ENGENHARIA SOCIAL: O ELO MAIS FRÁGIL DA SEGURANÇA NAS EMPRESAS

Clayton Silvestre da Silva [1], Adriano Carlos Moraes Rosa [2], Daniel Faria Chaim [3], Roberto José Carvalho [4], Vanessa Cristhina Gatto Chimendes[5]
[1,2,3,4,5]Fatec Guaratinguetá
clayton-fatec@live.com, adriano.carlos.rosa@gmail.com,
chaim@fatecguaratingueta.edu.br, robertjc@uol.com.br,
vanessa@fatecguaratingueta.edu.br

Resumo
A tecnologia se mostra como fator de sucesso para muitas empresas. Atualizar equipamentos e sistemas de segurança demanda muita atenção e conhecimento de área. Mesmo com um sistema de segurança atualizado empresas ainda se defrontam com um grande problema detectado já por alguns anos no mercado: vulnerabilidade em relação aos ataques da engenharia social, profissionais que buscam romper a tecnologia de segurança para ganhos próprios. Este trabalho objetiva questionar se as pessoas que manipulam tais sistemas possuem atributos para fazê-lo da melhor forma como também, informar a todos os interessados que a segurança vai além dos equipamentos e que a capacidade humana de persuadir o próximo para conseguir o se quer pode trazer grandes danos. A engenharia social pode ser o elo mais fraco da segurança de dados e informações confidenciais.

Palavras-chave: Engenharia Social. Pessoas. Segurança. Sistema. Tecnologia.

Abstract
The technology shows up as a success factor for many companies. Upgrade equipment and security systems demand much attention and knowledge of the area. Even with an upgraded security system companies still face a big problem detected for some years on the market: vulnerability to social engineering attacks, professionals seeking to break the security technology for their own gains. This work aims to question whether people who manipulate such systems possess attributes to make it as best as also inform all stakeholders that security goes beyond the equipment and the human ability to persuade the next to get what you want can bring great harm. Social engineering may be the weakest link in the security of sensitive information and data.

Keywords: Social Engineering. People. Security. System. Technology.

1. Introdução

Com o grande avanço na tecnologia nesta década (2010 em diante), muitas empresas mostram-se atentas para atualizar seus equipamentos computacionais e assim obterem melhores desempenho e segurança na transmissão de dados. Espera-se que os dados não sejam revelados ou "roubados" para não lhes exporem e acarretarem problemas futuros.

Mesmo com um sistema de segurança sofisticado as empresas ainda enfrentam um grande problema de vulnerabilidade a ataques, que mesmo identificados (exemplo: software malicioso), ainda são preocupantes, pois, se questiona a na pessoa que manipula este sistema e seus atributos para fazê-lo da melhor forma.

Ataques destinados as informações não ocorrem apenas diante do mundo tecnológico ou em computadores. No dia a dia de qualquer pessoa passam despercebidos.

Um grande exemplo pode ser citado com as ligações feitas de dentro dos presídios brasileiros onde vítimas de ataques contam que acabam fazendo o que é pedido de uma forma rápida e mais tarde descobrem que

sofreram abordagem com falsas informações onde os agressores as manipulam as deixando fragilizadas e expostas. Da capacidade humana de persuadir o próximo para se conseguir o que se quer se produzem grandes danos. O interesse de pesquisar sobre o tema surgiu com a veiculação de notícias onde a engenharia social é vista como um dos *malwares* mais velhos do mundo e mesmo assim continua muito utilizada. Controlar pessoas pelas informações é algo difícil, entretanto, possível. Declara-se que o "elo mais frágil" da segurança de dados e informações confidenciais não está no sistema, e sim, na pessoa que interage com este sistema.

1.1. Problemas de pesquisa

Para este estudo se desenvolvem os questionamentos/hipóteses: Existe a melhor adequação do sistema ao funcionário que opera com este sistema; O funcionário é uma vitima fácil da engenharia social; As empresas de médio e grande porte se preocupam com este tipo de ataque; O funcionário pode "entregar" dados valiosos.

1.2. Objetivos

A seguir são declarados os objetivos geral e específico deste trabalho:

Objetivo Geral deste artigo é explicar a engenharia social, onde ela esta sendo aplicada no dia a dia, como ela é usada e como passa despercebido pela maioria das pessoas e empresas, como também, conscientizar sobre os ataques das ferramentas (de TI). Já os Objetivos Específicos são: mostrar as principais técnicas e métodos usados pelos engenheiros sociais e como se prevenir dos ataques, analisar se empresas particulares e privadas entendem a engenharia social como um fator importante da segurança, qual é o foco dos engenheiros sociais atualmente.

1.3. Justificativa

Pode se afirmar que o aumento de ataques de *hackers* no mundo aumenta a cada dia, e as empresas se tornam alvos fáceis de pessoas com más intenções, onde muitas dessas empresas se preocupam com o "software" em suas atualizações de segurança, mas, não se atentam a vulnerabilidaque passa do *software* e atinge pessoas. A empresa de segurança *Check Point* onde foram entrevistados 850 (oitocentos e cinquenta) profissionais de TI, 48% foram vitimas de engenharia social e tiveram 25 ou mais ataques e custaram às vítimas de 25.000 a 100.000 dólares por incidente, sendo que por esta estatística observa-se que muitas empresas dão mais importância para o software onde muitos "engenheiros sociais" aproveitam para subestimar a capacidade humana para ter o acesso a todos os tipos de informações desde as mais básicas até as confidencias, que podem trazer um grande prejuízo para toda a empresa (CIOUOL, 2011).

