HACKERS e suas características

Juliano Vieira da Rocha

Instituto de Ciências Exatas e Tecnológicas (ICET) – Universidade Feevale – Câmpus II - ERS-239, 2755 - CEP 93525-075 - Novo Hamburgo – RS – Brasil

Julianov.rocha@gmail.com

Abstract. *The term hacker has already owned several different definitions that evolved as the time went by and technology also developed. This article aims to identify briefly some of these meanings. Hackers: who they are and what they do. Their differences and species. This paper also discuss the hackers development process and the ongoing search for their skills and knowledge - since it is not easy at all to become a hacker. A list of the most ordinaries types of attacks will be specified. There will be a discussion under the facilities of being a hacker in Brazil in contrast on the laws evolution progress in the country and how the system is on a try to adapt itself for the incoming times.*

Resumo. *O termo hacker já possuiu várias definições diferentes que foram evoluindo conforme o tempo foi passando e a tecnologia se desenvolvendo. Este artigo visa identificar, resumidamente, alguns destes significados. Quem é e o que faz esse tipo de pessoa, os tipos existentes e as diferenças entre si. Será abordado o processo de evolução, a busca contínua por habilidades e conhecimentos, já que o indivíduo não se torna hacker do dia para a noite. Alguns tipos de ataques mais comuns serão especificados. Haverá uma discussão de o porque no Brasil não existirem tantos hackers presos, como estão evoluindo as leis deste País e como o sistema está se adequando aos novos tempos.*

Palavras-chave: Hackers, crakers, vulnerabilidades, engenharia social, crimes, leis

1. Introdução

No mundo digital assim como no mundo real, para manter um sistema seguro e estar preparado a ataques externos, é preciso conhecer o inimigo, como ele age, como se organiza, quais suas ações, suas técnicas, suas tecnologias para, dessa forma, adiantar-se, prever suas ações e preparar defesas e contramedidas. Deve-se refinar os processo e mantê-los em um ciclo, sempre melhorando e evoluindo, pois os *Hackers* estão lá fora, sempre na busca de um espaço, uma brecha, uma vítima vulnerável, para invadir uma rede e roubar suas informações.

Para tanto, este artigo será iniciado tratando da origem do termo, quais as características dessas pessoas, quais os conhecimentos adquiridos. Também serão descritos os tipos existentes, suas definições. Também descreverá as etapas percorridas por um indivíduo, desde um aspirante, percorrendo suas evolução, depois seu exílio, até se tornar um especialista de verdade. Serão descritos alguns de seus principais ataques,

suas principais técnicas para enganar sistemas e acessar informações e dados ocultos ou protegidos.

Serão identificadas e descritas as ações cometidas pelos *Hackers* bem como suas técnicas e os tipos de ataques mais comuns que utilizam para invasão e roubo de dados. Por fim serão apresentadas as leis criadas pelo governo para inibir e punir os crimes cometidos por estes indivíduos.

2. Origem do termo

O termo *Hacker* originalmente foi utilizado na denominação de carpinteiros que faziam móveis com machados (*hack* é a onomatopéia para essas ferramentas em inglês). Já nos anos de 1940 e 1950, o termo foi utilizado para descrever radioamadores e *hobbystas* de mecânica ou eletrônica. Somente na década de 60 o termo passou a ser aplicado na informática, conforme descrito pelo jornalista americano Steven Levy(1984) no livro *Hacker, heroes of the computer revolution*. O autor descreve que nesta época o termo *hack* passou a ser utilizado por alunos do *Massachussetts Institute of Technology* (MIT) para designar brincadeiras e trotes na instituição. Mais tarde foi incorporado como jargão de uma agremiação do MIT: o *Tech Model Railroad Club*(TMRC). Os participantes deste grupo tinham como principal atividade produzir miniaturas motorizadas de trens e estradas de ferro. Desde então o termo *Hack* passou a ser utilizado como designação de projetos que exigiam muito tempo e concentração do indivíduo, porém sem nenhum retorno financeiro ou acadêmico para o mesmo, apenas a satisfação pessoal e prazer de cumprir o projeto. Para ter esta qualificação era necessário ser inovador, ter estilo e habilidades técnicas fora dos padrões. (MORAIS, 2005).

