- Abrasca e The Security Design Lab, em parceria com a Howden, desenvolveram o primeiro estudo no país a medir o grau de maturidade das companhias de capital aberto e chamar a atenção para a importância deste problema no mercado de capitais – 109 empresas participaram;

- Resultados: a maioria das empresas (93%) possui mecanismos para detectar ataques cibernéticos, porém, 42% não têm plano de resposta a incidentes de cibersegurança e não contam com executivos responsáveis pela segurança da informação, e 65% não orientam as equipes para lidar e responder a este tipo de incidente;

- A Howden analisou empresas de capital aberto, que foram vítimas de incidentes cibernéticos nos últimos 3 anos. Conforme avaliação, essas empresas apresentaram, além de prejuízos substanciais, perda do valor de ação no mercado, no período de 6 meses. Alguns cases neste sentido são apresentados por Marta Schuh, Diretora de Cyber Insurance da Howden, que diz: “Empresa brasileira do segmento de saúde, de capital aberto (na B3), que faturou R$ 4 bilhões de reais em 2022, ao sofrer um incidente cyber de *ransomware*, as perdas foram referentes a 23% do faturamento do trimestre, um impacto no valor da ação de -43%”.

Foi divulgado nesta quarta-feira (13), em evento na sede do Insper em São Paulo, o primeiro estudo do Brasil a avaliar a maturidade das companhias de capital aberto (com ações listadas na B3) em cibersegurança, revelando que uma parte das maiores empresas do país está distante das recomendações e melhores práticas indicadas pelas principais agências mundiais de cibersegurança. A Pesquisa Setorial em Cibersegurança foi desenvolvida de forma inédita pela Associação Brasileira das Companhias Abertas (Abrasca) e pelo The Security Design Lab (SDL) – rede global de pesquisa e desenvolvimento de cibersegurança com operação na América do Sul e Europa –, em parceria com a Howden (multinacional de seguros independente), utilizando a metodologia Cyber Score, que mediu as respostas das 109 empresas participantes dos seguintes setores: Agronegócio, Educação, Energia, Engenharia, Financeiro, Indústria, Óleo & Gás, Saúde, Serviços, Tecnologia, Telecomunicações e Varejo. A nota média ficou em 4,9 numa escala de 0 a 10, o que indica um grau de maturidade mediano.

O questionário de 86 perguntas segmentadas em 12 capítulos foi aplicado entre os meses de maio e agosto deste ano. A metodologia Cyber Score já é utilizada por várias empresas globalmente e esta é a primeira aplicação em um levantamento setorial.

A partir dos dados colhidos, a Abrasca visa apoiar as áreas técnicas e de compliance das empresas de capital aberto para disseminar a relevância do assunto entre os C-levels, conselhos de administração e acionistas. “A importância do tema no mercado de capitais é crescente e sem volta. Deixou de ser um problema de TI e se transformou em um problema para todas as companhias, abertas ou não. O mundo está se movimentando no sentido de regulações mais adequadas à nova realidade e de melhores práticas, daí a importância de termos dados atualizados para entender onde estamos e, com isso, balizar a discussão ‘com os pés no chão’, de forma pragmática e eficiente”, afirma Pablo Cesário, presidente-executivo da Abrasca.

Melhores avaliações

As empresas que alcançaram os maiores índices de compliance em cibersegurança são dos setores da Indústria / Manufatura, Telecomunicações, Óleo & Gás e Financeiro. Segundo os aplicadores da pesquisa, não existe nota de corte quando a segurança da informação é analisada, pois cada empresa e setor possuem particularidades. Contudo, uma avaliação de 7,5 já é considerada muito boa.

“A nota de 5 sobre 10 obtida na média geral demonstra muito espaço para melhorias, mas trata-se de um cenário não destoante do que apontam pesquisas globais. Estar em conformidade com as recomendações e melhores práticas em cibersegurança ajuda as companhias a estabelecer medidas de proteção, reduzindo a sua área de exposição contra potenciais ataques”, pontua Alexandre Vasconcelos, diretor para a América Latina do The Security Design Lab.

O relatório da Abrasca e do SDL aponta que, por um lado, 93% das empresas possuem algum mecanismo para detectar ataques cibernéticos e 65% se dizem capazes de identificar e agir em resposta a incidentes para assegurar a continuidade do negócio e suas funções. Por outro, 42% não possuem um plano de resposta a incidentes de cibersegurança, 65% não orientam a equipe para lidar e responder a incidentes de cibersegurança e 73% não possuem mecanismos de controle de acesso para sistema OT (Tecnologia Operacional) e ICS (Sistemas de Controle Industrial). A título de comparação, a última pesquisa America’s Most Cybersecure Companies, realizada pela Forbes, com 200 empresas americanas identificou que apenas 30% delas possuem um executivo de segurança da informação (CISO), enquanto a pesquisa brasileira mostrou que este número é superior, chegando a 58% no país.

