69 - Outubro de 2005

A segurança será comprometida, é uma questão de tempo.

Este é mais um dos comentários da série que explica e procura ilustrar cada uma das afirmativas do artigo “O que eu não gostaria, mas preciso dizer sobre segurança”.

> *“A quebra de confidencialidade, integridade ou disponibilidade das informações é certa. O que especialmente difere uma empresa de outra, é a forma como estão preparadas para reagir e administrar a situação. “*

É quase uma afirmação matemática, pois se existem falhas e ameaças, portanto risco, o impacto resultante da exploração da primeira pela segunda é certo e está exclusivamente dependente do tempo. Probabilisticamente em algum momento a segurança será quebrada, de uma forma ou de outra, e a eficácia do seu processo de gestão de riscos diante da necessidade de responder ao incidente é que vai determinar sua qualidade.

Muitas empresas, que aos olhos do mercado e do seu cliente estão sólidas, ‘protegidas’ e imunes aos ataques a informação, estão na verdade sendo competentes. Não em se cercar de todos os mecanismos de forma a eliminar o risco, mas competentes por estarem administrando tão bem os problemas diários com a segurança que sequer seus clientes percebem a ocorrência deles. É simples assim.

Tomando emprestado novamente o modelo automobilístico para clarear as idéias, podemos analogamente comparar uma corrida de velocidade como a Fórmula 1 com o problema descrito. Os automóveis que participam de uma corrida como esta, em que todos os seus componentes são exigidos ao extremo, só têm uma expectativa: quebrar. Quebrar é o fator mais previsível. Óbvio, não falo das quebras fatais em que o carro sequer chega aos boxes, mas das pequenas quebras que podem tirar tempo precioso do piloto e podem ser administradas nas paradas.

A natureza da atividade já pré-supõe a existência de potenciais problemas no percurso, o mesmo que ocorre com a empresa que resolve usar o ambiente de rede pública da Internet para suportar seu modelo de comércio eletrônico. A diferença e a competência de ambos será medida pela forma com que irão responder aos incidentes, como irão reparar o aerofólio rachado sem interromper a prova ou o link de rede sobrecarregado por um novo vírus de computador sem interromper as vendas no portal web.

Para cumprir essa tarefa com eficácia é muito importante experimentar situações, construir cenários, simular ações e reações para que os problemas, quando aparecerem, sejam conhecidos ou tenham sido previamente estudados para que agora só seja preciso seguir os passos da mitigação ou recuperação.

O exercício de previsibilidade é fundamental, mas não só o exercício técnico em que problemas e possíveis soluções são estudadas, mas também exercícios táticos e estratégicos.
É igualmente importante saber se o carro deve continuar na corrida ou não caso não seja possível reparar uma peça, pois pode ser arriscado demais para o negócio tomar esta decisão ou simplesmente pode ser estrategicamente importante deixá-lo seguir adiante.

Sendo prático, a análise poderia seguir esta linha de raciocínio: a peca pode ser substituída ou reparada à tempo? Se sim: troque ou repare a peça. Se não: a peça quebrada coloca a vida do piloto em risco? Se sim: interrompa a corrida. Se não: o carro pode ser totalmente comprometido? Se sim: qual o valor do carro? Existe tolerância financeira capaz de aceitar a perda do carro? Se não: vale à pena correr o risco de perder todo o carro para o piloto dar sua última volta e assim ganhar o campeonato, gerando lucro suficiente para a aquisição de 3 novos carros? Se não: interrompa a prova. Se sim: vá em frente e boa sorte.

Todo esse processo pode parecer demais para algumas empresas, mas na verdade seu método se aplica a qualquer empresa, qualquer atividade, qualquer modelo de negócio e até mesmo pode ser aplicado ao usuário doméstico de computador. Pense no seu computador, um *notebook*, por exemplo, como uma importante ferramenta usada para pagar contas via Internet, fazer trabalhos do mestrado, armazenar fotografias de família e para produzir seu primeiro romance. Agora pense na possível perda do seu disco rígido, onde tudo está gravado e transmitindo a você uma falsa sensação de segurança de que tudo está seguro e acessível a qualquer hora.

Pois sem consultar os astros ou os búzios é possível afirmar que um dia você perderá seus documentos armazenados neste disco. Verdade. Seja por um defeito de máquina, seja por uma queda, um raio, um curto-circuito, um grande copo de refrigerante derramado sobre o teclado, um furto, a ação devastadora de um vírus ou pelo simples descuido do usuário ao apagar inconscientemente seu conteúdo, você o perderá. Neste momento, a forma como você exercitou a previsibilidade determinará o resultado. A peca pode ser substituída ou reparada? Não: existe alguma alternativa para recuperar seu conteúdo? Se sim: restaure o backup, parabéns! Se não: esteja mais preparado da próxima vez, comece o retrabalho.

Marcos Sêmola *é Consulting Business Development da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC e do Computer Security Institute, Professor da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003/2004. Visite www.semola.com.br ou contate marcos@semola.com.br*