Como é a atuação do advogado especialista em crimes cibernéticos?

O exercício da Advocacia especializada em crimes virtuais vem chamando a atenção de inúmeros profissionais e alguns fatores são considerados chave, como o crescimento das fraudes, golpes e ofensas praticadas pela internet.

O número de crimes virtuais vem crescendo desenfreadamente em todo o mundo. No Brasil não é diferente. De acordo com um relatório global publicado pela Symantec, o Brasil é o terceiro país que mais recebe ataques cibernéticos em dispositivos conectados à internet, considerando que de todas as ameaças detectadas, 9,8% ocorreram no Brasil, que fica atrás apenas dos Estados Unidos, com 10,1% e da China com 24%.

A quantidade de denúncias de crimes na internet cresceu 109,5% em 2018, segundo a associação SaferNet Brasil. A popularização do uso das redes sociais e das tecnologias, além do natural aumento da superexposição, aliada a ausência de programas de educação digital, favorecem igualmente o surgimento de golpistas e exploradores digitais.

Casos comuns de atuação

A atuação deste profissional é variada, podendo atuar em casos de perseguição virtual, stalking, crimes contra a honra, calúnia, injúria, difamação, cyberbullying e até em crimes eleitorais. Para se ter uma ideia, de acordo com uma pesquisa realizada pelo Fundo das Nações Unidas para a Infância (UNICEF), ao analisar trinta países, chega-se a conclusão que um em cada três jovens foram vítimas de cyberbullying e muitos relataram que abandonaram a escola devido essas violências virtuais.

No aspecto patrimonial, crescem os delitos de estelionato digital e furto mediante fraude. Alguns exemplos recentes foram os casos de golpes envolvendo o auxílio emergencial destinado a trabalhadores informais e autônomos neste momento de pandemia do Covid-19, que chegaram a atingir 7 milhões de pessoas no Brasil, segundo os dados da PSafe.

Outras técnicas utilizadas, como chip swap, vem permitindo que atacantes tomem posse de ativos digitais das vítimas, incluindo contas bancárias e a partir delas conseguem realizar saques em ativos ou solicitar empréstimos.

Por falar em crimes patrimoniais, é impossível que o advogado especialista em crimes virtuais não lide com pelo menos um caso de extorsão online. Cresceram os casos de ransomwares, nos quais os atacantes criptografam os discos da vítima, bloqueando seus dados, solicitando resgate, normalmente em bitcoins, para que os dados sejam liberados. De acordo com os dados da Emsisoft, empresa de segurança especializada no atendimento a casos desse tipo, houve um aumento de 41% nas infecções por malwares que sequestram computadores e redes em 2019, sendo que 205,2 mil organizações foram vítimas de ataques desse tipo, com uma média de US$ 84,1 mil nos valores do resgate.

Além disso, o phishing scam, que consiste na tentativa de fraudulenta de “pescar” (a palavra phishing, deriva do inglê fishing) informações confidenciais, através de mensagens aparentemente reais para obter, por exemplo, dados bancários, continua em alta e lesando inúmeras pessoas em todo Brasil.

São diários os casos envolvendo crimes de pornografia infantil, onde o profissional precisa adotar procedimentos ágeis para cessar o conteúdo, impedir o constrangimento e muitas vezes apurar a autoria. Além disso, este profissional atua para empresas em questões envolvendo ataques direcionados, ataques de negação de serviços, invasões e até mesmo em questões envolvendo propriedade intelectual e

softwares irregulares no ambiente corporativo, que também podem caracterizar condutas criminosas.

O Advogado especialista em crimes cibernéticos também vai lidar constantemente com processos de apuração de autoria, bloqueios de conteúdos e aprenderá logo cedo a lidar com a resistência das empresas e algumas redes sociais em cumprirem ordens expedidas por juízes do Brasil, como aplicativos de mensagens, dentre outros. A base para a guarda de registros é o Marco Civil da Internet, Lei 12.965/2014, legislação basilar para quem atua na área.

Ainda, em alguns casos, muitas vezes precisará do MLAT (mutual legal assistance treaty) para obter registros de provedores de aplicações sem sede ou localização no Brasil.

Formação desejada

Como se pode verificar, atuar como advogado especialista em crimes virtuais exige, logicamente, conhecimento em tecnologia da informação, compreensão das principais técnicas utilizadas pelos atacantes para lesar e praticar crimes pela internet e conhecimento de procedimentos para apuração da autoria, já que em parte dos crimes cibernéticos que se apresentam, não se conhece, a princípio, os autores por trás da ofensa.

