A era da vingança privada virtual

Vivemos em um Estado Democrático de Direito. A Constituição Federal de 1988, dentre os princípios e garantias fundamentais, estabelece em seu art. 5o, inciso XXXV, que a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito, prevendo ainda, dois incisos após o citado, que não haverá no Brasil juízo ou tribunal de exceção;

Há muito tempo não resolvemos os litígios com as próprias mãos (Quero acreditar). E não podemos nos esquecer disto. É claro que o homem vem evoluindo ao longo do tempo, mas se houvesse a certeza de que respeitaria a vida, os animais, a honra, a integridade física e os demais bens jurídicos, desnecessárias seriam as Leis, bem como como a estrutura Estatal para operacionalizá-las, com Policia, Ministério Público e Judiciário. Nos primeiros anos de graduação em Direito aprende-se que o Jus Puniendi (direito de punir) é do Estado. De mais ninguém. Nem seu, nem meu.

Diante de fatos praticados por transgressores e supostos criminosos, temos presenciado atos de menor nobreza ainda, por aqueles que não só se revoltam com a situação, amparados pelo mesmos sentimentos que motivaram o criminoso: a agressividade e o estado instintivo. A cada dia, mais e mais, presenciamos atos que excedem o inconformismo ou o protesto, que são legítimos, e entram na seara das agressões, vias de fato, linchamentos, ataques a terceiros, ofensas a familiares e destruição de patrimônio. E a situação se agrava com a Internet, que tem o poder da “eternização” e do “não esquecimento”.

Verdadeiros desregulados, com uma câmera de celular nas mãos, ou usando de modo inconsequente as redes sociais, podem fazer estragos inimagináveis. E os exemplos não faltam. Um policial

que se sente no direito de filmar com seu celular cidadãos abordados e compartilhar em grupos nas redes sociais com comentários jocosos, o que excede o procedimento comum. Em outro vídeo, um desentendimento de trânsito que vai às vias de fato e alguém com um celular, sentindo-se no direito de registrar, comentar a desavença de terceiros e compartilhar para todo o mundo virtual. Mais, a suposta criminosa é filmada, a população se revolta e a lincha, sendo que depois, descobre-se que não era ela. Em mais um exemplo, a foto de um suposto agressor é editada com frases agressivas, identificada sua residência, seus familiares, seus dados pessoais e tudo é enfaticamente publicado e republicado em inúmeros grupos de milhares de pessoas na Internet. Outra, uma falsa denúncia de maus tratos feita por uma falsa consumidora (fake) e o faturamento da empresa despencando em 80%, sendo seus familiares proibidos de sair de casa, com medo. Danos irreparáveis a pessoas que muitas vezes sequer foram julgadas.

Estamos vivendo, lamentavelmente, a era da vingança privada, agora virtual. Em tal fase, que existiu até o século XVIII, cometido um crime, ocorria a reação da vítima, de seus parentes e até do grupo social, agindo sem proporção à ofensa, atingindo não só o ofensor mas todos os seus familiares e grupos. Combateremos instinto com instinto? Penas severas, cruéis e desumanas. Um garoto de 12 anos me disse recentemente: “Na escola meus amigos procuram no Google e ficam falando do processo que meu pai teve antes mesmo de eu nascer”. O pai já pagou a pena imposta pelo Estado, mas está eternamente condenado por um “alguém de banda larga” que, sequer investido do poder judicante, passou sua sentença no mundo virtual, vista por milhares de pessoas, sem direito a esquecimento.

Para os que assim agem, “Pouco importa se o Estado vai condenar ou absolver. Nós o condenaremos na Internet”. Tudo, sem direito a contraditório, ampla defesa e demais institutos relativos ao devido processo legal. O Código Penal pune aquele

que busca fazer justiça com as próprias mãos, para satisfazer pretensão, muito embora legitima, nos moldes do crime de exercício arbitrário das próprias razões, em seu art. 345. O mesmo Direito Penal aqui citado assegura o princípio da instranscendência, pelo qual, nenhuma pena passará da pessoa do condenado. Mas, quantas mulheres, pais, esposas e filhos, que nada tem a ver com o incidente, sendo atacados e ameaçados pelas "sentenças virtuais" a uma pessoa, preferidas nas redes sociais?

A mesma Constituição que assegura a liberdade e o direito de ir e vir também é taxativa em relação ao direito à segurança e a inafastabilidade do Judiciário. Quem deve condenar é ele. Não eu, nem você. E se ele é ineficaz, a conversa é outra.

Não podemos aplaudir o uso inconsequente das tecnologias. Não podemos consentir com o barbarismo sob o pretexto de se ver cumprir as Leis ou estaremos regredindo e dando uma resposta medíocre a toda evolução do Estado, ressuscitando o "olho por olho dente por dente", Código de Hamburabi ou Lei das XII Tábuas. Quem suportará isso? Amanhã você poderá ser o condenado, sem saber, e esta pena se aplicará a toda a sua casa e familiares, indistintamente. Que se tenha, por favor, a mínima dimensão, de quão grave é incentivar o ódio e a tão repudiada vingança privada, por meio da Internet.

Livro Marco Civil da Internet é o mais vendido da Saraiva

Nosso livro recém lançado, escrito em coautoria com o Professor Damásio de Jesus, já é referência sobre o tema e o

mais vendido na livraria Saraiva. A obra está disponível na versão impressa e também digital. Você pode encontrar o livro em: http://www.saraiva.com.br/marco-civil-da-internet-comentarios-a-lei-n-1296514-7984114.html

Um abraço e até o próximo.

