Engenharia Social (ou o carneiro que afinal era um lobo)

Ricardo Pais[1], Fernando Moreira[2], João Varajão[3,4]

[1] EGP-UPBS – University of Porto Business School, Portugal
[2] Universidade Portucalense, Portugal
[3] Universidade de Trás-os-Montes e Alto Douro, Portugal
[4] Centro ALGORITMI, Portugal

ricpais@tvtel.pt, fmoreira@uportu.pt, jvarajao@utad.pt

Resumo. Todos os anos perdem-se milhares de milhões de euros devido a atos de espionagem industrial, muitas vezes sem que as organizações lesadas sequer se apercebam. As organizações devem estar alerta para esta ameaça algo silenciosa que, na quase totalidade dos casos, parte de dentro de si próprias, sob a forma de Engenharia Social. Neste capítulo exploram-se os conceitos de Engenharia Social, as suas manifestações mais populares e as formas de deteção, prevenção e combate. A importância do tema para as organizações e para a economia em geral fazem surgir a necessidade de uma sensibilização em torno destas ocorrências e para a definição de uma política de segurança clara e comum a toda a organização. A atual falta de formação e até mesmo ingenuidade dos colaboradores das organizações perante este tema proporciona um campo fértil para a proliferação de atividades da Engenharia Social.

Palavras-chave: Engenharia Social, espionagem industrial, segurança, organizações, corrupção, economia.

1 Introdução

Num passado recente, os ataques a computadores e a outros dispositivos informáticos de rede caracterizavam-se pela sua grande escala, pois tipicamente tinham como finalidade atingir o maior número de sistemas possível e causar o máximo de dano, tanto no *software* como no *hardware*. Estes ataques não eram, no entanto, movidos por qualquer objetivo específico. Com a evolução do comércio eletrónico e da própria *World Wide Web*, tem-se observado uma alteração de paradigma, dado que os ataques se estão a tornar, por um lado, mais complexos e, por outro, mais direcionados.

É neste contexto que surge a Engenharia Social. Trata-se de uma forma ilegítima de obtenção de informação sensível de um indivíduo ou de um colaborador de uma organização.

Normalmente o atacante (*hacker*, *cracker* ou simplesmente denominado por "engenheiro social") faz-se passar por uma pessoa com algum tipo de autoridade para requisitar essa informação confidencial, tendo como objetivo final aceder a sistemas (por exemplo, bases de dados).

De acordo com Kevin Mitnick, famoso *hacker* atualmente reformado e consultor de segurança, "A Engenharia Social é o uso da manipulação, engano e influência sobre um indivíduo pertencente a uma organização, para que este adira a um determinado pedido. Esse pedido poderá consistir na divulgação de determinada informação ou o desempenho de determinada tarefa que beneficia o atacante. Poderá ser tão simples quanto falar ao telefone, até algo tão complexo como fazer com que o alvo visite um determinado *website* que explore uma falha técnica e permita ao *hacker* tomar conta do computador" [Mitnick, 2002].

Um "engenheiro social" basicamente recorre ao telefone ou à Internet para enganar, levando as pessoas a ceder informação confidencial ou a quebrar ou tornear as regras de segurança instituídas.

Ao recorrer a estas técnicas, os "engenheiros sociais" aproveitam-se da tendência humana para confiar nos outros, levando a que o princípio básico utilizado pela Engenharia Social seja o de que os humanos são o elo mais fraco dos mecanismos de segurança.

A Engenharia Social é bem retratada por Hollywood nos seus filmes:

- Guerra das Estrelas: R2-D2 acede ao computador central da "Estrela da Morte" conseguindo autenticar-se no sistema e desligar o contentor de lixo, salvando assim a vida a Leia, Hans Solo e Chewbacca que lá estavam presos;
- Independence Day: Recorrendo a uma nave extraterrestre antiga como disfarce, o Capitão Steven Hiller (Will Smith) e David Levinson (Jeff Goldblum) conseguem infiltrar-se na nave-mãe extraterrestre e fazer o *upload* de um vírus que corrompe os seus sistemas, permitindo desativar as suas proteções e possibilitando um contra-ataque terrestre bem-sucedido.