Assim, não se pode afirmar que um profissional sem background técnico atuará com a mesma precisão de alguém que se dedica para ter uma complementação na carreira e mais afinidade com a informática. Por outro lado, isso não significa uma graduação em tecnologia, já que, hoje, muitos treinamentos e cursos de extensão são úteis e recomendados, como o curso de perícia forense digital (https://bityli.com/9Jyef) que ministro para muitos advogados que atuam com direito digital, que participam com o escopo de compreender melhor os processos de apuração de autoria, quebra de sigilo, investigação informática, recuperação e preservação de evidências.

Dentre as competências esperadas pelo especialista em crimes

cibernéticos, encontram-se a produção da prova digital, compreensão das técnicas de ataques digitais, fundamentos de redes e sistemas operacionais, entendimento sobre principais vulnerabilidades web, dentre outras.

Em meu livro, Manual de Crimes Informáticos (https://cutt.ly/ooMiv16) trato das 10 vulnerabilidades OWASP, instituição que apresenta as principais e mais sérias vulnerabilidades em aplicações WEB. Atualize-se nestas técnicas.

Assistência técnica da Perícia em Informática

Ao longo de anos atuando com perícias e assistência técnica especializada em crimes informáticos, percebo cada vez mais a importância, seja na acusação ou na defesa, da figura do assistente técnico, profissional de tecnologia da informação, comumente especializado em perícia forense digital, para auxiliar tecnicamente o trabalho do profissional do direito ou penalista especialista em crimes virtuais.

Este perito digital auxiliará em diversos momentos, desde inquéritos policiais, nas delegacias ou especializadas, na instrução, na formulação de quesitos, acompanhamento de exames técnicos e outras diligências, inclusive, avaliando os exames dos peritos oficiais e identificando falhas e omissões. Também pode atuar dando suporte ao advogado para redação das teses e na produção de provas técnicas simplificadas.

Tendências e como começar?

Furto de criptomoedas, pontos de milhagem, ativos virtuais, questões envolvendo jogos online e extraterritorialidade, atuação de bots na seara eleitoral, deep fakes, fake nudes dentre outras questões que surgem diariamente no mundo da Internet e tecnologia da informação, continuarão a crescer e demandarão ainda mais da atuação do profissional especializado em crimes cibernéticos.

A cada dia novos jogos, aplicativos, técnicas e práticas se revelam verdadeiros perigos da internet. Os novos regulamentos de proteção de dados, como a LGPD e GDPR também estabelecem direitos aos titulares de dados e aumentam a preocupação de agentes de tratamentos com invasões e outros ataques e suas consequências, o que também abrirá um novo campo de mercado para os profissionais que se especializarem em crimes digitais.

Nos Estados Unidos, a atual preocupação passa a ser os crimes tributários e lavagem de dinheiro com criptoativos, nos quais inúmeros profissionais em crimes cibernéticos e lawtechs já atuam na investigação, perícia e defesa em casos desta natureza.

Assim, o advogado especializado em crimes cibernéticos deverá estar em constante atualização, aprendendo conceitos de segurança da informação, principais formas de ataques e ameaças, estar bem assessorado tecnicamente por peritos e especialistas em tecnologia. Investir em aprimoramento é essencial e o diferencial entre profissionais que buscam, cada vez mais, atuar nesta promissora área do direito digital. Do mesmo modo que a sociedade migrou para a tecnologia, o crime também migrou e é neste contexto que o advogado em crimes cibernéticos apresenta um papel social relevante, como profissional fundamental na busca pela justiça, nos milhares de processos criminais envolvendo questões tecnológicas, que crescem a cada dia.

Quer compreender melhor os processos de apuração de autoria, quebra de sigilo, investigação informática, recuperação e preservação de evidências? Então se inscreva no **Curso de Perícia Digital e Investigação Forense Digital,** que apresenta uma abordagem 360º sobre o tema que visa preparar profissionais para este novo mercado de trabalho através de técnicas e melhores práticas, para que possam atuar com segurança nas mais variadas frentes da perícia voltada à tecnologia da informação.

A guerra podre eleitoral está por vir com a propaganda paga na Internet e as fakenews

A guerra podre eleitoral está por vir com a propaganda paga na Internet

A Internet sempre foi o maior receito dos políticos de carreira. Em um cenário onde muitos tem a máquina, dinheiro, ou dominam algum meio de comunicação em massa como rádio, concessões ou afiliadas de TVs, liberar a rede para propaganda eleitoral era um perigo, considerando que não se sabe como os candidatos “sem condições” conseguiriam se projetar.

