Alexandre Atheniense

Prevenção é palavra de ordem em ambientes digitais

Alexandre Atheniense é advogado formado pela Universidade Federal de Minas Gerais (UFMG) e especialista em Internet Law pela Berkman Center – Harvard Law School. É sócio da Aristoteles Atheniense Advogados.

Tomaino Almada

Política de segurança da informação

Na medida em que os serviços passam a ser prestados por meio eletrônico, surgem novas preocupações e riscos. Antes, o alcance das redes era interno às corporações, agora esse controle não existe, uma vez que as empresas estão abertas por meio de portais e outras ferramentas interativas da web 2.0.

Daí a necessidade de se estabelecer critérios para saber lidar com esse novo ambiente, estabelecer um regramento mínimo com relação aos termos de uso dos serviços, como também uma política de segurança da informação. A política se impõe porque hoje estamos trabalhando em rede, existem colaboradores internos e externos que acessam as bases de dados de diferentes locais e em diferentes níveis e, consequentemente, é necessário dar ciência a todo esse grupo de pessoas sobre como se dá o acesso e o compartilhamento dessas informações. Isso porque lidamos diariamente com situações envolvendo incidentes de segurança da informação, como os ocorridos em 2011 com invasões de sites do governo federal.

As políticas de segurança da informação devem ser construídas com a participação de especialistas de várias áreas, contemplando pontos de vista diferentes – tecnologia, segurança da informação, recursos humanos, jurídico.

Organizações devem estar preparadas

O que diferencia uma organização da outra não é somente saber se ela vai sobreviver a um ataque, mas como ela vai reagir diante de um problema dessa natureza, se há um plano de contingenciamento. Faço um alerta para o fato de que nem sempre as políticas criadas pelas empresas têm efetividade com relação aos aspectos jurídicos. É necessário, ao estabelecer uma regra de violação de conduta, que exista uma advertência ou punição correspondente. Por exemplo, nem sempre, na empresa, há ferramentas capazes de monitorar incidentes, ou preservar provas necessárias à identificação de autoria ou alcance das violações, questões previstas nas políticas. Se há regras, são necessários meios de produzir provas, formas de monitorar e, eventualmente, punir. O ambiente, a arquitetura, a maneira como as informações são acessadas e tratadas em cada instituição merecem tratamento individualizado.

As normas e as rotinas sistêmicas têm que viver em perfeita simbiose. Acima de tudo, têm que estar em conformidade com a lei brasileira.

Atualizações

De forma geral, a dinâmica é fator de geração de resultados. No caso de sistemas e aplicativos, por exemplo, estão sendo sempre atualizados e recebendo novas funcionalidades. Isso mostra que as políticas de segurança precisam ser atualizadas de forma sistemática, a fim de acompanhar essa evolução – pelo menos uma revisão anual.

Capacitação

Especialmente no caso do ambiente de governo, é extremamente importante desenvolver uma política adequada de capacitação dos servidores. Temos que partir do princípio de que as pessoas, de forma geral, não tiveram – na faculdade, na família ou em outro ambiente – qualquer tipo de capacitação sobre como lidar com a informação digital. A responsabilidade é do governo e das empresas de chamar para si esse papel de ensinar, de forma construtiva, e não punitiva.

Aí está a oportunidade de atrair e não segregar as pessoas envolvidas, para passar a elas uma série de informações, capacitação, orientações, aculturamento, para que elas entendam que o que está sendo empreendido não é unicamente para vigiar, é mais ainda para deixá-las aptas a conviver de forma correta no ambiente digital.

O empregado tem que saber, por exemplo, que a lei confere à empresa o poder de fiscalização sobre tudo o que acontece no ambiente de trabalho, e ser orientado para fazer o melhor uso possível dentro de suas atribuições. E quem provê uma infraestrutura de acesso tem o dever de controlar tudo o que ocorre dentro desse ambiente.

Consumidor e produtor de conteúdos

Com o avanço da web 2.0, o cidadão hoje é a própria mídia. A partir desse momento, quando ele cria um blog ou um perfil no Facebook, no Twitter, passa de consumidor a produtor de informações. E o brasileiro, de forma geral, muitas vezes não enxerga limites para fazer seus comentários. Culturalmente somos um povo expansivo, comunicativo; embora, em termos de privacidade, um pouco ingênuos. Uma informação importante: o segundo lugar em processos na internet é a difamação, especialmente em redes sociais.

Blindagem digital da reputação

É recomendado que organizações públicas e privadas estejam nas redes, para conhecer os conteúdos nos quais estão envolvidas no meio digital, realizando o monitoramento contínuo de assuntos e temas relevantes.

A ideia não é simplesmente reagir a qualquer julgamento negativo, mas, sobretudo, saber exatamente o que está acontecendo – quais os julgamentos positivos e negativos que estão ocorrendo nas redes sociais. As empresas estão criando equipes especialistas para cuidar desse assunto. Inclusive para identificar quando um fato tem relevância jurídica, quando ultrapassa o limite da liberdade de expressão – uma calúnia, por exemplo. As pessoas não se dão conta da importância de fazer o gerenciamento da reputação de pessoas, de marcas e de empresas.

O projeto de blindagem digital é esse monitoramento contínuo das mídias sociais. Muitas vezes significa monitoramento constante e reação imediata. Se não há essa resposta imediata, a versão acaba se transformando em fato, perde-se o controle.

Legislação

A lei acompanha essa evolução mais do que se imagina. Há alguns aspectos que ainda precisariam ser aprimorados, como o projeto de lei que trata da questão da privacidade dos dados. A nossa lei que fala sobre privacidade está circunscrita à Constituição de 1988; muita coisa mudou desde então. Há países, como Espanha e Argentina, que já fizeram leis específicas para tratamento de privacidade de dados. Temos basicamente dois dispositivos na lei que tratam do tema, mas que são insuficientes para as diversas situações que encontramos. A informação é o petróleo do século XXI e precisamos saber lidar com isso. A nossa legislação não foi criada para tratar com dados, mas com coisas. Em alguns casos, é possível usar analogia, mas no direito penal isso não é possível.

Boas práticas para manter sua reputação na mídia digital

- Pesquise a si próprio diariamente.
- Saiba discernir as críticas e não revide provocações, pois você acaba dando mais visibilidade para o comentário negativo.
- Evite criticar pessoas e empresas sem bons argumentos.
- Entre na conversa.
- Crie o hábito de preservar as provas dos incidentes de TI.
- Seja transparente.
- Crie conteúdos de boa reputação, gere referências positivas.
- Proteja sua marca, registrando nomes de domínio, IDs.
- Tome medidas extrajudiciais ou judiciais ou, se for o caso, imediatas, após a ciência de um incidente. A rapidez e continuidade no enfrentamento são essenciais para o resultado.
- Planeje o contingenciamento para enfrentar o ataque, envolvendo a equipe com vários representantes de diferentes setores, para que o trabalho em equipe seja eficiente.