CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso de Análise de Sistemas e Tecnologia da Informação

OS ATAQUES DE HACKERS CONTRA A SEGURANÇA DA INFORMAÇÃO ESTUDO DE CASO: KEVIN MITNICK

FERNANDO MOREIRA DA SILVA

Americana, SP
2013

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso de Análise de Sistemas e Tecnologia da Informação

OS ATAQUES DE HACKERS CONTRA A SEGURANÇA DA INFORMAÇÃO ESTUDO DE CASO: KEVIN MITNICK

FERNANDO MOREIRA DA SILVA
fmsmoreira@hotmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso de Bacharelado em Análise de Sistemas e Tecnologia da Informação da Fatec-Americana, sob orientação da Profª Acácia de Fátima Ventura

Área: Segurança da Informação

Americana, SP
2013

BANCA EXAMINADORA

Professora: Acácia de Fátima Ventura

Professor: Diógenes de Oliveira

Professora: Luciene Maria Garbuio Castello Branco

AGRADECIMENTOS

Agradeço primeiramente a todos os meus familiares, amigos e empregadores que compreenderam (ou não) minha ausência e reclusão nos últimos meses para me dedicar à realização desse trabalho.

Também agradeço aos meus professores e colegas de faculdade por terem me ajudado a chegar nessa etapa final, e acima de tudo, a minha orientadora, por ter me motivado e ajudado a realizar um trabalho dessa qualidade.

DEDICATÓRIA

Dedico este trabalho a Deus, aos meus pais, pelo apoio e paciência, aos meus amigos que aqui fiz e que eternamente estarão em minhas lembranças.

RESUMO

Este trabalho tem como objetivo fazer um levantamento bibliográfico sobre a informação e a importância da segurança da informação, bem como estudar os hackers e suas mais variadas classes, denominadas de acordo com o foco de seus ataques. O estudo atrela-se a uma pesquisa sobre os hackers mais famosos e suas façanhas, com uma ênfase especial para Kevin Mitnick. Por fim, descreve algumas sugestões de como fortalecer a segurança da informação em uma corporação, dadas pelo próprio Mitnick e outros especialistas no tema. A relevância está no conhecimento que o leitor poderá ter sobre a vulnerabilidade dos sistemas de informações.

Palavras Chave: informação; segurança; hacker

ABSTRACT

This work aims making a bibliographical survey about the information and the importance of information security. A study of the hackers and their various categories, named according to the focus of their attacks. Research was also raised about the most famous hackers and their exploits, with a special emphasis on Kevin Mitnick. Finally, some suggestions given by the Mitnick and other specialists about how to strengthen information security in a company. The relevance lies in the knowledge that the reader may have about the vulnerability of information systems.

Keywords: information, security, hacker.

SUMÁRIO

INTRODUÇÃO

A gestão da segurança da informação é um assunto que está sempre em pauta, em toda empresa ou organização que priva de conteúdo, dados e todo tipo de informação. A necessidade de segurança, para Nakamura (2003) é um fato que transcende o limite da produtividade e da funcionalidade. Mesmo que a velocidade e a eficiência em todos os processos de negócios possuam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em enormes prejuízos e falta de oportunidades de negócios.

Vulnerabilidades sempre existem e não são poucas. Até mesmo muito desconhecidas ou imperceptíveis dentro de qualquer organização, independente de ser de Tecnologia da Informação ou não. Para Mitnick (2003), pouca ou nenhuma empresa deixa de estar completamente vulnerável, no entanto, uma ênfase exagerada pode atrapalhar a realização dos negócios, inibindo assim o crescimento e a prosperidade da empresa, fazendo com que o grande desafio seja alcançar um equilíbrio entre segurança e produtividade.

Mitnick (2003) recomenda que se deva levar em consideração que os ativos[1] devem ser considerados de forma minuciosa, como ponto vital para o efetivo sucesso de administrar por onde passa, com quem passa e até onde chega essa informação.

Visando garantir a integridade desses dados confidenciais, as empresas se veem obrigadas a aderir protocolos de segurança cada vez mais rígidos, dificultando cada vez mais o acesso de pessoas sem permissão. Porém, o desafio de quebrar a segurança de sistemas de informação é um grande atrativo para os hackers. As atividades dos hackers, para Rufino (2002), podem ser subdivididas por categorias (*phreaker, carder, defacer, etc*), no entanto, um indivíduo pode pertencer a mais de uma categoria, ao passo que existem algumas que são antagônicas.

[1] tudo que manipula direta ou indiretamente a informação, inclusive ela própria, ou seja; em termos de segurança das informações, um ativo pode ser um computador, uma impressora, um fichário na mesa da secretária ou até mesmo o próprio usuário, não devendo ser confundido com o ativo patrimonial

Esses elementos são descritos no livro Segurança Máxima (2000), cujo autor não se identifica, como pessoas intensamente interessadas nos trabalhos que envolvem mistérios e esoterismo de qualquer sistema operacional de computador. Os hackers são frequentemente programadores e possuem conhecimento avançado de sistemas operacionais e linguagens de programação; são capazes de descobrir brechas dentro de sistemas e as razões para tais brechas. Estão sempre buscando mais conhecimento e compartilhando o que eles descobrem, jamais corrompendo dados intencionalmente. Já o cracker, é aquele que domina ou de outro modo, viola a integridade de um sistema de maquinas remotas, com intenção maliciosa, destruindo dados vitais, negando serviço de usuários legítimos ou causando problemas para seus alvos.

O estudo sobre hackers, crackers, as artimanhas que utilizam, aproveitando-se de brechas na segurança da informação e da fraqueza ou ignorância do ser humano é importante para reduzir ao menos a inocência de pessoas que possam ser a chave para o ataque dos mesmos.

Sendo o hacker, independente da índole, portador de uma inteligência avançada, pode-se questionar o que o levaria a realizar tais ataques, se é apenas a busca por novos desafios ou a forma mais lucrativa que encontrou de ganhar dinheiro com seus conhecimentos, ainda que de forma ilegal e imoral.

A pesquisa realizada tem vital importância para o campo de atuação, pois, muitas vezes, poderá se utilizar de tais conhecimentos para fortalecer os protocolos de segurança de um sistema para impedir a invasão de hackers ou até mesmo encontrar as brechas que poderiam ser vias fáceis para o mesmo. Ainda que o ser humano muitas vezes tenda a ser facilmente corruptível, ao menos, a partir do momento que se tem uma base de informação, erros por ignorância serão reduzidos, diminuindo em partes a fragilidade do fator humano diante de um ataque.

Já o **Problema** foi: A vulnerabilidade na segurança da informação diante de um hacker, pois como cita Nogueira (2008), este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem

consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. E, por mais rígidos que sejam os protocolos de segurança de um sistema, ainda é quebrável diante do fator humano. Segundo Fontes (2008), de nada adianta uma superestrutura de proteção técnica se os colaboradores não internalizam os conceitos de segurança.

Como **Pergunta** que se buscou responder: como reduzir a vulnerabilidade da segurança de um sistema de informação?

As **Hipóteses** foram: a) Promover reuniões e palestras para conscientizar e prevenir sobre os riscos de vulnerabilidade da segurança, sempre fiscalizando os resultados e aderindo a políticas de segurança mais rígidas, alterando constantemente códigos de acesso. b) O fato do ser humano ser facilmente corrompido diante de condições favoráveis para o mesmo, tanto financeiramente quanto por questões de ego. c) A constante troca de senhas e códigos pode minimizar os riscos, assim como a conscientização de funcionários para que não ocorra brechas na segurança devido a falta de informação e malícia, mas diante do fator humano, a vulnerabilidade sempre irá existir. Como não se pode fazer muito diante da possibilidade do ser humano ser corrompido ou subornável, a alternativa é investir cada vez mais em novos protocolos de segurança cada vez mais rígidos.

O **objetivo geral** consistiu em estudar o perfil do hacker, objetivando a redução de interferências dos seres humanos no sistema de informação.

Os **objetivos específicos** foram: 1. Fazer um levantamento bibliográfico sobre a informação e sua segurança. 2. Estudar os mais variados tipos de hacker, assim como a biografia de alguns hackers famosos. 3. Fazer um estudo de caso sobre Kevin Mitnick, seu histórico e seu perfil psicológico.

Como **metodologia** para o desenvolvimento deste trabalho, do ponto de vista da sua natureza, a pesquisa é básica, pois segundo Silva e Menezes (2001), objetiva gerar conhecimentos novos que serão úteis para o avanço da ciência, envolvendo verdades e interesses universais.

Do ponto de vista da forma de abordagem do sistema, segundo Silva e Menezes (2001) é qualitativa, pois leva em consideração a existência de uma relação dinâmica entre o mundo real e o sujeito, ou seja, há um vínculo indissociável entre o mundo objetivo e a subjetividade do sujeito que não pode ser traduzido em números. O ambiente natural é a fonte direta para coletar dados e o pesquisador é o instrumento chave, fazendo-a de forma descritiva e os demais pesquisadores tendem a analisar esses dados de forma indutiva. O processo e seu respectivo significado são os focos principais de abordagem.

Do ponto de vista de seus objetivos, a pesquisa é descritiva para Gil (1991), ela tem como foco descrever as características de uma determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Utiliza técnicas padronizadas de coleta de dados, como questionário e observação sistemática, assumindo a forma de levantamento.

Do ponto de vista técnico, a pesquisa é bibliográfica e documental, explicada por Gil (1991), como sendo elaborada a partir de material já publicado, principalmente livros, artigos de periódicos e atualmente com material disponibilizado na Internet e a partir de materiais que não receberam tratamento analítico.

O método utilizado para Lakatos (2010) foi o Dialético, pois foi desenvolvida unificando a interpretação de diferentes autores. As quatro leis fundamentais desse método são: a ação recíproca, unidade polar ou “tudo se relaciona”; mudança dialética, negação da negação ou “tudo se transforma”; passagem da quantidade à quantidade ou mudança qualitativa; interpenetração dos contrários, contradição ou luta dos contrários. Esse método penetra o mundo dos fenômenos através de sua ação recíproca, da contradição inerente ao fenômeno e da mudança dialética que ocorre na natureza e na sociedade.

O trabalho foi estruturado em quatro capítulos, sendo que o **primeiro** conceitua a informação e sua segurança, o **segundo** traz um breve conceito sobre hacker e os mais variados tipos existentes de hacker, além de uma breve biografia dos hackers mais famosos**,** o **terceiro** faz um estudo de caso sobre o hacker Kevin Mitnick, narrando sua trajetória. Por fim, o **quarto** apresenta sugestões para tornar a

segurança da informação menos vulnerável ao ataque de pessoas mal-intencionadas.

Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o quinto capítulo se reserva às **Considerações Finais**.

1. CONCEITUANDO INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO

Todo conteúdo ou dado de valor para um indivíduo ou uma empresa pode ser entendido como informação. Consiste em qualquer conteúdo com capacidade de transferência ou armazenamento, que tenha serventia para determinado propósito e tenha utilidade ao ser humano. Para a proteção de tais dados, existe a segurança da informação, para preservar seus respectivos valores para o individuo ou organização.

