SEÇÃO INTERATIVA: TECNOLOGIA

USO DO DISPOSITIVO PESSOAL NO AMBIENTE DE TRABALHO: NÃO É TÃO SEGURO

Atualmente, os funcionários trazem dois milhões de dispositivos móveis para o trabalho, mas, enquanto o uso do iPhone, do iPad e de outros dispositivos de computação móvel no local de trabalho está crescendo, assim também estão crescendo os problemas de segurança. Quer esses dispositivos sejam fornecidos pela empresa, quer sejam de propriedade dos funcionários, eles estão abrindo novos caminhos que permitem acessar os dados corporativos que precisam ser monitorados de perto e protegidos. Os dados sensíveis armazenados em dispositivos móveis trafegam, tanto física quanto eletronicamente, do escritório para a casa e possivelmente para outros locais. Um bom número de especialistas em segurança acredita que os smartphones e outros dispositivos móveis representam, atualmente, uma das mais sérias ameaças de segurança para as organizações.

Um dos maiores perigos de segurança dos smartphones é que eles podem ser perdidos. Isso coloca em risco todos os dados pessoais e corporativos armazenados no dispositivo, bem como o acesso aos dados corporativos nos servidores remotos. De acordo com um estudo do Instituto Ponemon, envolvendo 116 organizações, 62% dos dispositivos móveis que foram perdidos ou roubados continham dados sensíveis ou informações confidenciais. Um relatório sobre o Estado da segurança móvel, publicado pela Information Week em 2013, afirmou que 78% das empresas pesquisadas respondeu que sua maior preocupação com relação à segurança dos dispositivos móveis é a perda ou roubo dos dispositivos, e 45% dos entrevistados relataram que dispositivos móveis contendo dados corporativos haviam desaparecido nos últimos 12 meses.

O acesso físico aos dispositivos móveis pode ser uma ameaça maior do que a invasão em uma rede por um hacker, pois requer menos esforço para consegui-lo. Atacantes experientes podem facilmente contornar senhas ou bloqueios nos dispositivos celulares ou acessar dados criptografados. Isso pode incluir não apenas dados corporativos encontrados no dispositivo, mas também senhas que residem em lugares como o iPhone Keychain, o que poderia permitir o acesso aos serviços corporativos, como e-mail ou a rede privada virtual. Além disso, muitos usuários de smartphones deixam seus telefones totalmente desprotegidos para iniciar a sua utilização. No Websense e no Estudo global sobre os Riscos da Mobilidade realizado pelo Instituto Ponemon, 59% dos entrevistados relataram que os funcionários contornavam ou desabilitavam os recursos de segurança, como senhas e proteção de teclado. Os invasores também podem ganhar o acesso físico aos dispositivos móveis, conectando em um dispositivo usando uma conexão USB ou o *slot* para cartão SD. Deixar um dispositivo sozinho em uma mesa ou cadeira mesmo que durante um minuto pode levar a danos graves.

Outra grande preocupação hoje é o maior vazamento de dados causados pelo uso de serviços de computação em nuvem. Funcionários estão cada vez mais usando os serviços de nuvem pública, como Google Drive ou Dropbox para compartilhamento de arquivos e colaboração. A Mashery, uma empresa de 170 empregados que ajuda outras empresas a desenvolver aplicativos, por exemplo, permite que seus funcionários munidos de iPhones utilizem o Dropbox, Box, YouSendIt, Teambox e Google Drive, para armazenar memorandos, planilhas e informações de clientes. Esses serviços são vulneráveis. Em julho de 2012, o Dropbox relatou uma perda de nomes de login e senhas de um grande número de clientes e, em 2011, hackers chineses conseguiram acessar centenas de contas do governo dos Estados Unidos no Gmail do Google. Não há muita coisa que uma empresa possa fazer para prevenir que funcionários autorizados a utilizar seus smartphones para acessar dados corporativos encaminhem um documento da empresa para um serviço de armazenamento em nuvem a fim de poder trabalhar nele mais tarde.

Embora os ataques deliberados por parte de hackers nos dispositivos móveis tenham sido limitados em alcance e impacto, essa situação está piorando, especialmente entre dispositivos Android vulneráveis a aplicativos maliciosos. A segurança na plataforma Android é muito menor sob o controle do Google do que nos dispositivos da Apple rodando iOS, porque o Google tem um modelo de aplicativo aberto. O Google não analisa nenhum app Android (como a Apple faz com os seus apps), mas, em vez disso, baseia-se em obstáculos técnicos para limitar o impacto dos códigos maliciosos, bem como no feedback de usuários e especialistas em segurança. Os aplicativos do Google são executados em uma "caixa de areia" ("*sandbox*"), onde eles não conseguem afetar ou manipular outros recursos do dispositivo sem a permissão do usuário. O Google remove do Google Play, sua plataforma oficial de distribuição, quaisquer apps que não sigam suas regras contra atividade maliciosa.

