

NÃO PODE FALTAR

## PROTEÇÃO PARA DISPOSITIVOS MÓVEIS

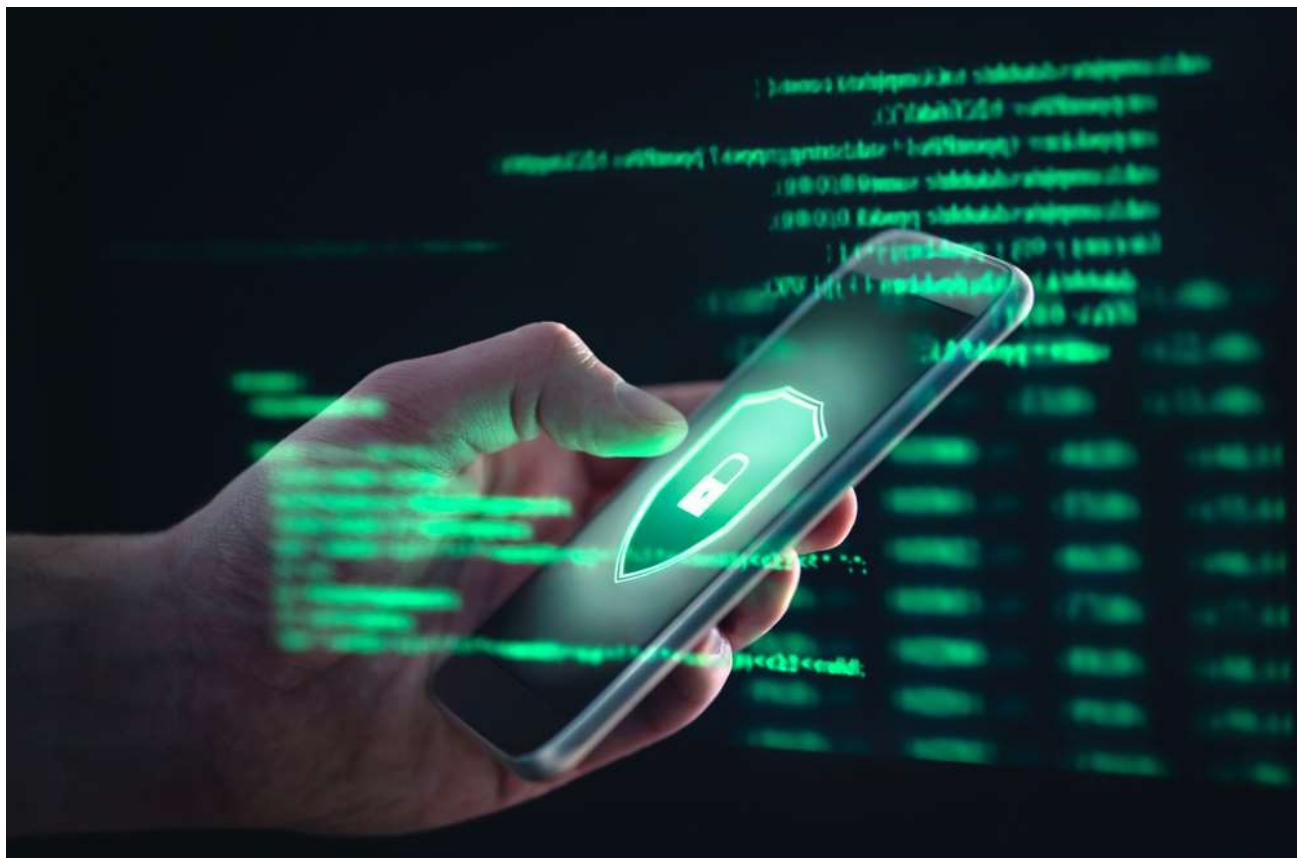
Emilio Tissato Nakamura

0

Ver anotações

### QUAIS SÃO OS RISCOS NO USO DE DISPOSITIVOS MÓVEIS NO MUNDO CORPORATIVO?

Além dos riscos já comuns em outros ambientes, há também os riscos pelas próprias características dos dispositivos móveis, que passam a ser mais distribuídos, os dados corporativos passam a existir fora dos servidores da empresa e há a mistura com os dados pessoais que podem comprometer a privacidade dos usuários.



Fonte: Shutterstock.

**Deseja ouvir este material?**

Áudio disponível no material digital.

### PRATICAR PARA APRENDER

Olá, nesta aula discutiremos um dos assuntos mais importantes para a estratégia de segurança e privacidade das empresas: o uso de dispositivos móveis. Eles são um dos principais vetores de ataques, por meio dos quais os criminosos virtuais

buscam maximizar seus resultados visando o canal em que há maior número de alvos e possibilidades de sucesso.

Os dispositivos móveis representam um grande desafio para as empresas, já que, além dos dados corporativos, há os dados pessoais de seus usuários. E isso implica no aumento da complexidade de proteção, além do intrínseco aumento de riscos. Um exemplo desse desafio é quando um colaborador instala jogos em seu dispositivo móvel, mas a partir de fontes não confiáveis. O resultado pode ser a introdução no dispositivo de malwares que comprometem a privacidade do colaborador, assim como dos dados confidenciais corporativos que podem estar no dispositivo ou serem acessados a partir dele.

Nesta aula entenderemos também as ameaças e os ataques voltados para o mundo móvel, para então provermos a defesa necessária. E os elementos de segurança são diferentes do tradicional, já que os dispositivos móveis têm características próprias que precisam ser consideradas. Uma delas é o seu formato, que é portátil e, portanto, pode levar ao acesso físico ao dispositivo que contém dados. Outra característica para as empresas é que os dispositivos móveis expandem o perímetro da empresa, com os dados sendo distribuídos de uma forma ampla e sem limites físicos.

Há modelos de implantação de dispositivos móveis nas empresas, que levam em consideração a propriedade dos dispositivos, e a permissão para uso particular. E as políticas e configurações desses dispositivos devem ser gerenciados de uma forma adequada.

Para os desenvolvedores de aplicativos móveis há uma série de cuidados de segurança e privacidade que precisam ser tomados para que vulnerabilidades não sejam introduzidas nesses aparelhos.

Você verá que os dispositivos móveis seguem um ciclo de vida que vai do planejamento da implantação até as operações e descarte, que deve ser feito de modo a não comprometer os dados pessoais e os dados confidenciais da empresa.

