ENGENHARIA SOCIAL
Um Perigo Eminente

Marcos Antonio Popper
Juliano Tonizetti Brignoli
Instituto Catarinense de Pós-Graduação – ICPG
Gestão Empresarial e Estratégias de Informática

Resumo

As empresas estão investindo na modernização de seus parques tecnológicos e estão deixando de lado o fator humano. A engenharia social explora essa vulnerabilidade. Os principais alvos são as grandes corporações porque, segundo pesquisa realizada nos Estados Unidos em 2002 pela revista Information Secutiry, os investimentos em segurança não acompanham o crescimento das empresas. Os ataques de engenharia social não possuem fórmula nem método definido. Eles podem ter aspectos físicos e psicológicos. No físico, exploram o local de trabalho, vasculham lixeiras, e por telefone se passam por outra pessoa. No psicológico, exploram o lado sentimental das pessoas. No Brasil ainda não há uma legislação específica que puna estes tipos de crimes; então, além da conscientização e treinamentos constantes, as empresas devem possuir um plano de contingência para eventuais ataques e assim garantir a continuidade dos negócios.

Abstract

The companies are investing in up-to-dating their technological fields and are not paying attention to the human factor. The social engineering explores this vulnerability. The main targets are the big corporations because, according to a research done in the United Stated in 2002 by the Information Security magazine, the investments in security do not follow the companies growth. The social engineering attacks do not have a formula nor a determined method. They can have physical and psychological aspects. In the physical one, they explore the working place, rummaging garbage cans and, by phone, pretending being another person. In the psychological one, they explore the sentimental side of people. In Brazil, there is not a specific law that punishes these kinds of crimes; so, besides the continuous consciousness-raising and training, the companies must have a contingency plan for eventual attacks and, so, guarantee the business continuity.

Palavras Chave: Engenharia Social, Hacker, Informação.

1. INTRODUÇÃO

Apesar do nome, a Engenharia Social nada tem a ver com ciências exatas ou sociologia. Na verdade, trata-se de uma das mais antigas técnicas de roubo de informações importantes de pessoas descuidadas, através de uma boa conversa (Virinfo,2002).

Com o crescente número de invasões sofridas pelas empresas em suas bases de dados, estas estão voltando suas atenções para a modernização de seus parques tecnológicos, com

atualizações de *firewalls*[1], formas de criptografia[2], e muitos outros mecanismos de segurança, deixando o fator humano em segundo plano.

A Engenharia Social, de maneira simples, caracteriza-se por explorar essa fragilidade. Em outras palavras, consiste na habilidade de obter informações ou acesso indevido a determinado ambiente ou sistema, utilizando técnicas de persuasão (Vargas,2002).

2. ALVOS DE UM ATAQUE

Se formos analisar de forma minuciosa, dificilmente encontraremos alguém ou alguma empresa que não tenha sofrido um ataque de engenharia social.

O dito popular "jogar verde pra colher maduro" define bem o tema. Quem nunca se viu envolvido sendo questionado sobre um determinado assunto e, quando se deu conta, já tinha "entregue o ouro pro bandido?" Isso quando a pessoa se dá conta; muitas vezes ela fala e nem percebe o conteúdo do que foi dito.

Podemos citar os mais variados exemplos; entre eles, uma oferta de emprego que nos interessa e, quando chegamos lá, nosso amigo já ocupou a vaga, ou quando temos uma venda praticamente concretizada ou uma boa oferta de compra e novamente nosso amigo chegou na frente. Então nos questionamos: Mas como ele sabia? Só que esquecemos da cervejinha de sábado à tarde quando estávamos todos juntos "jogando conversa fora" e sem perceber o assunto foi comentado.

Em grandes empresas, instituições financeiras, militares, órgãos do governo e até mesmo hospitais, a situação é semelhante. Só que, nesse caso, envolvem pessoas preparadas, os chamados *hackers*[3], e as formas de ataque utilizadas são mais audaciosas. A meta desses *hackers* é obter acesso não autorizado a sistemas, sabotar informações, espionagem industrial, roubo de identidade ou simplesmente sobrecarregar os sistemas a ponto de tirá-los de operação.

