31 – Março de 2001

Equacionando a gestão de riscos

Lecionando a cadeira de Segurança da Informação em cursos Master in Business Administration (MBA), onde o grande público possui perfil executivo ou empreendedor, sou freqüentemente questionado sobre os desafios da segurança, a solução mais adequada, e principalmente sobre a possível existência de uma equação que viabilize a gestão de riscos.

Não é tarefa das mais fáceis encontrar uma resposta padrão que equacione e solucione definitivamente o problema, afinal segurança total inexiste. Mas acabamos por não fugir de premissas há muito validadas, que hoje sustentam com sucesso iniciativas corporativas de segurança da informação.

Sabemos que cada tipo de negócio, independente de seu segmento de mercado e seu core business, possui dezenas, talvez centenas de variáveis que se relacionam direta e indiretamente com a definição do seu nível de segurança mais adequado. Identificar estas variáveis passa a ser a primeira etapa do desafio.

Adotando analogicamente o exemplo do médico, o negócio deve passar por uma análise contextualizada antes que se possa especificar um tratamento medicamentoso a fim de solucionar sua enfermidade. É justamente a fase do diagnóstico que será capaz de identificar as ameaças internas e externas, as vulnerabilidades físicas, tecnológicas, e humanas, e os possíveis impactos financeiros, operacionais e morais.

Já possuíamos subsídios para esboçar a equação.

Risco = Ameaças x Vulnerabilidades x Impactos

Façamos uma breve análise dos termos antes mesmo de voltarmos a discutir o desafio da segurança agora equacionado.

Ameaça

Atitude ou dispositivo com potencialidade para explorar e provocar danos à segurança da informação, atingindo seus conceitos: Confidencialidade, Integridade e Disponibilidade.
Consultando a definição no dicionário, encontraremos: “Ameaça: palavra, gesto ou sinal indicativo do mal que se quer fazer a alguém; prenúncio de um mal ou doença; advertência;”. Exemplos: concorrente, sabotador, especulador, hacker, cracker, erro humano (deleção de arquivos digitais acidentalmente etc), acidentes naturais (inundação etc), funcionário insatisfeito, técnicas (engenharia social, trasing etc), ferramentas de software (vírus, sniffer, trojan horse etc).

Identificar as ameaças é fator crítico de sucesso para a correta dimensão do risco e principalmente para a modelagem de uma solução de segurança corporativa personalizada, afinal, como se defender do que não se conhece?!

Vulnerabilidade

Evidência ou fragilidade que eleva o grau de exposição dos ativos que sustentam o negócio (infra-estrutura física, tecnologia, aplicações, pessoas e a própria informação), aumentando a probabilidade de sucesso pela investida de uma ameaça.
Resgatando o termo em dicionário, encontraremos: “Vulnerabilidade: qualidade de vulnerável. Vulnerável: que, ou por onde, pode ser ferido; diz-se do ponto fraco de uma pessoa, coisa ou questão;”. Exemplos: falhas de infra-estrutura física (carência de mecanismos de controle de acesso físico na sala dos servidores etc), falhas tecnológicas (configuração inadequada do firewall, erros em projeto de software básico Sistemas Operacionais etc), falhas de mídias (fitas de backup impróprias para restauração por deterioração etc); falhas humanas (ausência de conscientização provocando displicência ao criar e manter em sigilo a senha pessoal etc).

Impacto

Resultado da ação bem sucedida de uma ameaça ao explorar as vulnerabilidades de um ativo, atingindo assim um ou mais conceitos da segurança da informação.
Em mais uma consulta ao dicionário, encontraremos: “Impacto: choque; embate; encontrão; colisão entre dois corpos, com a existência de forças relativamente grandes durante um intervalo de tempo muito pequeno; abalo moral por um acontecimento doloroso ou chocante; impressão profunda provocada por ocorrência grave ou inesperada;”. Exemplos: prejuízo financeiro, perda de competitividade, perda de mercado, danos à imagem; depreciação da marca, descontinuidade etc.

Conclusão

Agora que já equacionamos o risco com a identificação das variáveis, precisamos ratificar que a gestão corporativa da segurança da informação deve estar sempre orientada a considerar as particularidades de cada negócio, em busca da implementação de controles que reduzam os riscos - fazendo-o tender à zero – e da eliminação e administração das vulnerabilidades dos ativos, evitando assim que as ameaças as explorem gerando impactos e comprometendo o negócio.

Diante disso, antes mesmo de traçar a estratégia de segurança e os planos de ação, dedique um bom tempo para analisar o contexto em que seu negócio opera, identifique as variáveis internas e externas, aspectos físicos, tecnológicos e humanos, sua sensibilidade diante de possíveis impactos, para só então iniciar a modelagem uma solução corporativa de segurança da informação sob medida, eficiente e capaz de proporcionar o melhor retorno sobre o investimento.

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