Não demorou muito para estes jovens aficionados e talentosos conhecerem os computadores. Em 1959 o MIT passou a oferecer um curso de programação de computadores, ministrados pelo matemático John McCarthy, criador do termo Inteligência Artificial (IA). Foi a partir de então que o termo passou a ser usado como sendo a designação de especialistas em computadores. Porém, nesta época, ainda era comumente utilizado para especialistas de qualquer área, como astronomia ou até mecânica de automóveis. (ULBRICH; DELLA VALE, 2004).

3. Hacker e seus significados

Basicamente o termo *Hacker* possui dois significados distintos, um bom, no qual é utilizado para descrever uma pessoa que possui um grande conhecimento na área de informática, e outro mal, referindo-se a invasores e vândalos digitais. Ambos especializam-se no entendimento do funcionamento, ao menor detalhe de um *software* ou dispositivo (*hardware*), analisando estes sistemas com técnicas de engenharia reversa, identificando suas vulnerabilidades. Porém o indivíduo mau utiliza-se deste conhecimento para e explorá-las e utilizá-las, para desta forma conseguir alterar o funcionamento dos mesmos, fazendo com que realizem ações que nem os projetistas originais conceberam, seja apenas para desbloqueá-los de suas “travas” de fábrica ou para invadir redes e sistemas. (ULBRICH; DELLA VALE, 2004).

Por conta de vários escândalos e descobertas de ataques altamente prejudiciais, a imprensa e a população em geral acostumaram-se a utilizar o termo no sentido negativo.

Porém algumas fontes como o *Jargon File*, editado por Eric Raymond, defendem que o real significado do termo seria o primeiro e que os criminosos devem ser identificados como *crackers*, termo criado pela própria comunidade para sua distinção. Raymond (2000) enfatiza sempre que refere-se as diferenças de *hackers* e *crackers*. "A diferença básica é esta: *hackers* constroem coisas, *crackers* as destroem." Em algumas das versões do *Jargon File* publicadas na internet, pode ser identificados oito significados para o termo. (The Jargon File, 2000).

> *"1. Aquele que gosta de explorar os detalhes de sistemas programáveis e procura ampliar suas capacidades, em oposição à maioria dos usuários, que prefere aprender apenas o mínimo necessário. 2. Aquele que programa (computadores) de modo entusiástico (ou mesmo obsessivo) ou que prefere dedicar-se à programação em vez de apenas teorizar sobre programação. 3. Aquele capaz de apreciar o valor de um hack. 4. Uma pessoa que é boa em programar com rapidez. 5. Especialista em um determinado programa, ou que frequentemente trabalha na modificação de um determinado programa ou usando-o; como em 'Unix hacker'. (As definições 1 e 5 são correlatas, e as pessoas que se encaixam nelas congregam-se.) 6. Um especialista ou entusiasta de qualquer tipo. É possível ser hacker em astronomia, por exemplo. 7. Alguém que aprecia o desafio intelectual de ultrapassar ou contornar limitações. 8. [desaprovado] Um intrometido mal-intencionado que tenta obter informações sensíveis bisbilhotando. O termo correto para este sentido é cracker." (The Jargon File, 2000).*

Ainda falando dos maus exemplos de *Hackers*, como técnica de engenharia reversa utilizada por eles, foi identificado o desbloqueio de dispositivos IOS(Apple) chamado de *Jailbreak*, conforme dito pela matéria do TecMundo (2009). Este procedimento é o equivalente a "rootar" aparelhos com sistema operacional *android*, ou tornar-se o administrador total de aparelhos *Windows*, no qual o aparelho perde (além da garantia é claro), o bloqueio estipulado pelo fabricante, deixando o mesmo vulnerável e exposto a qualquer tipo de alteração ou ataque em seu SO (sistema operacional), como instalação de *softwares* de origem duvidosa e alguns outros tipos de configurações e personalizações.