1.1. INFORMAÇÃO

Informação, segundo Peixoto (2006), se define como o ato ou efeito de informar ou informar-se. É o conjunto de conhecimentos sobre algo ou alguém; conhecimentos obtidos por alguém. Fato ou acontecimento que é levado ao conhecimento de alguém ou de um público através de palavras, sons ou imagens. Elemento de conhecimento suscetível de ser transmitido e conservado graças a um suporte e um código.

> A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional da empresa. (SÊMOLA apud PEIXOTO, 2006, p. 37).

Fontes (2008) afirma que a informação sempre foi um bem de grande importância para as organizações, porém, há alguns anos, a informação mais crítica para a empresa poderia ser simplesmente guardada e trancada dentro de uma gaveta. Entretanto, hoje, independente do estágio de tecnologia da organização, a proteção da informação tem que ser uma das principais preocupações dos executivos e proprietários das empresas. O executivo não precisa ser um especialista em segurança da informação, mas precisa possuir conhecimentos básicos sobre o assunto.

O Código de prática para a gestão da segurança da informação apresenta o seguinte:

> A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais

> interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS-ABNT, 2005, p.2)

Nem todas as informações são vitais, mas algumas podem ter tamanha importância que todo e qualquer custo aplicado para manter sua integridade não seria nada quando comparada ao custo de não dispor dessas mesmas informações. Para que se possa medir o grau de importância de uma informação, Wadlow (2000) classifica-a por níveis de prioridade que respeitam a necessidade de cada empresa, assim como a importância da classe de informação para a manutenção das atividades da empresa. Esses níveis seriam:

· **Pública:** Informação que pode vir a público sem maiores danos ao funcionamento normal da empresa, e cuja integridade não é vital.

· **Interna:** O acesso livre a este tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital.

· **Confidencial:** Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, a perdas financeiras ou de confiabilidade perante o cliente externo.

· **Secreta:** Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número reduzido de pessoas. A segurança desse tipo de informação é vital para a companhia.

Como o acesso a informações confidenciais foi se tornando cada vez mais visado por pessoas mal intencionadas com o intuito de sabotagem, passou a ser necessário adotar medidas de segurança para que esses ataques não causassem impactos maiores.

1.2. SEGURANÇA DA INFORMAÇÃO

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ABNT NBR ISO/IEC 27002, 2005).

Peixoto (2006) define que o termo “segurança da informação” pode ser designado como uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade.

Pesquisas realizadas no início desse século indicam que 53% das empresas brasileiras apontam os funcionários insatisfeitos como a maior ameaça à segurança da informação; 40% delas afirmam ter sido vítimas de algum tipo de invasão, 31% não sabem dizer se sofreram ataques e somente 29% alegam nunca ter sofrido ataques. Em 22% dos casos de ataque, as organizações não conseguiram detectar as causas e, em 85% dos casos não souberam quantificar o prejuízo. (BANNWART, 2001 apud PEIXOTO, 2006, p. 36).

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware (ABNT NBR ISO/IEC 27002, 2005).

Segundo Peixoto (2006), a segurança da informação é formada por três princípios básicos, que podem ser definidos da seguinte maneira:

PRINCÍPIOS BÁSICOS	DEFINIÇÃO
Confidencialidade	Garantia de que as informações que se deseja transmitir realmente cheguem ao seu destino sem ocorrer nenhum desvio para algum outro lugar no qual não deveria passar. Há muitas tecnologias, como criptografia e autenticações que, desde que seja mantida a integridade das informações, podem ser utilizadas para essa finalidade.
Integridade	Garantia de que não haja nenhuma alteração das informações durante o

	trajeto de remetente á destinatário, garantindo, dessa maneira, a real veracidade após chegar ao destino final.
Disponibilidade	Garantia de que será mantida a estrutura de passagem de informações, sempre com confiabilidade e integridade, impossibilitando que as informações sejam captadas. A informação tem que estar sempre disponível quando desejada, pois de nada adianta haver integridade e confidencialidade, se ela não estiver disponível.

Alguns modelos incluem mais dois pilares básicos que seriam:

Não repúdio e autenticidade: Geralmente conhecido como responsabilidade final. Sua meta é fazer a verificação da identidade e autenticidade de alguém ou até mesmo de um agente exterior para que seja possível garantir a integridade de origem.

Tais princípios refletem na organização e envolvem três aspectos principais:

Pessoas: Usuários bem munidos de orientação, treinamento e conscientização.

Processos: Protocolos de segurança da empresa sobre a utilização dos seus recursos tecnológicos e leis de punições rigorosas para infratores, no caso de desvio de informações.

Tecnologia: Sistemas com boas implementações que garantam a proteção das informações da empresa.

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado. [...] a função da segurança da informação é viabilizar os negócios. [...] (ABNT, 2005, p.2).

Segundo o Comitê Gestor da Internet no Brasil (2006), pessoas mal intencionadas tentam invadir computadores a fim de usar computador de terceiros para atividades ilícitas para dificultar sua identificação; lançar ataques contra outros computadores; usar seu disco rígido para armazenar dados; destruir informações; disseminar *Spam*; se passar por outras pessoas em mensagens de *e-mail*; espalhar vírus de computador; furtar número de cartões de credito ou senhas de banco e, furtar dados do seu computador em geral como, por exemplo, informações do seu imposto de renda.

Pipkin (2003) relata que com o rápido avanço do uso de computadores e da difusão da Internet, consequentemente houve uma expansão nos números de crimes computacionais e uma vasta diversidade de criminosos de computador.

Tanto as organizações como os seus sistemas de informação e redes de computadores estão expostos a vários tipos de ameaças à segurança da informação, como fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Cada vez se tornam mais comuns, ambiciosos e sofisticados os danos causados por código malicioso ou hackers estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

As medidas de segurança da informação são importantes para os negócios, independentes de serem do setor público ou privado e para proteção das infraestruturas críticas. Para ambos os setores, a segurança da informação tem como função viabilizar os negócios como o egov (governo eletrônico) ou e-business (comércio eletrônico), evitando e reduzindo os riscos de relevância. O controle de acesso é ainda mais dificultado com a interconexão de redes públicas e privadas e o compartilhamento de recursos de informação. A eficácia da implementação de um controle de acesso centralizado é reduzida com a tendência da computação distribuída.

> Diversos sistemas de informação não foram projetados para serem seguros. A segurança da informação pode ser alcançada por meios técnicos, mas acaba sendo limitada, tendo que ser reforçada por uma gestão e por métodos apropriados. É necessário um planejamento cuidadoso com atenção minuciosa aos detalhes para fazer uma identificação dos controles a serem implantado, podendo ser necessário também a participação de acionistas, fornecedores,

> terceiras partes, clientes ou outras partes externas, assim como uma consultoria externa (ABNT NBR ISO/IEC 27002, 2005).

Segundo Fontes (2008), existem dez principais aspectos da segurança da informação que todo proprietário ou executivo de uma organização deve conhecer. Eles são:

Não é um assunto somente da tecnologia: Muitas empresas pecam por acharem que somente soluções técnicas, como programas antivírus, podem estar protegendo a informação. É fundamental a empresa ter uma boa proteção tecnológica, mas não é o suficiente, podendo ser necessário contar com a ajuda de especialistas.

É uma decisão empresarial: Caso aconteça um fato no qual a empresa tenha um grande prejuízo ou impedida de continuar ou realizar seu negócio, serão os acionistas que perderão o investimento realizado.

Não acontece por milagre: Toda organização tem condições financeiras de realizar uma proteção adequada.

Deve fazer parte dos requisitos do negócio: A segurança da informação deve ser encarada como um elemento crítico que possibilita a realização do negócio.

Exige postura profissional das pessoas: Devem existir regulamentos, normas e políticas que valem para todos.

É liberar informação apenas para quem precisa: Se alguém não precisa da informação, não deve ter acesso, independentemente do nível hierárquico que exerça.

É implementar o conceito de Gestor da informação: Pode até continuar permitindo que a área de tecnologia seja a responsável pela autorização e liberação da informação para o usuário, porém, deve que existir uma autorização da área proprietária daquela informação.

Devem contemplar todos os colaboradores: Os parceiros da organização devem ter o mesmo nível de comprometimento que os seus funcionários.

É considerar as pessoas um elemento vital: De nada adianta uma super estrutura de proteção técnica se os colaboradores não internalizam os conceitos de segurança.

Exige alinhamento com o negócio: Não se deve estruturar e implementar um novo produto de negócio para depois considerar a proteção da informação.

1.3. FATOR HUMANO

Segundo Mitnick (2003), mesmo que uma empresa adquira as melhores e mais caras tecnologias de segurança, ou faça um investimento pesado em treinamento de pessoas e se implante protocolos de segurança mais rigorosos possíveis, a empresa ainda assim estará vulnerável.

> Ao testemunhar no Congresso há pouco tempo, expliquei que poderia conseguir senhas e outras informações sigilosas nas empresas fingindo ser outra pessoa e simplesmente pedindo essas informações. (...) O fator humano é o elo mais fraco da segurança. (MITNICK, 2003, p. 3)
>
> Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro. (EINSTEIN apud MITNICK, 2003, p.3)

Mitnick (2003) relata que muitos profissionais da tecnologia da informação conservam erroneamente a ideia de que tornaram suas empresas imunes ao ataque porque usaram produtos de segurança padrão, como firewalls[2], sistemas de detecção de intrusos ou dispositivos de autenticação avançados, como por exemplo, cartões biométricos inteligentes ou tokens baseados no tempo. Achar que produtos de segurança isoladamente oferecem a verdadeira segurança é um grande erro.

Aqueles que abusam do fator humano para aplicar seus golpes são denominados Engenheiros Sociais, que Mitnick (2003) descreve como pessoas que

[2] dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede

geralmente são charmosas, educadas e agradam facilmente, traços sociais determinantes para que se estabeleça uma relação de afinidade e confiança.

O fator humano é frágil por si já nas questões culturais, sobretudo na cultura ocidental, Mitnick lembra que não somos treinados a desconfiar do próximo, pelo contrário, o ser humano é ensinado a amar o próximo e ter fé e confiança nos outros. Fazendo uma analogia com suas vidas pessoais, as pessoas desobedecem até as organizações de segurança quando essas insistem em manter traçadas suas casas e carros, fazendo com que esse tipo de vulnerabilidade presente no ser humano se torne evidente.

2. CONCEITO DE HACKER E CRACKER

O hacker é um indivíduo que se dedica de forma intensa a conhecer e modificar os aspectos mais internos de programas, redes de computadores e dispositivos. Com seus conhecimentos avançados, conseguem romper as barreiras que deveriam impedir o acesso a informações restritas e suas motivações podem variar desde curiosidade á necessidade profissional, patriotismo, ativismo, competição ou pura vaidade, ou simplesmente cometer um crime. Os hackers que utilizam seus conhecimentos para fins imorais são denominados crackers. Dentro desses dois tipos de hackers, encontramos diversas facções e subgêneros caracterizados pelos tipos de ataques e conceitos éticos. Lembrando que, o mesmo individuo pode sim pertencer a mais de um grupo, tudo depende das atividades desempenhadas pelo mesmo.

2.1. HACKER

Hacker é a pessoa viciada em computadores, com conhecimentos de informática, que utiliza esse conhecimento para o benefício de pessoas que usam o sistema, ou contra elas (MICHAELIS, acesso em: 30/08/2013).

