Hackers e Crackers [1]

Andréia Patrícia da Silva, Cínthia Soares, Isabelle Ulysséa [2]

Resumo

Esse artigo tem por objetivo esclarecer sobre o verdadeiro conceito de *hacker*, quais são os tipos mais conhecidos, assim como apresentar alguns dos fundamentos jurídicos que estão relacionados às invasões digitais. Discorre, ainda, sobre a técnica conhecida como "engenharia social" - muito utilizada e que possui fins não-éticos – como também descreve os alvos preferidos dos chamados "piratas digitais". A importância do profissional de segurança da informação também é abordada, e estão dispostas dicas de como se obter um sistema mais seguro nas empresas, auxiliando, assim, a tomada de decisão do gestor da informação.

Palavras-chave

Hackers; *crackers*; Segurança da Informação; Invasão Digital; Engenharia Social; Piratas Digitais.

Summary

This article is intended to explain the real concept of the word hacker, what are the most known kinds of hackers, as well as to introduce some of the legal basis that are related to digital invasion. It also describes the technique known as "Social Engineering" – used for non-ethic purposes – and it also describer de main targets of the so-called "digital pirates". The importance of the information security professional is approached, and tips are displayed to show how to get a more secure system in the corporation, collaborating to the information manager's decision.

Keywords

Hackers; Crackers; Information Security; Digital Invasion; Social Engineering; Digital Pirates.

1 Trabalho desenvolvido na Pós-Graduação da UCB

2 Alunas do Curso de MBA em Gestão de Sistema de Informação da UCB

1. Introdução

Não é de hoje que muitos dos chamados “piratas digitais” fazem com que as pessoas preocupem-se e tenham um medo maior de utilizar o computador. Esse medo virou pânico em pleno século XXI. Devido às maravilhas do mundo moderno, dados navegam por linhas telefônicas, cabos e satélites, diminuindo distâncias entre povos e iniciando a nova era digital. Ladrões assaltam bancos de outros países, desviando o dinheiro para a Suíça. A espionagem industrial é um dos problemas agravados. Nesse artigo, vamos desmistificar esses piratas, quais são os tipos mais conhecidos de *hackers*, quem são os mais conhecidos.

Também será apresentado o que se tem hoje de legislação relacionada a crimes digitais (os fundamentos jurídicos), o que significa Engenharia Social, quais as formas mais comuns de ataques, quais são os alvos preferidos dos *hackers* e os motivos que levam às suas ações.

Ao final do trabalho, são apresentadas algumas informações sobre como se proteger desses piratas digitais. Dessa forma o profissional responsável pela segurança da informação de qualquer empresa poderá defender-se das ameaças do mundo digital.

2. Características de um Sistema Inseguro

A segurança de sistemas existe por um conjunto de fatores. Está enganado quem pensa que somente por utilizar uma plataforma Unix ao invés de Windows está seguro, ou que apenas colocar um antivírus e um *firewall* na sua empresa já é o bastante. A proporção do problema é bem maior. Geralmente os sistemas mais vulneráveis da rede possuem dois pontos em comum:

2.1 - Administrador

Esse é o ponto-chave para qualquer sistema de computador. O administrador é responsável por fazer com que tudo corra de forma perfeita. Ele verifica os dados, administra os usuários, controla servidores e verifica logs todos os dias. Porém a grande maioria dos administradores atualmente não se preocupa com a segurança como deveriam. Isso implica que mais cedo ou mais tarde terá problemas com o sistema.

Mesmo que uma rede utilize um sistema operacional que possua muitas falhas, os bons administradores todo dia estarão à procura de falhas descobertas e para corrigi-las.

2.2 - Sistemas Operacionais

Não há realmente um sistema que seja melhor que o outro. Existem vantagens e desvantagens de cada um. A intenção do sistema também importa. Não é a solução indicada utilizar sistemas com suporte de rede simplificados. O sistema também vai depender do tipo de rede. Se houver um servidor Web ou algum tipo de acesso externo, então será mais prudente utilizar o **Linux** ou o **Windows NT**.

