1.Alvos de *hardening*

A configuração padrão de um sistema operacional recém-instalado raramente é segura, exigindo ajustes adicionais para aumentar a proteção. Identificar exatamente quais configurações precisam ser alteradas pode ser um desafio, mas muitos fabricantes oferecem **guias de segurança (hardening guides)** específicos para cada sistema ou aplicação. Caso um dispositivo não tenha um guia oficial, é possível buscar informações junto ao fabricante ou em fóruns especializados, onde a comunidade pode compartilhar recomendações de segurança.

Dispositivos móveis são exemplos de equipamentos que exigem o fortalecimento da segurança. Fabricantes frequentemente disponibilizam diretrizes para proteger esses dispositivos, além de lançar atualizações que corrigem falhas e adicionam novas proteções. A aplicação dessas atualizações é fundamental, pois evita que vulnerabilidades sejam exploradas por invasores. Outra prática essencial é a **segmentação de dados**, separando informações pessoais de dados corporativos. Esse isolamento impede que um ataque em um segmento comprometa todos os arquivos do dispositivo.

Empresas que gerenciam um grande número de dispositivos móveis geralmente utilizam **soluções de Mobile Device Management (MDM)** para monitorar e aplicar configurações de segurança remotamente. No entanto, a necessidade de segurança não se limita a dispositivos móveis. **Workstations, servidores e infraestrutura de rede** também precisam ser protegidos contra ameaças.

Sistemas operacionais como Windows, macOS e Linux recebem atualizações frequentes que incluem correções de segurança. Muitas empresas compilam esses patches e os lançam em dias específicos do mês para facilitar a aplicação em ambientes corporativos. Além das atualizações, uma prática recomendada é **remover softwares desnecessários**, reduzindo a superfície de ataque e eliminando potenciais vulnerabilidades.

Dispositivos de rede, como **switches, roteadores e firewalls**, também precisam ser reforçados. Esses equipamentos geralmente utilizam sistemas operacionais proprietários e exigem cuidados específicos, como a **alteração de credenciais padrão** e a implementação de **autenticação centralizada**. Como os fabricantes raramente lançam atualizações para esses dispositivos, qualquer patch de segurança disponibilizado deve ser tratado como prioridade.

Organizações que utilizam **infraestrutura em nuvem** precisam adotar medidas específicas para proteger seus sistemas. O conceito de **privilégio mínimo (least privilege)** deve ser aplicado, garantindo que usuários e aplicações tenham apenas as permissões estritamente necessárias para suas funções. Além disso, a adoção de **soluções de Endpoint Detection and Response (EDR)** auxilia no monitoramento contínuo e na detecção de ameaças. **Backups regulares** devem ser feitos,

preferencialmente em provedores de nuvem distintos, garantindo a recuperação dos dados em caso de falha.

Servidores, sejam físicos ou virtuais, também precisam de fortalecimento da segurança. Aplicação de patches, configuração de autenticação forte e restrição de acesso a dispositivos específicos são medidas fundamentais. Além disso, servidores devem ser protegidos por **firewalls, antivírus e soluções antimalware**, impedindo a execução de códigos maliciosos.

Ambientes industriais frequentemente utilizam **SCADA (Supervisory Control and Data Acquisition)** e **ICS (Industrial Control Systems)** para monitorar e controlar equipamentos críticos. Esses sistemas operam em redes isoladas e raramente possuem conexão direta com a internet, garantindo maior segurança contra ataques externos.

Sistemas embarcados, como televisores inteligentes e dispositivos IoT, também apresentam desafios de segurança, pois seus sistemas operacionais são frequentemente inacessíveis para atualizações. Sempre que um patch de segurança for disponibilizado, sua instalação deve ser priorizada. Para minimizar riscos, recomenda-se **segmentar redes** e isolar esses dispositivos, utilizando firewalls para limitar seu acesso a outros sistemas.

A adoção de **Sistemas Operacionais em Tempo Real (RTOS)** em equipamentos industriais, automóveis e dispositivos militares garante a execução de processos em períodos específicos, priorizando eficiência e segurança. Esses sistemas devem ser isolados de redes corporativas e configurados para executar apenas os serviços essenciais.

Por fim, **dispositivos IoT** utilizados para automação de iluminação, climatização e segurança devem ser configurados com cuidados extras, pois fabricantes desses equipamentos nem sempre priorizam a segurança. **Patches de segurança devem ser aplicados assim que forem disponibilizados**, e esses dispositivos devem ser mantidos em redes isoladas para evitar que ataques comprometam a infraestrutura principal.

Garantir a segurança de sistemas operacionais, redes e dispositivos exige uma combinação de boas práticas, atualizações regulares e políticas rigorosas de controle de acesso. Ao implementar essas medidas, empresas e usuários minimizam riscos e fortalecem a proteção contra ameaças digitais.