Nove em cada 10 organizações no Brasil foram atingidas por pelo menos uma violação de segurança no ano passado, sendo que a maioria das violações foi classificada como grave, de acordo com o novo relatório divulgado pela CompTIA, associação do setor de TI. O relatório Tendências Internacionais em Segurança Cibernética também revela que as organizações estão alterando as práticas e políticas de segurança devido à maior dependência da computação em nuvem e soluções de tecnologia móvel.

Mais de 1.500 executivos de negócios e de tecnologia em 12 países foram pesquisados. O relatório inclui dados da Austrália, Brasil, Canadá, Alemanha, Índia, Japão, Malásia, México, África do Sul, Tailândia, Emirados Árabes Unidos (EAU) e Reino Unido (UK). No Brasil, 126 executivos foram pesquisados.

A pesquisa aponta que 73% das organizações relataram alguma brecha no ano passado. Na comparação com os demais países pesquisados, o Brasil ficou entre os mais vulneráveis a riscos de segurança. "Apenas 13% das empresas brasileiras afirmaram não ter tido qualquer tipo de experiência com violação de segurança", destacou a executiva de negócios da CompTIA, Tatiana Falcão.

"Nosso levantamento também constatou que 90% das empresas brasileiras esperam que cibersegurança torne-se uma prioridade mais elevada ao longo dos próximos dois anos", disse Tatiana. Ainda segundo a executiva, existe uma forte tendência no País de direcionamento de recursos para o aprimoramento do desenvolvimento profissional dos funcionários.

Cenário nacional

No País, 87% das organizações disseram que experimentaram pelo menos uma violação de segurança cibernética ou incidente nos últimos 12 meses. 81% das empresas brasileiras relatam violações de segurança cibernética relacionadas a dispositivos móveis, tais como dispositivos perdidos, malware móvel e ataques de phishing, além da desativação dos recursos de segurança pelos funcionários. Os erros humanos são os que mais causam riscos a segurança cibernética com 58%, contra 42% de erros tecnológicos.

Mudanças nas operações de TI, quer devido a uma maior dependência da tecnologia móvel, pelo uso de soluções baseadas em nuvem ou algum outro fator, são os principais caminhos para alterar as abordagens à segurança cibernética.

Educação

As organizações estão tomando medidas para avaliar e melhorar o conhecimento sobre cibersegurança entre os seus empregados. As práticas incluem orientação a novos funcionários, programas de formação contínua, cursos on-line e auditorias de segurança aleatória.

Mas os resultados até agora têm sido mistos. Apenas 27% das organizações avaliam sua educação e seus métodos de treinamento como extremamente eficazes. Fazer o treinamento de funcionários ser obrigatório, entregar uma formação mais abrangente e mais frequente, com a combinação de testes e avaliações são algumas das medidas que melhorem a eficácia, disseram executivos.

Os principais pontos que necessitam de atenção na abordagem no Brasil são mudanças nas operações de TI; adquirir conhecimento por meio de treinamento e certificação; foco em uma nova indústria vertical e relatórios de violações na cibersegurança de outras empresas.

Nove em cada 10 executivos e gerentes no Brasil acreditam que é importante testar o funcionário após o treinamento de segurança cibernética para confirmar os ganhos de conhecimento, enquanto que 93% indicam que as certificações para profissionais de TI são valiosas ou muito valiosas como uma forma de validar conhecimentos e habilidades relacionadas à segurança cibernética.

Fonte: Risk Report, em 18.05.2016.