O capítulo está organizado da seguinte forma: na secção 2 é realizado um breve enquadramento conceptual sobre Engenharia Social e sobre os fatores que normalmente proporcionam um terreno fértil a ataques por parte de "engenheiros sociais"; na secção 3 abordam-se diversas manifestações da Engenharia Social; a secção 4 é dedicada a defesas contra a Engenharia Social; na última seção são indicadas algumas considerações finais.

2 A Engenharia Social

Hoje, mais do que nunca, as ameaças de segurança são da maior importância para as organizações, independentemente do seu setor de atividade ou do mercado de atuação. Tal leva as organizações a empenhar-se cada vez mais na segurança dos seus sistemas, investindo na criação de melhores e mais sofisticadas defesas. Estas medidas permitem à atividade económica tornar-se mais eficaz no bloqueio de ameaças do exterior e dificultam o acesso indevido aos sistemas. A maioria das ameaças externas de segurança está bem identificada, existindo um conjunto

diversificado de técnicas e ferramentas para proteger os sistemas (por exemplo, *firewalls*, antivírus, dispositivos de controle de acesso biométrico, etc.).

No entanto, a opção de promover um controlo apertado sobre as ameaças externas deixou as organizações à mercê de um novo conjunto de riscos que não provém do exterior, mas sim do próprio interior. No "Global Security Index Report" (IBM, 2005), a IBM identifica uma tendência crescente para ataques pequenos e mais específicos em detrimento de ataques em massa tais como vírus e SPAM (mensagens de correio eletrónico não solicitado enviadas em massa). Em 2006, no relatório "Stopping Insider Attacks" (IBM, 2006), a IBM sugere que a prioridade dada aos ataques externos em detrimento dos ataques internos está errada e que esse facto está a permitir aos *hackers* explorar as fragilidades na estratégia de segurança das organizações. A Engenharia Social, pela sua simplicidade e engenho, é a forma mais fácil e eficaz de tornear os obstáculos que os sistemas de segurança impõem. Por exemplo, as vulnerabilidades na *Web* e os *Trojans* estão atualmente em destaque. Este facto é particularmente interessante, pois estes dois tipos de ameaça estão diretamente dependentes da "colaboração" dos utilizadores dado que a hipótese de sucesso está inteiramente dependente da capacidade do utilizador em conseguir identificar a ameaça. Por outro lado, práticas inseguras e roubo ou perda de computadores ou de outro suporte de armazenamento de memória têm pesado significativamente no total de incidências.

Mesmo assim, atualmente, uma parte significativa da pesquisa nesta área é feita dentro da área "técnica" da segurança de sistemas, quer ao nível da segurança de redes (*firewalls*, sistemas de deteção de intrusão, métodos de encriptação de *wireless*), como ao nível de *software* (*buffer overflows*, vírus ou *malware*). A parte "Social" da segurança dos sistemas de informação tem sido deixada para trás, como se esta não fosse essencial para o processo de proteção dos sistemas de informação. Este facto pode ser constatado quando se observa que, numa grande parte dos ataques mais recentes a organizações, o alvo têm sido os colaboradores.

As ameaças "tradicionais" têm como objetivo atingir as vulnerabilidades dos dispositivos de rede existentes na organização e que têm acesso ao exterior. Na maioria dos casos, essas vulnerabilidades deixam de ter razão de ser a partir do momento em que os dispositivos se encontram devidamente configurados e atualizados. Como exemplos, podemos referir acessos indevidos e não autorizados a redes e o *Denial of Service*. Este último tem como objetivo sobrecarregar os dispositivos de rede ou os servidores com pedidos de "serviço". Já o acesso não autorizado a redes tem por objetivo quebrar a proteção externa dos dispositivos para, de uma forma não autorizada, aceder à rede da organização.

Ambos os casos têm em comum o facto de o alvo não serem os utilizadores mas sim a organização a que pertencem. Este não é o caso das "novas" ameaças trazidas pela Engenharia Social ou os ataques "sócio tecnológicos". Estes baseiam a sua atuação principalmente na ignorância dos utilizadores acerca das políticas de segurança em geral e do real impacto dos danos que os seus comportamentos poderão causar.