A campanha de OBAMA em 2008 e a da sua reeleição mostraram o poder do uso correto da Internet, de técnicas de otimização para os sites (SEO) a postagens recorrentes em horários estratégicos, passado por crowdfunding e pela presença em outras mídias pouco exploradas pela concorrência. Chegou-se a um resultado onde o mapa eleitoral se equivalia à curtidas e crescimento dos ativos digitais.

Em 2008, a primeira resolução que permitia a propaganda na internet era extremamente limitada e só permitia a propaganda via “sites”. Em 2009 a Lei eleitoral era alterada para permitir a internet como plataforma de propaganda de propaganda eleitoral. De lá para cá em todas as reformas eleitorais, um ponto nunca fora alterado: Não se poderia por dinheiro na Internet.

Na Internet era proibida qualquer tipo de propaganda eleitoral paga. E isso se justificava pois se na Internet fosse permitido “colocar dinheiro”, ela se equipararia à meios

tradicionais, onde poucos tem acesso pleno (como revistas, jornais, etc.), mais uma vez se tornando uma forma de propaganda que privilegia alguns em detrimento da maioria dos candidatos. Tudo mudou.

A reforma trazida pela Lei 13.488/2017 que alterou a Lei das Eleições liberou o impulsionamento de conteúdos contratados diretamente (e não via agências de marketing) com os provedores de aplicação de Internet, como Facebook, Instagram, etc, desde que com sede e foro no País.

Não bastasse, equiparou, para fins de impulsionamento, a priorização paga de conteúdos resultantes de aplicações de busca na Internet. Ou seja, está liberado pagar para "ser bem ranqueado" no Google (adwords) e outros buscadores. O cidadão está preparado para lidar com esta propaganda?

Quebra-se a isonomia e mais uma vez, quem tem mais irá aparecer em destaque, só que desta vez, não no rádio, TV, jornal ou nas ruas, mas na Internet. Mas não é só isso. Embora os gastos com impulsionamento sejam considerados gastos de campanha, sabe-se que existem formas de se impulsionar sem que necessariamente se tenha gastos. Estes meios "não oficiais" embora vedados pelo TSE, não encontram amparo investigativo e certamente serão utilizados para viralização de conteúdos e criação de caixas de ressonância, com destaque para os chatbots e botsprofiles, que são contratados a partir de outras aplicações que se conectam às redes sociais.

E não é só. A partir do primeiro dia de propaganda seremos bombardeados com posts pagos e impulsionados que terão a expressão "propaganda eleitoral", mas em meio a um mar de propaganda patrocinada e impulsionada, quem garantirá que terceiros não impulsionem propagandas negativas disfarçadas? Ou mesmo quem garantirá quem estará na frente de quem nas buscas? Mais uma vez estamos falando dos algoritmos das redes sociais. Eles são honestos? Ou os mais habilidosos em palavras chave e otimização de campanhas se destacarão?

Já se pode imaginar, por exemplo, o impulsionamento e patrocínio de postagens a partir de palavras chave envolvendo o concorrente, ou mesmo de palavras negativas. Como reagir a isto na celeridade de um pleito eleitoral? A guerra podre da propaganda paga na Internet vai começar. Aos candidatos e comitês caberá monitorar as redes, reportar e representar ofensas, mas principalmente, em determinados casos, realizar judicialmente a quebra de sigilo e a busca de informações sobre os impulsionamentos e suas configurações, de modo a constatar se existe ou não alguma prática considerada abusiva ou impulsionamentos por meios não autorizados. Resta saber se o TSE, comitês e principalmente, provedores de aplicações, estão preparados para absorver estas demandas, impedindo que a internet seja usada para manipular a decisão de milhões de eleitores.

Quando os algoritmos falham e o combate ao Fakenews causa outros danos

A maior rede social do mundo enfrenta grandes problemas diante do vazamento de dados de 50 milhões de perfis a partir de aplicativo instalado em mais de 250 mil destes, que serviram de insumo para análises pela Cambridge Analítica, de uso na campanha eleitoral norte-americana para direcionamento de propaganda.

Em tempos de novo regulamento de proteção de dados pessoais aprovado na União Europeia e enrijecimento da proteção aos dados dos norte-americanos (Já se discute o *Honest Ads Act*, proposta que obriga empresas de tecnologia a revelarem

compradores de publicidade que sejam políticos) o descrédito e a queda do valor das ações estão fazendo Facebook tomar medidas drásticas, sobretudo com vistas às eleições do Brasil e México.