Estes tipos de ataques são altamente eficazes e com um custo relativamente baixo, em função da experiência do atacante. Muitas das empresas atacadas, a exemplo das pessoas, também nem percebem que foram alvos de um ataque, porque estes piratas deixam poucos ou falsos rastros, que dificultam a rastreabilidade das ações e a mensuração dos prejuízos decorrentes dos mesmos.

Mesmo aquelas que descobrem que foram atacadas, dificilmente admitem o fato, com receio de prejudicarem sua reputação. Na Inglaterra, por exemplo, as empresas já podem ostentar um certificado de que exercitam boas práticas de mercado no que diz respeito à segurança da informação, que rapidamente está se tornando um diferencial competitivo para as empresas que souberem administrá-lo (Saldanha,2002).

---

[1] - Firewalls são programas especiais que têm por objetivo evitar acessos não autorizados a computadores (Módulo,2002).

[2] - Criptografia é a técnica de escrever em cifra ou código, composto de técnicas que permitem tornar incompreensível uma mensagem transmitida. Somente o destinatário poderá decifrá-la (Módulo,2002).

[3] - Hackers são também conhecidos como piratas da Internet, que tem como objetivo invadir os computadores desprotegidos utilizando as mais variadas técnicas para roubar informações (Módulo,2002).

3. FORMAS DE ATAQUE

As formas de ataque são as mais variadas, sempre explorando a fragilidade e ingenuidade das pessoas. Nenhum artigo sobre ataques de engenharia social estaria completo sem citar Kevin Mitnick (Goodell,1996), que, até ser capturado, era considerado o maior *hacker* de todos os tempos. Iguais a ele, atualmente existem muitos, e as táticas utilizadas são basicamente as mesmas.

Antes de citar as diversas formas de ataque, o ideal é citar quem são os atacantes. Engana-se quem pensa que os ataques sempre são executados pelos *hackers*. A tabela a seguir mostra alguns tipos de intrusos e seus principais objetivos.

TABELA 1 – Tipos de Intrusos

Intrusos	**Objetivos**
Estudantes	Bisbilhotar mensagens de correio eletrônico de outras pessoas por diversão;
Hackers/Crackers	Testar sistemas de segurança, ou roubar informações;
Representantes Comerciais	Descobrir planilhas de preços e cadastro de clientes;
Executivos	Descobrir plano estratégico dos concorrentes;
Ex-funcionários	Sabotagem por vingança;
Contadores	Desfalques financeiros;
Corretores de valores	Distorcer informações para lucrar com o valor das ações;
Vigaristas	Roubar informações, como senhas e números de cartões de crédito;
Espiões	Descobrir planos militares;
Terroristas	Espalhar pânico pela rede e roubo de informações estratégicas.

Os ataques de Engenharia Social podem ter dois aspectos diferentes: o físico, como local de trabalho, por telefone, no lixo ou mesmo *on-line*, e o psicológico, que se refere à maneira como o ataque é executado, tal como persuasão.

3.1. Local de Trabalho

Nomes, lista de ramais, endereços eletrônicos, organogramas e outros dados da empresa, comumente ficam expostos em lugares onde transitam pessoas estranhas. Um *hacker* pode simplesmente entrar na empresa como se fosse um técnico em manutenção ou consultor que tem livre acesso às dependências da empresa e, enquanto caminha pelos corredores, pode ir captando todas estas informações que porventura estejam expostas (Maia,2002).

3.2. Engenharia Social por Telefone

Esta modalidade de ataque vai desde roubar informações de funcionários ingênuos até a clonagem ou grampo telefônico. Um *hacker* chega na empresa passando-se por um técnico que fará manutenção da central telefônica e, em seguida, desvia uma linha de onde pode efetuar ligações para qualquer parte do mundo, ou então pode grampear os telefones de algum executivo.

Outro alvo importante, também são os *call centers*[4]. Os atendentes têm por obrigação atender a todos da melhor maneira possível, solucionando todas as dúvidas possíveis. Então entra em cena o talento do *hacker* que poderá, com isso, conseguir dicas de utilização dos sistemas e até senhas de acesso (Granger,2001).