4. Um exemplo de hacker

No mundo inteiro existem milhares, talvez milhões de *hackers* em ação neste momento, porém um exemplo de um ex-hacker é Kevin Mitnick. Este é o *Hacker* mais famoso do mundo, com fama e feitos mundialmente conhecidos, considerado um herói e exemplo por alguns, porém criminoso pelo governo americano. (MITNICK; KEVIN, 2005)

Atualmente Kevin mudou de lado, se tornou, sem dúvida alguma, uma das maiores autoridades no assunto de invasão, roubo de dados, segurança da informação e engenharia social, sendo nesta última considerado um precursor neste tipo de ataque. Começou cedo na área de TI e logo percebeu seu talento. Ainda aos 12 anos, descobriu como adulterar cartões perfurados de controle de baldeações de ônibus em Los Angeles.

Dessa forma, andava o dia todo, a qualquer lugar da cidade, sem pagar por isso. (MITNICK; KEVIN, 2005)

Em 1995, em razão de seu ego e em busca de mais um desafio, Mitnick invadiu o computador pessoal do especialista em segurança da informação do MIT, o professor Tsutomu Shimomura, que recebeu o ataque como ofensa pessoal e uma afronta a seus conhecimentos. Este foi um grande erro de Kevin, pois Shimomura passou a dedicar-se a localizar aquele hacker petulante, passou a persegui-lo incessantemente, preparando armadilhas, e depois de um tempo, acabou levando Kevin a cometer seu primeiro erro em anos, no qual foi localizado e preso. A sentença recebida por Kevin foi de cinco anos em regime fechado, após isso, mais três em liberdade condicional, porém, nesse período, foi impedido de se aproximar de qualquer dispositivo eletrônico.

Após cumprir sua pena, o *Cracker* largou sua vida do submundo a passou a dedicar-se a consultorias de segurança, dando palestras pelo mundo todo, ensinando empresas e instituições as melhores práticas de defesa contra ataques *hacker*. Inclusive no Brasil, em 2006 (TECMUNDO; 2009) e na *Campus Party* 2010 conforme divulgado pelo G1 no mesmo ano.

> *"Alguns hackers destroem os arquivos ou unidades de disco inteiras das pessoas. Eles são chamados de Crackers ou vândalos. Alguns hackers novatos não se preocupam em aprender a tecnologia; eles apenas querem baixar as ferramentas dos hackers para entrar nos sistemas de computadores. Esses são chamados de script kiddies. Os hackers mais experientes, com habilidades em programação, desenvolvem programas para hackers e os postam na Web e nos sistemas de bulletin board. Em seguida, temos os indivíduos que não têm nenhum interesse em tecnologia, mas que usam o computador apenas como uma ferramenta que os ajuda a roubar dinheiro, bens ou serviços."* (MITNICK;KEVIN, 2005)

5. Os tipos de *Hackers*

Existem *Hackers* do bem, também chamados de *White Hats*(chapéu branco), *Gray hats*, os que ainda estão em cima do muro. Estes fazem pequenos ataques DOS (*Deny of Service*) para derrubar alguns sites, ou escrevem algum software para derrubar a licença de alguns programas. E por fim, os *Black Hats*, que também podem ser chamados de *Crackers*, os chamados de vândalos digitais, estes são verdadeiramente criminosos, sem escrúpulos, que se utilizam de seu conhecimentos apenas para obter lucros sobre qualquer outra pessoa. (SKOUDIS; HALL, 2005)

Uma das coisas que realmente difere um tipo de *Hacker* do outro é a motivação, assim como existem muitas pessoas diferentes no mundo, suas motivações também são muito variadas, incluindo curiosidade, necessidade profissional, vaidade, espírito competitivo, patriotismo, ativismo ou mesmo crime. Como exemplo de atividade profissional existe o grupo chamado *Ethical* Hacker, que faz parte dos *White hats*. Eles são colaboradores diretos da empresa ou de empresas terceiras contratadas para consultorias e auditorias, que trabalham em *Pentest* (Teste de penetração de sistemas autorizados). Esses são muito importantes para testar possíveis vulnerabilidades de

redes e sistemas, antes de pessoas mal intencionadas o fazer. Este mercado vem crescendo bastante no mundo, devido ao aumento na preocupação das empresas de manter seus dados em segurança. (AMARAL; SÉRGIO, 2012)

