29 – Fevereiro de 2001

Estratégia de Segurança: o jogo dos 7 erros

Plano Diretor de Informática, já é expressão conhecida nos grandes ambientes corporativos. Consomem tempo de planejamento e principalmente elaboram altos investimentos para permitir que as empresas mantenham e atinjam patamares crescentes de competitividade. Foram ganhando ainda mais importância ao longo do tempo, diante da velocidade com que a tecnologia da informação foi penetrando nos ambientes, e pela mesma velocidade com que as informações foram sendo digitalizadas e compartilhadas.

Simultaneamente, diante do crescente resultado de exposição dessas empresas, foram surgindo correntes preocupadas com a segurança das informações. Estas preocupações aos poucos foram sendo absorvidas pelos gestores de tecnologia, os mesmos responsáveis por disponibilizar infra-estrutura tecnológica e ferramentas eletrônicas, que viabilizavam as idéias mirabolantes dos homens de negócio.

Erro número 1: Atribuir a responsabilidade pela gestão da segurança à estrutura organizacional de Tecnologia da Informação.
O momento refletia a interseção de atividades ímpares, pois quando relacionadas à tecnologia eram facilmente mensuráveis, e principalmente, podiam ter seu valor agregado quantificado e o investimento justificado. Em contrapartida, as ações de segurança eram dificilmente visíveis e raramente proporcionavam retornos imediatos. Nessa época, assumiam caráter reativo orientado por situações de quebra de segurança, desta forma minimizando os impactos emergenciais.
Conclusão: no apagar das luzes, em se tratando de um orçamento comum, as prioridades acabavam tendendo inevitavelmente para as ações tecnológicas, o que colocava a segurança em segundo plano.

Erro número 2: Segurança disputando e compartilhando orçamento com TI.
Além da perda de prioridade, as ações de segurança ainda eram associadas apenas à esfera tecnológica e atreladas à estrutura organizacional de TI.
Foi preciso entender que as informações mais valiosa das empresas não estão apenas em formato digital trafegando pelas redes, mas também – apesar de em menor quantidade – em papéis impressos ou escritos à mão, em reuniões, conversas pessoais ou via telefone, e principalmente na memória dos funcionários. Definitivamente estão distribuídas pelos diversos processos de negócio que alimentam o organismo corporativo. Diante disso, passaram a perceber que os problemas de segurança são físicos, tecnológicos e também humanos. Assim, surgiram questionamentos: como atribuir a responsabilidade da gestão de segurança à uma esfera estritamente tecnológica? Como as ações de segurança que partissem de TI, e portanto planejadas no PDI, poderiam atingir e solucionar os problemas nos mais distribuídos ambientes corporativos?

Erro número 3: Entender que os problemas de segurança são exclusivamente tecnológicos.

Depois desse momento de elucidação, e assumindo que a partir de agora o papel de gerir a segurança não deva ser exclusivamente da área tecnológica, uma pergunta ainda permanece: de quem será essa atividade?
Muitas empresas iniciaram um processo distribuído em busca da segurança. Reuniram departamentos, atribuíram autonomia e permitiram que cada um percebesse suas fraquezas, necessidades e buscassem soluções personalizadas que efetivamente elevassem o nível de segurança de cada perímetro. Contudo, mais uma vez a empresa fora vítima de sua própria visão míope sobre o problema. Apesar de já saberem que os problemas de segurança físicos, tecnológicos e humanos se encontravam espalhados por toda a empresa, não percebiam que através de soluções isoladas não conseguiriam reverter o quadro geral e elevar o nível de segurança do negócio.

Erro número 4: Satisfazer-se com a falsa sensação de segurança oferecida por ações isoladas e pontuais.
Imagine a empresa como um organismo vivo. Do que adiantaria garantir que o coração bombeasse adequadamente o sangue para o restante do corpo, se o fígado não for eficiente na filtragem das impurezas do sangue? O organismo não estaria igualmente comprometido? Aproveitando o assunto, me vem a lembrança do lançamento do foguete espacial Challenger da NASA. Ainda lembro quando em 1987, após 73 segundos de seu lançamento, houve uma explosão que chocaria o mundo e abalaria a hegemonia americana na exploração do universo. Um projeto grandioso, que consumiu milhões de dólares, milhares de horas de trabalho e dedicação de centenas de profissionais das mais diversas especialidades. Todo o investimento comprometido por uma única peça defeituosa, especificamente o retentor do tanque de combustível, que custava nada mais que U$900.

Erro número 5: Não perceber a segurança como uma corrente composta por elos, onde um único elo fraco pode comprometer a segurança do negócio.
Depois de aprender com os erros cometidos, muitas empresas apararam as arestas e iniciaram internamente um trabalho de gestão da segurança. Porém, por não possuir know how específico no assunto, não souberam definir o posicionamento adequado da equipe no organograma da empresa, organizar o comitê de segurança e ainda adotar um modelo de gestão corporativa de segurança da informação que coordenasse e buscasse a integração das diversas ações departamentais. Resultado: criaram uma equipe para responder às tentativas de quebra de segurança e não para estudar o passado, gerir o presente e preparar o futuro.

Erro número 6: Julgar que o papel da segurança não deva ser preventivo.
Logo ficou visível a ineficiência do posicionamento reativo. Medidas emergenciais apenas remediavam os impactos já gerados ao negócio e não evitavam que os mesmos voltassem a ocorrer. Não havia ritmo adequado para reparar as vulnerabilidades antes de terem sido exploradas por invasores, hackers etc. A situação se agravava a cada dia, de acordo com a velocidade e dinamismo com que as informações eram digitalizadas e compartilhadas, elevando o nível de exposição da empresa. Faltava sensibilização do corpo executivo. Faltava comprometimento de todos os funcionários. Faltava organização e planejamento.

Erro número 7: Não possuir um Plano Diretor de Segurança.
Felizmente o pensamento corporativo associado a Segurança da Informação evoluiu para muitas empresas – mérito atribuído principalmente pelo aprendizado extraído dos erros –

que já programam desenvolver um Plano Diretor de Segurança estratégico para sustentar e viabilizar um modelo de gestão corporativa, capaz de orientar, organizar e planejar as ações em busca do nível de segurança adequado ao negócio.

Aspectos, etapas e atividades para se construir um Plano Diretor de Segurança serão assuntos do próximo artigo.

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 de Produto e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br