- Estudo de seguro cibernético da Howden aponta os principais pontos de atenção das empresas globais
- Empresas brasileiras com seguro cyber não pagam resgate e alocam recursos para a apólice
- Seguradoras têm flexibilizado termos de contratações das apólices de cyber das PMEs e apoiado melhorias internas de cibersegurança para minimizar acionamentos de incidentes cibernéticos

Por Marta Schuh

Crédito: Depositphotos

Assim como no mercado global, o Brasil vive um momento de crescimento do seguro cyber. Lá fora, a atividade de ramsonware aumentou quase 50% até maio desse ano, em comparação ao mesmo período de 2022. No entanto, o preço do seguro cibernético caiu 9% entre janeiro e junho de 2023, de acordo com os dados do **estudo de seguro cibernético Coming of Age**, realizado pela Howden, corretora internacional de seguros independente.

No Brasil, esse mercado também é crescente. Dados divulgados pela Trend Micro colocaram o Brasil como o segundo colocado entre os países mais afetados por incidentes de ramsonware em 2022, o que fez com que o prêmio local fosse elevado. Segundo dados da SUSEP, em 2021 o valor do prêmio emitido foi de R$ 105 milhões; em 2022 cresceu para R$ 181 milhões. Nesse ano, o valor se manteve crescente até abril, com 19% de aumento com relação ao mesmo período do ano passado.

De acordo com Marta Schuh, Diretora de Cyber Insurance da Howden, “o Brasil vive um momento de ajustes. Antes da pandemia, as seguradoras adotaram uma estratégia de avaliação de subscrição de risco que não evidenciava efetivamente uma postura de cibersegurança dos segurados. Com a chegada de sinistros de forma simultânea, foi necessário entender os controles e a abrangência da aplicação de tecnologia para minimizar o impacto dos acionamentos”, explica.

Ainda de acordo com a especialista, de lá para cá as coisas mudaram no mercado de seguros e as áreas de subscrição se tornaram mais técnicas, passaram a ser compostas também por especialistas da área de tecnologia para melhorar a subscrição, assim como se tornou necessário o uso de algumas ferramentas para avaliação de maturidade. Esse é um ponto importante, já que os melhores resultados de subscrição geram resultados positivos para os compradores de seguros”, reforça.

Novas regras e orientações, como as da Securities and Exchange Commission (SEC), equivalente à Comissão de Valores Mobiliários (CVM) americana, têm como foco expandir a supervisão em torno da segurança cibernética.

“Sob a perspectiva regulatória, seja voltada ao mercado de capitais ou às regras locais, como LGPD, Circular Susep, Resolução 4658 do BACEN, regra ANEEL e outras, os benefícios do seguro cibernético podem ser considerados como uma medida de proteção do ponto de vista regulatório e de mercado, ou seja, ter uma apólice cibernética em vigor faz parte da resposta das empresas regulamentadas às propostas dos órgãos reguladores. Isso evidencia o gerenciamento de riscos cibernéticos e a capacidade de acessar conhecimentos relevantes”, diz Marta.

Seguro cyber e PMES

As pequenas e médias empresas brasileiras se encaixam em outro modelo em se tratando de cibersegurança. De acordo com dados da Accenture, as PMEs sofrem 43% dos ataques cibernéticos

por terem menos recursos e uma infraestrutura de segurança cibernética menos robusta. Marta reforça que há grande necessidade de trazê-las para o ecossistema de governança, já que muitas fornecem serviços para grandes organizações.

“Para favorecer a subscrição de seguros para as médias e pequenas empresas, as seguradoras têm flexibilizado termos de contratações e apoiado melhorias com ofertas casadas de soluções gratuitas na contratação da apólice, como ferramentas de antivírus, sistemas de varredura de vulnerabilidade e serviços de incidente e resposta”, esclarece a executiva.

Impactos financeiros x resgate por ataque ramsonware

O **estudo Coming of Age** aponta que os primeiros cinco meses de 2023 registraram um aumento significativo de ataques ramsonware, embora a divulgação das seguradoras mostre que isso não foi acompanhando de aumento da sinistralidade, apontando para o sucesso dos controles de riscos em tornar as empresas mais resilientes e suportar condições mais estáveis do mercado de seguros este ano, apesar das atividades de ramsonware.

Um ponto de divergência entre os demais países para o Brasil é com relação ao pagamento de resgate por ataque ramsonware: de acordo com dados separados da Sophos, 58% das empresas com cobertura autônoma de seguro cyber pagam resgates, contra apenas 15% sem nenhum seguro cyber. No Brasil, a situação é outra – “as empresas não pagam resgate e alocam recursos da apólice em incidente e resposta, o que dá fôlego financeiro, além de contar com a expertise de profissionais qualificados para tratar a crise e minimizar impactos”, conta Marta.

A pesquisa The State of Ramsonware, da Sophoda, aponta que quase 70% das empresas brasileiras ouvidas sofreram ataques de ramsonware, sendo que vários casos se tornaram públicos e tiveram grandes desdobramentos, incluindo empresas que perderam aproximadamente R$ 1bi e tiveram impacto em valores de ações no mercado de capitais.

