Consumerização dá nova arma ao gestor de TI. Os vírus benéficos
Matt Hamblen

Eles serão códigos embutidos em dados confidenciais que podem identificar dispositivos não autorizados a usá-los e se destruírem.

Os gerentes de TI que lutam com as políticas do tipo 'traga o seu próprio dispositivo' (BYOD) podem esperar ver uma explosão de diferentes smartphones e tablets sendo utilizados por seus funcionários nos próximos anos.

Como um resultado disso, as instalações de TI não serão capazes de acompanhar as demandas de suporte necessárias para proteger os dados da empresa utilizados em vários dispositivos, disse o analista do Gartner, Ken Dulaney, em uma recente entrevista.

"Nos próximos anos, o número de dispositivos pessoais em uso vai ultrapassar a habilidade da TI de manter a empresa segura", disse ele. "A TI não pode lidar com todos esses dispositivos. O pessoal de TI está enlouquecendo. Eles entram em discussões para saber se os usuários devem ou não fazer atualizações".

E devido ao fato de que as instalações de TI não serão capazes de manterem-se atualizadas, os fornecedores de software serão forçados a inovar e a criar o que Dulaney chamou de "vírus benéficos" – softwares que serão incorporados em dados corporativos confidenciais, tais como informações financeiras ou de pacientes que sejam carregadas em um smartphone ou em outro tipo de dispositivo móvel. Esses vírus benéficos funcionarão como o software de Gestão de Direitos Autorais (Digital Rights Management – DRM) usado em arquivos de vídeo e música, que requer uma licença para reproduzir o arquivo, explicou Dulaney.

Em sua concepção, contudo, os vírus benéficos levariam as coisas mais além: dados confidenciais "seriam inteligentes o bastante para se auto apagarem...", disse Dulaney.

"É hora da SAP e da Oracle começarem a pensar em fazer isso. E a tarefa é algo muito mais complicado do que pensamos", disse Dulaney. "Dentro de cada pedaço de dados [corporativos] haveria um vírus benéfico que, sempre que os dados se encontrassem no lugar errado [tal como em um dispositivo não autorizado], ele diria, 'Eu não vejo uma permissão para estar aqui e vou me apagar'".

Hoje em dia, as empresas dependem de diferentes empresas de softwares de Gestão de Dispositivos Móveis (Mobile Device Management - MDM) para monitorar quais usuários com smartphones ou tablets têm autorização para acessar certos aplicativos e se eles podem utilizar os dados na sua forma off-line, ou fora de uma nuvem corporativa. Mas Dulaney disse que essa não é uma abordagem suficientemente segura, e ele prevê que a MDM – uma "invenção tática" - não será viável por mais que três anos.

"Precisamos ser mais inteligentes em relação à segurança em dispositivos móveis", disse ele. "No momento, os dados dependem da proteção do ambiente no qual estão armazenados. Mas existem vazamentos de dados fora da empresa com muitos pontos de entrada para a mesma [muitas vezes a partir de dispositivos móveis que podem debilitar a segurança da empresa]"

"Pagar por MDM é uma boa ideia hoje, mas eu não consigo ver a indústria de computação móvel se estabilizando para que, assim, possamos fazer as coisas que fizemos com os notebooks e desktops por anos", disse ele. "As pessoas estão sendo movidas pela moda ao trazerem tantos dispositivos novos para dentro da empresa".

Há anos, Dulaney vem aconselhando milhares de gerentes de TI e de CIOs sobre as políticas BYOD, estimulando-os a dar aos usuários opções de escolha de smartphones além do clássico BlackBerry, com sua segurança BlackBerry Enterprise Server.

A abordagem de Dulaney é parcialmente projetada para impedir que as instalações de TI entrem em conflito com os usuários que queiram escolher seus próprios smartphones ou, mais

recentemente, seus tablets. “As instalações de TI introduzem exigências de segurança sobre os dispositivos e sobre a TI, isso tem valor para o usuário final, mas o usuário final encara isso como uma limitação à sua liberdade”, disse ele.

O conselho atual da Gartner sobre a gestão de dispositivos móveis para as instalações de TI é o de considerar a criação de todos ou de alguns dos três diferentes camadas de suporte – plataforma, ferramenta e portas. No suporte a plataformas, a TI oferece ao dispositivo um suporte completo do tipo que é oferecido para computadores, e o dispositivo é escolhido pela TI e será tipicamente utilizado em aplicações verticais.

Com o suporte ao nível de ferramentas, a TI dá suporte um estreito conjunto de aplicativos em um dispositivo móvel, incluindo suporte a aplicativos baseados em servidores e em web em um conjunto mais amplo de dispositivos pré-aprovados. Os aplicativos locais não são suportados.

Com o suporte ao nível de portas, a TI fornece suporte prático, principalmente para ensinar os funcionários, para dispositivos não suportados ou aplicativos não suportados em um dispositivo suportado. Os custos para o suporte nesse tipo de abordagem, que podem ser generosos, são cobrados dos usuários.

“Com o declínio do RIM, a ascensão da Apple e dos iPads tornou o BYOD um assunto importante para a TI”, disse Dulaney. “Muitas empresas ainda utilizam o Blackberry como uma base para suas práticas móveis, mas permitem que os usuários comprem dispositivos com sistemas Android e Apple para uso de aplicativos restritos, às vezes exigindo que eles sejam apenas aplicativos baseados em navegador”.

Um exemplo da abordagem baseada em navegador é a da American National Insurance Company (ANICO), que anunciou na terça-feira que tem trabalhado com a IBM e a parceira da IBM, Streebo, para estender as informações de clientes existentes baseadas em computadores para dispositivos móveis incluindo os iPhones, iPads e dispositivos Blackberry e Android. Milhares de agentes podem utilizar as capacidades móveis para buscar políticas existentes de seguro e ajudar os clientes a se inscreverem no seguro, disse Deanna Walton, vice-presidente assistente dos sistemas de campo da ANICO, em uma entrevista.

Utilizar uma abordagem baseada em web foi “a coisa mais fácil, rápida e correta a se fazer, e não precisamos tocar no dispositivo nativo” para adicionar o novo aplicativo, disse Walton. No futuro, ela disse que a ANICO pode encontrar a necessidade de implantar aplicativos móveis nativos utilizados em campo pelos agentes que lidam com dados confidenciais.

“Se formos nessa direção, nós definitivamente iriamos precisar prestar atenção ao aspecto da segurança”, disse ela. “A maior parte dos agentes são independentes e nós teríamos de resolver como iríamos lidar com a perda de um dispositivo”.

Do ponto de vista de Dulaney, o sucesso móvel da ANICO é uma exceção no mundo atual do BYOD.

Fonte: IDG Now! [Portal]. Disponível em: <http://idgnow.uol.com.br/ti-corporativa/2012/05/16/consumerizacao-da-nova-arma-ao-gestor-de-ti-os-virus-beneficos/>. Acesso em: 16 maio. 2012.