Peck
Advogados

Legal | Innovation
Security | Day

Apoiadores:

CREDILINK INFORMAÇÕES DE CRÉDITO

SIKUR

tabapuã CONSULTORIA EM SEGUROS

THALES Together • Safer • Everywhere

OneTrust PRIVACY, SECURITY & GOVERNANCE

No Dia Internacional da Segurança da Informação (30/11), o Peck Advogados promoveu o evento **Legal Innovation - Security Day**, que reuniu diversos especialistas da área para discutir as melhores práticas e os principais desafios que envolvem a proteção de dados no país.

Com a participação de profissionais de diferentes setores e de grande relevância no mercado, o encontro on-line contou com quatro painéis, numa manhã de muita troca de experiências, a apresentação de cases e a análise de tendências esperadas para 2022.

Além da sócia-fundadora da banca e Conselheira Titular do Conselho Nacional de Proteção de Dados (CNPD), Patricia Peck, outro destaque foi a presença de Arthur Sabbat, Diretor do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD). Confira mais detalhes neste material exclusivo, que traz ainda um guia de **Protocolo de Resposta a Incidentes | Ataques de Ransomware**, elaborado pelo sócio de Gestão de Crise e Contencioso Digital, Henrique Rocha.

Patricia Peck
Conselheira Titular
CNPD

Arthur Sabbat
Diretor
ANPD

CIBERSECURITY: PRINCIPAIS DESAFIOS

Na abertura do evento, Patricia Peck apresentou alguns números para ilustrar o crescimento não só do mercado de segurança da informação, mas também dos ciberataques. A advogada chamou atenção para o fator preocupante que é a recorrência do Brasil como alvo dessas violações, numa realidade que gera prejuízos e transtornos que vão de perdas financeiras, paralisação das operações e até danos reputacionais muitas vezes irreversíveis.

> “O mercado da segurança da informação cresceu muito no país, principalmente após a regulamentação da proteção de dados com a criação da Lei de Proteção de Dados Pessoais (LGPD). Houve um grande investimento em ferramentas protetivas, mas ainda restam muitas lacunas, tais como a carência por profissionais no mercado para trabalhar com a Segurança da Informação.”

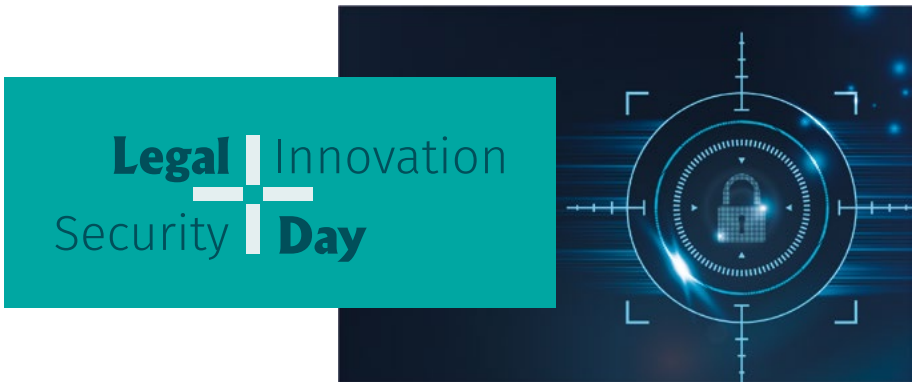
Na avaliação da profissional, é necessário haver parcerias com universidades para fomentar o ensino e a prática da cibersegurança, bem como investimentos para concretizar a Política Nacional de Segurança Cibernética.

Arthur Sabbat, Diretor do Conselho Diretor da ANPD, reforçou a importância dos esforços realizados pelo setor público, ao promover medidas regulatórias significativas, e pelo privado, que caminhou rápido na trajetória de adequação.