Quando falamos em Engenharia Social, para que um ataque tenha sucesso, são mais as habilidades psicológicas requeridas por parte do "atacante" que ganham destaque, do que propriamente as tecnológicas. Na generalidade, pode-se observar um

conjunto de características que intrinsecamente influenciam a predisposição do indivíduo para ser alvo de práticas de Engenharia Social [Mitnick, 2002]:

- Poder e autoridade – Na maioria das situações, a autoridade não é objetiva mas, sim, uma questão de atitude. Os indivíduos dificilmente questionam a autoridade de outros que pretensamente se fazem passar por seus superiores. Desta forma é fácil para um "engenheiro social" contornar as regras simplesmente agindo como se de uma figura da autoridade se tratasse;
- Tendência natural para agradar e ser útil – Face a uma pretensa figura de autoridade, a reação mais usual é a de tentar ser afável, na expectativa de mais tarde ser recompensado e elogiado junto dos seus superiores como um indivíduo proactivo e solícito. Ao se deparar com uma pretensa figura de autoridade, que se apresenta como uma possibilidade para o indivíduo "brilhar", este irá criar todas as condições para possibilitar ao "engenheiro social" a eliminação das barreiras que se apresentam, permitindo o acesso deste à informação que pretende;
- Ligação e similaridade – "Colocar-se nos sapatos do outro" permite criar um ambiente de empatia que é favorável à troca de informação. A estranheza pode apresentar-se como uma barreira ao objetivo do "engenheiro social" daí que, seja de todo o interesse encontrar pontos de contacto com o seu interlocutor. Muitas das vezes interesses, *hobbies*, gostos em comum ou pura e simplesmente o acesso ao nome do interlocutor, são o suficiente para o "atacante" estabelecer uma ligação com este e, assim, ver o seu objetivo concretizado;
- Reciprocidade – "Fico-te a dever um favor" – A busca de benefícios futuros com base no favor prestado poderá revelar-se uma ferramenta muito útil ao "engenheiro social". Para que isto aconteça basta que este demonstre que tem potencial para criar vantagens ao interlocutor;
- Envolvimento e consistência – Na maioria das vezes, um ataque é planeado com paciência e premeditação de modo que, o "engenheiro social" procurará ambientar-se com o quotidiano tanto da organização como dos interlocutores que pretende abordar. Será assim de todo o interesse entrar na rotina das "vítimas" selecionadas e, pouco a pouco, tornar-se "invisível" à organização, ganhando assim a capacidade de poder deslocar-se dentro da mesma, de uma forma livre, sem levantar suspeitas. Isto poderá ser possível através do acesso a posições de pouco destaque e projeção, tais como pessoal de limpeza, serviço de cafetaria, serviço de cópias, serviços de entregas, segurança, entre outros;
- Baixo envolvimento – É uma atitude típica da maioria dos colaboradores dos níveis inferiores da organização e é um campo favorável para o "engenheiro social". É um ato de afastamento e desresponsabilização pessoal em relação às consequências e danos que poderão advir de determinadas ações executadas por ele próprio. Aqui o objetivo é relativizar o acontecimento, procurando levar a que o interlocutor não veja a ação como uma ameaça à organização ou ao indivíduo alvo, mas como uma ação de pouca relevância.

Em suma, o "engenheiro social" faz bem o seu "trabalho" quando a informação é extraída sem que seja levantada qualquer suspeita.

Para além dos fatores psicológicos, de acordo com Miguel Tames Arenas (2008), existe um histórico comportamental na relação entre os utilizadores e os sistemas de informação que é propício à atuação dos "engenheiros sociais". De facto, muitos dos riscos de segurança devem-se aos utilizadores, em especial à sua ingenuidade e não observância dos princípios básicos das políticas de segurança de sistemas de informação. De forma sucinta [Arenas, 2008]:

- Na generalidade dos casos, o conceito de *Spyware* é bem conhecido, embora não seja bem apreendido o conceito de *Phishing*;
- Os utilizadores que estão a par das políticas de segurança, fazem uma melhor gestão das suas *passwords*;
- Normalmente, os utilizadores não se recordam do conteúdo dos "Acordos de Utilização dos Computadores" (quando existem);
- Existe um desprezo generalizado em relação aos "Acordos de Utilização de Software" quando se trata da instalação do mesmo tanto a nível doméstico como profissional;
- A maioria dos utilizadores não se importa de ceder informação sensível acerca das suas *passwords* desde que a questão seja abordada de uma forma correta.