A Cadeia de Suprimentos (Supply Chain) tem sido um alvo crescente e preferencial para os criminosos cibernéticos. Alguns ataques impactam diretamente a cadeia de suprimentos, como o ocorrido na Solar Winds, afetando mais de 18 mil empresas. “Uma companhia pode ter a sua operação afetada, sem ter sido alvo direto de um ataque. A pesquisa nos mostra um dado preocupante, onde 52% das companhias não implementam gestão de riscos para esta cadeia”, alerta Vasconcelos.

Aumento dos ataques no mundo e custos para as empresas

Os custos de crimes cibernéticos à economia mundial devem saltar de US$ 3 trilhões por ano em 2015 para US$ 10,5 trilhões em 2025, de acordo com um levantamento elaborado pela Howden, multinacional de seguros independente. Sobre a frequência de ataques cibernéticos no mundo, a empresa analisou dados do NCC Group e identificou que, nos primeiros cinco meses deste ano, comparado ao mesmo período de 2022, houve um aumento de 48% no número de ataques do tipo *ransomware* (sequestro de dados com cobrança de resgate). Segundo pesquisa da Verizon (2023), cerca de 83% das violações envolvem atores externos às companhias, com 95% dos ataques sendo motivados por questões financeiras e o maior índice de ataques externos vindo do crime organizado.

Ainda de acordo com levantamento global da Howden, foram pagos em reinvindicações de incidentes relacionados a *ransomware* o equivalente a R$ 247 milhões nos últimos três anos, tendo o setor de saúde como o mais afetado, seguido por empresas de varejo, finanças e serviços. No Brasil, segundo a empresa, os incidentes em que foram acionadas apólices de seguros tiveram o pagamento de despesas entre R$ 2 milhões e R$ 65 milhões, frente às reinvindicações junto ao mercado local.

“Estamos discutindo um tema que afeta não só o valor de mercado da companhia, mas também coloca em questão a continuidade dos negócios. E mais ainda, está se refletindo no custo de capital das companhias. Já vemos um encarecimento de operações de crédito por conta deste tema, assim como a revisão de notas de agências de *rating* levando em conta a análise de cibersegurança”, diz Rafael Sasso, coordenador da CINC – Comissão de Inovação Coorporativa da Abrasca.

Guia de Segurança da Informação

Paralelamente à divulgação do resultado da pesquisa, o SDL, em conjunto com empresas patrocinadoras e apoiadores – incluindo a academia, representada por professores da FGV-RJ, Insper, FIPECAFI/ USP e IMREDD/Université Côte d’Azur –, lançou o primeiro Guia de Segurança da Informação voltado a executivos, conselheiros de administração e investidores. O documento foi elaborado em linguagem acessível e contendo orientações que permitam aos tomadores de decisão entenderem o tema e dialogar com as áreas técnicas sobre a estratégia de cibersegurança de suas

companhias.

"Embora a tecnologia seja amplamente utilizada em todos os setores, seus riscos ainda não foram totalmente compreendidos pelos órgãos de gestão das empresas. O aumento na quantidade e na frequência de incidentes, assim como nas somas significativas de prejuízos e outros impactos, não são somente responsabilidade do CISO, mas de toda a alta gestão. Esse tema requer urgentemente a compreensão do risco de segurança cibernética e das possíveis implicações para as companhias", alerta Marta Helena Schuh, diretora de Cyber Insurance da Howden.

“A Howden analisou empresas de capital aberto que foram vítimas de incidentes cibernéticos nos últimos 3 anos. Conforme avaliação essas empresas apresentaram, além de prejuízos substanciais, perda do valor de ação no mercado, no período de 6 meses”, conta Marta.

Segundo ela, como demonstração desse cenário temos, por exemplo, empresa brasileira do segmento de saúde, de capital aberto (na B3), que faturou R$ 4 bilhões de reais em 2022. Ao sofrer um incidente cyber de *ransomware*, que comprometeu suas operações, as perdas foram referentes a 23% do faturamento do trimestre, um impacto no valor da ação de -43%.

Em outro exemplo, dessa vez com empresa multinacional com forte prestação de serviços de telecom no Brasil, de capital aberto (na Nyse), que faturou 2 bilhões de dólares no ano passado, após o incidente cyber teve perdas da ordem de 46 milhões de dólares, com um impacto no valor da Ação de -70%.

Estados Unidos e mercado de capitais

A diretora destaca que, nos Estados Unidos, o tema também está em alta com as novas regras mais rigorosas de cibersegurança anunciadas pela SEC – órgão de regulação do mercado americano de ações –, que devem ecoar em diferentes locais do mundo, incluindo o Brasil, e que chamam cada vez mais a atenção dos investidores. Os novos regulamentos da SEC para entidades de mercado visam padronizar o risco de cibersegurança e melhorar a estabilidade financeira. Gary Gensler, presidente da instituição, sugeriu que empresas de investimento, consultores e outras entidades de mercado sejam obrigados a notificar os clientes cujas informações confidenciais tiveram vazamento em, no máximo, 30 dias após o incidente. A SEC deverá ser notificada por escrito imediatamente, seguido de um relatório mais detalhado em 48 horas.