3. A segurança ao longo da história

Anos atrás, os operadores de um computador ENIAC se depararam com um inseto que havia ficado preso dentro da máquina e estava atrapalhando o funcionamento da mesma. Desse fato surgiu o termo *bug* (inseto) que virou sinônimo de falha. Hoje quando se descobre um erro em algum programa, se diz: “*novo bug descoberto*”. De lá

pra cá, as coisas evoluíram muito, mas os *bug*s continuam a existir. Muitos deles são frutos da história do próprio programa ou sistema.

A Internet também tem seus problemas ligados à história de sua origem. Desde que se chamava Arpanet e foi criada pelo exército americano para resistir à Guerra Fria, a rede evoluiu muito e foram criados novos serviços. Milhões de computadores juntaram-se a ela e seus recursos são cada vez mais sofisticados. Mas alguns problemas bem antigos ainda prejudicam. Uma falha na implementação do TCP/IP (conjunto de protocolos no qual a Internet se baseia), por exemplo, facilita o ataque de um *hacker* mal-intencionado.

4. Invasores digitais

Todos os dias ouvimos notícias sobre piratas digitais na televisão e na Internet. Para entender melhor como se organiza a hierarquia virtual da Internet, veremos seus principais integrantes:

4.1 - *Hackers (white-hats)*

São os usuários que se envolveram tanto com os computadores que conseguem superar até os limites das máquinas e dos programas. É um curioso por natureza, uma pessoa que tem em aprender e se desenvolver um *hobby*, assim como ajudar os "menos prevalecidos". Um bom exemplo para ilustrar um *hacker* foi quando o *cracker* Kevin Mitnick invadiu o computador do analista de sistemas Shimomura. Mitnick destruiu dados e roubou informações vitais. Shimomura é chamado de *hacker*, pois usa sua inteligência de forma ética, e possui muito mais conhecimentos que seu inimigo digital. Infelizmente a imprensa confundiu os termos e toda notícia referente a baderneiros digitais se refere a *hacker*. Os *hacker*s em geral partem do princípio de que todo sistema de segurança tem uma falha, e a função deles é encontrar essa porta.

4.2 - *Crackers (black-hats)*

Do verbo em inglês "*to crack*", significando, aqui, quebrar códigos de segurança. Com um alto grau de conhecimento e nenhuma ética, os *cracker*s invadem sistemas e podem apenas deixar a sua "marca" ou destruí-los completamente. Geralmente são *hacker*s que querem se vingar de algum operador, adolescentes que querem ser aceitos por grupos de *cracker*s (ou *script-kiddies*) e saem apagando tudo o que vêem, ou são *experts* de programação que são pagos por empresas para fazerem espionagem industrial. *Hacker*s e *cracker*s costumam entrar em conflito. Guerras entre grupos é comum, e isso pode ser visto em muitos fóruns de discussão e em grandes empresas, as quais contratam *hacker*s para proteger seus sistemas.

4.3 - *Phreakers*

Os *phreaker*s são os maníacos por telefonia. Utilizam programas e equipamentos que fazem com que possam utilizar telefones gratuitamente. O primeiro *phreaker* foi o *Capitão Crunch*, que descobriu que um pequeno apito encontrado em pacotes de salgadinhos possui a mesma freqüência dos orelhões da AT&T, fazendo com que discassem de graça. Outra técnica muito usada - principalmente no Brasil - é a de utilizar um diodo e um resistor em telefones públicos. Técnicas como essas são utilizadas no mundo inteiro. O *phreaker* é uma categoria à parte, podem ser *hacker*s, *cracker*s ou nenhum dos dois.

