

Por Carlos Henrique Andrade (*)

Segurança da informação é composta por pessoas, processos e tecnologias. Por isso, não basta comprar aquele firewall ou antivírus de última geração se a empresa não for capaz de acompanhar a evolução de ameaças

É fato que a informação tem grande valor para a humanidade e é fator determinante para o fortalecimento de nações e de potências comerciais. Nos dias atuais, o volume de informações alcança proporções astronômicas, assim como aumenta também sua importância e a necessidade de protegê-las. A criação de mecanismos para classificar, avaliar e tratar cada tipo de informação representa direcionar recursos e esforços diferentes para cada uma delas.

Uma pesquisa realizada pela consultoria PwC revela um crescimento de 274% no número de ataques cibernéticos no Brasil. Vimos, desde o começo do ano, ataques a grandes empresas como UOL, Google, divulgação de senhas do governo e até mesmo o Sisu não foi poupado, tendo inscrições de candidatos alteradas. Esses são apenas alguns exemplos de ataques que aconteceram em território nacional.

Sabemos que todas as empresas impactadas por esses ataques possuem grandes soluções de segurança implementadas, times de segurança da informação bem estruturados assim como investimentos consideráveis em segurança. Ao passo que os ataques cibernéticos estão cada vez mais elaborados e sofisticados as empresas, por sua vez, têm de acompanhar esse cenário e desenvolver mecanismos capazes de antecipar esses ataques, bem como reagir de forma adequada para cada tipo de incidente.

Precisamos mesmo ser tão reativos?

Boas práticas não faltam no mercado, assim como soluções tecnológicas complexas e caras, que prometem proteções eficazes contra diversos tipos de ataques e vulnerabilidades. Mas será que somente isso basta? Se temos soluções de alta tecnologia, grandes empresas por trás delas, times de segurança (que deveriam ser bem treinados), bases de conhecimento abertas, por que então em vez dos ataques diminuir eles só aumentam? Ou melhor, por que temos a sensação de que não conseguimos combater ou nos anteciparmos aos ciberataques de forma eficaz?

A resposta é simples: Segurança da informação é composta por pessoas, processos e tecnologias, ou seja, não basta comprar aquele firewall, SIEM, IPS ou antivírus de última geração se a estratégia de implementação, ciclo de vida, sustentação e resposta a incidentes não forem capazes de acompanhar a evolução de ameaças nos dias de hoje.

Muitas empresas montam seus planos e estratégias de proteção baseadas em dados que não refletem o cenário atual de ameaças ou que não endereçam de forma adequada a proteção de pessoas, processos e tecnologias. Implementações de frameworks como ISO 27001, PCI-DSS, HIPAA e SOX não alcançam seu objetivo real se a motivação para os adotar tiver propósito apenas comercial, em vez de ter como objetivo atender ao que cada um desses frameworks se propõe. Implementar uma metodologia de proteção de dados simplesmente porque a empresa terá vantagem comercial não significa dar importância à segurança da informação.

Muitos C-levels enxergam ou investem mais em tecnologias de segurança e menos em campanhas de conscientização ou em processos e controles internos.

Melhores práticas podem ajudar?

Não existe uma receita pronta ou um método 100% eficaz para se aplicar de forma generalizada em todas as empresas ou em seus ambientes, mas de uma forma geral, a definição de uma boa estratégia de segurança começa pelo entendimento correto de seu escopo, ou seja, definir o

alcance real de proteção do que será protegido. Na sequência, análises críticas, de risco e maturidade de processos dará a visibilidade dos principais pontos fracos e fortes de sua empresa.

Com esse mapeamento definido é possível identificar e classificar os tipos de informações a serem protegidas e os níveis de proteção mais adequados para cada uma delas. Otimizando os recursos dessa forma é possível gerenciá-los e direcioná-los de acordo com as necessidades de cada empresa.

Implementar um sistema de gestão de segurança da informação ou algum framework de segurança não impede que incidentes aconteçam, mas endereçam diversas medidas que diminuem suas probabilidades, além de propor métodos capazes de medir se a implementação dos controles e processos adotados são eficazes ou não. Campanhas de conscientização, desenvolvimentos de políticas e procedimentos bem balanceados ainda são os grandes aliados para prevenir incidentes de segurança.

(*) **Carlos Henrique Andrade** é especialista em GRC da [Cipher](#).

Fonte: [Computerworld](#), em 23.06.2017.