Por Pamella Cajano

A cybersegurança nunca foi mais essencial, por pelo menos quatro principais razões. Primeiro, companhias têm mais ativos digitais do que tinham há dez anos, e estes ativos valem mais do que valiam antes. Eles incluem informações pessoais dos consumidores, financeiras e de transações; ativos dos proprietários, incluindo fontes de código de produtos; processos de negócios automatizados; comunicação sensível com fornecedores e parceiros; e outros dados. A segurança em volta desses ativos varia grandemente dependendo do percebido (em oposição ao atual) valor estratégico e financeiro para o negócio, bem como a efetividade da segurança tecnológica e processos no local.

As consequências imediatas para uma companhia que lida com uma falha de dados de consumidores são severas e podem incluir repercussão negativa na imprensa, queda nas vendas e diminuição de preços (pelo menos imediatamente após a falha); ameaças de advogados de clientes e parceiros, além de investigações legais. Quando o ataque gera acesso a fontes de códigos de softwares, os responsáveis podem encontrar e explorar novas vulnerabilidades que podem afetar sistemas corporativos e do consumidor, dados e serviços. Como exemplo da vulnerabilidade digital está a Adobe, que em 2013 sofreu um ataque que resultou no roubo de dados de mais de 38 milhões de consumidores e de fontes de códigos valiosas de alguns dos produtos mais usados da Adobe, como Reader, PhotoShop e ColdFusion.

Para a Bain & Co, muitas organizações falham ao alinharem suas segurança de T.I. com seus objetivos maiores e apetite por risco. Isso acontece quando negócios e T.I. não discutem ameaças emergentes ou a importância relativa de diferentes classes de espaços digitais; desconexões entre os esforços de gerenciamento de risco das organizações e o desenvolvimento de capacidades necessárias de cybersegurança; abordagem inconsistente de planejamento de segurança, operações e financiamento. Estes erros podem criar gaps na estratégia e operação que deixam a organização vulnerável.

Nuvem: Hoje, os dados corporativos e do consumidor residem pertencem tanto aos centros de dados quanto às nuvens públicas e privadas, distribuídos por lugares remotos. Enquanto as arquiteturas de nuvens híbridas oferecem benefícios econômicos significativos, a adoção delas requer uma abordagem mais sofisticada da cybersegurança, incluindo o gerenciamento de segurança no nível de ativos digitais individuais e monitoramento e gerenciamento integrado das capacidades por todo o ambiente da nuvem híbrida.

Uso perverso de dispositivos mobile pelo staff e executivos. Uma pesquisa recente da ISACA descobriu que mais de 66% das organizações vão adaptar em breve políticas traga-seu-próprio-aparelho" (BYOD, na sigla em inglês). Com isso, o T.I. corporativo tem que gerenciar de forma onipresente a segurança de muito mais plataformas e dispositivos, além de gerenciar a identidade do usuário e acesso aos dados sensíveis da empresa.

Compliance: Numa pesquisa recente da Bain, mais de 75% dos CIOs identificaram os requerimentos de compliance como os mais determinantes para investimentos em segurança de T.I. Outra pesquisa recente da ISACA descobriu que fora das obrigações de compliance, o T.I. tem recursos insuficientes e envolvimento limitado do negócio para um efetivo gerenciamento de riscos. Essas descobertas trazem à luz a abordagem operacional de cybersegurança tomada por muitas organizações. Compliance deveria definir o limite inferior de capacidades de segurança enquanto o limite máximo deveria aspirar às prioridades estratégicas da organização, incluindo proteção do IP, contínuas operações e uma repuração de companhia segura, que podem ser resumidos em seis tópicos:

- Proteger seus dados, reputação e negócio;

- Entender os ativos-chave da organização e o apetite por risco;
- Identificar os riscos e gaps de segurança;
- Definir a estratégia de cybersegurança;
- Enfatizar gaps, prioridades e estratégias para o CEO e conselho; e
- Trabalhar com especialistas renomados em segurança.

Fonte: Agência IN, em 27.04.2016.