4.4 - Funcionários

Hoje 60% das invasões ocorrem dentro da própria empresa, por funcionários insatisfeitos ou ex-funcionários que querem vingança. Utilizam-se do conhecimento adquirido e arrasam dados do sistema. Copiam informações do seu interesse ou instalam jogos em rede que podem comprometer a segurança do sistema, pois normalmente eles não se preocupam em utilizar o antivírus. Utilizam *trojans*, *scanners* e *sniffers* para capturar o que lhes interessa. A utilização de um *firewall* é ineficaz contra eles. Afinal, do que adianta a Grande Muralha da China se algum soldado é o traidor?

4.5 - *Lammers*

Este é o principiante que acha que sabe tudo porque buscou na Internet alguns programas de invasão e segurança e com ele consegue fazer algo que os leigos ficam espantados, mas de fato ele não sabe nada do que está fazendo.

Os *lammers* são aquelas pessoas que entram nos *chats* anunciando "vou te invadir, sou o melhor", mas acabam desistindo porque não conseguem nem mesmo descompactar um arquivo do tipo ZIP.

4.6 - *Wannabes* ou *script-kiddies*

Estes sabem um pouco mais que um *lammer*, já não são novatos, porém têm muito o que aprender. Eles dominam alguns programas de invasão e começam a entender o funcionamento da coisa.

Os *wannabes* ou *script-kiddies* são aqueles que acham que sabem, dizem para todos que sabem, se anunciam, ou divulgam abertamente suas "façanhas". Usam em 99% dos casos *scripts* ou *exploits* conhecidos, já divulgados, denominados "receitas de bolo". Não têm um alvo certo, procuram invadir tudo que vêem na frente. Aproveitam-se das ferramentas encontradas na Internet.

A maioria não possui escrúpulo algum, portanto, tomar medidas de cautela é aconselhável. Os *wannabes* geralmente atacam sem uma razão ou objetivo, apenas para testar ou treinar suas descobertas, o que nos torna - usuários da Internet – alvos potenciais.

4.7 - *Carder*

É um especialista em fraudes com cartões de crédito. Considerado um *expert*, o *carder* conhece os meios para conseguir listas de cartões válidos nos sites de compra. Por exemplo, consegue gerar números falsos que passam pela verificação e até mesmo roubar e clonar cartões verdadeiros.

4.8 - *War Drivers*

Um tipo recente de *cracker*. Sabe aproveitar as inúmeras vulnerabilidades das atuais redes sem fio - as chamadas *wireless* - e conectar-se a elas. Os *war drivers* europeus foram mais longe e criaram o *war chalking*, que consiste em desenhar com giz símbolos no chão que indicam a melhor posição de conexão para outros *war drivers*.

5. Os hackers mais famosos da história

Antes mesmo do computador ser inventado, já havia gente com o espírito de *hacker*: pessoas fanáticas por tecnologia, com profundo senso de lógica, curiosidade inesgotável e criatividade - para o bem ou para o mal.

5.1 - Ada Byron Lovelace (1815)

Matemática e musicista inglesa, filha do escritor Lord Byron. Tornou-se conhecida por ser a primeira pessoa a quem podemos chamar de programadora de computador. Escreveu o primeiro texto explicando o processo de programação de uma máquina.

5.2 - Dennis Ritchie e Ken Thompson (1969)

Programadores da Bell Labs. Inventaram o sistema operacional Unix.

5.3 - John Draper (1971)

Descobriu como fazer ligações telefônicas sem pagar, usando um apito que vinha de brinde com um cereal matinal. O apito produzia a mesma freqüência usada para por a central telefônica em espera. Bastava apitar perto do microfone do telefone e discar o número.

5.4 - Johan Helsingius (Finlândia)

Hacker que usava e abusava do seu servidor de e-mail anônimo. Uma vez publicou todos os documentos secretos da igreja Cientologia na Internet e por isso acabou preso.

5.5 - Mark Abene (Phiber Optik) (1985)

Fundou um grupo *hacker* chamado *Masters of Deception*, que inspirou milhares de jovens a vasculharem o funcionamento do sistema telefônico dos EUA.