Ver anotações

Você é o especialista em segurança e privacidade de um inovador site de comércio online em que pequenos negócios são conectados com os consumidores em uma plataforma digital baseada no uso de inteligência artificial. A sua função é essencial para a empresa, e você participa de todas as decisões sobre a evolução da plataforma. Há as questões envolvidas com o desenvolvimento seguro, para que vulnerabilidades não sejam inseridas indevidamente no sistema. Há ainda as questões de segurança e privacidade envolvidas com o uso de provedor de nuvem. E, como a empresa trabalha com inteligência artificial, há necessidade de fazer o desenvolvimento utilizando bases de dados que não interfiram na privacidade dos clientes.

Ver anotações

Além da segurança da informação da plataforma da empresa, que está hospedada em um provedor em nuvem na Europa, você tem três preocupações principais:

1. Como diminuir as possíveis fraudes cometidas por usuários falsos que se passam por clientes, com uso de identidades falsas ou uso de recursos financeiros ilícitos.
2. Como diminuir as possíveis fraudes cometidas por pequenos negócios falsos, que podem não cumprir os compromissos comerciais estabelecidos com os clientes que utilizam a plataforma digital.
3. Como proteger os dados pessoais dos clientes principalmente contra vazamentos, que pode levar a sanções previstas na LGPD.

Após já ter mostrado um planejamento sobre os aspectos que devem ser considerados pela empresa para a definição de uma estratégia de segurança e privacidade, com o seu direcionamento quanto à segurança em transações *web*, vamos para o próximo passo. O que deve ser planejado agora é a expansão para a nova versão da plataforma, baseada em aplicativos para dispositivos móveis. Apresente o seu planejamento, pensando que neste novo cenário você terá colaboradores que também utilizarão dispositivos móveis para expandir a rede de

pequenos negócios parceiros. Esses colaboradores farão os contatos com os pequenos negócios assim como o acesso junto com eles na plataforma digital, utilizando dispositivos móveis.

0

Ver anotações

Os desafios de segurança e privacidade relacionados aos dispositivos móveis são grandes e oferecem grandes oportunidades. Seja para desenvolver aplicativos móveis com mais segurança ou para implantar o uso de dispositivos móveis de uma forma segura, esses tópicos são importantes e fazem parte de nossas vidas.

o

Ver anotações

## CONCEITO-CHAVE

### DISPOSITIVOS MÓVEIS

Um dispositivo móvel é, segundo o *National Institute of Standards and Technology*, NIST (NIST, 2020), um dispositivo computacional portátil que possui um formato pequeno e que pode ser carregado por um indivíduo, sendo construído para operar sem uma conexão física, com armazenamento de dados local não removível e que funciona por um período de tempo com uma fonte de energia própria. Pode incluir capacidades de comunicação por voz e sensores que possibilitam a captura de informação e tem a capacidade de sincronização com locais remotos.

As principais características de dispositivos móveis são, assim, portabilidade, comunicação sem fio, armazenamento local e funcionamento por bateria. Essas características influenciam diretamente nos aspectos de segurança e privacidade, por mudarem, principalmente, os perímetros das empresas, que se expandem com os dispositivos móveis.

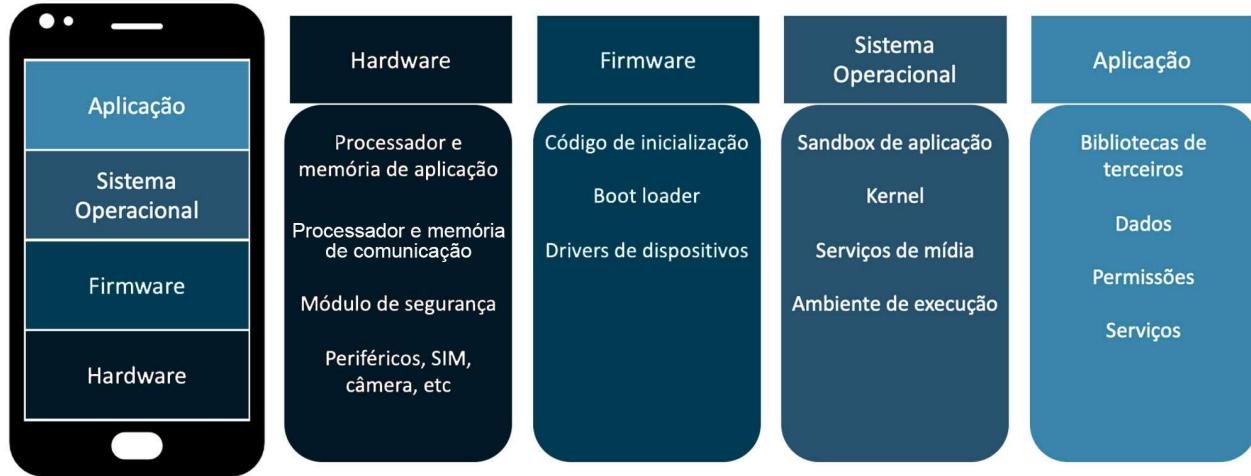
Além delas, a conexão em redes celulares sempre ativas também é uma característica relevante para os aspectos de segurança, mas não é uma realidade em todos os dispositivos móveis, como nos tablets.

#### REFLITA

Com a chegada da rede 5G, o que acontece com a segurança e a privacidade? A tecnologia 5G possibilita conexões com maior velocidade e menor latência, além de conexões permanentes de qualquer coisa ou dispositivo, tornando a internet das coisas (IoT) onipresente, com tudo conectado, desde drones até cafeteiras, incluindo carros (HIGA, 2016).

Os principais componentes dos dispositivos móveis podem ser vistos na Figura 3.9, com a divisão entre *hardware*, *firmware*, sistema operacional e aplicação. Cada um destes componentes representa pontos que podem ser atacados (FRANKLIN *et al.*, 2020).

Figura 3.9 | Componentes de dispositivos móveis



Fonte: adaptada de Franklin *et al.* (2020).

O uso de dispositivos móveis traz uma série de vantagens para as empresas, principalmente com o aumento da eficiência e produtividade decorrente do acesso aos recursos da empresa a qualquer momento, de qualquer localidade. E isto resulta em necessidades de segurança (NCCoE, 2020), devido aos riscos existentes neste ambiente.

