Por Alexandre Finelli

Diante de um cenário cada vez mais fortalecido por cibercriminosos especializados, a Segurança da Informação está em evidência. Não apenas pela sua importância, mas também pela necessidade de rever suas estratégias centrais para conter o avanço dos ataques cibernéticos e, consequentemente, os prejuízos gerados às organizações. Para isso, é fundamental que as empresas tracem políticas internas mais atualizadas e estratégias de compliance, além de estabelecer novas normas a fim de minimizar riscos e vulnerabilidades. Este foi o tema que marcou o início da segunda edição do Security Leaders Fórum Rio de Janeiro, que reuniu hoje (14) um time de C'levels e especialistas para saber como as organizações estão tratando deste assunto.

Segundo Roberto Engler, IBM Security Systems Brand Manager, o compliance de quatro ou cinco anos atrás cumpria bem seu papel, mas, com a evolução dos ataques, é preciso ter cuidados redobrados. "Há casos em que o compliance cega, porque transforma medidas em checklist e muita coisa acaba sendo deixada de lado, permitindo brechas", explica. Engler ainda ressaltou que, na maioria dos casos, os próprios atacantes têm conhecimento do compliance e sabem como podem aproveitar essas vulnerabilidades.

Na opinião de Julio Urdangarin, diretor de Operações do Iplan, o ano de 2014 foi marcado pelo grande número de ataques com uma característica em comum. "Foi possível perceber que os atacantes se aperfeiçoaram utilizando técnicas já conhecidas", disse. Por isso a importância de conhecer o próprio nível de maturidade dentro de cada organização para diminuir o número de incidentes com ameaças já conhecidas.

De acordo com Renato Marinho, pesquisador da Morphus Labs, anos atrás, todos os métodos eram focados em prevenção. "Inicialmente, empresas implementavam antivírus e firewall, medidas que eram suficientes. Mas hoje, com os ataques mais focados, o modelo de defesa é baseado em sistemas de detecção e reação ao incidente", afirmou. Ter visibilidade em tempo real passou a ser primordial para que a equipe de segurança consiga reagir a um ciberataque.

"É uma questão evolutiva. Tem que haver uma mudança dentro da SI a fim de se tornar mais estratégica e menos técnica, investindo em processos", complementa William Bini, especialista e membro da Coordenação de Planejamento de Segurança da Informações da Dataprev. Além disso, ele destacou que a capacitação precisa ser intensificada, olhando as boas práticas sem deixar de lado as tendências apontadas pelo mercado. "Segurança tem que ser simples. Se você cria muita complexidade, fica inviável", finaliza Vladimir Alem, Security Brand Manager da Dell Software America Latina.

Fonte: Risk Report, em 14.05.2015.