60 – Agosto de 2004

Pareto e a Segurança

O cientista italiano Pareto descobriu no século passado, uma relação de causa e efeito em que 80% dos resultados são gerados por apenas 20% do esforço. Pode parecer irreal, mas o tempo e os exercícios contínuos com os números foram mostrando aos gestores que 20% dos vendedores de uma empresa geram 80% das vendas; 20% dos clientes são responsáveis por 80% da receita ou que 20% dos produtores rurais de uma cidade geram 80% da produção.

A importância de Pareto para a Segurança está associada à grande dimensão do esforço necessário para reduzir e administrar continuamente os riscos da informação. Apesar das vulnerabilidades físicas, tecnológicas, humanas e processuais crescerem e se renovarem diariamente, o montante de investimento compatível com o valor do bem que se quer proteger, ou simplesmente disponível, é finito.

Essa limitação é real e os problemas são muitos além de heterogêneos, portanto, o grande e atual desafio dos Chief Security Officers e das Consultorias especializadas, é a estrutura de suporte ao processo decisório que definirá o que deve ser postergado, o que deve ser priorizado e até mesmo, o que deve ser esquecido e não poderá ser atendido pelos investimentos.

É uma situação difícil, sem dúvida, mas a busca cega pela excelência teórica baseada apenas em normas internacionais e melhores práticas, devem ceder à necessidade prioritária de gerir baseando-se nos interesses do negócio. O ato de investir em segurança da informação deve ser conduzido com a mesma seriedade com que um executivo decide ampliar sua linha de produção ou automatizar sua força de vendas, ou seja, pensando no resultado. Não faz sentido algum investir tempo, dinheiro ou recursos de qualquer natureza, que valham mais do que o próprio bem protegido. Não faz sentido realizar ações em processos longos de análise de segurança se eles não puderem orientá-lo a corrigir falhas com velocidade. Não faz o menor sentido despender esforço para obter a certificação BS7799, por exemplo, se os maiores problemas que comprometem a confidencialidade, integridade e a disponibilidade de suas informações, continuam sendo o vírus, o perímetro Internet, sua infra-estrutura elétrica e a conduta de seus funcionários. É como preparar um automóvel para uma viagem dura de 2.000km instalando pneus reservas, piloto automático, peças sobressalentes para o motor e sistemas de posicionamento global, e esquecer de abastecer o tanque de combustível.

A regra de Pareto deve nortear executivos de segurança e consultorias, pois tempo e dinheiro são finitos, mas os problemas não. Decidir o que é prioritário, o que é mais representativo para a natureza do negócio, avaliar o que é mais relevante, contextualizar as falhas e identificar as ações que representam os 20% de esforço que proporcionarão 80% do resultado.

Investimento inteligente é a chave que pode tirar das costas o peso do investimento que não consegue ser medido; dos projetos que geram apenas belos e pesados relatórios; da busca inconsistente pela certificação; da solução apenas academicamente perfeita e da especificação de políticas de segurança enlatadas e utópicas. Mesmo aplicado à segurança, estamos falando de investimento que, como em qualquer outra situação, deve estar orientado aos interesses do negócio e de seus gestores, proporcionando a geração de mais dinheiro, a redução de perdas e a redução dos riscos de responsabilização.

Considerações para apoiar o processo de decisão e maximizar os investimentos em segurança da informação:

- Considerar os requisitos do negócio (natureza das atividades, sensibilidade, tolerância, criticidade);
- Considerar os planos de negócio de curto, médio e longo prazo (plano de desenvolvimento e investimento);
- Considerar a relevância dos processos para o negócio (relação direta e indireta com os resultados financeiros);
- Considerar a percepção de prioridade dos ativos da informação (dependência dos processos de negócio);
- Considerar as limitações técnicas, temporais, financeiras, legais e outras específicas (regulamentações setoriais, Constituição, plataformas tecnológicas etc);
- Considerar risco inerente, risco presente e risco residual (configuração de risco previsível, risco atual e risco final ou desejável);
- Considerar a situação atual e situação desejada (nível de segurança ideal para o contexto do negócio: compatibilidade de investimento e tolerância), e
- Considerar um modelo de maturidade (acompanhamento de indicadores e medição dos resultados para retro-alimentar o processo de gestão de riscos).

Marcos Sêmola *é SAM Security Consulting Manager da multinacional Atos Origin, Consultor Sênior em Gestão de Segurança da Informação, CISM – Certified Information Security Manager, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus e eleito pelo prêmio SecMaster, Profissional de Segurança da Informação de 2003 cat4.*
marcos@semola.com.br