Por Ian Chicharo Gastim

Maioria das companhias afirma que não possui os recursos humanos necessários para prevenir um ataque digital

O ataque de um grupo de hackers, que tirou dor ar as redes de videogame Xbox Live, da Microsoft, e PlayStation Network, da Sony, no final do ano passado, evidencia a necessidade de as empresas possuírem sistemas sólidos de cibersegurança. O objetivo é evitar prejuízos tanto para a imagem, quanto para a manutenção do serviço. Especialistas consultados pelo Estado, no entanto, alertam: a implementação de sistemas de segurança digital em companhias brasileiras está muito atrasada.

De acordo com uma pesquisa da consultoria Alvarez & Marsal (A&M), 60% das organizações brasileiras dizem que não têm os recursos humanos necessários para se proteger ou responder a um ataque digital. Diretor da A&M, William Beer afirma que as companhias, apesar de alguns avanços, ainda não dão a devida importância à cibersegurança dentro das suas estruturas de governança corporativa. "É uma situação confusa. Muitos executivos acham que é somente um problema da área de tecnologia, mas não é."

A pesquisa indicou que 47% das empresas consideram que existe um baixo nível de diálogo entre as equipes de segurança e os líderes empresariais. Segundo Beer, o "Brasil está muito atrasado" na implementação da cibersegurança, o que representa oportunidades para ataques cibernéticos. "O mercado online do País é grande e os criminosos estão vendo que o Brasil não investe em cibersegurança, o que é preocupante. Falta governança para as empresas se protegerem", completa.

PhD em Segurança da Informação, Paulo Pagliusi também afirma que a implementação de sistemas de cibersegurança em empresas brasileiras não acompanha a tendência mundial, o que representa riscos. "Existem várias formas de um ciberataque se concretizar. Além da possibilidade de vazamento de propriedade intelectual, um ataque pode afetar a infraestrutura da empresa, como os sistemas de refrigeração, rede elétrica e internet, prejudicando até a linha de produção", afirma.

De acordo com Pagliusi, uma empresa pode ser alvo, por meses, de um criminoso "profissional", e a defesa, portanto, deve ser preventiva. "É preciso mudar o comportamento dos funcionários em torno da segurança cibernética, envolver toda a corporação, para levantar o nível de maturidade."

Além da necessidade de as empresas ampliarem a segurança digital, William Beer, da A&M, defende que o governo deve reforçar o combate e a prevenção. "O ciberataque é um problema complicado, novo, mas é fundamental e necessário o debate com o governo, que atualmente não tem uma estratégia nacional", afirma.

Para o diretor de Tecnologia da Informação da recrutadora Michael Page, Cristiano Aron, a contratação de executivos para implementar sistemas de cibersegurança deve crescer nos próximos anos. "No ano passado, auxiliamos a contratação de três executivos com foco em cibersegurança. O tema sempre existiu, mas agora está em alta."

"As empresas têm o conceito da segurança digital mais tradicional, como anti-vírus, não a cibersegurança como um sistema sólido", explica Aron.

Marco Civil. Sócio da área de Tecnologia da Informação do Veirano Advogados, Fábio Pereira enxerga que, apesar da cibersegurança ainda não estar enraizada, a tendência é de que empresas passem a tratar esse tema com maior solidez, em virtude de questões como a regulamentação do Marco Civil da Internet. “É importante estabelecer que tipo de padrão de segurança as empresas vão ter de ter quanto à guarda de dados. [Com o decreto federal de regulamentação] vamos ter mais clareza sobre os critérios de segurança e sigilo”, completa.

Apesar do aumento de custos que a guarda de informações representa, Pereira defende que a cibersegurança é vital para a saúde de uma companhia. “Toda empresa sofre ataques e existe uma série de implicações jurídicas. Se forem dados sigilosos, a empresa é responsável perante consumidor e parceiros”, afirma o advogado. “Não é só se preocupar em resgatar os dados em um caso de ataque, pois a empresa também tem responsabilidade em caso de exposição de dados.”

De acordo com a procuradora do Ministério Público Federal, Neide Cavalcanti, que atua no combate a crimes digitais, a regulamentação não pode “burlar normas previstas no Marco Civil” em relação à guarda de dados. Provedores de aplicativos, como o Google, devem guardar dados por seis meses, e de acesso, como a NET, por até um ano. “Para fazer uma investigação, precisamos desses dados devidamente guardados, com segurança e sigilo. Não conseguimos chegar ao autor de um crime cibernético sem eles”, afirma.

Fonte: O Estado de São Paulo, em 17.02.2015.