Celulares são ameaça às corporações
Fernanda K. Angelo

Funcionalidades como câmera digital, gravador de voz, vídeo, acesso à internet e mensagem de texto fazem dos telefones celulares verdadeiras ferramentas de espionagem. Pelo menos é o pensa Andrew Sheldon, consultor de perícia forense da britânica Evidence Talks, especializada em segurança da informação.

Em entrevista ao Computerworld, Sheldon diz que tudo o que alguém mal-intencionado precisa para roubar dados críticos para uma empresa é um smart phone. "As corporações normalmente não monitoram o uso desses aparelhos em suas dependências, mas eles equivalem a ferramentas de espionagem. É possível fotografar documentos ou gravar conversas confidenciais com um telefone", alerta o especialista. "O mesmo vale para os handhelds e PDAs."

A adoção de políticas de uso dos aparelhos portáteis, incluindo a auditoria de equipamentos, é o primeiro passo em direção à segurança dos dados corporativos. Outra dica para os responsáveis por TI é que eles identifiquem os locais onde, de fato, está o risco para os dados da empresa. "Uma vez identificadas essas áreas de risco, os profissionais devem adotar medidas para bloquear a conectividade de telefones celulares", sugere Sheldon. Ele lembra, porém, que bloquear a conectividade não impede usuários de tirarem fotos ou fazerem gravações. Neste caso, a sugestão é mais drástica: "Os equipamentos devem ser impedidos de entrar nas áreas de risco".

Sheldon enumera os pecados capitais do departamento de TI em relação à segurança dos dados críticos para uma empresa:
- desconhecimento de um equipamento no ambiente corporativo;
- falta de controle sobre os equipamentos portáteis pessoais;
- desconhecimento daquilo que constitui risco para os dados da empresa;
- ausência de políticas de uso dos dispositivos móveis;
- ausência de sistemas de detecção e prevenção de acesso a redes por equipamentos móveis;
- inabilidade para auditar os dados e aplicativos armazenados em equipamentos corporativos, e
- ignorar a existência de celulares e PDAs.

Afinal, se você não pode vê-los, como vai gerenciá-los?

Computerworld online - acesso em 10/6/2005