## AMEAÇAS E SEGURANÇA EM DISPOSITIVOS MÓVEIS

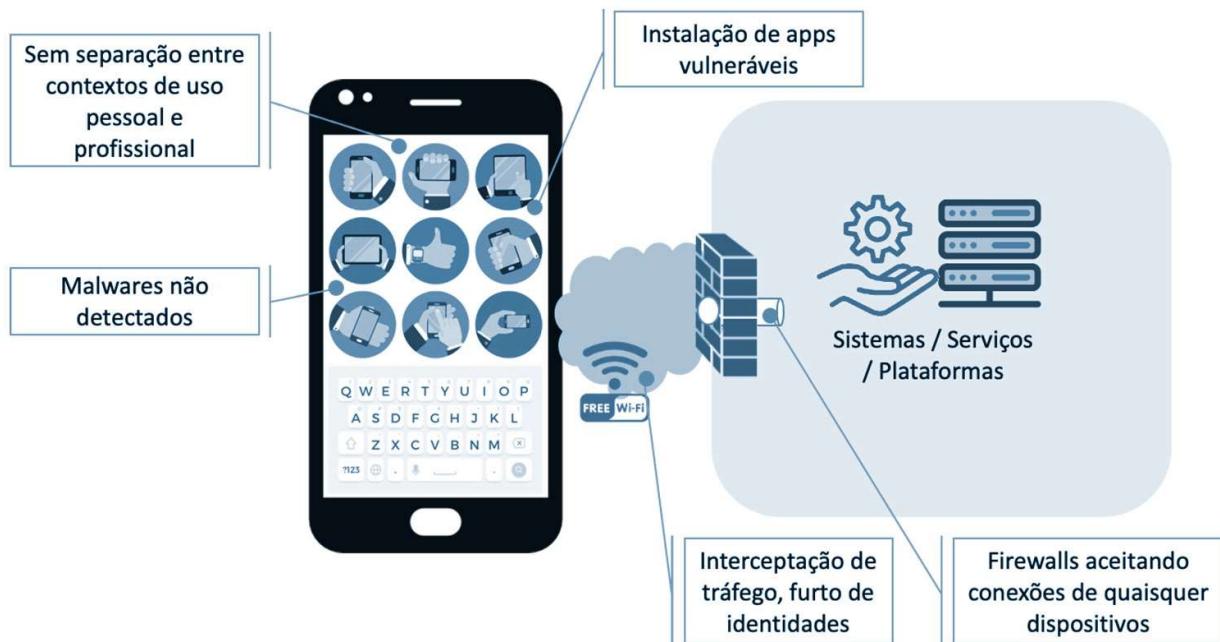
Os principais riscos envolvidos com o uso de dispositivos móveis no mundo corporativo podem ser vistos na Figura 3.10, e são (HOWELL *et al.*, 2020):

- Comprometimento da privacidade do usuário ou dos dados sensíveis da empresa a partir na inexistência de separação entre contextos de uso pessoal e profissional, de modo que problemas de segurança em um contexto afetam o outro.
- Instalação de aplicativos vulneráveis a partir de fontes não oficiais, o que aumenta a chance de inserção de vulnerabilidades no ambiente.

- Instalação de *malwares* a partir de fontes não oficiais, que podem vir junto de aplicativos falsificados ou cavalos de Troia.
- Interceptação de tráfego a partir de conexões não confiáveis, que pode resultar em vazamento de dados e furto de identidades.
- Conexões não confiáveis aceitas pela empresa, que precisa abrir o *firewall* para as conexões de quaisquer dispositivos.

Ver anotações

Figura 3.10 | Riscos no uso de dispositivos móveis no mundo corporativo



Fonte: adaptado de Howell *et al.* (2020).

#### ASSIMILE

As ameaças existentes no mundo móvel são muito similares às de outros ambientes, apesar de algumas especificidades. Os níveis de risco das empresas mudam, pelas próprias características dos dispositivos móveis, que aumentam a superfície de ataque ao ampliar os parâmetros da empresa, que passam a ser mais distribuídos. Os dados corporativos passam a existir fora dos servidores da empresa e há a mistura com os dados pessoais que podem comprometer a privacidade dos usuários.

As ameaças para dispositivos móveis precisam ser entendidas para que a melhor estratégia de segurança possa ser definida pela empresa, incluindo a aplicação de melhores práticas de segurança e o uso de soluções de segurança para a proteção de todo o ambiente (BROWN *et al.*, 2016) (NIST, 2020).

As principais ameaças relacionadas aos dispositivos móveis são descritas a seguir e detalham os principais riscos vistos na figura 3.10 (HOWELL *et al.*, 2020) (NCCoE, 2020) (FRANKLIN *et al.*, 2020):

- **Acesso não autorizado às informações sensíveis via aplicação maliciosa ou intrusiva para a privacidade:** uma aplicação móvel, mesmo legítima, pode tentar coletar e enviar qualquer informação a que ela tem acesso. Alguns exemplos de informações que podem ser acessadas de acordo com os níveis de permissão da aplicação são os contatos, calendários, histórico de ligações ou as fotos, e ainda as informações gerais do dispositivo, como o *Mobile Equipment Identity* (MEI), fabricante, modelo e número de série. Além disso, uma aplicação maliciosa pode explorar vulnerabilidades de outras aplicações, do sistema operacional ou do *firmware* para escalar privilégios, visando obter o acesso não autorizado aos dados armazenados no dispositivo.
- **Furto de identidade por campanhas de *phishing* por *Short Message Service* (SMS) ou e-mail:** uso de técnicas de engenharia social e uso de senso de urgência para obter a atenção e promover o direcionamento das vítimas a *sites* fraudulentos, onde eles entregam suas credenciais de acesso e outras informações sensíveis.
- **Aplicações maliciosas instaladas via URLs em mensagens SMS ou e-mail:** uso de técnicas de engenharia social e uso de senso urgência para instigar a vítima a clicar em um *link* que contém *malware*, que é então instalado no dispositivo móvel.
- **Perda de confidencialidade e de integridade com a exploração de vulnerabilidades conhecidas em sistema operacional e firmware:** a

exploração de vulnerabilidades pode levar à execução de códigos arbitrários e à instalação de *malware*, como um *backdoor*.

- **Violão da privacidade por mal-uso de sensores do dispositivo:** sensores como microfone, câmera, giroscópio e *Global Positioning System* (GPS) podem ser explorados para obter informações sensíveis ou comprometer a privacidade dos usuários.
- **Comprometimento da integridade do dispositivo ou da comunicação de rede pela instalação de *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM), perfis de rede, *Virtual Private Network* (VPN) ou certificados digitais maliciosos:** com a instalação de EMM/MDM malicioso, o agente de ameaça pode ter acesso à plataforma de gerenciamento dos dispositivos móveis, tendo o controle do dispositivo e das comunicações, podendo assim instalar aplicações maliciosas, localizar remotamente um usuário, ou apagar remotamente os dados. Já a manipulação da rede e da VPN possibilita o direcionamento das conexões para redes não confiáveis, de onde os dados são furtados. A manipulação de certificados digitais estabelece uma relação de confiança falsa que possibilita a conexão a servidores e redes contaminados e a instalação de aplicativos maliciosos.
- **Perda de confidencialidade por monitoramento de comunicações expostas:** redes sem fio públicas abertas são alvos de monitoramento e ainda podem levar a ataques como o *watering hole* ou o *Man-In-The-Middle* (MITM). Além disso, podem levar os usuários a se conectarem a sites falsos.
- **Comprometimento da integridade do dispositivo móvel pela observação, inferência ou força-bruta do código de desbloqueio do dispositivo:** além do acesso aos dados do dispositivo, a obtenção do código de desbloqueio pode levar ao acesso a outras aplicações, caso o código de desbloqueio seja utilizado como credencial de acesso para outros sistemas.
- **Acesso não autorizado a serviços de *backend* pela autenticação ou falhas no armazenamento de credenciais em aplicações desenvolvidas**

Ver anotações

**internamente:** aplicações próprias devem ser desenvolvidas com cuidados na implementação de mecanismos de autenticação e armazenamento de credenciais, além de não inserir vulnerabilidades que podem dar o acesso a essas informações essenciais para um ataque.