Segundo Himanen (2001), o termo hacker vem sendo de forma incorreta, designado a programadores que praticam atividades criminosas: aqueles que atuam violando os sistemas de empresas e que roubam números de cartões de crédito ou contas bancárias, na verdade, não passariam de crackers. A palavra inglesa hacker,

em seu sentido original, refere-se a programadores de computador entusiasmados, que compartilham seu trabalho técnico, científico ou artístico com outros. O termo hacker, que Himanen resgata, surgiu no início dos anos 1960 como a autodenominação utilizada por um grupo de jovens programadores do Massachusetts Institute of Technology (MIT), que tinham em comum o gosto pelos estudos, o conhecimento de informática e o jeito de lidar com os negócios.

> Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. (NOGUEIRA, 2008, p.61)

Himanen (2001) menciona que o hacker é também um indivíduo obcecado pelo trabalho, mas não pelos prazos. Seu compromisso não é com um emprego, mas com a expressão de sua realização como indivíduo; sua recompensa não é apenas o salário, mas o reconhecimento do seu trabalho pelos interessados neste trabalho. Os hackers creem que a revolução digital deve ser traduzida também em um tempo lúdico para a humanidade. A plena realização de suas capacidades criativas depende de seus impulsos, não podendo ser determinada por terceiros.

Segundo Freire (2004), um hacker do mal, por definição, é um sujeito com bons conhecimentos de programação e informática que os usa para espionagem industrial ou para lesar financeiramente pessoas, empresas ou instituições. Quem invade sites para fazer pichações virtuais, por exemplo, nem é mais considerado hacker hoje em dia.

São muito comuns os criminosos de a informática ser chamados de hackers, porém, essa nomenclatura não é a mais adequada. Os profissionais ligados á informática, preferem chamar os criminosos de crackers.

De maneira geral, os hackers, assim como os crackers, possuem um vasto conhecimento de informática, sabem como encontrar de forma fácil qualquer brecha de segurança nos sistemas, mas sem danificá-los.

Outro temo comumente associado aos hackers, segundo Assunção(2008), é o “White Hat”, que é designado para aqueles que, apesar do conhecimento sobre as brechas e falhas do sistema não cometem nenhum crime.

Segundo Assunção (2008), o Hacker White-Hat seria o “hacker do bem”, chamado de “hacker chapéu branco”. É aquela pessoa que se destaca nas empresas e instituições por possuírem um conhecimento mais elevado do que os demais colegas, por conta do autodidatismo e a paixão pelo que faz. Não chega a invadir sistemas e causar danos, exceto quando realiza testes de intrusão. Em outras palavras, tem um vasto conhecimento, mas não o utiliza de forma banal e irresponsável.

Rufino (2002) subdivide os hackers por facções, afirmando a existência de *phreaker*, *cracking*, *virii*, *warez*, *carding* e *coders.*

2.2. CRACKERS

Os crackers são criminosos que possuem um vasto conhecimento em informática, utilizando seus conhecimentos para encontrar brechas de segurança para causar danos a terceiros ou obter informações confidenciais.

> São pessoas especializadas em quebrar senhas. Ao contrário dos hackers, os crackers tem intenção criminosa (o cometimento de fraudes, espionagem, etc.) (CASTRO, 2003, p.219)

Enquanto os hackers costumam ser denominados como White hat, os crackers possuem o pseudônimo de Black hat, também podendo ser chamados de “hackers do mau” ou “hacker chapéu negro”.

Segundo Assunção (2008), o hacker Black-hat utiliza seus conhecimentos para roubar senhas, documentos, causar danos ou até mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido.

Segundo Rufino (2002), desde que o termo hacker surgiu nos meios de comunicação, perdeu-se a conotação romântica de antigamente. Antes, esse termo

era designado para indivíduos aficionados por computadores, atualmente é designado para piratas eletrônicos que possuem ligação com crimes utilizando computadores. Rufino desacredita que a associação do termo cracker com “aqueles que quebram sistemas”, para que não se haja uma conotação injusta com o termo hacker, é uma causa perdida.

Levando em consideração a carga pejorativa que o termo hacker adquiriu, os vendedores de serviço de segurança criaram o termo “hacker ético” para minimizar o impacto que causa ao cliente, e é a palavra ética que, segundo Rufino (2002) faz toda a diferença.

Os hackers e crackers possuem inteligência avançada, porém , ela é utilizada para fins diferentes, os hackers para o bem e os crackers para fins maliciosos.

Uma publicação do site TechWeb (2006), cita a existência de diversos relatos de sites que são invadidos diariamente pelos crackers. Muitas vezes, quando um site é invadido, são colocadas mensagens ofensivas (muitas vezes relativas à política) nesses sites com “assinaturas” do cracker que invadiu o sistema, gerando prejuízos incalculáveis. O pentágono e o FBI nos Estados Unidos já foram invadidos por crackers, diversas vezes. Quando se invade um site, o cracker assume um nível de controle parcial ou total, nesse último, gerando um prejuízo ainda maior.

Alguns hackers são contratados por sites para descobrirem vulnerabilidades das quais os crackers podem utilizar para invadi-los. Dessa forma, o hacker está realizando uma boa ação, fazendo com que o site se tornar mais seguro.

Muitos crackers se tornam hackers após serem pegos e punidos, como é o caso de alguns hackers famosos que serão mencionados nos próximos capítulos.

Segundo a matéria exposta no site InfoEscola (2013), os crackers ganham poder, fama e dinheiro com seus ataques, roubando contas bancárias, números de cartão de crédito, informações confidenciais, projetos secretos, projetos de produtos que serão lançados no mercado, dados pessoais e outras informações valiosas. Eles assumem o poder e subornam vítimas, pedindo dinheiro em troca dessas valiosas

informações roubadas, sendo que, é muito difícil capturá-los, já que possuem um enorme conhecimento computacional e capacidade de se superar a cada dia.

Neto (2009) divide os crackers conforme sua área de atuação, ou nível de conhecimento, como *phreaker*, *spammers*, *defacer* ou *pichador virtual*, *lammer* ou *carders*.

2.2.1. PHREAKER

Os phreakers são considerados por Spyman (2001) como hackers de telefonia, pois são especialistas em burlar os sistemas das operadoras de telefonia. Seus crimes mais frequentes são a clonagem de celulares, escutas telefônicas sem autorização, alteração do sistema de cobrança de telefones, etc.

Suas principais atividades são ligações gratuitas interurbanas, urbanas ou internacionais e a reprogramação de centrais de escuta. Sempre que o telefone tocar, o hacker será alertado para que se possa escutar a conversa sem consentimento do usuário. Há técnicas que permitem que fique invisível durante um possível rastreamento, fazendo com que o culpado pela ligação fraudada ainda pague pela conta gasta pelo phreaker.

Segundo Ulbrich (2006), o termo “phreaker” é composto pela junção das palavras *phone* e *freak* (maluco). Alguns anos atrás, esses indivíduos utilizavam gravadores de fita e outros dispositivos para produzir sinais de controle e enganar o sistema de telefonia e suas técnicas foram ficando mais complexas na medida em que as companhias telefônicas foram reforçando sua segurança. Atualmente, o phreaking é uma atividade elaborada na qual são poucos os hackers que possuem domínio.

2.2.2. SPAMMERS

Segundo Teixeira (2004), o spammer é o indivíduo que envia e-mail para uma ou mais pessoas sem que seja solicitado. São os responsáveis pelo envio em massa de mensagens não solicitadas, denominadas como spam. O envio dessas

mensagens em alguns países é considerado uma prática ilegal, mas o combate a elas ainda não é eficaz.

Já houve casos de prisão de spammers, mas decorrentes do crime que eles cometeram e não pelo envio do spam. Esses crimes podem ser um spam com programas maliciosos, com fins de invasão de sistemas e captura de senhas ou até mesmo fazendo se passar por outra pessoa.

Os meios de envio de spams são diversos, mas a mais frequente e popular é através do correio eletrônico. Os spammers utilizam programas ou sites que auxiliam na obtenção de listas de e-mails e enviam para um número extenso de destinatários. Outros meios de envio de spam são por telefone móvel (através de SMS), InstantMessaging (através de programas como o Skype), Newsgroup e fórum, mensagens de jogos online, blogs, wikis, livros de visitas, redes sociais, etc.

Teixeira (2004) explica que os spams enviados por esses indivíduos são de muitos tipos, como por exemplo: hoax (histórias falsas), correntes, propagandas, scam (golpes visando tirar proveito financeiro dos alvos), phishing (estelionato), programas maliciosos, vírus, worms, trojans ou simplesmente ofensivos, com conteúdos agressivos contra certos grupos, defendendo ideologias extremistas e fazendo apologia a violência, racismo, xenofobia e pedofilia.

A motivação para essa prática é o custo baixo, e a facilidade de enviar grandes quantidades de mensagens sem nenhum custo. Algumas pesquisas apontam que a porcentagem de pessoas que acabam caindo nos golpes do spammers, mas pode ser uma parcela significativa se levar em consideração o alto índice de mensagens enviadas por eles.

2.2.3. LAMMER

Lammer é o termo designado a quem se considera hacker, mas no entanto, não é muito competente e precisa de ferramentas para suas práticas. O termo Lammer, segundo o Dicionário Britânico (2006) é designado a uma pessoa ineficaz ou inepta. Esse termo possui um sinônimo mais moderno que é o *Script Kiddie*. Também são chamados de arackers por outros hackers.

Script Kiddies são descritos por Raymond (2003) no New Hackers Dictionary, na sua tradução literal significa garoto dos scripts, é uma forma depreciativa que foi atribuída aos crackers com pouca experiência, que necessitam do conhecimento de verdadeiros especialistas para desenvolverem suas atividades. São indivíduos que não possuem conhecimentos tecnológicos e não têm interesse em aprender, estão interessados apenas em ganhar fama ou em lucros pessoais.

Essa categoria de hacker é responsável por um numero considerável de ataques virtuais, geralmente, utilizando ferramentas prontas de crackers, como *trojans* e *exploits*. Uma prática muito comum desses elementos é camuflar um vírus em arquivo, tipo de ataque considerado amador pelos hackers profissionais. Muitas vezes os lammers são chamados de newbe, ou seja, aquele que se trata daquele que não possui conhecimentos de hacker ou cracker, mas insistem em se comportar como um, se vangloriando por saber utilizar os conhecimentos de outros.

2.2.4. CARDERS

São aqueles que realizam compras com cartões de crédito alheios ou gerados, ou seja, esses indivíduos possuem enorme facilidade de fazer compras pela Internet. São adeptos da prática do *carding* que Rufino (2002) descreve como a manipulação de cartões magnéticos (clonagem, leitura programação de chips) e telefônicos.

Spyman (2001) descreve os golpes desses indivíduos da seguinte maneira: Primeiramente, os cartões de crédito são totalmente verdadeiros. Quando o portador do cartão paga uma conta com o mesmo, seus dados são enviados a agenciadora deste cartão. Depois que esse cartão é debitado na agenciadora, entram os Crackers. Eles invadem o sistema, pegam todos os arquivos de cartão de crédito e distribuem no IRC (International Relay Chat) tornando ainda mais difícil identificar os crackers que pegaram os cartões. Uma vez distribuídas no IRC, as informações obtidas sem autorização sobre os cartões são passadas para os carders, por sistema de troca, normalmente uma conta Shell (conta especial em Linux ou Unix). Cada usuário carder irá usar o cartão em um ponto diferente do mundo.

