Por Cristina Maria de Fiori (*)

Hoje não se discute mais se a sua empresa sofrerá um ataque virtual, mas sim quando isso acontecerá. Os riscos cibernéticos vieram para ficar. Com o uso cada vez mais corrente dos canais digitais, as empresas se tornam alvos altamente expostos às ações de diversas características e naturezas.

O WannaCry elevou o tópico ‘segurança digital’ no ranking de preocupações executivas, afetando mais de 230 mil sistemas ao redor do mundo por meio de técnicas de phishing, como empresas, serviços de saúde, operadoras de telecomunicações, empresas de transporte, organizações governamentais, bancos e universidades, causando um prejuízo de dezenas de milhares de dólares. Mais recentemente, o Petya, outro ransomware, afetou não só os países europeus, e impactou também o Hospital do Câncer de Barretos.

Muitas empresas se enganam ao achar que o seu business não é atrativo o bastante para sofrer ameaças, mas as pesquisas revelam que não existe atividade que não seja sedutora aos vários perfis de agentes criminosos. A motivação deles é variada e extensa, visando à obtenção do acesso a informações de clientes, banco de dados, plano de negócios, senhas e propriedade intelectual.

Existem inúmeros tipos de malwares na prateleira dos hackers: phishing, ransomware, spyware, worm, vírus encaminhados com spams, entre outros. A lista evolui constante e rapidamente, o que requer, como primeira ação, a conscientização de todos os colaboradores sobre, por exemplo, a importância de não abrir e-mails de destinatários desconhecidos ou links e arquivos anexos que pareçam suspeitos. Esses descuidos, aliás, entram no guarda-chuva de ‘ameaças internas’, em que o risco parte de dentro da própria organização, incluindo ainda os ataques propositais, como vazamento de dados.

O desenvolvimento dessa cultura de mitigação de riscos é fundamental, assim como outras formas de recursos para evitar essas situações: criptografia de dispositivos tecnológicos, testes de phishing, melhoria de controle de SPAM, dupla autenticação de senhas para acesso a redes, controle efetivo e rigoroso de acessos e atualização de aplicativos e firmware. Trata-se de um trabalho conduzido por vários departamentos, envolvendo, naturalmente, a área de tecnologia, mas também risco e compliance e outras, dependendo do caso.

Importante mencionar ainda que um programa de cibersegurança efetivo compreende tópicos como governança, compliance, consultoria de risco, segurança de software, gestão de segurança de rede, educação e conscientização dos colaboradores, continuidade do negócio e recuperação de desastres. Também envolve identificação dos dados (quais são, onde estão e como estão protegidos), monitoramento de segurança, governança de identidades e acessos e, dependendo do tipo de empresa, governança global.

Algumas análises podem ainda fazer com que a empresa inteira tenha um entendimento comum sobre ameaças e adversários, assim como estabelece as camadas necessárias para evitá-los ou como se defender, definindo um programa de segurança da informação, política e processos bastante abrangentes, que devem ser ajustados e melhorados continuamente.

Não à toa, a ANBIMA publicou em 3 de agosto de 2016 um Guia de Cibersegurança, com o objetivo de citar práticas efetivas para orientar a implantação de um programa efetivo de segurança cibernética, contribuindo para o aprimoramento da segurança digital no mercado financeiro e de capitais do Brasil. A proposta não é a de exaurir o que pode ser feito em relação ao assunto, mas, antes de tudo, ser um norte para que as instituições possam se programar e se proteger contra estas ameaças que colocam em risco toda a estrutura do negócio.

Dessa forma, muitas instituições aderentes à ANBIMA já estão se adequando e definindo sua política de cibersegurança e procedimentos relacionados, de segurança preventiva ou corretiva. Além disso, está em tramitação o Projeto de Lei 5.276/2016, que dispõe sobre a privacidade de dados e estipula, dentre outros assuntos, a necessidade da proteção dos dados pessoais, medidas de segurança para protegê-los e o que deve ser feito em caso de vazamento. Todo esse cenário já tem se traduzido em ações práticas. Cerca de 40% das empresas listadas da Bolsa de Valores, por exemplo, já incluem em seus relatórios informações sobre investimentos em segurança digital.

As empresas globais já vêm se adiantando e se adequando a esse cenário, garantindo segurança e conferindo tranquilidade aos seus clientes. É nítido o movimento do mercado em se preparar e proteger de forma adequada, seja pela forma de autorregulação ou por iniciativas corporativas internas, ainda que as ameaças desse setor sejam contínuas e evoluam rapidamente.

(*) **Cristina Maria de Fiori** é Gerente de Compliance e do Jurídico na Claritas Investimentos.

Fonte: Press à Porter, em 22.08.2017.