- **Acesso não autorizado a recursos da empresa a partir de dispositivos comprometidos ou não gerenciados:** dispositivos não gerenciados não

utilizam os mecanismos de segurança definidos pela empresa.

- **Perda de dados da empresa devido à perda ou furto do dispositivo:** a

probabilidade aumenta pela natureza dos dispositivos, que é portátil, e o agente de ameaça pode ter acesso não autorizado dos dados sensíveis ou recursos disponíveis no dispositivo.

- **Perda de confidencialidade dos dados da empresa devido ao**

**armazenamento não autorizado em serviços sem homologação:** o uso de serviços não gerenciados pela empresa impossibilita o monitoramento e acompanhamento dos serviços. O resultado pode ser o acesso não autorizado aos dados da empresa a partir destes serviços.

O *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM) é um dos principais controles de segurança para dispositivos móveis das empresas (FRANKLIN *et al.*, 2020). O EMM/MDM é uma solução para prover segurança em dispositivos móveis de usuários que são autorizados a acessar recursos da empresa.

Geralmente o EMM/MDM é composto por dois componentes principais. O primeiro é um serviço *backend* que os administradores utilizam para gerenciar as políticas, configurações e outras ações de segurança que são aplicadas nos dispositivos móveis. O segundo componente é um agente que é instalado no dispositivo que permite a aplicação das ações definidas pela empresa.

Há o provisionamento dos perfis de configuração para os dispositivos, a aplicação das políticas de segurança nos dispositivos e o monitoramento de conformidade com as políiticas peios dispositivos. O agente no dispositivo pode enviar

Ver anotações

notificações em caso de configurações não conformes com a política da empresa, e pode corrigir automaticamente configurações desta natureza.

O EMM/MDM pode ainda prover informações importantes para a segurança do ambiente. Os dados de conformidade com a política de disponíveis móveis, por exemplo, podem ser utilizados pela empresa para o controle de acesso, como um parâmetro adicional para aceitar as conexões somente de dispositivos que estejam cumprindo um determinado nível de segurança.

Ver anotações

#### **ASSIMILE**

O *watering hole* é um golpe direcionado e personalizado, em que os atacantes comprometem algum *site* que eles sabem que o alvo irá visitar, para que assim o infectem com um código malicioso. Com isso, a taxa do golpe dar certo aumenta consideravelmente. Para este ataque, os atacantes podem utilizar dados expostos de tráfego, em que aprendem o comportamento do alvo.

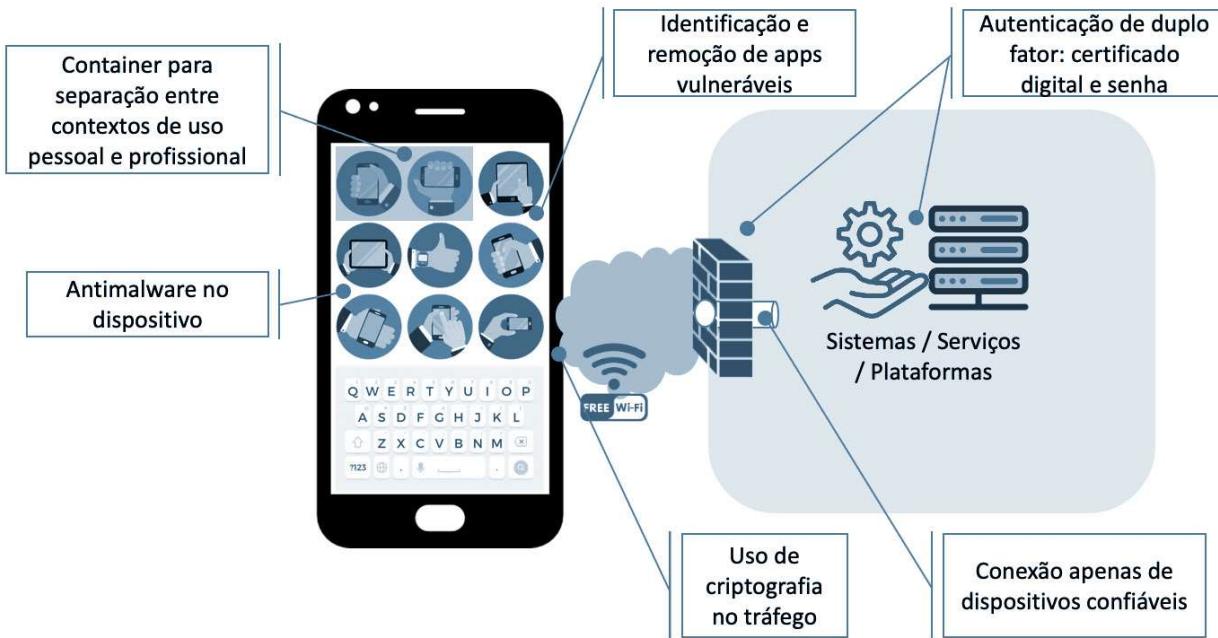
O ataque *watering hole*, assim, é similar ao *spear phishing*, que é direcionado e personalizado (ROHR, 2016).

Assim, vimos os principais riscos e as principais ameaças que devemos considerar para a segurança em dispositivos móveis. Os objetivos de segurança no uso de dispositivos móveis no mundo corporativo devem ser, no mínimo, os relacionados a seguir. Eles também são apresentados na Figura 3.11 (HOWELL *et al.*, 2020):

- Usar contêiner para isolar o contexto pessoal do contexto profissional, de modo que problemas de segurança em um contexto não afete o outro.
- Identificar e remover aplicativos vulneráveis, bem como definir e aplicar uma política de segurança clara sobre a instalação de aplicativos nos dispositivos.
- Usar *antimalware* nos dispositivos, bem como definir e aplicar uma política de segurança clara sobre a instalação de aplicativos nos dispositivos.
- Usar criptografia nas conexões com a empresa, como uma VPN.

