Consumerização de TI traz novos desafios para empresas

O crescente uso de dispositivos móveis, como smartphones e tablets, e de redes sociais no ambiente corporativo vem fazendo com que as empresas se tornem cada vez mais expostas a ameaças e ao risco de vazamento de dados, o que vem aumentando a pressão sobre os gestores de TI. E o cenário futuro não é nada tranquilizador. "É um novo vetor. Uma nova dificuldade para as empresas enfrentarem, em razão principalmente da expansão do uso de dispositivos móveis e de redes sociais", observa José Roberto de Oliveira Antunes, gerente de engenharia de sistemas da McAfee no Brasil. "As empresas estão cada vez mais submetidas aos riscos trazidos pelas novas tecnologias, por isso devem se preocupar em promover as melhores práticas de segurança da informação", alerta André Carraretto, diretor de engenharia de sistemas da Symantec Brasil.

Nos últimos anos, de acordo com empresas de segurança na web, os ataques têm tido como alvo preferencial os usuários do Facebook e do Twitter, e de aparelhos móveis que utilizam o sistema operacional Android, do Google, e o iPhone, da Apple. Uma pesquisa recente divulgada pela fabricante de software de segurança McAfee aponta que o número de malware para smartphones cresceu 46%, na comparação de 2009 com o ano passado. Outro estudo, este da Kaspersky Lab, revela que os ataques de programas maliciosos direcionados a usuários de plataformas móveis saltou 65% no período, com cerca de mil variantes de 153 diferentes famílias de ameaças.

Diante desse quadro, especialistas em segurança da informação dizem que o desafio que se impõe hoje às empresas é como lidar com o fenômeno que ficou conhecido como consumerização da TI, a pressão dos funcionários para utilizar novas tecnologias no trabalho. Um estudo inédito conduzido pela Intel e pela Maritz Research investigou o impacto da consumerização nos departamentos de TI e no comportamento dos funcionários. Dividida em três etapas, a pesquisa acompanhou o dia-a-dia de funcionários e departamentos de TI para entender quão graves são os conflitos gerados pelo fenômeno e que efeitos eles geram na produtividade da empresa.

O levantamento revelou um cenário bastante complexo para o gestor de TI. O obstáculo mais mencionado por eles foi a questão da segurança: expandir as opções em termos de dispositivos, serviços ou software pode abrir novas brechas na segurança de todo o sistema da companhia. Para piorar a situação, há um consenso entre os CIOs de que os maiores riscos vêm dos próprios usuários, que acabam criando vulnerabilidades de segurança com o uso de smartphones e de redes sociais no ambiente de trabalho. Isso acontece também porque esses sites e dispositivos são a forma mais fácil de se chegar à empresa, observa o presidente da Fortinet para o Brasil e América Latina, Pedro Paixão. Ele

alerta que, ao usarem redes sociais no trabalho, os funcionários muitas vezes podem revelar informações confidenciais, sem nem mesmo saber que são valiosas. "Essa democratização gera um problema maior para as empresas controlarem a segurança, pois facilita os ataques e a propagação de malware", diz Paixão.

O diretor de engenharia de sistemas da Symantec Brasil, André Carraretto, diz que as redes sociais representam duas vertentes de perigos principais. Uma delas diz respeito ao fato de muitas empresas já estarem utilizando as redes sociais como ferramenta de marketing ou para se relacionarem com os clientes, o que potencializa o risco de vazamento de informações confidenciais. A outra vertente refere-se justamente aos dispositivos móveis, já que os usuários, que acessam a rede corporativa com seus dispositivos, podem receber algum código malicioso no aparelho por meio do site de relacionamento e com isso propagá-lo por toda a empresa. "O dispositivo móvel muitas vezes é do funcionário e não dá empresa, e ele usa como quiser. Muitas vezes, ao conectar-se à rede da empresa, ele traz um risco muito grande", diz Antunes. Para minimizar esse problema, ele diz que as empresas devem investir na compra de soluções de mobilidade para repassá-las aos funcionários, mas já com ferramentas de segurança integradas para prevenir possíveis ataques. "As empresas já estão olhando a mobilidade e têm montado estruturas para municiar os funcionários com dispositivos móveis já equipados com soluções de segurança. Mas isso ainda é muito incipiente e tem ocorrido apenas para os funcionários de cargos mais altos", enfatiza.

Os especialistas em segurança salientam que é crucial para as empresas educarem os funcionários sobre o uso de dispositivos móveis e redes sociais no ambiente corporativo. "O importante é a educação do usuário e estabelecer políticas de segurança", ressalta Paixão. "As empresas não podem barrar o uso de dispositivos móveis e redes sociais, por isso precisam criar políticas de uso para impedir o vazamento de informações confidenciais. Essa questão de cultura é essencial. Por mais tecnologia que você coloque você sempre tem que ter uma atenção especial com a questão da educação", finaliza Antunes.

Fonte: TI Inside, por Victor Hugo Cardoso Alves