Hackers — administração do previsto

Luiz Antonio Titton

Recebida em março/96

A administração inclui, na sua função planejamento, a previsão de ações contra problemas inesperados gerando Planos de Contingência. Um novo fator a ser considerado nesses planos é a ação de ***hackers***, de maneira geral especialistas em informática — qualquer funcionário ou pessoa externa à empresa — que podem em algum momento colocar em risco todo o Sistema de Informações do negócio.

Embora não haja definição clara do que seja o *hacker*, sua presença começou a ser notada quando foram criadas senhas para acesso a programas de computador e estas foram **quebradas** pela primeira vez. Há conotações positivas e negativas para o termo, mas o fundamental para o ponto de vista do Administrador é ser essa denominação muito mais um atributo que se poderia dar a um técnico de informática do que, efetivamente, uma profissão ou qualificação.

O QUE SÃO?

Propõe-se uma classificação dos *hackers* em três tipos básicos: *CyberPunk*, Terrorista ou *Hacker* Interno e *Hacker* Bonzinho ou *Hacker* Contratado.

CyberPunk

É conhecido como o destruidor de bancos de dados e divulgador de informações confidenciais. Invade sistemas alheios sem convite e considera sua atividade como a de um **conquistador** de troféus quando é divulgado que seu trabalho provocou danos de alto valor econômico a empresas ou entidades públicas.

As pessoas que atuam nessa atividade situam-se na faixa etária entre 12 e 25 anos. Isto pode ser explicado pelo fato de a **iniciação** ocorrer quando se objetiva a utilização de algum *software*, normalmente um jogo, protegido contra cópias por meio de senhas. A maneira de fazer essa utilização é obtida através de contatos com pessoas já iniciadas; após algum tempo, essa prática torna-se conhecimento sedimentado.

Sua ação é sempre marcada pela divulgação de seu pseudônimo, conhecido na comunidade de *hackers* à qual pertence.

Luiz Antonio Titton, graduado em Administração de Empresas pela Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, é Consultor de Empresas e Sócio-Diretor da MEBAN Metodologia Bancária.
E-mail: luiz.titton@mandic.com.br

Caso recente (1995) ocorreu na Empresa Brasileira de Pesquisas Agropecuárias (Embrapa), que teve seus arquivos acessados e destruídos. Esse mesmo *hacker* deixou mensagens em várias universidades, entre elas as de Campinas e São Carlos.

Terrorista ou *Hacker* Interno

Trata-se do caso comum de funcionário que ao sair da empresa deixa **bombas** que irão provocar danos. Podem ser vírus de computador, mensagens de correio eletrônico com programas de formatação embutidos (*ANSI Bombs*) ou mesmo **travas** de programa (o programa pára ou começa a ter problemas depois de algum tempo).

Não há no Código Penal, explicitamente, enquadramento dessa atividade como crime.

Tem-se conhecimento de um funcionário da Aerolíneas Argentinas que propiciou facilidades para o acesso dos computadores da Varig, com a emissão de passagens que tentou colocar no mercado até ser descoberto.

Hacker Bonzinho ou *Hacker* Contratado

Normalmente é consultor externo contratado pelo próprio empresário como medida preventiva contra a ação de *hackers* em geral, sejam estes internos ou externos. Está em contato com essa comunidade, mas com o objetivo de conhecer suas técnicas para poder formular posturas defensivas. Habitualmente, as técnicas dos *hackers* estão à frente das medidas defensivas.

Outra maneira conhecida de atuação é entrar nos sistemas, sem autorização, e divulgar seu trabalho na empresa invadida, comprovando que os meios de proteção contra a sua entrada foram ineficazes e, portanto, estariam invalidados em face de novas invasões.

Em 1995, um norte-americano de 19 anos foi contratado pela polícia norte-americana para auxiliar em uma investigação sobre abuso sexual. O trabalho infrutífero de um mês da polícia foi resolvido em 45 minutos pelo *hacker*.

AÇÃO PUNITIVA?

Não há no Código Penal, explicitamente, enquadramento dessa atividade como crime. Portanto, não pode haver punição a partir de ação legal.

O artigo 163 do Código Penal prevê pena para crimes contra o patrimônio de União, Estado, Municípios ou Órgãos Públicos e o 159 dispõe que quem "causar prejuízo a outrem, fica obrigado a reparar o dano".