O assunto abordado neste artigo é importante, pois se trata de uma ação praticada por muitas pessoas. É também um tema que não se aplica apenas a área de informática, pois, engloba gestão de pessoas, finanças, logística, dentre outros.

Os "ataques" referenciados a seguir podem ser aplicados em qualquer empresa, qualquer momento e a qualquer hora do dia, basta que o "agressor" perceba uma oportunidade e que exista uma vítima desatenta.

1.4. Metodologia

Foram realizadas pesquisas exploratórias (bibliográfica e de campo) orientadas pelos professores das áreas de administração e metodologia e desenvolvidas pelo autor junto a instituições de ensino e empresas entre setembro a novembro de 2011 utilizando questionário (apresentado a frente) e observação pessoal.

2. Embasamento Teórico

Para a elaboração deste artigo foram pesquisados em publicações de autores renomados o assunto engenharia social e

respectivas técnicas de ataque. Seguem as bases conceituais.

2.1. Engenharia Social

De acordo com FERREIRA (2009) têm-se os seguintes significados para *Engenharia:* aplicação de conhecimentos científicos e empíricos e certas habilitações especificam a criação de estruturas, dispositivos e processos para converter recursos naturais em formas adequadas ao atendimento das necessidades humanas (p. 754) e *Social*: da sociedade ou relativo a ela, sociável (p. 1864).

Ou seja, Engenharia Social é a aplicação de conhecimentos empíricos e científicos de um modo sociável de acordo com as necessidades humanas para obter informações (como dados pessoais e contas bancarias). É uma ação onde se manipula uma possível "vitima" de modo que ela não perceba e acabe fornecendo as informações pedidas pelo engenheiro social. A engenharia social passa muitas vezes despercebida por muitas pessoas, pois as vitimas adquirem confiança pelo "agressor" e assim se tornam alvo fácil de ser manipulado e enganado por ele. O "agressor" finge ser funcionário motivado e amigo que estuda a empresa e pessoas percebendo onde estas não estão realmente capacitadas e que possam lhe fornecer informações importantes causando-lhes danos financeiros.

De acordo com Mitnick e Simon (2003) uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos estarão vulneráveis.

Diante do exposto pelo autor, afirma-se que a segurança empresarial é aperfeiçoada a cada dia, entretanto, ainda se tem um grande problema, porque mesmo com aparatos de ultima geração não se tem total segurança, ou seja, mesmo com os melhores sistemas sempre as empresas estarão vulneráveis a ataques. Em um exemplo simples, uma pessoa que tranca uma bicicleta com uma corrente e um cadeado simples, pensando na segurança muda para uma corrente acoplada a cadeado de códigos cria um pensamento de que tornou sua bicicleta imune a furtos. Se o ladrão observar o elo frágil e estiver com um alicate rompe tal sistema. O proprietário da bicicleta reforçou a segurança, mas ainda continua vulnerável.

Para Security One (2011) o "ataque" do engenheiro social pode ocorrer através de um bom papo, numa mesa de bar, ao telefone ou, em casos mais sofisticados, através da sedução. O sucesso do "Ataque" está no fato de o usuário abordado nem se quer dar conta do que acabou de acontecer.

Dessa forma, o "engenheiro social", não escolhe hora tempo ou, dia para realmente fazer o ataque, ele simplesmente analisa o melhor momento para conseguir informações de um jeito fácil. Seja num encontro ou em uma simples conversa, o engenheiro social tem como único objetivo retirar informações "sigilosas" ou informações "pessoais", fazendo com que as vítimas não percebam que estão contribuindo com o envio dessas informações.

Para Schneier *apud* Mitnick e Simon (2003, p.16) a segurança não é um produto, ela é um processo. É comparada como um produto de teste. Coloca-se e se vê o poder que o sistema tem. Infelizmente, se esquece de que não basta apenas comprar instalar o sistema "deixar rodando". Muito pelo contrário, pode se estar ainda mais vulnerável do que antes, pois muitas empresas não se preocupam com o processo de adequação ao sistema.

A etapa de adequação deveria ser levada "muito mais adiante", antes mesmo que se pensasse em comprar um sistema de segurança mais sofisticado o conhecimento sobre o processo é essencial. Conhecendo o processo e tendo um sistema de segurança robusto instalado, um profissional capacitado de segurança da informação e conhecedor de normas é também necessário. Então tem-se segurança. A empresa estará mais adequada, sem pontos de vulnerabilidade onde engenheiros sociais consigam ter acesso.

De acordo com Artigonal (2010) a engenharia social não é exclusivamente utilizada em informática, é uma ferramenta onde se exploram falhas humanas em organizações físicas ou jurídicas onde operadores do sistema de segurança da informação possuem poder de decisão parcial ou total ao sistema de segurança da informação seja ele físico ou virtual, porém deve-se considerar que as informações pessoais, não documentadas, conhecimentos, saberes, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas na qual a engenharia social passa a ser auxiliada por outras técnicas como: leitura e linguagem corporal. Delas se obtém informações que não são físicas ou virtuais e sim comportamentais e psicológicas.

Segundo Mitnick e Simon (2003) a grande maioria dos colaboradores transferidos, demitidos ou rebaixados não causam problemas. Mesmo assim entre mil dos citados é preciso apenas um deles para prejudicar a empresa. Estatísticas mostram que a maior ameaça para a empresa vem de dentro e são as pessoas que têm um conhecimento grande do lugar onde ficam e tem acesso as informações valiosas.