3 Manifestações da Engenharia Social

Como já foi referido, a maior fonte de risco para a segurança reside cada vez mais nos indivíduos de uma organização visada, do que propriamente em ameaças externas. Isto deve-se, principalmente, ao facto de muitas vezes serem os únicos elementos da cadeia de segurança com capacidade para quebrar as regras. As pessoas podem ser coagidas, enganadas, manipuladas, ou forçadas a violar algum aspeto das políticas de segurança de forma a conceder acesso de algo a alguém de forma indevida.

A maioria das soluções de segurança compreende apenas dispositivos "tecnológicos" para o combate às ameaças, existindo uma lacuna nesta área que necessita de uma abordagem diferente, assente principalmente no treino e formação dos colaboradores e na definição clara de uma política de segurança a cumprir.

A proteção contra a Engenharia Social baseia-se, assim, principalmente na formação. Treinar os colaboradores a identificar ataques e a reportar interações estranhas pode revelar-se uma defesa eficaz, para isso é necessário que toda a organização esteja desperta para uma realidade de que todos poderão ser alvo. De facto, quanto mais o indivíduo acreditar que a sua posição é irrelevante para a companhia, não se considerando um alvo, maior será a probabilidade de ser visado [Mitnick, 2002]:

Importa definir de que formas se poderá revestir um ataque/ameaça [Thapar,2007]:

- ***Spyware*** – são aplicações informáticas que recolhem informação acerca do comportamento do utilizador. Pode ser instalado num computador de diferentes formas:
    - *Trojans* – são instalados sem o consentimento dos utilizadores quando este visita *websites* que contêm determinados controlos

ActiveX ou linhas de código malicioso que explora vulnerabilidades do *browser*;
    - *Shareware* e *Freeware* em que o *Spyware* está incluído na aplicação de instalação do *software*.

  Na generalidade, o *Spyware* pode ser instalado com ou sem o conhecimento e consentimento do utilizador, poderá ou não disponibilizar informação sobre o tipo de informação que recolhe, bem como a finalidade da recolha dessa informação. Na generalidade dos casos, o tipo de informação recolhida prende-se com as moradas dos *websites* mais visitados, os motores de busca utilizados, a versão do sistema operativo, a listagem de aplicações de *software* utilizadas e o correio eletrónico. Depois da informação recolhida ser processada, é enviada a companhias terceiras que utilizam as contas de correio eletrónico e os padrões de comportamento para publicitar produtos ou para enviar correio eletrónico com conteúdo malicioso, tentando direcionar os utilizadores para *websites* falsos ou requerer a disponibilização de informação sensível (normalmente bancária);
- ***Phishing*** **–** Pode ser descrito como a tentativa de aceder, de forma fraudulenta, a informação financeira ou pessoal. Normalmente estes tipos de ataques são iniciados por correio eletrónico, chamadas telefónicas ou mensagens instantâneas, fazendo-se o atacante passar por um colaborador legítimo ou uma pessoa/instituição credível. Existe uma diferença muito ténue entre as técnicas de *Phishing* e de Engenharia Social. Na maioria das vezes as duas definições cruzam-se. Se, por um lado, o *Phishing* tem um âmbito muito mais alargado, por outro lado, recorre na maioria dos casos a técnicas de Engenharia Social para atingir os seus objetivos;
- ***Spear Phishing*** – É uma técnica relativamente nova que não recorre a ataques maciços como o *Phishing*, mas sim a ataques focados. O objetivo é fazer com que o utilizador acredite que a fonte do correio eletrónico é alguém de confiança de dentro da mesma organização ou com algum tipo de autoridade. Por outro lado, enquanto o objetivo do *Phishing* é roubar informação do indivíduo, o *Spear Phishing* procura o acesso ao sistema de informação ao qual o utilizador está ligado. Este foco tão específico torna o *Spear Phishing* muito mais perigoso que o *Phishing* comum, logo sendo provavelmente mais utilizado para ataques visando obter ganhos económicos, segredos ou informação militar;
- ***Spy-Phishing*** – É um ataque que consiste no envio de um correio eletrónico ou de um *link* do atacante para o alvo. Este contém um código (*software*) que, quando executado, se instala e fica a monitorizar o tráfego de dados até que o utilizador-alvo visita um *website* específico. Quando o utilizador chega a esse destino, o *software* torna-se ativo, rouba a informação de *log in* ou outra informação sensível e envia-a para o atacante;
- ***Footprinting*** – Trata-se basicamente do ato de recolher informação. É normalmente efetuado para investigar um alvo pré-determinado e explorar as melhores oportunidades para o abordar. O *Footprinting* pode incluir desde chamadas telefónicas simulando uma personagem fictícia que coloca questões aparentemente inocentes até à análise detalhada da planta de um edifício ou de *data centers*;

- **Engenharia Social por telefone** – Apesar da proliferação da *Web*, o meio mais comum para ataques de Engenharia Social continua ainda a ser o telefone, uma vez ser o meio de comunicação impessoal que permite uma maior interação Social. Por exemplo, pode ser efetuada uma chamada imitando alguém com autoridade reconhecida dentro da instituição e gradualmente vai-se retirando informação do colaborador. Os alvos preferenciais para este tipo de ataques são os serviços de apoio ao cliente;
- ***Dumpster Diving*** – Também apelidado de *trashing*, o *dumpster diving* é outro método popular de Engenharia Social. Uma quantidade enorme de informação pode ser recolhida através da análise do lixo da empresa, podendo representar fugas de segurança. Como exemplos temos listas telefónicas da empresa, organigramas, manuais de procedimentos, calendários com anotações de reuniões, eventos e férias, manuais de sistemas, impressões de informação sensível (por exemplo, dados de *login* e *passwords*), disquetes, cassetes, papel timbrado, formulários de memorandos ou *hardware* ultrapassado, entre outros;
- **Engenharia Social Inversa** – Trata-se de um método avançado de aceder a informação ilicitamente. Acontece quando o "engenheiro social" cria uma *persona* que parece desempenhar um papel de relevo na organização. Os colaboradores pedem a esta *persona* informação (ao invés de lhe ceder). Quando esta técnica é bem explorada, planeada e executada permite ao "engenheiro social" obter mais facilmente informação valiosa dos colaboradores. Um processo de Engenharia Social Inversa passa por três fases: A sabotagem, o anúncio e a assistência. Por exemplo, o "engenheiro social" sabota a rede criando problemas de acesso; anuncia que ele é a pessoa indicada para resolver esta falha, sendo para tal necessário requer determinado acesso a informação sensível conseguindo o que pretendia inicialmente. Desta forma os colaboradores nunca pensarão que se trata de uma quebra de segurança devido a um ataque pois o seu problema é resolvido e todos voltam à sua rotina.

É curioso notar que na *Wikipedia*[1] se encontra, para além do famoso *hacker* Kevin Mitnick, a história recente que recorda outros grandes "engenheiros sociais" tais como os irmãos Badir (Ramy, Muzher e Shadde), cegos à nascença, que desenvolveram uma fraude telefónica e informática em Israel. Nos anos 1990 eles recorreram à Engenharia Social, através de dissimulação vocal e computadores com interface Braille. Outras referências são Frank Abagnale, Dave Buchwald, David Bannon, Peter Foster, Stanley Mark Rifkin e Steven Jay Russell.

Em suma, é necessário efetuar uma reflexão profunda acerca da própria cultura organizacional procurando fundamentalmente responder às seguintes questões:

- Qual é a importância da formação na prevenção das violações das regras de segurança?
- Como evitar ataques de Engenharia Social e ameaças internas?
- Como é que o ambiente organizacional afeta a forma como os utilizadores reagem a estas ameaças?

Na secção seguinte abordam-se algumas respostas para estas questões.

[1] http://en.wikipedia.org/wiki/Social_engineering_(security)

4 Defesas contra a Engenharia Social

Qual é a importância da formação na prevenção das violações das regras de segurança?

A maioria das vulnerabilidades que criam oportunidades para ataques por parte dos "engenheiros sociais" pode ser facilmente ultrapassada proporcionando aos utilizadores formação adequada no que respeita ao tratamento de informação empresarial (e mesmo pessoal), de forma a criar políticas de segurança internas para a gestão dos ativos empresariais (e pessoais). A ideia é que os utilizadores tenham a noção das técnicas usadas pelos atacantes e, mais importante ainda, desenvolver neles a perceção de que a segurança da informação é parte integrante do seu papel na organização. Por outro lado, é fundamental que tenham consciência que este mal existe e, mesmo se a organização não estiver ligada a nenhum sector de atividade sensível ou vulnerável, ela poderá mesmo assim ser alvo de ataques. Os colaboradores têm de ser formados sobre qual a informação que precisa de ser salvaguardada e como essa salvaguarda deve ser feita. A partir do momento em que houver essa interiorização, estarão numa posição muito melhor para reconhecer este tipo de ataques.

Como evitar ataques de Engenharia Social e ameaças internas?

A melhor forma que as organizações têm para proteger a sua privacidade contra os ataques dos "engenheiros sociais" é formar as suas equipas sobre o uso adequado das políticas de segurança. Esta formação tem como principais objetivos:

- Criar uma "*Firewall* Humana" – as quebras de segurança por parte dos colaboradores está-se a tornar no maior risco de segurança do século XXI. No entanto, a maioria das organizações ignora a sua maior fonte de exposição – a componente humana;
- Defender o lado humano da Segurança – necessidade de se estabelecer uma cultura de segurança na organização;
- Realizar auditorias de vulnerabilidade a ataques de Engenharia Social – no sentido de perceber o nível de fragilidade da companhia, através da análise:
    - Da informação da organização que está abertamente disponível,
    - Das políticas e procedimentos de segurança estabelecidos,
    - Do tráfego telefónico,
    - Do tráfego de correio eletrónico e das pesquisas na Internet,
    - Do comportamento dos colaboradores,
    - Do nível geral de segurança das instalações;
- Desenvolver procedimentos de resposta a crises – quando existe quebra de segurança, é importante que a resposta da organização seja rápida e eficaz de forma a:
    - Perceber exatamente como é que a quebra de segurança ocorreu,
    - Determinar o impacto que terá,
    - Prever os próximos passos que o "engenheiro social" dará,

    - Promover a consciencialização dos colaboradores sobre como dar resposta à quebra corrente e a futuros ataques por parte do "engenheiro social";
- Detetar a intrusão por parte de "engenheiros sociais" – através da implantação de sistemas de monitorização de várias fontes de risco potencial (correio eletrónico, telefone, mensagens instantâneas, *World Wide Web*, *wireless*, e infraestruturas) que permitam o *drill-down* de uma visão geral até um incidente isolado.

Para além da parte formativa, é necessário definir, com clareza, uma política de segurança na empresa. Uma política é definida como um conjunto de regras e regulamentos definidos pela organização em consonância com a lei geral, regulação sectorial e decisões dos administradores da empresa. As políticas poderão variar de empresa para empresa, mas na generalidade incluem linhas orientadoras, objetivos, comportamentos e responsabilidade dos utilizadores. Na maior parte dos casos, as políticas são seguidas por instruções e procedimentos. A importância das políticas de segurança reside no facto da maior parte das organizações tentar assegurar as suas operações instalando tantos dispositivos de segurança quanto possível (criando uma falsa sensação de segurança), enquanto que as políticas e procedimentos que esses dispositivos necessitam para serem implementados com sucesso ficam por aplicar. De acordo com Chad Perrin[2], um passo importante para que uma política de segurança tenha sucesso é que ela seja desenvolvida juntamente com os utilizadores e não contra eles.

Como é que o ambiente organizacional afeta a forma como os utilizadores reagem a estas ameaças?

Na maioria dos casos, quando os utilizadores não seguem as políticas, não é porque não quererem seguir as regras, mas sim porque, no desejo de melhor executar a sua função, consideram que estas regras e procedimentos atrasam o seu desempenho e representam uma barreira à execução da mesma, em vez de as considerarem como ferramentas úteis para o cumprimento dos seus objetivos diários. A solução é simples: não ignorar as necessidades dos utilizadores finais aquando do desenho e implementação de uma política de segurança. Quando os departamentos de sistemas de informação se recusam a dar soluções para os problemas dos utilizadores, estes têm de procurar soluções noutras fontes, e é desta forma que a maioria das regras de segurança se quebra.

Apesar da enorme ameaça que a Engenharia Social coloca, pouco tem sido feito para lhe ser atribuída a devida importância. A principal razão para a falta de discussão acerca do tema está intrinsecamente ligada com a vergonha, uma vez que a maior parte das vítimas vê a Engenharia Social como um ataque à sua inteligência e capacidade (ninguém quer ser considerado ingénuo ou ignorante por ter sido enganado). É por esta razão que a Engenharia Social continua "escondida na gaveta" como um assunto tabu, embora qualquer pessoa seja passível de ser atingida por um ataque.

---

[2] Chad Perrin, "Work with End Users, not against them, to improve security": http://blogs.techrepublic.com.com/security/wptrackback.php?p=290

Encontrar exemplos destes ataques é difícil. As organizações visadas, ou não querem admitir que foram vítimas de um ataque (pois ao admitir uma quebra de segurança para além de embaraçoso, é danoso para a sua imagem e reputação) ou o ataque não foi bem documentado e ninguém sabe ao certo se foram mesmo sujeitos a um ataque.

Cabe, assim, à comunidade académica e profissional o desenvolvimento de mais investigação nesta área, de forma a dar mais exposição ao tema. Parte da investigação também tem de ser direcionada para perceber quais as motivações que estão por detrás da atuação dos "engenheiros sociais". É importante "entrar na mente" do "engenheiro social" e saber se a sua motivação é originada pelo desafio intelectual, pela necessidade de afirmação político-social, para obter acesso a informação sensível, simples curiosidade, ou qualquer outro motivo.

5 Conclusão

No quotidiano das sociedades modernas as questões da segurança tornaram-se um imperativo. Contudo, muitas organizações esquecem-se dessa questão que são muitas vezes os seus próprios recursos humanos o centro da maior parte das quebras de segurança. Neles, a Engenharia Social encontra um terreno amplo para proliferar, recorrendo a técnicas mais ou menos complexas que têm na maioria dos casos uma intenção maliciosa promovida pelo valor que essa informação poderá ter no mercado.

É por isso necessário implementar práticas de segurança eficazes que permitam lidar com este problema. De notar que não se defende a criação de um "sistema policial" ao qual a liberdade e privacidade de cada indivíduo estejam subjugadas, mas sim um conjunto de procedimentos que orientem a relação do indivíduo com a informação, para que esta seja utilizada de forma consciente e responsável. Não podemos também esquecer que o fator humano é essencial para os sistemas de informação, pois sem ele desaparece o bom senso e o juízo crítico, que são fatores essenciais para a tomada de decisão. Isto também implica que a ameaça é universal, qualquer que seja o *hardware* ou *software* utilizado. A solução passa por mais investigação sobre o tema, uma subsequente e progressiva consciencialização para a ameaça que representa, com o intuito que todos tenham um papel ativo na implementação de políticas de segurança. Esta tomada de consciência pode ser alcançada através de programas de formação contínua, que procurem promover um maior conhecimento por parte do indivíduo acerca das técnicas utilizadas, medidas a adotar e precauções a tomar, mas sem sobrecarregar as suas tarefas diárias. São muitas as técnicas utilizadas, desde o *Spyware*, passando pelo *Footprinting*, até ao *Dumpster Diving*, mas a mais eficaz é, sem dúvida, o aproveitamento da ingenuidade que caracteriza o ser humano e que é alimentado pela ignorância. Esta representa atualmente o maior desafio para os sistemas de segurança e ao mesmo tempo a maior oportunidade contra a Engenharia Social.

Referências

Arenas, M., Master Thesis on 'Social Engineering and Internal Threats in Organizations', Blekinge Institute of Technology, Sweden (2008).

Barman S., "Writing Information Security Policies", New Riders (2001).

http://en.wikipedia.org/wiki/Social_engineering_(security). Consultado em 6 de Julho 2009.

Dhamija R., Tygar J., Hearst M., "Whitepaper on 'Why Phishing Works'", Harvard University, University of California (2006).

Granger, S. "Social engineering reloaded", Security Focus (2006).

Hamlen K., Mohan V., Mohammad M., Khan L., Thuraisingham B. "Whitepaper on 'Exploiting an Antivirus Interface'", University of Texas (2009).

Jones C., "Social Engineering: Understanding and Auditing", GSEC, SANS Institute (2004).

Mitnick, K., Simon, W., Wozniak, S., "The Art of Deception", John Wiley & Sons (2002).

Olzak T., "Whitepaper on 'A Practical Approach to Managing Information System Risk'" (2008).

Qin, T., Burgoon, J. "Whitepaper on 'An investigation of heuristics of human judgment in detecting deception and potential implications in countering Social engineering'", University of Arizona, Tucson (2007).

Thapar Ashish. "Whitepaper on 'Social Engineering - An attack vector most intricate to tackle!'", www.infosecwriters.com (2007).