30 – Março de 2001

Plano Diretor de Segurança: fator crítico de sucesso!

Depois de muitos erros cometidos na tentativa de reparar os problemas de segurança espalhados pelos diversos perímetros da empresa, identificou-se um fator crítico de sucesso: Plano Diretor de Segurança.

Mais do que um orçamento, como sugere o já tradicional Plano Diretor de Informática, o PDS tem de ser dinâmico e flexível para suportar as novas necessidades de segurança que surgem em virtude da velocidade com que os fatores físicos, tecnológicos e humanos mudam.

O início da modelagem do PDS está diretamente associado a ações de levantamento de informações do negócio, similar à uma consulta médica onde além da anamnese inicial, são realizados exames e testes para diagnosticar os sintomas, as anormalidade e riscos potenciais do paciente, ou seja, identificar as ameaças, vulnerabilidades, riscos e impactos potenciais ao negócio.

Temos que tem em mente que o Plano deve, entre outras coisas, especificar dentro de um modelo de gestão corporativo de segurança da informação, as ações e atividade que deverão ser executadas ao longo da vigência do plano, afim de reduzir ao máximo os riscos e ainda de permitir que a empresa atinja o nível de segurança projetado.

Não há um modelo de plano que seja capaz de atender à todo tipo de empresa, por mais que sejam empresas do mesmo porte e até mesmo do mesmo segmento de mercado. Existem particularidades intrínsecas como ameaças, riscos, sensibilidades, impactos e vulnerabilidade físicas, tecnológicos e humanas que tornam o problema único. Portanto, seguindo a analogia com a medicina, este paciente terá de ser atendido por um receituário medicamentoso único e personalizado capaz de sanar e estancar a enfermidade também única.

Diagnóstico

Esta etapa é composta por diversas atividades. Não é tarefa fácil quando se trata de uma empresa de grande porte, pois dificilmente se encontrará um grupo acessível, pequeno e coeso capaz de ter uma visão corporativa ampla e completa. Além disso, a complexidade dos ambiente, heterogeneidade de tecnologias, acessos híbridos e a previsível distribuição de responsabilidades de segurança pelos departamentos são fatores dificultadores.

Identificação dos processos de negócio

Reunindo os principais gestores, comumente da esfera executiva-gerencial, esta atividade objetiva identificar – através de entrevistas - os processos de negócio que serão alvos das atividades subsequentes. Partindo da premissa de que as ações de segurança devam ter o foco no negócio e nas informações que o sustenta, é imprescindível elencar os processos

mais sensíveis. É como se perguntássemos ao paciente as dores que está sentindo e a localização delas. Além disso, buscamos identificar as necessidades tecnológicas e de conectividade desses processos para todo o negócio.

Estudo de Impactos CIDA

Identificados os processos de negócio críticos na atividade anterior, é hora de realizar estudos que apontarão a sensibilidade de cada um deles diante da possível quebra de Confidencialidade, Integridade, Disponibilidade e Autenticidade. Este último, apesar de não ser uma propriedade específica da informação, mas sim dos interlocutores de um relacionamento real ou eletrônico, tornou-se importante atualmente para realçar possíveis necessidades específicas. O estudo acontece através de entrevistas – também com os principais gestores, comumente da esfera executiva-gerencial – e tem como possíveis respostas: não considerável, importante, crítico e vital. O resultado desta atividade – que organiza e indexa os processos por grau de impacto potencial - irá se juntar ao resultado das demais para nortear a modelagem do plano diretor de segurança.

Estudo de Prioridades GUT

Ainda reunidos com os principais gestores, esta atividade se preocupa em pontuar e priorizar os processos de negócio de acordo com a, já conhecida por muitos, matriz de GUT: Gravidade, Urgência e Tendência. Questiona-se o quão grave seria para o negócio se algum fato atingisse qualquer um dos conceitos de segurança. Qual a urgência para o negócio em solucionar e reduzir os riscos no referido processo de negócio. E ainda qual a tendência do processo se nenhuma atividade de segurança fosse aplicada. Temos nestas perguntas, respostas como 5 níveis para cada dimensão, tendo como GUT máximo 5x5x5, ou seja, 5 extremamente grave, 5 imediata e 5 vai piorar rapidamente.