2.2.5. OUTRAS CATEGORIAS

Além dos grupos já citados anteriormente, existem também outras designações para categorias de hackers e crackers como é o caso do defacer, white-hat, black-hat, gray-hat, newbie, hacktivist, virii, warez, coders, samurai, sneaker, etc. Alguns deles serão descritos a seguir.

Defacer é o indivíduo que pratica “pichação virtual”, que, no conceito de Rosa (2006), consiste em colocar indevidamente textos ou figuras em sites de terceiros sem autorização. No entanto, essa prática só é considerada um crime, caso ela provoque prejuízo patrimonial ao dono do site. Dependendo da interpretação, o simples fato de colocar um desenho ou assinatura em uma página pode não ser vista como um prejuízo. No Brasil, por exemplo, essa prática não é considerada um crime.

White-hat é a denominação para o hacker que estuda sistemas computacionais em busca de falhas na segurança, mas sempre seguindo os princípios da ética hacker. Quando encontra uma falha, normalmente esse hacker comunica primeiramente os responsáveis do sistema para que tomem as devidas providências. Assunção (2008) o descreve como o indivíduo que se destaca nas empresas e instituições por possuir um nível de conhecimento mais elevado que o dos demais, caracterizando-se por ser autodidata e por gostar do que faz. Tem um vasto conhecimento sobre informática, mas não o utiliza de forma irresponsável ou banal.

Black-hat é o oposto do *White-hat*, esse hacker não apenas deixa de respeitar a ética hacker, como também usa seu conhecimento, na maioria das vezes, para fins criminosos ou maliciosos. Segundo Assunção (2008), esses indivíduos utilizam seus conhecimentos para o roubo de senhas, documentos e causar danos ou realizar espionagem industrial. Costumam definir bem seus alvos, podendo levar até semanas antes de conseguir acesso onde deseja, caso o sistema seja bem protegido. É uma conotação alternativa para cracker, assim como o termo *“dark-side-hacker”.*

Gray-hat é literalmente traduzindo, o hacker chapéu cinza. Raymond o descreve como um meio termo entre o *White-hat* e o *Black-hat*, caracterizando-se por invadir sistemas por diversão mas evitando danos sérios e não copiando dados confidenciais.

Newbie é a conotação designada por Raymond para hackers principiantes, enquanto o termo *hacktivist* é dado por ele ao *hacker* que utiliza seus conhecimentos e habilidades com a intenção de praticar o bem, ajudando causas políticas e sociais.

Já Rufino (2002) atribui aos *hackers* que programam e colecionam vírus a denominação de *virii*, e *warez* para aqueles que realizam pirataria de software.

Já os *coders* são codificadores. Rufino (2002) descreve esses indivíduos como pessoas que possuem conhecimento em uma ou mais linguagens de programação, permitindo construírem programas, exploits e ferramentas de invasão e segurança. Geralmente examinam código-fontes em busca de vulnerabilidades que permitam a invasão.

Há também os termos *samurai* e *sneaker*, no qual Oliveira (2008) atribui a algumas classes de hackers éticos. Samurai é o hacker que atua na intenção de desvendar alguma falha de segurança, característica semelhante a do *hacktivist*. Investigando o direito de privacidade, menosprezam os crackers pelos propósitos que possuem, como destruir o sistema das empresas. O *sneaker* pode ser considerado o hacker que foi contratado pelas próprias empresas para desvendar as falhas de segurança de um sistema, para que se possa aperfeiçoá-los.

2.3. HACKERS FAMOSOS

Muitos indivíduos adeptos das práticas aqui citadas se sobressaíram e fizeram história. É o caso de Kevin Mitnick, John Draper, Mark Abene, Vladimir Levin, entre outros. Um breve histórico de alguns hackers famosos e suas respectivas proezas serão descritos a seguir.

2.3.1. JOHN DRAPER

Nascido em 1943, nos EUA, e conhecido como CaptainCrunch, é descrito por Spyman (2001) como sendo praticamente um ídolo para outros hackers conhecidos como Mitnick, Poulsen e Abene, também por figuras conhecidas no ramo da informática, como Steve Jobs e Steve Wozniak. Foi Draper que introduziu o conceito de phreaker, após conseguir realizar ligações gratuitas utilizando um apito de plástico que vinha de brinde em uma caixa de cereais que produzia um tom de 2.600 Hz, obrigando dessa maneira todo o EUA a trocar de sinalização de controle nos seus sistemas de telefonia.

John Draper possui o apelido de *CaptainCrunch* por ser o mesmo nome do mascote do cereal que ele encontrou o apito. Seguindo aos passos do pai, ele entrou na força aérea na década de 60, e nessa época ajudou membros das forças armadas no Alasca a fazer telefonemas de casa gratuitos, inventando acesso a um painel de comando de telefone local.

Filho (2010) relata que na década de 70, Draper ensinou suas habilidades de *phreaking* para Steve Jobs e Steve Wozniak, antes deles fundarem a Apple. O próprio Draper chegou a ser empregado na Apple, criando a interface telefônica para o Apple II que não chegou a ser comercializado.

Atualmente Draper faz softwares de segurança e é responsável pelo desenvolvimento do KanTalk, um software VoIP voltado para estudantes que querem praticar algum idioma. Também organiza um programa de TV na internet que leva o seu nome.

2.3.2. JOHAN HELSINGIUS

O finlandês mais conhecido como Julf, é, segundo Spyman (2001), o responsável por um dos mais famosos servidores de e-mail anônimo. Foi preso em 1995 quando se recusou a fornecer dados de um acesso que publicou documentos secretos da *Church of Scientology* na Internet. Para essa façanha, ele tinha apenas um 486 com 200MB de HD, sem nunca precisar usar seu próprio servidor.

2.3.3. VLADIMIR LEVIN

O russo Vladimir Levin pode ser considerado o ladrão digital mais notório da história, a ponto de a Interpol ter que intervir em seu caso. Segundo Spyman (2001), ele foi preso pela Interpol após meses de investigação, nos quais ele liderou uma gangue russa que invadiu os computadores do Citibank, transferindo dez milhões de contas bancárias dos clientes deste banco. Formado na universidade de Tecnologia de St. Petersburg, foi preso na Inglaterra enquanto tentava fugir do país. Insistiu em alegar que um dos advogados contratados para defende-lo era na verdade um agente do FBI.

2.3.4. EHUD TANEBAUM

Mais conhecido como Analyser, Tanebaum é israelense, e foi preso no fim da década de 90 após participar de um ataque organizado contra computadores do Pentágono. Segundo a matéria da revista Veja (25 mar 1998), Tanebaum contou com a ajuda de quatro jovens, dois israelenses e dois californianos.

2.3.5. MIKE CALCE

Mais conhecido como Mafiaboy, o canadense é um exemplo de Script Kiddie. Segundo Silva (2004), com apenas 15 anos confessou ser o autor dos ataques de indisponibilidade de serviço que derrubaram muitos sites renomados como Yahoo!, CNN e ZD Net, no início de 2001. O fato de ter alardeado demais os seus feitos acabou fazendo com que fosse preso, pegando oito meses de prisão.

2.3.6. MARK ABENE

Esse hacker americano, segundo Spyman (2001), foi inspiração para toda uma geração a explorar os sistemas públicos de comunicação. Com sua popularidade chegou a um nível de ser eleito uma das 100 pessoas mais “espertas” de Nova Iorque. Passou a trabalhar como consultor em segurança de sistema, utilizando o seu conhecimento para o bem. Abene é fundador de uma associação chamada “mestres da fraude”, estimulando aprendizes do mundo todo a invadir os sistemas telefônicos de seus países. Foi condenado a um ano de prisão, sendo homenageado em uma festa organizada por seus fãs.

2.3.7. ROBERT MORRIS

Americano que, segundo Spyman (2001), espalhou “acidentalmente” um worm que infectou milhões de computadores e fez boa parte da internet parar em 1988. Ironicamente, é filho de um cientista chefe do National Computer Security Center, parte da Agência Nacional de Segurança. Atualmente, Morris é considerado um mestre para os criadores de pragas virtuais.

2.3.8. HERWART HOLLAND-MORITZ

Mais conhecido como WauHolland, foi um hacker alemão nascido em 1951 e falecido em 2001. Foi um dos fundadores do CCC, um dos mais antigos clubes de *hacking* da década de 80. A fama desse grupo se deve ao episódio em que seus membros expuseram falhas de segurança do Bildschirmtext, um serviço online de videotexto interativo, que foi lançado nessa mesma década pelo Deutsche Bundespost, o serviço postal da Alemanha Ocidental. Aplicaram um golpe no qual o banco lhes enviou uma quantia correspondente a 68,513 euros, porém, no dia seguinte eles devolveram toda a quantia.

Holland dava conferências abordando o controle de informação, tanto governamental como para o setor privado. Sempre lutou contra a proteção anti-cópia e outras formas de censura, defendendo a infraestrutura de informação aberta.

Nos últimos anos de vida, se dedicava a aulas de ética e a ciência do hacking em centro de jovens, tendo o fino senso de humor como uma de suas características mais marcantes. Faleceu aos 49 anos por complicações de um acidente vascular cerebral.

2.3.9. JULIAN ASSANGE

Nascido em 1971 em Queensland, na Austrália, é mais conhecido por ser o principal porta-voz do site WikiLeaks, um wiki de denúncias e vazamento de informações. Fundou o WikiLeaks em 2006, fazendo parte do seu conselho consultivo.

Assange esteve envolvido nas publicações de documentos sobre execuções extrajudiciais no Quênia. Também divulgou documentos sobre resíduos tóxicos na África, o tratamento recebido pelos prisioneiros da prisão de Guantánamo. Em 2010, o WikiLeaks divulgou detalhes sobre o envolvimento dos Estados Unidos nas guerras do Iraque e Afeganistão e juntamente com parceiros, esse wiki passou a divulgar os telegramas secretos da diplomacia dos EUA.

Segundo o artigo publicado por Cardoso (2010) no portal R7, Assange foi acusado de estupro e abuso sexual na Suécia, perdendo sua cidadania sueca. Foi colocado na lista de procurados da Interpol, passando a temer uma possível extradição para os Estados Unidos, onde seria processado por abuso de computadores, espionagem e fraude. Porém, conseguiu abrigo na embaixada equatoriana em Londres.

Assange começou a *hackear* com pseudônimo de Mendax, com apenas 16 anos. Pertenceu a grupos de hacker que tinham como regras jamais danificar os sistemas de computador que podem acessar e jamais alterar as informações contidas nesses sistemas e compartilhar informações. Já foi acusado de ter acessado os computadores de uma universidade australiana, da Nortel do Canadá e de outras organizações por via modem. Assange alega que “hoje o Google sabe mais sobre você que sua mãe, esse é o maior roubo da história”.

Em entrevista à Forbes (2010), fez o seguinte comentário: "É um pouco chato, na verdade. Porque eu escrevi um livro sobre isso (ser hacker), existem documentários sobre isso, as pessoas falam muito sobre isso. Elas podem cortar e colar. Mas isso foi há 20 anos. É muito irritante ver artigos modernos me chamando de hacker de computador. Eu não me envergonho disso, estou muito orgulhoso disso. Mas eu entendo a razão pela qual sugerem que eu sou um hacker de computador agora. Há uma razão muito específica".

