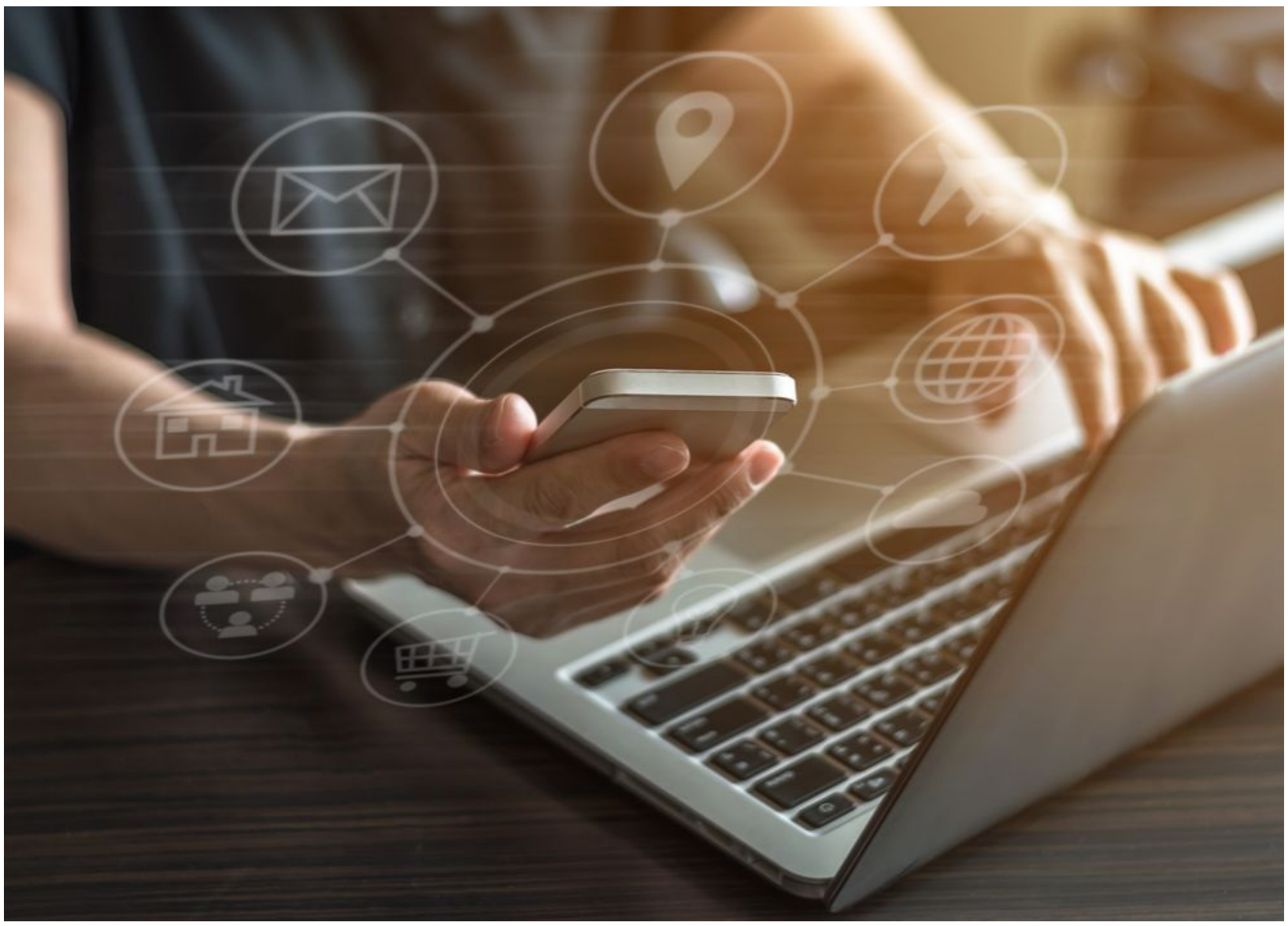
FOCO NO MERCADO DE TRABALHO

PROTEÇÃO PARA DISPOSITIVOS MÓVEIS

Emilio Tissato Nakamura

QUAIS SÃO OS OBJETIVOS DE SEGURANÇA NO USO DE DISPOSITIVOS MÓVEIS NO MUNDO CORPORATIVO?

Separação do contexto pessoal do profissional, identificação remoção de aplicativos vulneráveis, uso de *antimalware*, uso de criptografia no tráfego, autenticação de duplo fator, conexão apenas de dispositivos confiáveis e política de segurança de instalação de aplicativos.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

O planejamento da nova versão da plataforma digital, baseada em dispositivos móveis, e com a nova função dos colaboradores para a expansão da rede de pequenos negócios parceiros, pode ser dividida em três grandes desenvolvimentos:

1. Desenvolvimento do aplicativo móvel para os consumidores.
2. Desenvolvimento do aplicativo móvel para os colaboradores.
3. Desenvolvimento do aplicativo móvel para os pequenos negócios.

Os aplicativos podem ser agregados, ou seja, pode haver somente um aplicativo que tenha as três funções: consumidor, colaborador e pequenos negócios. Os servidores e o *backend* estão em um provedor em nuvem na Europa.

