Hackers to Law: Lei Azeredo pode tornar inviável cultura e pesquisa hacker

Como deveria ser do conhecimento de todos, hackers, ao contrário de crackers, utilizam seus conhecimentos para o aprimoramento da segurança de sistemas, e não invadem sistemas com a intenção danosa. Mas invadem sistemas, fato!

Mas será que o PL 84/1999, a chamada "Lei Azeredo", alcança esta distinção técnica, ou trata todos como cibercriminosos, como é, aliás, o entendimento de algumas autoridades que se manifestam a respeito? Em maio de 2011, o Projeto 84/1999 teve novo relatório, também pelo (agora Deputado) Azeredo, que tentou costurar alguns termos de modo a tornar o projeto "mais aprazível". Fato é que o mesmo será votado pela Comissão de Ciência e Tecnologia da Câmara, e pode ser aprovado a qualquer momento.

Mas, suprimir "termos polêmicos" da legislação projetada, como o próprio Senador anunciou, significa efetivamente preservar direitos e garantias fundamentais dos cidadãos e pesquisadores de segurança? Vejamos, no decorrer desta análise.

Dentre as principais modificações do relatório, tivemos a remoção dos textos "dispositivos de comunicação" e "rede de computadores" dos tipos penais trazidos, segundo o relator, para "impedir a criminalização de condutas banais". Mas condutas banais continuam em risco de serem consideradas criminosas.

Três artigos, com profundo impacto nas pesquisas realizadas por profissionais de segurança, serão estudados, abaixo

descritos:

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado

Art. 285-A. *Acessar rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização do legítimo titular, quando exigida:*

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação

Art. 285-B. *Obter ou transferir dado ou informação disponível em rede de computadores, dispositivo de comunicação ou sistema informatizado, sem autorização ou em desconformidade à autorização, do legítimo titular, quando exigida:*

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço.

Inserção ou difusão de código malicioso

Art. 163-A. *Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado.*

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º *Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:*

Pena – reclusão, de 2(dois) a 4 (quatro) anos, e multa.

Bom, para entender quais foram as mudanças nos artigos, apenas os leia sem as expressões "rede de computadores" e "dispositivo de comunicação". Avançamos realmente em prol de uma legislação lúcida, no que tange às pesquisas de segurança? Receio que não.

Primeiramente, em se tratando do crime previsto no art. 285-A (Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado), o "acesso" continua sendo "não autorizado", de modo que deixa a cargo do titular do "sistema informatizado" reputar as condições de autorização (que podem não ser tão expressas), como "integrador" da lei penal, o que é um perigo, diante de nítida subjetividade, que pode ensejar manobras maliciosas para prender pesquisadores e profissionais éticos.

Imagine que você, ao invés de acessar um site via browser, utiliza um crawling ou se utiliza do comando "wget" no site; este acesso está se dando a um sistema informatizado (website) e de uma forma não trivial (browsing), logo, você pode ser punido por fazer download do site.

Imagine em um pentest (teste de intrusão), onde via "sql injection" você consegue bypassar o sistema de login do precitado portal, adentrando na área administrativa ou mesmo descobre o arquivo de conexão que lhe permite realizar uma conexão nativa com o banco de dados. Ora se hoje, CSOs na grande maioria, são arredios e se revoltam com

“pesquisadorezinhos” que se intrometem em seu trabalho e expõe vulnerabilidades, imaginem, quando eles descobrirem que tais atividades passam a ser criminosas?

Uma simples script em php usando a expressão <? passthru($_GET[“cmd”]); ?>, concatenado em uma querystring, para gerar um registro no errors.log, que simplesmente te permite a execução do Shell (cmd), e que o pesquisador testou em um sistema, mesmo que não tenha sido contratado, causado dano, indisponibilidade ou copiado informação alguma, apenas para provar o conceito, seria, em tese, acesso indevido a sistema informatizado. Ora, como testar a segurança de um sistema se o acesso é criminoso?

E que nem se argumente que pode-se inserir na redação do tipo a expressão “através de meio fraudulento” e estaria resolvido o problema, sendo que somente crackers seriam pegos. Ledo engano, os hackers utilizam de destreza e técnicas de subversão de sistemas, logo, é fato que adulteram, enganam os sistemas testados. O que difere um cracker de um hacker não são, em regra, as ferramentas ou meios usados, mas a intenção dos agentes.