Estudo de Perímetros

Agora que já temos os elementos geradores de dor, sua localização, os possíveis impactos ao corpo se fossem afetados, e a prioridade em reduzir os riscos de impacto, chega o momento de identificar os ativos – infra-estrutura, tecnologia, aplicações, informações e pessoas – que sustentam e suportam os processos de negócio. De acordo com os aspectos e conceitos da segurança da informação, os ativos possuem vulnerabilidades que deverão ser eliminadas e minimizadas pelas ações de segurança. Diferente das atividades anteriores, esta reuni em entrevistas os principais gestores da esfera técnica-tática que irão levantar números e informações topológicas, físicas e tecnológicas ligada diretamente e indiretamente aos processos de negócio. Diante disso, a atividade passa a ser primordial para que os projetos necessários sejam identificados e passem a integrar o Plano Diretor de Segurança.

Estudo de Atividades

É o momento do médico especialista analisar as reclamações de dor, os resultados dos exames, o contexto, o comportamento habitual e necessidades do presente e futuro do paciente para dimensionar a solução corporativa de segurança, composta por projetos que

irão subsidiar a modelagem do PDS. É hora de planejar as ações que ocorrerão em ambientes e perímetros distintos e isolados, mas que estarão sendo coordenados e principalmente, em conformidade com as diretrizes de segurança da empresa proposta pelo modelo de gestão corporativa de segurança da informação.

Como resultado desta atividade, destacamos alguns projetos que poderão ser receitados" e farão parte de cada um dos processos de negócio alvo desta etapa de diagnóstico:

Análise de Riscos e Vulnerabilidades
Análise de Código de Aplicação
Especificação de Controles e Ferramentas
Campanha de Divulgação de Política de Segurança
Classificação de Informações
Equipe de Resposta a Invasões
Informativo Técnico de Segurança
Política de Segurança
Implementação de Controles e Ferramentas
Capacitação em Conceitos de Segurança
Plano de Continuidade de Negócios
Teste de Invasão
...

Organização do Comitê Corporativo de Segurança

Paralelamente às atividades de diagnóstico, é fator crítico de sucesso iniciar a organização de um grupo convencionalmente chamado de Comitê Corporativo de Segurança. A primeira atividade é definir as responsabilidades de planejamento, execução, monitoração, seu posicionamento dentro do organograma da empresa garantindo que tenham acesso à esferas decisivas que possam atuar sobre toda a corporação. Seguido da divulgação interna e oficialização deste grupo formado por representantes de diversas áreas estratégicas da empresa, que reúnem especialidades e visões distintas. Seu principal papel será organizar, concentrar e planejar as ações de segurança que irão interferir em todos os ambientes e processos, tendo a possibilidade de redirecionar os planos de acordo com as mudanças físicas, tecnológicas e humanas que inevitavelmente ocorrerão.

Organização do Security Officer

Esta ocupação deve existir oficialmente na empresa cujas responsabilidades e habilidades estejam diretamente associadas à liderança do Comitê Corporativo de Segurança e à interação com os líderes dos Comitês Interdepartamentais de Segurança. Perfil técnico aprofundado, visão corporativa e destreza para gestão são elementos fundamentais para que haja uma canalização de esforços de forma coerente com os macro objetivos da segurança e do próprio negócio. A propósito, negócio e segurança devem coexistir em harmonia, onde o primeiro aponta as carências, estratégias e necessidades de novas aplicações, e o segundo se empenha em reduzir os riscos e o potencial de impacto através de controles bem empregados corporativamente. O Security Officer tem de ser mediador, orientador,

questionador, analisador de ameaças, riscos, impactos, e do consequente estudo de viabilidade dos próximos passos.

Organização de Comitês Interdepartamentais de Segurança

Com uma esfera de abrangência menor, estes comitês tem importante papel no modelo de gestão de segurança da informação. Apesar de estares sendo orientados por diretrizes maiores na esfera do Comitê Corporativo de Segurança, estes deverão medir os resultados dos ambientes específicos, reportas novas necessidades e situações que exponham a informação.

Depois de explicitados acima os fatores críticos de sucesso dentro do modelo de gestão corporativa da segurança da informação, podemos didaticamente sintetizar a estrutura proposta através da expressão: ação local orientada por visão global.
Diante disso, imagino que perceba a partir de agora o quão necessário é a aplicação desse modelo em seu negócio, o que torna conveniente uma frase de estímulo: "Plano Diretor de Segurança: você também pode!"

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