A preocupação do mercado segurador, do órgão regulador e demais agentes do setor financeiro com os crimes cibernéticos foi a pauta do segundo dia do evento “Oficina Brasil Fides de Inovação em Seguros: intercâmbio de oportunidades e experiências em ESG e riscos cibernéticos”, realizado em Brasília, na sexta-feira (14). O diretor técnico da CNseg, Alexandre Leal, informou que o Brasil ocupa hoje o segundo lugar no ranking da América Latina com maior número de tentativas de ataques cibernéticos, tendo sido registradas 100 bilhões de investidas nesse sentido em 2022. O primeiro lugar é do México, com registro de 187 bilhões de tentativas no ano passado.

“Isso explica a razão de o tema sobre cyber segurança estar na pauta de todos os agentes do setor e precisa ser enfrentado com urgência. O cenário dos riscos cibernéticos evoluiu rapidamente por conta da digitalização dos processos e foram agravados pela pandemia”, comentou Leal, acrescentando o dado de que no ano passado houve cerca de 360 bilhões de tentativas de ataques deste tipo aos sistemas de empresas e organizações na América Latina e Caribe. Em termos de coberturas desse tipo de risco, o diretor informou que, em 2022, o valor arrecadado foi de R$ 170 milhões e o total de indenizações pagas chegou a R$ 64 milhões, o que demonstra ser um ramo ainda incipiente, mas com potencial de crescimento.

Durante os dois dias da Oficina Brasil FIDES, foram debatidos aspectos da evolução do setor segurador em segurança cibernética e de adoção de boas práticas nos temas ASG, com destaque para o meio ambiente, mudanças climáticas e políticas de diversidade e inclusão nas empresas no Brasil e nos outros países do Cone Sul da Fides (Argentina, Paraguai e Uruguai).

Laboratório de segurança cibernética

O coordenador de TI da Febraban, Bento Filho, em sua palestra apresentou a iniciativa de criação do laboratório de segurança cibernética para atender as necessidades de prevenção e combate ao cybercrime, tornando-se o primeiro centro feito pelo sistema financeiro voltado para o treinamento e capacitação em cyber segurança, realização de simulações de ataques cibernéticos para se desenvolver respostas aos incidentes, aplicação de inteligência, padronização de ações e busca de inovação permanente. “Os bancos investem por ano cerca de R$ 30 bilhões em tecnologia e 10% disso são direcionados para a segurança, física e digital”, afirmou o representante da Febraban.

As seguradoras brasileiras estão mobilizadas nesse tema. De acordo com João Passos, executivo da Brasilseg, a pandemia promoveu uma aceleração da transformação digital em todos os segmentos, o que também ampliou os riscos. “Por isso, estamos nos dedicando a maturar as ações de segurança”, afirmou ele. Robson do Amaral, da Liberty Seguros, acrescentou que as empresas devem fazer autoavaliações sobre a que riscos estão mais expostas e esse “olhar para dentro de casa” precisa ser exercitado. “Não se trata só de ter um departamento de TI, ele nos dá o suporte. Mas é preciso que haja pessoas dedicadas a avaliar os riscos dentro das estratégias e também fomentar uma cultura de cyber segurança entre os colaboradores. Todos somos responsáveis”, defendeu Amaral.

Normas são fundamentais para dar o norte

Os executivos das seguradoras e os representantes da CNseg foram unânimes em afirmar que o envolvimento do órgão regulador de seguros é muito importante, pois são as normas que padronizam ações e elevam os debates e as trocas de informações sobre o tema. Representantes da Superintendência de Seguros Privados (Susep), responsáveis pela supervisão da aplicação das normas, destacaram o acompanhamento da adesão à circular 638/2021 que trata da política de segurança cibernética das seguradoras.

“Dentro desse contexto de transformação digital é possível ver oportunidades, mas não se pode esquecer dos riscos envolvidos”, afirmou Saulo Valle. “E vemos muito valor em trabalhar em parceria com o mercado, não de cima para baixo, mas com troca de informações e experiências para evoluirmos juntos”, completou Fernando Abreu. Ambos integram a Coordenação de

Supervisão de Estrutura de Gestão de Riscos e Governança da Susep.

Compartilhamento de incidentes cibernéticos

O fundamental para se ampliar a proteção a ataques cibernéticos é a troca e o compartilhamento de dados, defendeu o diretor de Serviços da CNseg, André Vasco, ao apresentar no evento as principais características do banco de dados sobre incidentes cibernéticos coordenado pela entidade. O banco está disponível para as associadas da Confederação e ele centraliza informações sobre a ocorrência de incidentes em todo o mundo. Ao captar algo, o sistema dispara alerta às associadas e oferece uma proposta de correção para aumentar a proteção à falha. “Com um compartilhamento rápido de informação, ajudamos a reduzir riscos e aumentamos a proteção”, comentou Vasco.

Os representantes das associações da indústria seguradora de Argentina, Paraguai e Uruguai parabenizaram o Brasil pelas iniciativas de investimento em cyber segurança, admitindo que seus países ainda precisam avançar muito nesse tema. “Temos ainda um mercado muito pequeno nesse ramo, com poucas apólices voltadas a cobrir o risco cibernético. Estamos alguns passos atrás”, afirmou Gustavo Trias, diretor-executivo da Associação Argentina de Companhias de Seguros. Ele comentou sobre algumas ocorrências e tentativas de ataques registrados na Argentina, mas acrescentou que ainda não há uma consciência das empresas em comunicar os incidentes, o que ajudaria numa evolução mais rápida.

O presidente da Associação Paraguaia de Companhias de Seguros, Antonio Vaccaro, afirmou que também falta uma cultura de cyber segurança em seu país, o que faz com que não haja produtos de seguro nesse tema. No campo da gestão, ele informou que existem iniciativas, mas incipientes, de regulação da tecnologia da informação das empresas seguradoras por parte do órgão regulador local. O diretor-executivo da Associação Uruguaia de Empresas de Seguros, Alejandro Veiroj, relatou uma situação parecida com a dos dois vizinhos, afirmando que o Uruguai ainda está muito atrás na questão de cyber segurança.

Fonte: CNseg, em 17.04.2023.