Faculdade de Administração e Negócios de Sergipe

Associação de Ensino e Pesquisa "Graccho Cardoso"

Autorizada a funcionar por intermédio da Portaria Ministerial nº 2.246 de 19/12/1997

Pós-graduação MBA em Gestão de redes e Segurança da Informação

Leite, Elson Paixão Silva.

Graduado em Gestão de tecnologia da Informação - FANESE/Aracaju

Segurança da Informação e Engenharia Social

Comportamento humano como um fator de risco

Aracaju

Sergipe – Brasil

2016.1

Elson Paixão Silva Leite

Segurança da Informação e Engenharia Social
Comportamento humano como um fator de risco

Artigo apresentado como requisito para obtenção de aprovação no curso de Pós Graduação MBA em Gestão de Redes e Segurança da Informação, da Faculdade de Administração e Negócios de Sergipe.

Prof. Adriano Lima

Aracaju
Sergipe – Brasil
2016.1

Resumo

Este projeto tem propósito de apresentar de forma clara e objetiva as técnicas mais utilizadas em engenharia social, trazendo um leque de informações relevantes sobre o assunto, demonstrando a engenharia social com um dos fatores de risco para a segurança da informação e que o aspecto humano contribui para que a segurança torne-se mais vulnerável às ameaças. A ideia é que o leitor reconheça os diversos tipos de abordagens de engenharia social, para que não seja um canal de vulnerabilidade para esta ameaça. O material chama a atenção para o interesse e a conscientização dos envolvidos com a tecnologia da informação dentro das organizações fazendo com que este perigo iminente e pouco difundido, possa ser enquadrado como aspecto de grande importância nos procedimentos de segurança da informação. Este documento não abordará especificações técnicas e nem políticas de segurança da informação e sim o assunto de forma simples, partindo do princípio de que a maioria dos usuários não compreende que, comportamentos humanos, seja de forma negligente, inexperiente ou imprudente, possam causar sérios danos ao ambiente computacional, caracterizando leigos nesse assunto. O material está divido em três etapas, na primeira será abordado o conceito de engenharia social e segurança da informação e suas respectivas relações, assim como a importância da informação para as diversas atividades e principalmente para as organizações. Em seguida, serão expostas algumas características relacionadas ao fator humano como canal de segurança vulnerável, assim como também as características do engenheiro social, para que assim possa ser reconhecido. Também serão tratados os procedimentos que não podem ficar de fora de uma política de segurança da informação, como por exemplo: Os planos de treinamento e conscientização dos funcionários. Por último, serão descritos informações de como se proteger para não ser mais uma vitima da engenharia social.

Palavras- Chave: Engenharia Social, Segurança da informação, vulnerabilidades, politicas de Segurança.

Abstract

This project is designed to introduce a clear and objective way the techniques most used in social engineering, bringing a range of relevant information on the subject, demonstrating the social engineering with one of the risk factors for information security and the human aspect contributes so that security become more vulnerable to threats. The idea is that the reader recognize the various types of social engineering approaches, so that is not a vulnerability channel for this threat. The material draws attention to the interest and awareness of those involved in information technology within organizations making this imminent danger and little widespread, can be classified as an aspect of great importance in information security procedures. This document does not address technical specifications, or information security policies, but it simply, assuming that most users do not understand that human behavior, whether negligent, inexperienced or recklessly, can cause serious damage to computing environment, featuring lay this matter. The material is divided into three stages, the first will address the concept of social engineering and information security and their relationships, and the importance of information for the various activities and especially for organizations. Then will be exhibited some characteristics related to the human factor as vulnerable security channel, as well as the characteristics of the social engineer, so that it can be recognized. They will also be dealt with procedures that cannot be left out of an information security policy, such as: Training plans and employee awareness. Finally, it will be described information of how to protect not to be a victim of social engineering.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

Em tempos atuais, a informação passou a ser um dos recursos mais valiosos para as organizações, com isto, tornou-se cobiçada por pessoas mal intencionadas e com diversos objetivos: furtar em beneficio próprio, curiosidade, desafio, prejudicar ou trazer danos apenas pela diversão do vandalismo, em muitos casos até por vingança; pelo fato de esta disponível em muitos lares ou organizações, as informações muitas vezes ficam vulneráveis não apenas pelos meios físicos, mas também pelos comportamentos dos humanos, seja por imperícia, negligência ou ingenuidade. Este projeto tem o objetivo de abrir o conhecimento de forma simples e dinâmica sobre aspectos relacionados à engenharia social fazendo uma relação humana com a segurança da informação, conhecer especificamente as vulnerabilidade que o recurso humano pode abrir dentro de um sistema de informação e conhecer métodos e ferramentas com que os atacantes utilizam em conjunto com a engenharia social para alcance de seus objetivos. Não está comtemplado neste, documentos políticas, técnicas ou normas que integrem um Sistema de gestão de segurança da informação (SGSI), mas sim, algumas recomendações que normas atuais sobre o assunto abordam. A pesquisa tem como uma de suas finalidades expor a existência da engenharia social como um dois fatores que contribuem para a fragilidade da segurança da informação, a ideia é distribuir conhecimento sobre as formas e as técnicas utilizadas na engenharia social, utilizando o fator humano como canal de ataque, conhecido por diversos autores como parte mais fraca no sistema de segurança da informação. Justifica-se tal pesquisa, pelo fato da contribuição da engenharia social para os aumentos dos casos de incidentes de segurança da informação no país. Acredita-se que com as informações destacadas neste documento, aumente o conhecimento e a conscientização dos envolvidos com a tecnologia da informação, para que boas práticas sejam voltadas a impedir técnicas de engenharia social. Para o desenvolvimento da pesquisa foram realizadas pesquisas bibliográficas para levantamento das informações, dados recolhidos de forma qualitativa, estudo de casos concretos e diversas pesquisas na internet sobre o assunto relacionado. Um projeto como este torna- se de grande relevância, uma vez que não ficam destinados só para quem gerência ou administra um sistema de informação, mas também para os demais envolvidos como os usuários em geral. O mesmo contribui para uma abordagem simples sobre o assunto, expondo de forma dinâmica e simples as técnicas de Engenharia social explorando a vulnerabilidade humana.