Assim, o que já ocorre em outros países pode ocorrer aqui também, por meio da técnica de fact-cheking, ou seja, a partir de um link que o usuário pretende postar, o Facebook utilizará parceiros para avaliar a notícia e motivar o usuário a repensar antes de postar, além de estratégias convencionais, como reduzir alcance de páginas que costumam divulgar informações falsas.

Porém só isso não adianta, pois sabe-se que um bot irá aprender a postar a notícia falsa a despeito do aviso de que algo "não é bem assim". Por isso a rede está testando o aprendizado de maquina, de forma a detectar paginas e conteúdos enganosos e poderá até mesmo remover automaticamente os mesmos.

Recentemente identifiquei que rede já está "taggeando imagens", ou seja, a partir de inteligência artificial e algoritmos, consegue identificar o contexto das imagens postadas, certamente para detectar conteúdos abusivos e fakes também em formato visual. Na minha imagem que postei, o Facebook até detectou que eu estava de "terno".

Sabe-se que as vitimas de fakes podem recorrer ao Judiciário, por meio de um advogado em direito digital, em busca da exclusão do conteúdo, como recentemente ocorrido no caso da vereadora Marielle, onde um processo no Rio de Janeiro indaga o Facebook se o MBL pagou para impulsionar FakeNews, havendo risco de multa suspensão e bloqueio no Brasil, caso descumpra a ordem.

Na ânsia de frear o FakeNews, a rede corre um outro risco, o

de ser responsabilizada por interferir no conteúdo, rotular indevidamente e excluir perfis que não espalhavam desinformações, além de gerar “bolhas de opiniões” ou “caixas de ressonância”, priorizando a usuários conteúdos que os mesmos possuem afinidade, ainda que proveniente de fontes duvidosas. Algoritimos falham ou podem ser usados para criar estados artificiais, fazer deduções equivocadas ou mesmo influenciar decisões. Não se sabe, até hoje, como o Facebook trabalha os seus códigos neste sentido.

Recentemente, até mesmo alguns novos chatbots foram bloqueados, diante das medidas anunciadas pela empresa para aprimorar a privacidade, englobando o seu Messenger.

Neste contexto, pessoas e empresas prejudicadas e que tiveram páginas excluídas podem recorrer ao Judiciário e processar a rede para manterem seus conteúdos no ar, ilegitimamente excluídos por erros, má intenções ou manipulações de códigos e algoritmos.

Não demais destacar, no entanto, a questão da onda de Fakenews e da violação a privacidade também pode ser evitada ou minimizada pela ação de usuários. De nada adianta as ações propostas como o Fatima (*chat bot que esclarece usuários sobre fakenews*) se estes continuam trocando sua privacidade por inutilitários que os mostram mais velhos, parecidos com algum artista ou mesmo no sexo oposto. Ao aceitar estes Apps, muitos usuários não vêem, mas estão concedendo acesso para que o token usado no App permita a coleta de informações e alimente o mercado de Fakenews, com nítida interferência no debate e no contraditório, que deveria ser o natural nas redes sociais, ameaçando a própria Democracia.

Medida sérias para provedores negligentes, lei de proteção de dados pessoais e educação digital, além de incentivo a aplicações ofereçam meios para o usuário detectar uma notícia aparentemente falsa. Não existem segredos para minimizarmos a onda de exposição indevida de dados e combate às notícias

fraudulentas.

Ao leitores e usuários do Facebook, recomendo uma extensão do Firefox, chamada Facebook Container (https://addons.mozilla.org/en-US/firefox/addon/facebook-container/), que acaba de ser lançada e assegura maior privacidade ao usuário de Internet, impedindo o compartilhamento de informações de outros sites com a rede social. Acaba assim com a publicidade segmentada e direcionada com base no que o usuário pesquisou ou acessou, atuando sobre os cookies do computador.

José Antonio Milagre é Advogado especializado em Direito Digital, Mestre e Doutorando em Ciência da Informação pela UNESP e pesquisador do Núcleo de Estudos em Web Semântica e Dados Abertos da Universidade de São Paulo.

Vazam senhas dos principais sites de e-commerce brasileiros: Como se proteger e o que diz o direito digital

Em 17 de julho foi divulgado pelo Tecmundo a notícia de um arquivo disponibilizado via Pastebin, com nome de usuários e senhas para as principais plataformas de ecommerce do Brasil e alguns serviços de hospedagem. Estão na lista Netshoes, Extra, Centauro, Casas Bahia, PagSeguro, Terra, eFácil, Ponto Frio, HostGator etc.

