53 – Novembro de 2003

# Perspectivas 2004 para o mercado de segurança da informação

Passados praticamente doze meses da última previsão para o mercado de segurança da informação no Brasil nos deparamos com novas surpresas, e parece que desta vez a velha conhecida Lei de Murphy entrou em ação explicando – sob a ótica da segurança - a máxima de que o pão sempre cai com a manteiga virada para baixo na proporção direta do valor do tapete. Isso por que o crescimento que este mercado esperava para o ano de 2003 não ocorreu de fato e com isso, pudemos acompanhar apenas uma acomodação dos conceitos e o amadurecimento de algumas linhas de atividade.

Avaliando os principais momentos de 2003 vividos pelas empresas, os incidentes de segurança de massa que mais repercutiram, a natureza dos produtos e serviços mais demandados e tudo o que foi compartilhado nos principais eventos de segurança do Brasil, podemos ainda exercitar mais um prognóstico para o ano de 2004.

Parece que este foi o ano das fraudes eletrônicas, do SPAM (propaganda eletrônica não solicitada) e dos onipresentes vírus. Aparentemente problemas técnicos, de baixa complexidade quando os comparamos aos desafios do gerenciamento corporativo da segurança da informação, mas que cumpriram muito bem o seu papel e provocaram pânico, desconforto, prejuízo e principalmente, a reflexão dos empresários no sentido de tomar uma atitude coerente e eficaz imediata.

É verdade que não podemos associar este diagnóstico a todos os segmentos de mercado, nem tão pouco a todas as empresas, pois existem particularidades em seus modelos de negócio que as tornam diferentes e, portanto suscetíveis a impactos distintos. Contudo, foram eventos tão abrangentes e representativos, atingindo segmentos igualmente tão presentes ao nosso cotidiano, que podemos usá-los como referência do comportamento global.

Pontos fracos

Vimos a materialização do conceito do elo fraco da corrente quando os vírus de computador fizeram parar redes locais e metropolitanas inteiras apesar de todos os demais aparatos de segurança adotados em outros perímetros como detectores de intrusos, firewall, virtual private network, serviços de autenticação etc.
Constatamos a fragilidade do ativo humano pelo comportamento e atitudes de risco resultantes da falta de cultura, da falta de regras claras e principalmente, da falta de instrumentos que possam reduzir os efeitos da curiosidade, desatenção, incompetência, esquecimento e de muitas outras fragilidades potenciais do indivíduo.

Em contrapartida, vimos a norma de segurança da informação ISO 17799:1 amadurecer ainda mais e ser adotada pelas empresas como um instrumento de orientação, seja para a definição de um plano estratégico, seja para a especificação, priorização e orientação de

projetos ou ainda, para a contratação de serviços de segurança. Este dado é muito positivo e se valoriza ainda mais ao constatarmos maturidade avançada das empresas que planejam primeiro a adoção de controles de segurança que as levem a operar sob grau de risco controlado, para só então, pensar em obter a certificação associada.

Certificação BS7799

Segundo informações obtidas no mês de novembro junto ao BSI, o número de empresas certificadas BS7799 no mundo praticamente dobrou quando comparamos com o ano de 2003. São mais de 420 empresas que obtiveram o reconhecimento do trabalho. Apenas 2 no Brasil, mas talvez um sinal positivo considerando a conclusão anterior de que não se está procurando o selo pelo selo, mas primeiro a certeza de estar cercado pelas melhores práticas de gestão de segurança.

Administração responsável

Esta é outra boa conclusão que podemos extrair do ano. Os desafios e responsabilidades pela gestão de riscos atingiram a camada mais alta da administração das empresas e desta vez, a segurança têm sido pensada como instrumento estratégico de negócio, portanto, algo que só tem valor se puder ser convertido em benefício direto para o modelo de negócio. Seja como instrumento de ganho de credibilidade, seja como uma forma de reduzir custos diretos e indiretos ou como alternativa para minimizar os prejuízos, os investimentos não mais ocorrem em segurança pela segurança, mas em segurança pelo negócio.

Objetividade do CSO

Falando em perseguir continuamente o retorno sob os investimentos, chegamos à grata surpresa de ver que os Chiefs Security Officer (CSO) ou demais responsáveis por propor ações de segurança estão mais objetivos e focados. Procuram identificar os problemas de forma pró-ativa, priorizá-los com base nos impactos que podem provocar à continuidade do negócio e então, adotar medidas objetivas e principalmente, que dêem retorno rápido para a redução dos riscos.

Apesar de estarem pensando no todo e continuarem sonhando com um grande e completo Security Operation Centrer (SOC), com suas dezenas de indicadores de segurança, sensores, alarmes, times de resposta a incidentes, planos de continuidade, e tudo mais necessário para se ter controle centralizado e corporativo dos riscos - um verdadeiro Security Score Card - eles estão imediatistas.

Resultados de curto prazo

Os profissionais de segurança querem construir a grande muralha, tijolo a tijolo, garantindo que estejam bem instalados e principalmente, alinhados com as diretrizes maiores da empresa e as melhores práticas. Assim, quando muitos tijolos estiverem empilhados, com seus respectivos papeis bem definidos e executados, poderão se dar conta de que construíram um modelo funcional de gestão de riscos e proteção do negócio.

O que vêem são percepções e conclusões extraídas ao longo do ano, considerando ainda o histórico do próprio mercado de segurança brasileiro. Assim, podemos sinalizar alguns caminhos e tendências para 2004.

