38 – Janeiro de 2002

Perspectiva 2002 para o mercado de segurança da informação

É sempre uma tarefa difícil e no mínimo arriscada tentar prever o futuro. A dificuldade é ainda agravada quando estamos falando de futuro no mercado de tecnologia, mais especificamente o mercado de segurança por estar muito incipiente, eu diria engatinhando, haja visto o baixo grau de percepção, amadurecimento, e conseqüente baixo investimento, realizado por parcela representativa do empresariado brasileiro.

Desnecessário ainda dizer que os fatos terroristas que abalaram diretamente a América do Norte e indiretamente todo o resto do mundo, potencializaram a sensibilidade dos governantes e empresários à luz dos efeitos causados em seus negócios. As empresas seguradoras, Internet Data Centers que proporcionam hospedagem de equipamentos e sistemas, e ainda as empresas fornecedoras e mantenedoras de planos de continuidade tiveram, à partir de então, seu momento de alta valorização. Estas talvez tenham sido as estrelas mais brilhantes, portanto perspectivas previsíveis para 2002.

Mas de que adianta falarmos do que já era previsto?

Baseado na experiência de anos acompanhando e atuando no mercado de segurança, acompanhando a evolução conceitual da segurança da informação proporcionada pela dedicação aplicada dos especialistas e estudiosos, e ainda vendo surgir tecnologias afins, sinto me mais confiante ao continuar escrevendo este breve rascunho – organizado em tópicos - do que poderá ser o ano de 2002 para o mercado em geral e os profissionais de segurança.

- Segurança para todos. Independentemente do porte do negócio, faturamento anual, abrangência geográfica, natureza do trabalho e característica física, tecnológica e humana, todos estarão mais preocupados e dispostos a pensar e reagir à questões de segurança. Os investimentos em segurança tenderão a ser proporcionais e relativos aos investimentos realizados em tecnologia da informação. Especula-se sobre os índices de 2% a 8% em empresas tradicionais que usufruem de tecnologia e explorem o mercado eletrônico como canal alternativo de negócio. Os percentuais sobem e ficam na faixa de 10% podendo atingir 25% em função do grau de automação, informatização e dependência de processos tecnológicos para a continuidade operacional do negócio.

- Investimento será a palavra do ano. A segurança deixará de ser percebida como despesa – outrora com poucas chances de ser justificada – e passará a ser viabilizada por análises e estudos do ROI – Retorno sobre o Investimento, que serão considerados e valorizados pelos sócios, investidores e pelo próprio mercado, provocando reflexos no fortalecimento da imagem da empresa e a sua conseqüente valorização.

- As grandes corporações deixarão de buscar soluções de segurança pontuais e isoladas que cumprem um papel limitado e auxiliam paliativamente a empresa no

objetivo maior de reduzir seu risco operacional. Estarão com isso organizando o departamento de segurança corporativa, liderado pela figura do Security Officer, e posicionando-o com maior autonomia no organograma. O reflexo disso será o tratamento integrado das demandas de segurança orientadas pelas necessidades do negócio e não necessariamente as perspectivas do departamento de Tecnologia da Informação.

- Foco é outra palavra de ordem. A competitividade do mercado, mais visível nos segmentos financeiro, telecomunicações e energia fará com que as empresas não gastem seus esforços em atividades que não fazem parte de seu core business, ou seja, estarão organizando melhor sua área de segurança sob o ponto de vista de gestão, mas contarão com apoio externo de empresas especializadas que possam servir de retaguarda. Desta forma, terão os processos de segurança sob controle, mas interferirão apenas na organização, coordenação e acompanhamento dos trabalhos terceirizados que envolvem tecnologias heterogêneas e extremamente perecíveis e dinâmicas que obrigam altos investimentos em capacitação.

- A complexidade crescente dos processos de negócio, a heterogeneidade de tecnologias, o alto grau de conectividade e compartilhamento de informações, e ainda os novos planos de negócio da empresa serão fatores ainda mais relevantes para a gestão do Security Officer. Diante disso, possuir um Plano Diretor de Segurança será condição si ne qua non para a orientação do profissional de segurança na relação com os executivos principais da empresa, investidores e conseqüentemente com a empresa especialista que atuará como retaguarda de segurança.

- Os planos de continuidade de negócio, divididos em plano de recuperação de desastres, plano de administração de crises e plano de continuidade operacional, receberão grande destaque na primeira metade do ano, principalmente em empresas que dependerem de operações críticas cujo prejuízo é proporcional ao tempo de indisponibilidade. Contudo, a euforia por esta solução deverá se amenizar, equilibrando e distribuindo os investimentos também em ações preventivas ligadas à auditoria, administração, monitoramento e capacitação.