2. RELEÇÃO ENTRE ENGENHARIA SOCIAL E A SEGURANÇA DA INFORMAÇÃO

2.1 Conceito de Engenharia social

A Engenharia social na tecnologia da informação é caracterizada pela arte de manipular pessoas com práticas ou técnicas para obtenção de informações importantes ou sigilosas, seja nas organizações ou em qualquer outro lugar que detenha informações, ocorrendo por meio de enganação ou exploração da confiança das pessoas. Quando abordamos este tema, seja Hacker ou Cracker, temos que evidenciar: Kevin D. Mitnick, este foi um dos mais famosos crackers de todos os tempos, e muitos de seus ataques foram originados através de técnicas de Engenharia Social nos anos 90, época em que esse termo ficou mais conhecido. Existem dois tipos de ataque de engenharia social, o direto: que são aqueles onde o atacante entra em contato direto com a vítima, ou seja, geralmente os alvos são bem definidos como também seus objetivos, diferente dos indiretos que não tem um alvo específico.

> “Você esta em um elevador quando de repente, um disquete cai no chão, você olha, tem um logotipo de uma grande empresa e a Frase: “histórico salarial", movido pela curiosidade, você abre o disquete em sua casa e talvez haja um ícone para o Word, então ao clicar, aparece a frase: “ocorreu um erro ao tentar abrir o arquivo”, você não sabe ,mas um backdoor acabou de ser instalado em sua máquina. Você imediatamente leva o disquete até o setor responsável em devolvê-lo ou guardá-lo, o setor por sua vez também abrirá o disquete, agora o hacker tem acesso a dois computadores "(trecho do livro “*A arte de enganar* ” de Kevin Mitinick).

A citação no texto do livro de Mitnick demonstra claramente o ataque de forma indireta, o atacante social não precisou contado direto com a vítima, na verdade o mesmo não sabe nem quem vai ser a sua próxima vítima, ação de forma aleatória.

A Engenharia Social pode ser também definida como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações. (SILVA, E. 2008).

O termo “Engenharia” foi atribuído a essa prática porque é construída sobre informações e táticas de acesso às informações sigilosas de forma indevida. Já o termo “Social” foi atribuído porque utiliza pessoas que vivem e trabalham em grupos organizados. Essas práticas simplesmente ganharam esse novo porque são bastante utilizadas por detetives a fim de obterem informações e também por magistrados com o objetivo de comprovar se um declarante fala a verdade. (SANTOS, 2004).

Quando imaginamos um ataque em um sistema computacional de forma ampla, pensamos logo em corrigir as falhas computacionais que possam favorecer estes ataques; então fechamos nossos sistemas por *firewalls*, instalamos antivírus e *anti-spywares* para detecção e remoção de programas maliciosos, atualizamos sempre todos os programas na esperança corrigir estas possíveis falhas. Por mais que sejam cuidadosas as políticas de segurança de um sistema computacional, este sempre poderá ser comprometido por fruto de uma falha de seu operador, abrindo assim uma segunda alternativa para os invasores: o erro humano.

2.2 Conceito de informação

Nos dias de hoje, as informações são muito visadas, principalmente com a interconectividade dos dispositivos, sendo expostas às diversas ameaças e vulnerabilidades. Com este valioso recurso, as organizações podem tornar-se competitivas no mercado, abrir novas oportunidades de negócio fazendo com que esta seja parte do seu processo produtivo; são consideradas para muitas empresas o seu maior patrimônio, requerendo assim uma atenção especial. Sua falta, indisponibilidade ou inconsistência constitui uma forte ameaça para os negócios, podendo levar uma empresa a uma inevitável extinção. Tudo isso atribui à informação título de importante recurso corporativo, transformando-a em um ativo essencial, necessitando ser protegida como qualquer outro bem.

> "A informação representa a inteligência competitiva dos negócios e é reconhecida com ativo crítico para a continuidade operacional da empresa" (PEIXOTO, 2006).

No ambiente da informação, permeiam alguns conceitos, nos quais encontramos definições específicas e importantes como: **Dados, Informação, Conhecimento e Inteligência**. Esses conceitos alcançam áreas específicas, como por exemplo: militar, cuja atividade de inteligência está voltada para defesa do estado, e a empresarial: que direciona essa atividade para os negócios. Os **Dados:** compreendem a classe mais baixa da informação. A **informação:** são os dados que passam por algum tipo de processamento para serem utilizados de uma forma inteligível. O **conhecimento:** é a informação cuja sua relevância, confiabilidade e importância foram avaliadas, sendo obtida pela interpretação e integração de vários dados e informações para iniciar a construção de uma situação. A **Inteligência:** é a informação com oportunidade, ou seja, é a parte do conhecimento que habilita a tomada das melhores decisões (Cardoso Júnior, 2005).

2.3 Segurança da informação

A norma (NBR ISO/IEC 27002:2005) conceitua segurança da informação como: a proteção das informações quanto a vários tipos de ameaças, de modo que garanta a continuidade do negócio, minimizando os riscos para o negócio, maximizando o retorno sobre o investimento e as oportunidades de negócio. Para que seja utilizada, a informação necessita garantir três modelos fundamentais: a integridade, a disponibilidade e a confidencialidade, características estas que devem ser preservadas, pois são regidas como princípios da segurança da informação:

A Integridade: é a garantia da exatidão e completeza da informação e dos métodos de processamento. Então a integridade esta ligada a garantia de que a informação não seja modificada, alterada ou destruída sem autorização durante o seu manuseio ou armazenamento, e a certificação de que ela seja legítima e permaneça consistente. Esta quebra ocorre quando a informação é corrompida, falsificada, roubada ou destruída.

Garantir que isto não ocorra e manter a informação na sua condição original. Diversos fatores contribuem para a perda da integridade: inserções, substituições ou exclusões de parte do conteúdo da informação, que podem se ocasionadas por alterações na estrutura física e lógica onde ela está armazenada, ou quando as configurações de um sistema são alteradas para se ter acesso a informações restritas, bem como são superadas as barreiras de segurança de uma rede de computadores.

A Disponibilidade: é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (NBR ISO/IEC 27002:2005). Ocorre a não disponibilidade, quando a informação não está disponível para ser utilizada, ou seja, ao alcance de seus usuários e destinatários, não podendo ser acessada no momento em que for necessário utilizá-la. Garantir a disponibilidade é assegurar o êxito da leitura, do trânsito armazenamento da informação.

A Confidencialidade: é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso (NBR ISO/IEC 27002:2005). Esta será afetada quando a informação esta disponível para pessoas não autorizadas, e a abertura do seu acesso restrito. A quebra da confidencialidade é a perda do segredo da informação. Garantir a confidencialidade é assegurar o valor da informação e evitar a divulgação indevida.