Alguns podem argumentar que os riscos de injustiças acima expostos não existem, já que a conduta punível deve ser sempre “dolosa”, com intenção, porém, não nos perece crível que um pesquisador de segurança tenha de provar que não tinha intenção fraudulenta ou de obtenção de quaisquer vantagens, tendo de se expor constantemente em face de investigadores, inquéritos, averiguações, dentre outras. O simples fato de comparecer em um “DP” para prestar esclarecimentos, para um pesquisador Hacker, é fato constrangedor ao extremo e pode se intensificar com a aprovação da lei.

Já, em se analisando o artigo 285-B da “Lei Azeredo”

(Obtenção, transferência ou fornecimento não autorizado de dado ou informação), temos o mesmo problema e pior, com uma conduta passiva do hacker, “obter”, ou seja, alguém que receba por e-mail, skype ou de qualquer forma dados de uma pagina ou aplicação web, banco de dados ou dispositivo informático, poderá incidir no tipo ora previsto. Não bastasse, mais uma vez tem-se um conceito subjetivo, “sem autorização”, que pode ser utilizado por pessoas maliciosas para incriminar inocentes. Um contratante, por exemplo, buscando a rescisão com um pesquisador de segurança, sem pagar-lhe o devido, pode “armar” uma cilada, modificando os termos de acesso ao sistema informatizado, fazendo com que este, inconscientemente, incida na conduta prevista como criminosa.

Alguém que faça ou receba um script e faça um “file include” e que demonstra uma URL vulnerável, e que encaminha as análises para um grupo de pesquisadores, estaria em tese cometendo a conduta criminosa.

Ademais, hackers que participam de listas não estão imunes à atuação de kiddies tolos que por prazer e sem cérebro postam dados de suas “façanhas”. Neste caso, hackers estariam “obtendo” dados de sistemas informatizados sem autorização. Logo, criminosos! Divulgações de pesquisas, repositórios de códigos e provas de conceito podem estar comprometidas, pois darão margem a uma interceptação ampla por parte de vítimas, delegados, promotores, etc.

Já o tipo previsto no art. 163-A, pune aquele que insere ou difunde código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado (Agora, só “sistema informatizado”). Ora, e quem irá dizer o que é “código malicioso”? É o mesmo que tentar explicar se uma “faca” é um instrumento malicioso! Vocês conhecem o T50? O SqlMap? O Metasploit? Pois é, exploits, provas de conceito e ferramentas de auditoria estão ameaçadas. E um mero scriptzinho VBS ou

viruszinho de macro (Do tipo,“Seu pc está sendo formatado…”), mesmo sem comprovada eficácia do meio, podem ser considerados códigos maliciosos? Quem vai dizer são os operadores da lei, e é aí onde mora o perigo.

Se você apenas injetou o ou executou o exploit, mesmo que não haja dano, pode ser punido pela “inserção”. Se você mandou o link do código (exploit) para alguém, “difusão”, Se você colocou aquelas “aspas simples” em um “textbox” em algum site, (viu algo como *“Erro: Incorrect syntax near ”, senha, 0) retorno, tipo, codigo, acessos from usuario where usuario = ”.”)* mas o gerente de TI registrou seu IP no access.log e passou para um advogado, cana!

“Onde você estava quando estas aspas simples foram registradas nos logs da vítima? Elas vieram do seu IP! Confesse!”

Bom, e se você instalou um plugin no seu browser para te dar privacidade do tipo “X-Forwarded-For Spoof” e lá colocou um javinha alert e percebeu que dezenas de sites estão vulneráveis a XSS-Crossite (em referrer)? Você estava simplesmente garantindo sua privacidade, esbarrou com falhas, e ainda pode ser indiciado por “inserção” de “código malicioso”! Pode?

Você compra um “Iphone” e instala uma aplicaçãozinha que permite acessar o root do sistema de arquivos ou para desbloquear alguma função. (jailbreak). Pergunto, a Apple autoriza? Você não inseriu código malicioso em sistema informatizado? Crime!