Não se pode afirmar seja autêntica, o fato é que existem aproximadamente 360 logins e senhas e segundo o site o arquivo

poder ser uma amostra. Não se trata de um vazamento em massa, porém alguns alertas são válidos. O site não divulgou o arquivo pois logicamente poderia ser utilizado por criminosos.

Ao que parece as contas publicadas estavam desativadas. De qualquer maneira, as vitimas devem diante deste cenário trocar imediatamente as senhas destes serviços. Caso a senha não entre, pode ter sido alterada, momento em que é importante um contato telefônico com as lojas virtuais. É preciso rememorar quais sites online o usuário já comprou e para isso, vale avaliar a caixa de correio eletrônico e outros documentos digitais.

Não se sabe se os dados foram obtidos por meio de phishing scam (e-mails e sites falsos) ou por meio de algum código malicioso nos clientes. Neste sentido, aqueles que perceberem qualquer atividade anômala poderem realizar uma perícia digital em seu equipamento, através de um especialista, de modo identificar a origem de alguma exploração maliciosa. Não é porque conseguiram acesso a conta que hackers poderão comprar produtos, mas no mínimo podem ter acesso a dados cadastrais e em alguns casos sim, acesso a dados cartões de crédito.

De se destacar que diferentemente do Brasil, nos Estados Unidos a lei obriga as empresas a reconhecerem e publicarem os vazamentos de dados. Aqui, o projeto de proteção de dados pessoais trata deste tema, mas longe está de ser uma legislação. As lojas Centauro e Netshoes se manifestaram no sentido de não terem sofrido qualquer ataque, o que leva a crer tenham os dados coletados ou obtidos diretamente dos consumidores.

Logicamente, as vitimas, caso a vulnerabilidade seja nas lojas virtuais, poderão buscar a reparação judicial e a responsabilização das mesmas pelos danos causados, considerando que disponibilizaram um serviço “em tese” vulnerável e que pode ter lesado o consumidor. Por outro lado,

se a loja demonstrar em juízo por meio de uma perícia em informática que seu sistema não foi violado, comprovando culpa exclusiva do consumidor ou exploração de vulnerabilidade em seu equipamento, pode não ser condenada a reparar e ser absolvida de um processo ou ação reparatória. A batalha é técnica e consiste em provar quem estava seguro e quem estava vulnerável e quem deu causa ao vazamento dos dados. Um especialista (expert do juízo) pode ser nomeado para solucionar a controvérsia.

Seja como for, para o Direito Digital, sem prejuízo do crime pela obtenção indevida de dados, o acesso indevido por meio login e senha, violando mecanismo de segurança ou autenticação é crime, previsto na lei de crimes informáticos, lei 12.737/2012 (Carolina Dieckman) . É possível, igualmente, medida judicial em face do Pastebin, para que forneça os registros de acesso à aplicação daqueles que postaram o conteúdo. Embora a principio permita colagens anônimas, não se admite que o serviço não registre de alguma forma os dados de conexão de seus utilizadores.

José Antonio Milagre é perito digital. facebook.com/josemilagreoficial

---

Sobre o áudio de Joesley Batista: É preciso decência na atividade pericial.

No dia 26 foi apresentado ao STF Laudo da Polícia Federal sobre o Áudio de Joesley Batista com o Presidente Michel Temer. Como verificamos das notícias sobre a análise da Polícia Federal, o áudio apresentou 294 descontinuidades.

É preciso destacar, em esclarecimento, que as descontinuidades são consideradas interferências técnicas e não montagens. Elas decorrem muitas vezes de equipamentos que são acionados com a intensidade sonora e param de gravar diante de lapsos de silêncio. De modo a demonstrar que não se trata de edição, uma das técnicas simples é observar o que se chama de "encadeamento lógico das ideias e assuntos". Um áudio editado, via de regra, interrompe sequencias de raciocínio na grande maioria das vezes detectáveis pela chamada "oitiva crítica".

Outras técnicas podem ser usadas para detectar a montagem, adulterações e edições em áudios. Pode-se apreender o equipamento utilizado para se fazer simulações (assinatura do equipamento), deve-se observar os metadados dos arquivos de áudio para se identificar modificações, análise oitiva (onde pode-se observar por exemplo alterações do som ambiente). Ainda existe a possibilidade da conversão do som em gráficos, por meio de software forenses, onde é possível observar uma sequencia da frequência dos áudios. Pode-se conduzir análises de forma da onda (wave form), espectograma ou sonograma, formantes, dentre outras análises para detectar montagens e até autenticidade.

Dependendo da pericia, pode-se fazer gravações com o suspeito para se identificar o timbre da voz (espectografia do som), mais comum para se apurar a autoria de um som.