2.3.10. JOH JOHANSEN

Hacker norueguês mais conhecido como DVD Jon, conquistou fama após descobrir como burlar a proteção regional inserida nos discos de DVD comerciais.

Segundo Rosa (2006), Jon desenvolveu o programa que quebra essa proteção quando tinha apenas quinze anos, por conta disso, os pais dele é que foram processados. Foi absolvido com a lógica de que os DVDs são objetos relativamente frágeis quando comparado a livros, portanto, as pessoas deveriam ter o direito de fazer uma copia de segurança para seu próprio uso.

Mais tarde, Johansen desenvolveu um programa com capacidade de violar o dispositivo anti-cópia dos arquivos de áudio da Apple Inc e mais tarde confessou ter conseguido quebrar o código de ativação do iphone. Atualmente, está trabalhando para quebrar os sistemas anticópias do Blu-ray e do HD-DVD.

2.3.11. KEVIN MITNICK

Nascido em 1963 no estado da Califórnia, foi um cracker que ganhou fama mundial na década de 90, seu nick era o Condor.

Spyman (2001) o descreve como o mais famoso hacker do mundo, já foi preso por quatro anos, condenado por fraudes no sistema de telefonia, roubo de informações e invasão de sistemas. Os danos materiais causados por ele são incalculáveis.

Mitnick chegou a roubar 20 mil números de cartões de crédito, passando com desenvoltura pelo sistema telefônico dos EUA. Foi o primeiro hacker a aparecer na lista dos dez criminosos mais procurados pelo FBI. Atualmente está em liberdade e tem uma empresa que presta consultoria em segurança de sistemas.

Os primeiros delitos de Mitnick ocorreram em 1990, consistindo na invasão de diversos computadores, como operadora de celulares, empresas de tecnologia e provedores de internet. Além dos cinco anos que esteve preso, passou três anos em liberdade condicional, sob a restrição de não se conectar á internet e tendo seu telefone monitorado.

Ainda na adolescência, nos anos 70, chegou a invadir o computador da escola, alterando algumas notas, e posteriormente, desenvolveu enorme interesse

por pirataria de sistemas telefônicos de tal forma que chegou a invadir as instalações da Pacific Bell, furtando alguns manuais técnicos.

Mitnick violou sua condicional viajando para Israel, com o intuito de encontrar alguns amigos crackers. Como a polícia mantinha suspeita de que continuava invadindo sistemas, resolveu desaparecer com uma identidade falsa. Com isso, sua atividade cracker continuou com maior intensidade.

Mitnick foi descoberto após uma armadilha feita por Tsutomu Shimomura, especialista em segurança no Centro Nacional de Supercomputação, que descobriu que Mitnick havia invadido seu computador, e a partir de uma mensagem deixada por ele, a policia pode rastrear e identificar de onde ele estava atuando.

Atualmente, segundo Mitnick e Simon (2003), Mitnick é consultor de segurança para corporações em diversos países e co-fundador da DefensiveThinking, empresa de consultoria sediada em Los Angeles. Também escreve livros e artigos sobre segurança da informação e ministra palestras por todo o mundo.

Os feitos e o histórico de Mitnick serão abordados de forma mais detalhada no capítulo 3.

2.3.12. TSUTOMU SHIMOMURA

Formado em física, o "samurai" trabalha como especialista em sistemas de segurança do Centro de Supercomputadores de San Diego, na Califórnia, Estados Unidos. Sua fama se deve à peça que conseguiu pregar naquele que foi considerado o mestre dos criminosos cibernéticos, Kelvin Mitnick, em um golpe conhecido como "Takedown".

Conhecido como Takedown, Shimomura é um cientista da informação e hacker com certa notoriedade nascido no Japão e naturalizado norte-americano, trabalha como especialista de segurança no Centro de Supercomputadores de San Diego, Califórnia. Shimomura foi peça-chave na captura de Kevin Mitnick, após este ter invadido seu computador, criou uma armadilha que levou á prisão de Mitnick, que

mandava mensagens provocando-o, se referindo a Tsutomu como “meu aprendiz”. A façanha de Shimomura na captura de Mitnick foi relatada no livro escrito pelo próprio Shimomura, “Contra-Ataque”.

Takedown deu origem a um filme que relata esse duelo entre Shimomura e Mitnick. No filme, vemos Shimomura como um grande especialista em segurança, que, durante suas férias, teve seu computador pessoal invadido por Mitnick, que além de ter roubado informações pessoais, acabou encontrando o programa “desprezo”, um poderoso vírus capaz de afetar milhares de computadores.

Dessa forma, o objetivo de Mitnick é decifrar o arquivo e compartilhar com o mundo todo. A partir daí, Tsutomu se empenha na busca por Kevin, viajando para vários países, passando madrugadas monitorando, motivando e recrutando outros profissionais para auxiliá-lo e, quando finalmente Kevin conseguiu decifrar o arquivo, foi surpreendido por uma força tarefa, decidindo então fazer o compartilhamento, mas Shimomura consegue interceptar o envio, fazendo com que Kevin seja preso e julgado.

2.3.13. KEVIN POULSEN

Kevin Poulsen é o hacker Watchman, também americano e descrito por Spyman (2001) como amigo de Mitnick, também especialista em telefonia, de habilidade rara, ganhava concursos nas rádios frequentemente. Em 1990 ganhou um porsche por ser o 102º ouvinte que telefonou, quando na verdade ele invadiu a central telefônica, interceptando ligações, garantindo seu prêmio de forma fácil. Passou quatro anos preso e atualmente é diretor do site Security Focus. Embora tenha quebrado quase todo tipo de site, Poulsen tem predileção por sites com dados militares, fazendo com que isso complicasse seu período de encarceramento.

3. ESTUDO DE CASO: KEVIN MITNICK

O mais famoso hacker do mundo, Kevin Mitnick, responsável por tornar popular o termo Engenharia Social, foi fonte de inspiração para outros hackers e para a criação de livros e filmes a seu respeito. Em seu próprio livro, “A Arte de Enganar”, conta como foi o seu primeiro contato com a técnica, ainda precocemente. Em uma pesquisa sobre o tema, é impossível não dar uma ênfase especial para Kevin, que para a realização de seus ataques, tinha como arma principal não somente recursos e seu vasto conhecimento tecnológico, mas a capacidade de enganar as pessoas, aproveitando-se das fraquezas do fator humano.

3.1. TRAJETÓRIA DE KEVIN MITNICK

> Todas as noites eu “conecto” com o intuito de poder desabafar ao máximo, até me cansar para, então, o sono chegar, e levar-me para a cama. Tento imaginar o futuro todo dia, e o único futuro que desejo observar, é a solução para uma dor que me consome sem pressa de acabar. A solidão realmente gostou da minha pessoa. Gostou tanto que resolveu me visitar todas as noites. E sempre muito mal educada, pois chega, sem avisar, sem pressa para terminar suas pressões psicológicas. (SPYMAN, 2001, p.1)

> Mas, a solidão não contava de encontrar um cara tão maluco quanto ela. Pois, sou um Hacker, e a rede me trouxe felicidade. Felicidade de saber que a solidão não me faria chorar de desgosto, e cair em suas tentações e infelicidades. A Rede com suas fantasias e mistério, numa conectada me traz tesão, me faz ter desejo, me faz forte e quente, me faz chorar e rir, me faz ter vontade de correr, vontade de gritar, de amar, vontade de viver e esquecer tudo. É uma força que dificilmente conseguiríamos sozinhos, é um amigo para todos os problemas, é uma janela para um mundo quente, lento e misterioso. Todos têm o seu porque, eu tenho o meu, e com certeza, você deve ter o seu. Muitos acham isso uma loucura. Loucura é a minha vida... Hacker! (SPYMAN, 2001, p.1)

> Nós nascemos com um impulso interno de explorar a natureza daquilo que nos cerca. Como todos os jovens, Kevin Mitnick e eu éramos muito curiosos sobre o mundo e ansiosos para testar a nós mesmos. Quase sempre fomos recompensados pelas nossas tentativas de aprender coisas novas, solucionar quebra-cabeças e ganhar jogos. Mas ao mesmo tempo, o mundo ao nosso redor nos ensinou regras de comportamento que restringiam nossa necessidade de exploração livre. Para os nossos ousados cientistas e empreendedores tecnológicos, bem como para pessoas como Kevin Mitnick, seguir essa vontade traz as maiores emoções e permite que realizemos coisas que os outros acreditam que não podem ser feitas.(WOZNIAK apud MITNICK, 2003, p.9).

Mitnick (2003) se descreve tendo sido uma criança bonita e feliz, porém, chateada. Cresceu em Los Angeles, filho de pais separados, desde que ele tinha três anos, e sem muitos recursos financeiros, sua mãe teve que trabalhar como garçonete após o divórcio. Seu primeiro truque ocorreu ainda na adolescência, quando utilizou um furador de papel para fraudar bilhetes de ônibus para viajar sem comprar passagens. Um motorista amigo, ao responder suas perguntas cuidadosamente formuladas, acabou contando onde ele poderia comprar aquele tipo especial de furador de papel.

A explicação que Mitnick (2003) dá a esse seu primeiro golpe é que as baldeações permitem a troca de ônibus para continuar a viagem até o destino, mas ele havia descoberto como usá-las para viajar para qualquer lugar que quisesse de graça, pois as lixeiras dos terminais de ônibus estavam cheias de blocos de passagens parcialmente usados, os quais eram jogados pelos motoristas no final de seus turnos. Com um bloco de passagens em branco e o furador, era possível marcar as próprias baldeações e viajar para qualquer parte aonde fossem os ônibus de Los Angeles.

Outro interesse pessoal de Mitnick que surgiu precocemente foi o fascínio por mágica. Sempre buscava aprender como os novos truques funcionavam e estava sempre os praticando até que dominasse. Ele relata que foi a partir daí que sentiu o prazer por enganar as pessoas.

O primeiro contato de Kevin com aquilo que viria a chamar de engenharia social ocorreu durante o ginásio, quando conheceu outro aluno que foi pego com um hobby chamado *phonephreaking*. Esse é um tipo de hacking que possibilita vasculhar a rede telefônica explorando os sistemas de telefone e os empregados da empresa de telefonia. Esse amigo lhe mostrou os truques que podiam ser feitos com um telefone, como por exemplo, obter todas as informações que a empresa de telefonia possuía sobre um determinado cliente e como utilizar um número de teste secreto para realizar ligações interurbanas gratuitamente.

Após observar os feitos desse amigo phreaker e de outro que conheceu posteriormente, não demorou muito tempo para Mitnick passar a desenvolver seus próprios truques e utilizar-se desses meios por mais de uma década.

Uma das peripécias que Mitnick (2003) define como uma de suas preferidas era obter o acesso não autorizado a uma central telefônica e alterar a classe de serviços de um colega phreaker. Assim, sempre que a vítima tentava realizar uma ligação de sua residência, o mesmo recebia uma mensagem solicitando o depósito de vinte e cinco centavos, alegando que a central da empresa de telefonia teria recebido informações de que estivesse ligando através de um telefone público.

