Levantamento global com 500 organizações aponta que as empresas continuam falhando no processo de governança de TI. Pesquisa também revela as principais ameaças, os setores mais vulneráveis e os princípios básicos de segurança

A segurança de dados passou a ser item fundamental nas organizações, principalmente, após as novas ondas de invasões cibernéticas. Casos recentes, como o escândalo do Facebook, mostraram quão desprotegidas estão as empresas no ambiente virtual. Somente no mega-ataque intercontinental de maio de 2017, mais de 1,1 mil computadores no Brasil foram infectados. O dado é alarmante e pode ser explicado por meio do novo Relatório de Ameaças à Segurança 2018, desenvolvido pela consultoria global Protiviti. A pesquisa compartilha as ameaças digitais mais comuns, que desafiam as empresas atualmente.

O relatório é baseado em análises aprofundadas de varreduras de vulnerabilidades e testes de sistemas e infraestrutura de TI em mais de 500 organizações. As análises foram realizadas nos laboratórios de segurança cibernética da empresa nos EUA ao longo de um período de nove anos. A conclusão é a de que as empresas continuam a falhar no quesito governança, quando o assunto é a proteção das operações. Outros aspectos importantes revelados no estudo são:

- Vulnerabilidades facilmente corrigidas não estão sendo feitas em tempo hábil, particularmente dentro dos aplicativos;

- As organizações ainda estão executando um número significativo de sistemas não suportados, aumentando muito o risco de violações;

- Pouco menos da metade das vulnerabilidades identificadas durante o teste têm código de exploração publicamente disponível (a partir do momento do teste);

- Empresas de produtos de consumo, serviços financeiros, saúde e ciências da vida, tecnologia, mídia e telecomunicações, fabricação e as indústrias de energia são as mais vulneráveis.

De acordo com Marco Ribeiro, líder da prática de gestão de risco de TI da Protiviti, a maioria das questões identificadas no estudo pode ser facilmente corrigida de forma proativa e programática. "Infelizmente, o cenário aponta que as ameaças cibernéticas se tornaram perigosas e é apenas uma questão de tempo para as empresas serem atacadas, por isso é importante reforçar a implementação de um programa de segurança da informação imediatamente", afirma o especialista.

Com base na análise, a Protiviti ainda identificou cinco princípios básicos de segurança para garantir a redução do risco de violações, que se adequam às empresas brasileiras:

1. Manter um adequado processo de governança na gestão de identidade para o controle de acesso, atribuindo perfis adequados de acordo com o cargo, além de assegurar o bloqueio de ex-funcionários. A verificação rotineira de acesso diminui os riscos;
2. Conscientizar os funcionários sobre os cuidados para manter um comportamento virtual seguro, evitando a abertura de e-mails e mensagens instantâneas recebidas. São por essas vias que há o maior índice de invasão às redes das empresas;
3. As organizações devem se preocupar em conhecer seu parque de TI e ter um inventário atualizado dos dispositivos que mantêm nas modalidades on premise e na nuvem, para identificar softwares e hardwares obsoletos, buscando mecanismos para atualizar e proteger esses ambientes;
4. Manter políticas e modelos de segurança adequados de acordo com a necessidade da empresa, ou seja, que envolvam todos os dispositivos e ambientes on premise e na nuvem, para garantir que essas políticas não sejam perdidas;

5. Utilizar profissionais especializados em segurança da informação para prestar o serviço de avaliação dos riscos de vulnerabilidades e de testes de invasões reais dentro da rede e do ambiente de TI da empresa.

Fonte: IMAGE Comunicação, em 21.05.2018.