O Google também toma medidas preventivas para reduzir o número de apps com *malware*, como examinar cuidadosamente os antecedentes dos desenvolvedores e exigir que eles se registrem no seu serviço de pagamento Checkout (a fim de incentivar os usuários a pagar por aplicativos que utilizam seu serviço, mas também para forçar os desenvolvedores a revelar suas identidades e

informações financeiras). As recentes melhorias de segurança para o Android incluem a atribuição de vários níveis de confiança para cada aplicativo, ditando que tipo de dados de um aplicativo pode acessar dentro seu domínio e proporcionar uma forma mais robusta para armazenar as credenciais de criptografia usadas para acessar informações e recursos sensíveis. Ainda assim, do ponto de vista corporativo, é quase impossível impedir que os funcionários efetuem download de aplicativos que possam rastrear informações críticas quando as pessoas usam seus próprios dispositivos no local de trabalho.

Além da ameaça dos apps suspeitos, os smartphones de todas as faixas são suscetíveis a *malware* baseado em navegador que se aproveita de vulnerabilidades em todos os navegadores.

As violações de segurança de dispositivos móveis carregam um preço elevado. Segundo a pesquisa sobre o Estado da Mobilidade, realizada pela Symantec em 2012, o custo médio anual de incidentes em dispositivos móveis, incluindo perda de dados, danos à marca, perda de produtividade e perda da confiança do cliente foi de US$ 429 mil para grandes empresas. O custo médio anual de incidentes móveis para as pequenas empresas foi de US$ 126 mil. Essas brechas de segurança também podem causar enormes prejuízos intangíveis à reputação de uma empresa. A Comissão de Valores Imobiliários norte-americana exige que a divulgação de informações confidenciais não autorizada, seja por dispositivos não seguros, por aplicações não confiáveis ou por falha de segurança na nuvem, deva ser anunciada publicamente, se a informação puder afetar o preço das ações de uma empresa.

Fontes: Michael Finneran, "2013 State of Mobility Survey", *Information Week*, jun. 2013; Symantec Corporation, "State of Mobility Global Results", 2013; Dan Goodin, "Google Strengthens Android Security Muscle with SELinux Protection, ArsTechnica, 24 jul. 2013; Acronis, "Top 5 Security Threats for the Mobile Enterprise and How to Address Them", 2013; Karen A. Frenkel, "Best Practices of Mobile Technology Leaders", CIO Insight, 24 jul. 2013; Don Reisinger, "Mobile Security: Why It's Your Biggest Threat", *CIO Insight*, Quentin Hardy, "Where Apps Meet Work, Secret Data Is at Risk", *New York Times*, 3 mar. 2013; Ponemon Institute, "Global Study on Mobility Risks", fev. 2012; e Matthew G. Cook, Bruce Wiatrak e Keith Olsen, "5 Top BYOD Threats for 2013", *Information Week*, jan. 2013; e Zach Epstein, Sara Gates, "iPhone Malware: Kaspersky Expects Apple's IOS to Be Under Attack By Next Year", *Huffington Post*, 15 mai. 2012.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Um smartphone é um microcomputador em sua mão. Discuta as implicações de segurança dessa afirmação.
2. Quais questões humanas, organizacionais e tecnológicas devem ser consideradas pela segurança do smartphone?
3. Quais problemas as falhas de segurança do smartphone podem causar para as empresas?
4. Quais passos as empresas e os indivíduos podem tomar para tornar seus smartphones mais seguros?

GARANTIA DA QUALIDADE DE SOFTWARE

Além de implantar segurança e controle eficientes, as empresas podem melhorar a qualidade e a confiabilidade dos sistemas por meio de métricas e testes rigorosos de software. Métricas de software são premissas objetivas do sistema na forma de medidas quantificadas. O uso contínuo de métricas permite que o departamento de sistemas de informação e os usuários finais meçam conjuntamente o desempenho do sistema e identifiquem problemas à medida que eles ocorrem. Exemplos de métricas de software incluem números de transações que podem ser processadas em uma unidade específica de tempo, tempo de resposta on-line, número de cheques de pagamento impressos por hora e número de erros conhecidos por centenas de linhas de código. Para que as métricas sejam bem-sucedidas, precisam ser cuidadosamente definidas e devem ser formais, objetivas e usadas com consistência.

O teste inicial regular e completo também contribuirá significativamente para a qualidade do sistema. Muitos consideram esse teste uma maneira de provar a exatidão do trabalho realizado. Na verdade, sabemos que todo software, independentemente de seu tamanho, está recheado de erros que precisam de testes para serem descobertos.

O bom teste começa antes de o software sequer ser escrito, por meio de um *acompanhamento* (walkthrough) — uma revisão de uma especificação ou documento de projeto realizada por um pequeno grupo de pessoas cuidadosamente selecionadas com base nas habilidades necessárias para