- **Orientação por Perímetro.** Este deverá ser o foco de parcela representativa do mercado. Qualquer que seja o estágio atual de segurança da empresa, esta irá diagnosticar os riscos, priorizá-los e implementar controles imediatistas sempre segmentando por perímetro. Desta forma, consegue-se em espaço significativamente menor de tempo, reduzir os riscos e avançar substancialmente na sua administração quando se faz em pedaços. É como dividir um grande problema em pequenos e significativos pedaços para assim, tratar os mais importantes com profundidade.

- **Paralelismo estratégico.** Conceitualmente não se deve tratar a segurança de forma reativa ou pensando apenas no curto prazo. Por isso, contrapondo à primeira tendência, deverão existir ações estratégicas em paralelo para garantir a preparação de um alicerce estável e que irá suportar as ações de médio e longo prazo. Desta forma, análises de risco estratégicas, Gap Analysis baseadas na BS7799 ou ainda em leis, padrões e regras próprias devem ser ações implementadas para se desenhar um plano de investimentos e montar a estrutura que poderá materializar o tão sonhado SOC e Securty Score Card.

- **Análise de Riscos focada em processo**. Felizmente o ser humano evolui e com ele as ferramentas, conceitos e técnicas. Acompanhando este momento de maturidade e objetividade dos gestores de segurança, os serviços de análise de riscos terão de mudar. Apesar de serem úteis em perímetros muito pequenos e cujo objetivo é traçar atividades operacionais, as análises de risco que resultam em centenas de folhas de papel com milhares de vulnerabilidades e recomendações não fazem mais tanto sentido. Para que saber que 80% da estações de trabalho estão com uma vulnerabilidade XPTO se o que mais me interessa é saber o que fazer estruturalmente para que elas deixem de ocorrer? O foco deverá ser na identificação da origem dos riscos e não dos seus efeitos de primeiro nível. Os desafios de segurança tendem a ser contínuos e por isso, tratar a dor sem perseguir a causa deve levar as empresas à sangria de recursos infinita e portanto, totalmente desalinhadas com os interesses do negócio.

- **Segurança aplicada**. Como ocorre com outras ciências que mantém teoremas, fórmulas e conceitos genéricos válidos, mas têm seu potencial de retorno maximizado quando deixam de ser ciências puras e passam a aplicadas, as empresas deverão fazer o mesmo com a segurança. Ao contratar serviços das consultorias, por exemplo, tendem a procurar no fornecedor o diferencial de conhecer os meandros e características intrínsecas do seu modelo de negócio ou segmento de atuação para que o knowhow de segurança possa ser maximizado e a modelagem das soluções seja contextualizada. É uma forma inteligente de ganhar tempo, reduzir custos e principalmente, aumentar a chances de acertar da primeira vez.

- **Gerência de mudanças**. Tende a ser componente onipresente nos projetos de segurança da informação. Considerando o ativo humano um dos mais frágeis na corrente de segurança, e ainda, considerando que de uma forma ou de outra este ativo é sempre envolvido nas ações e projetos, torná-lo um aliado é fator crítico de sucesso para os resultados diretos da ação ou projeto e também elemento básico para a continuidade da gestão de riscos. Conhecer os formadores de opinião, mapear o nível de cultura, identificar os entusiastas, sépticos e reativos e desenvolver um plano de ação para que todos joguem no mesmo time e tenham atitudes seguras é a chave.

- **Monitoramento por perímetro tecnológico**. Sistemas de segurança que segmentem o ambiente tecnológico em perímetros, sistemas que monitorem o movimento dentro dos perímetros e ainda que reajam à situações e comportamentos suspeitos dos ativos da informação deverão ser uma forte tendência para 2004 seguindo o próprio movimento iniciado em 2003. O segredo está na busca pela resposta rápida a uma situação de risco e seu isolamento no menor tempo possível para que aumentem os mecanismos de manobra e contenção.

- **Certificação ISO17799**. Ainda não será um objetivo de massa para 2004, pois dificilmente as empresas atingirão um grau de maturidade dos controles que lhes permita o reconhecimento do trabalho através do selo. Exceto para aquelas focadas explicitamente em explorar o potencial de marketing do instrumento e assim, dedicadas a escopos muito pequenos, restritos funcionalmente e normalmente sem associação direta com a atividade fim da empresa.

- **Smartcard para tudo e todos.** Por mais um ano os cartões inteligentes smartcards e certificados digitais estarão ocupando um espaço cada vez maior nas relações eletrônicas. À medida que forem se tornando mais baratos e assim, viáveis financeiramente, estarão substituindo os antigos métodos de autenticação. Parece que 2004 será o ano deles, pois muitas *killer applications*, ou melhor, aplicações que adicionam valor e mostram a aplicabilidade e o retorno da adoção do dispositivo, estão na prancheta e deverão ser implementadas. Para dar ainda mais força, as fraudes foram uma constante e já representam um dos principais motivos para a adoção do cartão em larga escala. Ocorrendo isso, veremos surgir novas tendências ligadas à necessidade de integrar aplicações e maximizar o uso deste dispositivo tão versátil e multifuncional. Mas esse assunto já pode ficar para a previsão de 2005.

Mais objetivas e aparentemente mais coerentes que as do ano anterior, as percepções de 2004 revelam o direcionamento do mercado em busca do retorno rápido e efetivo dos investimentos sem perder de vista a estrutura de gestão de longo prazo.

Empresas preocupadas em tornar seus negócios mais competitivos, estáveis e produtivos, mesmo que para isso elas não tenham de implementar tudo que dizem ser bom ou todos os controles que as melhores práticas “genéricas” de mercado recomendam.

***Marcos Sêmola*** *é Consultor Sênior em Gestão de Segurança da Informação, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação e autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus 2003. Atualmente é Security Consulting Practice Manager da Schlumberger Worldwide IT Partner.*
*marcos@semola.com.br*