2.4 Normas de Segurança da informação voltada para os recursos humanos.

Para segurança da informação de maneira efetiva e formal, diversos procedimentos, técnicas e normas estão disponibilizados por diversos órgãos de controle, entre elas a norma (ISO/IEC 27001:2013), esta vem para prover diversas normas dentro de um sistema de segurança da informação, com o objetivo de preservar a confidencialidade, integridade e disponibilidade das informações por meios de um processo de gestão de risco, fornecendo confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

No anexo A da tabela especificamente no item "A.7. "Segurança em Recursos Humanos" da norma ISSO/IEC 27001:2013 estão descritos recomendações relacionadas aos recursos humanos com o objetivo de assegurar que funcionários e partes externas entendam as suas responsabilidades e se estão em conformidade com os papeis para ao quais eles foram selecionados, envolve também pessoas envolvidas nos processos que demandam informações, aborda principalmente aspectos ao acolhimento do colaborador na organização, gestão deste durante sua vida na empresa e medidas adotadas quando na sua saída da organização. Abaixo algumas informações a respeito:

No corpo **A7.1** esta relacionado os processos antes da contratação, descreve no corpo da norma os objetivos de assegurar que funcionários e partes externas entendam as suas responsabilidades e que estão em conformidade com os papéis para os quais eles foram selecionados.

Item A.7.1.1: Recomenda a verificações dos históricos que devem ser realizadas para todos os candidatos a empregos, de acordo com a ética, regulamentação e leis relevantes e devendo ser proporcional aos requisitos do negócio, aos riscos percebidos e a classificação das informações a serem acessadas.

Item A.7.1.2: Recomenda que Termos e condições de contratação: controle das obrigações contratuais com funcionários e partes externas deve declarar as suas responsabilidades para com a segurança da informação organização.

No corpo **A7.2**, refere-se os procedimentos durante a contratação, Tem com objetivo de assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação:

Item A.7.2.1: Recomenda como responsabilidades da direção, requerer aos funcionários e as partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas politicas e procedimentos da organização.

Item A.7.2.2: Recomenda conscientização, educação e treinamento em segurança da informação a todos os funcionários da organização, partes externas devem receber treinamento educação, e conscientização apropriados e as atualizações regulares das políticas e procedimentos organizados relevantes para as suas funções.

Item A.7.2.3 Recomenda procedimentos onde deverá existir um processo disciplinar formal implantado e comunicado, para tornar ações conta funcionários que tenham cometido uma violação de segurança da informação.

No corpo **A7.3**, refere-se ao encerramento e mudança da organização , tem o objetivo , proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

A.7.3.1 Recomenda responsabilidades pelo encerramento ou mudanças de contratação, o controle sobre as responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação, devendo ser bem definidas, comunicadas aos funcionários ou partes externas e cumpridas.

2.5 Vulnerabilidades do fator humano

Uma organização poderá se proteger com as melhores tecnologias de segurança que possam existir, possuindo pessoal altamente treinado para resguardo de informações confidenciais ou cercar-se de guardas de segurança para o prédio, mas mesmo com todo este aparato, ainda estará vulnerável. Até os especialistas no assunto podem ser vítimas de técnicas maliciosas. Podemos imaginar que os cuidados com a segurança da informação no meio residencial seja mais brando e reativo, e que nas organizações esta seja tratada de forma mais proativa, o fato e que a informação nunca estará cem por cento segura, o que pode ser feito é minimizar os fatores de risco, diminuindo as aberturas para as ameaças; diversas ferramentas de controle e bloqueio de ataques ou invasões podem ser utilizadas, como firewalls, anti-malwares sistemas de detecção de intrusos (IDS).

Dispositivos de autenticação cada vez mais sofisticados como Tokens ou Smart cards, biometria dentre outros, não serão de plena utilidade se o fator humano não for trabalhado de forma contínua, entre toda esta estrutura de segurança, o fator humano torna-se sempre o elo mais fraco e vulnerável dos sistemas, este demanda ou controla estes dispositivos e podem ser alvos fáceis para ataques de forma social, assim, seria como trancar todas as entradas, mais sempre alguém deverá esta com uma chave para entrada, é ai onde entra a engenharia social. Poderemos fizer uma analogia da arte de enganar as pessoas com um fato bíblico: "*o da queda do homem nos tempo de Adão e Eva*" com a premissa do poder persuasão e convencimento, com artifícios de influência e manipulação, este exemplo expõe a estratégia que a serpente desenvolveu bem, sendo consagrada como a pioneira na arte de manipular e enganar.

> O próprio Mitnick considerado o maior especialista em engenharia social do qual se tem notícias, em uma das suas raras vindas ao Brasil, no final do ano de 2003, concedeu uma entrevista para a Information Week Brasil, onde declarou que foi vítima de engenharia social ao receber uma ligação de um jornalista dizendo que havia conversado com seu editor; desatendo, Mitinick confiou na palavra do jornalista e deu uma entrevista sobre o livro, depois, quando a reportagem foi publicada, o editor de Mitcnick ligou para ele furioso, pois toda a estratégia para o lançamento do livro The ART of Deception (A Arte de Enganar) havia sido prejudicadas por causa da entrevista, que o editor não havia autorizado. (PEIXOTO, 2006).

O erro humano pode ser definido como todo comportamento que seja inseguro, seja ele um ato contínuo ou fruto de um momento de distração, podendo este ser usado por um atacante para que este consiga comprometer um sistema. O grande problema com o erro humano é que ele não pode ser completamente corrigido, apenas mitigado, se partimos da premissa de que nenhuma pessoa é perfeita e nenhum treinamento poderá mudar isto.

O importante é salientar que a engenharia social independe de sistemas ou softwares, o elemento mais vulnerável do sistema de segurança da informação é o ser humano, este é detendo de traços comportamentais e psicológicos que o torna vulnerável a ataques de engenharia social. Abaixo podemos destacar alguns:

Autoconfiança: Pessoas podem buscar transmitir em diálogos atos de sempre fazer algo de bom, transmitindo segurança, conhecimento, com o objetivo de criar uma relação sólida para inicio de uma comunicação ou ação favorável a uma organização ou a outro individuo.

Necessidade de ser útil: É normal as pessoas se comportarem de forma cortês, bem como praticar atos de ajuda a terceiros.

Fazer novas amizades: Existem pessoas que fazem amizades mais facilmente e que expões a sua vida com mais naturalidade, são abertas a prestarem informações pessoais, se tornando vulneráveis.

Vaidade: O ser humano torna-se mais receptivo com aqueles que concordam com suas ações e opiniões.

Persuasão: Capacidade de convencimento na busca de obter respostas, isto é inerente as pessoas uma vez que possuem comportamentos característicos que as tornam vulneráveis à manipulação.

As pessoas cometem erros e geralmente sempre os mesmos, em razão destas questões, sempre ocorrerão falhas de segurança devido ao comportamento humano e sua falta de conscientização em relação a segurança da informação.

