1.Vulnerabilidades de dispositivos móveis

Garantir a segurança de dispositivos móveis é um grande desafio, pois eles exigem políticas, procedimentos e tecnologias específicas para proteção. Esses aparelhos são pequenos, podem ser facilmente ocultados e estão em constante movimento, dificultando seu rastreamento e gerenciamento. Além disso, armazenam informações sensíveis tanto de usuários individuais quanto de organizações inteiras, enquanto permanecem continuamente conectados à internet, tornando-se alvos potenciais para ataques remotos.

Embora esses dispositivos possuam várias camadas de segurança integradas, algumas pessoas buscam métodos para contornar essas proteções, como **o jailbreaking no iOS e o rooting no Android**. Essas técnicas substituem o sistema operacional original por versões modificadas, permitindo a instalação de aplicativos não autorizados e a desativação de restrições de segurança. Se um funcionário realizar esse processo em um dispositivo corporativo, ele estará eliminando todas as proteções implementadas pelo gerenciador de dispositivos móveis (MDM), deixando o equipamento vulnerável a ameaças.

Outro problema grave é a instalação de aplicativos de fontes não confiáveis, que podem conter códigos maliciosos. Por isso, muitos sistemas operacionais e soluções MDM limitam a instalação de aplicativos apenas a lojas oficiais ou bibliotecas corporativas. **Quando um usuário instala apps de terceiros por meio de sideloading**, ele pode estar abrindo uma porta para malware e comprometendo a segurança dos dados armazenados no dispositivo.

A instalação de sistemas operacionais ou softwares não autorizados geralmente é proibida pelas políticas da empresa, sendo estipulada em manuais e nos termos de uso aceitáveis (AUPs). Caso um funcionário viole essas diretrizes ao modificar o sistema operacional do dispositivo, ele pode estar sujeito a sanções, incluindo o desligamento da organização. Dessa forma, o uso responsável de dispositivos móveis dentro de um ambiente corporativo é fundamental para manter a segurança da informação e evitar brechas que possam ser exploradas por atacantes.