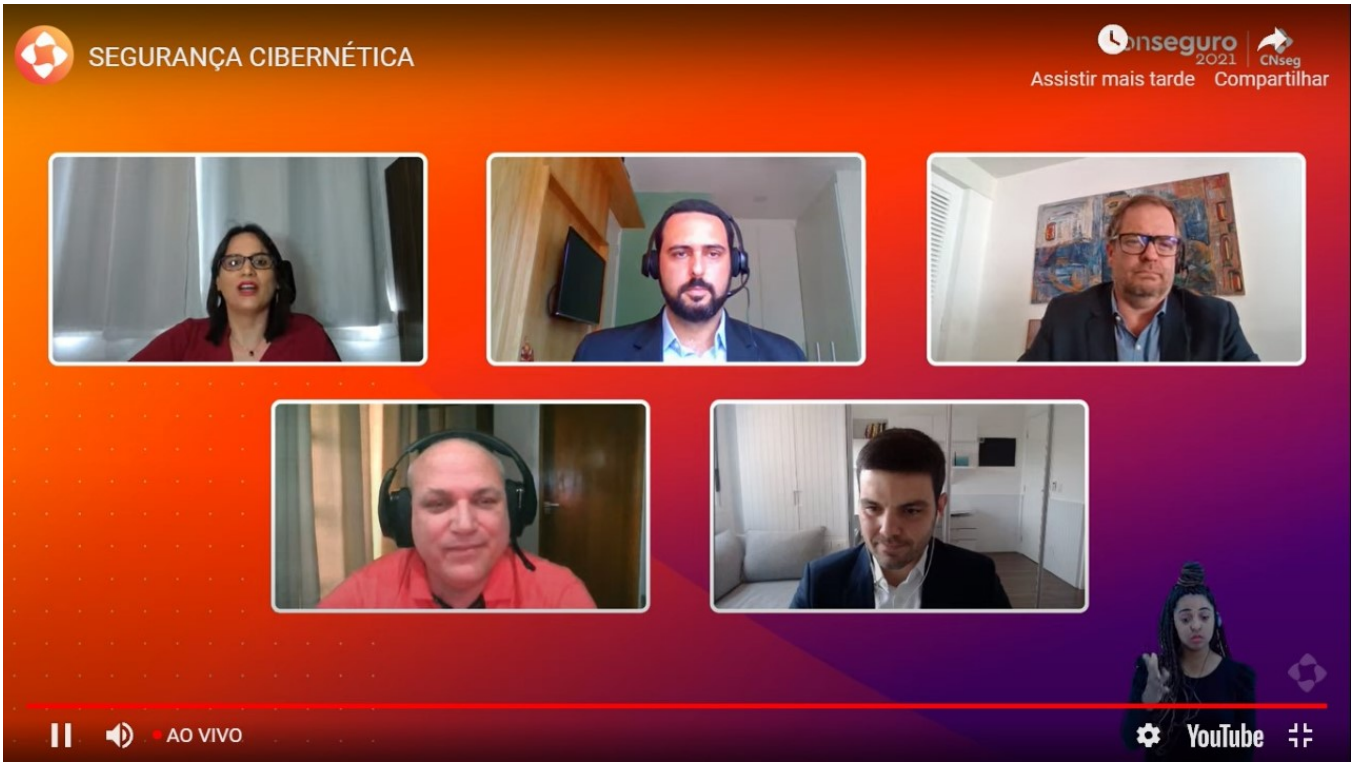

A rápida digitalização da economia como resposta à política de isolamento social e combate à Covid-19 teve como efeito colateral um aumento expressivo dos ataques cibernéticos. O chamado ransoware, invasão dos sistemas com posterior pedido de resgate, disparou ao longo da pandemia e colocou todos em alerta. No setor de seguros, uma das respostas à nova realidade é a circular 638, da Superintendência de Seguros Privados (Susep) que dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras.

“Há um mundo novo que vem com novos riscos. Os ataques cibernéticos não são uma ameaça, mas uma realidade. O regulador, naturalmente, reage a este novo cenário, tomando o cuidado de adotar medidas que impulsionem a transformação e não a retarde, de forma segura”, comentou Victor de Almeida França, coordenador de Regulação de Riscos Ativos e Controle Internos da Susep, ao participar do painel “Segurança Cibernética”, na Conseguro 2021 da Confederação Nacional das Seguradoras – CNseg.