Do mesmo modo, um exame técnico desta natureza não pode se dar em softwares utilizados por usuários, mas destinados a pericia e análises técnicas, como Cedar, Sound Cleaner, OTExpert, DClive, iZotope, Adobe Audition, Praat, dentre outros.

A Policia Federal concluiu, após minucioso exame, que pelas técnicas aplicadas na realização dos mesmos, não foram encontrados elementos indicativos de que a gravação questionada tenha sido adulterada com relação ao áudio original, sendo a mesma consistente com a maneira em que alega ter sido produzida.

Neste sentido, verifica-se o afastamento de laudo de assistente técnico de uma das partes, que concluía pela existência de adulterações no áudio e que o mesmo era imprestável. Alegações aliás que não vieram providas de embasamentos técnicos mínimos. Ademais, outros especialistas iniciaram análises relâmpagos, que culminaram com conclusões precipitadas e que não podem ser consideradas e só contribuíram mais para a polêmica sobre os áudios.

Exames de autenticidade, em tempos em que programas podem simular a voz de qualquer pessoa (https://olhardigital.com.br/noticia/novo-programa-da-adobe-consegue-imitar-qualquer-voz/63760) são essenciais como no polêmico caso, mais do que apenas exame da integridade do áudio. Por outro lado, mais do que avaliar as técnicas usadas nos exames, devemos refletir sobre o compromisso da figura do assistente técnico. Ética, responsabilidade e dever com a verdade, não usando técnica para confundir. Na dúvida, outros peritos podem ser consultados para corroborar ou divergir. A atividade de um assistente técnico, que nitidamente distorce conclusões e exames de demais especialistas, em nítida tentativa de beneficiar seu cliente, não pode ser considerada exercício do direito de defesa ou opinião técnica, mas uma fraude processual.

É preciso decência na atividade de assistência técnica pericial. Lamentavelmente, diante da ausência regulatória e de fiscalização, continuaremos tendo peritos de "Media Player e Sony Vegas" ganhando a mídia, gerando controvérsias, alterando a verdade e descredenciando o trabalho sério e embasado dos órgãos periciais oficiais.

José Antonio Milagre é Perito em Informática, Advogado, Mestre e Doutorando em Ciência da Informação pela UNESP. www.josemilagre.com.br/blog

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

---

WhatsApp Forensics: Análise forense e investigacão digital

Não restam dúvidas que uma análise de um dispositivo móvel que contenha WhatsApp a qualquer momento chegará nas mãos de qualquer profissional de computação forense. Crimes, fraudes e ilícitos podem ser praticados por intermédio do mensageiro.

Recém comprado pelo Facebook, o aplicativo é padrão em comunicação instantânea no Brasil, e constantemente objeto de estudos, quando o tema é "quebrar" sua criptografia.Porém são raras pesquisas que se dediquem a tratar sobre a auditoria ou mesmo sobre a computação forense aplicada aos rastros deixados por este aplicativo, repise-se, febre no Brasil.

Além de texto plano a aplicação também permite o compartilhamento de fotos e vídeos, com uma agravante, o sistema de "aceitação" é precário. Se alguém compartilha conteúdo ilícito ou te insere em um "grupo" para atividades ilegais, é você quem deve estar esperto e sair ou recusar o conteúdo.

Neste excelente guia sobre “Live Memory Forensics” às fls 73 e seguintes, temos uma importante referência de Estudos para a coleta de evidências no WhatsApp. Um plugin com a utilização do Volatility permite realizar o parsing das conversações persistentes na memória.

Lembrando que o Volatility tem uma API pública e vem com um extensível sistema de plugins que permitem a escrita de novos códigos e a extração de novos artefatos, daí porque trata-se de um importante aliado para análise de memória de dispositivos móveis.

Outro trabalho interessante vem da Índia, especificamente, escrito por profissionais e pesquisadores do “Institute of Forensic Science”, Guajarat. Ele também envolve análise não volátil e se aplica ao concorrente, o VIBER. Porém os pesquisadores utilizaram o UFED (solução proprietária) para todo o trabalho.

Em síntese, para uma análise não volátil é interessante que o examinador colete os seguintes arquivos (Lembrando que a pasta Media e ProfilePictures não são encripitadas):

Ocorre que a empresa cifrou seus dbs, não sendo mais tão simples a coleta e análise das conversações e outros elementos. Hoje identificamos um msgstore.db.crypt:

Fonte: http://resources.infosecinstitute.com/android-architecture-forensics/

Alguns scripts (python) chegaram a ser criados para quebrar a criptografia, mas hoje não estão funcionais, mas estude os códigos aqui:

Fonte: yagi15/whatsapp-hacking-2013-lucideus-tech-private-limited

Alguns textos recomendam submeter o arquivo crypt ao http://www.recovermessages.com/ que “em tese” quebraria a criptografia da última versão do aplicativo. Não realizei testes, tampouco posso atestar a veracidade.

