# Evento discute “Ransomware – Prevenção e Reação a Ataques Cibernéticos” com sócios de diferentes especialidades; leia o e-book e reveja trechos

**05.10.2021 5 minutos de leitura**


**Autores**

**Francisco Antunes Maciel Müssnich (Chico Müssnich)**

**Felipe Palhares**

**Fernanda Pereira Carneiro**

**Luís Flaks**


**Áreas relacionadas**

Proteção de Dados e Cybersecurity

**Assuntos**

Proteção de Dados e Cybersecurity | Segurança Cibernética

Ataques de ransomware têm se tornado cada vez mais frequentes ao redor do planeta. A prática, que consiste em fazer um ataque digital com objetivo de cobrar resgate pelos dados sequestrados e criptografados, foi intensificada com o contexto pandêmico, que expôs muitas falhas de segurança nas empresas.

Um ataque dessa magnitude, que pode inclusive ameaçar divulgar dados sigilosos, gera diferentes impactos, alguns deles para os quais as empresas e seus diretores podem se preparar previamente. Por isso, tornou-se um tema extremamente debatido dentro do direito digital.

Para discutir as diferentes implicações desses ataques cibernéticos por distintos vieses, os sócios do BMA promoveram o webinar multidisciplinar "Ransomware – Prevenção e Reação a Ataques Cibernéticos" na quinta-feira, 30 de setembro.

Com abertura de Francisco Müssnich, que também moderou as perguntas respondidas ao final, a apresentação contou com explanações de Felipe Palhares, sócio das áreas de Proteção de Dados e Cybersecurity e Tecnologia e Negócios Digitais.

Bernardo Weaver, sócio das áreas de Penal Empresarial e Compliance, Investigações & Direito Sancionador; Luís Loria Flaks e Fernanda Carneiro, sócios da área de Direito Societário; e Franciny de Barros, sócia da área de Direito Tributário. Clique aqui para conferir trechos do webinar.

"Todas as companhias, abertas ou fechadas, têm discutido a questão da proteção de dados de forma bem profunda.

O BMA tem tido um resultado muito profícuo em gestão de riscos", disse Chico Müssnich, do nosso escritório de advocacia, ao abrir o evento, concluindo com uma frase emprestada de uma poesia de sua filha que representa bem o que é preciso fazer em momentos delicados como um ataque cibernético: "Tomar decisões é o melhor modo de prever o futuro".

## A ANATOMIA DO ATAQUE E QUESTÕES PENAIS

Palhares deu seguimento ao evento lembrando que o Brasil é o segundo país mais afetado por ataques de ransomware no mundo e que uma das medidas mais eficazes é justamente investir em prevenção e informação, para que todos saibam o que fazer caso seja necessário.

"Toda organização deveria ter um plano de resposta a incidentes, um documento que prevê passo a passo o que todos os colaboradores precisam fazer em caso de um incidente, e treinar as pessoas nesse plano, como fazem com os treinamentos de incêndio", explicou.

"Um segundo ponto é avaliar a contratação prévia de assessores externos, para que, na hora de um incidente, você já saiba quem acionar. No momento em que um ataque é anunciado, é crucial contar com quem já passou por isso, todo segundo importa.

Aqui no BMA, nós temos uma hotline ransomware, para que nossos clientes que passem por isso possam entrar em contato com o time a hora que for", exemplificou Palhares, que disse ainda que os ataques de ransomware hoje estão ainda mais sofisticados. "Antes, eles só criptografaram seus arquivos e você não conseguia acessar suas informações.

Hoje, eles fazem uma extorsão dupla, dizem que não vão devolver a chave criptográfica e, se isso não for importante porque você faz backups recorrentemente, o hacker fala que vai vazar todas as informações da sua organização e vai fazer isso publicamente para saberem que você foi afetado e não quis pagar pelo resgate", contou.

Além das preocupações com o ataque em si, é preciso notificar uma série de autoridades sobre o ocorrido. "Do ponto de vista técnico, esses crimes são muito sofisticados e de difícil elucidação", lembrou Bernardo Weaver, sócio de Direito Penal Empresarial do nosso escritório de advogados.

"É preciso deixar bem claro que a companhia foi vítima de um crime. Dado isso, não existe uma obrigação legal de que a vítima de qualquer crime registre esse crime perante as autoridades, o que não quer dizer que isso não precise acontecer. Essa é uma análise muito difícil, que vai ser baseada em uma investigação que vai ser a base de várias tomadas de decisão", concluiu Weaver.

## AS PREOCUPAÇÕES DAS COMPANHIAS ABERTAS E IMPACTOS FISCAIS

"Ransomware não é algo que não se prevê mais. A diretoria de uma companhia não pode dizer que não sabia que isso poderia acontecer, se diz hoje que não é se vai acontecer, mas quando vai acontecer", resumiu Luis Flaks, nosso sócio de Societário.

No caso de companhias abertas, é preciso um cuidado extra com as ações

negociadas em bolsa e possíveis informações vazadas, além, claro, da avaliação da necessidade de notificar órgãos competentes, como a Comissão de Valores Mobiliários (CVM), e de realizar um comunicado ao mercado ou fato relevante, dependendo do desenrolar do ataque.

"A primeira coisa que a gente recomenda para as companhias abertas é que, no início do ataque, comece um blackout period, porque isso protege todo mundo. Não é preciso avisar o motivo do blackout period, só anunciar. Ao final do período, quando resolvido o problema do ataque, tem que se tomar a decisão se vai soltar um fato relevante ou não, observando se houve ou não oscilação de mercado", apontou Flaks.

Registrar todos os passos também é essencial para proteger a companhia. "Quando a companhia sofre um ataque desses, a administração volta toda a sua energia para resolver a crise, mas numa companhia aberta você tem que ter esse cuidado a mais para não ter problemas com a CVM.

Há uma questão procedimental muito forte, é importante deixar tudo registrado e ter um plano de ação antes do ataque começar", completou Fernanda Carneiro, que lembrou ainda que as medidas de prevenção citadas por Palhares são essenciais para proteger a diretoria em eventuais investigações.

Nossa sócia de Societário explicou ainda que as penalidades podem ser bastante elevadas para as companhias em caso de insider trading. "Um administrador, mesmo quando tem um seguro de D&O, esse seguro não cobre casos de insider porque ele é só para casos de gestão.

A pessoa realmente tem que ficar muito atenta a esses aspectos", concluiu. "Não negocie, nem deixe que terceiros de sua confiança negociem as ações da companhia quando existe alguma coisa nessa linha", reforçou Müssnich.

Passado o susto com o ataque e sua resolução imediata, é preciso seguir vigilante em relação aos documentos que podem ter sido atingidos e notificar todas as autoridades competentes. "Obviamente, as implicações fiscais em torno desse tema não estão no radar quando um ataque dessa natureza acontece, mas, como em quase tudo na vida, há implicações fiscais.

A depender do ataque que aconteceu, pode haver o sequestro de documentos e arquivos fiscais e pode ser preciso avisar a Receita. Não raro são criminosos internacionais que estão envolvidos e isso demanda a contratação de consultores internacionais, o que pode implicar em uma alta tributação, entre outras questões", listou Franciny de Barros, nossa sócia de Direito Tributário.

Quer saber mais sobre Ransomware? Confira o e-book que nossos sócios prepararam sobre o tema.

› PROFISSIONAIS

# Profissionais que aliam visão jurídica e visão de mercado

**Francisco Antunes Maciel Müssnich (Chico Müssnich)**

**Felipe Palhares**

**Fernanda Pereira Carneiro**

**Luís Flaks**