De acordo com algumas declarações feitas no último dia 10 de junho por Luis Aguilar, membro da Securities and Exchange Commission (CVM), um dos principais reguladores dos Estados Unidos, muitas companhias de capital aberto, que são vítimas de ataques cibernéticos, devem considerar fortemente a divulgação de informações adicionais, além do que é solicitado. Isso vem com a intenção de ajudar a proteger clientes cujos dados privados poderiam estar em risco.

O executivo Aguilar, disse que incentivaria as companhias a irem além do impacto causado no próprio ambiente organizacional; mas ele também considera o impacto que isso pode ocasionar nos outros. Além disso, ele observou que "é possível que um cibertaque não tenha impacto adverso material direto na companhia. Entretanto, um prejuízo pessoal e financeiro de dados poderia ter efeitos devastadores nas vidas dos clientes da organização e de muitos norte-americanos.

**Alertas Sobre Possíveis Ataques Cibernéticos**

Em situações assim, a coisa mais coerente a fazer é emitir a estas vítimas um alerta, para que elas possam se proteger contra possíveis danos. Os comentários de Aguilar surgem na sequência de vários ciberataques contra companhias, incluindo a Adobe Systems e a Target. Vale ressaltar que esses incidentes despertaram debates em Washington entre aplicadores da lei, reguladores e legisladores, sobre como os clientes devem ser alertados, quem deve arcar com o custo dessas falhas, e como tais informações devem ser divulgadas, tanto para o governo como para o público de um modo global.

Além de tudo, Aguilar observou que as empresas precisam ficar mais atentas à supervisão da gerenciamento de riscos, pois as investidas contra o setor corporativo e o nível de comprometimento relacionado às informações dos clientes dessas companhias, está sendo cada vez mais visado. Esse tipo de situação ocasiona danos à reputação das empresas, devido a perda da confiabilidade que seus clientes depositam nas mesmas.

No ano passado, um estudo realizado pela corretora Marsh, divulgado em junho durante evento do setor que ocorreu no Reino Unido, mostrou que 71% das empresas pesquisadas aumentaram seus receios em relação à ocorrência de eventuais riscos cibernéticos na última década. O mais crítico disso tudo, é que 54% das pessoas entrevistadas, afirmou que sua empresa havia sofrido um ataque de crackers recentemente. Enquanto 17% delas estima que as perdas financeiras com um ataque em sua rede possa atingir os US$ 5 milhões, 22% admitiu que sua empresa ainda não possui um estudo para indicar possíveis impactos financeiros no caso de um ataque.

O estudo "Cyber Risk Survey", apesar de ter sido limitado à companhias situadas no continente europeu, enfatiza um assunto que a cada ano ganha mais importância e proecupação, principalmente entre as empresas brasileiras: a Segurança da Informação. A temática que envolve o "risco cibernético" é de tamanha amplitude e abrange qualquer problema que possa ocorrer no ambiente de processamento de dados e tecnologia da informação das corporações, e tem como componentes mais drásticos o roubo ou vazamento de informações, da própria empresa.

Isso envolve desde a lista de fornecedores até às informações comerciais confidenciais, ou mesmo dados de terceiros sob sua custódia, tais como informações pessoais, endereços, dados da conta bancária e do cartão de crédito, que podem cair em mãos erradas, ocasionando perdas milionárias com indenizações e reparações de danos, prejuízo à reputação da companhia, principalmente se envolver o vazamento de dados de clientes, e até mesmo a interrupção temporária de suas atividades.

Além do mais, a importância desse assunto levou as seguradoras a desenvolver, nos últimos anos, seguros em caso de invasão de redes por hackers, violação e vazamento de dados e a eventual paralisação dos negócios. A novidade começa a ganhar impulso no Brasil. Conforme declarou Celso Soares, presidente da Comissão de Linhas Financeiras da Federação Nacional de Seguros Gerais (FenSeg), existe muito mercado para esse seguro entrar em pleno crescimento. E mesmo que as empresas se protejam e invistam em segurança da informação, é lógico que ninguém quer perder negócios por causa de atividades cybercriminosas ou por qualquer outra investida maliciosa proveniente da Web.

**Necessidade de Projetar Sistemas de Segurança mais Sofisticados**

Vale ressaltar que o evento recente de espionagem contra o governo, reacendeu a preocupação das empresas em criar sistemas de proteção mais sofisticados. O assunto sai do plano teórico e começa a se tornar factível, disse Celso Soares. Confirmando seu pioneirismo na venda desse produto no país, a AIG Brasil oferece cobertura contra riscos cibernéticos desde o mês de agosto de 2012. O gerente de linhas financeiras da seguradora, Lucas Scortecci, explica que o produto foi desenvolvido para garantir proteção em duas frentes. De um lado, para indenizar a tomadora em casos onde a invasão de crackers tenha interrompido os processos de prestação de serviços ou a venda de produtos – no caso de um site de e-commerce.

Dessa forma, haveria uma garantia em relação à cobertura de lucros cessantes por interrupção de rede. Ao mesmo tempo, o seguro contemplaria uma cobertura de responsabilidade civil, que permite ao tomador a responsabilidade com o pagamento de indenizações em casos de reclamações de terceiros.

**Ataques Cibernéticos Estão mais Ousados e Inovadores**

Os ataques cibernéticos são cada vez mais destaque nos principais noticiários de tecnologia no mundo inteiro, e o Brasil é um dos países que mais sofre com esse tipo de investida. Dessa forma, a probabilidade de que mais uma empresa, seja ela de qualquer lugar do mundo, a qualquer momento, anuncie aos seus clientes e usuários que o seu sistema foi violado e seus dados estão comprometidos, é enorme. Esses muitos ataques possuem os mais variados objetivos, que vão desde fraudes e espionagem econômica à destruição de informações. Independentemente das razões, esses ataques virtuais estão aparecendo cada vez mais em todos os noticiários e tem deixado os especialistas em segurança bastante proecupados.