Para o desenvolvimento do aplicativo móvel para os consumidores e os pequenos negócios, deve-se seguir as boas práticas de segurança, evitando as vulnerabilidades, principalmente aquelas citadas pelo OWASP: uso impróprio de plataforma, armazenamento de dados inseguros, comunicação insegura, autenticação insegura, criptografia insuficiente, autorização insegura, má qualidade de código, modificação de código, engenharia reversa e funcionalidade exposta. Além da prática para a codificação, é preciso estar atento para os demais controles de segurança necessários, como as avaliações de segurança, por exemplo.

Para o desenvolvimento do aplicativo móvel para os colaboradores, além de seguir as recomendações apresentadas, é preciso planejar como o uso do dispositivo móvel será implantado pela empresa.

Um ponto a ser definido pela empresa é o modelo de uso dos dispositivos móveis. De quem será o dispositivo móvel? O colaborador poderá utilizar o dispositivo móvel para fins pessoais? A definição será formalizada em uma política de segurança para dispositivos móveis, e os mecanismos para garantir que ela seja cumprida também precisa ser definida.

Os modelos possíveis são:

- Uso exclusivamente corporativo de dispositivos móveis providos pela empresa.
- Permissão para uso pessoal de dispositivos móveis providos pela empresa, no modelo conhecido como *Corporate-Owned Personally-Enabled* (COPE).
- Uso de dispositivos móveis pessoais dos próprios colaboradores para o uso corporativo, no modelo conhecido como *Bring Your Own Device* (BYOD) ou *Choose Your Own Device* (CYOD).

O uso de dispositivos móveis pelos colaboradores deve também ser definido com a condução de atividades essenciais:

- Conduzir uma análise de riscos em dispositivos móveis e para as informações acessadas por eles, considerando todos os elementos do risco: componentes, vulnerabilidades, ameaças, probabilidade, impacto, e agentes de ameaça.

- Adotar tecnologias de segurança móvel como *Enterprise Mobility Management / Mobile Device Management* (EMM/MDM), plataformas de defesa contra ameaças móveis ou serviço de veto a aplicações móveis, que utiliza uma variedade de técnicas estáticas, dinâmicas e comportamentais para determinar, com o uso de uma pontuação, se uma aplicação ou dispositivo demonstra qualquer comportamento que representa um risco de segurança ou de privacidade. Este serviço de veto pode ser utilizando antes da instalação nos dispositivos móveis.

- Reforçar o ciclo de vida de implantação de dispositivos móveis corporativos, com passos-chave para que os dispositivos cheguem aos colaboradores de uma forma segura, incluindo a análise de riscos, o modelo adotado que pode ou não permitir o uso de dispositivos particulares, inventário, monitoramento e atualizações.

- Implementar e fazer um piloto da solução de dispositivo móvel antes de colocá-la em produção, considerando conectividade, proteção, autenticação, funcionalidades, gerenciamento, registros e desempenho.

- Prover a segurança em cada dispositivo móvel corporativo antes de permitir o acesso a sistemas e informações corporativas, com uso de uma solução de gerenciamento de mobilidade corporativa (EMM/MDM).

- Manter atualizados o sistema operacional e os aplicativos móveis, minimizando as vulnerabilidades.

- Manter regularmente a segurança dos dispositivos móveis, fazendo avaliações periódicas de segurança e de cumprimento da política de segurança.

AVANÇANDO NA PRÁTICA

DADOS CONFIDENCIAIS NOS DISPOSITIVOS MÓVEIS DOS DIRETORES

Em uma análise sobre o ambiente tecnológico da empresa em que você trabalha, você observou que acessos foram sendo concedidos para os diretores, de modo que se perdeu o controle sobre o perímetro da empresa e sobre os dados confidenciais que agora existem fora da empresa, nos dispositivos móveis. O uso do dispositivo móvel tanto para assuntos pessoais quanto para assuntos corporativos é um outro desafio. Cite os principais pontos ou capacidades de segurança que você deve propor para que o uso de dispositivos móveis na empresa possa ser feito de uma forma formal e segura.

RESOLUÇÃO

A formalização do uso de dispositivos móveis na empresa segue o modelo em que é possível usá-los tanto para fins profissionais quanto para fins pessoais. Para os diretores, a empresa disponibiliza o dispositivo móvel, que precisa ser gerenciado com uma solução como o *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM), que aplicará as configurações definidas e manterá atualizados os componentes do dispositivo móvel, tratando as vulnerabilidades.

Uma campanha de conscientização para os diretores também é planejada, para que eles fiquem cientes dos riscos existentes no uso de dispositivos móveis, e também para que entendam como funcionará o gerenciamento e as atualizações. E a conscientização também considera recomendações para que os diretores não sejam vítimas de *phishing* ou *SMiShing*.

Algumas questões de segurança envolvidas com o uso de dispositivos móveis que devem ser consideradas para a definição da sua proposta são:

- Mistura de dados pessoais e dados corporativos.
- Instalação de aplicativos vulneráveis.
- Instalação de *malwares* a partir de fontes não oficiais.
- Interceptação de tráfego a partir de conexões não confiáveis.
- Conexões não confiáveis aceitas pela empresa.

A sua proposta para a defesa de dispositivos móveis, assim, define os seguintes pontos:

- Proteção dos dados armazenados no dispositivo móvel.
- Gerenciamento centralizado para aplicar políticas e configurações aos dispositivos.
- Avaliação da segurança das aplicações móveis.
- Proteção contra o acesso indevido aos dados do dispositivo móvel.
- Configurações de privacidade para proteger os dados dos usuários.
- Proteção contra tentativas de *phishing*.