Então, ironicamente, o maior perigo para empresa vem dela própria, pois, alguns engenheiros sociais conhecem a empresa mesmo nunca tendo trabalhado nela (através de algum funcionário demitido ou transferido) ou até mesmo o próprio funcionário com pouco conhecimento sobre a engenharia social pode causar danos catastróficos. Por ter trabalhado na empresa conhece seu dia a dia, os pontos mais fracos onde poderá agir em cima deles com mais precisão de sucesso, e assim, obter informações com mais facilidade. Uma pessoa que nunca trabalhou na empresa terá um trabalho muito maior, pois irá levantar pesquisas e gastará muito mais tempo para ter o sucesso no "ataque" do que um ex-funcionário insatisfeito.

De acordo com Ciouol (2011) os *hackers* hoje utilizam uma variedade de técnicas e aplicações de redes sociais para obter informações pessoais e profissionais sobre uma pessoa, para encontrar o elo mais fraco dentro de uma organização. Entre os que responderam à pesquisa, 86% reconhecem a engenharia social como uma grande preocupação. A maioria dos entrevistados - 51% - citou o ganho financeiro como a principal motivação dos ataques. Outras razões seriam a obtenção de vantagem competitiva e vingança. Os vetores de ataque mais comuns em casos de engenharia social são e-mails de *phishing* (47% dos incidentes), seguidos de sites de rede social (39%).

O avanço da engenharia social é preocupante. A cada dia novas redes sociais como *facebook*, *twitter*, etc aparecem e com elas, a probabilidade e facilidade que *hackers* têm ao acessar informações. Manipular vítimas se torna atividade comum, onde os principais motivos dos ataques são ganho financeiro, vantagem competitiva (desafio) e vingança. Muitas vezes usa-se o *phishing* que é uma forma de enviar mensagens através de correio eletrônico (*spams*), que parece ser de instituições renomadas como bancos, governos e multinacionais, fazendo com que as vítimas "entreguem" dados confidenciais (número de cartões, documentos e senhas).

Através das redes sociais o engenheiro social não pede, mas sim, apenas "coleta" informações, pois, muitas pessoas entregam ou facilitam tais informações sem saber o grande risco que correm ao publicar dados como CPF, RG ou senhas de forma

equivocada na internet. Segundo Ciouol (2011) novos empregados são mais propensos a caírem em golpes de engenharia social, segundo o relatório. Em seguida aparecem os terceirizados (44%), assistentes executivos (38%), recursos humanos (33%), líderes de negócio (32%) e pessoal de TI (23%). Contudo, quase um terço das organizações afirmou não ter programas de alerta e prevenção de engenharia social. Entre os pesquisados, 34% não têm qualquer treinamento de funcionários ou políticas de segurança para prevenir técnicas de engenharia social. No entanto, 19% afirmaram ter planos de implantá-los.

O contentamento ao conseguir um emprego novo ou o empenho nos primeiros dias de trabalho torna-se perigosos para o novo funcionário, pois a forma de agir e mostrar dedicação, ajudar a empresa a crescer ocasiona às vezes o inverso. Se o novo funcionário não souber lidar com a emoção, agir com competência e calma, o trabalho pode tornar seu trabalho uma armadilha. O funcionário novo será vigiado pelo engenheiro social e muitas vezes este "entrega" de forma fácil as informações sigilosas, mostrando que muitas empresas atualmente não possuem uma política de segurança e/ou um sistema robusto contra este tipo de ataque, e que muitos funcionários não recebem uma capacitação ou orientação sobre o assunto, fazendo com que a própria empresa dê uma "ajuda" para o engenheiro social, facilite o seu trabalho na captura de informações desejadas.

Mitnick e Simon (2006) descrevem o engenheiro social como o profissional que emprega técnicas persuasivas no dia-a-dia. Assumindo papéis, tentando obter credibilidade e cobrando obrigações recíprocas. Mas, ao contrário da maioria dos profissionais, o engenheiro social aplica essas técnicas de maneira manipuladora, enganosa, altamente antiética e em geral com efeito devastador. Mesmo existindo política de segurança na empresa ela ainda estará vulnerável, pois, as habilidades de um engenheiro social ultrapassam tais barreiras. Parecem inofensivos e são capazes de assumirem papéis, obterem confiança e credibilidade com outras pessoas e mostram-se educados e sociáveis.

Mitnick e Simon (2003) também declaram que a maior ameaça à segurança da empresa ó o perfil enganoso que esse personagem passa. Quase sempre é tão amistoso, desembaraçado e prestativo que faz com que o contratante se sinta feliz por tê-lo encontrado. Atualmente é atribuída aos engenheiros sociais práticas tecnológicas como aplicação de *malwares* (vírus) controlados, onde como *crackers* eles tem acesso as informações através de programas maliciosos. Entretanto, sua maior vítima são as pessoas. Não se objetiva apenas a invasão ou ataque direto ao computador e sim, a vítima que opera este computador/sistema.

Segundo Datcu *apud* Techtudo (2010) um estudo conduzido mostrou que pessoas tendem a revelar informações absolutamente sigilosas (como endereços e senhas) a desconhecidos no *Facebook* desde que acreditem que tenham algo em comum com eles. A autora realizou uma pesquisa com profissionais de TI e *hackers*. No estudo, 81% das pessoas revelam o nome de suas mães, 78% dos *hackers* também o fizeram. E 7% dos hackers deram suas senhas para a pesquisadora.