> “É essencial ter objetivos estratégicos sólidos e ações que sejam convergentes entre os dois lados. Por parte do Executivo Federal, podemos citar o Decreto 10.222, que aprovou a Estratégia Nacional de Segurança Cibernética, e o Decreto 10.748, que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos. Foram providências que pavimentaram o caminho para estabelecer a Política Nacional de Segurança Cibernética e que elevaram o tema a um viés nacional, já que é um assunto que não pode ser setorizado.”

Sabbat revelou que a ANPD tem feito um intenso trabalho com empresas de diferentes atividades econômicas para explicar a urgência em alterar a conduta diante desse cenário de riscos e ameaças, e que conceitos de segurança e transparência devem fazer parte do DNA de uma organização. Ele também foi enfático ao dizer que não é necessário ter medo da ANPD, principalmente em relação ao art. 48 da LGPD, que traz a obrigação de comunicar a ocorrência de incidentes de segurança.

> “Essas violações precisam ser reportadas à autoridade. Os registros são usados para traçar estratégias de mitigação, levantar dados estatísticos, mensurar o nível de segurança cibernética, visando beneficiar o titular de dados, inserido nesse ecossistema de segurança. O esforço da autoridade é alimentar essa cultura de proteção de dados, respostas a incidentes e segurança cibernética, porque a tendência, com o advento das novas tecnologias e principalmente do 5G, é agravar esse cenário de crimes digitais no país.”



O evento on-line realizado pelo Peck Advogados teve **MAIS DE 800 INSCRITOS**, em painéis mediados pelos advogados e sócios do escritório.

MEDIADORES E DEBATEDORES **PECK ADVOGADOS**

Caroline Teófilo
Sócia

Henrique Rocha
Sócio

Leandro Bissoli
Sócio

Letícia Málaga
Sócia

Lorena Botelho
Sócia

Marcelo Crespo
Sócio

SEGUROS, TERCEIRIZADOS E RESPONSABILIDADES NA LGPD

Arthur Sabbat esteve presente no primeiro painel do evento, **Incidentes de Segurança e responsabilidade na LGPD**, que teve como moderador o sócio Henrique Rocha. Além deles, Alexandre Ernest Reis, executivo da Tabapuã Seguros, também falou sobre as várias demandas surgidas após a entrada da regulamentação de dados no país. Segundo o profissional, a carteira de clientes da empresa praticamente dobrou após a vigência da LGPD, com várias organizações que contrataram apólices de riscos cibernéticos.

> “Como as seguradoras oferecem ferramentas que servem de apoio não só no momento do ataque, mas também no pós-incidente para reduzir os danos, a busca pelo produto cresceu muito. É um mercado que vem se adequando há pelo menos dois anos para esta fase, já que poucas instituições viam a necessidade desses recursos antes da lei.”

Reis também afirmou que o formato dessas contratações está cada vez mais simples e facilitado, justamente para ter uma abrangência maior entre os serviços que podem representar uma vulnerabilidade maior, como entre os terceirizados.

Camila Costa, coordenadora jurídica da área de Contratos e Consultivo da construtora Tenda, contou um pouco mais sobre o projeto de assessment realizado pela companhia, que “viabilizou um grande amadurecimento no uso dos dados, principalmente para encarar ocorrências e problemas em relação ao tratamento dessas informações.” Foi um trabalho que envolveu todas as áreas da empresa, inclusive com a participação do corpo diretivo, que esteve presente em todas as etapas necessárias para efetivar as mudanças de conceito e cultura.

> A ação se deu por meio de orientações e treinamentos exaustivos - interno e externo. Assim que as pessoas começaram a entender do que se tratava a lei, os dados que circulavam por toda a nossa rede, começaram a ficar mais preocupadas e cautelosas com o tratamento.

Mauro Melo, CEO da Credlink, enalteceu como a segurança dos dados favorece pessoas e empresas a terem melhores condições na sociedade, e que é preciso um trabalho colaborativo entre todos os setores para detectar as falhas, reduzir as ameaças e desenvolver uma cultura de proteção e privacidade.