Os *hackers* do tipo curioso exploram invasões apenas pelo desafio, pela adrenalina, geralmente são iniciantes que após invadir um sistema com sucesso, as vezes nem sabem o que fazer lá dento e fazem apenas alguma alteração insignificante somente para o administrador descobrir o acesso e passa para o próximo desafio. Estes geralmente deixam rastros, do tipo que o dono chega em casa e vê a porta aberta. São considerados ruins para Hackers de espírito mais competitivo de categoria mais elevada, pois a cada ataque sem planejamento efetuado, é uma chance a menos de sucesso, pois estes desajeitados fazem com que o sistema e os administradores estejam cada vez mais preparados e seguros. (ULBRICH, DELLA VALE; 2004)

O tipo vaidoso é o que faz suas invasões e as divulga, se promove, quer ser conhecido na comunidade. Após seus ataques ele lança o desafio a outros para que façam melhor, e claro, sem serem descobertos, pois um *Hacker* de verdade não é localizado ou identificado. (ULBRICH, DELLA VALE; 2004).

Os tipos patriota e ativista são pragmáticos, diferindo-se apenas em relação ao que protegem. O primeiro, como seu nome diz, defende apenas os ideais de seu país, já o segundo defende as pessoas e a população em geral. Ambos acreditam que devem desobedecer algumas leis em nome de um ideal ou um bem maior, trabalham atacando governos considerados inimigos ou perigosos, buscam e roubam informações divulgando-as para desmoralizá-los. Estes também são os responsáveis por identificar e exibir informações de criminosos, como traficantes, terroristas, pedófilos e assassinos. (ULBRICH; DELLA VALE, 2004)

E por último mas não menos importantes, os verdadeiros responsáveis pela mancha no termo *Hacker*, os criminosos digitais, que pouco se interessam por conhecimento ou tecnologia. Assim como um criminoso comum utiliza um maçarico para um roubo a caixa eletrônico, estes buscam apenas ferramentas para obtenção de ganhos e lucros em detrimento de outras pessoas, seja por fraude, desvio de dinheiro, roubo e venda de dados ou informações sigilosos, clonagem de cartões de créditos, etc. Este tipo se difere de criminosos comuns apenas pelo não uso de violência porém causando os mesmos danos ou piores. (MITNICK;KEVIN, 2006)

6. Estágios na vida de um hacker

Segundo as pesquisas de ULBRICH; DELLA VALE (2002) o *hacker* não recebe este título por livre escolha ou por vontade própria, existe um começo e uma escalada para se tornar um, quase um plano de carreira, onde o que conta é a experiência e conhecimentos adquiridos. A seguir serão descritas algumas dessas fases :

- *Newbie* (núbi) referindo-se aos iniciantes, os novatos na área, também conhecidos como *Script Kiddies*. Geralmente adolescentes aficionados por tecnologia, ainda sem um ideal concreto, querendo apenas fazer parte de alguma tribo ou simplesmente aprender algo novo;

- *Luser* - este é utilizado como termo pejorativo, vindo da união das palavras em inglês *looser* (perdedor) e *user* (usuário). Este indivíduo, ao contrário do *Newbie*, não quer aprender nada, adquire o mínimo possível de conhecimento, só para achar alguma ferramenta útil, algum programa que desfigure um *site*, ou ainda, algum *Trojan* que roube a senha do wifi do vizinho.

- *Lamer* - este é o usuário com um pouco mais de experiência, com o tempo um Newbie ou Luser acabam aprendendo a utilizar um pouco melhor alguns programas, embora não saiba como o mesmo funcione exatamente. Ele ainda não possui muita experiência e por isso não sabe criar suas próprias ferramentas, então utiliza-se de *scripts* e *softwares* prontos localizados na web. A palavra é derivada do inglês *lame*, que significa manco ou aleijado.

- *Wannabe*(ou *wannabee*) - esta palavra foi utilizada nos anos 80 para designar os fãs da cantora Madona que se vestiam como ela e a imitavam, desta forma também na informática os *wannabes* tentam se tornar um *hacker* . Ele pode ser utilizado para descrever tanto uma pessoa que já leu bastante e está prestes a entrar no último estágio antes de ser um *hacker*, no chamado *larval stage*, ou para os que querem entrar nesse mundo, mas não fazem ideia do que estão fazendo ali.

