comitê de segurança pode avaliar a criticidade de uma vulnerabilidade e decidir se um determinado sistema pode operar sem ser corrigido. Essa decisão pode ser baseada no nível de risco envolvido, considerando fatores como a dificuldade de exploração da vulnerabilidade e a sensibilidade dos dados armazenados no sistema.

Por exemplo, algumas vulnerabilidades só podem ser exploradas por atacantes que tenham acesso físico ao servidor. Se esse equipamento estiver localizado dentro de um data center altamente seguro, a probabilidade de exploração pode ser considerada baixa, justificando a decisão de não aplicar o patch até que eventuais conflitos sejam resolvidos. Esse tipo de decisão normalmente não é tomada por um único indivíduo, mas sim por um grupo que avalia os riscos e define se uma exceção será concedida.

Mesmo quando um patch é aplicado, é fundamental verificar se ele foi instalado corretamente e se realmente eliminou a vulnerabilidade. Após a implementação de uma atualização, é recomendável realizar uma nova varredura de vulnerabilidades para confirmar que o problema foi resolvido e para identificar possíveis sistemas que ainda precisem da correção. Além disso, muitos sistemas de gerenciamento de patches fornecem relatórios detalhados sobre o status das atualizações, permitindo que as equipes de TI validem a eficácia do processo.

Para organizações de grande porte, a implementação de um sistema de relatórios é essencial para monitorar quais patches foram implantados, quais falharam

e quais sistemas ainda precisam de atualização. Esse monitoramento se torna ainda mais crítico conforme o número de dispositivos cresce. Relatórios periódicos podem fornecer insights valiosos sobre o nível de vulnerabilidades na organização, identificando sistemas desatualizados e alertando para ameaças emergentes.

Esse tipo de análise permite visualizar quantos sistemas foram corrigidos e quantos ainda estão vulneráveis, facilitando a priorização das ações de segurança. Além disso, ao acompanhar as notificações de novas ameaças ao longo do tempo, a organização pode tomar decisões mais embasadas para proteger sua infraestrutura de TI de maneira eficaz.