- Os Internet Data Centers, que até então têm se limitado a oferecer serviços de hospedagem enfatizando a redundância de equipamentos e meios de conectividade, irão unir forças com empresas especializadas em segurança da informação a fim de somar controles físicos, tecnológicos e humanos que elevem efetivamente o nível de segurança de seus serviços, e representem um diferencial competitivo junto aos concorrentes. Nascerá o Security Internet Data Center.

- Mesmo sabendo da diretriz correta de tratar a gestão de segurança de forma corporativa, muitas empresas ainda não estarão preparadas financeiramente – principalmente as empresas de pequeno e médio porte - para suportar e fomentar planos completos de segurança, contudo, não mais se satisfarão com peças soltas do quebra-cabeça. Buscarão peças ou conjunto delas que estejam orientadas e

preparadas para o encaixe gradativo em busca do uma visão integrada: ESP – Enterprise Security Planning.

- Em função dos altos custos relacionados à administração de equipamentos, atualização de softwares, mais especificamente sistemas operacionais, e a monitoração de serviços retratados em 2001, será uma tendência a adoção de serviços terceirizados de gestão remota de firewall, intrusion detection system, roteador, servidor e aplicações críticas. Desta forma reduzirão os custos diretos, e os custos indiretos relacionados à capacitação constante de equipes multi-especialistas.

- Controle do ativo humano, especificamente nas relações com funcionários, terceirizados, fornecedores, parceiros e clientes receberá ênfase em 2002 por conta dos altos índices de quebra de segurança associados aos capital humano, pelos altíssimos índices de improdutividade e danos provocamos por mal uso dos recursos disponibilizados e permissões de acesso errôneos, e ainda motivado por interpretações recentes da justiça e responsabilizações civis ligadas à pirataria de software, pedofilia, vírus e crimes previstos em lei.

- Smartcards, e principalmente os Certificados Digitais estarão por toda a parte. O barateamento desses recursos atrelado ao grande leque de aplicações que poderá fazer uso deles tornará seu uso uma comodities. Complementarmente à evolução dos softwares que já nascerão preparados para usufruir dos benefícios da tecnologia PKI (PKI ready ou preparadas para infra-estrutura de chaves públicas), a legislação brasileira estará ainda mais madura e sinalizando o reconhecimento legal de documentos eletrônicos assinados digitalmente primeiramente no âmbito da administração pública federal, estadual e municipal.

- Os dispositivos de biometria ainda não serão uma realidade neste ano em função de seu custo, exceto em pequenas e restritas comunidades que por sua natureza de operação, viabilizarão financeiramente o investimento considerando os altos valores em risco operacional.

- O conceito de segmentação da proteção se fará ainda mais presente através de mecanismos de software e hardware destinados ao perímetro do usuário, ou seja, preocupados com a segurança da estação de trabalho. Ilustrativamente falando, as empresas não manterão apenas um grande escudo de proteção, mas também entregarão pequenos escudos à cada funcionário buscando fortalecer o conjunto. Firewall pessoal, antivírus ativo, aplicação de criptografia, certificado digital para email e logon em rede e dispositivos de controle de acesso físico são algumas das formas.

- A norma ISO 17799 será a verdadeira bússola do setor de segurança da informação, devendo orientar o desenvolvimento e adequação dos serviços oferecidos por empresas especializadas e consequentemente orientar a gestão do Security Officer. A junção das partes 1 e 2 da norma, respectivamente o código de conduta para tratamento da segurança e a especificação de controles e implementação do ISMS –

Information Security Management System, irá fortalecê-la dando-lhe gradativamente importância similar à norma de qualidade ISO9001.

É bom parar por aqui, afinal o artigo já se estendeu demais e não quero que seja confundido com um daqueles mapas astrais que ano após ano prometem revelar em detalhes as nuances da vida de pessoas, o prognóstico de empresas e o destino de países.

Este artigo reflete o meu entendimento - deveras otimista por sinal - do segmento de segurança da informação, considerando principalmente experiências passadas e sensibilidades futuras, e visa compartilhar esta percepção de forma a fazê-los refletir, ratificar e até mesmo retificar algumas das minhas conclusões. No fundo, espero estar certo.

Mas não esqueça que você e sua empresa fazem parte do jogo e poderão interferir na concretização deste "planejamento", portanto, faça a sua parte. Trabalhe por resultados, alinhe-se às estratégias do seu negócio, organize um Security Office, realize investimentos, busque a gestão integrada, oriente-se por um Plano Diretor de Segurança e viabilize assim um prognóstico ainda melhor para 2003.

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente Nacional de Produtos e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br