Fernanda Kac: Colaboração é essencial sucesso do cibersecurity

No fim de setembro desse ano, a Organização dos Estados Americanos (OEA), atenta aos avanços dos crimes cibernéticos ao redor do mundo e ao crescimento da preocupação dos países com a segurança cibernética, promoveu um Simpósio de Cybersecurity em Washington, D.C. (EUA).

Durante quatro dias de intensos debates, diversos profissionais de 26 países da América Latina, inclusive do Brasil, reuniram-se para discutir os desafios envolvendo a segurança cibernética, bem como para fomentar as estratégias necessárias à proteção da rede mundial de computadores.

Parece ser um consenso entre os especialistas da área a ideia de que todos estamos sujeitos a ataques cibernéticos, sendo uma questão de “quando” e não “se” seremos vítimas um dia.

Nessa linha de raciocínio, o fortalecimento da segurança cibernética no desenvolvimento das atividades tanto no setor público, como também no setor privado, apresenta-se como uma premissa primordial cada vez mais defendida pelos profissionais da área.

Não por outro motivo, os investimentos em cybersecurity ao redor do mundo vêm crescendo exponencialmente à medida em que os criminosos vão aprimorando suas técnicas de ataques a pessoas físicas, governos e empresas privadas, especialmente com o uso de tecnologia avançada, dificultando a investigação dos incidentes pelas vítimas.

Diante desse cenário, a prevenção em relação aos ataques cibernéticos significa dificultar a atuação dos criminosos de forma a evitar ser alvo de oportunidade.

Muito embora os ataques cibernéticos mais conhecidos sejam o *Phishing*, *Ransomware*, *Botnets*, DDOS, existem muitos outros que não são de conhecimento do público em geral, o que denota a grande quantidade de modus operandi dos criminosos e a dificuldade enfrentada para a proteção dos ambientes virtuais.

Tanto isso é verdade que pesquisa realizada pela Kroll Global Fraud Risk Report em 2017, com 540 executivos de diversos países, apontou que 86% dos executivos em cargos de liderança passaram por incidentes cibernéticos.

No Brasil, 89% dos executivos afirmaram já ter sofrido uma fraude cibernética em suas companhias.

Os alvos das ameaças se concentraram em informações dos clientes (47%) e segredos industriais ou de pesquisas (44%), sendo que os agentes foram em sua maioria ex-funcionários (32%) e concorrentes (21%). Além disso, 80% dos entrevistados acredita que as fraudes impactaram negativamente a privacidade, segurança e satisfação dos consumidores (80%), além do moral dos funcionários (76%).[1]

O fator humano no comprometimento da segurança cibernética das empresas também deve ser avaliado, na medida em que estudo da Kapersky Lab aponta que apenas 12% dos funcionários conhece e respeita as políticas em vigor nas organizações, razão pela qual o desconhecimento das regras de segurança tem vitimado empresas em todo o mundo[2].

No que diz respeito especificamente à proteção dos ambientes virtuais das instituições financeiras, o Banco Central do Brasil editou a Resolução 4.658 em abril desse ano, dispondo sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados.

De acordo com a referida resolução, os prazos a serem atendidos pelas instituições financeiras são:

- 23 de outubro de 2018: Apresentação ao Bacen de cronograma de adequação, para instituições que já tenham serviços relevantes contratados;
- 06 de maio de 2019: Aprovação da Política de Segurança Cibernética e Plano de Ação e Resposta a Incidentes;
- 31 de dezembro de 2021: Prazo máximo para adequações a serem previstas no cronograma.

Em resumo, as instituições financeiras devem demonstrar a sua capacidade para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, disseminando a cultura de segurança cibernética para seus funcionários, parceiros e clientes de forma proativa.

Paralelamente, a Lei Geral de Proteção de Dados Brasileira (LGPD – Lei 13.709/18) foi sancionada em 14 de agosto desse ano, após oito anos de debate e com base no Regulamento de Proteção de Dados da União Européia (GDPR – General Data Protection Regulation).

Aplicável a qualquer pessoa, seja natural ou jurídica de direito público ou privado que realize o tratamento de dados pessoais (artigo 5º, inciso X), a nova lei trará impactos para diversas empresas, assim como para as instituições financeiras, que coletam dados pessoais que permitem a identificação de uma pessoa natural (artigo 5º, inciso I).

Importante destacar as disposições contidas nos artigos 46 e 50 da LGPD, que tratam da adoção de medidas de segurança com o intuito de proteger os dados pessoais de acessos não autorizados ou tratamento inadequado, bem como de boas práticas de governança com estabelecimento de regras para a organização.

No caso de descumprimento das disposições legais, são definidas diversas sanções administrativas, havendo a possibilidade de aplicação de multa de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50 milhões por infração.

Diante do panorama geral aqui delineado sobre as questões envolvendo a segurança cibernética, além da proteção em si do ambiente virtual, mediante a contratação de ferramentas tecnológicas avançadas e força de trabalho treinada para atuar na área de *cybersecurity*, também é altamente recomendável a investigação dos incidentes de segurança com o máximo rigor, de forma a contribuir para a identificação

dos criminosos cibernéticos, evitando-se que novas vítimas sejam atacadas.

Não há dúvida de que os ataques cibernéticos representam um problema comum a todos os países, tornando o debate do tema extremamente relevante no cenário econômico atual.

Nesse escopo, alguns países já estão bem avançados em relação a uma Política Nacional de Cybersecurity, como é o caso dos Estados Unidos, trazendo diretrizes e apontando um norte para a segurança do espaço cibernético[3].

Durante o Cyber Security Summit Brasil 2018, evento que reuniu a cúpula mundial da segurança cibernética, o Chefe de Operações e Attaché do FBI no Brasil, David Brassanini, ressaltou a importância da união de especialistas e corporações na luta contra o cibercrime: “Tudo indica que, em algum momento, nós tenhamos de juntar forças. E por que não juntar agora?”[4]

Diante de tantos desafios envolvidos no combate ao cibercrime, seguramente o engajamento de diferentes profissionais com *backgrounds* diversos auxilia na visão mais ampla do problema e na busca de soluções cada vez mais efetivas.

Nesse momento em que todos os olhos estão voltados para a proteção de dados, por exemplo, com o já vigente GDPR europeu (General Data Protection Regulation) e a LGPD brasileira (Lei Geral de Proteção de Dados) que entrará em vigor em fevereiro/2020, não evoluir com a segurança do ambiente cibernético terá o mesmo significado que não evoluir com a própria tecnologia e ficar para trás em relação aos demais.

Diante disso, evidente que a palavra-chave para o sucesso das estratégias de *cibersecurity* é a colaboração, mediante o intercâmbio de informações entre todos os países, no âmbito mundial, e entre empresas, governo, acadêmicos e sociedade no âmbito nacional.

Não se ignora os entraves vislumbrados em razão da soberania dos países, concorrência comercial, proteção de reputação, entre outros, mas a reunião de forças parece ser o único caminho viável para garantir a segurança do espaço cibernético.

---

1 Fonte: http://www.fraudescorporativas.com.br/2018/07/indice-global-de-fraudes-ciberneticas-corporativas-permanece-alto/

2 Fonte: https://computerworld.com.br/2018/01/11/desconhecimento-das-regras-de-seguranca-tem-vitimado-empresas-em-todo-o-mundo/

3 https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

4 https://ecommercenews.com.br/noticias/balancos/chefe-do-fbi-no-brasil-faz-alerta-sobre-o-numero-de-denuncias-de-cibercrime-durante-o-cyber-security-summit-brasil-2018/

Date Created

31/12/2018