37 – Dezembro de 2001

Descobrimos a agenda do Security Officer para 2002

Agora que estamos perto do fim de mais um ano, alguns desafios postergados e muitos outros ainda por vir, as empresas começam a dimensionar seus orçamentos para o ano 2002. Não se trata de uma atividade linearmente simples, afinal, certos aspectos relacionado à operação do negócio não podem ser previstos e muitos outros ainda nem existem mas certamente surgirão durante o próximo ano em virtude da incidência de variáveis macro-econômicas, mercadológicas, culturais e principalmente tecnológicas.

Enganados estão os que associam esta última fase do ano, destinada aos planejamentos e previsões orçamentárias, exclusivamente aos Chief Executive Officers (CEO), Chief Information Officer (CIO) e seus consultores diretos. Lado a lado está o Comitê Executivo, agora com a presença de uma nova figura que representa os interesses da empresa associados à continuidade do negócio, à viabilidade de aplicações e principalmente na segurança da informação com forma de adicionar valor, o Security Officer.

E como não poderia deixar de ser, este executivo da informação também precisa dimensionar esforços, planejar atividades comumente plurianuais e estabelecer planos orçamentários a fim de fomentar a criação (para os que ainda não dispõem) e a manutenção do processo de gestão corporativa de segurança da informação. Seu principal objetivo? Preparar a empresa para suportar, reduzir e administrar os riscos ligados à segurança da informação que existem e passarão a existir a curto, médio e longo prazos à medida que mudanças físicas, tecnológicas e humanas ocorram, incidindo direta e indiretamente na operação do negócio. Em suma...viabilizar o sorriso dos sócios e possivelmente dos investidores, ao lerem a última linha do balando: LLE – Lucro Líquido do Exercício.

Pensando nesse complexo objetivo e buscando um direcionamento, esbocei o que poderíamos chamar de Agenda do Security Officer para o ano de 2002. Vejamos o resultado:

Jan/2002

- Reunião do Comitê Corporativo de Segurança da Informação
  - Análise e definição do apoio externo de empresa de consultoria especializada em gestão de segurança da informação
- Reunião do Comitê Executivo
  - Palestra de sensibilização “Desafios de Segurança de 2002”
  - Apresentação das macro atividades do Security Office
  - Apresentação das métricas, índices e indicadores do Security Office
  - Comunicação do início dos trabalhos com o mapeamento de ameaças, riscos e impactos através da execução do projeto Plano Diretor de Segurança

Fev/2002

- Execução do projeto Plano Diretor de Segurança
  - Mapeamento dos processos de negócio críticos, ativos físicos, tecnológicos e humanos associados, ameaças, riscos e sensibilidades diante da quebra de segurança: confidencialidade, integridade, disponibilidade, autenticidade e legalidade. Identificação de desafios, necessidades e especificação dos projetos que irão formatar a Solução Corporativa de Segurança.
- Execução do projeto Teste de Invasão
  - Verificação do nível de segurança de um ambiente ou processo de negócio crítico através da simulação de tentativas de invasão, cujos resultados poderão servir de instrumento de sensibilização do Comitê Executivo no momento de definir prioridades de ação.
- Reunião do Comitê Executivo
  - Apresentação dos resultados obtidos no projeto Teste de Invasão
  - Apresentação do Plano Diretor de Segurança
  - Aferição do Plano de Ação e a priorização das atividades

Março/2002 – Junho/2002

- Reunião do Comitê Executivo (mensal)
  - Apresentação dos resultados parciais e finais dos projetos executados.
  - Redefinição de prioridades e intervenção no Plano de Ação
- Execução do projeto Treinamento em Segurança da Informação
  - Seminários de sensibilização dos funcionários (técnicos e usuários) quanto aos aspectos de segurança da informação.
- Execução do projeto Análise de Vulnerabilidades
  - Identificação e mapeamento de vulnerabilidades nos ativos tecnológicos: equipamentos, links, sistemas de computador, redes etc; nos ativos físicos: infra-estrutura elétrica, infra-estrutura de telecomunicações, combate à incêndio, controle de acesso físico, salas cofre etc; nos ativos humanos: cultura dos funcionários, comportamento, regras, padrões, critérios de manuseio, armazenamento, transporte e descarte de informações.
- Execução do projeto Política de Segurança
  - Definição de Diretrizes e Normas de segurança que especificam padrões, critérios, regras, responsabilidades e permissões para o adequado uso da

informação. Definição de Procedimentos e Instruções para ambientes, aplicações e processos de negócio específicos.

- Execução do projeto Campanha de Divulgação
  - Ações de comunicação interna para sensibilização dos funcionários (usuários e técnicos) para aos aspectos de segurança da informação, conscientização das Diretrizes e Normas Gerais da Política de Segurança. Exemplo de recursos: cartazes, mouse pads, screen savers, seminários, revistas, jogos e vídeos.
- Execução do projeto Implementação de Recursos de Segurança
  - Aplicação de elementos de software, hardware e peopleware para elevação do nível de segurança, incluindo instalação, configuração, capacitação, e definição de normas técnicas específicas. Exemplo de recursos: firewall, programas de atualização de sistemas operacionais, detector de intrusos, mecanismos de auditoria de log, filtros de acesso lógico, dispositivos de autenticação biométrica e criptografia.

Julho/2002 – Novembro/2002

- Reunião do Comitê Executivo
  - Apresentação das métricas, índices e indicadores do Security Office
  - Apresentação dos resultados parciais e finais dos projetos executados.
  - Redefinição de prioridades e intervenção no Plano de Ação
- Formatação e operacionalização de atividades de gestão: Administração de Recursos de Segurança
  - Continuidade das funções de Planejamento, Coordenação, Execução Controle, organizando novas demandas, analisando necessidades originadas de mudanças, auditando e monitorando os recursos de segurança. Este processo passa a assumir o eixo central do modelo de gestão corporativa de segurança da informação.
- Execução do projeto Plano de Continuidade de Negócio
  - Especificação de alternativas para contingenciar situações onde a quebra de segurança não fora previsível ou fora inevitável, minizando os impactos no negócio. Plano de Continuidade Operacional, Plano de Recuperação de Desastres e Programa de Administração de Crises se complementam em busca da garantia de continuidade do negócio.

Dezembro/2002

- Análise holística dos resultados obtidos no exercício
- Mensuração do Retorno sobre os Investimentos (ROI)
- Mapeamento dos desafios atuais e futuros

- Dimensionamento orçamentário para 2003

Ao término do cumprimento dessa agenda, mesmo que tenha havido modificações ou limitações em função do seu contexto, mais um ano transcorrerá, novos desafios e oportunidades surgirão e – como no xadrez – dependendo do movimento de peça que fora feito em 2002, sua empresa poderá continuar na partida em 2003 ou estará correndo altos riscos de sofrer um cheque mate.

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