> Clientes são pessoas e pessoas são dados. Então é preciso tratar as informações com seriedade e credibilidade, para garantir a qualidade no tratamento e na prestação de serviço aos consumidores.

O segundo painel do dia, **Gestão de risco em terceirizados: melhores práticas**, foi mediado pela sócia de Governança de Proteção de Dados, Núcleo DPO e Segurança da Informação, Caroline Teófilo, e teve participação da sócia de Contratos, Societário e Inovação, Lorena Botelho. As advogadas falaram sobre aspectos e critérios ao contratar parceiros de negócios, incluindo aceitar e mitigar riscos.

Ronaldo Fenelon Santos Filho, Head do Jurídico Global do Grupo SEB, também esteve presente e destacou que além de identificar, é indispensável mensurar quais vulnerabilidades são aceitáveis ou não conforme a estrutura da organização.

> Isso engloba fazer uma boa discussão das cláusulas e fiscalizar regularmente os contratos, ter ferramentas de negociação e de assessment para garantir procedimentos e termos de entrega adequados, além de incluir os fornecedores dentro da gestão de riscos.

Outra participante foi Tatiana Penha, gerente jurídica da RD, que destacou como auditorias periódicas e um acompanhamento próximo junto com o parceiro de negócios pode favorecer a criação de um ambiente mais seguro.

> É juntar forças para minimizar riscos que estamos propensos com os terceiros. Saber como minimizar os impactos, por exemplo, ao restringir o acesso dos dados. Nada mais é do que ter assertividade nas ações, por meio de uma gestão que utilize ferramentas que ajudam nesses desafios.

Evaldo Osório Hackmann, executivo jurídico da SIKUR, também esteve presente e abordou como a gestão de risco de terceirizados é uma estratégia fundamental para evitar danos reputacionais.

> Não basta que a organização tenha recursos suficientes para se proteger. O parceiro de negócios precisa agir de maneira preventiva e informar quais possíveis vulnerabilidades no seu escopo, e de forma colaborativa, tentarem juntos encontrar soluções efetivas para os problemas. Assim, conhecer cada fornecedor para desdobrar processos críticos específicos faz toda diferença.

O coordenador jurídico da Aliansce Sonae Shopping Centers, Raphael Amar, lembrou que a avaliação dos riscos relacionados aos terceiros - conhecer suas fragilidades de ponta a ponta - é um pilar fundamental na governança de privacidade.

> É um programa custoso, que deve levar em conta se há orçamento para arcar com possíveis falhas. Cumprir o art. 50 da LGPD vai muito além de ter boas práticas, é preciso a adoção de mecanismos internos e externos que impactam na contratação, com uma instrumentalização robusta nas políticas aplicadas e nos requisitos técnicos.

PRESSÕES E PROJEÇÕES

Na sequência, foi a vez do sócio Marcelo Crespo ser o moderador do painel **Sob pressão: como responder a ataques em setores críticos**, que também contou com a participação do sócio Leandro Bissoli. Os advogados indicaram as posturas fundamentais em casos de violações, tais como ser ágil e coerente – e não afobado -, e ter um protocolo estruturado conforme a dimensão da sua organização, que inclui detecção, triagem, resposta e lições aprendidas.

Eloisa Crivellaro, Diretora Jurídica e Compliance do CNA Idiomas, falou sobre a experiência de organizar um comitê de privacidade e proteção de dados.

> Foi um processo que resultou em atribuições e estruturações em diferentes áreas, ou seja, definimos responsabilidades para garantir a tomada de decisão baseada num programa de compliance. As regras e procedimentos incluíam desde as ações em casos de incidente, a necessidade de identificação de lacunas até o acompanhamento de mudanças regulatórias.

A especialista em Privacidade da OneTrust Brasil, Érica Costa, criticou o comportamento de muitas organizações nacionais em não tomar medidas preventivas e agir somente depois que os problemas acontecem.

