Palestrantes discutem o significado do ransomware, LGPD e penalidades, além da amplitude da cobertura do seguro cibernético e os pré-requisitos técnicos necessários para a contratação

No último dia 29, a Academia Nacional de Seguros e Previdência - ANSP realizou o seminário "Seguro Cibernético aplicado - Ransomware". A live foi apresentada pelo presidente da instituição, João Marcelo dos Santos e mediada pelo Diretor e Vice-coordenador da Cyber Risks da ANSP e instrutor em Cybersecurity pela IBM, Rogério Vergara. Teve as participações do Fundador da Clamapi Seguros Cibernéticos, Claudio Macedo Pinto, do Gerente do Departamento de Linhas Financeiras e Riscos Cibernéticos da Tokio Marine Seguradora, Gerente do Departamento de Linhas Financeiras e Riscos Cibernéticos da Tokio Marine Seguradora, Daniel Lamboy, e do Líder de Financial Lines & Liability da Lockton Brasil Consultoria e Corretora de Seguros e Coordenador da Cátedra de Tecnologia e Cyber Risks da ANSP, Mauricio Bandeira.

O ransomware é um tipo de software malicioso (malware) que "sequestra" o computador da vítima e "cobra" um valor em resgate, geralmente usando moedas virtuais. O sequestro se processa por meio de criptografia dos dados contidos no computador/servidor. Este tipo de "vírus sequestrador" age codificando os dados do sistema operacional de forma com que o usuário não tenha mais acesso. "Nesta edição do café com seguro, vamos abordar as consequências desse tipo de ataque para as empresas, como as seguradoras se posicionam diante de um determinado fato, que tipo de subscrição fazem, como aceitam seus negócios e como o corretor precisa se posicionar na oferta do seguro para seus clientes", indicou Vergara.

Segundo ele, passou a fase de ataques direcionados a uma só pessoa, empresa ou organização, para aumentar cada vez mais a capacidade de geração de pagamentos efetivos para os ataques o ransomware passou a ser disseminado na rede, na forma de SaS - software as a Service. No começo, os ransomwares eram criptografias simples que permitiam aos proprietários, após o pagamento do resgate, recuperar seus dados, mediante a aplicação das chaves de acesso oferecidas pelos atacantes, mas, face ao aumento do uso de métodos de "descriptografia" já conhecidos pelas empresas de serviços de cibersegurança, houve uma evolução e hoje o atacante de ransomware adota cópias dos arquivos em servidores públicos para coagir as empesas ao pagamento - se não pela chave de "descriptografia" então pela não liberação na rede mundial dos arquivos sequestrados, muitas vezes confidenciais ou de propriedade intelectual.

Uma visão atualizada desse tipo de risco no mundo e no Brasil - Claudio Macedo Pinto

Conforme Cláudio o seguro de cyber chegou ao Brasil em 2012, trazido pela AIG. Até 2018 o mercado andava muito tímido. No início de 2017 havia apenas duas seguradoras e, no final do mesmo ano, existiam quatro. Hoje, existem nove seguradoras atuando no ramo e uma décima seguradora deve lançar esse produto ainda esse ano, sem contar as companhias estão estudando entrar nesse mercado.

"Entretanto, o fato de ter novas seguradoras não significa que o cliente final tem nove cotações. Isso porque, cada seguradora tem um tipo apetite de risco. Algumas focam em nas Micro e Pequenas Empresas, outras em PMEs, algumas que só querem trabalhar com apólice assegurando risco e em excesso de apólices de R$20 ou R$30 milhões", aponta o executivo. Por conta da pandemia, houve uma explosão global na quantidade de ataques cibernéticos e de indenizações nos mercados globais, tanto para pagar ransomware quanto multas.

"Estamos vivendo o movimento que chamamos de hard market para determinados riscos e para as médias e grandes empresas. Além da vulnerabilidade das pessoas, que passaram a trabalhar de casa e não tinham o nível de proteção que se tem dentro de uma empresa, os hackers se aproveitaram do tema pandemia para fazer uma série de ataques", enfatizou Cláudio. Já para as empresas menores está mais acessível fazer seguros, ao passo que as seguradoras oferecem os facilities, que são produtos de prateleira, com regras pré-definidas, e tem tido boa no mercado.

Além disso, a sinistralidade nessas companhias está baixa, devido ao fato de que as seguradoras estão disponibilizando ferramentas para que elas se protegerem melhor, para mitigar o risco. "Esse é um mercado que atualmente fatura R$ 33 milhões. Ou seja, faturou no primeiro semestre quase o que foi faturado em um ano inteiro. E já tem cerca de 6 milhões de sinistro pagos no mesmo período. Esse é um setor promissor, que vai crescer bastante" finalizou.

A experiência da seguradora - Daniel Lamboy

Na visão de Daniel Lamboy, o mercado de seguro de risco cibernético brasileiro é muito pequeno se comparado com o mercado mundial, que tem expectativa de 15 milhões. E por isso mesmo, é um nicho que tem muito potencial de crescimento. De acordo com o executivo, a pandemia criou um ambiente de home office forçado, o que culminou na inobservância dos critérios de segurança. Foi uma ótima porta de entrada para que malfeitores pudessem acessar os sistemas das empresas. Ele acredita que períodos como esses, tornam as pessoas mais suscetíveis a cair em armadilhas cibernéticas. Segundo especialistas, o elo mais vulnerável de qualquer sistema é o usuário.

