65 - Março de 2005

O que eu não gostaria, mas preciso dizer sobre segurança.

Risco

- Nenhuma empresa estará um dia totalmente protegida das ameaças que colocam em risco suas informações. Isto seria absurdamente caro ou seus processos ficariam extremamente engessados.
- Os problemas e riscos de segurança tendem a crescer exponencialmente enquanto os orçamentos para as contramedidas nunca conseguirão acompanhar este índice.
- 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.
- Sem um estudo do risco aceitável para o negócio, o melhor a fazer é deixar que alguém melhor preparado para proteger as informações corporativas o faça.

Investimento

- Os acionistas e executivos têm que identificar e tangibilizar valor para decidir investir em segurança, não havendo outro motivo que os faça sair da inércia.
- Há muito tempo os especialistas procuram por fórmulas de ROI para justificar matematicamente os investimentos em segurança da informação, e continuarão procurando.
- Leis específicas, regulamentações gerais, setoriais e as auditorias internas e externas são, até o momento, os mais eficazes instrumentos motivacionais de investimento em segurança da informação.
- Apesar da regra de Paretto 80/20 se aplicar à segurança da informação, se lhe restar apenas “um real” para investir em segurança, desista. Você não conseguirá fazer nada efetivo com tão pouco.

Conformidade

- A norma ISO17799 não é a solução para o problema de segurança da informação, mas um guia recheado por conselhos que facilitam o diálogo entre técnicos e executivos de empresas distintas.
- As referências ISO17799/BS7799, COBIT, COBRA, ISO13335, ISO15408, ITIL, entre outras, serão apenas parte de mais uma lista de acrônimos geradores de trabalho e custo se não forem aplicadas de forma contextualizada à realidade de cada negócio.
- Seguir as recomendações da ISO 17799 ao pé da letra pode não levar sua empresa ao nível de segurança adequado, mas sua responsabilidade diminui, afinal, praticamente todos estão seguindo a mesma direção.
- A lei Norte Americana Sarbanes-Oxley é sem dúvida, o mais novo e eficaz fator motivacional de conformidade, afinal quem está sob risco é justamente o dono do orçamento.

Pessoas

- O nível de segurança no comportamento de um usuário é diretamente proporcional às facilidade de uso e às conseqüências negativas que podem advir para sua carreira

- O ser humano é o único ativo da equação de risco que tem perenidade e que pode evoluir cumulativamente sem requerer *upgrades* dispendiosos.
- Qualquer processo de segurança estará tão seguro quanto à segurança oferecida pelo ativo humano que o compõe.
- As pessoas são naturalmente diferentes em seus gostos, suas vontades e seus valores, por isso, toda solução de segurança deverá identificar os fatores motivacionais de cada grupo para transformá-los em agentes e não ameaças.

Solução

- As soluções de segurança baseadas puramente em hardware e software têm eficácia temporal, pois as tecnologias mudam antes mesmo que atinjam seu nível máximo de maturidade de proteção.
- Muitos anos já se passaram e a ciência da criptografia continua sendo a base dos mais eficazes métodos de proteção das informações.
- Se sua empresa não for visionária, ela não vai investir em determinadas tecnologias até que muitas outras tenham colecionado experiências negativas suficientes.
- As soluções de segurança precisam acompanhar o dinamismo dos agentes de risco, por isso, saiba que as tecnologias passam e só os processos resistem.

Profissional

- Decidir o que postergar e o que priorizar fará a diferença entre o Chief Security Officer ousado e o irresponsável.
- Os Security Officers, em sua maioria, ainda são apenas “pára-raios” corporativos e não têm posicionamento adequado, autonomia, poder e recursos suficientes para realizar um trabalho integrado e estruturado para a gestão de riscos.
- Não existe curso de qualquer natureza que preparem gestores de segurança da informação, pois eles são formados fundamentalmente pela vivência e o acúmulo de experiências técnicas, gerenciais e especialmente humanas.
- Cuidado com os ditos "especialistas". Em geral são exímios técnicos e estudantes, mas pecam no primeiro contato com um ativo que anda, fala, pensa e não reage de forma binária.

Fornecedor

- As consultorias não são as donas da verdade, mas podem ajudar muito, fazendo-o não perder dinheiro e tempo em caminhos que elas já conhecem por terem recomendado a algum cliente um dia.
- As consultorias de segurança deveriam se posicionar como verdadeiras assessorias financeiras, orientando o cliente a aplicar melhor seu capital considerando as particularidades do seu perfil de investidor.
- Não existe metodologia, ferramenta, treinamento ou procedimento que torne o serviço de consultoria amplamente escalável. O dia que isso ocorrer, estaremos vendendo e comprando alguma outra coisa.
- Teoricamente, o fornecedor que reúne todos os componentes de uma solução de segurança, mas pode comercializá-los em pedaços, é o que está mais preparado para assistir empresas que possuem níveis distintos de maturidade de gestão de riscos.

Conclusão

- Conceitualmente, atingiremos a maturidade adequada do nível de segurança quando ela não for perceptível. Em poucas palavras, pode-se dizer do processo de segurança que quando as coisas vão bem, ninguém sequer lembra que ele existe. Mas se os

processos estão emperrados, os usuários insatisfeitos por terem de trocar mais de senhas do que de roupa e o CEO se questionando porque apesar de todos os investimentos em segurança ele ainda continua a receber mais spams do que e-mails confiáveis, certamente algo está muito, muito errado.

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 do, ISACA, ISSA, IBGC e do Computer Security Institute, 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 premiado pelo ISSA por dois anos consecutivos SecMaster, Profissional de Segurança da Informação de 2003 e 2004 cat4. Visite* www.semola.com.br *e contate marcos@semola.com.br*