3.3. Lixo

O lixo das empresas pode ser uma fonte muito rica de informações para um *hacker*. Vasculhar o lixo, é um método muito usado pelos invasores, porque é comum encontrarmos itens como cadernetas com telefones, organograma da empresa, manuais de sistemas utilizados, memorandos, relatórios com informações estratégicas, apólices de seguro e até anotações com *login* e senha de usuários.

As listas telefônicas podem fornecer os nomes e números das pessoas-alvo, o organograma mostra quem são as pessoas que estão no comando, as apólices mostram o quanto a empresa é segura ou insegura, os manuais dos sistemas ensinam como acessar as informações e assim todo e qualquer lixo poderá ser de grande valia para uma pessoa mal intencionada (Granger,2001).

3.4. Desafio das Senhas

As senhas são os principais pontos fracos das empresas. É comum as pessoas dividirem senhas com outras ou escolherem senhas fracas, sem a menor preocupação. Muitos usam como senha, palavras que existem em todos os dicionários, seus apelidos, ou até mesmo o próprio nome que, com um *software*[5] gerenciador de senhas, é possível decifrá-las em segundos(Virinfo,2002). Segundo Kevin Mitnick (2001), elas chegam a representar 70% do total de senhas utilizadas nas empresas.

3.5. Engenharia Social *On-line*

Talvez a maneira mais fácil de se conseguir um acesso é através da *internet*[6]. A displicência dos usuários que criam senhas fáceis de serem descobertas, que ficam longos períodos sem alterá-las, e ainda utilizam a mesma senha para acesso a várias contas, torna o ataque mais simples. Basta enviar um cadastro oferecendo um brinde ou a participação em um

[4] - Call Center são centros de atendimento ou suporte a usuários via telefone.
[5] - Software são programas para computadores.
[6] - Internet o mesmo que rede mundial de computadores.

sorteio que solicite o nome e senha do usuário e pronto. O *hacker* terá a sua disposição tudo o que é necessário para um ataque, sem grande esforço (Granger,2001).

As salas de bate-papo também são um canal explorado para o roubo de informações. Homens e mulheres se dizem jovens, atraentes e de bom papo. Na verdade podem ser farsantes que manipulam os sentimentos das pessoas em busca de informações (Maia,2002).

Outro meio de se obter informação *on-line*, é se passar pelo administrador da rede, que, através de um *e-mail*[7], solicita aos operadores nome e senha. Porém, este tipo de ataque já não é mais tão eficaz, porque os operadores que trabalham nessas áreas geralmente são pessoas mais experientes e não caem nesse tipo de truque tão facilmente.

Os *e-mails* também podem ser usados como meio para conseguir acesso a um sistema. Por exemplo, um *e-mail* enviado para alguém pode conter um vírus de computador ou cavalos de tróia[8], que, quando instalados no computador da vítima, podem destruir todas as informações, ou simplesmente ficar ocultos e transmitindo ao invasor todo tipo de informação como, senhas, números de cartão de crédito, ou mesmo abrir o *firewall* da empresa, deixando-a vulnerável a qualquer tipo de ataque (Granger,2001).

3.6. Persuasão

Os próprios *hackers* vêem a engenharia social de um ponto de vista psicológico, enfatizando como criar o ambiente psicológico perfeito para um ataque. Os métodos básicos de persuasão são: personificação, insinuação, conformidade, difusão de responsabilidade e a velha amizade. Independente do método usado, o objetivo principal é convencer a pessoa que dará a informação, de que o engenheiro social é, de fato uma pessoa a quem ela pode confiar as informações prestadas. Outro fator importante é nunca pedir muita informação de uma só vez e sim perguntar aos poucos e para pessoas diferentes, a fim de manter a aparência de uma relação confortável.

Personificação geralmente significa criar algum tipo de personagem e representar um papel. Quanto mais simples esse papel, melhor. Às vezes, isto pode ser apenas ligar para alguém e dizer: “Oi, eu sou Marcos do setor de informática e preciso da sua senha”. Mas isto nem sempre funciona. Outras vezes, o *hacker* vai estudar uma pessoa de um departamento e esperar até que se ausente para personificá-la ao telefone. De acordo com Bernz (1996), um *hacker* que escreveu extensivamente sobre o assunto, eles usam pequenas caixas para disfarçar suas vozes e estudam os padrões de fala. Este tipo de ataque é menos freqüente, pois exige mais tempo de preparo, mas acontece.

