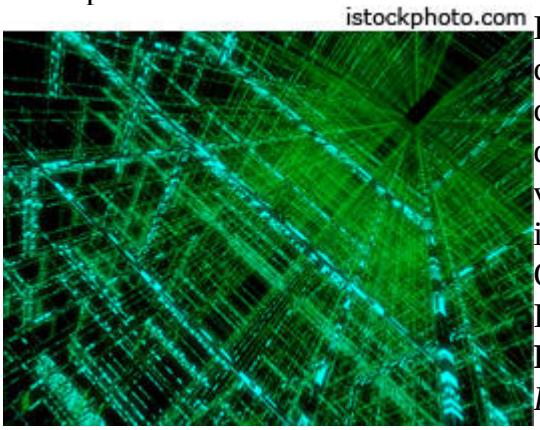
Manual explica crimes digitais e orienta sobre como aplicar a legislação

istockphoto.com



Hackers atacam portal da presidência, cartões de créditos clonados, sites de bancos invadidos — cada vez mais esse tipo de crimes digitais, com conseqüências reais, chega ao conhecimento do público. No entanto, pela sua natureza tecnológica, muitas vezes fica difícil para o profissional de Direito saber como identificar e proceder diante do ato ilícito. Pensando nisso o Coordenador da Ouvidoria do Conselho Nacional do Ministério Público e especialista em direito aplicado à informática, **Wilfredo Pacheco**, elaborou *o Manual de Responsabilização Penal de Hackers, Crackers e Engenheiros Sociais*.

O objetivo do *e-book*, de 52 páginas e gratuito, é esclarecer conceitos relativos aos novos fenômenos jurídicos que surgiram com o avanço tecnológico no setor da informática, bem como traçar conceitos e apontar as conseqüências jurídicas pertinentes a tal fenômeno. É uma espécie de guia a ser utilizado por delegados, promotores e advogados, entre outros profissionais que queiram saber as definições de alguns tipos de crimes virtuais e quais penalidades a lei prevê para eles.

Faz alguns meses que o site do Panalto foi invadido por crackers e acabou saindo do ar. Pacheco explica que nesse caso foi utilizada uma tecnologia chamada *malware*, “um gênero que engloba o vírus Cavalo de Tróia”. A pessoa recebe um e-mail, aparentemente inocente, e ao abri-lo aparece o conteúdo malicioso. Automaticamente aquele computador estará sob controle dos crackers e programado para acessar o site do Planalto. “Acontece que o site não comporta tantos acessos em um curto espaço de tempo, e como o vírus foi enviado a milhões de computadores, o sistema acaba caindo”. Essa é uma forma política de demonstrar a vulnerabilidade do governo diante de crimes dessa natureza.

Segurança nacional
Se o vírus for implantado num sistema de propriedade federal, será crime de dano qualificado (artigo 163, parágrafo 1º, inciso III do Código Penal), ou se invadir sistemas, como o do Ministério da Defesa ou da Agencia Brasileira de Inteligência, expondo dados afetos à segurança nacional, será crime de segurança nacional, incurso nas condutas típicas previstas na Lei Federal 7.170, de 14 de dezembro de 1983. Crimes contra a segurança nacional podem ser punidos com 3 a 15 anos de reclusão.

Recentemente a imprensa noticiou a onda de divulgação de informações confidenciais pelo site WikiLeaks. "A depender do teor de tais dados, a divulgação pode perfeitamente se adequar aos tipos previstos na referida lei", diz Pacheco.

O *e-book* explica que pode ser imputada a conduta de atentado contra a segurança de serviço de utilidade publica, caso a atuação do cracker através do seu conhecimento prejudique o fornecimento de água, luz, esgoto ou coleta de lixo (artigo 265 – atentar contra a segurança ou o funcionamento de serviço de água,

luz, força ou calor, ou qualquer outro de utilidade pública podendo haver reclusão de um a cinco anos, e multa), bem como o crime de perturbação ou interrupção de serviço telegráfico ou telefônico, se afetar as redes de telecomunicação (com previsão de 1 a 3 anos de pena).

Outra modo de cometer um ilícito previsto no manual de Pacheco é por meio da *SQL Injection*, que resulta quando o agente criminoso consegue acessar e influenciar as consultas realizadas pela Linguagem de Consulta Estruturada (*Structured Query Language*) – SQL que uma aplicação passa ao seu banco de dados.

Em fevereiro de 2002, o cracker americano Jeremiah Jacks descobriu que o site *guess.com* era vulnerável à técnica do *SQL Injection*, resultando no acesso de informações de cartões de crédito de, ao menos, 200 mil clientes. Em junho do mesmo ano, Jacks utilizou esta técnica novamente no site *PetCo.com*, ganhando acesso aos dados de 500 mil cartões de crédito, por meio de uma falha no banco de dados SQL. Esses e outros trechos históricos sobre crackers ilustram o guia.

O manual também explica que esta modalidade de invasão pode ser considerada conduta intermediária dos tipos penais de furto e estelionato, caso o agente aufira irregularmente valores pecuniários da conta corrente, ou outra vantagem pecuniária em prejuízo da vítima, tal como o pagamento indevido de boleto bancário em favor de terceiro.

Outra modalidade criminal muito utilizada e comentada no guia, é o Cavalo de Tróia, cujo propósito aparente é realizar operações legítimas no equipamento implantado, enquanto clandestinamente realiza tarefas maliciosas. Um exemplo, seria quando o usuário instala um programa que automatiza a inserção de senhas e logins em determinada interface de autenticação, mas, ocultamente, este software armazena tais dados e o remete ao agente.

Caso a utilização do Cavalo de Tróia desencadeie a aquisição de senha de acesso à conta corrente pela Internet (home banking), e o agente invasor consiga acesso aos dados bancários da vítima por meio telefônico, deste resultado pode ensejar a cominação das penalidades previstas para o tipo penal previsto na Lei Complementar 105, de 10 de janeiro de 2001. Esta Lei dispõe sobre o sigilo das operações das instituições financeiras, visando tutelar o bem jurídico consistente no segredo de tais atividades financeiras.

Por fim, o autor comenta que o Brasil é um terreno fértil para crimes virtuais, haja vista que o povo brasileiro vem mostrando forte inclinação ao uso da internet. Seu guia tem por objetivo servir como liame entre a lei e o conhecimento.

Clique **aqui** para ler o manual.

Date Created
17/09/2011