Existem projetos de lei para enquadrar essa ação como crime, mas nada há de concreto com relação à punição dessa atividade quando realizada de forma destrutiva. Atualmente, o único enquadramento legal que poderia acontecer no Brasil seria o de danos provocados por terceiros, isto se for possível comprovar que houve o dano e se houver uma ligação direta com alguém.

Há casos exóticos, como o de um cidadão britânico que acionou judicialmente um *hacker* por uso não-autorizado de sua energia elétrica e seus recursos de informática. A invasão era constante, mas não havia dano algum para reclamar.

É conhecido também o caso dos *hackers* alemães que, nos anos 80, divulgaram na Internet estar ainda em andamento o Projeto Guerra nas Estrelas, apesar dos pronunciamentos do então Presidente Reagan anunciando seu encerramento. Neste caso, em que houve uma ação política internacional, a punição seria aplicável?

Durante a ação estudantil na Praça da Paz Celestial, na China, e em várias tragédias climáticas foram também os *hackers* que divulgaram fotos e textos para a imprensa e na Internet sobre os fatos que as condições impediam de chegar ao conhecimento do restante do mundo. Dessa maneira, propiciaram ação humanitária e política. Nestes casos a ação dos *hackers* aproxima-se daquela dos radioamadores nos anos 60 e 70.

A INTERNET É UMA PORTA ABERTA?

Sim. Qualquer empresa, ao se conectar com o mundo, poderá ser acessada a partir de qualquer ponto do planeta e, portanto, pelo menos teoricamente, poderá receber mensagens que poderão ser *ANSI Bombs*.

Entretanto, essa porta deve ser aberta, para que a empresa não corra o risco de ficar isolada das vantagens oferecidas pela rede. Não deve ser adotada a postura de que "desligando o *modem* está resolvido", pois seria o mesmo que justificar o fechamento de uma empresa por causa de assaltos, enchetes ou qualquer outro motivo deste tipo.

Existem sistemas de proteção. Sobre eles pode-se afirmar, com segurança, haver para cada método pelo menos um *hacker*, talvez até um funcionário do próprio fabricante, empenhado em descobrir falhas, seja para seu saneamento, seja para justificar eventual vingança futura.

O VÍRUS TEM ALGO A VER COM OS *HACKERS*?

O vírus de computador é um programa como qualquer outro, com as características básicas descritas a seguir.

- **Capacidade de proliferação** — o programa-vírus copia-se para a memória do computador e a cada inserção de mídia (disquete, por exemplo) ou programa copia-se para a novo meio.

- **Capacidade de auto-reconhecimento** — um vírus nunca infesta uma mídia se esta já estiver contaminada por ele próprio. Isto se deve à adoção de uma **assinatura**, ou seja, uma palavra que indica já estar aquela mídia, ou programa, contaminada por ele. Essa assinatura evita que determinado vírus contamine infinitas vezes o mesmo programa, por exemplo, lotando o disco rígido do computador e, assim, denunciando antecipadamente a contaminação.

- **Capacidade de disparo da ação** — o disparo é o momento em que o vírus **ataca**, destruindo, emitindo mensagens ou fazendo qualquer ação para a qual tenha sido programado. Trata-se de característica comum à maioria dos vírus. Em alguns casos ela não está presente, pois existem determinados vírus cujo efeito é simplesmente o retardamento da velocidade do desempenho de computadores.

Os vírus não são elaborados necessariamente pelos *hackers*. Contudo, estes têm capacidade para tanto, pois as características descritas são consideradas simples para um programador mediano, faltando apenas o conhecimento de algumas técnicas de linguagem de baixo nível.

Há também os geradores de vírus, programas que facilitam muito essa atividade. Um vírus inédito pode ser **fabricado** em menos de cinco minutos, inclusive com opções que provocam o erro dos detectores de vírus mais conhecidos.

As **vacinas** e os detectores de vírus **residentes** baseados em reconhecimento de **assinaturas**, o mais comum, são praticamente ineficazes no combate aos vírus por não terem duas características fundamentais:

- não possuem as assinaturas dos vírus mais recentes. Deveriam ser atualizados em tempo real com a descoberta desses vírus, mas isto é impraticável porque a detecção somente ocorre após algum efeito destrutivo;
- há vários vírus que alteram o funcionamento desses detectores, impossibilitando seu desempenho conforme descrito nos manuais de instrução.

Existem os detectores de ação de vírus que travam o computador quando um procedimento duvidoso é solicitado a ele por um programa ou manualmente. Neste caso, a rotina de trabalho torna-se tão **amarrada** à digitação de senhas para liberação de acesso às atividades básicas que a produtividade fica muito comprometida.

