59 – Julho de 2004

Criptografia, Biometria, Backup e Sono

Essa cena lhe parece comum? Diariamente você enfrenta as filas nos aeroportos levando seus *gadgets* inseparáveis. O celular no bolso do paletó pronto para receber uma ligação, uma mensagem ou um email. O PDA ou computador de bolso permanece obviamente, no outro bolso enquanto ainda não se integrou ao celular, e se mantém lá, acessível para que a qualquer momento você possa tomar nota de um compromisso que acabara de firmar, consultar sua agenda e evitar um conflito, ou ainda para checar sua planilha de projeto ou planilha financeira antes de responder a uma importante pergunta do CFO que está ao telefone.
Enquanto uma de suas mãos manipula, ora o celular, ora o PDA, a outra transporta sua tradicional pasta. Comumente uma pasta à altura do perfil executivo com divisórias para hospedar documentos, para guardar por períodos mais longos o PDA, para transportar seu *pen drive* de 256Mb, seu mais novo "brinquedinho", e naturalmente, para acomodar o todo poderoso *notebook*. Este com todos os recursos que se pode imaginar e aparentemente camuflado em um repositório que difere da habitual pasta preta com alças e logomarca do fabricante.

Por se tratar de um profissional atualizado e consciente dos aspectos de segurança, você está sempre atendo ao movimento periférico. Coloca rapidamente seu celular e pasta na esteira do aeroporto para evitar o sinal sonoro do detector de metais e logo os recupera para então esperar seu vôo no saguão. O celular toca cerca de 3 vezes por minuto, como de costume. O PDA se faz necessário por pelo menos 6 vezes enquanto checa a agenda do dia, relembra o endereço do seu primeiro destino e faz algumas anotações. A pressão imposta pelo atual mercado de trabalho o faz pensar em sacar o notebook e aproveitar a janela de tempo de 8 minutos para responder aqueles quase 40 emails que ficaram sem resposta no dia anterior, mas felizmente o embarque se inicia.

O dia parece agitado como de costume, mas ao chegar no aeroporto destino e pegar um táxi que possa te levar ao destino, você é surpreendido por uma situação que nunca imaginou que pudesse ocorrer, um assalto. Parece uma operação de guerra. Dois motoqueiros se aproveitam de um engarrafamento e empunhando belas armas batem no vidro e pedem seus pertences. Primeiro o celular que já estava à mão. Em seguida o PDA que já estava no colo no meio de uma anotação e por fim, o mais precioso, a pasta. E com ela o *notebook*, o *pendrive* e tudo mais que comumente acompanhar uma pasta executiva.

O exercício involuntário do cérebro nos faz recordar a cena em *replays* contínuos e desordenados, como se estivesse em *loop*, mas logo vem a razão e com ela a sensação de perda, passividade, risco e os exercícios de quantificação do prejuízo. Primeiro os bens materiais, o custo da reposição dos equipamentos e em seguida a perda de tempo para recompor tudo como era, seja na digitação dos números de telefone do celular, seja na configuração do PDA. Mas o pior vem agora com a sensação de quebra de privacidade. Esse sentimento invasivo pode ser horrível dependendo do seu grau de compromisso com

as melhores práticas de segurança da informação. Se seu celular não tem código de acesso ao chip ou se o código permaneceu o mesmo definido pelo fabricante, se seu PDA não dispõe de recursos de criptografia e biometria para autenticação, ou ainda, se seu *notebook* não está amparado por recursos inteligentes de criptografia de dados, você tem problemas. Essa estória que parece descrever mais uma cena metropolitana de violência, se transforma agora em um filme de terror à medida que o perímetro do impacto se amplia. Agora seus dados pessoais e principalmente profissionais estão em mãos desconhecidas. As informações valiosas da empresa que transitavam desprotegidas no seu *notebook* agora não estão mais em seu poder, talvez nem possam ser recuperadas por falta de backup e ainda podem estar em mãos erradas, podendo ser usadas contra você, seja comprometendo uma oportunidade de negócio, seja revelando segredos que implicam na continuidade operacional da sua empresa, seja em uma potencial exposição e descrédito da marca.

Em contra-partida, essa situação desesperadora poderia ser muito diferente se medidas preventivas tivessem sido aplicadas. A simples troca da senha de bloqueio do smartcard celular, a adoção de um mecanismo de autenticação para o PDA, o uso de criptografia inteligente no *notebook* e a prática sistemática de um procedimento de backup poderiam transformar essa manhã desastrosa em um fim de semana descontraído, apesar de caro, à procura de seus novos *gadgets* pelo shopping.

Assim, conhecendo tantos conceitos de segurança da informação, tantos métodos de gestão de riscos, convivendo com tantas tecnologias, ferramentas e processos que envolvem pessoas e máquinas, em situações como esta uma única combinação poderia fazer a vítima relaxar e dormir um sono profundo: criptografia, biometria e backup. Pratique essa idéia!

Marcos Sêmola *é Security Consulting Manager da multinacional Atos Origin, Consultor Sênior em Gestão de Segurança da Informação, CISM – Certified Information Security Manager, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus e eleito pelo prêmio SecMaster, Profissional de Segurança da Informação de 2003.*
marcos@semola.com.br