Diante das proteções implementadas, mais e mais ganha-se relevância a análise de memória dos dispositivos móveis. Especificamente quando falamos de WhatsApp, muitos artefatos na RAM não estarão criptografados, como estão no disco. Assim, fica recomendada esta pesquisa Forensic Analysis of WhatsApp on Android Smartphones de junho de 2013, que é muito interessante a medida em que conclui que os mensageiros contemporâneos usam sistemas similares para armazenar mensagens e atualizar os bancos de dados. A pesquisa apresenta o whatsappRamXtract um bash script que pode ler um arquivo de memória extrair fragmentos gerados pelo comunicador.

Recomendo também aos interessados, considerando a imprescindíviel necessidade do perito em dominar o Volatility, que acessem periodicamente o Volatility Labs Blog e mantenham-se atualizados acerca das iniciativas para tunar a ferramenta, sobretudo a adaptando às características das novas aplicações, bem como sobre os desafios da forense em memória.

Não custa lembrar, o presente texto orienta para os estudos e pesquisas na área forense. Qualquer utilização não autorizada pela justiça ou mal-intencionada poderá ser considerada criminosa, sujeitando os infratores às penas da Lei.

VideoCast 01 – Propriedades da Segurança da Informação

Sobre o anúncio da venda de negros no Mercado Livre

Seria reinventar a roda dizer que as pessoas por trás da ofensa podem ser responsabilizadas. De igual modo é chover no molhado dizer que é cabível a responsabilização do site que hospedou a ofensa. Igualmente, dizer que a internet vem a favorecer práticas racistas…

Sobre a responsabilidade civil do meio que hospeda o crime cometido por terceiros, é engano, por outro lado, dizer que é absolutamente pacífico o dever de indenizar. No momento em que estiver lendo este artigo, haverá pelo menos um provedor de serviços sendo absolvido no Judiciário, alegando que "é o meio" e que não pode "julgar o que é legal ou ilegal", logo não podendo remover o conteúdo de plano.

Claro, inafastabilidade do judiciário. Até aí tudo bem. Agora, diante de uma página que estampa crianças negras sendo vendidas a um real, não seria normal ao homem mediano (e até ao abaixo da média) compreender que ali se estampava um crime? Por que esperar para remover? E nos crimes de vazamentos de vídeos de menores ou fotos intimas? Minutos a mais no ar representa a difusão do conteúdo para todo o planeta… Dano potencializado e a culpa é de quem? Do usuário que não denunciou?

Neste ponto outra desculpa esfarrapada. Os sites de serviços agora transformaram seus clientes em “fiscais”, e diante de um crime grave em uma de suas páginas, simplesmente alegam “Ora, temos um botão disponível para o usuário denunciar abusos”.

O que? Um botão? Um código html capaz de afastar a responsabilidade do site de avaliar crimes cometidos em suas páginas e transferi-la ao usuário? Não, isso não pode prosperar e é uma dinâmica mais que desproporcional.

Grandes sites e portais investem milhões em atendimento, otimização de conteúdo e coleta de dados para traçar padrões de consumo, mas não movem uma palha para usarem filtros e análise de dados para identificar conteúdo abusivo e ilegal. Em investigação e perícia, um mínimo. E diante do crime… “Existia um botão para denuncias…”

Ação Civil Pública pode ser proposta além de ações individuais por todas as pessoas que se sentiram lesadas no caso do anúncio preconceituoso. O meio deve ser responsável pela postagem sim, pois não é crível que não disponha de mecanismos tecnológicos e recursos humanos para de plano identificar ações como esta, em tempo de cadastro. Será que realmente estamos na idade da pedra e é preciso deixar alguém publicar um anuncio para só então constatar um abuso?

De qualquer modo, importante mencionar que o Marcado Livre aparentemente forneceu os dados do possível suspeito diretamente à Ouvidoria Nacional de Igualdade Racial, órgão vinculado à Secretaria de Promoção da Igualdade Racional e também ao Ministério Público. Percebam, não forneceu a um Juiz de Direito e não se recusou a fornecer a uma entidade legitima, como fazem a maioria dos provedores de serviços do Brasil, que só agravam o crime e a lesão aos direitos e garantias individuais das vitimas de crimes na internet.

