TÃO ESSENCIAL QUANTO A BATERIA

POPULARIZAÇÃO DE SMARTPHONES E TABLETS ATRAI A ATENÇÃO DE CRIMINOSOS VIRTUAIS, QUE FATURAM MILHÕES, E EXIGEM MAIS ATENÇÃO DE USUÁRIOS E EMPRESAS COM A SEGURANÇA

Segundo pesquisa divulgada pela Juniper Research, empresa especializada em estatísticas do setor de telecomunicações, o mercado de softwares de segurança para dispositivos móveis (incluindo tablets, smartphones e feature phones) deve ultrapassar US$ 1 bilhão já em 2013, e quase US$ 3,7 bilhões em 2016 - quando haverá 277 milhões de aparelhos com algum tipo de proteção instalada. Quase 69% das vendas desse tipo de solução serão destinadas ao mercado empresarial.

A presença de softwares de segurança é comum no setor de computadores e laptops há muitos anos, mas ainda não nos dispositivos móveis. O aumento explosivo nas vendas de smartphones e tablets, que cada vez mais substituem outros dispositivos como principal terminal de acesso à Internet, no entanto, tem continuamente atraído a atenção de criminosos virtuais. Assim, explica a Juniper, a conscientização do público sobre a vulnerabilidade desses aparelhos também aumenta.

"Os usuários corporativos são o maior alvo em potencial devido à segurança móvel insuficiente", diz Nitin Bhas, analista da Juniper e autor do relatório da pesquisa. "As empresas terão que incorporar dispositivos móveis às suas redes corporativas, como forma de reforçar políticas de proteção e auditar os aparelhos."

A pesquisa descobriu que as empresas estão começando a gastar mais em aplicativos de segurança para dispositivos móveis, conforme se tornam parte crítica da política empresarial. No entanto, apenas um em cada 20 smartphones e tablets possui softwares de segurança de terceiros instalado, apesar do aumento das ameaças.

EMPRESAS

De olho não só no tamanho do mercado, mas também na migração natural para os dispositivos móveis, os grandes players desenvolvem linhas completas de segurança móvel, seja para o consumidor final ou corporativo. "As companhias de todo o mundo

estão interessadas em trazer a mobilidade para dentro de suas organizações", diz Chris Kenworthy, vice-presidente sênior mundial da McAfee para grandes empresas. A McAfee, explica, está apostando em segurança para todo tipo de endpoints, pois eles são extensões de uma mesma rede.

Kenworthy acredita que as companhias não deveriam ter que criar todo um ecossistema separado para proteger apenas dispositivos móveis. Mas isso, explica, esbarra em uma série de dificuldades, principalmente dos departamentos de TI. "Este grande fenômeno que chamamos de mobilidade está entrando nas empresas mais rápido do que elas são capazes de se adaptar".

Segundo o executivo, as tecnologias predecessoras vieram devagar, e os departamentos de TI conseguiram controlar a entrada dos respectivos dispositivos nas redes empresariais e assegurar a segurança. Com os dispositivos móveis foi diferente, e as corporações se veem obrigadas a trabalhar muito rapidamente.

No entanto, as tecnologias desenvolvidas para este mercado ainda são muito recentes, e muitas vezes os gestores desconhecem os portifólios de proteção móvel das empresas. "0 desafio para os profissionais de TI é saber o que usar e comprar, pois as empresas precisam da mesma proteção de antes."

Para Kenworthy, as companhias já estão correndo atrás do prejuízo: 70% delas permitem o uso de tecnologias móveis na rede corporativa. "Há uma série de vantagens nisso, como a diminuição na carga de trabalho dos funcionários que operam o sistema de telefonia tradicional nas grandes empresas. A maioria dos funcionários também está feliz com a migração."

HACKERS

Roubar informações, incluindo arquivos e dados de contatos, além de obter acesso a servidores corporativos remotos e localidades geográficas: esses são os principais objetivos dos hackers que desenvolvem malwares para smartphones e tablets, diz Vanessa Pádua, engenheira de sistemas da Fortinet. "Os principais alvos são quaisquer dispositivos móveis que possuam conectividade", explica. Esses aparelhos, que armazenam informações profissionais e pessoais de seus usuários, ainda são afetados por dois fatores agravantes: estão conectados em todos os lugares, o tempo todo.

"Na verdade, o perfil dos criminosos

70% das organizações já permitem o uso de tecnologias móveis na rede corporativa, segundo estudo

cibernéticos mudou bastante nos últimos anos", diz Ascold Szymanskyj, vice-presidente de vendas e operações para América Latina da F-Secure. "Antigamente os vírus eram escritos por adolescentes, e a principal motivação era deixar uma marca, como um pichador. Hoje existem verdadeiras quadrilhas organizadas nesse tipo de crime pela Internet, que movimentam milhões de dólares."

Para Szymanskyj, os dispositivos móveis são ainda mais vulneráveis do que os PCs. Primeiro, porque passam a falsa sensação de que os vírus atacam mais os desktops e notebooks, e "qualquer dispositivo que esteja conectado à Internet pode sofrer algum tipo de invasão". Além disso, com a utilização de smartphones e tablets no ambiente corporativo, o interesse dos cibercriminosos por dados sensíveis aumenta.