Mitnick (2003) relata que despertou interesse por tudo que fosse referente a telefones, não se limitando apenas a eletrônica, mas também a organização corporativa, os procedimentos e as terminologias. Esse interesse, com o passar do tempo, fez com que possuísse mais conhecimento sobre sistema de telefones do que qualquer funcionário da empresa. Suas habilidades se desenvolveram ao ponto de, ainda com 17 anos, ser capaz de falar com a maior parte dos empregados da empresa de telefonia sobre quase tudo, tanto pessoalmente como por telefone.

Sua tão “aclamada” carreira de hacker teve início nos tempos do colégio, sendo que, segundo o próprio Mitnick (2003) uma das metas principais para suas primeiras ações foi com o intuito de ser aceito no grupo de hackers. Ainda que, nessa época, a terminologia do hacker era atribuída na descrição do indivíduo que passava a maior parte do tempo mexendo com hardwares e softwares, tanto para o desenvolvimento de programas mais eficientes ou na eliminação de etapas desnecessárias e realizar um trabalho de forma mais ágil. Embora hoje, o termo hacker tenha ganhado um significado maléfico, o próprio Mitnick alega que utiliza ainda o termo hacker no seu sentido mais antigo e benéfico, destinado a programadores de computador que possuíam grande entusiasmo pelo o que faziam e sempre partilhavam seu trabalho técnico, cientifico ou artístico com outros.

Após o término do colégio, Mitnick (2003) conta que fez um curso sobre computadores no Computer Learning Center, em Los Angeles. Meses depois, o gerente de computadores da escola notou que uma vulnerabilidade no sistema

operacional havia sido descoberta e havia ganhado alguns privilégios administrativos totais sobre o minicomputador IBM dele. Nem mesmo os melhores especialistas em computadores do corpo docente foram capazes de detectar como ele havia feito aquilo. Graças a sua façanha, Mitnick recebeu uma proposta irrecusável, para que criasse um projeto dentro dos padrões e normas visando à melhora da segurança nos computadores, caso contrário, teria uma suspensão pelo o seu feito. Dessa maneira, não restou alternativa a não ser acatar.

> Tive sorte e gosto do meu trabalho. Você não pode imaginar o desafio, a gratificação e o prazer que sentia no período em que trabalhei como detetive particular. Eu estava aperfeiçoando meus talentos na arte teatral chamada engenharia social — fazer com que as pessoas façam coisas que normalmente não fariam para um estranho — e sendo pago para fazer isso. (MITNICK, 2003, p. 13)

Para Mitnick (2003), não houve dificuldades para que se tornasse proficiente em Engenharia Social, pois o lado paterno de sua família trabalhava com vendas há gerações, herdando assim a arte da influência e persuasão. Ele relata que quando há a combinação da inclinação para enganar as pessoas com talentos da influência e persuasão é possível chegar ao perfil de um engenheiro social.

Mitnick (2003) explica que há duas especialidades dentro da classificação do cargo de artista da trapaça. Aquele que faz falcatruas e engana as pessoas com o intuito de tirar benefício financeiro pertence a uma subespecialidade denominada como grifter. Já aqueles que utilizam a fraude, a influência e persuasão contra as empresas com o intuito de obter suas informações, se enquadram em outra subespecialidade, a de engenheiro social. Mitnick já reconhecera um talento para descobrir os segredos que não deveria saber desde os tempos em que aplicava seu truque com a baldeação de ônibus, quando ainda era jovem e sem a noção do quanto era errado o que estaria fazendo.

A maneira que Mitnick (2003) recorreu para aperfeiçoar sua arte foi escolhendo certas informações nas quais aparentemente não se importava e ver como seria possível convencer alguém do outro lado da linha a fornecê-las, com o intuito exclusivo de aperfeiçoar suas habilidades. Dessa forma, ele praticou a criação de pretextos da mesma maneira que praticava seus truques de mágica e, através

desses ensaios, descobriu que era possível obter qualquer informação que desejasse.

> Tive acesso não autorizado aos sistemas de computadores de algumas das maiores corporações do planeta, e consegui entrar com sucesso em alguns dos sistemas de computadores mais protegidos que já foram desenvolvidos. Usei meios técnicos e não técnicos para obter o código-fonte de diversos sistemas operacionais e dispositivos de telecomunicações para estudar suas vulnerabilidades e seu funcionamento interno. (MITNICK, 2003, p. 13)

Desde a época de sua prisão que Mitnick (2003) diz ter reconhecido que suas ações eram ilegais e que ele cometeu invasões de privacidade. No entanto, alega que seus crimes foram motivados pela curiosidade, já que o que mais queria era saber o máximo possível sobre a maneira em que funcionavam as redes de telefonia e os prós e os contras da segurança de computadores.

Kevin Mitnick passou de uma criança que adorava fazer truques de mágica para o hacker mais conhecido do mundo, temido pelas corporações e pelo governo. Mitnick (2003) cita que ao pensar nesses últimos 30 anos, tem que admitir que tomou algumas decisões ruins, motivadas pela sua curiosidade, pelo desejo de aprender sobre a tecnologia e pela necessidade de um bom desafio intelectual. Porém, alega ser outra pessoa atualmente.

> Estou transformando meus talentos e o extenso conhecimento que reuni sobre a segurança das informações e sobre as táticas da engenharia social para ajudar o governo, as empresas e os indivíduos a evitar, detectar e responder às ameaças da segurança da informação. (MITNICK, 2003, p.14)

A trajetória de Mitnick como hacker tem início em 1980, quando, com o auxilio de outros hackers, invadiu a rede da empresa US Leasing. Posteriormente, em 1984, Mitnick teve sua casa vasculhada por policiais, estando ele escondido da justiça.

No período entre 1985 e 1987, Mitnick invadiu a rede da National Security Agency (Centro de Espionagem do Governo dos EUA) e da Santa Cruz Operation (fabricante de softwares), pegando três anos de liberdade condicional. Nesse mesmo período, casou-se com a namorada Bonnie Vitello.

Um ano depois, o site da NASA (Agência Nacional do Governo dos EUA) foi invadido, e tal ataque foi atribuído a Mitnick pela imprensa. O hacker acabou sendo preso pelo FBI, recebendo a sentença de um ano de reclusão e mais cinco anos de liberdade condicional. Divorciou-se da esposa nessa época.

Em 1992, Mitnick passa a trabalhar para uma empresa de detetives, violando dessa maneira sua condicional. O hacker foge após FBI tentar prendê-lo. Dois anos depois, o governo da Califórnia oferece a recompensa de um milhão de dólares pela captura de Kevin, que por sua vez, invadiu a rede particular do especialista Tsutomu Shimomura, que um ano depois, após persegui-lo, consegue localizar Mitnick, resultando na prisão do hacker após ter invadido a rede do provedor The Well. Somente em 1999, após quatro anos preso, sem direito a julgamento, Mitnick faz acordo com o governo dos EUA, sendo solto em 2000 após pagar uma multa de U$ 4.000, porém, impedido de trabalhar ou usar um computador. Essa restrição durou até 2003, mais precisamente até o dia 21 de janeiro, a partir daí pode acessar a internet normalmente.

Apesar de suas diversas capturas na década de 80, Mitnick sempre voltou a praticar invasões, aproveitando-se das penas relativamente pequenas que recebeu. A não ser pelo episódio em que invadiu de forma audaciosa o computador do cientista e especialista em segurança Tsutomu Shimomura, que vinha ganhando fama por sua colaboração com o governo americano.

O resultado da caçada cibernética foi a desgraça de Mitnick, localizado e preso num apartamento alugado na Carolina do Norte, sendo encarcerado por cinco anos. Sua prisão causou revolta entre seus fãs e ajudou a alimentar o mito do hacker na internet, que chegou a servir como forma de arrecadar fundos para a defesa legal de Mitnick.

O Departamento de Justiça dos EUA estima que Mitnick tenha causado prejuízos de US$ 1 milhão, no entanto os promotores de acusação estimam um valor em torno de US$ 300 milhões.

Apesar da capacidade de Mitnick de manipular redes de telefonia celular para acessar a internet sem ser detectado e outros feitos tecnológicos consideráveis, a estratégia principal utilizada na invasão de computadores foi a engenharia social, que nada mais é do que o ato de enganar funcionários de empresas de informática para conseguir senhas e contas de acesso.

Uma marca registrada nas invasões de Mitnick é que, embora muitas vezes sejam feitas em redes altamente confidenciais, não possui a agressividade associada aos demais invasores digitais, sendo a destruição de arquivos alheios uma atitude extremamente rara.

A necessidade de acessar sistemas proibidos sempre foi uma constante na vida do hacker. A começar por sua ex-mulher, Bonnie Vitello que nada mais era do que uma funcionária da companhia telefônica General Telephone, que o auxiliou nas práticas de invasões. Na época em que os dois namoravam, mais precisamente em 1987, foram presos pelo FBI, sendo ela liberada meses depois, casando-se então com ele.

Mitnick não se diz arrependido, alega que o que fez não era ilegal quando começou, mas se tornou crime depois que a nova legislação foi aprovada, sendo que ele continuou mesmo assim. Além do mais, o mesmo alega que o principal motivo de suas ações foi por pura diversão.

Em setembro de 2003, foi lançado um filme que conta a história sobre a caçada de Kevin Mitnick, intitulado de Takedown, baseado no livro de mesmo nome escrito por Tsutomu Shimomura, no qual o autor relata a façanha pela captura do hacker mais famoso daquela época.

O filme, no entanto aponta algumas contradições com a realidade. No filme, Mitnick é caracterizado como uma pessoa simpática, porém com tendência a ataques de raiva, com certa atração por escutas eletrônicas, além de nutrir um ódio por mulheres. Seu intuito era utilizar seus conhecimentos na criação de um grande blecaute.

No entanto, o verdadeiro Mitnick invadiu redes de operadoras de telefonia celular, provedores de internet e universidades. O próprio Mitnick desaprovou o filme. “Estou desapontado, pois o filme me mostra fazendo coisas que não são reais”, disse em entrevista ao site “SecurityFocus”.

> Kevin Mitnick é uma das melhores pessoas que conheço. Pergunte e ele responderá de forma direta que aquilo que ele fazia — a engenharia social — era trapacear as pessoas. Mas Kevin não é mais um engenheiro social. E mesmo quando o era, o seu motivo nunca foi enriquecer ou causar danos às outras pessoas. Isso não quer dizer que não existam criminosos perigosos e destrutivos que usam a engenharia social para causar danos reais. (WOZNIAK apud MITNICK, 2003, p.9)

3.2. TAKEDOWN – O FILME

Filme baseado no livro de mesmo nome de Tsutomu Shimomura, o qual ele foi coprodutor, acompanhando as filmagens e guiando os atores, relatando como Mitnick deveria agir em cena. Quem assistir o filme, e conhecer a fisionomia de Shimomura, verá o mesmo em cena, fazendo figuração na cena em que o personagem Shimomura dá uma palestra sobre segurança.

Mitnick é interpretado pelo ator Skeet Ulrich (mais conhecido por seus papéis em Pânico, Jovens Bruxas, Aventuras no Alasca e pelo seriado Jericho), enquanto Shimomura é interpretado por Russel Wong (conhecido por suas atuações nos filmes Romeu tem que Morrer e A Múmia 3: A Tumba do Imperador Dragão).