- *Larval Stage* - também chamado de *Spawn*, este é literalmente um estágio larval, no qual o indivíduo se isola por um tempo para trabalhar e desenvolver integralmente na produção de códigos, pois este é uma habilidade indispensável para um *hacker*. Este estágio pode variar de seis meses a dois anos, no qual o candidato "renasce" como um programador.

- *Hacker* - nesta fase o indivíduo se torna realmente um especialista em diversas técnicas na arte de invasão, adquire um profundo conhecimento em, pelo menos um tipo de sistema operacional. E por terem vencido o estágio larval, se tornaram excelentes programadores e administradores de sistemas.7. References

7. Tipos de ataques

Existem inúmeros tipos de ataques efetuados contra redes e sistemas, serão listados alguns na sequência:

Botnet - são vírus criados para infectar computadores de forma aos donos nem perceberem, fazendo com que comuniquem-se entre si, desta forma criando uma rede de "robôs" controlados remotamente. Quando necessário, o controlador executa um certo comando, o qual faz com que inúmeras máquinas façam o que ele quiser, seja acessar um mesmo *site* (DDos), seja enviar *Spams*, ou até mesmo em casos sofisticados, o controlador faz os "zumbis" processarem pedaços de algoritmos de ataques massivos a sistemas maiores, como Bancos ou governos. (SKOUDIS; HALL, 2005)

DDoS/Dos(*Distributed Deny Of Service attack*) - também conhecido como ataque de negação de serviço, este tipo de ataque visa derrubar algum tipos de sistema *online* ou *web sites*. Ele consiste em efetuar um grande número de acessos simultâneos, sendo o DOS partindo de um único ponto, DDos partindo de várias máquinas, sendo uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus

utilizadores. Este é o mais comum e é responsável por criar um mercado paralelo de *Bot nets* onde ataques massivos podem ser encomendados e direcionados mediante a um pagamento pré-estabelecido. (SKOUDIS; HALL, 2005)

BruteForce - este é um sistema mais simples que consiste basicamente em um *script web* rodado e testando vários caracteres seguidos que podem ser utilizados como senhas padrões de sistemas ou sites publicados na *web*. (SKOUDIS; HALL, 2005)

Phising - este é um dos mais utilizados atualmente e com grande retorno para o *hacker*. Consiste em *spams* enviados aleatoriamente, no qual o *email* tenta imitar da melhor forma o *email* de um banco ou operadora de cartão de crédito, que solicita ao usuário que o mesmo faça a "atualização" de seus dados cadastrais, como nome, endereço, CPF e ainda casos que solicita o número completo de cartão de crédito e até o preenchimento do cartão de *token* dado pelo banco. (SKOUDIS; HALL, 2005)

Engenharia social - além dos ataques técnicos descritos, existem também várias outras formas de adquirir informações, pois o conhecimento e ação *hacker* não restringem-se apenas ao uso da tecnologia ou de computadores para os ataques, eles utilizam-se também de várias outras facetas, como, por exemplo, a engenharia social, neurolinguística, disfarces para visitas ao local físico, conhecer pessoas, buscar informações nas redes sociais, tentar interações com funcionários descontentes, ex-funcionários raivosos. Por exemplo, um *hacker* pode fazer-se passar por funcionário terceiro de alguma empresa de limpeza, pode participar do dia a dia da empresa, escutar conversas sigilosas de corredor, recolher os lixos, pois algumas pessoas costumam anotar as senhas até decorá-las e após não dar o descarte correto para as mesmas, como um triturador de papel com acesso restrito e recolhido por uma empresa especializada para incineração. Parece muito, mas sabe-se o que alguém poderia fazer com umas lista de clientes impressa por engano, ou uma lista de cargos e salários do setor de recuros humanos. (MITNICK; KEVIN, 2006)

7. Leis para Crimes digitais

No Brasil, crimes digitais ainda não são tão comuns para o judiciário, desta forma muitos crimes acabam não sendo julgados da forma correta.

