83 – Janeiro 2007

Top 10 - Tendências do mercado Brasileiro de segurança em 2007

Previsão. Nada mais do que o exercício de antecipar tendências baseado no acompanhamento dos mercados, na experiência profissional e no feeling pessoal. Certo ou errado, acredito ser um exercício saudável e representa a verdadeira fronteira entre a ousadia e a irresponsabilidade que só o tempo irá definir. Vamos ao resultado:

1. As empresas estão mais maduras e querem algo mais do que soluções técnicas de retorno imediato. Este comportamento refletirá no estabelecimento de processos mais bem definidos e a adoção de ferramentas de gestão de riscos da informação e conformidade para suportar decisões executivas e atividades internas e externas de auditoria.

2. Motivadas pelos altos custos do suporte, das implicações legais e fraudes ligadas ao roubo de identidade e ao acesso indevido, as empresas intensificarão os investimentos em sistemas de gerenciamento de identidade e na adoção integrada de tecnologias de biometria, certificação digital e criptografia/smartcard/RFID e outros dispositivos inteligentes. Desta forma, irão fortalecer as interfaces de autenticação, definindo de maneira mais eficaz e restrita os perfis de acesso, o que desencadeará projetos de implementação de mais de um fator de autenticação.

3. Altos níveis de acessibilidade, mobilidade e trabalho remoto elevam as preocupações com o perímetro do usuário. Assim, se espera investimentos ainda mais abrangentes e contínuos em processos corporativos de conscientização, gerenciamento de mudanças e treinamento dos usuários da cadeia produtiva. Tudo para torná-lo um aliado e reduzir riscos por falha, negligência ou despreparo maximizados pela crescente onda das técnicas de engenharia sócia e phishing que tomou a Internet nos últimos 12 meses.

4. A alta conectividade pressiona as empresas a fortalecer os investimentos em sistemas de controle e filtragem de conteúdo, SPAM e softwares maliciosos em geral, a fim de reduzir os custos de rede, gerenciamento de sistemas corporativos, baixa de produtividade e o potencial vazamento de informação e contaminação por virus. Soluções que integrem essas funcionalidades e ofereçam uma visão analítica que suporte ações pró-ativas serão demandadas.

5. A percepção de continuidade deixa de ser exclusividade dos ambientes industriais e extremamente críticos e a estratégia de continuidade torna-se um componente de praticamente qualquer negócio. A figura do especialista em continuidade tende a ser formalizada no organograma de empresas de setores sensíveis, ou a figura do conselheiro externo nos demais setores da economia. Ambos com o foco em criar e manter planos e alternativas viáveis de mitigação de impactos através do gerenciamento de crises, recuperação de desastres e continuidade operacional. O assunto deixa de ser

tratado como uma pasta no arquivo e passa a requerer manutenção e tratamento como um processo contínuo.

6. Depois de lições aprendidas, empresas dos principais setores da economia amadurecem a percepção do valor agregado pela função de seguranca. O reflexo será a oxigenação do cargo com a renovação dos CISOs - Chief Information Security Officers muito técnicos, ligados exclusivamente a TI e focados na infra-estrutura, por experientes profissionais que possuam uma visão integrada da técnica e do negocio, bom relacionamento com parceiros, fornecedores e clientes. Esta nova geração de gestores será ainda mais capaz de contribuir diretamente com a definição estratégia do negocio através da visão do componente de risco vinculado aos planos de negocio de curto, médio e longo prazo. A velha tendência conservadora e econômica, à primeira vista, de promover antigos funcionários de TI e infra-estrutura ao cargo de CISO, por exemplo, dá lugar a contratação de gestores especialistas de mercado que possam ocupar esta nova função executiva.

7. Terceirizar parte da estrutura de gerenciamento de riscos ainda é tendência. Com isso, serviços que não requeiram conhecimento profundo do negócio serão adquiridos de parceiros. Isso tende a acontecer com o processo de monitoramento e gerenciamento de dispositivos de segurança com o objetivo de identificar ataques, combater fraudes e situações de risco pró-ativamente. As empresas deverão criar internamente pequenos núcleos de comando com apoio operacional terceirizado, que definirá novos processos de investigação e gerenciamento de fraudes e ataques, para identificar agentes, origens, a extensão de impactos e ainda para preservar as evidencias ou provas, necessárias ao suporte de auditorias e requerimentos legais.

8. Os aspectos de proteção dos ativos da informação se infiltram em praticamente toda a estrutura corporativa, com isso, tende a ser notada maior cooperação e integração de ações entre as áreas técnica, jurídica e de recursos humanos. O primeiro reflexo tende a ser o desenvolvimento de programas de conscientização dos usuários que misturem aspectos legais, técnicos e éticos que envolvem a relação de trabalho empregado-empregador. A análise dos aspectos de risco da informação em contratos, projetos e na manipulação de documentos deixa de ser uma iniciativa isolada e passa a fazer parte de um processo formal.

9. Tendência de aumento significativo do controle sobre os computadores e dispositivos móveis que se conectam a rede corporativa. As soluções deverão restringir a mobilidade do usuário ao mudar configurações, instalar programas e fazer acessos híbridos de forma a “blindar” o perímetro do equipamento ou, ao menos, reduzir as ameaças que chegam ao usuário e ficam em suas mãos a decisão de assumir ou não o risco.

10. Aumento significativo da importância e da demanda por profissionais técnicos e executivos de segurança da informação, especialmente aqueles que detenham conhecimento multidisciplinar, larga experiência prática e teórica chancelada por certificações de reconhecimento internacional. Tudo aponta para um crescimento da ordem de 35% do mercado de segurança da informação no Brasil, o que induz a uma procura natural por mão-de-obra capacitada. Associada ao aumento de maturidade das

empresas em relação ao gerenciamento de riscos, esta demanda tende a ser mais qualitativa e irá beneficiar especialmente aqueles com uma visão mais apurada da ligação tecnologia-negócio.

De acordo com a obra A Arte da Guerra, do general filósofo Sun Tzu, para atingir uma meta é preciso agir em conjunto, conhecer o ambiente de ação, o obstáculo a ser vencido e conhecer seus próprios pontos fortes e pontos fracos. Qualquer similaridade com a batalha da segurança da informação, não é pura coincidência. Que venha 2007!

Marcos Sêmola *é Diretor de Operações de Security & Information Risk da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, certificado CISM, BS7799 Lead Auditor, Membro da ISACA, ISSA, CSI e fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV, Pós Graduado em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Premiado SecMaster® em 2003 e 2004, tornando-se membro da comissão em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br*