2.5.1Tipos de pessoas

Um dos grandes desafios do engenheiro social é de como este poderá lidar com os diversos tipos de personalidade humana. As pessoas podem mudar de comportamento muito facilmente de acordo com o seu meio externo. A tabela abaixo demonstra os diversos tipos de comportamento e como seriam uma interação ideal de interlocução com estes diversos momentos do ser humano:

Tipos de pessoas	Como reconhecer	Como lidar
Nervosas	**Aparentam cansaços e com raiva, são inquietos e Impacientes, praticam passos fortes e falam muito alto, reclamam demais.**	**Investir na Paciência, tranquilidade Consideração, Educação, presteza agilidade e sangue frio. Empatia atenção**

		redobrada e bom humor, uso do medo se necessário.
Indecisas	**São apreensivos, querem conversar mais sobre o assunto, receosos de cometer erros, falantes e transmitem insegurança.**	**Moderação, calma, cortesia, confirmar suas próprias opiniões e demonstrar conhecimento e paciência usando a use a simpatia.**
Desagradáveis	**Céticos (descentes) são questionadores, conversadores e insultantes.**	**Agir demonstrando fraqueza, conhecimento, agilidade, cortesia e calma, ter controle próprio também usar o temor e o medo.**
Duvidosos	**Críticos, indiferentes silenciosos, perguntam demais.**	**Conhecimento da empresa, tão perseverança, ser convincente. Citar seus conhecimentos de normas seus limites**
Silenciosos	**Não tem conhecimento, podem ser pensadores ou estarem fingindo saber. Podem esta infelizes.**	**Faça-lhes uma pergunta que os leve a responder algo que gere mais confiança. Tenha consideração e cortesia**
Dependentes	**Tímidos e sensíveis indecisas, infantis.**	
De bom senso	**Agradáveis e inteligente**	**Faça com que eles esperam, seja eficiente e eficaz, cortesia e considerações conquiste-os rapidamente e use curiosidade.**

Tabela_1 tipos de pessoas

Fonte (Flavio, Araújo, 2010, p 134)

2.5.2 Fatores emocionais

O engenheiro social detém forte experiência em manipular os sentimentos das suas vítimas, conduzindo-as a fazerem o que ele quer, citados abaixo os mais comuns:

Curiosidade: Inerente do ser humano, a curiosidade faz parte da interação do ser em relação ao ser meio, onde o mesmo explora seu universo agregando informações ás que já possui, sabendo disso o engenheiro social buscará ativas diversas formas de curiosidades.

Confiança: Meio muito utilizado pelos engenheiros sociais para manipular as pessoas, este método é muito utilizado para inicio de um ataque, esta pode se manifestar de diversas formas como: se passar por um funcionário de outra filial no caso de uma organização, ou oferecer-se para ajudar em alguma coisa, outros acontecimentos comuns é o recebimento de e-mail com endereços de origem de um conhecido vindo com anexo, muitos contendo vírus, sendo que este pode ser forjado.

Simpatia: Uma das melhores demonstração e simpatia esta relacionada com a sedução feminina. Será bem mais fácil uma mulher ser bem sucedida em uma técnica de engenharia social em uma abordagem com seguranças de uma organização, do que um homem, ou seja, um contato pessoal ou por telefone, pois no caso de uma pessoa com más intenções fala com a vítima em um tom de voz feminino doce e meigo, dificilmente alguém poderá identificar algum golpe por traz disto.

Culpa: As pessoas quando tomadas por algum sentimento de culpa, estão mais propensas a fornecer ajudar, isso também ocorre no meio da engenharia social. Uma situação na prática seria culpar alguém, convencendo-a desta condição, e fazendo com que essa pessoa te ajude no que você quiser. Outra situação seria dentro e de uma organização, onde colaboradores mais vulneráveis, geralmente são os que acabaram de chegar à empresa querendo mostrar serviço.

Medo: A imposição do medo esta dentre as armas mais poderosas para obtenção de resultados rápidos. Isso porque ninguém consegue aquentar a pressão psicologia por muito tempo e acaba entregando informações de forma rápida. No mundo coorporativo as ameaças geralmente partem de pessoas com hierarquia superior do ameaçado. Dentro de uma organização, a resposta diante de uma ordem de pessoa de mesma hierarquia completamente diferente de uma vinda de alguém de hierarquia superior. Uma ordem da presidência por exemplo aliando aos artifícios de engenharia social com a imposição do medo, fazendo-se passar por pessoa de maior hierarquia, contribui de forma eficaz o sucesso do ataque.

3. ABORDAGENS DO ENGENHENIRO SOCIAL

Nesta etapa, o projeto tem o objetivo de demonstrar os métodos de manipulação usados na engenharia social:

Por e-mail: O engenheiro social poderá enviar um e-mail para seu alvo onde contenham informações que deseja, seja um pedido de algum documento importante ou se passando por alguém da TI solicitando mudança de senhas. De qualquer uma destas formas será com correspondência eletrônica ou ela fica quase perfeita com as identificações do grupo que a vítima pertença.

Pessoalmente: Método arriscado, porém muito eficiente exemplo: bem trajado e com uma boa aparência e acessórios caros, passando-se e por um cliente ou colaboradores da organização ou parceiro de negócios, varias possibilidade em aberto para este método.

Por telefone: Técnica de se passar por alguém importante ao telefone, fingir precisar ou oferece ajuda, o objetivo é manipular o sentimento das pessoas, fazendo com que estas entreguem algo nem ao menos saberem como foi.

3.1 Técnicas de engenharia social

Estas são algumas técnicas que são usadas na Engenharia Social que muitas pessoas nem dão a mínima importância, principalmente dentro das empresas.

Disfarces: Princípio fundamental de qualquer ataque de Engenharia Social é a capacidade do responsável pelo ataque esconder-se assumindo outra a identidade, de preferência alguém que possua o acesso à informação alvo do ataque.

Descarte incorreto de informações: O descarte de informações na forma impressa ou no ato de esvaziar a lixeira de um *desktop* não podem serem considerados seguros o suficiente nos casos de informações sigilosas, uma vez que em uma incursão mais cautelosa, o atacante poderá ter o acesso à estas. Para garantir o descarte seguro das informações, devemos utilizar meios adequados como a queima no caso da informação em papel, o uso de softwares seguros para apagar de forma definitiva de dados sigilosos do computador.

Redes sociais: Familiares amigos e conhecidos transformam-se em valiosas fontes de informações se bem explorada. Assim, um engenheiro social experiente se aproximará destas pessoas a fim de obter informações e ou favores.

