1.*Baselines* seguras

A implantação de uma aplicação exige a adoção de diversas medidas de segurança para proteger não apenas o próprio software, mas também o sistema operacional, dispositivos de rede e demais componentes relacionados. Para garantir a proteção adequada, é necessário configurar firewalls corretamente, manter os aplicativos e sistemas sempre atualizados e seguir as melhores práticas recomendadas pelos fabricantes.

Cada vez que uma nova instância de uma aplicação é implantada, todas as configurações de segurança devem ser aplicadas de forma consistente. Monitoramentos regulares são essenciais para verificar se essas configurações permanecem ativas e eficazes. Caso alguma falha de segurança seja identificada, medidas corretivas devem ser implementadas imediatamente.

A criação de um conjunto de padrões de segurança (security baselines) é um dos primeiros passos nesse processo. Felizmente, muitas empresas desenvolvedoras oferecem diretrizes de segurança para seus produtos, simplificando esse trabalho. Os fabricantes de software podem fornecer recomendações sobre permissões de arquivos, configurações de sistema e ajustes específicos para garantir a proteção da aplicação. Além disso, fornecedores de sistemas operacionais, como a Microsoft, disponibilizam suas próprias diretrizes de segurança, incluindo ferramentas como o **Security Compliance Toolkit (SCT)**, que facilita a implementação dessas medidas.

A definição inicial de padrões de segurança pode parecer complexa, pois envolve um grande número de configurações. Por exemplo, no Windows 10, há mais de **3.000 configurações de política de grupo**, embora apenas uma parte delas seja voltada para segurança. Para simplificar esse processo, a Microsoft e outros fabricantes oferecem modelos predefinidos que podem ser personalizados conforme as necessidades da organização.

Após definir os padrões de segurança, o próximo passo é aplicá-los de forma consistente em toda a infraestrutura. Isso pode ser feito por meio de **consoles centralizados**, como o próprio **Microsoft Security Compliance Toolkit**, ou por meio de ferramentas como o **Active Directory Group Policy**, que permite distribuir automaticamente configurações para diversos dispositivos. Outras soluções, como sistemas de **gerenciamento de dispositivos móveis** (**MDM**), podem ser utilizadas para garantir que dispositivos móveis sigam as mesmas políticas de segurança.

Dado o volume e a complexidade dessas configurações, a automação é essencial para facilitar a implementação e garantir que as políticas sejam aplicadas corretamente em centenas ou milhares de dispositivos. Uma vez implementados, esses padrões de segurança raramente precisam ser alterados, mas podem exigir atualizações quando

novas vulnerabilidades são descobertas ou quando há mudanças na aplicação ou no sistema operacional.

Conflitos podem surgir entre diferentes padrões de segurança recomendados por distintos fabricantes, exigindo que a equipe de TI avalie e escolha a melhor abordagem para cada situação. Antes de aplicar qualquer mudança na produção, é recomendável realizar **testes e auditorias** para garantir que as configurações atendam às exigências de segurança e não causem problemas operacionais. Após a implantação, verificações periódicas são essenciais para garantir que os padrões de segurança continuem sendo seguidos.