> O mercado brasileiro só atua na dor, com medidas analgésicas. Uma prova é que não temos o hábito de contratar seguros. É necessário acabar com o negacionismo e investir em privacidade. Afinal, um planejamento para evitar incidentes é complexo, abrange vários aspectos da gestão, e precisa envolver todas as pessoas e áreas da empresa.

Abílio Branco, Head de Proteção de Dados da Thales, reforçou a importância de encarar o investimento em segurança não como custo, mas sim como investimento.

> Faz parte do controle do negócio e é indispensável para garantir a governança corporativa. São soluções que evoluem cada vez mais e é fundamental estar em dia com esses recursos, já que o próprio dado tem controle tecnológico para ajudar na resposta rápida quando ocorrem violações.

Para encerrar, a sócia Letícia Málaga foi a moderadora do painel **Tendências para 2022: Data Ethics by Design**, e juntamente com Patricia Peck, apontou as iniciativas essenciais para conseguir estabelecer uma cultura de agilidade que viabiliza a evolução dos negócios digitais.

> O papel do advogado é dar suporte enquanto ainda não existem regulações para determinadas inovações. A governança e a estrutura de uma organização configuram um processo vivo e é função desse profissional ter uma visão multidisciplinar, e agir na consulta e orientação para garantir a segurança jurídica.

Ricardo Leite Raposo, Diretor de Data & Analytics da B3, corroborou a visão de que a governança não é uma estrutura monolítica, e por isso é fundamental pensar em práticas e

metodologias que garantam a agilidade, levem em conta o ecossistema, e tenham como base a ética.

> “É atuar com consistência na gestão, estabelecer uma estrutura de acordo com os valores da organização, ter controle desses processos e permanecer dentro da lei - mas sem deixar de fazer negócios.”

Outro participante do painel foi Alexandre Zavaglia, Data Driven Consultancy da LegalScore, que tratou sobre o desafio de definir a “ethics by AI”, já que os algoritmos funcionam em muitas esferas, mas podem resultar em vieses que trazem consequências negativas para muitas pessoas.

> “De forma prática, é preciso estabelecer muito bem os valores da companhia, com a documentação e monitoramento frequente desses tópicos, que devem fazer parte do ambiente de discussão da empresa. Além de criar um comitê de ética e indicar qual o poder de cada integrante. É essencial para unir o lado social e político dentro da gestão corporativa.”

PROTOCOLO DE RESPOSTA A INCIDENTES | ATAQUES DE RANSOMWARE

Por Henrique Rocha, sócio de Gestão de Crise e Contencioso Digital do Peck Advogados

Dentre os vários tipos de fraudes e investidas realizadas em ambiente digital, o ransomware é o que mais aterroriza encarregados de proteção de dados, gestores de TI e board de diretorias atentas aos desafios da era digital. Somente em 2021, as violações deste tipo aumentaram 92% de acordo com relatório da Infoblox, empresa de soluções de segurança.

Os desdobramentos após um incidente variam de acordo com o contexto de cada organização, mas as dúvidas em relação ao que fazer são um dos aspectos que mais prejudicam a minimização dos prejuízos. As incertezas vão desde as medidas iniciais a serem aplicadas, ou mesmo o que não se deve ou pode fazer, já que tais condutas podem, em alguma medida, não só comprometer a investigação, mas também prejudicar a própria posição da vítima frente aos reguladores de mercado.

A intenção desse breve estudo é justamente abordar os questionamentos mais recorrentes frente a esse tipo de incidente, que se mostra tão desafiador no dia a dia de trabalho da operação de pequenas, médias e grandes companhias, independentemente do tipo de dado tratado.

SIMPLIFICANDO O TEMA

O prefixo ransom, em tradução livre, significa resgate. Eis a explicação terminológica do ataque envolvendo ransomware, que basicamente configura a execução de software malicioso que, ao ser instalado, sequestra os dados da vítima (pessoais ou corporativos), de modo que as informações só são reestabelecidas mediante pagamento de resgate.

Geralmente o valor é exigido em criptomoeda para evitar o rastreamento dos recursos. Logo, o tradicional *follow the money* investigativo fica parcialmente comprometido.

