Por Alexandre Finelli

Segundo o relatório Midyear Security Year 2015, mais de 19 bilhões de ameaças são bloqueadas diariamente. Este montante é consequência das centenas de milhares de malwares que são criados todos os dias a fim de burlar as atuais técnicas de defesa corporativas. Diante de um cenário tão ameaçador, cabem às organizações estabelecer novas políticas internas, governança e compliance para reduzir o tempo de detecção e minimizar os danos causados pelos ataques, cada vez mais agressivos.

O tema em questão será um dos destaques no Security Leaders Fórum Belo Horizonte, que acontecerá em breve, 02 de setembro, no Ouro Minas Palace Hotel. Para debater este assunto, Afonso Kalil, profissional com mais de 40 anos de experiência em governança de TI, segurança e risco, com passagens pelo Banco Central, Bank Boston, Fiat, entre outras corporações, estará presente e comenta, em entrevista exclusiva à Risk Report, como as empresas devem agir diante do atual cenário de cibersegurança e sugere que as políticas sejam totalmente revisadas e atualizadas com foco expressivo nos fundamentos básicos de controles internos.

Risk Report: O quanto as políticas atuais, inclusive de compliance, precisam ser repensadas, já que foram concebidas em um cenário diferente?

Afonso Kalil: Devem ser totalmente revisadas e atualizadas com foco expressivo nos fundamentos básicos de controles internos que, na sua essência, é a base para todas as demais gestões em um ambiente informatizado: gestão da governança, riscos, conformidade, Segurança da Informação, crises e continuidade de negócios.

As políticas devem enfatizar de modo claro os graus de responsabilidade de cada gestor nos diferentes níveis hierárquicos da empresa em relação à qualidade e pertinência dos controles em cada disciplina, as suas medições periódicas, o monitoramento constante dos resultados, a análise dos eventuais desvios e o estabelecimento de planos de ação para minimizá-los ou eliminá-los.

Todos os processos e respectivos controles utilizados para monitoramento devem ser considerados nas políticas, formalizados e aprovados nos níveis competentes a fim de dirimir quaisquer dúvidas sobre os resultados das avaliações periódicas decorrentes e o “conhecimento prévio” dos problemas mais sérios por parte da Direção.

As políticas normalmente se prendem às normas, diretrizes e procedimentos sendo, na sua grande maioria, omissa quanto aos controles necessários para que o gestor possa avaliar a qualidade da aderência das operações do “dia a dia” principalmente para as situações de exceção.

O cenário atual exige que todos os gestores e diretores de uma empresa tenham muito mais do que o simples entendimento e conscientização das políticas. Exige-se o comprometimento enraizado – até mesmo obstinado – sobre a existência de relevantes e adequados controles internos e a constante vigilância para que eles sejam efetivamente exercidos, analisados e seus resultados convenientemente tratados.

RR: Um estudo recente constatou que apenas 56% de todos os funcionários das empresas passam por algum tipo de treinamento sobre segurança ou sensibilização quanto à política da empresa. Que tipo de ações práticas as organizações devem adotar para aumentar o nível de conhecimento e consciência dos riscos entre seus colaboradores?

AK: Existem alguns procedimentos muito simples e abrangentes que minimizam bastante os riscos de baixa (ou nenhuma) sensibilização em relação à política de segurança da empresa. Ela deve

estar atualizada (a cada período de 12 meses), aprovada e disponível para todos os usuários. O meio mais barato, eficaz, fácil e rápido é disponibilizá-la na Intranet da empresa com acesso de leitura permitido a todos.

Na admissão ou após a contratação de terceiros, conceder um prazo (uma ou duas semanas) para que o novo colaborador leia e entenda a Política. Ao final deste prazo, deve ser emitido um documento (eletrônico) em que o colaborador alega a ciência do teor do documento. É importante que o enfoque seja mais voltado para o comprometimento do colaborador não só no atendimento às normas como também na sua atitude quando identificar algum desvio. Posteriormente, a cada período (dois anos, por exemplo) o procedimento deve ser repetido para cada colaborador, inclusive para que as alterações e atualizações da política sejam efetivamente conhecidas por todos.

