

Especialista fala sobre riscos cibernéticos, principais coberturas e como se prevenir contra ataques

O ataque cibernético em escala mundial ocorrido na última sexta-feira, 12 de maio, quando o conteúdo de milhares de computadores foram sequestrados em troca de resgate, fez ascender a luz vermelha em pessoas e empresas, no Brasil e no mundo, sobre a necessidade de uma maior preocupação com segurança cibernética. Para falar sobre o tema, o Portal da CNseg entrevistou o superintendente de Financial Line & Liability da Argo Seguros, Gustavo Galrão, que também é membro da Comissão de Linhas Financeiras da Fensseg. Confira:

De acordo com estudo do Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD), os incidentes cibernéticos crescem proporcionalmente mais no Brasil que no resto do mundo. As empresas brasileiras estão suficientemente cientes dos riscos e preparadas para lidar com eles?

Gustavo Galrão: Não. Diferentemente de países desenvolvidos, o Brasil carece de cultura de gerenciamento de riscos. A importância dada às ferramentas de gerenciamento dos riscos, tais como o seguro, só aumenta quando há uma experiência pessoal ou quando eventos de grandes proporções são divulgados na mídia.

Porém, vale lembrar que o mercado de seguros para riscos cibernéticos está em fase inicial e possui um enorme potencial de crescimento, haja vista o processo de transformação digital que vivemos e também o aumento de número e tipos de ataques de hackers.

O que verificamos, de um modo geral, é uma baixa conscientização sobre a importância do gerenciamento de risco dentro das empresas brasileiras. O risco cibernético, embora cada vez mais relevante, é algo relativamente novo, tanto para as empresas, quanto para as pessoas. Certamente há um longo caminho em termos de conscientização sobre o risco e o aprendizado das ferramentas eficazes para o tratamento do risco cibernético.

Qual o tamanho do mercado de seguros contra riscos cibernéticos no Brasil? E no mundo?

Gustavo Galrão: O mercado de seguros contra riscos cibernéticos está em franca expansão no mundo devido ao crescimento no número de incidentes, tais como ataques de hackers, e ao aumento da conscientização sobre a importância do gerenciamento deste risco. Nos EUA, por exemplo, a estimativa de mercado atual é de USD 4 bilhões, sendo que, há dois anos, este mesmo mercado era estimado em USD 2 bilhões.

No Brasil, os maiores contratantes de seguros contra riscos cibernéticos são as empresas de tecnologia e as instituições financeiras. Contudo, o interesse das empresas dos demais setores tem crescido consideravelmente e a expectativa é que o mercado cresça significativamente nos próximos anos.

Embora não exista uma mensuração oficial do tamanho deste mercado no país, estima-se atualmente o tamanho do mercado de Responsabilidade Civil Cibernética em torno de R\$ 2 milhões. Todavia, a expectativa é que este mercado supere, por exemplo, o mercado emergente de D&O, que em pouco mais de 10 anos alcançou porte de R\$ 400 milhões em prêmios anuais.

Como é uma apólice padrão de seguro contra riscos cibernéticos? O que cobre e o que não cobre?

Gustavo Galrão: Existem alguns produtos nesse segmento de riscos cibernéticos, como o seguro de Responsabilidade Civil Profissional para Empresas e Profissionais de Tecnologia. Este seguro contratado por empresas e profissionais de TI para transferir riscos relacionados a reclamações de

terceiros (clientes) decorrente de falha profissional, tais como:

- Problemas na implementação de sistemas
- Erros de projeto
- Falha no desenvolvimento do software
- Falha no armazenamento de informações / perda de dado

Já os produtos de Responsabilidade Civil Cibernética para empresas de outros segmentos ainda não são oferecidos no Brasil devido à fraca demanda, mas já são comercializados em mercados mais maduros como nos EUA e em outros países europeus, tais como Inglaterra, Alemanha etc.

O Produto oferecido nos EUA é dividido em coberturas *first party* e *third party*:

As coberturas *third party* são aquelas para o risco de reclamações de terceiros (ex. clientes), tais como: quebra de confidencialidade de dados causados pela empresa segurada ou seus funcionários; difamação, violação de direitos de propriedade intelectual ou privacidade decorrente de violação de publicação de informações através de mídias da empresa; e comprometimento de rede, tais como acesso não autorizado ou uso não autorizado do ambiente computacional da empresa segurada que resulte em:

- roubo, destruição ou corrupção de dados digitais
- quebra de confidencialidade de dados pessoais ou informações confidenciais
- contaminação de dados pessoais ou informações confidenciais causada por transmissão de código malicioso, tais como vírus, worms etc
- ataques de negação de serviços

As coberturas *first party* são aquelas para fazer frente a reclamações de terceiros (ex. clientes), tais como perdas decorrentes de destruição de dados, extorsão, roubo, hacking, ataque de negação de serviços, interrupção de negócios, multas regulatórias etc.