"Hoje é comum a figura dos crackers, cuja principal motivação é o roubo de dados que possam ter algum valor comercial, como informações cadastrais, números e senhas de contas bancárias e cartões de crédito", diz o executivo da F-Secure, que lista ainda aplicativos maliciosos que se instalam no dispositivo e gravam tudo o que o usuário digita.

Apesar de ainda poucos (com relação aos malwares para sistemas operacionais em computadores), o número de novos vírus específicos para dispositivos móveis tem crescido exponencialmente. Segundo Ascold, um levantamento apontou que, apenas no primeiro trimestre deste ano, mais de 600 tipos de malwares para sistemas operacionais móveis. "Todos são considerados alvos; não existe um sistema operacional imune a ataques", diz.

Chris Kenworthy, da McAfee, explica que, além dos malwares tradicionais, como vírus, trojans e worms adaptados para dispositivos móveis, há outras áreas de risco na mobilidade corporativa, como os aplicativos. "Nos velhos tempos dos desktops, 95% do que fazíamos se restringia ao e-mail, web e editores de texto e planilhas. Nas lojas online são milhares de novos aplicativos móveis disponíveis todos os dias. Será que pensaram na segurança?"

Websites maliciosos também representam risco. Segundo Kenworthy, os usuários de dispositivos móveis são três vezes mais suscetíveis a fraudes bancárias na web, pois

"É importante uma reeducação digital por parte do consumidor"
Ascold Szymanskyj, da F-Secure

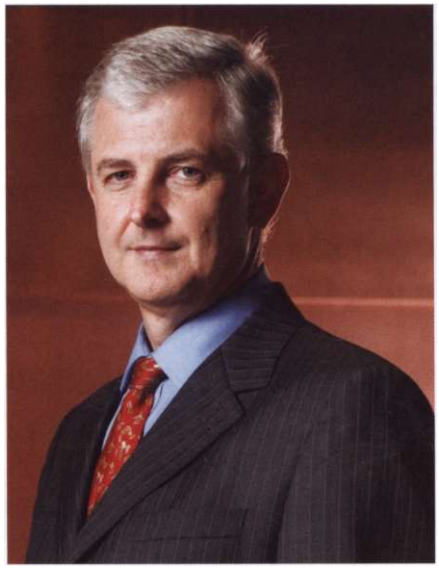
FOTOS DIVULGAÇÃO

não conseguem identificar com clareza se estão em um site autêntico em uma tela tão pequena. "O que os hackers fazem é seguir o dinheiro. Quanto mais transações financeiras são feitas em smartphones, mais os hackers vão tentar encontrar um meio de explorar isso. Hoje eles faturam muito mais através dos PCs, mas isso vai mudar."

SOLUÇÕES

As soluções oferecidas pelas empresas se destinam tanto ao consumidor final quanto às empresas. A McAfee, por exemplo, já conta com uma unidade específica apenas para desenvolvimento e pesquisa em segurança móvel. Outras fornecedoras, como a Fortinet, apresentam alternativas específicas para dispositivos (como apps de varredura) e também para redes móveis corporativas.

O controle parental, que identifica sites potencialmente perigosos antes que sejam



"A mobilidade está entrando nas empresas mais rápido do que elas são capazes de se adaptar"
Chris Kenworthy, da McAfee

acessados, também é uma constante no portfólio das empresas, bem como soluções de rastreamento de dispositivos roubados ou perdidos. "Se perder um device já é ruim, perder os dados nele contidos pode ser pior ainda", diz Kenworthy, da McAfee, que oferece uma solução que permite apagar remotamente os dados contidos em um aparelho.

Ascold Szymanskyj, da F-Secure, acredita que, além do esforço da indústria no desenvolvimento de soluções eficientes, é necessária "uma reeducação digital por parte do consumidor. Há muita informação do usuário flutuando na nuvem sem muitos critérios de segurança." Segundo ele, é fundamental possuir um software de segurança associado ao dispositivo e mantê-lo sempre atualizado. A proteção ideal, diz, combina solução de antivírus com backup dos dados.

Outras precauções também são importantes, enumera Vanessa Pádua, da Fortinet: evitar abrir e-mails, mensagens SMS e links desconhecidos nas redes sociais; verificar pontuações e quantidade de downloads durante a instalação de um novo aplicativo; desconfiar de aplicativos gratuitos que solicitam informações pessoais; manter o dispositivo sempre ao alcance.

Precauções

- EVITAR ABRIR EMAILS, MENSAGENS SMS E LINKS DESCONHECIDOS NAS REDES SOCIAIS
- VERIFICAR PONTUAÇÕES E QUANTIDADE DE DOWNLOADS DURANTE A INSTALAÇÃO DE UM NOVO APLICATIVO
- DESCONFIAR DE APLICATIVOS GRATUITOS QUE SOLICITAM INFORMAÇÕES PESSOAIS
- MANTER O DISPOSITIVO SEMPRE AO ALCANCE

Fonte: Fortinet

Fonte: Teletime, São Paulo, ano 14, n. 148, p. 10-11, out 2011.