Apelo sentimental: Aspectos emocionais podem ser explorados de forma sistêmica, maneira mais fácil de manipular alguém. Inclusão de uma história convincente fazendo com que a vítima pense que esteja fazendo o bem, ou que ganhará algo em troca no final, pode ser determinante para o sucesso de um ataque de Engenharia Social.

Programação Neolinguística: Consiste no uso de dialetos de certos grupos e maneirismos artificiais por parte do engenheiro social a fim de que a vítima acredite na sua história e no seu disfarce. Aliado a isto, é criado um clima de confiança entre a vítima e o atacante facilitando assim um ataque de engenharia Social.

Pesquisas na Internet: Dispositivos de busca na internet são capazes de entregar milhões de informações em segundos, como por exemplo: concurso público feito por uma pessoa, seu CPF, a faculdade que cursou, a escola na qual se formou, entre outros dados, podem ser facilmente encontrados com uma busca na Internet. A rede mundial e as redes sociais permitem que um indivíduo mal-intencionado descubra diversas informações pessoais sobre seus usuários, comprovando que as informações obtidas na Internet são uma das maiores armas do engenheiro social.

Analise do Lixo: Imagina-se que muitas organizações não tem o cuidado de verificar o que está sendo descartado da empresa e de que forma é realizado esse tipo de descarte. O lixo pode ser uma fonte de riqueza de informações para os Engenheiros Sociais. De fácil acesso, as informações encontradas no lixo podem revelar dados suficientes para o início de uma engenharia social; nomes de funcionários, telefone, e-mail, senhas, contato de clientes, fornecedores, transações bancárias efetuadas, em fim, uma infinidade de material pode ser encontrado em um descarte de lixo mal elaborado.

Abordagem Pessoal: Pode ser uma boa estratégia de levantamento de informações, está técnica consiste em o Engenheiro Social realizar uma visita na empresa alvo, podendo se passar por um fornecedor, terceiro, amigo do diretor, prestador de serviço, entre outros, no qual através do poder de persuasão e falta de treinamento dos funcionários, consegue sem muita dificuldade convencer um segurança, secretária, recepcionista a liberar acesso ao datacenter onde possivelmente conseguirá as informações que procura. Apesar de esta abordagem ser arriscada, muitos Crackers já utilizaram e a utilizam até hoje.

3.2 Facilidades para engenheiro social

Muitas vezes ficamos vulneráveis sem perceber que estamos abrindo aporta para o engenheiro social, a figura abaixo demonstra muito bem isso, diversos veículos utilizam os adesivos de “Família Feliz”, (figura_1), pela lógica da imagem podermos constatar que este condutor (a) é casado, possui apenas um filho e que gosta de animais, até ai não tem nada de mais, se formos para o lado engenheiro social esta imagem poderá fornecer uma infinidade de informações suficientes para início de uma ataque.

Imagem 1-Adesivo família feliz

O perfil de rede social refere-se ao cadastro de dados de pessoais, de contato e preferencias de um determinado usuário, partes destes dados podem ser públicas, sendo compartilhados com os demais usuários, ou privados, dependendo do tipo de perfil, comunidade ou configuração de privacidades definidas pelo usuário. (https://pt.wikipedia.org/wiki/Perfil_(comunidade). Em resumo, um prato cheio para os ataques de engenharia social, uma vez que muitas informações pessoais ficam facilmente disponíveis na rede.

Figura_2 - perfil rede social

Sabemos que não é tão simples um ataque ou fraude em um sistema bancário ou em uma instituição comercial, para isto é necessário equipamentos técnicas e muito tempo disponível, desta forma os golpistas concentram, esforção na exploração de vulnerabilidades mais comuns como exemplos usuários finais, utilizando a engenharia social e outros artifícios os golpistas procuram persuadir as suas vítimas a entregarem informações importantes, com estes dados em mãos, os fraudadores efetuam transações financeiras, abrir contas dentre outras atividades delituosas.

Figura_3-Golpes na rede

3.3 Métodos utilizados pelos engenheiros sociais

Phishing: É um tipo de ataque de engenharia social muito comum. Consiste no envio de falsas mensagens falsas para a vítima, a fim de se obter, sem o conhecimento desta, informações sigilosas. O funcionamento baseia-se na exploração de um vínculo de confiança entre a vítima e por quem o atacante está se passando. Nesse ataque ocorre com frequência a cópia do *layout* do site pelo qual o atacante tenta se passar, seja esse *layout* usado na mensagem enviada para a vítima ou em um site falso.

Nesse segundo caso, também e necessário por parte do atacante mascarar a URL do site. Uma forma muito comum de fazer isso é usando encurtadores de endereços web, como o migre.me e o bit.ly, mas as vezes nem isso é necessário, como no exemplo a seguir:

http://www.paypal.com/
http://www.paypai.com/

A forma em caixa-alta da letra 'i' se confunde facilmente com a forma na em caixa-alta da letra 'i' se confunde facilmente com a letra 'l' em caixa-baixa, em algumas fontes isso se torna até imperceptível. Esse exemplo simples ilustra claramente a facilidade pela qual uma vítima desatenta pode cair em um ataque de phishing.

> Durante o trimestre de 2015, os produtos da Kaspersky Lab registraram mais de 50 milhões (50.077.057) de detecções pelo sistema antiphishing, o que revela um aumento de um milhão em comparação ao último trimestre de 2014, de acordo com o Relatório de Spam e Phishing do primeiro semestre da companhia, Geograficamente, o Brasil continua a ser o líder em volume de usuários atacados. Embora tenha diminuído 2,74% no primeiro trimestre, os brasileiros continuam sendo as vítimas preferidas dos phishers e representam 18,28% dos ataques no índice mundial. Índia (17.73%) e China (14,92%) também estão no pódio.
>
> Fonte: Fonte: http://convergecom.com.br/tiinside/seguranca/mercado-seguranca/03/07/2015/brasil-continua-como-maior-vitima-de-ataques-de-phishing/

Spear Phishing: São tipos de ataques mais sofisticados de engenharia social do que o phishing, geralmente direcionados para que sejam simulados envios de pessoas conhecidas das vítimas. As mensagens podem parecer que venha do seu empregador, ou de um colega de trabalho que poderia ter enviado uma mensagem de e-mail a todos na empresa. A mensagem pode solicitar nomes de usuários ou senhas ou conter softwares maliciosos, como um cavalo de Tróia ou um vírus.

Anexos Maliciosos: Dentre os mais antigos e conhecidos ataques de Engenharia Social, consiste no envio de mensagens contendo algum tipo de *malware* em anexo. O atacante busca seduzir a curiosidade da vítima para que esta execute o anexo infectado, contaminando o seu sistema no processo. Outro fator importante é a necessidade de se esconder a natureza do anexo, para isso empregam-se técnicas de esteganografia e aproveita-se de uma falha computacional.