5.6 - Robert Morris (1988)

Introduziu definitivamente o termo *"hacker"* no vocabulário das pessoas. Filho do cientista-chefe do Centro Nacional de Segurança de Computadores do EUA, acidentalmente colocou na Internet um vírus que infectou e travou milhares de computadores.

5.7 - Clifford Stoll (1989)

Quando um *cracker* invadiu seu laboratório de armas nucleares, monitorou-o até identificá-lo. Escreveu *"The Cuckoo's Egg"* (O Ovo do Cuco), um dos melhores livros sobre a cultura *hacker*.

5.8 - Kevin Poulsen (1990)

Tomou controle de todo o sistema telefônico da cidade de Los Angeles para ser o 102º ouvinte a ligar para uma rádio e ganhar um Porsche 944 - o que acabou conseguindo.

5.9 - Vladmir Levin (1995)

Matemático russo a quem se atribui ter sido o cérebro de uma gangue de *hackers* russa que roubou US$ 10 milhões dos computadores do Citibank.

5.10 - Kevin Mitnick (1995)

Primeiro *hacker* a ter o rosto publicado em um cartaz de "procurado" do FBI. Foi solto recentemente depois de cinco anos na cadeia por roubo de números de cartões de crédito e invasão do *Norad*, Sistema Nacional de Defesa dos EUA.

6. Mitos e fantasias

O maior mito existente na Internet é que o *cracker* pode invadir qualquer computador na hora que quiser, e outro mito é que o *hacker* e o *cracker* são vistos como gênios da informática. Antigamente realmente os *hackers* e *crackers* eram gênios da informática, mas a grande maioria que se diz “hackers” hoje em dia se aproveita das ferramentas encontradas na Internet, ou seja, mal sabem programar.

7. Engenharia Social

Engenharia Social é o termo utilizado para a obtenção de informações importantes de uma empresa, através de seus usuários e colaboradores. Essas informações podem ser obtidas pela ingenuidade ou confiança das pessoas para se conseguir vantagens. Os ataques dessa natureza podem ser feitos através de telefones, salas de bate-papo, e-mails e até mesmo pessoalmente. São muitas as formas e mecanismos de ataque mediante a fragilidade e ingenuidade das pessoas, e por esse motivo seguem algumas dicas que podem ajudá-lo a minimizar este problema e garantir a sua privacidade e a da sua empresa:

- Controle o acesso físico nas empresas;
- Classifique as informações da sua empresa, sabendo quais as informações podem ou não ser disponíveis;
- Desconfie das ofertas mirabolantes que circulam pela Internet;
- Desconfie de mensagens de correio eletrônico onde você não conhece o remetente, os ataques de engenharia social costumam utilizar a emoção;
- Ao receber um telefone de uma pessoa estranha, que conhece todos os seus dados e lhe transmite confiança, retenha desta pessoa o máximo de informações possíveis, não divulgue nada e peça o número de retorno dela para garantir que a ligação é procedente;
- Estabeleça uma política de segurança na sua empresa onde a informação, que é seu principal patrimônio, receba o tratamento correto com relação a segurança;
- Evite compartilhar sua senha de acesso, pois ela pode ser divulgada sem que você tenha sido a vítima do ataque de engenharia social;
- Conscientize seus funcionários a respeito do tema, realizando palestras e treinamentos onde o assunto seja abordado;

8. Fundamentos Jurídicos

O conhecimento das leis é uma das principais armas do *hackers*, que deve estar atento aos movimentos feitos pelos governos e as políticas instituídas pelas empresas quanto à manipulação de dados. A ignorância em relação às leis pode trazer sérios problemas, mesmo em casos simples em que o usuário age de forma inocente sem saber que está cometendo crime.

As grandes estratégias para o combate aos cibercrimes começaram a ser elaboradas após os atentados terroristas ocorridos nos Estados Unidos no dia 11 de setembro de 2001. Desde então o governo norte-americano passou a ditar o destino de *hackers* e *crackers* pelo mundo, exigindo de todos os outros governos leis que facilitem a ingerência dos Estados Unidos.