A indisponibilidade de dados causada por esse tipo de incidente digital é desastrosa e pode atingir companhias dos mais variados segmentos, de saúde a financeiro, causando prejuízos de grandes proporções, inclusive em serviços essenciais da sociedade. Um dos mais famosos casos de ransomware foi o WannaCry, responsável pelo maior ataque do tipo já registrado na história recente, que comprometeu indústria, varejo e até mesmo hospitais ao redor do planeta.

A encriptação provocada por esse tipo de ataque é a assimétrica, isto é, dispõe de chave pública para cifrar o conteúdo e chave privada para a liberação ao acesso do conteúdo. Essa última chave é mantida sob a posse do atacante, de forma que somente com o pagamento de resgate, por vezes realizado com criptomoedas, é que a vítima pode obter o acesso aos dados encriptados.

Embora possam sobrevir outros desdobramentos mais graves, como uma exposição posterior dos dados na grande mídia (agravando o incidente), o que o ransomware causa, em geral, é a indisponibilidade de uma informação. Na atual configuração da sociedade digital, esse impedimento do acesso de quem faz uso dos aludidos dados pode interromper operações parcialmente ou mesmo por completo.

Na prática, portanto, ao notar o incidente, a vítima enfrenta em uma crise que deve ser muito bem conduzida para não piorar o cenário já existente.

PROTOCOLO DE MEDIDAS: EXISTE JEITO CERTO DE ENFRENTAR O INCIDENTE?

Ao enfrentar um incidente de ransomware é importante assumir a premissa de que cada caso possui diferentes especificidades, seja em relação a vítima, contexto, reflexos e urgências. Dessa forma, cada ocorrência é gerida de forma artesanal, no modelo *tailor made,* e que pode exigir ou não a execução da mais variada gama de medidas.

Sobre o enfrentamento do incidente, sim, existe uma forma mais adequada para enfrentamento de cada incidente, especialmente os de indisponibilidade de dados, apesar de não haver uma regra única e engessada. Além de analisar o incidente e o risco à privacidade dos titulares, é necessário elaborar relatório de diagnóstico considerando as medidas para defesa em procedimento administrativo (formalização do tratamento do incidente) e comunicar à ANPD e/ou titulares de dados, caso o incidente possa acarretar risco ou dano relevante aos titulares.

Determinados pontos de contato são comuns e podem ser considerados como um roteiro de atuação frente ao problema criado, tais como:

- **Calma e pragmatismo** – No enfrentamento de qualquer incidente, o desespero e a ansiedade em resolver o problema podem ensejar a criação de outros, sejam de relacionamento ou mesmo para reestabelecimento do ambiente afetado. Pensar e agir de forma serena e focada em resultados práticos é um caminho positivo a seguir;

- **Atue em grupo** – Duas cabeças pensam melhor que uma. Conte com apoio de profissionais multisetoriais para compor um gabinete de crise. Em geral, o time jurídico precisa apoiar o time técnico e ambos serem bem compreendidos pela área de comunicação, seja ela interna ou externa, a fim de viabilizar uma atuação harmoniosa e coordenada em um momento de tensão e incertezas;

- **Preserve o ambiente** – Sempre que possível, é altamente recomendável recuperar o ambiente sem comprometer os registros para uma investigação. Por vezes, ao se reconstruir por completo um ambiente atacado, perdem-se também rastros digitais para a investigação e identificação das nuances do ataque sofrido;

- **Mão de obra qualificada** - Conte com apoio de especialistas, técnicos jurídicos e forenses, pois às vezes o que se assume como grave prejuízo, pode ser enfrentado e resolvido de forma mais amena;

- **Lições aprendidas** – Apesar do enfrentamento de crise parecer um trauma irreversível, o time que lida com esse desafio torna-se maior e mais resiliente com base nas lições aprendidas, sejam a causa, efeito ou cultura vivenciadas no episódio.

DEVO OU NÃO NOTIFICAR UM INCIDENTE?