E para completar o cenário de preocupações, ameaças e incertezas, o Brasil é uma das principais fontes de ataques cibernéticos do mundo. Para ter uma idéia, só no primeiro trimestre de 2013, o país liderou os registros de ataques devido ao vírus Conficker, sendo esta praga responsável por 26% do total de todas as investidas maliciosas que aconteceram. Em segundo lugar, ficaram os Emirados Árabes Unidos. Em terceiro, a França, com um registro de 11%. Essa análise comprova que os cybercriminosos brasileiros ou os que escolheram o país como alvo, estão cada vez mais perigosos e munidos de técnicas audaciosas e sofisticadas.

**Empresas e a Exposição aos Riscos Provenientes do Cybercrime**

Porém, a grande questão na verdade é: será que as empresas estão atentas aos riscos cibernéticos? De acordo com uma pesquisa realizada há cerca de 2 anos em relação aos riscos cibernéticos, patrocinada pela American International Group (AIG), demonstra que os grandes executivos enxergam tal perigo como uma das principais preocupações empresariais, com grande potencial de perdas, seja no âmbito financeiro ou mesmo na reputação da companhia, o que não é um bom sinal.

Além disso, mais de 85% dos mais de 250 tomadores de decisões pesquisados, disseram que estavam muito preocupados ou, pelo menos, muito mais cautelosos com o problema, em

comparação com a resposta do grupo para seis outras áreas de risco. Isso inclui a perda de renda (82% dos executivos estava muito ou pelo menos um pouco cauteloso), danos à propriedade (80%), e títulos e investimentos de risco (76%).

**Descuidos de Funcionários e Exploração de Vulnerabilidades**

As informações eletrônicas de uma organização, podem ficar expostas por diversos fatores, seja por erro humano, quando os funcionários se descuidam com os dados confidenciais, ou por causa de crackers, que tentam desestabilizar as operações das companhias com um nível de proteção bem abaixo do que o adequado. A Internet, por ser uma rede mundial de computadores, tornou os riscos cibernéticos um problema global. O anonimato é algo utilizado por muitos usuários, que podem estar a quilômetros de distância dos seus alvos, e assim, agir da maneira mais inescrupulosa possível.

**Cybercriminosos são Ávidos pelo Acesso aos Dados Confidenciais**

Vale deixar claro que o conceito mais conhecido quando se fala em dados confidenciais, é o de informações de transações relacionadas com os clientes, tais como informações sobre cartão de crédito ou médicas, em específico, os prontuários. Mas mesmo que a companhia use pouco a Internet, ela pode sim ser alvo de ataques. Esse é o caso de dados dos funcionários, como nome, endereço e números dos documentos de identificação, que são altamente visados pelos cybercriminosos.

Além do mais, esses invasores também estão à procura de dados de inteligência da concorrência, tais como as intenções de uma companhia de fazer uma aquisição, desenvolvimento de produtos novos e principalmente, patentes. Essa violação virou um negócio próprio para o cybercrime, no qual as informações confidenciais roubadas são comercializadas diariamente. Além disso, esses atacantes também são notórios pelas suas habilidade em atender os clientes, oferecendo inclusive, garantias de reembolso para as informações que forem roubadas.

**Estratégias para Lidar com Atividades Cybercriminosas**

Portanto, para que esse problema no cenário cibernético seja minimizado, as empresas precisam, urgentemente, avaliar riscos, além das necessidades e orçamentos, e desenvolver estratégias de gerenciamento e de respostas a quaisquer incidentes. Além disso, é fundamental que os funcionários sejam envolvidos no processo, pois eles precisam saber como agir em casos de ataques cibernéticos, pois os cybercriminosos não escolhem dia e nem hora para atacar.

Exsite ainda um outro fator que as empresas precisam levar em conta, que é em relação à área de tecnologia da informação (TI). É muito importante que esse setor seja sólido e seguro, visto que é o principal meio de defesa da empresa. Dessa forma, a responsabilidade cibernética precisa fazer parte dos planos para mitigação dos riscos; um pacote de seguros cibernéticos ajuda uma companhia a enfrentar a violação de seu sistema, a arcar com os custos de notificação, relações públicas e outros serviços que possam contribuir para mitigar o incidente.

**Cumprimento de Regulações**

Em uma economia global, as empresas multinacionais devem cumprir, de forma rigorosa, com as regulações locais, ainda que suas sedes estejam situadas em outros lugares. Podem abordar adequadamente as questões de regulamentação, as jurídicas, dos investidores e dos auditores, em situações quando o controle de riscos cibernéticos tiver uma abordagem hierárquica, a partir do qual o conselho administrativo reúne um grupo multidisciplinar que estabelece uma estratégia de melhores práticas e mantém o domínio.

E não importa o setor em que atuem; as companhias precisam mesmo prestar mais atenção nos

ataques cibernéticos. As empresas que são capazes de planejar com antecedência, de determinar como vão reagir a um ataque, estarão em melhores condições para proteger seus negócios, se preparar e evitar transtornos. É impossível eliminar as ameaças; então, saber como enfrentá-las e proteger a reputação organizacional, sem prejudicar a inovação e o crescimento dos negócios, deve ser uma questão prioritária. E esse processo começa prestando-se atenção à rápida mudança do panorama dos ataques cibernéticos.

**Fonte**: Under-Linux.Org, em 21.06.2014.