- Aceitar conexões apenas de dispositivos confiáveis, com uso de certificados digitais, que podem fazer parte da autenticação de duplo fator, o que aumenta a segurança em caso de furto de identidade.

Figura 3.11 | Objetivos de segurança no uso de dispositivos móveis no mundo corporativo



Fonte: adaptada de Howell *et al.* (2020).

Ver anotações

## ATAQUES E DEFESAS EM DISPOSITIVOS MÓVEIS

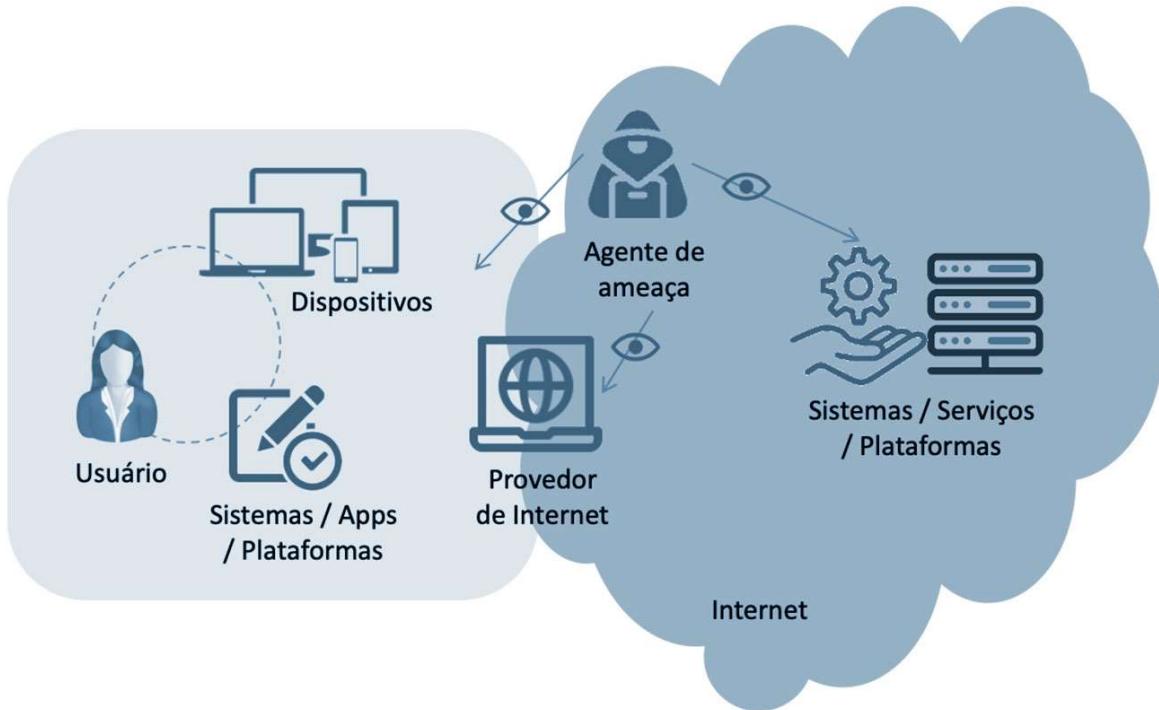
Os ataques relacionados a ambientes móveis envolvem todos os aspectos de segurança da informação. O agente de ameaça pode explorar o lado do usuário, fazendo com que o usuário clique em um *link* com conteúdo malicioso com um *phishing*, explorar o dispositivo móvel ou ainda uma aplicação. Ele pode ainda explorar a comunicação, atacando o provedor de internet, que pode ser uma rede wi-fi pública. E o atacante pode ainda atacar a empresa, explorando vulnerabilidades no ambiente formado por sistemas, serviços e plataformas, adicionalmente aos funcionários e processos da empresa. A Figura 3.12 mostra esses pontos de ataque, que complementa a visão dos principais riscos no uso de dispositivos móveis pelas empresas:

- Dados pessoais e dados corporativos se misturando.
- 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.

0

Figura 3.12 | Pontos de ataques em um acesso a empresas



Ver anotações

Fonte: elaborada pelo autor.

---

Os ataques em dispositivos móveis têm evoluído, partindo de instalação de *backdoors* e mineração de moeda digital, para códigos maliciosos mais sofisticados, capazes de esconder seus ataques, sendo mais difíceis de serem identificados e removidos (SECURITY, 2020).

---

Um dos ataques, ocorrido na Coreia do Sul, comprometeu uma empresa de *software* com boa reputação no país, fazendo com que os aplicativos usassem uma biblioteca e *plugin* modificados. O *malware*, conhecido como MalBus, fazia a coleta e o envio de informações confidenciais dos dispositivos das vítimas que utilizavam os aplicativos, que eram de utilidade pública, sobre o trânsito (SECURITY, 2020).

Para as empresas, que precisam proteger as informações sensíveis que estão agora fora do perímetro físico da própria empresa, há desafios como a particularidade dos ataques a dispositivos móveis, que estão sempre conectados

na internet e as implicações de privacidade com os colaboradores utilizando os dispositivos também para atividades pessoais (FRANKLIN *et al.*, 2019).

E há os desafios relacionados à forma como os controles de segurança para dispositivos móveis corporativos podem ser implementados (HOWELL *et al.*, 2020):

- **Bloqueio de acesso e remoção dos dados (*wiping*):** o uso do dispositivo para fins profissionais e pessoais é comum. Solução: bloqueio do acesso corporativo até uma nova concessão de acesso, de acordo com a política de segurança; remoção seletiva de dados, e não de todo o dispositivo; política que exige o *backup* dos dados pessoais, que poderão ser removidos.
- **Monitoramento do colaborador:** coleta e análise de dados sobre o dispositivo e suas atividades, que pode ser feito por múltiplos fornecedores. Solução: desenvolver uma política de segurança e utilizar técnicas que limitam a coleta de dados específicos; desenvolver uma política de segurança e utilizar técnicas para o descarte de informação de identificação pessoal.
- **Compartilhamento de dados:** uso de variados serviços e provedores de nuvens pode levar à confusão sobre quem possui o acesso às informações corporativas e aos dados pessoais. Solução: desenvolver uma política de segurança e utilizar técnicas de pseudonimização de dados; utilizar criptografia; desenvolver uma política de segurança e utilizar técnicas que limitam a coleta de dados específicos; utilizar contratos para limitar o processamento de dados por terceiros.

Além do aspecto humano para que os colaboradores não sejam vítimas de *phishing*, há a necessidade de configuração segura dos dispositivos e o provisionamento das políticas corporativas de gerenciamento dos dispositivos para a defesa. Isto pode ser feito com o *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM).