Porém, em maio de 2012 ocorreu um episódio que foi considerado o motivador para a contemplação de crimes digitais pelas leis nacionais. Nesta data ocorreu a divulgação não autorizada de fotos íntimas da atriz Carolina Dieckman na internet. Conforme noticiado na época, o fato ocorreu após a mesma deixar seu computador pessoal para assistência em um loja especializada, onde um indivíduo violou sua conta de *email*, obtendo acesso as imagens e passando a chantagear a atriz , ameaçando divulgar as imagens. (G1, 2012)

Após o início do julgamento, ocorreu a alteração da Lei nº 12.737, de 30 de novembro de 2012, publicada no Diário Oficial da União em 03 de dezembro de 2012, e em vigor 120 (cento e vinte) dias após a sua publicação oficial. Foi apelidada de Lei Carolina Dieckman, na qual "dispõe sobre a tipificação criminal de delitos informáticos;

altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências". (SIENA, 2013)

No artigo 2º, o responsável pela criação da norma reguladora criou a seguinte norma penal incriminadora, que passa a integrar a Seção IV ("Dos crimes contra a inviolabilidade dos segredos"), do Capítulo VI ("Dos crimes contra a liberdade individual"), do Título I ("Dos crimes contra a pessoa"), do Código Penal: (Lei nº 12.737)

"Invasão de dispositivo informático

Art. 154-A. *Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:*

Pena *- detenção, de 3 (três) meses a 1 (um) ano, e multa."*

Desta forma pela primeira vez a lei previa a detenção de indivíduos que cometerem atos de roubo de dados ou informações digitais, que neste caso eram imagens.(SIENA, 2013)

Outro avanço significativo, juridicamente falando, foi a LEI No 12.965 de 23 de abril de 2014, o chamado Marco Civil da Internet, criado pelo Legislativo para dar um norte aos magistrados do país que julgam diariamente crimes e contravenções do mundo digital. Dentre outras definições, o Marco Civil traz :

"CAPÍTULO II - DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7o.O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;"

O marco civil trata dos direitos e deveres das operadoras e dos usuários. Ela possui três pilares principais: Neutralidade da rede, a proteção da privacidade e a proteção da liberdade de expressão. Ela obriga que as operadoras garantam que os

pacotes de dados sejam tratados de forma isonômica, ou seja, sem que haja privilégios a qualquer tipo de conexão, conteúdo, origem e destino, serviço, terminal ou aplicação, por razão de pagamentos ou favorecimento de qualquer tipo. Garante também que o usuário possa acessar qualquer tipo de informação que queira.

No CAPUT da lei, na cabeça do documento, contém o conceito de neutralidade e no parágrafo 1º contém as duas únicas exceções admitidas pela lei, conforme segue:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

Ou seja, somente pode ser priorizado conexões de acordo com o protocolo e em serviços que mantenham a boa qualidade da rede, como por exemplo, priorizar uma comunicação de transmissão de vídeo ao vivo (streaming) e comunicação de voz sobre IP (VOIP) em detrimento de uma transmissão de email a qual não tem prioridade de transmissão de pacote sem tempo real.

E em segundo lugar, deve ser priorizado a comunicação a prestação de serviços de emergência, como por exemplo, uma cirurgia médica acompanhada remotamente sobre uma comunicação de email.

Outro ponto importante que a Lei trata é o registro de logs de usuários para apuração e combate a crimes na internet. Ficam responsabilizadas por armazenar informações pelo prazo de até cinco anos ou enquanto o consumidor manter contrato com a operadora, termo que gerou polêmica, pois vem em contrário ao termo de privacidade dos usuários. Elas também ficam responsáveis pela rastreabilidade e identificação dos acessos, caso solicitado judicialmente.

7. Conclusão

Para profissionais que trabalham diretamente com segurança da informação percebe-se que é muito importante o estudo sobre estes indivíduos, como agem, como operam estes atacantes da web, sejam eles sistemas ou pessoas, *hackers* testando seu conhecimento, *crackers* tentando roubar informações, *Scripties kiddies* iniciando sua escalada. Todos são ameaças em potencial, que estão dia a dia testando as defesas, em busca de vulnerabilidades, de falhas de controle.