A figura abaixo demonstra um e-mail recebido com anexo de origem duvidosa, onde o mesmo informa que a partir de uma determinada data será obrigatório a atualização de dados bancários e também um link para ser clicado; tudo isso seria um pouco verdade se ao menos o titular usuário do e-mail possuísse conta no referido banco, outro detalhe interessante, é o e-mail de resposta: "*equipe@mail.com.br"*. Totalmente diferente do nome do suposto banco remetente.

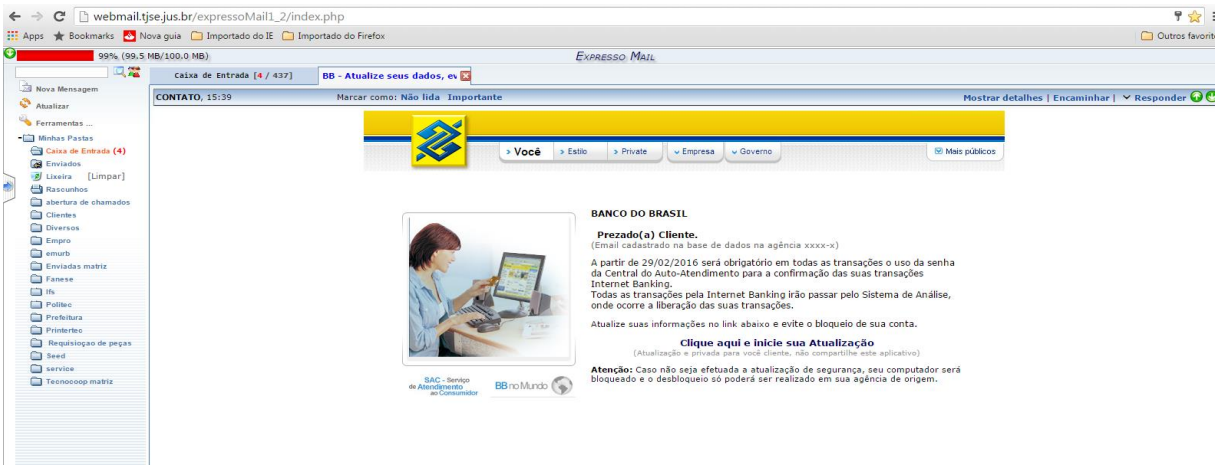

Figura_4 anexo malicioso

Falso Antivírus (*Rogueware*): Tipo de ataque recente que é a criação de *malwares* disfarçados de programas antivírus. Nesta técnica o atacante aproveita-se do medo do usuário de ter seu sistema comprometido, assim, o usuário é levado por um *pop-up* ou por uma busca na Internet para uma página contendo links para o download de um suposto software de antivírus, com isso essas páginas contém uma enganosa busca on-line por malwares e o computador da vítima, que alerta para a presença de programas maliciosos e sugere o download do software indicado na página. Ao instalar o programa este realiza uma nova falsa busca e informa falsamente que computador esta livre de ameaças. Assim o atacante consegue não só comprometer o computador da vítima como também, convencê-la de que seu computador não possui nenhum software mal-intencionado.

4. EVITADO ATAQUES DE ENGENHARIA SOCIAL

Diante de diversas ameaças, varias maneiras de proteção podem ser utilizadas para que sejam minimizadas as vulnerabilidades, tendo em vista a inexistência de uma proteção totalmente eficiente, o que pode ser feito é diminuir os fatores de risco: Abaixo estão citados alguns exemplos relacionados:

Segurança da conexão e criptografia: Diz respeito a uma prática de simples comportamento, porém com eficácia no combate à Engenharia Social, é a atenção à segurança da conexão e o não envio de dados sigilosos em uma conexão considerada insegura. Em uma conexão criptografada, impede que um terceiro obtenha dados de uma vítima e use-os contra ela em um posterior ataque de Engenharia Social. Para auxiliar os usuários a maioria dos navegadores atuais mostra se a conexão é criptografada e em caso positivo, o tipo da criptografia empregado. Também é recomendado o uso de protocolos seguros no referente ao acesso remoto, como por exemplo, o uso do SSH em substituição TELNET, uma vez que esse último não garante por padrão a segurança da conexão.

Sites e certificados digitais: Entidades certificadoras são instituições responsáveis pela emissão de certificados digitais que identificam pessoas, quanto a sites na Internet e seus respectivos proprietários. Quando uma unidade certificadora assinar digitalmente os certificados que emite, esta estará relacionando a identidade do portador do certificado, portanto da chave privada à chave pública existente no certificado. As maiorias dos navegadores já exibem se a página visitada possui um certificado digital válido, caso não possuir, o site provavelmente é sempre uma abertura para fraude.

Bom senso e atenção aos detalhes: Em grande parte dos ataques de Engenharia Social ocorrem erros de escrita. Isto é devido ao emprego de tradutores para passar a mensagem de sua língua original para outras. Além disso, outros detalhes podem expor um ataque: o domínio de um site, dados e outros. Conferindo as informações recebidas e não acreditando em tudo a primeira vista, o usuário consegue escapar de diversos ataques de Engenharia Social.

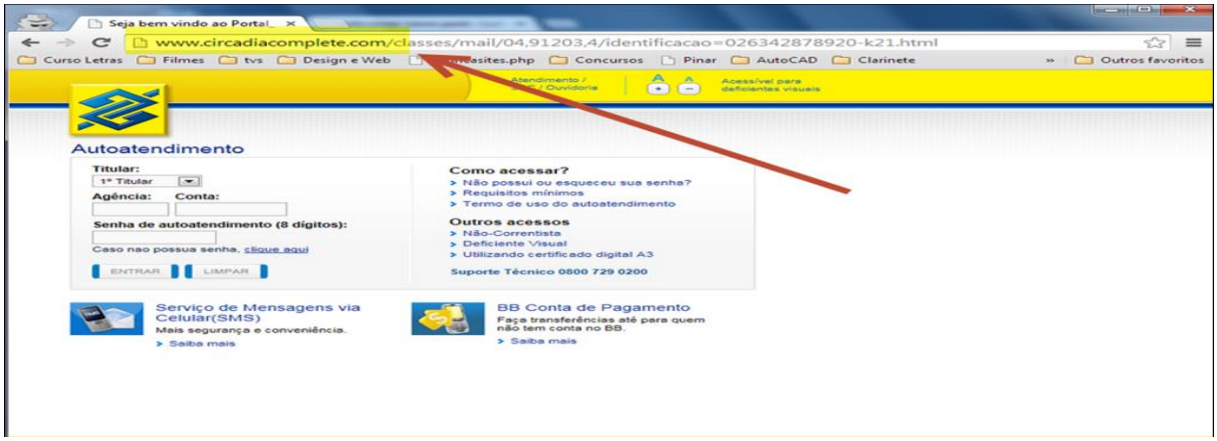

Figura_5 site falso

Uso de senhas fortes: Imaginamos a senha como uma chave de entrada, em caso deste possuir fragilidade, esta poderá ser facilmente copiada e utilizada, não se recomenda a utilização de senhas constituídas de informações pessoais que possam ser descobertas por um engenheiro social como números de CPF ou RG, datas de aniversário, nomes de amigos ou familiares endereços, o nome de um time de futebol e o próprio *login*, são exemplos de senhas que um atacante descobrirá rapidamente. É recomendado senhas extensas, com letras em caixa-alta e baixa, números e caracteres especiais.