A defesa de dispositivos móveis pode ser definida de acordo com um conjunto de capacidades de segurança para dispositivos móveis, como pode ser visto na Figura 3.13 (NCCoE, 2020):

- 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*.

Figura 3.13 | Capacidades de segurança necessárias



Fonte: adaptada de NCCoE(2020).

## ATAQUES DE CAMADAS DE APLICAÇÕES E ANTIVÍRUS PARA DISPOSITIVOS MÓVEIS

A camada de aplicação de um dispositivo móvel é uma das que podem ser atacadas pelos agentes de ameaça. Ataques na camada de aplicação em dispositivos móveis exploram as vulnerabilidades técnicas de aplicativos instalados pelo usuário. Desta forma, os desenvolvedores de aplicativos móveis devem evitar códigos que insiram vulnerabilidades.

Segundo a *Open Web Application Security Project* (OWASP), as 10 maiores vulnerabilidades em aplicativos móveis são (OWASP, 2016):

1. **Uso impróprio de plataforma:** uso incorreto de característica da plataforma ou falha no uso de controles de segurança da plataforma, como as permissões ou biometria.
2. **Armazenamento inseguro de dados:** a proteção deve considerar um agente de ameaça que tenha a posse física do dispositivo móvel, ou um *malware* ou outro aplicativo que é executado no dispositivo.
3. **Comunicação insegura:** dados que trafegam em um modelo cliente-servidor podem ser interceptados em diferentes pontos, tais como uma rede de acesso comprometido, dispositivos do provedor de internet atacados ou por um *malware* no dispositivo móvel.
4. **Autenticação insegura:** ataques que exploram vulnerabilidades de forma automatizada em busca de acessos usando credenciais falsas ou que podem ser dribladas.
5. **Criptografia insuficiente:** a proteção deve considerar um agente de ameaça que possui a posse física do dispositivo móvel, ou um *malware* ou outro aplicativo que é executado no dispositivo.
6. **Autorização insegura:** ataques que exploram vulnerabilidades de forma automatizada em busca de acesso a áreas após a autenticação.
7. **Má qualidade de código:** a proteção deve considerar agentes de ameaça que podem utilizar entradas não confiáveis para as chamadas do código, que podem levar à execução de códigos arbitrários.
8. **Modificação de código:** a exploração pode ser pelo uso de fontes de aplicativos de terceiros que hospedam os códigos modificados, ou pela instalação pelo usuário vítima de *phishing*.
9. **Engenharia reversa:** o atacante analisa o aplicativo com a ajuda de diversas ferramentas para entender e explorar as funções.

Ver anotações

10. **Funcionalidade exposta:** a exposição em aplicativos pode relevar funcionalidades de sistemas de *backend*, que pode então ser explorada diretamente.

Os antivírus para dispositivos móveis devem ser considerados uma camada de proteção, não podendo ser considerado uma solução para os problemas de segurança e privacidade. Muitos antivírus fazem a detecção de *malware* com base em assinaturas, o que significa que somente aqueles conhecidos poderão ser detectados. Os *malwares* novos e o *phishing* são detectados com dificuldades pelos antivírus e outros mecanismos devem ser utilizados pela empresa para complementar a proteção.

Ver anotações

## ■ ENGENHARIA SOCIAL (ACESSO AS INFORMAÇÕES PESSOAIS) DE DISPOSITIVOS MÓVEIS

O *phishing* conta com a engenharia social, que explora a atenção, curiosidade, caridade, medo ou possibilidade de obtenção de vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou *site* popular. Envolve a possibilidade de inscrição em serviços de proteção de crédito, ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas em que entregam suas credenciais, senhas ou informações sensíveis, além de poderem, ainda, instalar códigos maliciosos (CERT, 2020).

O usuário recebe um *phishing* e clica em um *link* que pode levar a um site onde ele entrega informações pessoais ou as suas credenciais de acesso, ou pode levar à instalação de *malware*.

### EXEMPLIFICANDO

O *phishing* é explorado também no mundo dos jogos eletrônicos, com os atacantes distribuindo *malwares* via *links* em *chat* de jogos e criando aplicativos falsos que visam ser populares, utilizando inclusive ícones similares para ludibriar as vítimas (SECURITY, 2020).

Um dos *malwares*, distribuído via mídia social, plataforma de jogos ou *chat* de jogos, é o LeifAccess ou o Shopper, que envia mensagens falsas de alertas para que o usuário ative serviços de acessibilidade do dispositivo móvel. O *malware* então utiliza as funções de acessibilidade para criar contas, baixar aplicativos e postar mensagens usando a conta da vítima (SECURITY, 2020).

Ver anotações

## SEGURANÇA EM DISPOSITIVOS MÓVEIS PARA EMPRESAS

Para as empresas é importante adotar uma arquitetura de referência para os dispositivos móveis de forma a prover acesso seguro ao mesmo tempo em que a privacidade dos usuários seja preservada (HOWELL *et al.*, 2020).

Um dos principais pontos da arquitetura é a definição do modelo a ser adotado, que pode ser a disponibilização de dispositivos móveis somente para o uso corporativo, a permissão para uso pessoal (*Corporate-Owned Personally-Enabled*, COPE) ou o *Bring Your Own Device* (BYOD) ou *Choose Your Own Device* (CYOD). No modelo BYOD ou CYOD, o dono do dispositivo móvel é o próprio usuário, enquanto nos outros a propriedade é da empresa. O modelo COPE provê flexibilidade de uso ao permitir que tanto a empresa quanto o usuário possam instalar aplicativos no dispositivo, que é de propriedade da empresa (NCCoE, 2020).

Neste contexto, algumas recomendações de segurança e privacidade para empresas adotarem no uso de dispositivos móveis são (FRANKLIN *et al.*, 2020):

- 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* (EMM), plataformas de defesa contra ameaças móveis ou serviço de voto 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 demonstram qualquer comportamento que representa

um risco de segurança ou de privacidade. Este serviço de voto pode ser utilizado 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.