A empresa deve providenciar um programa de educação e treinamento, via computador, com as explicações de cada parte da política com testes sobre cada um dos temas. Cada colaborador deve se submeter aos testes regularmente (cada dois anos, por exemplo) e obter uma nota mínima, estabelecida pela gerência. Paralelamente, a empresa deve disponibilizar cursos presenciais (em diferentes níveis de complexidade) e/ou programas de incentivo / atrativo, tais como “Semana da Segurança da Informação”, peças de teatro sobre o tema, Visuais e banners nos quadros de aviso, distribuição folhetos elucidativos, material de propaganda, etc.

RR: Até que ponto a burocracia é um fator que dificulta a implementação de novos processos, adoção de tecnologias mais recentes e outros procedimentos já que essa área exige um certo dinamismo para manter-se devidamente protegida e preparada para responder aos incidentes?

AK: Burocracia não é de todo um mal desde que ela sirva para ordenar criteriosamente as etapas de um processo. O que dificulta a agilidade e eficácia dos processos é a inadequação ou falta de integração com o negócio da empresa a fim de que as mudanças sejam providenciadas com o menor impacto possível ao negócio.

Uma das ferramentas úteis para eliminar os gargalos e os pontos negativos causados por demora na aprovação de providências é o estabelecimento de processos eficazes de “escalada” e a existência de “janelas” de decisão. Isto vale para qualquer processo.

RR: Tanto bancos como instituições públicas possuem diversos departamentos responsáveis por áreas específicas. Se houvesse uma melhor integração entre esses canais para gerir tantos dados não seria mais fácil elaborar políticas de SI mais efetivas?

AK: Claro que sim. Atualmente, já se fala no BI - IT, isto é, o “Business Inteligence for Information Techonology”. Trata-se da combinação de controles e procedimentos de TI focados nos sistemas aplicativos de negócios. É importante contemplar as áreas de negócio da empresa (Administração, Financeiro, Marketing, Compras, RH, etc.) e manter a integração entre elas de modo que os controles reflitam medições que possam agregar valor ao negócio.

Uma integração já utilizada por algumas organizações na área de controles qualitativos de entrega de serviços é o SLM (Service Level Management), que combina todos os SLAs (Service Level Agreements) dos diversos serviços disponibilizados para uma determinada área de negócio pelos fornecedores, sejam estes internos ou externos.

Além disso, existem ERPs que, na sua essência, são voltados para a integração planejada de recursos, no caso, incluídos os dados de negócio. As políticas de acesso aos ERPs são baseadas em diversos perfis com diferentes poderes de acesso para um controle mais eficaz do poder total de acesso concedido a uma só pessoa (princípio da separação de responsabilidades). Entretanto, nem todas as empresas possuem sistemas com tal integração, devido ao alto custo e complexidade de

implantação e manutenção.

Em relação às instituições financeiras o SPB (Sistema de Pagamentos Brasileiro) eliminou diversas lacunas de controles e estabeleceu um dos sistemas mais considerados no mundo na área bancária.

Entretanto, existem canais que ainda não são contemplados por estas tecnologias em termos de integração. Por este motivo, mais uma vez se faz necessário salientar a importância de controles internos específicos para minimizar desvios e/ou problemas indesejáveis.

Uma outra ferramenta valiosa é a revisão interna de um Sistema Aplicativo de Negócios, sob o foco do Proprietário do Sistema. Isto significa a revisão dos acessos, da documentação disponível, das funções do sistema, seus controles internos, os controles de interfaces com outras plataformas de entrada e de saída e a conciliação de totais de controle. Neste caso específico, existem checklists que auxiliam os proprietários e auditores nas revisões destes sistemas de negócios.

Fonte: Risk Report, em 03.08.2015.