O representante da Susep apresentou dados sobre a intensificação dos ataques cibernéticos, lembrando que o setor de seguros é bastante visado por ser intensivo em dados. Em 2019, segundo levantamento da Accenture, o custo médio de cada ataque no setor de seguros chegou a US$ 15 milhões no mundo. No Brasil, o custo médio gira na faixa de US$ 7 milhões anuais. Em relação às tentativas de ataque, foram registradas no Brasil 8,4 bilhões de tentativas no ano passado, contra 3,2 bilhões só no primeiro trimestre deste ano. “Os números mostram que as coisas não estão melhorando e é preciso avançar na proteção das informações”, ressaltou França acrescentando que os ransowares, como os que tiraram do ar o STJ por 15 dias, e a utilização de dados em nuvem, pelo risco de algum vazamento, preocupam o regulador.

Sobre a circular 638/21, o coordenador citou alguns pontos importantes, como definir que a política de segurança cibernética é complementar à política de gestão de risco, criar regras para terceirização de serviços de armazenamento de dados, definir a classificação de dados e situações de risco e dar diretrizes para a implementação de processos de segurança cibernética, entre outros. “Um ponto importante é que as seguradoras, quando forem alvo de um ataque, terão que compartilhar as informações a respeito do ocorrido, o que contribuirá para mitigar vulnerabilidades semelhantes que possam existir em outros players. Isto melhorará o risco sistêmico”, acrescentou.

Sylvia Varoto, presidente da Comissão de Assuntos Jurídicos da FenSeg e superintendente Jurídica da Allianz Seguros, elogiou a iniciativa da Susep. “É ótimo ter o órgão regulador ao nosso lado, preocupado com o risco cibernético, isto nos dá mais confiança no trabalho das seguradoras”, comentou a coordenadora do painel, acrescentando que o setor de seguros ficou muito mais exposto pela rápida digitalização dos processos ao longo da pandemia.

Sobre o compartilhamento das informações dos ataques feitos às seguradoras, que a Susep optou por deixar que as próprias empresas definam o melhor modelo, Wagner Pereira, especialista em Cyber Security da Zurich comentou que o tema já está em debate em comissões temáticas da CNSeg. “O objetivo é que o compartilhamento seja bastante técnico, mostrando qual o vetor de ataque, o método usado e o ponto de vulnerabilidade daquela seguradora”, explicou Pereira. “A troca de experiências vai aumentar a segurança de todo o mercado segurador ao evitar que aquele tipo de ataque por uma determinada vulnerabilidade se repita em outra seguradora”.

O executivo da Zurich lembrou que as seguradoras vêm investindo na segurança de seus sistemas, mas que há muito a ser feito. “Não basta ter uma equipe dedicada à segurança com riscos identificados e mapeados, é preciso também ter um plano de ação para falhas, já elaborado”, disse.

Em relação ao desenvolvimento de coberturas voltadas para proteção dos contra ataques cibernéticos, os painelistas lembraram que o caminho ainda é longo e que o limite de aceitação do risco pode ser uma dificuldade. “Existem vários tipos de ransoware e alguns com exigências de pagamento de resgates a valores enormes. Precisa ver se o mercado segurador tem apetite para tanto risco ou se vai seguir com sublimites para coberturas de ataques cibernéticos. É um debate importante”, comentou Fred Ferreira, CEO da Austral Seguradora. Ele acrescentou que antes de ofertar produtos específicos, muitas empresas fazem uma consultoria com as companhias para que elas melhorem e passem a ter um risco aceitável pelo mercado.

Diego Massara, membro da Comissão de Assuntos Jurídicos da CNseg e Superintendente Jurídico Corporativo da Junto Seguros, lembrou que além da circular 638, que vai exigir adaptações das seguradoras, outra ponto de atenção é a Lei Geral de Proteção de Dados (LGPD). “Você deve ter um executivo responsável, uma área dedicada à segurança, mas a responsabilidade é de todos. É preciso proteger os dados dos clientes, mas também dos corretores, colaboradores e outros prestadores de serviço”, comentou Massara.

Sobre a circular 638, o executivo elogiou a iniciativa da Susep, acrescentando que o primeiro passo e o mais essencial é mapear e conhecer os riscos de cada companhia. “Risco ruim é risco desconhecido. Temos novidades regulatórias, legais, e já sabemos como caminhar”, concluiu.

· O painel pode ser assistido na íntegra em https://www.youtube.com/watch?v=lVAZucZpEJo

· As inscrições podem ser feitas em http://conseguro.cnseg.org.br/

· O evento vai até 01/10

· A programação completa está disponível em http://conseguro.cnseg.org.br/

Fonte: CNseg, em 01.10.2021.