Outra tática comum que pode ser utilizada num ataque de personificação é o *hacker* se passar por assistente da gerência ou mesmo presidência e pedir a um funcionário, em nome do seu superior, alguma informação. Para não criar atritos com seu superior, o usuário fornece as informações sem muitos questionamentos. Numa grande empresa, não há como conhecer todos os funcionários; então, fingir uma identidade não é um truque muito difícil de ser aplicado.

---

[7] - E-mail são mensagens enviadas por correio eletrônico usando a Internet como meio de transporte.

[8] Cavalos de tróia são programas ou fragmentos de códigos maléficos que uma vez instaladas em um computador permitem o roubo de informações.

A conformidade é um comportamento baseado em grupo, mas pode ser usado ocasionalmente no cenário individual, convencendo o funcionário de que todos os demais estão fornecendo determinadas informações, solicitadas pelo *hacker*, como se este estivesse personificando a figura de um gerente. Quando os *hackers* atacam no modo de divisão de responsabilidade, eles convencem os funcionários a compartilharem suas senhas a fim de dividirem também a responsabilidade.

Quando em dúvida, a melhor maneira de obter informação no ataque de engenharia social é ser amigável. O local para abordagem não necessariamente precisa ser na empresa; pode ser num clube ou numa mesa de bar. O *hacker* só precisa conquistar a confiança do funcionário alvo, a ponto de convencê-lo a prestar "toda a ajuda solicitada". Além disso, a maioria dos funcionários responde bem a gentilezas, especialmente as mulheres. Uma bajulação pode ajudar a convencer o funcionário alvo a cooperar no futuro. Um *hacker* esperto sabe quando parar de extrair informações antes que a vítima suspeite que está sendo alvo de um ataque (Granger,2001).

3.7. Engenharia Social Inversa

Um método mais avançado de conseguir informações ilícitas é com a engenharia social inversa. Isto ocorre quando um *hacker* cria uma personalidade que aparece numa posição de autoridade, de modo que todos os usuários lhe pedirão informação. Se pesquisados, planejados e bem executados, os ataques de engenharia social inversa permitem ao *hacker* extrair dos funcionários informações muito valiosas; entretanto, isto requer muita preparação e pesquisa.

Os três métodos de ataques de engenharia social inversa são, sabotagem, propaganda e ajuda. Na sabotagem, o *hacker* causa problemas na rede, então divulga que possui a solução para este, e se propõe a solucioná-lo. Na expectativa de ver a falha corrigida, os funcionários passam para o *hacker* todas as informações por ele solicitadas. Após atingir o seu objetivo, o hacker elimina a falha e a rede volta funcionar normalmente. Resolvido o problema os funcionários sentem-se satisfeitos e jamais desconfiarão que foram alvos de um *hacker* (Granger,2001).

3.8. *Footprint*

Nem sempre o invasor consegue coletar as informações desejadas através de um telefonema ou uma conversa amigável, seja porque as pessoas não detêm o conhecimento necessário ou por não conseguir alcançar pessoas ingênuas.

Então o invasor utiliza uma técnica conhecida como *footprint*, que, através de softwares específicos, consegue as informações necessárias ao ataque.

Footprint é um perfil completo da postura de segurança de uma organização que se pretende invadir. Usando uma combinação de ferramentas e técnicas, atacantes podem empregar um fator desconhecido e convertê-lo em um conjunto específico de nomes de domínio, blocos de redes e endereços IP[9] individuais de sistemas conectados diretamente na Internet. Embora haja

[9] - IP são protocolos da Internet.

diversas técnicas diferentes de *footprint*, seu objetivo primário é descobrir informações relacionadas a tecnologias de *internet*, acesso remoto e *extranet*[10] (Veríssimo,2002).