Educação e treinamento: Importante metodologia para educar e conscientizar pessoas sobre a importância das informações para as organizações. O recurso humano mostra-se o mais fragilizado e propenso a ataques no que diz respeito à engenharia social ,durante muitas vezes é o responsável pela manipulação que esta na linha de frente no processo de segurança da informação sobre o valor e os impactos que a informação que elas dispõem e manipulam , seja ela de uso pessoal ou institucional. Informar os usuários sobre como age um engenheiro social.

Segurança física: Parte da ação de permitir o acesso às dependências de uma organização somente às pessoas devidamente autorizadas, bem como controle de acesso de funcionários de segurança a fim de monitorar entrada e a saída da organização.

Controle de acessos: Os mecanismos de controle de acesso tem o objetivo de implementar privilégios mínimos aos usuários, a fim de que estes possam realizar suas atividades. O controle de acesso pode também evitar que usuários sem permissão criem, removam ou alterarem contas ou instalem softwares danosos à organização.

Existem diversas situações informações sobre procedimento e boas práticas de como evitar se uma vitima da engenharia social, preservando a informações de maneira pratica, (Peixoto, 2006) descreve como sendo alguns dos maiores erros cometidos dentro do ambiente corporativo que aumentam potencialmente o risco de se tornar uma vítima de engenharia social:

a. Informar senha via telefone é um erro muito grave, pois antes de disponibilizar qualquer tipo de informação, deve-se saber com que se fala e de onde se fala, além de conferir através de identificadores de chamado se o telefone de origem da ligação é realmente o confirmado com o mencionado. É muito importante conferir o motivo pelo qual estão solicitando determinada informação. Existe uma técnica chamada "*Spoofing"* que faz com que o numero exibido pelo identificado de chamado seja aquele desejado pelo fraudador. Portanto não é seguro confiar somente nessa informação para ter certeza que o solicitado é realmente quem diz ser.
b. Os visitantes tem acesso à área interna obtendo contato com informações confidenciais.
c. Entrega de informações ou documentos sem o devido conhecimento real de quem transporte-as.
d. Entrada de pessoas não autorizadas ou principalmente sem identificação, com entradas abertas expostas a qualquer pessoa.
e. Recebimento de informações digitais (flash drive, DVD etc.)_ sem os prévios conhecimentos da procedência de onde realmente vem, e de quem vem, e do que se trata, sem primeiro fazer uma inspeção no material recebido em algum lugar ou equipamento que não comprometa a empresa ou organização.
f. Descarte incorreto de material que se acha inútil, como, exemplo não triturar documentos antes de jogá-los fora e de preferência em diversas lixeiras ou descarte de DVDS CDS e outros sem eliminar definitivamente as informações contidas nestas mídias.
g. Gavetas abertas, material em cima da mesa de fácil acesso a documentos.

h. Jogos online ou mesmo executando em pen-drives ou CD-ROM são passíveis de conter armadilhas, com ativação de Worms, cavalo de troia dentre outros perigos que se escondem por traz jogos envolventes ou diversões oferecidas.
i. Deixar expostos arquivos de backup, não guardando o em lugar seguro e confiável, além de demonstrar explicitamente que é um backup.
j. Nome de usuário e senhas expostas para qualquer um que passar ver ter e ter acesso.
k. Pen-drives, DVDs documentos material particular com bolsas carteiras em cima da mesa ou expostas, com grande facilidade de alguém se apoderar ou ter acesso, principalmente se as portas ou janelas ficam sempre abertas.
l. Programas, documentos digitais gravados em DVDS ou CDs, não sendo devidamente guardados em lugares seguros onde somente aqueles podem ter acesso seriam aqueles portadores da informação.
m. Computador ligado exibindo informações confidenciais como: login de usuário, códigos fonte.
n. Acesso a sites indevidos, não confiáveis, ou fora das políticas de trabalho da empresa.
o. Computador logado com a senha e nome de algum usuário, deixando o uso da estação disponível para alguém não autorizado. Sistemas de alarme desligado desativado ou inoperante, em caso de alguma urgência ou emergência.
p. Softwares em lugares não seguros bem como procedimentos, apostilhas etc. que contenham informações que sirvam como um facilitador em trazer palavras de cunho técnico de modo a disponibilizar ID, senhas sejam elas *default* ou não.
q. Enfeites, como vasos quadro dentre outros, servindo como mera distração fugindo do habitual e tradicional *layout* de arranjo do ambiente de trabalho. Podem ser alvos de suspeita, pois atrás desses “enfeites” podem estar guardados, escondidos ou implantados sistemas de escuta como: gravadores, dentre outros pequenos sistemas que podem colher informações ditas ou vivenciadas naquele ambiente.

> “A maior prova para se ter certeza de que você será a próxima vítima de engenharia social é simplesmente subestimar o praticante desta arte”. Mas como saber ao certo quem é afinal o engenheiro social naquele dado momento, lugar ou situação? Na primeira instancia. Apenas desconfiar de algum suspeito à medida que vá adquirindo o conhecimento das técnicas padrões e revolucionarias da engenharia social. E assim percebendo algumas gafes do engenheiro social, deixará a incerteza para então capturar o alvo certo entra e capturar o alvo errado. (Peixoto, 2006 P. 54)

4.1 Estatísticas de ataques

Segundo informações dos gráficos do Cert.br - Centro de estudos, resposta e tratamento de incidentes de segurança da informação no Brasil, informam que quase metade dos ataques e incidente de segurança da informação estão relacionados com algum tipo de fraude ,onde incidente de segurança da informação pelo Dicionário Houaiss:

