Advogado, perito em crimes cibernéticos, José Milagre, participa de uma entrevista para o CBN Campinas e alerta sobre possíveis golpes usando o nome de Brumadinho

Nosso advogado e perito em crimes cibernéticos, José Milagre, da uma entrevista para o CBN Campinas e alerta a todos sobre possíveis golpes utilizando a tragédia de Brumadinho.

Veja a matéria completa: https://portalcbncampinas.com.br/2019/01/advogado-perito-em-crimes-ciberneticos-jose-antonio-milagre-alerta-sobre-possiveis-golpes-usando-o-nome-de-brumadinho/

Perito em informática participa do programa Record News e alerta a todos contra golpes na internet nesse período de Pandemia do

Covid-19

O Perito em crimes cibernéticos , José Milagre, participou do programa Record News e alerta a todos contra criminosos que aproveitam para aplicar golpes na internet durante a pandemia do Covid-19.

Veja a matéria completa: https://www.youtube.com/watch?v=0prgpwmMyqM

VINGANÇA PORNÔ: O que fazer em casos de publicação de fotos ou vídeos íntimos na Internet?

José Milagre esclarece sobre a vingança pornô (revenge porn), e quais orientações as vítimas devem seguir para remover esses conteúdos de WhatsApp e Internet.

Procure um Perito em Informática.

Os direitos de quem perde

Bitcoins em corretoras e intermediadores

José Antonio Milagre

Não incomum no mundo todo problemas envolvendo segurança digital de corretoras, onde bitcoins são perdidos ou até mesmo “furtados”. Recentemente, a maior corretora de Bitcoins do Brasil, a FOX BIT, ficou fora do ar e perdeu R$ 1 milhão em saques duplicados.

Ao que parece, existiram 130 saques em duplicidade, algo em torno de 30 bitcoins perdidos. Alguns investidores já haviam demonstrado dispostos a devolver o dinheiro e a empresa já teria informado que teria caixa proprietário para cobrir as despesas. Não há duvidas que este é um processo demorado e complexo.

Logicamente que diante da falha, o sistema saiu do ar para manutenção. Embora não tenha sido um “ataque” hacker, questão que paira é sobre os direitos daqueles que são lesados em casos análogos ou similares. Os danos são desde a indisponibilidade do serviço e transações até mesmo àqueles que tiveram suas contas afetadas. Em que pese Exchange não sejam carteiras, a simples afirmação não pode afastar responsabilidade de quem lida, custodia, armazena, ainda que temporariamente, bitcoins de terceiros.

Não bastasse, o volume do Bitcoin no Brasil caiu 50% após a corretora ficar off-line. Assim, não importa se fora invasão ou falha de qualquer natureza. A resposta, satisfação aos investidores e garantias para cobertura dos fundos deve ser imediata, não podendo o consumidor responder por ações que não deu causa, em que pese armazenar ainda que transitoriamente bitcoins em Exchange, não seguindo recomendações de segurança. No caso em específico, a corretora está agindo corretamente,

prestando informação clara, posicionando-se e detalhando cada passo realizado para retorno das atividades.

No geral, alguns casos no mundo envolvendo Direito Digital já estão ligados a responsabilização de serviços de intermediários. Deve-se deixar claro que há evidente prestação de serviços realizada pelas corretoras. O usuário, em um ambiente descentralizado, podendo optar pelo risco de transacionar por conta e ponto a ponto, escolhe aquela empresa que lhe oferece maior segurança, agilidade, informações claras e logicamente, tem o direito de recuperar moedas roubadas em casos de incidentes ou ser ressarcido à altura do dano.

Havendo falha na prestação dos serviços, existe o direito à reparação, considerando igualmente que o serviço é prestado mediante comissionamento. Ainda que os termos de serviço da plataforma estabeleçam em sentido contrário, é importante mensurar, só vale o que está de acordo e não fere o Código de Defesa do Consumidor.

NOTAS:

1 Neste artigo do CONJUR https://www.conjur.com.br/2018-jan-02/jose-milagre-direito-cliente-corretora-bitcoin-quebre eu aprofundo a discussão sobre alguns direitos dos investidores em criptomoedas.

2 Recomendo igualmente a leitura deste trabalho “Bitcoin: Questions, Answers, and Analysis of Legal Issues” do Congressional Research Service https://fas.org/sgp/crs/misc/R43339.pdf

3 Já existem decisões judiciais no mundo, como a que determinou a perda de Bitcoins Roubadas https://www.coindesk.com/judge-orders-dea-stolen-bitcoin/

4 É possível recuperar os bitcoins? https://bravenewcoin.com/news/csi-crypto-can-victims-recover-stolen-coin/

O Direito Brasileiro e aspectos legais envolvendo a espionagem pela NSA de dados de brasileiros

Inicialmente o vazamento do programa PRISM e recentemente, mais documentos que comprovam a espionagem americana em relação ao Brasil. Diariamente novos documentos vazados por Snowden ganham os noticiários.

