61 - Setembro de 2004

Security Scorecard e a Fórmula 1

Poder monitorar o nível de risco e medir a eficácia dos controles de segurança adotados pela empresa parece ser o desejo de 11 entre 10 gestores de segurança da informação. Não é por menos. A partir do momento em que as ações de segurança tiveram de estar aderentes aos interesses, e especialmente à estratégia do negócio, medir a maturidade dos processos de gerenciamento de riscos da informação e mensurá-los em uma escala de maturidade passou a ser instrumento de sobrevivência para empresas e seus gestores.
Nem todos os controles são importantes ou aplicáveis, pois os negócios têm natureza distinta e particularidades físicas, tecnológicas e humanas que os tornam diferentes o bastante para precisarem acompanhar seus próprios indicadores. Desta forma, identificar o que é mais relevante para o negócio, definir seus indicadores estratégicos e em seguida descobrir os controles mais técnicos que irão alimentar estes indicadores, é o que precisa ser feito para se fomentar o que convencionei chamar de Security Scorecard ou simplesmente Painel de Controle da Segurança.

Aproveitando a expressão, podemos fazer uma analogia com um carro de Fórmula 1. Considerando a natureza de uma corrida de alta velocidade, o tipo de pista, as características das curvas, dos pontos de alta e baixa velocidade, o número de voltas, e até mesmo o estilo do piloto, a equipe precisa monitorar certos indicadores do carro que lhes darão insumos para decidir por uma parada, um reparo, uma nova regulagem de aerofólio, uma troca de pneus ou até mesmo a mudança de estratégia. Contudo, sem que sensores múltiplos tivessem sido adequadamente instalados no carro, não existiriam indicadores a serem monitorados, pois simplesmente, estes não seriam alimentados, não receberiam informações que permitissem gerar estatísticas e perceber situações de risco antes que eles se concretizassem ou se maximizassem. Perceber um superaquecimento no motor antes que sua performance seja afetada ou simplesmente quebre, é fator crítico para as equipes de corrida, entretanto, saber que o espelho retrovisor quebrou após uma ultrapassagem, pouco importa para o resultado e os objetivos do negócio: a vitória.

Cada empresa precisa identificar seus indicadores mais críticos e a partir deles, instalar sensores que os suportem. A evolução tecnológica aplicada às corridas de velocidade, nos mostra que os sensores foram sendo instalados gradativamente à medida que novas ferramentas e modelos matemáticos foram sendo desenvolvidos em busca do aumento da competitividade. Na década de 80, um carro de corrida vinha aparelhado com cerca de 15 sensores capazes de identificar a temperatura do motor, dos freios, a taxa de compressão, etc. Hoje, já são mais de 100 sensores distribuídos em mais de um quilômetro de cabos que não só indicam a saúde do motor como um todo, como também acompanham a eficiência de seus principais componentes, como a vela de ignição, além de muitos outros equipamentos de apoio. Para completar a comunicação com o carro feita por telemetria, a comunicação com o piloto já ocorre em tempo real, garantindo que na ausência de alguns sensores (ainda não desenvolvidos), o próprio piloto possa fornecer informações sobre o

comportamento do carro de modo a suportar decisões de sua equipe, como um verdadeiro sensor, humano.

É justamente o que ocorre com as empresas. Por conta da competitividade crescente do "campeonato", da heterogeneidade física, tecnológica e humana das "corridas" das quais participam diariamente, e principalmente, em função do tempo que se dedicou ao desenvolvimento de seu "carro de corrida", a realidade de dispor de um completo painel de controle de segurança parece distante. Algumas empresas sequer atingiram a maturidade para entrar em um campeonato tão veloz ou ainda estão tentando fazer seu carro durar o bastante para completar uma única volta. Entretanto, muitas outras já completam a corrida e algumas delas disputam de igual para igual e começam a buscar algo que as diferencie das demais para vencer. Para todas essas, incrementar os sensores, depurar os indicadores e ampliar o seu potencial de monitoramento é peça chave para garantir sua sobrevivência.

Qualquer que seja o porte e a situação da sua empresa, siga este caminho:

1. Identifique os requisitos de segurança baseando-se na natureza da atividade e nas características de seus processos de negócio e ativos.
2. Como em um carro, defina os indicadores que são críticos para o seu funcionamento e que, portanto, merecem ser monitorados.
3. Adote sensores físicos, tecnológicos e humanos, que sejam aplicáveis, e garanta que os mesmos alimentem os indicadores de monitoramento dentro de necessidades particulares de periodicidade.
4. Procure centralizar o controle de todos eles em um único ponto ou permita uma visão integrada de todos os indicadores.
5. Aos poucos, com a ampliação dos limites financeiros, temporais ou quaisquer outros que tenham limitado sua atuação até então, adote novos controles seguindo sua lista de criticidade e mantendo-os centralizados.
6. Se todas essas etapas forem seguidas, você já terá uma estrutura de painel de controle da segurança. O tempo lhe dará maturidade de gerenciamento.
7. A maturidade lhe permitirá depurar os sensores, interpretá-los dentro de métodos e escalas próprias de análise, adotar sensores complementares e até mesmo fazer correlação de sensores para extrair deles, informações novas que apóiem decisões e reações mais ágeis e precisas.

Depois de tudo isso, quando o trabalho parecer ter chegado ao fim, você perceberá que algo deverá ter mudado. Sejam aspectos físicos, tecnológicos e humanos da infra-estrutura que suporta o seu negócio, sejam aspectos externos como a política econômica, seu mercado ou seus competidores, qualquer um deles o motivará a rever os requisitos de segurança do negócio, voltando ao passo 1, e assim entrar no ciclo dinâmico do sistema de gestão de segurança da informação. Boa sorte.

Marcos Sêmola *é South America Security Consulting Manager da multinacional Atos Origin, Consultor Sênior em Gestão de Segurança da Informação, CISM – Certified Information Security Manager pelo ISACA, BS7799 Leader Auditor pelo BSI, Membro do Computer Security Institute, 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