Os métodos expostos anteriormente fazem parte das táticas comuns de ataque. Porém existem muitos outros truques não tão comuns, como por exemplo:

- Uma entrevista para uma vaga que não existe, que é feita somente para se obter informações a respeito dos concorrentes;
- Aquelas que acontecem por acaso, como numa conversa sobre assuntos confidenciais da empresa, em lugares de circulação de pessoas e que alguém de passagem sem querer capta alguma informação importante;
- Manipulação de informações para alterar o comportamento de usuários a partir de dados falsos ou sutilmente alterados.

4. FORMAS DE PREVENÇÃO

A prevenção não é uma tarefa fácil. A maioria das empresas não direciona recursos financeiros nem humanos para tal. No entanto, investem na manutenção de sistemas e em novas tecnologias, ao invés de direcionar parte desse investimento para combater um inimigo que pode ser bem mais perigoso, a engenharia social. A ameaça deste inimigo é real, tanto quanto as falhas em uma rede.

Os seres humanos são seres imperfeitos e multifacetados. Além disso, situações de risco modificam seus comportamentos, e, decisões serão fortemente baseadas em confiança e grau de criticidade da situação (Vargas,2002).

Em função desses fatores, sempre existirão brechas em seu caráter ou comportamento pouco consciente com relação à segurança, onde a engenharia social poderá ser plenamente eficaz.

Para amenizar estes riscos, é recomendável que as empresas criem políticas de segurança centralizada e bem divulgada, para que todos os seus colaboradores saibam como proteger as informações que estão em seu poder. As *intranets*[11] podem ser um recurso valioso para esta divulgação, assim como boletins periódicos *on-line*, lembretes no correio eletrônico, requisitos de mudança de senha e treinamento. O maior risco é de os funcionários tornarem-se complacentes e relaxarem na segurança; por isso a importância da insistência (Granger,2002).

O treinamento deve estender-se por toda a empresa. Diretores, gerentes, supervisores, e demais funcionários, todos devem ser treinados. Nestes treinamentos devem ser exploradas as táticas comuns de intromissão e as estratégias de prevenção. Quando alguém captar sinais de um ataque, deve imediatamente alertar os demais, para que não sejam também abordados.

Na tabela abaixo, estão expostas as principais áreas de risco de uma empresa, as táticas mais comuns usadas pelos *hackers* e também as estratégias de combate.

[10] - Extranet são redes de computadores externas de uma empresa.
[11] - Intranets são redes internas de computadores.

TABELA 2 – Áreas de Risco, Táticas e Estratégias

Área de Risco	**Tática do *Hacker***	**Estratégia de Combate**
Suporte de informática	Representação e persuasão;	Desenvolver na empresa uma política de mudança freqüente de senhas e treinar os demais funcionários para nunca passarem senhas ou outras informações confidenciais por telefone;
Entrada de edifícios	Acesso físico não autorizado;	Treinar os funcionários da segurança para não permitirem o acesso de pessoas sem o devido crachá de identificação e mesmo assim fazer uma verificação visual;
Escritórios	Caminhar pelo ambiente;	Não digitar senhas na presença de pessoas estranhas, a menos que você consiga fazê-las rapidamente;
Suporte telefônico	Usar de disfarces na hora de solicitar ajuda aos atendentes, geralmente se passando por outra pessoa;	Os atendentes devem solicitar sempre um código de acesso, para só então prestarem o suporte solicitado;
Escritórios	Caminhar pelos corredores à procura de salas desprotegidas;	Todos os visitantes devem ser acompanhados por um funcionário da empresa;
Sala de correspondência	Inserção de mensagens falsas;	Fechar e monitorar a sala de correspondência;
Sala dos servidores	Instalam programas analisadores de protocolo para conseguirem informações confidenciais, além da remoção de equipamentos;	Manter sala dos servidores sempre trancada, e o inventário de equipamentos atualizado;
Central telefônica	Roubar acesso a linhas telefônicas;	Controlar chamadas para o exterior e para longas distâncias, e recusar pedidos de transferências suspeitas;
Depósito de lixo	Vasculhar o lixo;	Guardar o lixo da empresa em lugar seguro, triturar todo tipo de documento, e destruir todo o tipo de mídia magnética fora de uso;
Internet e *intranet*	Criar e/ou inserir programas na *Internet* ou *intranet* para capturar senhas;	Criar senhas fortes e fazer uso consciente da mesma, alterando-a periodicamente. Os modens nunca devem ter acesso a *intranet* da empresa;
Escritório	Roubar documentos importantes;	Manter os documentos confidenciais fora do alcance de pessoas não autorizadas, de preferência em envelopes fechados.