Lucros cessantes no topo das preocupações

O relatório da Howden reforça que a privacidade de dados merece muita atenção, seguindo decisões recentes em alguns países, como os Estados Unidos, em torno dos dados de privacidade biométricos (BIPA), que revelaram um enorme potencial de exposições. O litígio sobre pixels nos EUA é outra tendência emergente a ser observada.

Empresas que coletam e retêm dados biométricos sem obter o devido consentimento, como impressões digitais e digitalizações faciais, enfrentam o risco de serem penalizadas significativamente devido aos danos acumulados por varredura, que podem datar até cinco anos. O problema é um dos mais impactantes, confrontando o mercado de seguros cyber.

Marta comenta que “no Brasil o cenário é semelhante, embora haja uma preocupação muito forte com relação às questões regulatórias. Há uma concentração de acionamentos e prejuízos muito maior quanto aos danos próprios dos segurados, em especial dos Lucros Cessantes , que são diretamente voltados à receita que a empresa deixa de gerar em virtude da indisponibilidade causada pelo incidente, além das despesas extras operacionais, que são demandadas em diversas esferas dentro da organização durante um incidente”.

Segurança na nuvem x Interrupções

O mercado de serviços em nuvem é altamente concentrado, com cerca de dois terços do abastecimento fornecido por três empresas: Amazon Serviços Web, Microsoft Azure e Google Cloud Plataforma. Essas empresas tendem a relatar apenas grandes interrupções em seus serviços, embora tenham sido centenas de interrupções de desempenho ocorridas em 2021 e 2022, com uma média mensal de 25.

O impulso para a inovação no setor de hospedagem vem com trade-offs, ou seja, é compensatório:

é difícil manter serviço ininterrupto quando a nova tecnologia está sendo constantemente lançada. Apesar do investimento na resiliência do data center pelos provedores, o tempo de inatividade pode ocorrer devido a uma matriz ou mistura de problemas em torno de software, hardware e a infraestrutura.

Dados do relatório da Howden revelam que a causa mais comum de interrupções relatada no ano passado foi erro humano, incluindo configuração incorreta e atividade de manutenção defeituosa. Problemas de conexão com a internet, sistemas sobrecarregado, falta de energia e problemas na infraestrutura física vêm na sequência. Isso realmente importa e mostra como o tempo de inatividade pode causar consideráveis prejuízos financeiros e de reputação às empresas.

Uma forma de proteção que pode ser adotada para minimizar prejuízos é o seguro de Cloud Parametrix, disponibilizado pela Howden. O seguro visa a cobertura da indisponibilidade causada por provedores de nuvem, através de um sistema de monitoramento constante do desempenho global da nuvem e serviços de terceiros até o milissegundo. Ele detecta eventos de indisponibilidade em tempo real e aciona automaticamente o pagamento de sinistros com tempos de espera de apenas uma hora. “Empresas com alta dependência da internet para a realização de suas atividades podem ser severamente afetadas por uma indisponibilidade, como varejistas, empresas de serviços financeiros e aplicativos”, explica Marta.

Marta Helena Schuh é bacharel em Business pela University of Arts London e especialista em CyberSecurity. Em sua longa trajetória no mercado de seguros, atuou junto a instituições financeiras, como AIB e Sociétè Générale, no mercado europeu. Os últimos 8 anos foram dedicados à JLT e Marsh, onde foi Líder de Riscos Cibernéticos.

É licenciada em Finanças pelo Chartered Institute for Securities & Investments (CISI), em Londres, e certificada em Economics of Cybersecurity pela Delft University of Technology.

Tem especialização em Direito Digital pelo Insper, em Cybersecurity for Insurance pela Universidade da Califórnia em Los Angeles (UCLA), em Cyber Attacks pelo Instituto Politécnico da Universidade de Nova Iorque (New York University Tandon School of Engineering) e em Cyber Diplomacy pela ONU. Entre 2022 e 2023, foi Presidente do Comitê de Riscos e Seguros da Câmara de Comércio e Indústria Britânica (BRITCHAM) no Brasil e, em 2022, recebeu pela Women in Cybersecurity (WOMCY) o prêmio de uma das 25 mulheres mais influentes em cyber segurança na América Latina.

Sobre a Howden Brasil

A Howden é uma corretora internacional de seguros e resseguros independente, parte do Howden Group Holdings, que fornece soluções para clientes na Europa, Ásia, Oriente Médio e América Latina e possui a maior agência de subscrição do mundo. No Brasil, a Howden conta com equipes próprias e especializadas em atender clientes corporativos nacionais e multinacionais, oferecendo serviços de Seguros, Resseguros, Consultoria de Risco e de Benefícios Corporativos. A Howden Brasil tem sede em São Paulo.

Marta Schuh,
Diretora de Cyber Insurance da Howden

09.08.2023