Responsabilidade dos provedores de hospedagem por invasão: Culpa do sistema ou do provedor?

Você mantém um site rodando sobre o motor wordpress, disponível via painel de controle em uma hospedagem qualquer. Estima-se que 19% dos sites rodem sobre WordPress. Seguiu todos os passos para o hardening, revisou http://codex.wordpress.org/pt-br:Blindando_o_WordPress e mesmo assim está encontrado problemas com injection, file include ou invasões.

Alterou a senha do blog, ftp e do banco de dados. Nada resolve. Alterou os prefixos das tabeas wp_, alterou as permissões, criou um novo usuário administrativo, removeu plugins, criou index.html em diretórios, ocultou a versão do seu CRM, tunou o .htaccess, instalou plugins de scannes de vulnerabilidades e nada…

Então, ao identificar o ip (no Bing, Ip:seu número de IP) para seu site descobre se tratar de um servidor com dezenas de sites. Um servidor compartilhado. Não há hardening de

WordPress que resista a um servidor compartilhado comprometido.

Quais as medidas de segurança que o provedor está adotando para proteger seus arquivos? Em servidores compartilhados as permissões de alterações de arquivos pode ser fatal. E o pior, o provedor pode "abafar" sua vulnerabilidade, alegando que não encontrou problema algum. E o usuário, muitas vezes consumidor, se complica para provar pois não tem acesso à infra do provedor.

O grande problema é que diante de tais incidentes, o primeiro cenário é buscar entender o que aconteceu com o provedor de hospedagem. Lamentavelmente, muitos provedores irão sempre jogar a culpa no código do cliente, nunca no servidor. Em alguns casos, simplesmente dizem que nada aconteceu, mesmo você mostrando para o helpdesk registros na tabela wp_posts cheios caracteres "estranhos" e posts não criados pelo administrador.

Sob o prisma jurídico, não há duvida que o provedor pode ser responsável, sobretudo quando alega que o problema é no seu código. É possível provar com um pentest que não é o código o problema!

O provedor, diante de um incidente, deve restaurar backup anterior a invasão e imediatamente encaminhar os logs (access) e outras informações. O backup deve envolver o banco de dados e é questionável a cobrança pela restauração de backups dos clientes.

Já se decidiu na justiça brasileira que a ausência de backup ou a corrupção do mesmo pelo cracker, pode ensejar responsabilização do provedor de hospedagem.

Mesmo o provedor tendo restabelecido o serviço, é direito do consumidor de serviços descobrir data e hora do acesso indevido, vulnerabilidade explorada e técnica utilizada. Se o provedor alega que se trata de um injection ou uma

vulnerabilidade no seu código que permitiria a injeção de um shell, mas não existe nada nos logs, esta afirmação pode não corresponder à realidade, sobretudo se o incidente se repetir.

Cabe, neste caso, a atuação com uma perícia ou auditoria externa, para constatar efetivamente se a afirmação do fornecedor de hospedagem realmente procede. Com a perícia em informática, pode-se identificar, por exemplo, vulnerabilidade no servidor ou serviços desnecessários rodando, não iniciados pelo cliente, sendo o caso de responsabilização do provedor.

Em Minas Gerais, ao julgar o recurso de apelação 433.758-0 (2.0000.00.433758-0/000.), o então Tribunal de Alçada responsabilizou provedor de hospedagem em caso em que defacer invadiu site e anexou fotos pornográficas no site da vítima. Por outro lado, nos termos do inciso II, parágrafo 3o. do Art. 14 do Código de Defesa do Consumidor, o provedor poderá provar culpa exclusiva da vitima, que por exemplo, não protegia o arquivo wp-config.php, permitindo que qualquer um conhecesse a senha para acesso ao banco de dados, ou mesmo mantinha uma senha fraca para seus serviços.

Recentemente, em 2013, um provedor foi condenado por não garantir segurança ao cliente, permitindo a invasão (http://www.ebc.com.br/tecnologia/2013/08/microsoft-e-condenada-a-indenizar-consumidora-que-teve-perfil-invadido)

Outro julgado pode ser encontrado em http://www.migalhas.com.br/arquivo_artigo/art20130828-11.pdf

A controvérsia é técnica e será decidida pela justiça. Vale quem produzir a melhor prova. Mais uma vez a perícia informática é fundamental, desta vez, para o prestador de serviços de hospedagem que pretenderá demonstrar que o problema não era com sua infra.

Seja como for, recomenda-se a ambas as partes o registro de todas as telas e detalhes da invasão, bem como das conversações (suporte, chamados, helpdesk, etc.) envolvendo o

incidente. A coleta de evidências dever ser ágil sim, mas sempre preceder qualquer medida para “apagar” o exploit ou arquivos plantados pelo atacante no FTP, pois serão provas em juízo. O contrato deve ser revisto, sempre, pois ele limitará, no que não for nulo ou abusivo, os direitos e deveres entre as partes, diante de um incidente.

Recomenda-se, em caso de servidor aberto ou compartilhado, mediante um ajuste com o prestador de serviços, a utilização do OSSEC (http://www.ossec.net/), que permite a análise de logs rapidamente, permitindo ainda monitorar arquivos quando os mesmos são alterados, garantindo a possibilidade de uma resposta rápida a um incidente.

Para segurança em WordPress, por fim, recomendamos o ebook http://ithemes.com/wp-content/uploads/downloads/2013/12/WordPress-Security-ebook.pdf