Ver anotações

As recomendações fazem parte do ciclo de vida de implantação de dispositivos móveis corporativos (Figura 3.14), que considera aspectos de planejamento, implantação e operação dos dispositivos móveis na empresa (FRANKLIN *et al.*, 2020):

- **Identificar os requisitos para o uso de dispositivos móveis**, com o entendimento do caso de uso e as capacidades existentes. É importante a visão de TI e de negócios. O caso de uso pode envolver a realização de atividades fora da empresa, bem a interação com profissionais de empresas parceiras. O caso de uso pode incluir elementos comuns como a definição dos usuários, a razão deles precisarem dos dispositivos móveis e quais aplicativos ou características do dispositivo móvel serão necessários para o cumprimento dos objetivos corporativos. As capacidades existentes envolvem os dispositivos

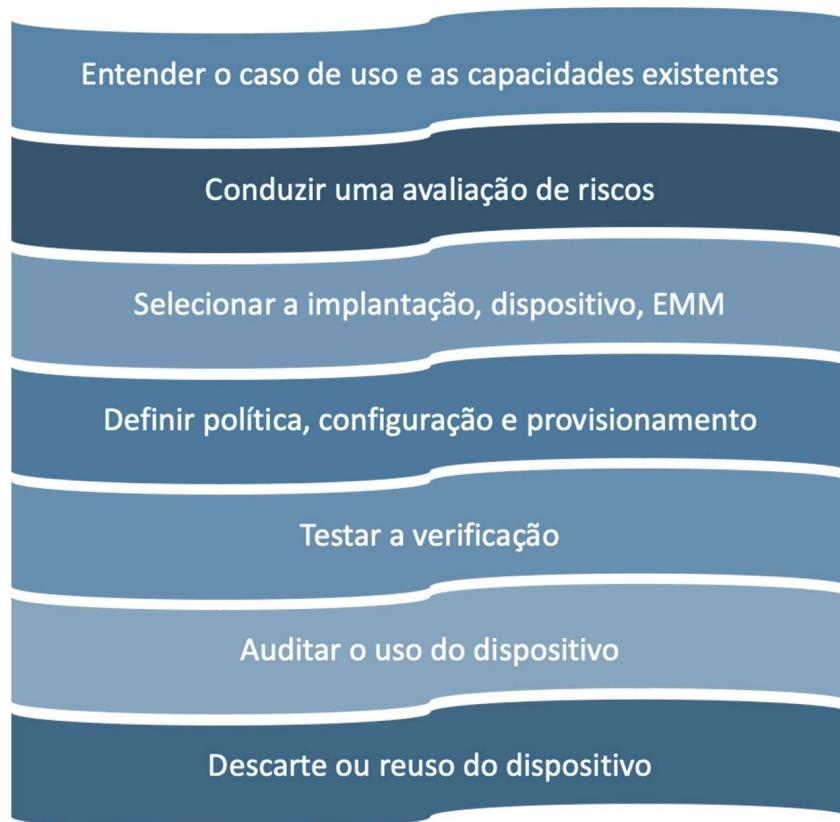
móveis atualmente utilizados pelos colaboradores, que influenciam na definição do modelo de implantação corporativo, que pode ser o uso estritamente corporativo, COPE ou BYOD / CYOD.

- **Fazer uma avaliação de riscos**, considerando os dispositivos móveis, aplicações e sistemas utilizados para gerenciar todo o sistema. É importante ter uma visão no nível organizacional, além do tecnológico.
- **Implantar a estratégia corporativa para o sistema móvel**, com o EMM/MDM podendo ser utilizado na empresa (*on-premise*) ou na nuvem. Os serviços de infraestrutura da empresa precisam se integrar ao EMM, como os serviços de autenticação.
- **Definir e implantar a política dos dispositivos**, incluindo o modelo de implantação corporativo, e a possibilidade de uso pessoal dos dispositivos. Após as configurações, os dispositivos móveis devem ser provisionados para os usuários.
- **Testar as configurações e os softwares instalados**, em um processo de gestão de mudanças, avaliando os impactos das implantações dessas mudanças, que devem envolver também as atualizações e instalação de *patches*. A implantação dessas mudanças também deve ser testada e planejada cuidadosamente.
- **Auditar todo o ambiente periodicamente para validar a efetividade dos controles de segurança**, e atualizar os mecanismos de segurança de acordo com os riscos, que são dinâmicos. Além da auditoria da segurança, é importante auditar o uso dos dispositivos pelos usuários, que devem estar de acordo com a política definida.
- **Descartar ou reusar os dispositivos móveis** após um processo de sanitização é importante para preservar as informações corporativas e pessoais existentes nesses aparelhos.

Ver anotações

---

Figura 3.14 | Ciclo de vida de implantação de dispositivos móveis corporativos



0

Ver anotações

Fonte: adaptada de Franklin *et al.* (2020).

#### EXEMPLIFICANDO

Um exemplo de caso de uso para dispositivos móveis é o desenvolvimento de pesquisas médicas, que antes eram feitas com os voluntários sendo conduzidos para a empresa. Em um novo cenário, os pesquisadores irão visitar os voluntários, coletando dados e fazendo diagnósticos de forma remota. É preciso que os pesquisadores tenham acesso aos dados históricos dos voluntários que estão no servidor da empresa, mas por meio do dispositivo móvel. A empresa precisa prover este acesso remoto ao servidor de uma forma segura.

#### SAIBA MAIS

Com o avanço no uso de dispositivos móveis, este canal tem se tornado o canal preferido pelos criminosos. O termo *phishing* surgiu no contexto de e-mails. O *phishing* conta com a engenharia social, que explora a atenção, curiosidade, caridade, medo ou possibilidade de obtenção de vantagem financeira, com o criminoso se passando por uma instituição como banco, empresa ou site popular. Envolve a possibilidade de inscrição em serviços

de proteção de crédito, ou o cancelamento de cadastro, conta bancária ou cartão de crédito, e leva a vítima a páginas falsas em que entregam suas credenciais, senhas ou informações sensíveis, além da instalação de códigos maliciosos.

Quando o ataque acontece por mensagens de texto SMS enviados ao dispositivo móvel do alvo, o termo utilizado pode ser *SMiShing*.

Ver anotações

#### PESQUISE MAIS

Para o desenvolvimento de aplicativos móveis seguro, você pode adotar os testes previstos no *Mobile Security Testing Guide* (MSTG), do OWASP (OWASP, 2019). Os testes propostos buscam identificar e tratar as vulnerabilidades, e visam a autenticação, rede, criptografia, qualidade do código, engenharia reversa e a educação do usuário. Há testes específicos para Android e para iOS.

OWASP. **Intermediate update 1.1.3** (OSS Release), 4 ago. 2019. Disponível em: <https://bit.ly/31cu55B>. Acesso em: 26 dez. 2020.

Chegamos ao fim dos aspectos de segurança e privacidade em dispositivos móveis. Atualmente, grande parte dos acessos a variados serviços é feito pelo dispositivo móvel. Como usuário, é importante saber utilizar o dispositivo móvel de uma forma segura. E, como profissional de segurança, vários aspectos devem ser planejados e implementados, começando com a definição do modelo, que pode ou não mesclar dados corporativos com dados pessoais, o que exige o planejamento e a implantação de diferentes controles de segurança. E as ameaças estão presentes em diferentes ambientes e em variados componentes.