Segundo levantamento global da Harvard Business Review, as empresas de capital aberto sofreram uma queda média de 7,5% no valor de suas ações após um ataque cibernético, juntamente com uma perda média de capitalização de mercado de US$ 5,4 bilhões. Estudos preliminares indicam que estes números devem subir em 2023. Em outro estudo, a Morningstar Sustainalytics detectou que, um ano após os ataques, 30% das empresas que tiveram incidentes ainda estão com movimentos ascendentes tímidos.

Principais resultados da Pesquisa Setorial de Cibersegurança

- 93% das empresas têm mecanismos para detectar ataques cibernéticos;
- 42% não possuem um plano de resposta a incidentes de cibersegurança;
- 38% das companhias não possuem um programa regular de treinamento em segurança da informação;
- 65% das empresas não orientam a equipe para lidar e responder a incidentes de cibersegurança;
- 42% das companhias não possuem um CISO ou posição similar (executivo responsável pela segurança da informação);
- 46% das companhias não possuem um comitê de segurança da informação;
- 51% não possuem uma análise de impacto de negócio;
- 40% não possuem um plano de continuidade de negócio;
- 52% não possuem procedimentos para gestão de riscos da cadeia de suprimentos (Supply Chain);

- 52% não implementam mecanismos para evitar danos de cibersegurança originados da cadeia de suprimentos;
- 43% das empresas autenticam em sistemas críticos, utilizando login e senha, e apenas 2% utilizam modernas tecnologias como passwordless (autenticação sem senha);
- 73% não possuem mecanismos de autenticação robusto para acesso a sistemas OT (Tecnologia Operacional) e ICS (Sistemas de Controle Industrial);
- 41% dos dispositivos conectados das empresas não implementam proteção de dados em trânsito.

Metodologia da pesquisa

A metodologia Cyber Score (www.cyberscores.io), desenvolvida e patenteada pelo SDL, baseia-se nas principais regulações e melhores práticas de segurança globais. Consultores das empresas Alvarez & Marsal, Urbano Vitalino Advogados, Howden, Elytron e Bidweb Security, foram treinados e certificados pelo SDL para aplicar o teste com diretores de TI (CIO), CISO ou executivo da área. As respostas foram classificadas entre A, B, C, D ou E, conforme a imagem abaixo:

De acordo com pesquisas de grandes consultorias globais divulgadas recentemente, segurança cibernética e privacidade de dados estão entre as 5 principais prioridades dos conselhos de administração para 2023. “Nós nos baseamos no que há de mais moderno em termos de melhores práticas e políticas de segurança das principais agências mundiais de cibersegurança, utilizando como parâmetros autenticação, nuvem e controle de acesso, criptografia de dados, governança, gestão de dispositivos conectados, gerenciamento de riscos da cadeia de suprimentos, continuidade de negócios, conformidade com a Lei Geral de Proteção de Dados (LGPD), entre outros”, detalha Vasconcelos.

Cada companhia recebeu o seu relatório individual, confidencial e privado, seguindo as exigências da LGPD. As informações foram usadas de forma anonimizada para os resultados da pesquisa. O acesso e o armazenamento dos dados coletados seguem todas as normas de segurança e são controlados e auditados, com uso das mais modernas tecnologias de segurança como passwordless, zero trust e criptografia, garantindo inviolabilidade.

Acesso ao conteúdo na íntegra da Pesquisa Setorial de Cibersegurança e do Guia de Segurança da Informação: https://www.cyberscores.io/pt/nova-pesquisa-setorial/

Sobre a Howden

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.

Sobre a Abrasca

A Abrasca - Associação Brasileira das Companhias Abertas é a única entidade que reúne voluntariamente as mais importantes companhias abertas de todos os setores e de todo o país: suas associadas somam 85% do valor de mercado do Brasil. A entidade é a soma de ações no interesse estratégico financeiro das companhias abertas.

É especializada em relações institucionais com foco em: direito societário, tributário, empresarial, regulação e autorregulação no mercado de capitais, normas contábeis, contabilidade e auditoria, instrumentos de captação e financiamento, fomento de negociação de valores mobiliários, relações com investidores e governança corporativa. Site: http://abrasca.org.br.

Sobre o The Security Design Lab

The Security Design Lab (SDL) é uma grande Rede de Colaboração fundada em 2021 para gerar discussões, experiências e disseminação de conhecimentos para auxiliar as empresas e governos a melhorar os seus níveis de segurança. Tem por objetivo fomentar debates e promover a troca de experiências para difundir conhecimentos sobre melhores práticas, políticas, padrões e regulações em cibersegurança. Site: www.securitydesignlab.com.

Fonte: Howden, em 13.09.2023.