72 – Janeiro de 2006

Segurança Tolerância Zero

Tolerância parece ser a palavra perfeita para nos ajudar a entender os desafios da segurança da informação. Existindo a situação de exposição ao risco, por conseqüência da existência de falhas potencialmente exploráveis por ameaças, o fator de tolerância entra em ação para ponderar e determinar que contramedidas devam ser tomadas.
Neste momento, deve-se fazer uso de uma árvore de decisão de risco baseada no contexto:

1. Rejeitar: esta opção deve ser considerada quando o risco não está sendo considerado pela estratégia do negócio, uma vez que o custo do controle, ou da contramedida, é superior ao risco ou ao bem a ser protegido.

2. Aceitar: esta opção deve ser considerada quando o risco é inerente à natureza e ao modelo de negócio, fazendo parte das operações normais e, portanto, tendo sido previsto na estratégia. A escolha dessa opção gera um outro nível de análise:

    a. Evitar: esta decisão se baseia na vontade e viabilidade de se eliminar totalmente a fonte de um risco específico.

    b. Transferir: esta decisão se baseia na relação custo-benefício e na viabilidade (disposição e capacidade financeira) de terceiros, para assumir o risco.

    c. Explorar: esta decisão se baseia no interesse e na possibilidade de se obter vantagens competitivas pelo aumento da exposição e do grau de risco.

    d. Reter: esta decisão se baseia no interesse do negócio, considerados custo e tolerância, de garantir a manutenção da exposição e do grau de risco.

    e. Mitigar: esta decisão se baseia na necessidade do negócio, considerados custo e tolerância, de diversificar, controlar e reduzir os riscos.

Pode parecer um elemento secundário, mas na verdade, o fator de Tolerância é determinante para que se definam investimentos compatíveis com o bem a ser protegido e principalmente, para que o nível de risco residual esteja dentro da zona de conforto.

Um exemplo rico e atual de gestão de riscos da informação baseado na tolerância, pode se obtido ao analisarmos a segurança dos Jogos Olímpicos de Inverno que se iniciarão na segunda semana de Fevereiro de 2006, em Torino, Itália.
Trata-se de uma competição esportiva de caráter mundial e de curta duração (17 dias). Onde 2.500 atletas de 85 países estarão disputando medalhas por 7 esportes diferentes, distribuídos em 8 sites de competição que incluem ginásios, estações de ski, pistas de alta velocidade etc. Cercados e monitorados por mais de 10.000 jornalistas de todo o mundo e, portanto, representando um ambiente de alta complexidade sob o ponto de vista tecnológico e de tolerância zero, sob a ótica da segurança da informação.

É sem dúvida um cenário crítico como num quebra-cabeça de centenas de milhares de peças em que cada uma desempenha um papel importante. Analisando a competição como o negócio que é, sua tolerância à falha é baixíssima, pois além de representar uma peça chave na cadeia produtiva que se forma ao redor do evento, as competições por si só não permitem uma segunda chance.

Enquanto os atletas, representando seus países, precisam ter garantido o acesso aos ambientes de treinamento, precisam ter seus equipamentos guardados em segurança e sua alimentação fornecida íntegra e no tempo programado, por exemplo, o público precisa ter acesso a um ambiente seguro de venda de ingressos. Que por sua vez precisa seguir um fluxo de confirmação de pagamento, entrega dos bilhetes e finalmente a garantia de que estará autorizado a entrar no site de competição no dia e horário marcados. Como se não bastasse, os bastidores dos jogos revelam ainda maior complexidade, dada pela intolerância das competições em se perder o sincronismo do cronômetro, que por sua vez está associado ao placar, está ligado aos juízes, alimenta a tabela de classificação dos competidores, e por fim, fornece informações dinâmicas aos jornalistas e a imprensa mundial em frações de segundos.

A velha brincadeira de empilhar dominós simboliza muito bem a criticidade do ambiente. Por tudo isso e muito mais que não pôde ser detalhado, processos robustos de monitoramento, identificação de falhas, segregação de ambientes, resposta a incidentes e administração de crise, devem ser adotados para compatibilizar o grau de risco ao nível de tolerância do evento. Este fator de tolerância é responsável por orientar decisões que ocorreram desde a fase de definição da arquitetura de rede, por exemplo.
Em ambiente de tolerância zero, as falhas na camada do negócio não são esperadas, por isso, evitar o risco deixando de fora uma tecnologia imatura, por exemplo, é uma decisão sábia. Definir configurações conservadoras, estabelecer perímetros físicos e lógicos segregados, estruturar níveis consistentes e limitados de permissão de acesso, bem como adotar processos de filtragem, avaliação e classificação de alertas também fazem parte de uma estratégia inteligente de eliminação de problemas. Além de tudo isso, testar é a palavra chave. Assim, centenas de cenários de crise devem ser imaginados, documentados e seus planos de mitigação e continuidade, testados exaustivamente até que a estrutura esteja pronta para reagir à qualquer potencial problema de segurança. Tudo isso para que nós expectadores, só nos preocupemos em torcer pelos atletas, em celebrar as medalhas e acompanhar mais uma bela edição dos Jogos Olímpicos.

Marcos Sêmola *é Consulting Business Development da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC e do Computer Security Institute, Professor da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus, autor de outras duas obras ligadas à gestão da informação pelas editoras Saraiva e Pearsons e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003/2004. Visite www.semola.com.br ou contate marcos@semola.com.br*