8.1 - A liberdade individual e o direito privado

As constituições de quase todos os países possuem algum dispositivo referente a liberdades individuais e o direito privado, e mesmo a Declaração Universal dos Direitos Humanos prevê a proteção à vida pessoal e privada das pessoas. Ninguém tem direito de invadir a privacidade das pessoas, mas todos os dias vemos novas tecnologias sendo aplicadas em controversas e arbitrários sistemas de monitoração como telefones grampeados, correspondências violadas (e-mails), seus passos seguidos e, nos anos 90, sua atividade na Internet vigiada. Fazer leis que protejam indivíduos e entidades públicas e privadas desses "*hackers* do mal" sem ferir os direitos de privacidade das pessoas é uma tarefa dificílima.

8.2 - A legislação brasileira

O grande trunfo dos *hackers* brasileiros é a falta de legislação apropriada para lidar com os crimes eletrônicos. A falta de leis específicas torna o Brasil um verdadeiro paraíso para todo o tipo de invasão e manipulação ilícita de dados. As punições aplicadas são baseadas em leis que se aproximam da situação do crime eletrônico. Grande parte dos casos resolvidos pelas autoridades nacionais é relativa a casos de pirataria, pedofilia, estelionato, e não invasão e "hackeamento" de sistemas.

A falta de proteção legal preocupa muito o governo e as grandes empresas, pois estas são obrigadas a gastar quantias elevadas de dinheiro com *software* e equipamentos para garantir a segurança de seus dados e mesmo assim não conseguem evitar a ação dos vândalos digitais.

A seguir, temos um trecho específico do projeto de lei criado pelo Deputado Décio Braga que dispõe sobre os crimes de informática e dá outras providências:

- **Dano a dado ou programa de computador:** apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada;

- **Acesso indevido ou não autorizado:** obter acesso, indevido ou não autorizado, a computador ou rede de computadores;

- **Alteração de senha, ou mecanismo de acesso a programa de computador ou dados:** apagar, destruir, alterar, ou de qualquer forma inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada;

- **Obtenção indevida ou não autorizada de dado ou instrução de computador:** obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador;

- **Violação de segredo armazenado em computador, meio magnético de natureza magnética, óptica ou similar:** obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada;

- **Criação, desenvolvimento ou inserção em computador de dados ou programa de computador com fins nocivos:** criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores;

- **Veiculação de pornografia através de rede de computadores:** oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Como podemos notar, o projeto é abrangente, lidando com assuntos que vão desde invasões até a criação de vírus e programas que possam danificar dados alheios. Com certeza, a "nação *hacker*" teria a maioria dos seus atos coibida caso a lei estivesse em vigor. Mas, além do processo de aprovação da lei, o governo tem de prover condições para que elas sejam executadas.

8.3 - Leis internacionais após o dia 11 de setembro de 2001

As condutas podem ser praticadas fora do território de um país e lá produzir resultados, o que faz necessário encontrar meios de fazer valer leis de proteção aos delitos digitais de um modo global.

8.3.1 - Nos Estados Unidos da América

Muita coisa mudou em relação à vida dos *hackers* no âmbito internacional. Estudos realizados pelo Pentagóno sobre o ciberterrorismo mostraram que ataques de *crackers* poderiam parar o país, já que o reservatório de águas, energia elétrica e gás são controlados por centros de computação que podem ser invadidos ridiculamente. Uma das leis criadas pelo departamento foi a USA *Act*, que possui uma seção especial voltada para o ciberterrorismo. A USA *Act* prevê punição para toda forma de vandalismo eletrônico, que possa atingir empresas e cidadãos, incluindo invasões vindas de outros países.

Com as novas leis e medidas americanas, os legisladores americanos transformaram milhares de *crackers* e *hackers* em terrorista por definição. Um dos parágrafos da PATRIOT (*Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act*) diz o seguinte: aquele que, com consentimento, cause transmissão de um programa, informação, código ou comando e, como resultado de tal conduta, intencionalmente cause dano sem autorização, para um computador protegido estará em violação deste estatuto.