> *“é qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.*

No gráfico abaixo, percebemos que de 1 milhão de incidentes no pais ,mais de 400 mil estão relacionados com algum tipo de fraude, onde provavelmente estes , no contexto de tecnóloga da informação, foram utilizado por meio de engenharia social comprovando o grande impacto , em números, que estes perfazem na

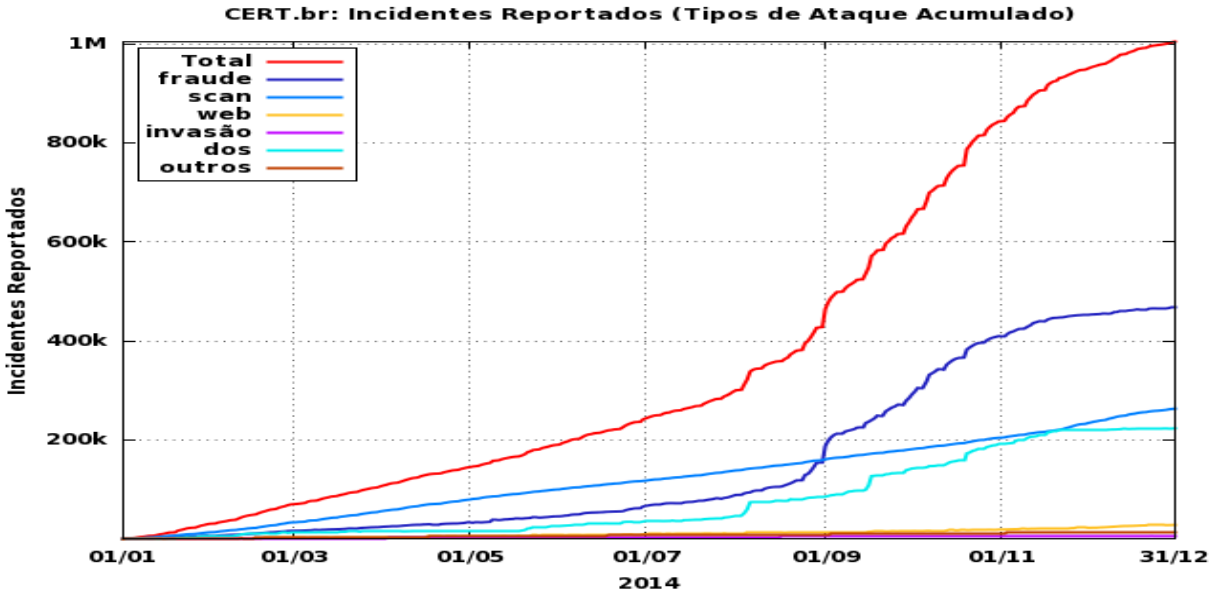

Figura_6 estatística de incidentes

Fonte http://www.cert.br/stats/incidentes/2014-jan-dec/tipos-ataque.html

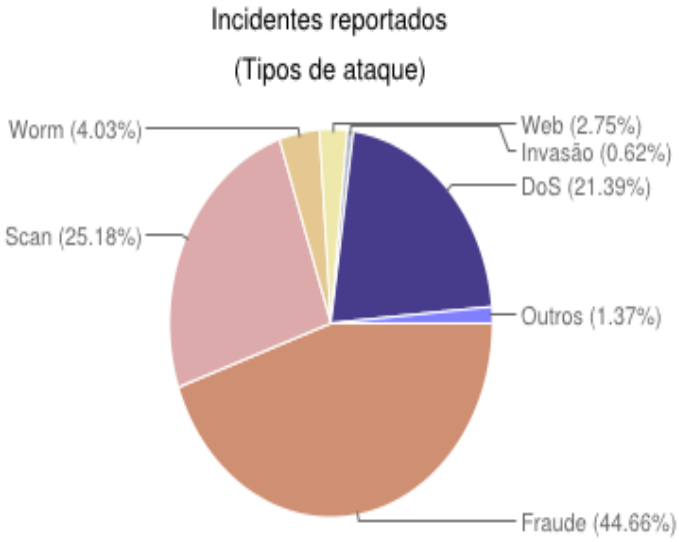

Figura_7 Gráfico incidentes

Fonte: http://www.cert.br/stats/incidentes/2014-jan-dec/tipos-ataque.html

5. CONSIDERAÇÕES FINAIS

O presente documento apresentou a engenharia social de forma simples, fazendo uma relação desta com a segurança da informação, enfatizando as vulnerabilidades do comportamento humano no ambiente corporativo, expondo principais formas de ataque por meio da engenharia Social. A ideia foi buscar informações e traduzi-las de forma simples orientando e conscientizando a todos que se utilizam da informação pelos meios tecnológicos. Percebemos que sempre devemos ter o máximo de cuidado em relação ao comportamento humano e que diversas práticas podem ser utilizadas para minimizar as ameaças, compreendemos que o fator humano torna-se o elo mais fraco de toda a cadeia de segurança, onde tudo pode ser perdido com um simples comportamento de risco, trazendo consequências graves. Subestimar ou achar que nunca será o alvo de um ataque de um engenheiro social faz com se torne mais uma provável vítima, fechando a porta depois de ser atacado, é importante salientar que mesmo com o máximo de cuidados ainda corremos o risco de cair em varias armadilhas.

REFERÊNCIAS

(https://pt.wikipedia.org/wiki/Perfil_(comunidade)acessado em 22/02/16. Acessado em 23/02/16.

Braga, Pedro Henrique da Costa- **Técnicas de Engenharia Social** A GRIS - Grupo de Resposta a Incidentes de Segurança -Cidade Universitária - Rio de Janeiro/RJ.
Fonte: Fonte: http://convergecom.com.br/tiinside/seguranca/mercado-seguranca/03/07/2015/brasil-continua-como-maior-vitima-de-ataques-de-phishing/. Acessado em 23/02/2016.

Dantas, Marcus Leal- **Segurança da informação**: uma abordagem focada em gestão de riscos. / Marcus Leal Dantas. – Olinda: Livro Rápido, 2011.
Notas de aula professor Jefferson costa – disponível www.jefessoncosta.com.br
http://www.profissionaisti.com.br/2013/10/**engenharia-social-as-tecnicas-de-ataques-mais-utilizadas**/acessado em 23/02/2016.

PEIXOTO, Mario C. P- **Engenharia social e segurança da informação na gestão corporativa**. Rio de janeiro: Brasport, 2006.

Souza, Diego dos santos,TCC Rio de Janeiro, 2003 Disponível em :http://pt.slideshare.net/diegosouzapc/tcc-pronto-33102992. Acessado em 23/02/2016
CARDOSO JÚNIOR, Walter Felix. **Inteligência empresarial estratégica**. Tubarão: Ed. Unisul, 2005.