Fica claro que a espionagem americana vai além dos fins de combate ao terrorismo e alcança civis, inocentes e pessoas sem qualquer ligação. Pelo que os documentos indicam, a utilização de sistemas *"Flying Pig" e "Hush Puppy"* monitorariam redes TLS/SSH de diversas companhias pelo mundo.

Técnicas de invasão, exploração de vulnerabilidades em criptografia e monitoramento eram discutidas nos documentos secretos que ensinam a "espionar". O fato é que o grande impulso da espionagem está nas vulnerabilidades em sistemas usados pelo Brasil e na cooperação de empresas de tecnologia e provedores de acesso.

Estamos a falar de empresas privadas, algumas com filiais no Brasil, que são consideradas co-autoras deste processo de espionagem ainda em fase investigativa. A própria ANATEL já declarou que iria investigar, juntamente com a Policia Federal, a atuação destes provedores. Entender como estes dados são captados é fundamental para adoção da resposta jurídica ou diplomática adequada. Esse é o desafio.

Uma das penas cabíveis para as teles que eventualmente

cooperaram para a agência americana é o cancelamento da licença de operação, considerando a proteção constitucional ao sigilo das comunicações, proteção esta também regulamentada pela agência.

A resposta do Brasil poderia ser o cancelamento de pactos e acordos com os Estados Unidos, até o esclarecimento dos fatos envolvendo a NSA, como aliás fora feito na Alemanha. Além disso, é interessante que a questão seja efetivamente levada a ONU, considerando a grave violação à Convenção de Viena e ao pacto internacional sobre Direitos Civis. Pressão junto a UIT (União Internacional de Telecomunicações) também demonstra-se interessante, sobretudo para estabelecer procedimentos para auditoria dos equipamentos e seus sistemas, evitando-se "códigos maliciosos ou vulnerabilidades embutidas". A democratização da ICANN (*Internet Corporation for Assigned Names and Numbers*), hoje conduzida pelo departamento de defesa norte-americano, é também pauta indispensável.

No Brasil, não consideramos ainda criptografia como algo estratégico e indispensável a segurança nacional e isto deveria ser revisto. Os Estados Unidos controlam a "exportação de armas cibernéticas", onde incluem-se ai tecnologias de criptografia e invasão. Coincidentemente, quem regula a exportação de criptografia nos Estados Unidos é o mesmo departamento que controla o ICANN, diga-se, o *Bureau of Industry and Security* do Departamento de Defesa. Nosso orçamento em defesa também necessita ser aprimorado, já que nos Estados Unidos, um quinto do orçamento anual é usado para financiar programas e operações de criptografia.

Se no âmbito internacional, ainda estamos na era da auto-composição, no âmbito interno, não restam duvidas que a o Marco Civil deve ser aprovado, com disposições que condicionem o armazenamento dos dados de brasileiros no Brasil ou que pelo menos fortaleçam nossa infraestrutura, hoje tão dependente da Estrutura Americana.

O Anteprojeto de proteção de dados pessoais também traz garantias essenciais em face do tratamento indevido de dados feito por provedores que prestam serviços no Brasil e incrementaria a proteção à privacidade dos cidadãos.

Ademais, do que diz respeito à responsabilização jurídica dos provedores "co-autores" do monitoramento, nos termos da Lei de Introdução às Normas do Direito Brasileiro, temos que para qualificar e reger as obrigações, será a aplicada a lei do país onde se constituírem, e, destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada.

Não bastasse, segundo a lei em comento, é competente a autoridade judiciária brasileira, quando for o réu domiciliado no Brasil ou aqui tiver de ser cumprida a obrigação.

E por fim, por mais que se alegue que nos EUA existam leis que permitam a espionagem ou o tratamento de dados de estrangeiros (como o Patriot Act), nos termos de nossa legislação introdutória ao Direito Brasileiro, especificamente no art. 17, tem-se que as leis, atos e sentenças de outro país, bem como quaisquer declarações de vontade, não terão eficácia no Brasil, quando ofenderem a soberania nacional, a ordem pública e os bons costumes.

Deste modo, segundo a lei processual civil brasileira, serão representados no Brasil, ativa ou passivamente, em ações movidas por cidadãos e inocentes por violações de dados, efetivamente comprovadas, a pessoa jurídica estrangeira, pelo gerente, representante ou administrador de sua filial, agência ou sucursal aberta ou instalada no Brasil.

O vazamento das informações sigilosas trouxe à tona um grande debate: A discussão sobre o gerenciamento da Internet. Mais cedo ou mais tarde, um dia veríamos este tema na pauta dos países. Era necessário apenas um vacilo dos Estados Unidos. Mais que isso, o vazamento de documentos ultrassecretos

reforçou a necessidade de infraestrutura de defesa cibernética e meios legais para proteção do nacional lesado no indevido tratamento de seus dados pessoais por pessoas jurídicas estrangeiras. O desafio está apenas começando.

Por fim uma boa dica para quem quer minimizar a exposição de dados em face do PRISM.