Está em elaboração um conjunto de novas leis (na verdade a ratificação legal da Doutrina Bush) chamado de *Homeland Security Act*, que promete endurecer o cerco aos inimigos dos Estados Unidos em todas as frentes: militar, comercial, armamentista, política e digital.

A lei americana pode funcionar como um modelo para definir os padrões mundiais que são discutidos anualmente pela Interpol, que criou uma divisão especial, a Unidade de Crimes de Alta Tecnologia, para combater os crimes eletrônicos.

8.3.2 - Na Europa

A maior parte dos grupos europeus tomou medidas semelhantes às dos Estados Unidos. Todas baseadas no rastreamento de informações pessoais sem qualquer aviso prévio, dando poder aos seus agentes de vasculhar as caixas de mensagens de qualquer provedor. A adoção do padrão norte-americano mostra mais uma vez que o mundo está próximo de estabelecer uma forte estratégia de combate aos cibercrimes, o que vai prejudicar muito a ação dos vândalos digitais. Como eleito colateral, ferirá também alguns direitos e a privacidade de cidadãos reconhecidamente inocentes (“Mate todos! Um deles é terrorista...”).

9. Motivos mais comuns para a prática do *hacking*

- Insatisfação de funcionários com a empresa em que trabalham: segundo especialistas, a maior parte das invasões acontece ou são planejadas de dentro das empresas atacadas. Esses ataques podem também ser fruto de concorrência entre empresas, que contratam *crackers* para praticar espionagem e provocar prejuízos.

- Fama: o invasor não visa lucro imediato, mas pode ser visto como um expert e, mais tarde, ser contratado por grandes empresas de segurança ou montar ele mesmo sua empresa. Ele busca também ser respeitado dentro da comunidade.

- Manifesto: quando os invasores atacam empresas ou sites com a intenção de fazer manifestação política ou social.

- Para ganhar dinheiro: dentro dessa atividade encontra-se o trabalho do "*hacker* ético" e o "trabalho" do *cracke*r. No caso do ético, ele utiliza sua experiência em invasão para proteção dos sistemas das empresas que os contratam. No caso do *cracker*, usa seu conhecimento para fazer chantagem ou espionagem entre empresas, que pagam a eles para atacar os sistemas das concorrentes.

10. Alvos preferidos e alguns exemplos de ataques

- **Sites famosos:** no dia 20/06/2004, a página principal do provedor de hospedagem HPG, foi desfigurada. Os atacantes protestaram contra o fato de o provedor ter passado a cobrar pela hospedagem, antes gratuita.

- **Governo:** no dia 15/11/2001, *crackers* supostamente portugueses atacaram o site do IBGE (Instituto Brasileiro de Geografia e Estatística). No lugar da página inicial deixaram um protesto contra os *"hackers"* brasileiros.

- **Empresas de segurança:** entre os dias 11 e 12/08/2001 três sites ligados à segurança na Internet sofreram a ação de *crackers* e tiveram suas páginas

desfiguradas. Os servidores invadidos foram os do LinuxSecurity Brasil, Tripwire e Hackertronics.com.

- **Empresas de telecomunicações:** no dia 26/04/2004, dois sites da operadora de telefonia celular Claro amanheceram pichados. O ataque foi assinado pelos *defacers* (desfiguradores de sites) Break_IDS e GagO_XegadoS, que se declaram pertencentes ao grupo brasileiro Data Cha0s.

- **Empresas de tecnologia:** no dia 06/06/2001, nada menos que quatro sites da poderosa Microsoft foram desfigurados por grupos de *crackers*. Três deles, pelo grupo brasileiro Prime Suspectz e o quarto pelo grupo BlackSun.

- **Concorrentes:** dois níveis: ataques a sites de "colegas" *crackers* conceituados ou ataques entre empresas do mesmo ramo em disputa pelo mercado.