O filme se passa na época em que Mitnick estava sob condicional, e com a ajuda de seu melhor amigo, consegue obter acesso ao código SAS, que permitia escutar o que era conversado na linha telefônica que ele desejasse ouvir, podendo agir e fugir antes que o FBI ou quem desejasse encontra-lo agisse.

Certo dia, ao acompanhar pela TV um congresso que contava com a presença de Tsutomu, falando a respeito do Nokitel, Mitnick se interessou por ter acesso a tais informações. Após ligar para Shimomura, tentando aplicar um de seus golpes de Engenharia Social, Mitnick não teve sucesso e ainda foi chamado de “relaxado”,

despertando sua ira, de forma que ligou para Shimomura novamente revelando que sabia sobre detalhes da vida pessoal do mesmo.

O embate dos dois só estava começando, Mitnick consegue hackear o computador pessoal de Shimomura, inclusive obtendo informações a respeito de um vírus perigosíssimo. Após um conflito entre ambos que se estende pelo filme, Shimomura consegue identificar o paradeiro de Kevin, resultando em sua prisão, e ainda conseguindo impedir o carregamento do vírus na rede.

O desfecho do filme se passa no presídio, em uma visita de Tsutomu a Mitnick, onde Mitnick questiona o porquê ele está lá e não Tsutomu, que reage como se as palavras de Kevin surtissem efeito em sua consciência e após o fim da sessão de visitas, Shimomura se dirige a um caixa bancário, tendo seu cartão preso na máquina e o saldo zerado, aparecendo no monitor a mensagem “Free Kevin”.

Uma passagem interessante do filme é, durante um ataque de ira de Kevin, onde ele questiona o porquê é considerado tão ardiloso, já que ele possuía conhecimentos e meios para esvaziar qualquer conta bancária, desviando para outra e não o fazia.

O filme foi bastante questionado pela crítica e até mesmo por Kevin Mitnick ou pessoas ligadas ao tema, por haver muitas contradições com os fatos reais e com a verdadeira personalidade dos personagens.

3.3. FREEDOM DOWNTIME

Trata-se de um filme-documentário feito por ativistas durante o processo de produção do filme Takedown, foi dirigido e narrado pelo também hacker Emmanuel Goldstein. O objetivo inicial era barrar a produção do filme, pois o mesmo iria ser lançado na época em que aconteceria o julgamento de Kevin Mitnick, logo, a imagem de criminoso do hacker exposta no filme poderia influenciar no resultado do julgamento.

O documentário se passa na época em que Kevin estava preso, aguardando julgamento e relata e até mesmo apresenta provas de que muitas acusações de

Kevin Mitnick não possuem fatos que as tornem verídicas, muitas delas foram desmentidas durante o filme.

Freedom Downtime conta com o depoimento de muitas pessoas ligadas a Mitnick, como Kevin Poulsen e até da mãe de Kevin, além de outros hackers e simpatizantes.

As pessoas ligadas a essa produção percorreram várias cidades e estados dos Estados Unidos que havia ligação com Kevin Mitnick, Tsutomu Shimomura e John Markoff promovendo a campanha “Free Kevin” (podendo ter influenciado o desfecho de Takedown). Aliás, Markoff teve enorme influencia na vida de Mitnick, sendo o responsável por publicar matérias sobre Kevin no The New York Times sempre se referindo a ele como alguém de alta periculosidade e demonstrando um enorme interesse por estudar sobre Kevin, inclusive sendo um dos autores do livro Takedown, ao lado de Shimomura.

Em Freedom Downtime, Markoff aceitou ser entrevistado e para a surpresa de quem teve a oportunidade de assistir, apresentou em muitos momentos uma certa falta de conhecimento sobre pontos de enorme relevância sobre Kevin.

4. SUGESTÕES PARA OS PROFISSIONAIS DE SEGURANÇA DA INFORMAÇÃO

Firewall, dispositivos de segurança avançados, sistemas de detectores de invasão, criptografia, acesso limitado aos números de telefone de discagem por modems, nomes de código nos servidores para dificultar que um estranho determine qual servidor pode conter os planos do produto. A grande verdade é que independente de qual dessas medidas e quantas delas serão implantadas por uma empresa, não existe uma tecnologia no mundo que evite um ataque, ainda mais vindo de um engenheiro social.

4.1. PROGRAMAS DE TREINAMENTO E CONSCIENTIZAÇÃO

O risco que a empresa corre não é reduzido com a criação de panfletos ou de páginas de intranet sobre a política de segurança adotada. Para Mitnick (2003), as empresas não devem somente definir por escrito as regras de política, mas também orientar a todos os que trabalham com as informações corporativas ou com sistemas de computadores para que eles aprendam e sigam as regras. Também é necessário fazer com que todos entendam a razão de cada política, para que as pessoas não tentem desviar essas regras por questões de conveniência. Caso contrário, a ignorância sempre será a desculpa mais frequente dos empregados, e essa vulnerabilidade que é explorada pelos engenheiros sociais.

> O objetivo central de um programa de conscientização sobre segurança é influenciar as pessoas para que elas mudem seu comportamento e suas atitudes motivando cada empregado a querer entrar no programa e fazer a sua parte para proteger os ativos de informações da organização. Um ótimo motivador nesse caso é explicar como a participação das pessoas beneficiará não apenas a empresa, mas também os empregados individuais. Como a empresa detém determinadas informações particulares sobre cada funcionário, quando os empregados fazem a sua parte para proteger as informações ou os sistemas de informações, na verdade eles estão protegendo também as suas próprias informações. (MITNICK, 2003, p. 198).

Um programa de treinamento de segurança ideal necessita de um suporte substancial. Para Mitnick (2003), o esforço do treinamento deve atingir cada pessoa que possui acesso a informações confidenciais ou aos sistemas corporativos de computadores. O treinamento deve ser continuo e sempre revisado para que se

possa atualizar o pessoal sobre as novas ameaças e vulnerabilidades. Deve ser perceptível para os empregados o quanto a direção está totalmente comprometida com o programa. Esse comprometimento deve ser real e não apenas um memorando carimbado. O programa deve ser fundamentado por recursos suficientes para desenvolver, comunicar, testar e medir o sucesso.

No entanto, Mitnick (2003) lembra que para aquelas empresas que não possuam recursos para desenvolver um programa interno, há diversas outras empresas que oferecem serviços de treinamento em conscientização sobre a segurança. As feiras, tais como a Secure World Expo, são pontos onde essas empresas podem ser encontradas.

> Como a conscientização e o treinamento para a segurança e o treinamento nunca são perfeitos, sempre que possível use tecnologias de segurança para aumentar seu sistema de defesa. Isso significa que a medida de segurança é fornecida pela tecnologia e não pelos empregados individuais, por exemplo, quando o sistema operacional está configurado para evitar que os empregados façam o download de software da Internet ou selecionem uma senha curta e fácil de adivinhar. (MITNICK, 2003, p.202).

Além dos programas de treinamento e conscientização sobre a segurança, Mitnick (2003) recomenda um programa ativo e bem divulgado de recompensas. Também sugere que as pessoas tenham ciência das consequências caso a política de segurança não seja seguidas por falta de cuidado ou resistência. Erros são frequentes, mas as violações constantes não devem ser toleradas.

> Você deve reconhecer os empregados que detectaram e evitaram uma tentativa de ataque de engenharia social ou que de alguma outra maneira contribuíram para o sucesso do programa de segurança das informações. A existência do programa de recompensas deve ser anunciada para os empregados em todas as sessões de conscientização sobre a segurança e as violações da segurança devem ser amplamente divulgadas em toda a organização. (MITNICK, 2003, p.205).

4.2. SUGESTÕES DE SEGURANÇA

Fontes (2006) disponibiliza algumas orientações objetivas para que o usuário se mantenha informado, permitindo a utilização de suas dicas nas políticas da empresa, desde que sejam devidamente creditadas.

Todos os impressos com informação confidencial devem ser armazenados em locais extremamente seguros de forma á evitar o acesso indevido. E caso de descarte, inutilize totalmente a informação, rasgando ou triturando o papel.

Diversas mensagens de correio eletrônico podem conter códigos maliciosos, portanto, ao receber um e-mail não esperado, não abra arquivos ou execute programas anexados, remova da caixa de entrada e jamais responsa, nem que seja para informar que não deseja mais receber esse tipo de mensagem.

Quando enviar uma mensagem de correio eletrônico (e-mail) deve-se garantir a confidencialidade da informação certificando de que além do destinatário, as demais pessoas copiadas devem receber essa mensagem. Também é necessário estar sempre alerta ao usar a opção *forward* (encaminhar), que tem o encadeamento histórico das mensagens. Outro cuidado primordial é ser sempre criterioso quanto a necessidade de envio de arquivos anexados.

Sempre que desejar enviar um e-mail, o ideal é certificar que o nome do destinatário está correto, para que não sejam enviadas informações para pessoas que não deveriam ter acesso.

Ainda sobre o uso do correio eletrônico, devem-se remover as mensagens que indicam recebimento de cartões virtuais mesmo sem abri-las. É uma forma muito eficaz de contaminar computadores.

Quando utilizar um computador portátil (notebook), sempre proteja o equipamento contra perda ou roubo. O usuário deve mantê-lo sob sua guarda quando estiver utilizando, e caso não for utiliza-lo mais, guarda-lo em armário fechado. Também é necessário tomar cuidado com a troca fraudulenta de pastas em locais públicos, como aeroportos e hotéis, tomar sempre cuidado para que não haja a troca por alguma pasta semelhante, com conteúdo alterado. Sempre deve transportar no porta-malas quando utilizar automóvel.

Ao terminar seu trabalho no computador, sendo ele portátil ou de mesa, o usuário deve desliga-lo, preservando pela vida útil do equipamento e evitando que invadam seu equipamento.

Prevenir é simples, eficaz e custa pouco! (FONTES, 2006, p.172)

Ao utilizar a internet, apenas acesse sites de organizações conhecidas, com credibilidade no mercado. Caso esse cuidado não seja tomado, aumenta o risco de contaminação da máquina com programas fraudulentos. Quando entrar em sites, o usuário deve evitar informar seu endereço virtual, disponibilizando-o apenas em situações profissionais específicas.

Caso o usuário esteja utilizando o computador e precise se ausentar, sempre deve deixar a máquina protegida, bloqueando o acesso.

Manter o sigilo das informações da organização quando estiver em um ambiente aberto. Atos como utilização de notebook, leitura de documentos, anotações em rascunho, descarte de papéis ou simplesmente conversas podem facilitar o vazamento de informação. Essas atividades devem ser realizadas com responsabilidade e profissionalismo.

Apagar ou destruir as informações registradas em quadro, papel de rascunho ou flip chart após as reuniões, dificultando o vazamento de informação.

Ainda sobre as reuniões, ao gerar informação por meio de comunicado, apresentação de slides, documentos ou outro tipo de material, deve ser identificado o nível de sigilo dessas informações, para que as demais pessoas presentes tenham o conhecimento se poderão compartilhá-las ou não.

Ao interagir com outras pessoas, buscar garantir que essa pessoa é quem ela diz ser, estar atento, pois a engenharia social é um tipo de fraude que visa enganar através de conversas aparentemente cordiais e verdadeiras.