Entendemos que a resposta correta é a preferida dos advogados: depende. Isso porque nem todo incidente causado por um ransomware envolve dados pessoais e, ainda que assim o fosse, a notificação à Autoridade Nacional de Proteção de Dados (ANPD) é obrigatória apenas no caso de dano ou risco relevante ao titular de dados.

Ainda que sobrevenha eventual dúvida se o incidente é ou não relevante, não se vislumbra uma regra para gerar a comunicação e enfrentar os desdobramentos questionadores do órgão - que demandarão mais esforço, tempo e esclarecimentos complementares.

Diante de uma ocorrência, é necessário uma reflexão madura e ponderada em fatos e provas acerca do grau de risco do incidente avaliado. Dificilmente um envio errôneo de simples e-mail contendo alguns poucos dados pessoais ensejaria o dever de comunicação ao regulador. Mas não são raros os casos em que, por temor desmedido ou certa inocência, o controlador assim procede e fica à mercê de consequências imprevisíveis, sejam internas ou externas, para com a autoridade ou mesmo com o titular envolvido.

Além disso, também existem normas e regras específicas determinadas por órgãos reguladores de cada setor e que podem demandar notificação. Algumas determinações nesse sentido são importantes de destacar:

- Empresas de capital aberto com ações listadas na bolsa de valores devem atender às disposições previstas na Instrução nº 358 da Comissão de Valores Mobiliários (CVM) quando algum fato relevante ensejar o comunicado ou ocorrer um incidente de segurança da informação "que afete processos críticos de negócios, ou dados ou informações sensíveis, e tenha impacto significativo sobre os clientes deve ser considerado relevante", conforme art. 35-D, §4º da Instrução nº 505 do mesmo regulador.

- No campo da saúde, a Agência Nacional de Saúde (ANS) editou a Resolução Normativa 443/2019 que versa exatamente sobre a obrigatoriedade das operadoras de saúde em atenderem e observarem os riscos inerentes ao tratamento de dados em seus sistemas, e o dever de gerir seus riscos com "vistas a conduzir tomadas de decisão que possam dar tratamento e monitoramento dos riscos e consequentemente aperfeiçoar os processos organizacionais e controles internos da operadora", conforme arts. 6º, III e 9, II da aludida RN.

- A Superintendência de Seguros Privados (SUSEP), por meio de sua Circular nº 638/21, determina em seu Capítulo V que além de registrar eventuais incidentes de segurança, as empresas submetidas a esse segmento devem realizar a cabível "comunicação com as partes afetadas pelo incidente,

sobretudo clientes e comunicação prévia com prestadores de serviços, parceiros e outras partes potencialmente envolvidas, com vistas à adoção de uma resposta coordenada", conforme art. 5º, VII e § 1º da Circular.

Com efeito, é sabido que nem todo incidente deve ser comunicado à ANPD, mas é imperioso que o controlador de dados ou mesmo a empresa que sofra com eventual incidente de segurança da informação, mesmo que não envolva dados pessoais, deve sempre observar se o segmento de atuação e seu respectivo agente regulador não exigem a comunicação, de forma não só a enfrentar o incidente em curso, mas também evitar a criação de um outro desafio frente ao órgão fiscalizador.

PAGAR OU NÃO PAGAR O RESGATE?

A recomendação primeira para essa dúvida é, em regra, negativa. Além da questão moral, no sentido de não se negociar com criminosos, como as organizações que praticam o ransomware, paira a incerteza quanto à efetiva liberação das chaves de decriptação. Ainda é comum o pagamento ser realizado e os arquivos manterem-se bloqueados mesmo após o fornecimento da suposta chave de decriptação.

Há uma terceira justificativa para não pagar, que encontra respaldo em orientações de autoridades ao redor do mundo, como o próprio *Federal Bureau of Investigation* (FBI), que apresenta postura categórica ao desaprovar esse tipo de medida, que pode ser propagada e melhorada com recursos advindos de vítimas lesadas, gerando um círculo vicioso no mercado.