Milhares de pessoas acessam as redes sociais diariamente e como essa ferramenta só tende a crescer, se transformam em potenciais instrumentos de pesquisas para os engenheiros sociais que coletam informações que para muitos são simples ou rotineiras (nome da mãe/esposa/filhos, local de trabalho) para um engenheiro social transformam-se em ferramentas de manipulação de fácil acesso.

2.2. Técnicas de Ataque

Engenheiros sociais utilizam muitas vezes técnicas que passam despercebidas pelas "vítimas". Observam e se utilizam dos modos e maneiras de agir habituais de qualquer pessoa. Por se passar por cidadão comum as vítimas não percebem que estão sendo alvo do ataque. Na maioria dos casos,

os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente, traços sociais necessários para estabelecer a afinidade e confiança. Um engenheiro social experiente pode ter acesso a praticamente qualquer informação alvo usando as estratégias e táticas da sua habilidade (MITNICK; SIMON 2003, p. 18)

O que o engenheiro social precisa adquirir a confiança de sua vítima, pois, com isso suas chances de sucesso são maiores. Como maioria das pessoas não têm o hábito de duvidar de todo mundo, se um engenheiro social chegar bem apresentável, for bem educado e se mostrar prestativo, que quer ajudar, logo a pessoa já o considera amigável. Nesse momento cai na armadilha.

Ao simular uma amizade consegue tornar mais fácil a captura de informações, pois a amizade é uma das primeiras técnicas usadas por um engenheiro. A amizade é a base para um ataque bem sucedido. Muitas vezes a vítima mal sabe que está sendo atacada.

Segundo Mitnick e Simon (2003) todos têm desafetos ou inimigos. Desde a infância sempre existe aquele "amiguinho" não se enturma e que sempre "arruma confusão". Pessoas que convivem com ele, se pudessem, fariam de tudo pra prejudica-lo, ou seja, desde pequeno se tem inimigos.

Nas empresas isso também sempre existiu. Deve-se assumir que em cada empresa cada pessoa também tenha os seus "impares". Os atacantes visam a infraestrutura da rede para comprometer os segredos da empresa. Questionam os desafetos para conseguirem informações.

Ter uma política de segurança rigorosa, treinamento especializado e bem planejado é essencial para a minimização dos riscos que se corre diante das ações de uma pessoa ou empresa rival. A capacidade do ser humano em achar que todo mundo é confiável que toda empresa é ética ajuda com que os engenheiros sociais tenham menos trabalho em conseguir informações.

De acordo com Tecmundo (2008) engenheiros sociais utilizam o telefone para obter informações se passam por algum funcionário e colega de trabalho, ou algum tipo de autoridade externa, como auditor por exemplo. Seus primeiros alvos são secretárias, recepcionistas e seguranças, pois esses funcionários estão sempre em contato (direto ou indireto) com as pessoas que detém cargos de poder dentro da empresa, os verdadeiros alvos. Assim, através de pessoas acessíveis e com cargos menores é possível obter informações sobre as mais bem posicionadas na hierarquia.

Ataques feitos por telefone onde o profissional "se passa por alguém", um funcionário, um advogado, uma celebridade ou representante da lei, são muito comuns no dia-a-dia. Bastam ter em mãos informações simples como nomes, número de documentos, etc.

Como a maioria das vezes as ligações são atendidas na recepção onde os secretários e recepcionistas sempre tem um contado direto e indireto com pessoas de cargos mais altos da devida empresa, o engenheiro social pode manipular a vítima se passando por este colaborador de cargo alto e enganar o/a atendente. Um exemplo desta prática acontece nos presídios onde detentos ligam e começam uma conversa básica até que a vítima dá ao detento alguma informação de alguém que está fora de casa, assim, o detento informa que houve um sequestro com esta pessoa pedindo um depósito em dinheiro em troca da liberdade da suposta vítima. Em estado de choque, o atendente não consegue se comunicar com o parente e o depósito muitas vezes é feito. Aconselha-se como prevenção deste tipo de ataque ter calma e procurar saber onde o parente que está "sequestrado" se encontra.

Cada corporação possui sua própria linguagem e expressões que são usadas pelos funcionários. A engenharia social criminosa estuda tal linguagem para tirar o máximo proveito disso. O motivo é simples: se alguém fala com você utilizando uma linguagem que se reconheça é mais fácil sentir-se seguro e a "baixar a guarda", falando o que o golpista quer ouvir (TECMUNDO, 2008).

A maioria das empresas possui uma forma de se comunicar internamente entre seus funcionários. É uma técnica que ajuda a prevenir muitos tipos de ataques, pois, só pela conversa você já analisa se realmente aquele funcionário trabalha ou não na empresa. Porém, elas ainda estão vulneráveis, pois, se o engenheiro social consegue ter acesso ao tipo de conversa consegue se passar por um funcionário.

Uma técnica de prevenção seria a adoção de um código interno para a transferência de dados, ou seja, só ocorre a transferência de qualquer tipo de informação mediante senha e contrasenha, se a pessoa do outro lado da linha ou pessoalmente conhecer o código de autorização de dados a conversa acontece. Consegue-se mais resistência ao engenheiro.