Existe também o seguro de Fraudes Corporativas (Crime e BBB) com cobertura para Fraudes por meio eletrônico, contratado por empresas para transferir riscos relacionados a:

- Prejuízo financeiro direto ocasionado por ato fraudulento cometido por qualquer empregado.
- Subtração, deterioração ou perda física de bens dentro das instalações
- Perda física de bens em trânsito
- Documentos Falsificados
- Dinheiro Falsificado
- Fraude por meio eletrônico
- Vírus de computador

Quais são os principais riscos cibernéticos a que pessoas e empresas estão expostas?

Gustavo Galvão: Todas as empresas e pessoas estão expostas. No caso das empresas, todas elas certamente têm algum nível de exposição. Além do ataque de ransomware (sequestro do computador), o vazamento de dados de clientes pode gerar perdas e danos para estes. Isso pode resultar em reclamações e processos judiciais por parte de clientes, por exemplo no caso de vazamento de prontuário médico de hospitais.

Já as pessoas, em sua grande maioria, possuem um smartphone com uma grande quantidade de dados. Informações bancárias, cartões de crédito, prontuário médico, fotos, e-mails etc. Ataques de hackers como o caso recente, onde os dados são sequestrados através de criptografia, podem acontecer com qualquer pessoa.

Que ações pessoas e empresas podem empreender para se prevenirem contra riscos cibernéticos?

Gustavo Galrão: Existe uma série de medidas que podem ser implementadas pelas empresas e pessoas para aumentar a proteção aos ataques cibernéticos. Obviamente que a necessidade de controle maior ou menor dependerá do tipo da atividade e da atratividade que os hackers têm sobre as informações ou possibilidade de obter vantagens sobre determinada organização.

Importante destacar que ainda que todas as medidas sejam tomadas sempre haverá risco de vazamento de dados, seja através de ataque de hackers ou até por conta da infidelidade de empregados e/ou pessoas próximas a nós. Exatamente por esse motivo o seguro se torna uma ferramenta importante para se ter uma gestão mais efetiva destes riscos.

Dentre as medidas que podem ser tomadas para aumentar o nível de segurança das informações dentro da empresa, elencamos, além da contratação dos contratos de seguros:

- Estabelecer procedimentos para o monitoramento do uso das contas de usuário e dos respectivos privilégios;
- Utilização de técnicas de criptografia para proteger confidencialidade, integridade e autenticidade das informações;
- Processo de gerenciamento de chaves para apoiar o uso de técnicas criptográficas;
- Desenvolvimento do nível de conhecimento técnico da equipe responsável pela administração dos controles de segurança da informação;
- Implementação de estrutura organizacional para garantir o atingimento dos objetivos de negócio e de segurança da organização;
- Criação de documentos informativos de fácil entendimento sobre a política de segurança da informação para os colaboradores;
- Treinamentos internos sobre segurança da informação;
- Implementação de auditoria com metodologia que aborde as diretrizes para a gestão de incidentes de segurança da informação;
- Criação de comitê de segurança da informação com colaboração e representantes de diferentes partes da organização- Implementação de controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, tais como vírus de computador, worms de rede, cavalos de Tróia e bombas lógicas;
- Política de controle de acesso à informação e serviços de rede;
- Procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços;
- Procedimento formal de concessão de senhas com requisitos do usuário assinar declaração ou termo de responsabilidade para manter a confidencialidade de sua senha;
- Estabelecimento e implementação de métodos apropriados de autenticação para controlar o acesso remoto dos colaboradores e terceiros contratados;
- Estabelecimento e implementação de métodos apropriados para prevenir acesso não autorizado ao sistema operacional ou a rede e para garantir a segurança da informação quando se utilizam da computação móvel e recursos de trabalho remoto;
- Políticas e procedimentos para tratamento de informação no formato digital;
- Gerenciamento dos serviços terceirizados para tratar das necessidades específicas de segurança da organização;
- Utilização de técnicas para gestão de vulnerabilidades, para garantir que as tecnologias de segurança colaborem na redução de riscos associados a exploração de vulnerabilidades conhecida
- Controles que impeçam a retirada ou transporte de equipamentos e dispositivos periféricos;
- Uso de técnicas para descarte de mídias eletrônicas ou impressas, para garantir que as tecnologias de segurança colaborem na redução de riscos associados a vazamentos de informações;
- Procedimento de cópia de segurança das informações (backup) com uso de criptografia e armazenamento externo as instalações físicas da empresa;
- Política, termo e procedimento quanto ao acesso, manuseio e transmissão de informações pessoais de clientes;
- Plano de continuidade de negócios, incluindo testes periódicos.

Fonte: [CNSeg](#), em 18.05.2017.