27 – Dezembro de 2000

Proteger seu Notebook também é proteger o seu negócio.

Aproximadamente 150 equipamentos portáteis foram roubados e furtados nos Estados Unidos em 1999. No Brasil, apesar de não haver qualquer indicador oficial para esse tipo de incidente, sabemos – ao ler os noticiários – que esta prática tem sido freqüente.

Há pouco mais de três meses, foi descoberta uma quadrilha que "operava" em aeroportos furtandoas pastas dos executivos que distraidamente faziam o checkin. Em frações de segundos o que parecia ser uma viagem de rotina para mais uma reunião, tornava-se uma catástrofe! Além de documentos pessoais, celular e o jornal do dia, fora perdido também o notável portátil. O notebook que além do valor financeiro , transportava arquivos corporativos sigilosos, únicos, fundamentais para a realização da reunião e igualmente importantes para a empresa.

Graças ao amadorismo dos criminosos brasileiros, muitas das investidas desse tipo AINDA têm como foco principal a comercialização do equipamento e não de seu conteúdo, o que acaba reduzindo o potencial impacto que os executivos e seus negócios poderiam sofrer.

É evidente que a portabilidade proporcionada por estas maquininhas é fantástica! Passamos a transportar o escritório em uma - nem sempre leve – pasta, nos permitindo interagir remotamente com a empresa, gerar documentos em trânsito, antecipar correspondências e decisões.

Diante das particularidades inerentes ao transporte de notebooks e informações corporativas, nos cabe identificar as vulnerabilidades, analisar os riscos e identificar os impactos proporcionados por um eventual acidente.

Partindo da premissa de que cada negócio, perímetro ou processo tem sua particularidade, ou seja, tem tolerância variável associada à quebra de confidencialidade, integridade e disponibilidade, torna-se necessário identificar com detalhes as informações que você transporta e as ameaças que estão à sua volta.

Depois de analisar suas particularidades, é preciso definir o nível de segurança adequado e implementar controles que farão com que os riscos tendam à zero, encorajando-o então a continuar transportando seu notebook e informações corporativas.

Cheque agora as dicas abaixo associadas à esse tipo de transporte e veja se você está mesmo reduzindo os riscos ou é mais uma vítima em potencial:

- Habilite a senha do setup (BIOS) do notebook;
- Adote uma senha forte que tenha mais de 6 posições e seja formada por letras em maiúsculo, minúsculo, números e caracteres especiais;
- Adote um sistema operacional que dê suporte à dispositivos de autenticação forte, ou instale um programa específico para tal. Dependendo de seu grau de risco e impacto,

opte pela associação de uma senha com um mecanismo de autenticação como: SmartCart ou Leitora de Impressão Digital (Biometria);

- Adote um programa de segurança que seja capaz de controlar o acesso aos recursos do computador, impedindo sua inicialização (boot) através do drive de disquete e CdROM, a inicialização do Windows em modo de segurança e ainda evitando o acesso aos arquivos do Hard Disk (HD) através do DOS ou outro sistema operacional;
- Adote um programa de criptografia e o aplique nos arquivos mais importantes e valiosos. Não deixe de utilizar uma senha forte e à altura do valor da informação que está protegendo;
- Esqueça a pasta fornecida pelo fabricante do notebook ou uma daquelas já conhecidas pastas pretas com quinas emborrachadas e alça comprida. Agindo assim, você estará revelando seu conteúdo e atraindo os interessados. Se não for mesmo possível abrir mão, fixe uma etiqueta grande colorida e não removível, personalizando-a;
- Dependendo do seu grau de risco e impacto, abra mão até mesmo do pin de sua empresa (broche com a logomarca) que geralmente o acompanha espetado ao paletó. Usando-o em conjunto com a pasta padrão Notebook, você além de estar comunicando à todos que transporta o computador, também está revelando a origem das informações que estão dentro dele;
- Habitue-se a adotar dispositivos de proteção física na pasta, como um cadeado. Assim você estará evitando um furto rápido quando o equipamento é substituído, num momento de descuido, por outro objeto de peso semelhante;
- Se estiver pensando em se hospedar, deixando o notebook no quarto do hotel, ou se precisar se afastar do notebook no meio de uma reunião, palestra ou congresso, não deixe de adotar dispositivos de proteção física para o próprio equipamento. Comumente um cabo de aço com recursos de alarme que pode ser fixado ao equipamento e depois preso à algum objeto grande e pesado como uma mesa;
- Atualize regularmente seu antivírus. Os principais fabricantes disponibilizam atualizações semanalmente;
-
- Estude a possibilidade de segurar o equipamento e até mesmo as informações transportadas por ele. As seguradoras já possuem produtos com este perfil com o prêmio orientado por uma Análise de Riscos.

Pode parecer exagerado, mas lembre-se que todas essas dicas e controles estão focados na proteção do bem mais valioso das empresas, a informação. Depois de analisar as características específicas do seu negócio e o seu relacionamento com a informação, você deve identificar o nível de segurança mais adequado, implementando então controles que reduzam os riscos fazendo-o tender à zero.

Lembre-se que protegendo seu notebook e as informações nele armazenadas, você está contribuindo com a proteção do seu negócio.

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente de Produto e Analista de Segurança da Módulo Security Solutions S.A.*

msemola@modulo.com.br