Para TecMundo (2008) boa parte das pessoas possuem perfis e contas em redes sociais, o que facilita a engenharia social criminosa. Ao criar perfis em sites de relacionamento é preciso ter cautela com os dados ali fornecidos, pois muitas vezes eles podem ser usados para prejudicar você. Não é aconselhável colocar telefones, endereço, empresa na qual trabalha e qualquer tipo de informação pessoal em seu perfil.

Os engenheiros sociais provocam um momento de condescendência ao fazer uma série de solicitações, a começar pelas inofensivas (MITNICK; SIMON 2006, p.200). No dia a dia, ao atacar, esses profissionais começam com perguntas que mal fazem diferença na vida de cada um em responder, porém, com o tempo o bate papo continua e o engenheiro social acaba se aprofundando mais nas perguntas mais abusadas. Aumenta a confiança e a vítima acaba entregando informações valiosas.

Além da amizade... Simpatia. Nos ataques mais comuns esta é a arma utilizada principalmente para obter dados bancários e financeiros das pessoas, como número de conta, senha, número do cartão de crédito, etc. Os assuntos dos e-mails normalmente são pertinentes a notícias divulgadas na mídia, seja pelo jornal, televisão, rádio ou Internet (TECMUNDO, 2008).

Como notícias estão cada vez mais rápidas na rede e muitas pessoas em questões de minutos já estão cientes do que seguem acontecendo pelo mundo, os engenheiros sociais acabam se aproveitando deste tipo de situação para fazer ataques e muitas vezes tem sucesso no seu objetivo pela grande "falta" de conhecimento dos usuários. Grande exemplo disso aconteceu quando morreu um dos maiores terroristas do mundo, onde engenheiros sociais usaram o fato para obterem informações com mensagens via e-mail, com a mensagem: "*Assista aqui o vídeo da morte do Osama Bin Laden*". Muitas pessoas inocentes acabaram clicando e fazendo o que era pedido e acabaram como alvos fáceis. Como as redes sociais proliferam este tipo de mensagem rapidamente o engenheiro social atinge o seu objetivo com êxito.

Atualmente a quantidade de *spams* recebida por todos os usuários de internet, é muito grande e qualquer pessoa que quiser pode ter o acesso a vários e-mails através de malas diretas. Como esses e-mails de *spans* espalham rapidamente pela rede existe a possibilidade de muitas pessoas caírem no golpe de *phishing*.

Phishing é considerado pela Norton (2011) como um golpe on-line de falsificação, e seus criadores são falsários e ladrões de identidade especializados em tecnologia. Eles usam spams, websites maliciosos, mensagens instantâneas e de e-mail para fazer com que as pessoas revelem informações sigilosas, como números de contas bancárias e de cartões de crédito. Trata-se do abuso de identidade de pessoas maliciosas em criar sites clones de empresas renomadas, bancos, dentre outros objetivando ter informações valiosas ou ganho financeiro.

Na Figura1 tem-se um grande exemplo de *phishing* muito usado onde muitas pessoas acabaram como vítimas.

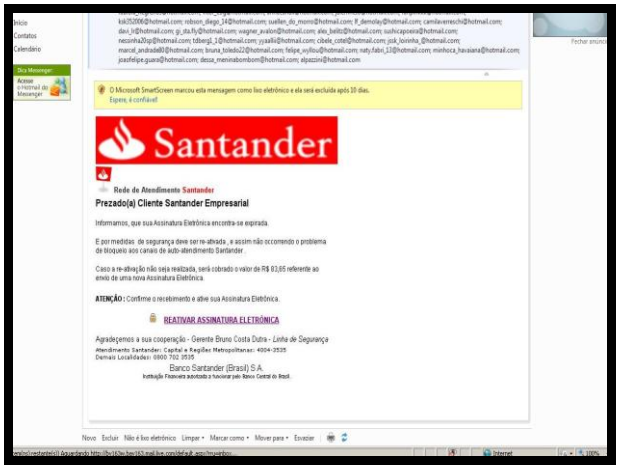

Figura1 – Exemplo Phishing

Como se pode notar na Figura 1, no exemplo de *phishing* mostra-se a imagem de um arquivo encaminhado por *mala-direta* para várias pessoas com uma mensagem persuasiva pedindo a atualização da conta no banco Santander. Ainda com falhas grotescas (a imagem é inteira, uma figura ou apenas um *link*) pessoas clicam e passam suas informações de conta ao "agressor". Deveriam suspeitar algo sobre o *e-mail*, pois a empresa citada não se comunica dessa forma com seus clientes. Outro motivo de desconfiança é que este *spam* é enviado para várias pessoas do mundo inteiro e nem todas essas pessoas possuem conta neste banco. Bancos e empresas de grande porte "não pedem nenhuma atualização" de cadastro via e-mail. Muitas pessoas mesmo sabendo dessas informações ainda acabam clicando para analisar e preencher a proposta de atualização onde caem no golpe.

Como se pode notar na Figura 2 o *link* de acesso para a atualização do banco. Observa-se que é uma pagina praticamente igual a que o banco disponibiliza (site verdadeiro), fazendo assim com que as pessoas que possuem contas neste banco, confiem pelo fato de ser idêntico ao verdadeiro, porém, na barra de endereço pode-se notar uma diferença, onde a página do banco possui um endereço "desconfiável" como "ddor.org". Muitas pessoas mal percebem este tipo de erro e acabam acessando e fazendo a atualização da conta, assim dando de forma rápida, pratica e fácil os dados aos engenheiros sociais. As vitimas só irão notar o ataque depois de alguns dias e será tarde demais. Uma forma de se proteger deste tipo de ataque é nunca fazer atualizações via internet, pois, bancos nunca solicitam este tipo de serviço *online*, e ao fazer algum tipo de transação *online*, deve-se programar o serviço de envio ao seu celular onde uma mensagem de hora dia e o valor da transação é enviada ao celular sempre que feita, sendo assim, ao receber algo que não foi feito comunica-se imediatamente o banco responsável.

