98 – Abril de 2008

Roubaram o notebook do funcionário, e agora?

Você não é o primeiro nem será o último a ter esse tipo de problema com algum membro da sua equipe. Cada vez mais comum, o roubo de equipamentos de computação móvel têm se tornado uma constante na rotina das empresas, sejam elas Brasileiras ou estrangeiras. A razão é relativamente simples.
Considere o barateamento dos notebooks, associe isso ao aumento dos níveis de conectividade das empresas, adicione a globalização e o interesse no barateamento dos custos através do tele-trabalho e por fim, tempere com a profissionalização do mercado negro de equipamentos e informações roubadas. Temos aí uma bomba relógio fazendo tictac na mão dos funcionários e pronta para explodir a qualquer momento.

Entretanto, diante da constatação do roubo, o melhor a fazer é reagir rápido para evitar a ampliação do estrago e principalmente, extrair ensinamentos do fato e aprimorar os controles e as medidas de segurança para evitar um próximo evento ou simplesmente, reduzir sua probabilidade de ocorrência.

Passado o susto dos primeiros 10 minutos, enxugue o choro e acione o plano de recuperação de desastres proposto a seguir:

- Procure imediatamente a polícia e faça o registro da ocorrência para que obtenha a evidência do roubo.
- Descreva as particularidades do equipamento à polícia, assim como da pasta em que o transportava e da situação em que o roubo ocorreu de forma a permitir a recuperação do equipamento nas primeiras horas, já que ainda deve estar fisicamente distante.
- Faça um registro do incidente. Comunique imediatamente o roubo ao departamento de segurança e ativos da sua empresa, de preferência acompanhado dos dados de identificação do usuário e de inventário para que possam conhecer o perfil do usuário e dos dados que transportava.
- Comunique imediatamente o roubo ao departamento de inteligência competitiva ou gestão do conhecimento da sua empresa, reportando sua avaliação sobre o valor das informações (classificação) recentemente manuseadas e armazenadas de forma a avaliarem o potencial impacto ao negócio.
- Informe ao mesmo departamento a melhor forma de ser contatado nas próximas 24 horas e fique disponível para que possa fornecer maiores detalhes sobre os dados transportados, pois só assim poderão medir a extensão dos danos e acionar possíveis planos de comunicação e administração de crises, especialmente se estivermos falando de dados sensíveis que possam afetar a empresa e suas relações com parceiros, clientes e investidores.
- Considerando a existência de um processo eficiente e integrado de gestão de incidentes, você será contatado pela área de suporte a fim de substituir o equipamento roubado e

restabelecer seu acesso às aplicações e dados providencialmente restaurados do último backup.

Se os ventos estiverem soprando a seu favor e sua empresa tiver feito o "dever de casa", o equipamento estará em conformidade com o nível de segurança básico, o backup estará atualizado e disponível; os dados do notebook estarão protegidos por criptografia forte; você só estaria transportando o mínimo necessário de informação corporativa; o equipamento contaria com softwares ou hardwares de rastreamento que permitirão sua localização física ou lógica e até a deleção de dados sensíveis remotamente se conectado a qualquer rede de dados, e por fim, tudo não terá passado de um susto de pouco mais de uma centena de dólares, sem sequer arranhar a imagem da sua empresa.

De qualquer forma, prevenir é sempre melhor do que remediar, além de ser mais barato. Por isso, se o fato descrito aconteceu com a sua empresa, aprenda com ele e aprimore. Mas se felizmente ainda não aconteceu, aproveite para aprender com este exercício também e se antecipe ao fato de que um dia, certamente irá ocorrer.

Marcos Sêmola *é Global IT GRA Compliance Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br*

Nota: Este artigo expressa exclusivamente a opinião pessoal do autor, não representando necessariamente a opinião da empresa citada.