4.1. Plano de Resposta a Incidentes

Mesmo a melhor infraestrutura de segurança da informação não pode garantir que intrusos ou outras ações maliciosas ocorram. Quando um incidente de segurança ocorre, é um fator crítico para a organização ter meios para responder a esse evento. A velocidade à qual uma organização pode reconhecer, analisar e responder a um incidente de segurança, limita os estragos e diminui os custos de restauração. A habilidade de usar essa informação para reparar ou prevenir ocorrências similares, aprimora a segurança geral a uma organização.

O Plano de Resposta a Incidentes é um documento que descreve as diretrizes gerais e procedimentos para tratamento dos principais incidentes de segurança que podem ocorrer na organização, proporcionando ao pessoal de suporte instruções sobre as medidas a serem tomadas para a definição e correção dos mesmos.

O tipo de tratamento dado aos incidentes de segurança varia de acordo com a sua intensidade e risco. Porém, o encaminhamento deve ser decidido em acordo com a alta direção da empresa e com o respaldo do departamento jurídico. As ações pertinentes podem envolver o relacionamento com entidades externas (como clientes, parceiros, provedores de serviços e outros) ou mesmo exigir o acionamento de autoridades e órgãos policiais. Principais pontos a serem considerados em um Plano de Resposta a Incidentes:

- Procedimentos para identificação e autoria dos ataques: identificar a intensidade e quantificar os prejuízos causados pelo incidente e também procurar identificar os responsáveis pelo incidente;
- Divulgação das informações: divulgar imediatamente o fato ocorrido para que outras áreas não sejam também abordadas;
- Procedimentos e pessoal responsável pela restauração: as ações de restauração como, mudança de senhas, troca de pessoal, intensificação dos níveis de controle, devem ser imediatamente tomadas a fim de evitar maiores prejuízos;
- Contatos com as fontes do ataque e órgãos de segurança: contatar os responsáveis pelos ataques, a fim de exigir a indenização dos prejuízos e também os órgãos de segurança para que fique registrado o fato ocorrido (Medeiros,2001).

A gama de formas de ataque de engenharia social é muito grande e os procedimentos de resposta a incidentes são particulares. Estas particularidades variam de acordo com o ramo de atividade de cada empresa; o que é imprescindível para uma, pode ser dispensável para outra. No entanto toda empresa, independente do porte, deve ter o seu Plano de Resposta a Incidentes.

5. PUNIÇÕES PARA OS CRIMES DE ENGENHARIA SOCIAL

Punir os responsáveis pelos ataques de engenharia social é uma tarefa difícil. Alguns desses delitos nem podem ser considerados crimes, como, por exemplo, captar informações que estejam expostas sobre uma mesa, vasculhar o lixo ou ouvir uma conversa em um lugar público.

Outro tipo difícil de ser combatido são os crimes que ocorrem on-line, devido a diversos fatores, entre eles o anonimato e a estrutura virtual. Em primeiro lugar, a rede não respeita fronteiras entre países, o que dificulta administrar as diferenças culturais ou aplicar leis nacionais.

Em segundo, a comunicação tem natureza mista, entre o público e o privado. A troca de mensagens de correio eletrônico é particular como um telefone; uma máquina na web é pública como um programa de TV.

Analisando o exemplo acima, conclui-se que a falta de limites geográficos estabelecidos na jurisdição, gera problemas relacionados à soberania nacional, como nos casos em que dois ou mais países estão envolvidos. Aparece, então, o problema relacionado ao princípio da territoriedade, ou seja, definir se a jurisdição se encontra no país de onde partiram os dados, onde estes dados estão armazenados ou onde o dano foi causado (Gomes,2001).

