Crimes Digitais e guerra cibernética são discutidos no “Papo Digital: Mesa Redonda”; confira o webinar

12.08.2021 4 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Compliance, Investigações e Direito Sancionador | Proteção de Dados e Cybersecurity | ANPD | Eventos | LGPD | Home Office | Felipe Palhares | Segurança Cibernética | Incidentes de segurança | Vazamentos de dados pessoais | Pandemia | Papo Digital | Penal Empresarial | Gerenciamento de riscos

Tornar-se digital é necessário a qualquer empresa que deseja manter-se relevante e atual no mercado, especialmente após a pandemia de COVID-19, onde o *home office* e *lockdowns* se tornaram uma saída para tentar desacelerar a disseminação do coronavírus. No entanto, a celeridade imposta pela pandemia para que essa inclusão digital acontecesse permitiu que criminosos observassem uma oportunidade para atacar o bem mais valioso de qualquer empresa do século XXI: seus dados.

Para conversar sobre **"Crimes Digitais e Guerra Cibernética"**, o **"Papo Digital: Mesa Redonda"**, série de webinars capitaneada pela área de Proteção de Dados, Tecnologia e Negócios Digitais do BMA, promoveu um bate-papo nesta terça-feira, 10 de agosto. A conversa, moderada pelo nosso sócio de Proteção de Dados Felipe Palhares e disponível acima e no canal do Youtube do escritório, contou com **Arthur Sabbat**, Diretor da Autoridade Nacional de Proteção de Dados (ANPD), **Rafael Galera**, diplomata e Coordenador-Geral de Segurança da Informação e de chefe da Equipe de Tratamento de Incidentes de Rede do Itamaraty, e Bernardo Weaver, sócio das áreas de Penal Empresarial e Compliance, Investigações & Direito Sancionador do BMA.

CIBERCRIMES, INVESTIGAÇÃO E PANDEMIA

"As características desses crimes se alteraram bastante. Os ataques cibernéticos eram motivados por manifestações de cunho político ou ideológico, com objetivo de provocar ou desacreditar determinado órgão. Agora, o que temos visto são ataques mais orientados para conseguir dados pessoais, ou para comercialização na deep web, ou para fraude. Por conta da pandemia, tem crescido os crimes para obtenção de ganhos financeiros, muitas tentativas de invasão e quebras de sistema com esse fim", contextualizou Arthur Sabbat. "É interessante observar essa mudança do criminoso, que era a pessoa que mostrava que conseguia acessar um sítio oficial, que ele conseguia estar lá naquele lugar, e agora ele ataca com fins financeiros", complementou Felipe Palhares.

Os crimes digitais carregam ainda uma particularidade na sua investigação, já que máscaras de IP e encriptação podem dificultar o acesso aos responsáveis, como explicou nosso sócio Bernardo Weaver. No entanto, "a gente viu esse incremento momentâneo na pandemia, mas os crimes digitais são apenas crimes. É que a vida ficou mais digital e os crimes começaram a acontecer também na vida digital", contou ele. "Dizem que os dados são a nova corrida do ouro, o novo petróleo, mas nem todas as empresas guardam os seus dados com o mesmo zelo com o qual

guardariam ouro ou petróleo. Isso, nesse momento da pandemia, permitiu que os oportunistas tenham tido êxito. Ainda mais porque existe essa dificuldade de prova, ainda que você saiba onde coletá-la", completou nosso novo sócio.

Um marco recente que certamente fortalecerá a legislação de dados brasileira foi a adesão a Convenção de Budapeste, comitê de especialistas para lidar com a "cibercriminalidade". "Isso nos dá uma série de ferramentas para lidar com esses crimes. Existem três formas de lidar com ataque cibernético, desde a esfera penal/criminal, a esfera diplomática e a esfera militar, que ainda não ocorreu efetivamente", explicou Rafael Galera. "Com a adesão a Convenção, nos obrigamos a ter uma nova quantidade de tipificações, para estar bem coberto em relação aos crimes digitais", elogiou Weaver, que acredita que o investimento de energia brasileiro não precisa necessariamente ser legislativo, mas "de capacitação técnica e de recursos para as autoridades investigarem" os crimes digitais.

Em sua fala, o diplomata lembrou ainda de reunião recente entre os mandatários dos Estados Unidos e Rússia parece ter surtido efeito para mitigar ações de grupos hackers supostamente russos. A pressão diplomática norte-americana supostamente fez com que sites de grandes grupos hackers saíssem do ar logo após o encontro entre Joe Biden e Vladimir Putin.

PAGAMENTO DE RESGATE

E no caso do sequestro de dados, o que os especialistas recomendam? Sabbat e Galera são contundentes em afirmar que o mais importante é que as organizações invistam em backup para não correr o risco de perder todas as suas informações caso se torne refém de criminosos digitais. Ambos acreditam também que não deve ser pago o resgate para os ciberbandidos. "Creio que não seja o caso de pagar porque corre-se o risco também do criminoso não restituir aqueles dados todos. Aconselho que a organização cuide bem dos seus dados e tenha sempre backup, porque, sem ele, ela está se expondo a um risco enorme", pontuou o diretor da ANPD. Galera fez coro: "Fazer backup é básico e, com o avanço da computação em nuvem, é barato também fazer a cópia. Quando a gente começa a pagar esses resgates, acabamos incentivando outros grupos a fazer esses ataques. Por mais que, para pessoa que sofreu o ataque compense, para a política pública isso é muito ruim".

Weaver, no entanto, acredita que cabe uma avaliação caso a caso. "É uma análise muito difícil e que vai ser feita em um momento muito delicado. As companhias precisam estar organizadas com seus comitês de crise e estar bem assessoradas para tomar essa decisão. Entendo o dilema de não pagar, mas ao contrario de outros bens, os dados têm uma natureza diferente. Uma vez feitos públicos, eles podem perder valor. O valor deles pode estar justamente no fato deles serem sigilosos, e aí não adianta ter backup", ponderou.

Leia mais:

- E-book – LGPD
- E-book – Incidentes de Segurança: Como Reagir

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares