Engenharia Social – Explorando o Medo

Inaldo Marques Monteiro

Divisão de Pós-Graduação Universidade de Fortaleza (UNIFOR) – Fortaleza, CE – Brasil.

inaldomonteiroti@gmail.com

Abstract. *This article aims to present the Social Engineering and show the techniques used to extract information from people and organizations. The article also aims to generate interest and awareness of people and organizations for this imminent danger, show how the emotional conditions of human beings are constantly affected when subjected to stress. The social engineer has as primary target explore this dynamic of human beings and their vital emotions to extract information from him or privileges. Of the various human emotions examine in more detail the fear and some cases of exploitation of this extremely vital sense to humans.*

Resumo. *O presente artigo tem como objetivo principal apresentar a Engenharia Social e mostrar as técnicas utilizadas para extrair informações de pessoas e organizações. O artigo também tem como objetivo despertar o interesse e a conscientização das pessoas e das organizações para esse perigo eminente, mostrar como as condições emocionais dos seres humanos são constantemente afetadas quando submetidos a estresse. O engenheiro social tem como alvo primário explorar essa dinâmica do ser humano e suas emoções vitais para extrair dele informações ou privilégios. Das várias emoções humanas examinaremos de forma mais detalhada o medo e alguns casos de exploração desse sentimento extremamente vital ao ser humano.*

Introdução

Quando observamos a vida como uma estratégia para se alcançar aquilo que desejamos. A engenharia social nos apresenta um conjunto de técnicas onde se exploram falhas humanas em organizações. Atua em um sistema que possuem características comportamentais e psicológicas na qual podemos obter informações sensíveis e privilegiadas.

Os engenheiros sociais estão percebendo que os sistemas e as redes estão cada vez mais seguras, porém o ser humano continua sendo o elo mais fraco da corrente. Devido à falta de treinamento e aos ambientes corporativos inseguros e competitivos os seres humanos se tornam marionetes na mão dos manipuladores sociais. A trama é séria e mesmo uma pessoa dotada de muita inteligência pode ser vítima. Só para dar uma noção da dimensão do problema, muitos cibercriminosos atingem seus objetivos através de técnicas de engenharia social. E tudo porque o humano é um ser que, ao contrário dos computadores, é constantemente afetado por aspectos emocionais.

As condições emocionais dos seres humanos são constantemente afetadas por aspectos como estresse e relações afetivas. O engenheiro social tem como alvo primário explorar essa dinâmica do ser humano e suas emoções vitais para extrair dele informações ou privilégios. Essas informações geralmente tem grande valor e bem utilizadas agregam valor a quem as detém.

"Os engenheiros sociais habilidosos são adeptos do desenvolvimento de um truque que estimula emoções tais como medo, agitação, ou culpa. Eles fazem isso usando os gatilhos psicológicos – os mecanismos automáticos que levam as pessoas a responderem as solicitações sem uma análise cuidadosa das informações disponíveis." (MITNICK, 2003, p.85).

"A proteção para os ataques envolve o treinamento nas políticas e procedimentos, mas também – e provavelmente mais importante – um programa constante de conscientização. Algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização." (MITNICK, 2003, p.195).

1. A engenharia social e a sociedade moderna.

Vivemos atualmente na sociedade da informação e do conhecimento. As organizações e a própria ONU costuma chamar de "Nova economia mundial" este novo modelo de organização das sociedades. A informação como meio de criação do conhecimento, desempenha um papel fundamental na produção de riquezas, contribuindo para o bem-estar e a qualidade de vida das pessoas. O modo como às pessoas começaram a se comunicar e buscar informações mudou muito, principalmente no que diz respeito às tecnologias por trás desta comunicação. Em um mundo onde somos dependentes economicamente e socialmente, existe a necessidade de trocar, conectar e compartilhar informações. Sem a possibilidade de comunicação entre os grupos, a sociedade adoece e entra em colapso porque o ato da troca é fundamental para a continuidade da vida. Não estamos somente falando da sobrevivência, mas de empregabilidade e de negócio.

De acordo com Fontes (2008): "A informação, independente de seu formato, é um ativo mais importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos". As empresas possuem informações que são consideradas vantagens competitivas, um diferencial para o negócio.

Quanto aos ambientes das empresas, a segurança, muitas vezes, gira em torno de prevenir vulnerabilidades nas instalações tecnológicas, nos acessos físicos a estas instalações, e como as pessoas frequentam os ambientes ou manuseiam os ativos de informação. Isso gera um custo muito alto de investimento, porém, ainda permanece sem o devido controle uma peça importante, o próprio ser humano. Segundo Mitnick (2003):

> Só existe uma maneira de manter seguros os seus planos de produto: ter uma força de trabalho treinada e consciente. Isso envolve o treinamento nas políticas e procedimentos, mas também é provavelmente mais importante um programa constante de conscientização. Algumas

> autoridades recomendam que 40% do orçamento geral para segurança da empresa seja aplicado no treinamento da conscientização.

Hoje conseguimos perceber que a informações é a alma das organizações. Elas estão nos papéis, armazenadas eletronicamente e são transmitidas em conversas, meios digitais e nas diversas relações diárias. Dada a sua importância, nasce a necessidade de se estabelecer uma política de segurança de informações abrangente. Precisando garantir a confidencialidade, integridade e disponibilidade das informações tanto pessoais quanto corporativas.

Tratando-se de engenharia social, o fator humano, é tão importante quanto o tecnológico e em algumas situações, até mais vulnerável por falta de conscientização ou de uma política que dê mais relevância a fatores que envolvem Segurança da Informação.

Podemos fazer analogias da engenharia social com a habilidade humana em manipular, que basicamente é convencer alguém de algo, e também dissimular, que significa fingir, fazer parecer diferente, encobrir, disfarçar. Com objetivo de obter informação privilegiada. Alguém manipulador não necessariamente o faz para o mal e caberá a pessoa a qual se tentou manipular, avaliar a situação. Para que haja alguém manipulando precisa haver alguém que se deixe manipular.

"Geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica. Possuindo uma conversa bastante envolvente." (ARAUJO, 2005, p.27).

"Uma empresa pode gastar centenas de milhares de dólares em firewalls, sistemas de criptografia e outras tecnologias de segurança, mas se um cibercriminoso engana uma pessoa de confiança dentro da empresa, todo esse dinheiro investido não servirá para nada", advertiu Kevin Mitnick.].

Para a ABNT NBR ISO/IEC 17799:2005 (2005, p.ix), "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

"Em primeiro lugar, muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança da informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema". (CAMPOS, 2007, p.29)

A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais. Segundo Campos (2077, p. 17), "um sistema de segurança da informação baseia-se em três princípios básicos: confidencialidade, integridade e disponibilidade.".

2. As emoções e o comportamento humano.

Embora pareça que tem uma grande distância entre a psicologia e o cibercrime, a realidade é que ambos se baseiam nos mesmo princípios. O desejo de cada pessoa por reciprocidade (se eu faço um favor espero que você faça outro para mim), por aprovação social (você acredita no

julgamento da maioria), por autoridade (ou seja, confiar em um policial, um médico, um técnico, etc) e muitos outros são formas universais de começar a construir um relacionamento com alguém e assistir às nossas necessidades humanas básicas. Um engenheiro social sabe que botões apertar para obter a resposta desejada a partir de nós, criando um contexto que permite que uma história inventada para ser crível permita a ele controlar o sentido de urgência e de tempo de toda a interação com a vítima. Não podemos esquecer que somente pessoas realmente inteligentes em uma fração de segundo são capazes de conseguir o que buscam.

A emoção tanto pode ser construtiva como destrutiva; tanto fortalecedora como debilitadora. (Hebb, 1971: 200)

Todos estes estados possuem pontos em comum. Todos eles constituem estados de motivação e vigilância. Esses estados (que por sua vez geram comportamentos) produzem emoções que podem afetar gravemente os processos que controlam a conduta organizada. (Hebb, 1971: 201)

Portanto, podemos resumir que a emoção está diretamente correlacionada com a vigilância. A emoção ou vigilância é motivadora até o ponto em que atividades conflitantes do córtex comecem a interferir entre si, evitando o domínio de uma atividade que possa produzir uma série de respostas organizadas à situação. (Hebb, 1971: 201)

É importante salientar que, a engenharia social é aplicada em diversos setores da segurança da informação independente de sistemas computacionais, software e ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social.

A questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam. (SILVA, M.; COSTA, 2009)

Dentre esses comportamentos, pode-se destacar:

• Formação profissional: O ser humano busca valorizar sua formação e suas habilidades adquiridas nesta faculdade, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal buscando o reconhecimento pessoal inconscientemente em primeiro plano.

• Vaidade pessoal e/ou profissional: O ser humano costuma ser mais receptiva a avaliação positiva e favorável aos seus objetivos, aceitando basicamente argumentos favoráveis a sua avaliação pessoal ou profissional ligada diretamente ao benefício próprio ou coletivo de forma demonstrativa.

• Vontade de ser útil: O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário. • Busca por novas amizades: O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.

• Autoconfiança: O ser humano busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou individuo.

• Propagação de responsabilidade: Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.

• Persuasão: Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

2. Explorando o Medo

Falar sobre medo é algo muito complexo, tendo em vista a singularidade do ser humano e a infinidade de fatores psicológicos capazes de desencadeá-lo.

A relevância deste artigo se dá pelo fato de abranger um tema que emerge em rodas de conversa, nos noticiários nacionais e internacionais e em todas as faixas etárias e pode de certa forma, implicar negativamente no convívio social. O medo que apavora, paralisa, impede e angustia que muitas das vezes se apresenta como queixa nos consultórios de psicólogos.

Segundo Dalgalarrondo (2006) apud Mira y López (1964), o medo se apresenta em escalas até a sua inativação, ou seja, ele vai paulatinamente tomando uma proporção até que o indivíduo tenha seus sentimentos e emoções estabilizados, dividindo-se em seis fases de acordo com o grau de extensão e imensidão, são eles: 1. Prudência; 2. Cautela; 3. Alarme; 4. Ansiedade; 5. Pânico (medo intenso); 6. Terror (medo intensíssimo).

Nessa abordagem mostraremos como o engenheiro social pode explorar essa emoção profundamente. Eles fazem isso usando os gatilhos psicológicos – os mecanismos automáticos que levam as pessoas a responderem as solicitações.

A função adaptativa do medo ajuda os organismos a enfrentar questões de sobrevivência postas pelo ambiente. Certos estados psicológicos e sociais podem perturbar a ação alterando e enviesando a maneira de pensar em face de determinados contextos que podem ser recordações do passado, ou situações presentes relativas a insucessos, fracassos e receios de acontecimentos que transtornem a vida pessoal, familiar e social dos sujeitos.

Atualmente há sistemas de manipulação através do medo cada vez mais elaborados. Tudo o que tememos prende a nossa atenção, que nesse sentido nos é intencionalmente fornecidas, de modo a agirmos quando uma determinada situação ocorrer.

Segue alguns casos de ataques que exploraram o medo de forma criminosa.

Caso 1 – Sequestro Virtual

Um golpe comumente conhecido como “seqüestro virtual”. Usa táticas de telemarketing da engenharia social. Eles afirmam que um membro da família da vítima foi raptada e um resgate deve ser pago para garantir sua segurança e liberdade. Na maioria das vezes, mesmo sem a confirmação do sequestro, a vítima termina pagando o resgate. Na região, onde estes tipos de crimes são comuns, os cibercriminosos exploram as fraquezas humana (urgência e medo) para obter lucro.

Além disso, é importante ter em mente que qualquer informação que você publicamos na rede (Facebook, Twitter, Foursquare, etc) pode ser uma pista fantástica para os cibercriminosos, fornecendo informações valiosas e tornando a vida deles mais fácil. Até mesmo uma lista de favoritos na Amazon poderia ser a porta de entrada para um épico truque de engenharia social.

Caso 2 - Terrorismo

Sendo o terrorismo entendido pela sociedade como um fenómeno aleatório, normalmente incompreensível e incontrolável, constata-se que os seus efeitos são normalmente catastróficos e afectam muitos inocentes. Independentemente das motivações políticas que estiverem na sua origem, os atentados terroristas pretendem sempre provocar o terror e o medo, aí residindo a raiz do seu impacto e poder.

A Internet tem vindo a constituir um autêntico campo de batalha digital sendo palco de ações de retaliação entre hackers associados a diversos países e atores estratégicos como Israel e a Palestina, Taiwan e a China, Paquistão e a Índia ou Estados Unidos e a China.

Tabela 1 - Probabilidade de Ocorrência das Ações de Guerra de Informação

Actividades de Guerra de Informação		Probabilidade de Ocorrência	Observações
Ofensivas	Destrutivas (foco alargado)	Moderada	Circunscrita a poucos Países.
	De Contenção	Idem	Idem.
Defensiva	Destrutivas (foco alargado)	Reduzida	Custa biliões e requer uma coligação de Países.
	De Contenção	Moderada	Circunscrita a poucos Países.
	Preventivas	Moderada	Os EUA já iniciaram esta estratégia em resultado dos Ataques de 11Set01.
Terroristas	De Contenção	Elevada	Vários grupos terroristas.
	Preventivas	Idem	Idem.
Criminosas	Contínuas	Muito Elevada	Actividades subversivas.
	Aleatórias	Elevada	Organizações Criminosas.
	Amadoras	Moderada	Pequenos Grupos ou Actores Individuais.

Fonte: Erbschloe (2001)

O ciberterrorismo poderá assim ser considerado uma ameaça, de impacto futuro mais consistente do que o que atualmente apresenta, posicionando-se como uma ferramenta auxiliar de importância crescente para o terrorismo transnacional.

Caso 3 – Extorsão pela internet.

Nome, idade e fotos falsas, endereço virtual instigante e misterioso (gatinhamanhosa@…): com esses atributos uma mulher conseguiu atrair um internauta, que caiu no "conto da chapeuzinho vermelho" e acabou extorquido em cerca de R$ 15 mil. A sorte da mulher, também, foi temporária: presa em flagrante, foi identificada e denunciada pelo MPDFT à Justiça local. Em 1ª Instância, o juiz da 7ª Vara Criminal de Brasília a condenou por estelionato e extorsão à pena de 9 anos, 4 meses e 15 dias de reclusão, em regime fechado. Em grau de recurso, a 2ª Turma Criminal a absolveu pelo crime de estelionato, mas manteve a condenação por extorsão, cuja pena definitiva ficou em 6 anos de reclusão, em regime semiaberto.

De acordo com a denúncia do MP, os fatos ocorreram no período de maio a julho de 2010, quando a vítima (do sexo masculino, idade > 40, casado) conheceu a denunciada em uma sala de bate-papo do provedor UOL. Ela se identificou como Amanda, 22 anos, nick name: gatinhamanhosa. Os encontros virtuais eram, a princípio, através de MSN, depois por e-mails, ligações e mensagens telefônicas. Fotos sensuais foram trocadas e por diversas vezes o internauta tentou marcar um encontro presencial, mas a "gatinhamanhosa" se esquivava.

Passado algum tempo, a idade dela mudou. Confessou, meio constrangida, que tinha apenas 19 anos. Contou que passava por dificuldades financeiras, pois não tinha mãe e morava com pai bravo e avó doente. O homem, solícito, ofereceu-lhe dinheiro. O primeiro depósito, segundo afirmou em depoimento, foi espontâneo. Depois vieram outros a pedido da "gatinha". De maio a junho de 2010, ele depositou R$ 5.060,00 para a moça numa conta na Caixa Econômica Federal. Depois, cansado das desculpas e dos encontros desmarcados, o homem informou que não faria mais depósitos. Foi então, que as extorsões começaram.

A moça de supostos 19 anos decidiu abrir o jogo: "Tinha 16 e ia contar para todo mundo que o homem era pedófilo!" As chantagens começaram e o internauta depositou na conta dela, de 2 de julho a 20 de julho, mais R$ 10 mil, sob pena de ser denunciado à polícia e à esposa. O homem recebeu diversas ameaças, não só da mulher como de comparsas. Amedrontado, decidiu, ele mesmo, procurar ajuda em uma delegacia. O flagrante foi armado no Shopping do Valparaíso, local da agência bancária na qual os depósitos eram efetuados. A mulher foi presa em flagrante: Francisca, 40 anos de idade.

O processo contra ela tramitou na 7ª Vara Criminal de Brasília. Em depoimento, a ré confessou a versão contada pelo internauta. Na sentença condenatória, o juiz afirmou: "É clarividente que a acusada se utilizou de artifício (falsa identidade, fotos que não eram suas, idade alterada) e das tragédias familiares que simulou para induzir a vítima em erro. Embora o ofendido tivesse interesse em obter vantagem sexual, especialmente motivado pela boa impressão que tinha da suposta aparência da acusada, sua conduta não tem reprovação jurídica". A conduta dela tinha: estelionato e extorsão, cujas penas somaram 9 anos, 4 meses e 15 dias de reclusão. Insatisfeita a mulher recorreu.

Ao analisarem o recurso, os desembargadores da Turma esclareceram que o estelionato não ficou configurado: "O crime de estelionato pressupõe uma vontade viciada da vítima, que entrega a coisa espontaneamente; o ofendido se equivoca quanto à realidade fática. No caso em questão, qualquer pessoa que frequente sala de bate papo ou sítios de relacionamentos na internet sabe que, nem sempre as informações passadas em tais redes sociais são condizentes com a verdade".

Nº do processo: 2010011135977-5

Caso 4 – Chantagem e Tortura.

Sexo, chantagem e internet. O suicídio de duas adolescentes depois do vazamento de imagens íntimas acordou o Brasil para os perigos da exposição nas redes sociais. Faltam leis para punir quem divulga vídeos e fotos. Falta controle das empresas

Elas haviam descoberto que imagens íntimas delas, compartilhadas com pessoas em quem confiavam se multiplicavam pela internet. Envergonhadas e desesperadas, totalmente inexperientes, decidiram fugir de uma situação que lhes parecia intolerável. Ao escolher o suicídio, tornaram-se vítimas, mais um par de vítimas, de um perigo assustadoramente próximo da nova geração: a exposição excessiva na internet, e suas terríveis consequências.

O criminoso que deteve as imagens chantageava as vitimas torturando as psicologicamente. O que ocasionou uma atitude extremista das vítimas.

Caso 5 – A estratégia da distração e da culpa

O elemento primordial do controle social é a estratégia da distração que consiste em desviar a atenção do público dos problemas importantes e das mudanças decididas pelas elites políticas e econômicas, mediante a técnica do dilúvio ou inundações de contínuas distrações e de informações insignificantes. A estratégia da distração é igualmente indispensável para impedir ao público de interessar-se pelos conhecimentos essenciais, na área da ciência, da economia, da psicologia, da neurobiologia e da cibernética.

"Manter a atenção do público distraída, longe dos verdadeiros problemas sociais, cativada por temas sem importância real. Manter o público ocupado, ocupado, ocupado, sem nenhum tempo para pensar; de volta à granja como os outros animais"

Fazer o indivíduo acreditar que é somente ele o culpado pela sua própria desgraça, por causa da insuficiência de sua inteligência, de suas capacidades, ou de seus esforços. Assim, ao invés de rebelar-se contra o sistema econômico, o individuo se auto desvalida e culpa-se, o que gera um estado depressivo do qual um dos seus efeitos é a inibição da sua ação. E, sem ação, não há revolução.

O seguinte documento, datado de Maio de 1979, foi encontrado em 7 de Julho de 1986 numa copiadora IBM comprada em leilão de equipamentos militares - Armas Silenciosas para Guerras Tranquilas

3. Conclusão

No decorrer deste trabalho, observou-se que as técnicas de Engenharia Sociais são capazes de atingir as pessoas e as organizações de forma ameaçadora. Entendemos também que o conhecimento de Engenharia Social pode ser usado para o bem e para o mal.

O estudo das emoções é muito importante com relação a nossa sobrevivência enquanto seres Humanos. Se não mantivermos nossas emoções bem estruturadas, nossas chances de sobrevivência ficam bem reduzidas. Somos seres com uma biologia elaborada e de emoções bem refinadas como medo, ansiedade, culpa. Mas é imprescindível que essas atividades emocionais sejam harmonizadas e equilibradas com o uso da racionalidade e do pensamento analítico e investigativo. Cultivando a tolerância e respeitando as diferenças individuais, a fim de termos

um convívio pacífico, teremos todas as chances possíveis para sobreviver em épocas tão difíceis quanto as que nos aguardam no futuro.

A maior parte dos desastres e incidentes com a segurança das informações tem como fator predominante a intervenção humana. 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.

4. Referências

Associação Brasileira de Normas Técnicas (ABNT). NBR ISO/IEC 27002:2005 – Tecnologia da informação – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005.

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.

Figueiró, T. (2010) "O ser humano è o elo mais fraco na segurança da informação" http://www.computerworld.com.pt/2010/03/16/o-ser-humano-e-o-elo-mais-fraco-na seguranca-da-informacao/. Acesso em: 29/07/2014.

Fontes, E. (2008). Praticando a Segurança da Informação. Rio de Janeiro: Brasport, 1ª Edição.

Mann, I. (2008). Engenharia Social. São Paulo: Blucher.

Mitnick, K. D. e Simon, W. L. (2003). A Arte de Enganar. São Paulo: Pearson Education do Brasil.

Silva, V. L. (2012) "Como proteger-se de ataques de Engenharia Social?" http://www.brasiladmin.com/index.php?option=com_content&view=article&id=156: como-proteger-se-de-ataques-de-engenharia-social&catid=55:seguranca-da informacao&Itemid=58. Acesso em: 29/07/2014.

http://blog.kaspersky.com.br/engenharia-social-hackeando-humanos/