Já no âmbito nacional, é possível combater alguns desses delitos, entretanto é necessária uma legislação que defina bem esses crimes, o que no Brasil ainda não existe.

6. CONCLUSÃO

A maior parte dos desastres e incidentes com a segurança das informações tem como fator predominante a intervenção humana. Segurança tem a ver com pessoas e processos, antes de ter a ver com tecnologia. Segundo especialistas em segurança da informação, a engenharia social será a maior ameaça à continuidade dos negócios desta década. Então de nada valerão os milhões investidos em tecnologia, se o fator humano for deixado em segundo plano. É recomendável que haja uma política de segurança centralizada e bem divulgada, para que todos saibam como se defender e a quem recorrer em caso de dúvidas. Não é necessário fazer com que as pessoas se tornem paranóicas, mas que estejam sempre alertas às solicitações que a elas sejam feitas e que saibam o valor das informações pelas quais são responsáveis.

As ferramentas de engenharia social estão de posse de todos; o uso consciente e planejado delas é que faz a diferença. Quanto mais bem preparados estiverem os colaboradores de uma empresa, mais segura ela será.

7. REFERÊNCIAS BIBLIOGRÁFICAS

BERNZ. The **Complete Social Engineering FAQ!**, 1996. Disponível em: <http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt>. Acesso em: 08 de outubro de 2002, às 12:30h.

GOMES José Olavo Anchieschi. A Criminalidade Cibernética e suas Conseqüências Legais. Security Magazine- Revista de Segurança em Informática,São Paulo, ano II, n. 8, pág. 5-7, jan/dez. 2001.

GOODELL, Jeff. O Pirata Eletrônico e o Samurai - A Verdadeira História de Kevin Mitnick e do Homem que o Caçou na Estrada Digital. Rio de Janeiro. Editora Campus. 1996.Trad. Ana Beatriz Rodrigues. Título Original: The Cyberthief and the Samurai.

GRANGER, Sarah. **Social Engineering Fundamentals, Part I: Hacker Tactics**. Atualizado em 18 de Dezembro de 2001. Disponível em: <http://online.securityfocus.com/infocus/1527>. Acesso em 15 de Abril de 2002, ás 18:30h.

_____. **Social Engineering Fundamentals, Part II: Combat Strategies**. Atualizado em: 09 de Janeiro de 2002. Disponível em: <http://online.securityfocus.com/infocus/1533>. Acesso em 15 de Abril de 2002, às 19:00 h.

MAIA, Marco Aurélio. **Formas de Ataque**. Disponível em: <http://www.scua.net/segurança/conceitos/ataques_engsocial.htm>. Acesso em: 15 de Julho de 2002, às 13:00 h

MEDEIROS, Carlos Diego Russo. Implantação de Medidas e Ferramentas de Segurança da Informação. Joinville. 2001. Monografia (Conclusão de Estágio do Curso de Informática). Universidade da Região de Joinville.

MITNICK, Kevin. **My First RSA Conference, Security Focus, April 30, 2001.** Disponível em: <http://online.securityfocus.com/news/199>. Acesso em: 13 de agosto de 2002 às 18:00h.

MÓDULO SECURITY MAGAZINE. **Glossário**. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 02 de outubro de 2002, 15:00 h.

SALDANHA. **Cuidado com os Hackers** [mensagem pessoal]. Mensagem recebida por marcos@fischer.com.br em 11 de junho de 2002, às 08:00 h.

VARGAS, Alexandre. **Ameaça além do Firewall. Porque as empresas devem se preparar contra a Engenharia Social** [mensagem pessoal]. Mensagem recebida por marcos@fischer.com.br em 11 de abril de 2002, ás 08:45 h.

VERÍSSIMO, Fernando. Segurança em Redes sem Fio. Rio de Janeiro.2002. Monografia (Pós-Graduação em Programa de Engenharia de Sistemas e Computação). Universidade Federal do Rio de Janeiro.

VIRINFO. **Engenharia Social**. Disponível em: < http://www.virinfo.kit.net/engesoc.htm>. Acesso em: 08 de Agosto de 2002, às 12:50 h.