Você gosta de engenharia reversa, usa um “decompiler” ou mesmo um “disassembler”, altera alguma aplicação em hexa, ou muda endereçamentos, inserindo novos códigos no executável, para avaliar sua segurança e comportamento? Você está inserindo código em “sistema informatizado”, crime!

Você acessa seu e-mail através de webmail, após o desligamento da empresa, você percebe que suas credenciais não foram removidas, e realiza um acesso de sua casa para acessar os últimos e-mails remetidos a você. Você está acessando indevidamente sistema informatizado (servidor e-mails) sem autorização! Crime!

São várias as condutas questionáveis!

Por fim, a supressão dos termos "dispositivo de comunicação" e "rede de computadores" dos crimes aqui estudados, alteram algo neste cenário? Apenas limito-me a descrever o conceito de sistema informatizado, mantido pela lei: *"qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente"*

A alteração, a nosso ver, em nada altera o cenário, pois o termo sistema informatizado é amplo e não vislumbro, na grande maioria das hipóteses, um dispositivo de comunicação ou rede de computadores (útil), sem um sistema informatizado. Ou seja, se o Senador removeu estes termos, foi por redundância, e não com intenções de "impedir a criminalização de condutas banais".

Vejamos, se você rodasse um nmap em um IP e verificasse que o mesmo está com a porta do Terminal Server aberta (3389), entrasse e, digitando as credenciais, acessasse o sistema, estaria em tese acessando indevidamente rede de computadores. (Mais, o próprio "ping" ou "nmap" para scanear portas, pode gerar logs nos IDS e firewalls, onde o agente estaria, em tese, inserindo dados em sistema informatizado!) Se, de outro modo, via wireless, encontrasse um dispositivo móvel fazendo gateway para Internet (via 3g ou gsm) e nele se conectasse, estaria acessando indevidamente um dispositivo de comunicação. O mesmo vale para os inúmeros hotspots liberados ou "liberáveis" (aircrack que o diga…) disponíveis em todo o Brasil, onde seus titulares sequer sabem de tal fato. Acessou rede alheia, aberta, porém sem autorização (aberta por

ignorância e não por consentimento), crime!

Removendo agora estes termos (redes de computadores e dispositivos de comunicação, mantendo somente sistemas informatizados), no primeiro caso, em uma interpretação maliciosa, poderiam as autoridades alegarem que o agente acessou o "sistema informatizado" operacional x ou y da vítima, via Terminal Server. No segundo caso, que o agente acessou o "sistema informatizado" android, symbiam, iphoneOS ou qualquer outro sistema da vítima, via wireless. Na terceira hipótese, que acessou o "sistema informatizado" do roteador (firmware) para acesso indevido à rede wireless alheia…

Ou seja, nada mudou, a interpretação de sistema informatizado é, do mesmo modo, ampla!

O mesmo vale para o verbo "obter" previsto no artigo 285-B. Não se obtém dados em redes de computadores e dispositivos de comunicação que não estejam, via de regra, suportados por sistemas informatizados. Pense conosco… Um firmware é sistema informatizado, um aplicativo é sistema informatizado, um utilitário é sistema informatizado, ou inutilitário é sistema informatizado… Acessou a página do LulzSecBrasil com dados da Dilma e Kassab? Criminoso! Você "obteve" os dados sem autorização do titular! Bandido!

Como explicado, não se ambicionou, com o presente, pregar a não necessidade de uma lei de crimes informáticos ou atacar o projeto como um todo (eis que parte dos artigos são válidos e pertinentes, como a proteção de dados pessoais prevista no art. 154-A), mas tão somente demonstrar, especificamente, no que tange à atividade hacker, que esta pode restar inviabilizada caso tais tipos não sejam reformulados, reestudados ou removidos da "Lei Azeredo".

A manutenção dos tipos penais, tal como se apresentam, constitui em risco para a cultura e pesquisa de segurança da informação, na medida em que colocam "nas mãos" dos titulares

de sistemas informatizados e na interpretação de autoridades, questões como a autorização ou não para acesso e envolvendo a intenção (dolo) do hacker suspeito, bem como criminaliza atividades triviais diuturnamente realizadas por pesquisadores, sempre, com as melhores finalidades. Como provar boas intenções neste cenário? Desculpem-me, mas este ônus não deve ser atribuído aos hackers.