"O lado bom é que esse ambiente todo contribuiu para a percepção de que existe o risco cibernético e, consequentemente, o aumento da busca dos usuários por proteção. A parte negativa é o aumento exponencial das taxas de sinistralidade", explica. Com isso, algumas companhias que já ofereciam seguro cibernético para determinado tipo de negócio estão deixando de oferecer. Em relação à legalidade, não existe hoje uma lei no Brasil que delimite até que ponto o pagamento de um resgate cibernético deve ser permitido. A territoriedade também não é clara. Não se sabe exatamente que leis se aplicam a qual geografia.

"Eu não acho que o caminho seja a proibição do pagamento de resgate, mas esteja muito mais na direção que a Casa Branca está caminhando, de regulamentar algumas regras sobre de que forma ou que circunstâncias ele deve ser pago", defendeu. Outro componente importante é a mensuração os custos. Sob a ótica meramente econômica, o valor que é cobrado pelo ransomware e costuma ser muito menor do que o prejuízo que o não restabelecimento do sistema vai causar. Sendo assim, o executivo acredita que faça sentido pagar o resgate.

Lamboy explica que a Tokio Marine Seguradora tende a olhar o pagamento de um randsomware como um reembolso de um prejuízo incorrido pelo segurado. Caso um segurado seja vítima de um ataque cibernético, existem três possibilidades, pensando na regulação do sinistro: a primeira coisa a ser feita é acionar a equipe de resposta a incidentes. Então, dá-se início a uma investigação forense para determinar que tipo de malware, que tipo de código malicioso está no sistema; na segunda possibilidade, o ataque já é conhecido e sabe-se que ainda não tem uma chave, um antídoto para o vírus. É um ataque muito sofisticado; a terceira possibilidade é a do usuário ter um histórico do malware. Vale lembrar que nem sempre que o resgate é pago o acesso ao sistema é devolvido. "Nesses casos, recomendamos que nossos segurados não paguem o resgate. Focamos na restauração de backups, na reconstituição de redes e sistemas. Nossa ideia não é enriquecer o malfeitor e sim reembolsar o nosso segurado de um prejuízo que ele correu", reforçou.

A experiência do corretor/distribuidor - Mauricio Bandeira

Em 2017, na minha visão, teve um evento que mudou bastante essa questão de materialidade, de como as empresas estão expostas a esses riscos cibernéticos e como isso pode ter consequências financeira, e muitas vezes também reputacional. Em maio do mesmo ano houve o vírus wanna cry, que ficou bastante famoso na época e afetou diversos países e empresas. Levou o sistema de saúde de Londres a ficar inoperante. No Brasil, a Petrobras teve que desligar a sua rede durante um dia. Tribunais também ficaram com instabilidade.

Logo na sequência um outro vírus afetou uma empresa de transporte marítimo. A materialidade de como existe esta questão de exposição e como ela pode afetar diretamente as empresas ficou muito mais tangível para o público em geral. Depois disso houve muitos outros casos e, atualmente, é possível afirmar que é raro passar uma semana sem um caso de vazamentos, sem

alguma questão relacionada a um vírus ou ataque.

"Como corretor de seguros tivemos alguns anos de investimento, fizemos um trabalho de conscientização das empresas e estabelecemos parcerias", comentou Maurício Bandeira. Em sua opinião, o mundo evoluiu bastante, tanto do lado do mal, quanto do do bem, felizmente. A sofisticação dos ataques, porém, tem afetado sobremaneira o mercado seguro. O ambiente mudou consideravelmente, não só a necessidade de informação, mas também a questão das condições do seguro. Hoje é comum se ter uma limitação da cobertura específica de ransomware. As seguradoras locais seguem os guideline de suas matrizes, principalmente dos Estados Unidos e Europa, onde um problema do ransomware é algo que realmente tem afetado o mercado e evidenciado não só essa questão de necessidade informações adicionais e as limitações de cobertura da apólice, mas também no reajuste de preços.

"Outro tópico importante do ponto de vista do corretor de seguros, distribuidor, é a questão de fazer sempre uma venda consultiva e estar ao lado do segurado quando da preparação do submission dos questionários", destacou. Ao final de sua exposição, o executivo também alertou que o seguro cyber deve ser tratado com extrema confidencialidade e falou de suas perspectivas para o mercado. "O que prevemos para o futuro é que os ataques tendem a aumentar. Os Estados Unidos devem apertar a questão de regulação das ciptomoedas. Além disso, acredito que pode ocorrer a proibição da cobertura de randsomware nas apólices de seguro cyber", concluiu.

Assista a live completa no canal da ANSP
https://www.youtube.com/watch?v=Yi3QXWlrmcE&t=2325s

Fonte: Oficina do Texto, em 09.08.2021