41 – Junho de 2002

Você já fez uma análise de riscos de verdade?

Esta pergunta talvez o tenha surpreendido, assim como provavelmente tenha feito com alguns dos responsáveis pela segurança da informação. Pode ter provocado uma sensação de dúvida ou desconfiança junto ao Security Officer, ao Diretor de Tecnologia, ao administrador de rede ou até mesmo pode ter tirado os analistas de segurança da zona de conforto.

Gosto muito do aprendizado com base nos questionamentos. Normalmente nos fazem enxergar o que está debaixo dos nossos narizes ou, em outra hipótese, nos fazem pensar em algo que estava aparentemente resolvido em nossas mentes. Por exemplo, algum problema que julgávamos ter solucionado ou assunto para o qual nos víamos como conhecedores e competentes para executá-lo com sucesso.

A análise de riscos é provavelmente um dos temas a provocar tal sensação. Em alguns casos, por desconhecimento ou conhecimento superficial da matéria. Em outros, por falta de informação especializada para estar certo da resposta. Os motivos não importam. O fator relevante é possuir subsídios que permitam escolher a melhor opção e assim assumir uma posição diante do questionamento.

Análise de vulnerabilidades é a expressão mais encontrada nos anúncios de serviços, nos livros puramente técnicos e talvez, pela pré maturidade do mercado de segurança, acabe sendo a mais adotada por dezenas de empresas de segurança com a promessa de mapear os riscos da empresa. Estamos diante do primeiro possível engano. Afinal, será que por trás desta expressão oferecem realmente o que você espera receber? Será que o que receberá condiz com as reais necessidades da sua empresa ou do perímetro que será alvo do serviço?

Infelizmente a resposta é não. Normalmente, os serviços de análise de vulnerabilidades são baseados nos ativos tecnológicos, ou seja, têm como alvo o perímetro de rede com seus servidores, sistemas operacionais, serviços eletrônicos e equipamentos de conectividade. E, pior, muitos apenas aplicam ferramentas de software, scanners que automatizam o trabalho de varredura à procura de falhas de segurança catalogadas em uma base de dados nem sempre atualizada, e emitem um relatório profundamente técnico e, principalmente, não contextualizado ao linguajar e às necessidades do negócio.

Tantos pontos negativos não implicam no desprezo pela análise. Ela tem seu papel dentro do modelo de análise de riscos, mas temos de ter em mente que representam apenas uma fatia de todo o trabalho de diagnóstico de segurança.

É bem verdade que os ativos tecnológicos vêm ganhando importância crescente e aplicabilidade exponencial nas empresas, sustentando processos importantes e inerentes ao core business, mas não esqueçamos das vulnerabilidades físicas e humanas que ficarão de fora. Afinal, o gestor está mais preocupado com a disponibilidade do servidor XPTO ou com o processo de atendimento ao cliente? É medido pela eficiência do bloqueio do

firewall ou pela rentabilidade do portal Internet? Tem como objetivo maior garantir a atualização dos sistemas operacionais ou atingir as metas de faturamento da empresa?

Executar uma verdadeira análise de riscos é transcender os aspectos puramente tecnológicos e realizar o mapeamento dos seus processos de negócio, seus planos estratégicos e seus valores. É identificar as características físicas, tecnológicas e humanas que suportam e mantêm a empresa ativa. É estar orientado por uma metodologia de análise subsidiada por uma base de conhecimento viva, munido de ferramentas e profissionais voltados a diagnosticar as ameaças e os riscos que efetivamente oferecem perigo à continuidade operacional. É oferecer como resultado um diagnóstico guiado pelo negócio e para o negócio, coerente com os anseios dos executivos, com um plano de ação priorizado para os gestores e informações operacionais para os técnicos.

É praticamente uma equação matemática em que o resultado é o produto de uma base de conhecimento técnico dinâmico; pesquisadores que mantêm a base atualizada; uma equipe de profissionais preparados para agir tecnicamente, mas orientados por necessidades mapeadas no negócio; metodologia de execução de projetos com processos certificados em qualidade e em conformidade com a norma internacional BS7799; completada com ferramentas de software que dão performance às atividades rotineiras sem impedir a personalização dos resultados.

Para auxiliá-lo a avaliar se o serviço que eventualmente executou ou que contratou de terceiros, se parece mesmo com uma análise de riscos, preparamos este teste em forma de checklist. Respondendo afirmativamente todas as perguntas, você terá obtido verdadeiramente um resultado de diagnóstico de risco ao negócio, portanto, terá realizado um investimento coerente com o modelo de gestão de segurança da informação.

- Promoveu um encontro inicial, envolvendo gestores e técnicos, com o objetivo de criar sintonia quanto aos conceitos de segurança, métricas e a metodologia de trabalho?
- Realizou uma reunião de planejamento, onde foi mapeada a representatividade dos equipamentos e usuários para identificar o percentual de amostragem da análise e construído um cronograma de trabalho detalhado?
- Realizou entrevistas com o corpo executivo a fim de medir a relevância dos processos de negócio que fazem parte do escopo do trabalho?
- Realizou entrevistas com o gestor de cada processo de negócio envolvido, a fim de identificar os ativos físicos, tecnológicos e humanos que o sustenta?
- Aplicou uma metodologia de execução de projetos consistente e em conformidade com a norma internacional BS7799?
- Realizou visitas físicas ao ambiente operacional a fim de mapear vulnerabilidades relacionadas, por exemplo, a incêndio, cabeamento estruturado, aterramento, acesso físico etc?
- Contou com uma equipe mista de profissionais especializados nas diferentes tecnologias presentes no escopo da análise?
- Contou com uma base de conhecimento rica e dinâmica para subsidiar as ações de análise técnica dos profissionais?

- Contou com ações presenciais de técnicos especialistas em busca das falhas técnicas de segurança mais recentes, mesmo quando estes se utilizam eventualmente de ferramentas de análise de vulnerabilidades rotineiras para aumentar a performance?
- Obteve como resultado um mapeamento classificado dos riscos ao negócio seguidos de recomendações?
- Obteve como resultado múltiplas visões do diagnóstico adaptadas aos diferentes perfis da empresa: executivo, tático e operacional?
- Obteve como resultado um plano de ação priorizado pelos valores do negócio, que organize atividades modulares em um formato que sirva de instrumento tanto para o gestor quanto para o técnico?

Não há outro motivo para a análise de riscos existir, senão dar ciência do nível de segurança e risco do negócio para todos os níveis corporativos, e fornecer os instrumentos necessários para promover os desdobramentos que conduzam a empresa para as fases de especificação, implementação e administração da segurança.
Talvez agora já tenha a resposta. Você já fez uma análise de riscos de verdade?

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