Quando escolher uma senha, jamais utilizar uma sequência óbvia de caracteres. Sempre utilizar caracteres especiais para criar uma senha forte, fácil de ser lembrada pelo usuário e difícil de ser imaginada por outra pessoa.

Sempre limpe periodicamente o ambiente computacional, fazendo a remoção de arquivos de dados e mensagens de correio eletrônico que não são mais necessários. Caso o usuário tenha espaço em disco na rede, limpe também esse ambiente, removendo os arquivos desnecessários. No caso de haver arquivos que eventualmente podem ser consultados, faça uma cópia de segurança antes de excluí-lo do computador.

O usuário deve acessar apenas informações necessárias para o desempenho de sua atividade profissional no ambiente organizacional. Quando o mesmo mudar de área na organização, deve solicitar que corte os acessos que não serão mais necessários na sua nova função.

Jamais disponibilizar informação pessoal ou confidencial da organização para pessoas que não possam ser avaliadas ou reconhecidas como pessoas autorizadas para esse acesso.

Sempre que for apagar arquivos e mensagens de correio eletrônico, jamais se esquecer de removê-los da lixeira posteriormente, caso não precise mais deles, dessa forma, libera-se espaço no equipamento além de aumentar o nível de proteção da informação.

5. CONSIDERAÇÕES FINAIS

É impossível não se aprofundar no tema sem ficar aficionado pela capacidade que alguns hackers famosos tiveram para realizar proezas que, no ponto de vista de pessoas comuns, são impensáveis, mas fizeram com enorme facilidade e competência, muitas vezes até com recursos limitados.

Outro ponto que se destaca é a quantidade de classes de hackers existentes. Podemos até nos prevenir contra os *script kiddies*, mas quanto aos hackers mais habilidosos, dificilmente estaremos seguros.

O objetivo geral, que consistia em estudar o perfil do hacker, visando reduzir a interferência dos seres humanos no sistema de informação foi atingido em partes. Foi possível realizar um bom levantamento bibliográfico sobre a segurança da informação e sua importância. Além do histórico de hackers famosos e como eles são classificados de acordo com o seus ataques, dando ênfase a Kevin Mitnick, o mais famoso de todos.

No entanto, reduzir a interferência de seres humanos no sistema de informação se mostrou uma tarefa mais difícil do que se possa imaginar. Por mais que nos prevenimos, esses indivíduos estão muito a nossa frente em termos de conhecimento, tanto é que, como preventiva, muitas corporações acabam contratando-os para que os próprios encontrem as fraquezas no sistema antes dos demais. Conscientização de pessoas, essa é a forma mais eficaz para impedir um ataque, que nem sempre tem origem virtual. Muitas informações são passadas pelas próprias pessoas que trabalham na empresa, vítimas da própria ignorância, ingenuidade ou descuido.

O problema, que se tratava da vulnerabilidade na segurança da informação diante de um hacker, pode não ter sido resolvido, no entanto, com as dicas de Mitnick e de Simon no capítulo 4, pode-se desenvolver um treinamento eficaz de conscientização de funcionários e fortalecer a equipe, punindo aquele que não seguir as regras de segurança, e premiando quem a execute de forma eficaz. Eliminando essa barreira da ignorância humana, é possível fazer com que as medidas de segurança tecnológicas tornem-se mais eficazes também.

No fim, a questão de como reduzir a vulnerabilidade da segurança de um sistema de informação, acabou podendo ser respondida com as três hipóteses levantadas no início do trabalho. Promover reuniões e palestras para conscientização de prevenção sobre os riscos de vulnerabilidade, fiscalizar resultados, aderindo políticas de segurança rígidas, alterar códigos de acesso a principio pareciam ineficazes. Porém Mitnick deu uma nova visão sobre a empregabilidade desses informativos. Recompensar quem descobrir essas brechas e punir severamente quem descumprir as regras é uma forma eficaz de fazer com que a politica de segurança não fique apenas no papel.

A hipótese do ser humano ser facilmente corrompido diante de condições favoráveis ainda procede. É possível eliminar a ignorância do funcionário, mas não sua corruptibilidade, ainda que, se o fizer, o mesmo saberá das consequências do seu ato, então, essa fraqueza também pode ser reduzida com um programa de treinamento corretamente empregado.

No entanto, a ultima hipótese que se tratava de uma resposta totalmente conformada diante da fraqueza do fator humano, admitindo que não era possível fazer muito para suprir, que o foco deveria ser voltado para protocolos de segurança mais rígidos, acabou se tornando descartada. É verdade sim que o fator humano é um empecilho difícil de contornar, no entanto, é a fonte para que um protocolo de segurança rígido venha funcionar.

Conclui-se, então, que a hipótese que melhor responde a pergunta é a hipótese A, conscientização e treinamento de equipe é a peça-chave para a segurança da informação de qualquer empresa.

Como dicas para futuras pesquisas, sugere-se:

A ética hacker – assunto bem questionável e trabalhado sucintamente nesse mesmo trabalho. A reflexão transmitida no filme Takedown, onde Mitnick questiona o porquê ele está preso e Shimomura não, já que seu rival utilizou-se de artifícios hackers para promover sua captura, e o vírus que Kevin planejava espalhar na rede foi desenvolvido pelo próprio Shimomura, faz com que nós mesmos nos perguntemos até onde possamos utilizar habilidades hacker sem fugir da ética.

Estudo da mente do hacker – algumas reflexões e desabafos apresentados por Kevin Mitnick, Spyman e outros hackers, ficam impossíveis de não ser notadas semelhanças nas características dessas pessoas, sugerindo um estereotipo específico de personalidade.

Pesquisas mais aprofundada sobre os demais hackers citados nesse trabalho como Mark Abene, Kevin Poulsen e John Draper.

A punição para os crimes de informática, segundo a legislação brasileira e de outros países.

Políticas de segurança e questionários mais detalhados que possam ser aplicados em uma empresa para garantir o sucesso da segurança da informação contra esse tipo de ataque.

Pesquisa de campo sobre os ataques de hackers ou de pura engenharia social sofrida por empresas locais e como elas fizeram para contorna-los.

6. REFERÊNCIAS

AMARIZ, Luiz C. **Hackers e Crackers.** Disponível em:<http://www.infoescola.com/informatica/hackers-e-crackers/>. Acesso em: 27 out. 2013.

AUTOR ANÔNIMO. **Segurança Máxima.** Campus, 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação**: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

_____. **NBR ISO/IEC 17799**: tecnologia da informação: técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p. Disponível em: <http://xa.yimg.com/kq/groups/21758149/952693400/name/ABNT+NBR+ISO+IEC+17799+-+27001-2005++Tecnologia+da+Informa% C 3%A7%C3%A3o+-+T%C3%A9cnicas+de+Seguran%C3%A7a+-+C%C3%B3digo+ de+Pr%C3%A1tica+para+a+Gest%C3%A3o>. Acesso em: 01 set. 2013.

ASSUNÇÃO, Marco F. A. **Segredos do Hacker Ético.** 2ª ed. Florianopolis: Visual Books, 2008.

CAMBRIDGE DICTIONARY. Disponível em: < http://dictionary.cambridge.org/us/>. Acesso em: 27 de Outubro de 2013.

CARDOSO, Oscar V. **Asilo e refúgio políticos:** o caso Julian Assange. Disponível em: < http://jus.com.br/artigos/22498/asilo-e-refugio-politicos-o-caso-julian-assange>. Acesso em: 27 out. 2013.

CASTRO, Carla R. A. **Crimes de Informática e seus Aspectos Processuais.** 2ª ed. Rio de Janeiro: Lumen Juris, 2003.

COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança. **Cartilha de Segurança para Internet**. São Paulo, 2006. 95 p. Disponível em: Acesso em: 23 ago. 2010.

FILHO, Glenio L.M, **Hackers e Crackers na Internet:** as Duas Faces da Moeda. Disponível em: < http://www.insite.pro.br/2010/Janeiro/hackers_crackers_internet.pdf>. Acesso em: 27 out. 2013.

FONTES, Edson. **Praticando a Segurança da Informação.** Rio de Janeiro: Brasport, 2008.

FONTES, Edson. **Segurança da Informação – O Usuário faz a Diferença.** São Paulo: Saraiva, 2006.

FREIRE, A., Machado. **Como Blindar seu PC:** aprenda a transformar seu computador. Rio de Janeiro: Campus, 2006. 181 p.

GIL, Antonio Carlos***. Como elaborar projetos de pesquisa.*** São Paulo: Atlas, 1991.

HIMANEN, Pekka. **A ética dos hackers e o espírito da era da informação.** Rio de Janeiro: Campus, 2001.

MARCONI, Marina A.; LAKATOS, Eva M. **Fundamentos de Metodologia Científica.** São Paulo: Atlas, 2010.

MICHAELIS MODERNO DICIONÁRIO DA LINGUA PORTUGUESA. Disponível em <http://michaelis.uol.com.br/moderno/portugues/index.php> Acesso em: 25 ago 2013.

MITNICK, Kevin; SIMON, Willian L. **A Arte de Enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Brasil, 2003.

NAKAMURA, Emílio T.; GEUS, Paulo L. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Futura, 2003.

NETO, Pedro A. **Crimes de Informática.** 2009. 81f. Monografia (Conclusão do curso em Bacharel de Direito). Univali/Itajaí/SC, 2003.

NOGUEIRA, Sandro D. **Crimes de Informática.** São Paulo: BH Editora, 2008.

OLIVEIRA, G. **Segurança de Redes.** Vila Velha: ESAB, 2008. (Módulo de Segurança de Redes, Curso de Pós-graduação Lato-sensu em Redes de Computadores, Escola Superior Aberta do Brasil).

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006.

PIPKIN, Donald L. **Halting the hacker**: a practical guide to computer security. 2nd ed. UpperSaddle River: Pearson Education, 2003.

RAYMOND, Eric S. **The New Hackers Dictionary.** Disponível em: http://www.outpost9.com/reference/jargon/jargon_toc.html>. Acesso em: 27 out. 2013

ROSA, Fabrizio. **Crimes de Informática.** 2ª ed. Campinas: Bookseller, 2006.

RUFINO, Nelson M. O. **Segurança Nacional:** Técnicas e Ferramentas de Ataque e Defesa de Redes de Computadores. São Paulo: Novatec, 2002.

SILVA, Edna L., MENEZES, Estera M. **Metodologia da Pesquisa e Elaboração de Dissertação.** Florianópolis: 2001.

SILVA, Regina S. **Engenharia Social:** um Enfoque no Mecanismo de Segurança da Informação. Rio de Janeiro: 2004.

SPYMAN. **Manual Completo do Hacker.** 4ª ed. São Paulo: Book Express, 2001.

TEIXEIRA, Renata C. **Combatendo o Spam:** Aprenda como Evitar e Bloquear e-mails não-solicitados. São Paulo: Novatec, 2004.

ULBRICH, Henrique C.; VALLE, James D. **Universidade Hacker.** 5ª ed. São Paulo: Digerati Books, 2006.

WADLOW, Thomas. **Segurança de Redes.** Rio de Janeiro: Campus, 2000.

VEJA. **O Rei dos Hackers.** São Paulo: Março, 1998. Mensal.