Qual o dano que o site teve em fornecer os dados? Nenhum, simplesmente amenizou sua responsabilização, não só removendo

o conteúdo, mas repassando os dados à autoridades e entidades para que procedam com as medidas cabíveis, antes de uma possível ordem judicial. Evitou uma ação de responsabilização e eventual condenação em honorários por ter dado causa ao ajuizamento de uma ação de quebra de sigilo. Sim, um exemplo que nos faz pensar:

Não seria o caso de repensarmos se a remoção de conteúdos em todas as situações dependem mesmo de ordem judicial? Ou em crimes flagrantes como preconceito no ambiente cibernético poderia-se cogitar de uma pronta remoção? Temos tecnologia para auditar tudo em tempo de execução do crime?

Não seria o caso de relativizarmos e imperativa necessidade de ordem judicial para identificação da autoria em crimes de preconceito, franqueando acesso às informações, em casos específicos, às autoridades policiais e Ministério Público? Ou no mínimo, não seria o caso de agilizarmos ordens judiciais em crimes graves desta natureza, que se propagam na velocidade da Internet? Um processo eletrônico para delitos tecnológicos? Existem correntes com fundamentos plausíveis em ambos os sentidos.

O que sabemos é: Precisamos de maior eficiência não só na criação de leis, mas na capacidade de fazer frente e investigar crimes cibernéticos. Na internet, tempo é dano. Provedores, repitam…

Enfim, os responsáveis pela publicação no Mercado Livre, se efetivamente identificados, estarão incursos no artigo 20 da lei n° 7.716/1989, que lembrando, não protege as pessoas apenas do preconceito racial, mas prevê pena de reclusão de dois a cinco anos e multa a quem pratica, induz ou incita a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

Mas de nada adiantará a Lei posta, se as pessoas lesadas não provocarem o Judiciário e provocarem (pela dor financeira) uma

mudança qualitativa no zelo de sites e provedores de serviços para com auditoria em suas redes, páginas e serviços em geral.

Cuidados jurídicos com o colocation

Locar estrutura de serviços pode ser um grande problema quando o objetivo é provar que a prestadora está falhando. Ou mesmo para a prestadora, que mais dia menos dia, se vê envolvida em litígios entre seus clientes e clientes de seus clientes…

É a lição que tomamos de uma ação, que tramitou na 22. Vara Cível de São Paulo, em que a empresa Requerente processava a Requerida, em decorrência de uma sublocação de espaço que mantinham junto a um provedor. A Requerente então levou cinco computadores para o local. Em virtude de uma desavença contratual, a Ré teria, "em tese" desligado os cinco computadores da Autora, prejudicando domínios de clientes desta. Mas esta poderia desligar os equipamentos?

A Requerente precisou ingressar com uma busca e apreensão para ter acesso a seus equipamentos que estavam na infra-estrutura de terceiros. Não poderia contatar diretamente o provedor pois era a Requerida que mantinha o contrato com este. A Ré ainda, em contestação, alegou que todos os servidores da empresa haviam sido derrubados pelo sócio da autora, razão pela qual desligou os servidores, para "evitar o dano".

Após a realização o de perícia, a Requerente não conseguiu provar que a Requerida havia maliciosamente desligado seus servidores. Segundo o juiz *"Não há prova de que a invasão tenha causado prejuízos à XXXXX, razão pela qual sua pretensão indenizatória não comporta acolhimento"*

Neste caso, aparentemente trata-se de um serviço de colocation (onde há a terceirização de estrutura física e da rede de tráfego) que foi por sua vez sublocado a outra empresa, a Requerente. A decisão reforça a ideia de que não só precisamos de cooperação do provedor de serviços para apurarmos o que aconteceu, mas principalmente, precisamos rever as políticas e contratos para fazer prever direitos quando o próprio prestador de serviços é quem está falhando.

E a situação se agrava quando falamos de cloud e outros desafios. Se estivéssemos falando de cloud, a busca e apreensão recairia sobre os dados e não sobre os ativos físicos, onde já podemos prever as complicações da execução de uma medida desta natureza.

Importa dizer que a sentença veio alguns dias antes da vigência da Lei 12.737/2012, pois caso contrário, a invasão com objetivos ilícitos poderia ser objeto de queixa criminal. Neste sentido, cabe também aos prestadores de colocation uma revisão completa de seus contratos, prevendo limites no fornecimento de dados e demais questões onde não poderá ser responsabilizado.

Processo número **0111550-16.2008.8.26.0100** 22 Vara Cível da Capital