MURALHAS DE FOGO

As empresas que estão aderindo à Internet com servidores conectados utilizam-se de ***fire walls***, ou literalmente **muralhas de fogo**, cujo objetivo é impedir o acesso de pessoas não-autorizadas à rede interna a partir das conexões externas.

Há *fire walls* elaborados por *softwares* residentes, os quais praticamente sofrem os mesmos riscos dos detectores de vírus residentes, e por *hardware*, programados internamente nos próprios equipamentos através de programação nos *chips* dos roteadores — circuitos que fazem as informações circularem entre os pontos da rede conhecidos como nós.

Existem empresas que adotam esses dois sistemas simultaneamente. No entanto, a solução mais adequada é fazer uma espécie de ***hall* de entrada**, ou seja, um computador ou uma rede com proteção por *software* ligado diretamente à Internet e outro computador ligado ao primeiro com um *fire wall*, fazendo a proteção em cascata e minimizando a perda de desempenho com o excesso de proteção simultânea e as incompatibilidades entre os dois subsistemas.

COMUNIDADE *HACKER*?

Todos os *hackers* contatam-se entre si, embora pouco saibam sobre seus nomes verdadeiros, pois normalmente tudo é feito por meio da própria Internet, preferencialmente por BBS's. Estas são simplificações da rede, de fácil manuseio, e podem ser montadas em minutos em qualquer computador com *modem*.

As BBS's assim montadas geralmente estão localizadas nas casas dos *hackers* e são **piratas**, tendo pouco tempo de duração. No período de um ano é provável que seu número para acesso mude pelo menos duas vezes.

Seus endereços são mutantes também em nível internacional, com velocidade ainda maior, o que justifica algumas de suas atitudes, como a adoção de linguagem escrita própria. Esta normalmente não é conhecida pelos demais e é impronunciável, consistindo de sinais que têm significado próprio. A palavra ***lamerz***, por exemplo, designa os que não são *hackers*, segundo os próprios. Outro exemplo é o sinal **;-)** que significa uma piscadinha de olhos.

O importante é que não se caracterize a linguagem utilizada com a intenção da pessoa, pois é sabido que os operadores de Telex também tinham sua linguagem, como **EH** para indicar o **É** por causa da ausência de acentuação. Esta forma ainda é utilizada, em especial pelos *hackers* novatos.

A comunidade é composta principalmente por pessoas com grande interesse pela informática, em especial

por autodidatas que se vangloriam de estar atrapalhando a vida dos **diplomados**.

CONCLUSÃO: PLANO DE AÇÃO

A partir do exposto, propõe-se um plano de ação. Naturalmente, deve-se estar consciente de que o mesmo será previsto pelos *hackers*. Seus principais pontos estão a seguir apresentados.

Contratação de consultoria externa

A primeira postura a ser adotada pela empresa é assumir que o invasor já pode estar dentro dela. Um funcionário futuramente insatisfeito poderá vir a ser um invasor. Assim, são os consultores externos os que têm maior eficácia no acompanhamento das atividades internas da empresa.

Criação de uma equipe interna

A empresa também deverá formar uma equipe interna de proteção com o objetivo de evitar os acessos externos e colaborar com a equipe de consultoria externa. Este trabalho conjunto é importante pelo fato de as empresas de consultoria estarem muito mais atualizadas do que as contratantes, que dependeriam de investimentos ininterruptos e onerosos para tanto.

Sistemática de *backup* terceirizada

O melhor método para precaver-se contra os problemas causados pela destruição parcial ou total de uma base de informações ainda é o *backup*. Todavia, ele deve ser feito com técnica adequada, infelizmente não possuída pela maioria das empresas. Em levantamento realizado em 1994 e 1995, aproximadamente 92% das empresas pesquisadas ou faziam *backup* com eficiência nula ou não o faziam.

A realização externa de *backup* possibilita que as cópias fiquem fora do alcance ou acesso dos possíveis *hackers* internos. Além disso, esse procedimento é uma ferramenta a mais de proteção contra outros tipos de contingências, como incêndio, roubo etc.

O papel do Administrador absorve, assim, mais uma atividade, relacionada ao surgimento desse novo tipo de agente do ambiente. É possível que no futuro a concorrência desleal contrate *hackers* para desorganizar corporações, além de para as atividades de espionagem industrial já denunciadas esporadicamente. ◆