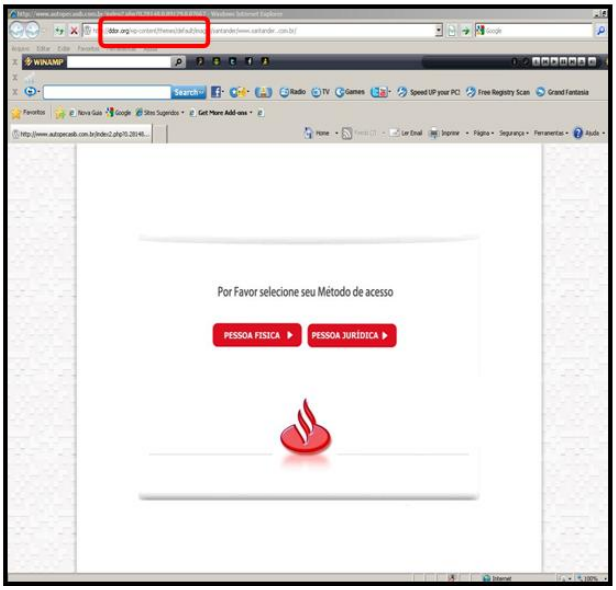

Figura 2 – Exemplo de Phishing

Mitnick e Simon (2003) descrevem outra ferramenta de pesquisa dos engenheiros sociais, o lixo alheio e "Virar latas" é uma expressão que descreve colocar as mãos no lixo do alvo em busca de informações valiosas. A quantidade de informações que você pode ter sobre um alvo é impressionante.

O engenheiro social pega no lixo os recibos de compras alheias que contém nomes documentos e endereços que pessoas acabam jogando no lixo de casa (na rua) ou até mesmo dos escritórios de empresas. Sem perceber, alguns papéis impressos errados que vão para o lixo muitas vezes são usados como rascunhos e podem fornecer informações relevantes. Torna outra "arma" para o profissional.

A melhor maneira de se prevenir é nunca usar folhas impressas erradas e também não jogar nenhum tipo de comprovante, recibo ou extrato de conta bancaria no lixo ou na rua. É mais seguro queimar ou picotar esse tipo de dado do que deixar exposto para muitas pessoas.

Em relação a melhor postura de combate ao engenheiro social mal-intencionado, Peixoto (2006) afirma que se todo funcionário fosse tão questionador como uma criança, demonstrando interesse nos mínimos detalhes, ouvindo mais, estando fortemente atento a tudo a sua volta, e principalmente fazendo o uso dos poderosos "porquês", com certeza as empresas transformariam os frágeis cadeados em legítimos dispositivos dificultantes da segurança da informação. Se o ser humano continuasse com a mesma curiosidade de quando era criança, muitos ataques poderiam ser evitados. Para entender o mundo muitas vezes quando crianças nós questionamos. Os "porquês" são inevitáveis, os pais ou quem foi interrogado pela criança não conseguem ou não sabem responder de uma maneira objetiva o que realmente a criança pergunta ou não respondem de forma que ela entenda. Se todos os funcionários continuassem com esse habito de questionamento, dificultaria e muito para que o engenheiro social tenha um ataque com 100% de eficácia, pois, muitos deles já vêm com respostas prontas para algumas perguntas, mas não para "todas" as perguntas. Não atacariam totalmente seguros. Mas, sabe-se que em muitas empresas a cultura do questionamento não é permitida e fazem que grande maioria dos funcionários apenas trabalhem alheios as informações adicionais.

3. Pesquisa de Campo

3.1. Como foi feita (quanto tempo, quem participou)

Apoiando a bibliografia exposta no capítulo anterior, foi realizada uma Pesquisa de Campo através de um questionário qualitativo elaborado pelo autor e professores orientadores, durante 2 meses e 15 dias (entre setembro e novembro de 2011) envolvendo 10 (dez) profissionais de instituições particulares e privadas envolvidos e atuantes nas áreas da educação e tecnologia da informação (TI), objetivando a análise de cada caso e respectivos riscos decorrentes de ataques de engenheiros sociais. Participaram profissionais da Liebherr (site Guaratinguetá), BASF (site Guaratinguetá), SENAC (unidade Guaratinguetá), FATEC (Guaratinguetá) e ETE (Alfredo de Barros Santos).

A pesquisa teve como objetivo focar profissionais das áreas de TI – Tecnologia da Informação e Educação de cada instituição visando o conhecimento de cada um sobre o assunto e se realmente existia preocupação com o tipo de segurança contra os ataques. Foi elaborado e aplicado um questionário com as questões que seguem:

- Os colaboradores da empresa estão cientes da política de segurança?
- Há treinamento e conscientização dos funcionários quanto à segurança das informações da empresa?
- Em sua opinião, qual o lado mais vulnerável quanto à segurança: as pessoas ou os hardwares e softwares?
- É utilizada alguma medida para prevenir "ataques" de engenharia social? Exemplo: formalização de solicitações de informações por algum documento
- Quais medidas são tomadas para prevenir "ataques" de Engenharia Social na empresa?
- O que você acha da importância da engenharia social, no dia a dia? Acha que muitas pessoas, não levam a sério um foco que realmente é o lado mais fraco da segurança?
- De acordo com Mitnick e Simon (2003) o treinamento de segurança com relação à política da empresa criada para proteger o ativo de informações precisa ser aplicado a todos que trabalham na empresa, e não apenas ao empregado que tem acesso eletrônico ou físico ao

ativo de IT da empresa. Qual a sua opinião sobre esse ponto?