Até a próxima aula!

#### FAÇA VALER A PENA

##### Questão 1

Um dos grandes desafios para a segurança em dispositivos móveis é que, além de ampliarem o perímetro da empresa, há dados pessoais junto dos dados corporativos, que precisam ser protegidos. Há alguns modelos que podem ser adotados pelas empresas quanto a este desafio.

O modelo que não permite que o usuário da empresa utilize o dispositivo móvel para fins particulares é o:

a. Dispositivo cedido para uso exclusivamente corporativo.

Correto!

O dispositivo cedido para uso exclusivamente corporativo não pode ter dados pessoais e é de propriedade da empresa.

b. Corporate-Owned Personally-Enabled (COPE).

c. Bring Your Own Device (BYOD).

d. Choose Your Own Device (CYOD).

e. Enterprise Mobility Management (EMM).

## Questão 2

Considere as seguintes capacidades de segurança:

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

Estas capacidades de segurança devem ser aplicadas no contexto de:

a. Dispositivos móveis.

Correto!

As capacidades de segurança citadas devem ser aplicadas a dispositivos móveis, os quais têm uma série de ameaças relacionadas.

b. Gerenciamento de riscos.

c. Phishing.

d. Auditoria.

e. Criptografia.

Ver anotações

### Questão 3

O *Enterprise Mobility Management/Mobile Device Management* (EMM/MDM) é um dos principais controles de segurança para dispositivos móveis das empresas. O EMM/MDM é uma solução para prover segurança em dispositivos móveis de usuários que são autorizados a acessar recursos da empresa.

Considere as seguintes afirmativas a seguir:

- I. O EMM/MDM provisiona os perfis de configuração para os dispositivos.
- II. O EMM/MDM aplica as políticas de segurança nos dispositivos.
- III. O EMM/MDM monitora a conformidade dos dispositivos com as políticas.

É correto o que se afirma em:

a. I, II e III.

Correto!

O EMM/MDM faz o gerenciamento de dispositivos móveis da empresa, executando as ações citadas. Geralmente o EMM/MDM é composto por dois componentes principais. O primeiro é um serviço *backend* que os administradores utilizam para gerenciar as políticas, configurações e outras ações de segurança que são aplicadas nos dispositivos móveis. O segundo componente é um agente que é instalado no dispositivo que permite a aplicação das ações definidas pela empresa.

b. I e III, apenas.

c. III, apenas.

d. I e II, apenas.

e. I, apenas.

Ver anotações

## REFERÊNCIAS

BROWN, C. et al. **Assessing Threats to Mobile Devices & Infrastructure** – The Mobile Threat Catalogue. Draft NIST 8144. **National Institute of Standards and Technology**. U.S. Department of Commerce, set. 2016. Disponível em: <https://bit.ly/39b20jr>. Acesso em: 22 dez. 2020.

CERT.br. Golpes na Internet. **Cartilha de segurança para internet**. Disponível em: <https://bit.ly/2Qq55FF>. Acesso em: 19 dez. 2020.

FRANKLIN, J. M. et al. Mobile Device Security – Cloud and Hybrid Builds. **NIST Special Publication 1800-4**. National Institute of Standards and Technology. U.S. Department of Commerce, fev. 2019. Disponível em: <https://bit.ly/3diWGMj>. Acesso em: 22 dez. 2020.

FRANKLIN, J. M. et al. Guidelines for Managing the Security of Mobile Devices in the Enterprise. **Draft NIST Special Publication 800-124**, Revision 1. NIST, National Institute of Standards and Technology. U.S. Department of Commerce, mar. 2020. Disponível em: <https://bit.ly/3vQgS9X>. Acesso em: 22 dez. 2020.

HIGA, P. **Por que o 5G vai mudar sua vida (mesmo que você não tenha nem 4G)**. Tecnoblog, 2016. Disponível em: <https://bit.ly/39cejvE>. Acesso em: 26 dez. 2021.

HOWELL, G. et al. NCCoE, National Cybersecurity Center of Excellence. NIST, National Institute of Standards and Technology. U.S. Department of Commerce. **NIST SPECIAL PUBLICATION 1800-21. Mobile Device Security**:

**Corporate-Owned Personally-Enabled (COPE).** Disponível em:

<https://bit.ly/2QCg672>. Acesso em: 22 dez. 2020.

**KASPERSKY. Top 7 Mobile Security Threats in 2020.** Disponível em:

<https://bit.ly/3slu5Mi> Acesso em: 26 dez. 2020.

**KRISTIINA. OWASP mobile top 10 security risks explained with real world examples.** The Startup, 17 mar. 2019. Disponível em: <https://bit.ly/3vZngIR>. Acesso em: 27 dez. 2020.

**MCAFEE. McAfee Mobile Threat Report – Mobile Malware Is Playing Hide and Steal,** 2020. Disponível em: <https://bit.ly/39aNXdN>. Acesso em: 26 dez. 2020.

NCCoE, National Cybersecurity Center of Excellence. NIST, National Institute of Standards and Technology. U.S. Department of Commerce. **Mobile Device Security.** Disponível em: <https://bit.ly/3vVrkUm>. Acesso em: 22 dez. 2020.

NIST, National Institute of Standards and Technology. U.S. Department of Commerce. NCCoE, National Cybersecurity Center of Excellence. **Mobile Threat Catalogue.** Disponível em: <https://bit.ly/31eAnl9>. Acesso em: 22 dez. 2020.

NIST, National Institute of Standards and Technology. U.S. Department of Commerce. Joint Task Force. **NIST Special Publication 800-53 Revision 5 – Security and Privacy Controls for Information Systems and Organizations,** set. 2020 Disponível em: <https://bit.ly/39cycmu>. Acesso em: 26 dez. 2020.

**OWASP. OWASP Mobile Top 10.** Disponível em: <https://bit.ly/3rleMSF>. Acesso em: 26 dez. 2020.

**OWASP. Intermediate update 1.1.3 (OSS Release),** 4 ago. 2019. Disponível em: <https://bit.ly/3sj3HCN>. Acesso em: 26 dez. 2020.

ROHR, A. O que são phishing, watering hole e golpes on-line: G1 Explica. **G1 Segurança Digital,** 18 ago. 2016. Disponível em: <https://glo.bo/39bMLH2>. Acesso em: 22 dez. 2020.

**SECURITY Magazine. 2020: The Year of Mobile Sneak Attacks?,** 9 mar. 2020. Disponível em: <https://bit.ly/2QCgSks>. Acesso em: 26 dez. 2020.

0

Ver anotações