No Brasil, o governo ainda não possui a tecnologia, as boas práticas e processos necessários, ou se quer leis atualizadas e prontas a atender e compreender estes tipos de crimes, para defender as corporações, instituições, entidades e até mesmo a sociedade como um todo.

Cabe aos profissionais de segurança se tornar *White hats*, *hackers* do bem, para zelar pelos sistemas, identificando suas fragilidades, suas vulnerabilidades antes dos demais. Deve-se sempre buscar, assim como eles, maiores conhecimentos, maiores informações, mais ferramentas, buscar o aprendizado de novas técnicas, para, desta forma, tentar manter-se um passo a frente, pois, neste processo todo, basta uma única

falha, um elo mais fraco, um processo mal desenhado para que uma invasão ocorra, colocando em risco o negócio ou até mesmo a empresa como um todo, podendo causar prejuízos incalculáveis.

Referências Bibliográficas

AMARAL, Sérgio Ferreira e PRETTO, Nelson de Luca". (2012) Ética, Hacker e educação Disponível em: < *http://www.lantec.fe.unicamp.br/lantec/publicacoes/lv_hacker.pdf* >. Acesso em: Abril de 2016.

ALMEIDA, Marcel da Silva. (2004) "Um Estudo de Crimes Digitais cometidos na Internet" Disponível em: < *http://www.sirc.unifra.br/artigos2004/Artigo25.pdf*>. Acesso em: Abril de 2016.

FOINA, Ariel."Hacking e as Organizações Criminosas", Disponível em: < http://www.geocities.ws/agfoina/rsd.html> . Acesso em: Abril de 2016.

Quem é Kevin Mitnick? (2009) Disponível em: < *http://www.tecmundo.com.br/historia/1842-quem-e-kevin-mitnick-.htm*>. Acesso em: Abril de 2016.

Lei nº 12.737, de 30 de novembro de 2012. (2012) Disponível em: < *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm*>. Acesso em: Abril de 2016.

LEVY, Steven. (1994) "*HACKERS, Heroes of the Computer Revolution"* - Delta Book

Marco Civil. (2014) Disponível em: < *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm*> Acesso em: Abril de 2016.

MITNICK, Kevin D.; SIMON, William L. (2005) " A arte de enganar" Pearson Education do Brasil. - São Paulo : Pearson Prentice Hall.

MITNICK, Kevin D.; SIMON, William L. (2006) "A arte de invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos", Pearson Education do Brasil , traduzido por César Pinto e Hoenir Ribeiro da Silva. - São Paulo : Pearson Prentice Hall.

MORAIS, Rodrigo de Oliveira. (2005) "Informacionalismo e Ética Hacker: Resistências digitais na Sociedade em Rede". Disponível em : < http://www.dominiopublico.gov.br/download/texto/cp022926.pdf>. Acesso em: Abril de 2016.

RAYMOND, Eric Steven. (1998) "A Catedral e o Bazar ", Disponível em : < http://duzeru.org/wp-content/uploads/2015/10/a-catedral-e-o-bazar-eric-raymond.pdf >. Acesso em: Abril de 2016.

RAYMOND, Eric Steven. (2000) “The Magic Cauldron”, Disponível em : < https://public.kitware.com/OpenSourceSoftwarePractice/images/5/5a/Magic-cauldron.pdf >. Acesso em: Abril de 2016.

RAYMOND, Eric Steven. (2000) “The Jargon File or The on-line hacker Jargon File”.Disponível em: <http://www.tf.hut.fi/cgi-bin/jargon>. Acesso em: Abril de 2016.

SAMANI, Raj, MCFARLAND. (2014) Charles.” *Hacking the Human Operating System”*. Disponível em : <http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf>. Acesso em: Março de 2016.

SIENA, David Pimentel Barbosa. (2013) Lei Carolina Dieckmann e a definição de “crimes virtuais”Disponível em: < https://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais>. Acesso em: Março de 2016.

SKOUDIS, Ed; LISTON, Tom; HALL, Prenticel. (2005) “Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses*”*

ULBRICH, Henrique Cesar; DELLA VALLE, James. (2004) “ Universidade Hacker: Desvendando todos os segredos do submundo dos hackers”. 4ª Edição – - São Paulo: Digerati