- Em sua opinião, é necessário prevenir ataques de Engenharia Social ou esse é um assunto de menos importância na política de segurança da empresa?
- Você já detectou algum ataque de Engenharia Social na empresa? Se sim, você pode descrever como foi feito o ataque e como foi detectado?

3.2. Resultados e Discussão

Diante exposto pelos autores Mitnick e Simon (2003), nota-se nas respostas dos entrevistados que novos funcionários realmente estão mais vulneráveis aos ataques de engenharia social. Como foi comentado por um dos entrevistados, muitas vezes pessoas ficam muito exaltadas pelo novo emprego e acabam não prestando atenção na política de segurança e às vezes fazem algo é proibido pela empresa.

Quando questionado se o mesmo assinou um contrato de política de segurança sobre o uso indevido de equipamentos da empresa ele afirma: "Não assinei nada e não vi nada sobre isso". Isso é algo que a empresa deveria tomar mais cuidado, pois a maioria dos funcionários muitas vezes tomam decisões erradas e precipitadas. Conforme Martins, a maioria das pessoas revela informações em redes sociais sem nenhum conhecimento do reflexo que isso traz.

Para Peixoto (2006), tais informações confidenciais encontradas em redes sociais, ou até mesmo nos lixos causam danos. Foi comentado por um entrevistado que a maioria das pessoas não tem nenhum conhecimento, são leigas e acabam se "abrindo" mais do que deveriam a desconhecidos, não só em redes sociais, mas, também em conversas presenciais, ou, então simplesmente jogam algum papel com dados (que pra ele não tinha nenhum problema) no lixo. Tornam-se um grande problema para a empresa/instituição. Muitos usam o simples comentário: "uma vez só não tem problema algum". Às vezes essa única vez poderá causar grandes transtornos sendo notado depois de muito tempo. O ataque passa despercebido.

Concordando com Schneier *apud* Mitnick e Simon (2003) a segurança pode ser considerada um produto e sim um longo processo. Foi percebido pela maioria dos entrevistados que não adianta apenas adquirir *hardware*, *software*, e/ou qualquer sistema "de primeira" se não existir um funcionário capacitada em exercer a função, como também, não adiantara ter um funcionário bem informado e capacitado com sistema ultrapassado. A empresa continuará vulnerável. Por isso, deve-se seguir um processo desde a implementação do sistema de segurança na empresa, capacitar não só os funcionários da área de TI, mas sim todos os envolvidos, como também, possuir um sistema adequado de segurança sempre atualizado.

Também de acordo com Mitnick e Simon (2003) mesmo tendo um sistema atualizado e ótimos equipamentos, mesmo assim deve-se desconfiar da invulnerabilidade. Pois, o lado mais frágil da segurança está nas pessoas. Deve-se praticar o questionamento (porque? como as crianças!), pois, as pessoas são domadas facilmente pela falsa segurança e muitas vezes o engenheiro social procura nessa falsa segurança sua vitima. Alguns entrevistados mencionaram que muitas pessoas não estão aptas para exercer esse tipo funções em empresas e acabam tomando decisões precipitadas sem saber o motivo e quando percebem esta sendo vítima, já perdeu muito tempo e para se recuperar em tempo gastará mais dinheiro e tempo. Capacitar um novo funcionário para exercer essa função com conhecimento seria ainda mais oneroso e a empresa opta pela permanência do colaborador dando a ele outra chance.

3.2.1. Demonstração dos Resultados

Seguem os gráficos com o tratamento percentual dos resultados:

3.2.1.1. Sobre a Política de Segurança

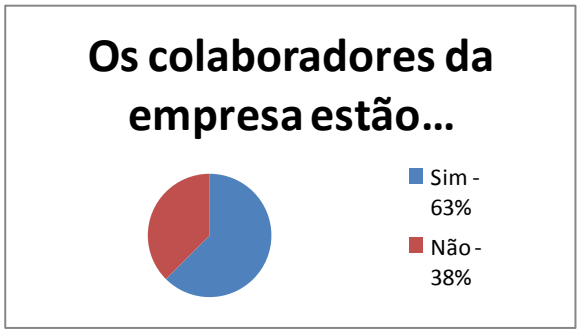

Gráfico 1 – Sobre a Política de Segurança

Como se pode observar no Gráfico 1 acima, a maioria dos funcionários estão cientes da política de segurança da empresa (63%). Atualmente muitos funcionários não se importam com as regras que a empresa impõe. Ex.: Um entrevistado diz que a política da empresa não permite que o colaborador use ou conecte nenhum tipo de *pendrive* nos computadores da empresa, e mesmo assim, um funcionário conectou um *pendrive*, foi pego fazendo o ato, mas, disse que não tinha assinado papel algum sobre os termos de política da empresa, ou seja, de que adianta ter uma política dentro da empresa se muitos funcionários não levam essa política a sério, faz-se que um setor fique vulnerável e deixa a empresa com um lado mais fraco.