- **Bancos**: *worms* que se autopropagam por e-mail e roubam dados e senhas das vítimas.

11. Tipos de Segurança

11.1 - Segurança Física

Algumas ameaças estão sempre presentes, mas nem sempre são lembradas: incêndios, desabamentos, relâmpagos, alagamentos, problemas na rede elétrica, acesso indevido de pessoas ao CPD, treinamento inadequado de funcionários e etc. Medidas de proteção física, tais como serviço de guarda, uso de *no-break*s, alarmes e fechaduras, circuito interno de televisão e sistemas de escuta são realmente uma parte da segurança de dados. O ponto-chave é que as técnicas de proteção de dados, por mais sofisticadas que sejam, não têm serventia nenhuma se a segurança física não for garantida. Por mais seguro que seu ambiente seja, ele não estará 100% seguro se a pessoa que deseja invadir seu sistema tiver acesso físico ao mesmo.

11.2 - Segurança Lógica

Envolve investimento em *softwares* de segurança ou elaboração dos mesmos. Um recurso muito utilizado para se proteger dos “bisbilhoteiros” da Internet é a utilização de um programa de criptografia que embaralha o conteúdo da mensagem de modo que ela se torna incompreensível para aqueles que não sejam o receptor ou emissor da mesma.

11.3 - Ferramentas de Segurança

Uso de *Firewall*, Sistemas de Detecção de Intrusos, Logs, Antivírus e Backup.

11.4 - Senhas

Uma senha fácil de se deduzir é a causa mais comum dos problemas de segurança. A senha não pode ser fácil de adivinhar, como o nome do marido ou da mulher, do namorado ou namorada, do seu cão, a placa do carro, a rua onde mora, a data do nascimento ou outra informação conhecida. Os *hackers* costumam usar os programas e dicionários on-line para adivinhar senhas fáceis e expressões mais usadas.

12. A Importância do Profissional de Segurança

É necessário que se tenha um profissional só para trabalhar com a segurança da empresa porque a área de segurança é muito grande e todos os dias alguém deve visitar os sites especializados e procurar por atualizações e correção de *bugs*. Um especialista em segurança não é aquele que é PhD em ciências da computação. A informática muda muito rápido e as pessoas que fazem curso superior nessa área têm tanta coisa o que estudar que muitas vezes a segurança não é aprendida a fundo. Os melhores profissionais são aqueles que fizeram cursos especiais (como cursos oficiais da Microsoft, da Conectiva ou da Cisco Systems).

13. Como conseguir uma política eficiente de proteção

Ler muito sobre as novidades do mundo da segurança; ver se o administrador realmente se preocupa com a proteção do sistema; fazer sempre backup dos logs e varredura do sistema por falhas; checar o computador dos funcionários procurando por programas escondidos e passar um bom antivírus neles são medidas importantes. Se usar algum programa de segurança, como *firewalls*, detectores de invasão e outros, dar preferência para aqueles mais conhecidos e confiáveis. Considere ainda mudar as senhas de acesso ao sistema quando alguém for demitido. E nunca discuta com um *cracker*.

14. Conclusão

De fato, Segurança da Informação é um assunto muito sério, e não pode ser deixado de lado. Deve ter um lugar de destaque, não apenas para as pessoas que trabalham diretamente na área de informática, como técnicos, analistas, programadores, como também para as pessoas que, de alguma forma, utilizam a informática como ferramenta para facilitar seus trabalhos, pois a informação não tem preço. É importante saber que, apesar de todos os cuidados nenhum sistema é 100% à prova de falhas. Mas pelo menos pode-se diminuir muito o risco.

Referências

[ARAÚJO ASSUNÇÃO, 2002] Araújo Assunção, M. F. – *"O Guia do Hacker Brasileiro"*.

[ULBRICH & DELLA VALLE, 2003] ULBRICH, H. C. e VALLE, J. D – *"Universidade H4CK3R"*. Digerati Books, 3ª edição, 2003.