UMA DISCUSSÃO SOBRE A SEGURANÇA DA INFORMAÇÃO: UM CONCEITO DESVALORIZADO NO BRASIL

DOMARYS DA S. CORRÊA[1]; MARILTON S. DE AGUIAR[2]

[1]Universidade Federal de Pelotas – domaryscorrea@gmail.com
[2]Universidade Federal de Pelotas – marilton@inf.ufpel.edu.br

1. INTRODUÇÃO

Os avanços tecnológicos propiciam uma evolução em diversas áreas, sendo que hoje dificilmente pode-se enxergar um mundo em que a tecnologia não esteja presente e trazendo inovações quase diariamente; porém, principalmente no Brasil, pouco se discute e se divulga quanto as necessidades em termos de segurança que esta evolução exige.

De acordo com o IBGE, em 2014 mais de 51% dos brasileiros passaram a ter acesso à Internet (GOMES, 2016). O ESTADO DE S. PAULO (2015) publicou que as queixas por crime virtual chegavam a 91 por dia. Um ponto importante é que as vítimas, por desconhecimento ou por não encontrarem apoio especializado, buscavam fazer atas notatorias em cartórios para que as provas casuais não se perdessem. Uma prática que se tornou habitual é tentar enquadrar estes crimes no Código Penal Brasileiro, mesmo que este não preveja os mesmos em suas definições.

A falta de um conjunto de leis e normas que protejam e amparem os usuários da rede mundial no Brasil deixa os mesmos desamparados em um ambiente conhecidamente rico em fraudes e crimes.

Apesar do aparente interesse do Brasil de aderir a Convenção de Budapeste (ou Convenção sobre o Cibercrime), este não se efetivou e como abordado pelo INSTITUTO DE RELAÇÕES INTERNACIONAIS E DEFESA (2007), “[…] o acordo é de difícil aplicabilidade [...]”.

2. METODOLOGIA

Este trabalho visa levantar a importância já reconhecida nos chamados países de primeiro mundo da divulgação e da implementação de uma regulamentação e legislação específicas, seja no âmbito acadêmico, civil, comercial ou empresarial, e indicar um ponto inicial para estas mudanças.

Para tanto, o primeiro passo é o levantamento mais preciso em termos de números e métodos dos ataques que ocorrem no país atualmente, suas origens, práticas e focos, seguido pelo estudo das legislações e políticas vigentes em outros países que mais se adéquem às necessidades e infraestrutura da população. Esta primeira etapa demandará uma procura, armazenamento e análise de um grande volume de informações para a construção e classificação de planos de ações e suas implementações em cada esfera, criando uma resposta geral e básica.

É importante entender que este tipo de trabalho possui um escopo enorme e deve ser iniciado a partir dos pontos mais urgentes e de um tratamento inicial adequado para estes.

Para a localização de tais dados atualizados existem variadas fontes, partindo de fontes oficiais de organizações e livros específicos da área de segurança computacional, sites especializados em notícias de cunho tecnológico – onde muitas vezes se noticiam os ataques e crimes virtuais – e sites da esfera jurídica.

Após a montagem de uma sólida reserva de dados deverão ser aplicadas definições para uma correta proposta de ação. Um exemplo da importância destas definições é citado por ELEUTÉRIO e MACHADO(2014) como a diferença entre o uso de recursos computacionais como apoio a um crime ou como meio essencial.

No caso do primeiro, em que o uso de tais ferramentas tecnológicas serve como suporte a uma ação, a predisposição indica que o crime deve ser jugado pelas leis existentes, pois caso não houvesse o uso da tecnologia, ainda assim o crime poderia ser efetuado.

No segundo caso, em que a tecnologia se faz necessária, apresenta-se a exigência de uma jurisdição especializada, pois o crime se desenvolve em um ambiente exclusivo e deve ser visualizado de forma exclusiva.

O passo posterior, na metodologia proposta, é a catalogação desta importante reserva de informações. Dentre estas informações, estão as ligações entre o estado atual do cibercrime no país, a criação de políticas de segurança para a prevenção, planos de apoio para a reversão, o destacamento dos pontos prioritários que devem ser analisados para o desenvolvimento futuro de normas e regras que apoiariam a criação de uma legislação própria.

A criação de políticas de segurança servirá como um guia, um local de partida, uma vez que é mais simples em um vasto campo como este, localizar onde pode-se ter segurança e, ao contrário, onde há a falta desta. Os planos de apoios virão a fim de elucidar as medidas cabíveis nos casos indicados, destacando assim quais são os pontos que deverão receber apoio de proteção, seja como uma indicação do que pode ser prejudicial, ou até mesmo a concepção de uma norma legislativa, ou uma lei.

Existem muitos casos em que um usuário desavisado se torna uma vítima em potencial. Por exemplo, uma pessoa que acessa sites inseguros, verifica seu e-mail ou uma conta em máquinas públicas e por consequência tem sua senha capturada, não poderia ser punida, mas deve ser divulgado amplamente que potencialmente é prejudicial.

Entretanto, se a senha capturada for utilizada para o acesso não autorizado em qualquer meio, então isto é caracterizado como um crime. A concepção de que se uma pessoa rouba a senha da outra deixando aquela a mercê de uma ação punitiva destaca o fato de que senhas devem ser bem protegidas.

E, por fim, serão buscados os pontos que requerem atenção e uma indicação de tratamento para os mesmos.

3. RESULTADOS E DISCUSSÃO

Este trabalho encontra-se em fase seminal, de revisão bibliográfica e análise dos métodos de classificação dos dados capturados. Espera-se que seja possível apresentar resultados mais concretos durante o evento.

4. CONCLUSÕES

Estudos e pesquisas semelhantes têm sido feitas, mas sem grandes impactos, não por falta de importância, embasamento ou qualidade, mas devido a uma noção geral incorreta que não prioriza não só a Segurança da informação, como a Segurança de Computadores e Redes, e a Computação Forense.

Com a finalização deste trabalho haverá a criação de uma importante base que poderá vir a servir de apoio para estudos posteriores que vissem prosseguir e aprofundar os estudos desta área para trabalhos mais personalizados para um segmento específico.

5. REFERÊNCIAS BIBLIOGRÁFICAS

ELEUTÉRIO, P. M. D. S; MACHADO, M.P.. **Desvendando a Computação Forense**. São Paulo: Novatec, 2014.

GOMES, H. S. **Internet chega pela 1º vez a mais de 50% das casas, mostra IBGE.** Globo.com: São Paulo, 2016. Acessado em: 04 julho 2016. Online. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/04/internet-chega-pela-1-vez-mais-de-50-das-casas-no-brasil-mostra-ibge.html

INSTITUTO DE RELAÇÕES INTERNACIONAIS E DEFESA. **Brasil não pode aderir a Convenção de Budapeste sobre o Cibercrime.** INFOREL: São Paulo, 2007. Acessado em: 1 agosto 2016. Online. Disponível em: http://www.inforel.org/noticias/noticia.php?not_id=2358&tipo=1

O ESTADO DE S. PAULO. **Quase 100 queixas de crime virtual são feitas por dia no Brasil.** EXAME.COM: São Paulo, 2015. Acessado em: 5 maio 2016. Online. Disponível em: http://exame.abril.com.br/tecnologia/noticias/por-dia-sao-feitas-91-queixas-de-crime-virtual