3.2.1.2. Lado Mais Vulnerável

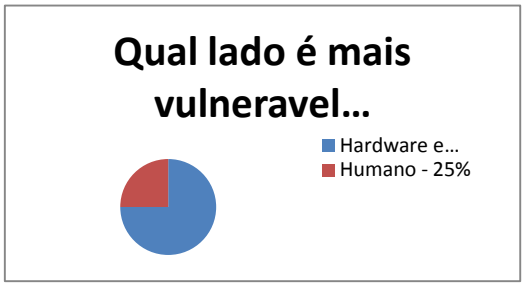

Gráfico 2 – Lado Mais Vulnerável

Conforme o mostra o Gráfico 2, a maioria dos entrevistados (75%) foca mais o sistema de softwares e hardwares da empresa deixando o fator humano em segundo plano. Pode-se considerar que com isso o sistema esta frágil a ataques.

A bibliografia pesquisada apresenta a importância do fator humano. O funcionário que exerce a função de controle/operação está frágil. Tem-se um gasto financeiro com sistemas de ultima geração enorme e pouco treinamento para os funcionários entenderem como lidar com ataques de engenharia social. Poderão ter um prejuízo muito maior depois que sofrerem um ataque por não capacitarem os funcionários para determinados situações do dia a dia da empresa.

3.2.1.3. Medidas de Prevenção

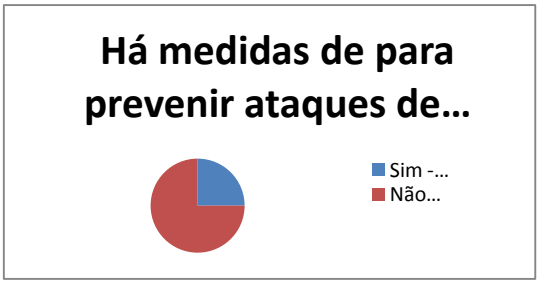

Gráfico 3 – Medidas de Prevenção

Conforme se observa no Gráfico3 não são tomadas medidas de prevenção de ataques de engenharia social. Fato pode ser explicado por dois motivos: é direcionada mais atenção para o sistema de hardware e softwares do que o fator humano (Gráfico2) e o segundo, não se conhecem a fundo como funcionam os ataques de engenharia social. Os entrevistados, embora trabalhem com a área de TI não mostraram muito conhecimento específico sobre o tema.

4. Considerações Finais

De acordo com as informações vistas conclui-se que as empresas ainda focam um lado totalmente oposto do que deveriam em relação a proteção e preservação das informações. Como exemplos, podem-se ser citados os sistemas atualizados e robustos que geram grandes investimentos nas empresas em contraste com a falta de capacidade humana para opera-los, principal foco de muitos engenheiros sociais.

Também foi visto que não só as empresas seguem com este grande gargalo de entender e trabalhar com o fator humano. Governo, igreja e corporações militares também possuem grandes dificuldades em analisar o que esta acontecendo com as pessoas e oque realmente pode-se fazer.

Ainda em pesquisa com as pessoas de grandes empresas possuidoras de tecnologia (na aplicação do questionário) pode-se perceber que algumas delas não conheciam o que era a engenharia social. Duas instituições tem política de segurança considerada adequada, entretanto, não oferecem nenhum treinamento específico para esse tipo de ataque.

Agindo por impulso ou por confiança extrema pessoas passam informações valiosas dessas instituições. O que se espera com este trabalho é que se diagnostique e que se divulgue o problema de sistema de segurança e que se providencie mais treinamento e maior dedicação ao lado humano dos funcionários, e assim, que o profissional da engenharia social tenha mais dificuldade para adentrar, retirar e divulgar informações sigilosas.

Referências

ARTIGONAL. **Desvendando Engenharia Social**. Disponível em: <HTTP//www.artigonal.com/tecnologias/engenharia-social.html>. Acesso em: 16/09/2011.

CIOUOL. **Novos Funcionários Estão Mais Propensos a Ataques de Engenharia Social**. Disponível em: <http://cio.uol.com.br/noticias/2011/09/21/novos-funcionarios-estao-mais-propensos-a-ataques-de-engenharia-social/>. Acesso em: 03/11/2011.

FERREIRA, A. B. H. **Novo Dicionário Aurélio da Língua Portuguesa**. 4ª. Ed. Paraná: Positivo, 2009.

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar:** ataques de hackers – controlando o fator humano na segurança da Informação. São Paulo: Makron, 2003.

MITNICK, K. D.; SIMON, W. L. **A Arte de Invadir:** as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo: Pearson, 2006.

NORTON. **Como Eles Atacam**. Disponível em: <http://br.norton.com/securityphishing.jsp>. Acesso em: 21/11/2011.

PEIXOTO, M. **Engenharia Social e a Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport 2006.

SECURITYONE. **Engenharia Social:** explorando os elos mais fracos. Disponível em: <http://securityone.com.br/artigos/resenha_engenharia_social.pdf>. Acesso em: 16/09/2011.

TECHTUDO. **Estudo Sobre Informações Cruciais no Facebook**. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2011/10/estudo-mostra-que-pessoas-revelam-informacoes.html/>. Acesso em: 05/11/2011.

TECMUNDO. **Cuidado com a Engenharia Social:** saiba dos cuidados necessários para não cair nas armadilhas dos engenheiros sociais. Disponível em: <http://www.tecmundo.com.br/msn-messenger/1078-cuidado-com-a-engenharia-social.htm>. Acesso em 05/11/2011.