Especialistas comentam sobre políticas e procedimentos de segurança para dispositivos de uso corporativo e pessoal

O Brasil está em 5° lugar no ranking global de tempo dispendido no celular. Os brasileiros passaram mais de três horas por dia usando o dispositivo móvel em 2018, de acordo com o relatório Estado de Serviços Móveis (da App Annie) divulgado no início deste ano. A tendência apontada pelo relatório revela o quão dependente estamos dos celulares, da internet e da tecnologia de modo geral, mas também evidenciam uma maior exposição aos riscos relacionados a crimes cibernético.

Não são raros os fatos que viram notícias na imprensa nacional e internacional sobre invasões de hackers contas de e-mails, redes sociais e aplicativos. Quando o crime envolve uma figura pública ou uma grande corporação, por exemplo, uma das consequências graves é o vazamento de conteúdo com informações sensíveis e sigilosas.

Para o especialista em investigações e riscos André Almeida, sócio da consultoria GRC Solutions, é possível minimizar esses riscos, mas é preciso, sobretudo, conhecer o perigo. “As estatísticas internacionais sobre crimes cibernéticos apontam que, em média, 2% dos norte-americanos acreditam que nunca serão vítimas de invasão por cibercriminosos”, aponta Almeida referindo-se às análises feitas pela Cyber Crime Watch no ano passado.

O percentual, na opinião de Almeida, deve ser mais expressivo no Brasil pois o país é o segundo no mundo com o maior número de crimes cibernéticos, ficando atrás apenas da China, de acordo com estudo do Norton Cyber Security Insights Report publicado pela Symantec em 2018. “Ainda há uma despreocupação de boa parte das pessoas com as informações e dados que trafegam diariamente nos dispositivos conectados à internet”, afirma o especialista.

Segundo André Almeida a situação fica mais delicada quando se trata de dispositivos pessoais utilizados como ferramentas de trabalho e vice-versa. De acordo com ele, nos dispositivos pessoais os riscos de uma invasão criminosa se agravam porque o usuário pode baixar aplicativos que contenham códigos não confiáveis ao mesmo tempo em que trata dados e informações corporativas confidenciais.

“A prática de usar dispositivos pessoais como ferramenta de trabalho é uma tendência e pode ser positiva, sem dúvida. Mas é preciso cautela e um intenso trabalho voltado à cibersegurança pois há um risco imensurável para a empresa. Uma invasão criminosa pode custar caro não apenas para a imagem da organização, mas também gerar grandes perdas financeiras”, adverte Almeida.

Do outro lado também há um risco a se considerar, na opinião de André Almeida: “Utilizar para fins pessoais os dispositivos disponibilizados pela empresa para atividades corporativas pode gerar uma exposição indesejada ao usuário. É extremamente importante que haja conhecimento sobre como se dá essa exposição para que o usuário esteja consciente e possa avaliar quando e como utilizar cada ferramenta disponível da forma mais segura possível”.

Políticas e procedimentos para proteção

Para minimizar esses riscos, o gerente da área de IT Services da GRC Solutions, aponta que é de suma importância a implementação de políticas e ferramentas direcionadas à BYOD (Bring Your Own Device) nas organizações. “A utilização de dispositivos pessoais para atividades relacionadas ao trabalho é uma realidade irreversível nas organizações. Primeiro pela preferência dos usuários pelos dispositivos móveis e, segundo, pelo claro aumento da produtividade na utilização desses dispositivos”, explicou Souza.

Além disso, o gerente aponta para a possibilidade de redução dos custos com compras de ativos – como computadores e celulares – e o direcionamento dos investimentos da área de tecnologia para

políticas, processos e ferramentas relacionadas à área de segurança de informações.

Na opinião de Souza as empresas precisam estar prontas para atender às demandas de compartilhamento de dados e acessos à rede corporativa de forma remota. “Para isso, é imprescindível à utilização de ferramentas voltadas ao gerenciamento e segurança de dispositivos móveis. Essas ferramentas são conhecidas no mercado tecnológico como Mobile Device Management (MDM) e visam garantir, por exemplo, a segregação total dos dados corporativos daquilo que é informação pessoal”, esclarece.

Souza destaca ainda que, além dos recursos de prevenção disponibilizados pelas empresas, é importante que os usuários também se preocupem com a segurança das informações pessoais utilizando ferramentas de proteção, a exemplo dos antivirus e anti-malware.

Fonte: **GRC Solutions**, em 12.06.2019.