Uma quarta justificativa para o não pagamento é a interpretação de que vítima de hoje seja um possível alvo no dia de amanhã, tanto pela vulnerabilidade explorada, como pela "colaboração" com o pagamento de um resgate por vezes dotado de expressivo valor.

Por fim, uma quinta e última razão milita pelo não pagamento de resgate, já que muitas organizações internacionais desenvolvem plataformas e ferramentas para auxiliar as vítimas

desses ataques, como é o caso da *No More Ransom*[1]. Assim, antes de realizar o pagamento, é imperioso averiguar se o software que infectou sua máquina já não goza de solução disponível, afastando a razão para qualquer pagamento de resgate.

A despeito das recomendações majoritárias pelo não atendimento do resgate exigido, não se descarta o pagamento de determinado resgate a fim de evitar um prejuízo ainda maior para a vítima, já que um dia de operação parada pode se mostrar muito maior que valor exigido pelo atacante.

COMUNICAR OU NÃO A POLÍCIA?

Em números absolutos, os ataques digitais já causam um prejuízo financeiro na casa dos 6 trilhões de dólares, conforme levantamento da consultoria alemã Roland Berger, e o Brasil é o 5º maior alvo de ataques no planeta[2].

Além do alinhamento à expectativa de esclarecimento e punição dos responsáveis por um ransomware ou qualquer outro incidente de igual relevância, tem-se que observar dois outros aspectos: um jurídico e outro reputacional.

O jurídico decorre do fato de que, diferente do servidor público e da própria autoridade policial, a vítima de um ataque digital ou mesmo de um crime não é obrigada a comunicar a autoridade policial, já que é dever desta providenciar a investigação cabível, conforme art. 6º e 301 do Código de Processo Penal. Logo, a comunicação a autoridade policial, a despeito de trazer alguma esperança e conforto à vítima e se constituir em importante instrumento de política social (já que informará ao Estado o volume de ilícitos ocorridos em determinada matéria, área ou contexto), não se constitui em obrigação para a parte.

Sob a ótica reputacional, é preciso ponderação e maturidade sobre o momento certo de se comunicar a autoridade policial, sob pena de, a depender desse desdobramento, agravar-se ainda mais o cenário por vezes já caótico de uma crise.

1 - A associação disponibiliza, de forma gratuita e com atualização periódica, uma série de chaves de decriptação para liberação de ataques sofridos. Disponível em https://www.nomoreransom.org/pt/index.html Acesso em 09/11/2021.
2 - Disponível em https://economia.uol.com.br/noticias/estadao-conteudo/2021/09/12/brasil-e-5-maior-alvo-de-ciber-crimes.htm Acesso em 09/11/2021.

CONCLUSÃO

Como resumo, tem-se que muitas nuances devem ser avaliadas frente a cada incidente de ransomware, como se há o comprometimento da indisponibilidade da informação ou até se gera eventual exposição dos dados colhidos pelo atacante.

Não se vislumbra, assim, uma regra única para condução desses incidentes, que devem contar com atenção dedicada de um time especializado e maduro para gerir a crise e garantir que ela não se agrave, interna ou externamente, sempre zelando pela transparência e interesses dos envolvidos, como a própria instituição vitimada.

Esclarecidas questões conceituais sobre o ransomware e sobre a necessidade ou não de comunicação aos agentes reguladores, que vão muito além da atenta ANPD, é imperioso que o enfrentamento do incidente e gerenciamento da crise sejam realizados com pragmatismo e serenidade, já que por vezes contexto externo de uma *war room* queira impor.

Peck

Advogados

Direito para Inovação Digital

Apoiadores:

CREDILINK® INFORMAÇÕES DE CRÉDITO

SIKUR

tabapuã CONSULTORIA EM SEGUROS

THALES Together • Safer • Everywhere

OneTrust PRIVACY, SECURITY & GOVERNANCE

Siga-nos nas Redes Sociais: