UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE – UERN
FACULDADE DE CIENCIAS NATURAIS E EXATAS – FANAT
DEPARTAMENTO DO INFORMÁTICA – DI

VINNÍCIUS LUAN DOS SANTOS COSTA

SEGURANÇA DA INFORMAÇÃO: USO DA ENGENHARIA SOCIAL COMO MÉTODO DE ATAQUE E COMO MITIGAR SEUS EFEITOS.

Mossoró/ RN

2016

VINNICIUS LUAN DOS SANTOS COSTA

SEGURANÇA DA INFORMAÇÃO: USO DA ENGENHARIA SOCIAL COMO MÉTODO DE ATAQUE E COMO MITIGAR SEUS EFEITOS.

Monografia apresentada a Universidade do Estado do Rio Grande do Norte – UERN, como um dos pré-requisitos para a obtenção do grau de bacharel em Ciências da Computação.

Orientador (a): Profª. MSc. Alexsandra Ferreira Gomes

Mossoró/RN

2016

Catalogação da Publicação na Fonte.

Universidade do Estado do Rio Grande do Norte.

Costa, Vinnícius L. S.

Segurança Da Informação: Uso Da Engenharia Social Como Método De Ataque E Como Mitigar Seus Efeitos. / Vinnícius Luan dos Santos Costa – Mossoró, RN, 2016.

60f

Orientador(a): Profª. Msc. Alexsandra Ferreira Gomes.

Monografia (Bacharelado) Universidade do Estado do Rio Grande do Norte. Curso de Ciências da Computação.

1. Segurança da Informação. 2. *Pentest*. 3. Vulnerabilidades. 4. Engenharia Social. 5. Soluções.

UERN/BC CDD 004

Bibliotecário:

VINNÍCIUS LUAN DOS SANTOS COSTA

SEGURANÇA DA INFORMAÇÃO: USO DA ENGENHARIA SOCIAL COMO MÉTODO DE ATAQUE E COMO MITIGAR SEUS EFEITOS.

Monografia apresentada como pré-requisito para obtenção do título de Bacharel em Ciência da Computação da Universidade do Estado do Rio Grande do Norte – UERN, submetida à aprovação da banca examinadora composta pelos seguintes membros:

Aprovado em: 08/12/2016

Banca Examinadora

Alexsandra Ferreira Gomes

Profª. Msc. Alexsandra Ferreira Gomes. (Orientadora)
Universidade Do Estado Do Rio Grande Do Norte – UERN

Luana Priscilla Rodrigues da Costa Lima

Profª. Msc. Luana Priscilla Rodrigues da Costa Lima
Faculdade Mater Christi - FMC

Ceres Germanna Braga Morais

Profª. Msc. Ceres Germanna Braga Morais
Universidade Do Estado Do Rio Grande Do Norte – UERN

DEDICATÓRIA

A Deus, pois em seu infinito amor resolveu escolher os menores, os mais fracos, para realizar Sua grande obra.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pois em seu amor e bondade, me deu todas as capacidades e faculdades para a realização deste trabalho. Em segundo lugar gostaria de agradecer especialmente a minha família por ter me dado todo o suporte necessário. A minha amiga, companheira de todas as horas, e meu amor Pâmella Rochelle Rochanne Dias de Oliveira, por ser o meu socorro nas horas mais difíceis e meu sorriso nos momentos mais felizes.

E também:

A toda a Faculdade de Ciências Exatas e Naturais (FANAT/UERN), em especial ao Departamento de Informática da Universidade do Estado do Rio Grande do Norte DI/UERN. De forma específica à pessoa de Alexsandra Ferreira Gomes, minha orientadora e amiga nesta reta final da graduação. Ainda a todo corpo docente do Departamento de Informática e a todos os técnicos que contribuíram de forma direta e indireta na conclusão do curso.

A todos os meus amigos, que caminharam junto comigo, conselheiros, companheiros das horas vagas, mas também suporte quando necessitei.

Aos meus amigos que não estão na universidade, em especial Allan Pablo, Alanzinho, Ticiana, Pedro, Ruan, Eliza, enfim a todos os “amiguinhos”.

A Comunidade Católica Shalom e todas as minhas autoridades por se mostrarem como o meu sustento espiritual, que em suas orações e súplicas me deram força para não desistir nesta reta final.

A todos que me deram a graça de boas conversas, que me auxiliaram em todo o meu processo formativo, que me permitiram ser quem me tornei.

RESUMO

Este trabalho busca investigar como a Engenharia Social age para burlar sistemas de segurança da informação, atentando para a compreensão de como a informação é construída, qual sua importância, como são descobertas as vulnerabilidades e como ocorre o processo de efetivação de uma defesa sólida e bem estruturada. O que se dá por meio da análise da metodologia OWASP para a realização de um *pentest*, com o intuito de buscar as falhas recorrentes em aplicações *web*, fornecendo um paralelo entre elas e como a Engenharia Social pode ser utilizada como fator potencializante em um ataque. Acredita-se que a relevância da presente pesquisa, está no fato de ampliar o seu foco além do contexto tecnológico para o humano. Uma vez que as falhas de segurança da informação estão diretamente ligadas a falhas comportamentais. Dessa forma, procura-se aqui perceber como a Engenharia Social explora as falhas tecnológicas e humanas do acesso a informação, atentando para suas consequências e como se dá o combate destas. Para tanto tem-se como base uma revisão bibliográfica com ênfase nos principais autores que tratam dos conceitos que serão abordados.

Palavras-Chave: Segurança da Informação; *Pentest*; Vulnerabilidades; Engenharia Social; Soluções.

ABSTRACT

This paper seeks to investigate how social engineering acts to circumvent information security systems. Attempting to understand how information is constructed, how important it is, how vulnerabilities are discovered, and how the process of effecting a solid, well-structured defense occurs. This is done by analyzing the OWASP methodology for the realization of a pentest, in order to search for the most recurring faults in web applications, providing a parallel between them and how social engineering can be used as a potentiating factor in an attack. It is believed that the relevance of the present research is in the fact of extending its focus beyond the technological context to the human. Since information, security flaws are directly linked to behavioral failures. In this way, we try to understand how social engineering explores the technological and human failures of access to information, paying attention to its consequences and how to combat them. For this, a bibliographic review is based on the main authors dealing with the concepts discussed here.

Keywords: Information Security; Pentest; Vulnerabilities; Social Engineering and Solutions.

LISTA DE IMAGENS

LISTA DE SIGLAS

ABNT – Agência Brasileira de Normas Técnicas.

AOL – America Online.

CERT – Centro de Estudo, Resposta e Tratamento de Incidentes de Segurança no Brasil.

CNSS – Comitê sobre Sistemas de Segurança Nacional.

DNS – Sistema de Nomes de Domínio.

FBI – Departamento Federal de Investigação

IDS – Sistemas de Detecção de Intrusão.

IDP – Sistema de Proteção de Intrusão.

ISSAF – Quadro de Avaliação de Segurança de Sistemas de Informação.

IP – Protocolo de Internet.

HIDS – Sistemas de Detecção de Intrusão em Hosts.

NIDS – Sistemas de Detecção de Intrusão em Redes.

NIST - Instituto Nacional de Padrões e Tecnologia.

OSSTMM – Metodologia Manual de Testes de Segurança de Código Aberto.

OWASP – Projeto de Segurança de Aplicações Abertas na *Web.*

PENTEST **–** Testes de Penetração.

PRI – Plano de Resposta a Incidentes

SELM - Minas Terrestres para Engenharia Social

SMTP – Protocolo de Transferência de Correio Simples.

SQL – Linguagem de Consulta Estruturada.

TCP – Protocolo de Controle de Transmissão.

UDP – Protocolo de Datagrama de Usuário.

URL – Localizador de Recursos Universal.

XML – Linguagem de Marcação Extensiva.

SUMÁRIO

INTRODUÇÃO

Sabe-se que atualmente a informação é o bem mais precioso de empresas e usuários (referenciar), sendo também muito desejável e visado por pessoas ou grupos mal-intencionados, que têm como finalidade o seu roubo ou destruição por diversos motivos.

Com isso, a preocupação com a segurança da informação por parte das empresas e dos usuários é real. Hoje diferentemente do que em qualquer outra época, mantê-las a salvo representa a lucratividade e competitividade entre as empresas.

A segurança da informação pode ser compreendida como uma área de estudo dedicada à manutenção das informações, visando restringir o seu acesso a terceiros que busquem danificá-la ou impossibilitarem o seu acesso. Dentre os principais estudos sobre a segurança da informação, um em especial se apresenta como de difícil combate e solução em relação as ferramentas tecnológicas, a Engenharia Social (referencial). Esta é utilizada tendo o seu enfoque no fator humano, considerado o elo fraco da corrente. Há assim um caminho diretamente proporcional, quanto mais evoluem as tecnologias da segurança, na mesma proporção o fator humano será explorado.

Na busca pelo encontro das vulnerabilidades tecnológicas e humanas, uma ferramenta se apresenta como de grande relevância, o *pentest*. Este consiste na procura por fragilidades tanto no nível técnico como a nível humano e psicológico, pois o responsável pelas buscas, se utilizará de ferramentas computacionais e comportamentais para de maneira direta ou indireta obter o acesso a informações das quais não possui.

A partir desse contexto, a presente pesquisa se propõe a compreender onde estão as principais falhas que podem ser exploradas por engenheiros sociais e apresentar algumas soluções que minimizem ao máximo as vulnerabilidades encontradas. Tendo como objetivo geral da pesquisa, perceber como a Engenharia Social explora as falhas tecnológicas e humanas do acesso a informação, atentando para suas consequências e o combate destas. Que acontecerá por meio dos seguintes objetivos específicos:

- Verificar qual a importância da segurança da informação a partir do aspecto humano e tecnológicos;

- Identificar as principais falhas através da análise de um *pentest* baseada na metodologia OWASP e como a Engenharia Social pode ser utilizada;
- Investigar em que afetam as falhas encontradas e revelar algumas possíveis soluções.

Para obter o sucesso desejado, se faz necessário o levantamento bibliográfico sob os conceitos que envolvem a segurança da informação e da Engenharia Social, na busca da identificação de vulnerabilidades que podem ser encontradas em ambientes corporativos e/ou residenciais. Bem como uma pesquisa sobre quais os tipos de ataques em aplicações *web* que ocorrem com maior frequência, como a Engenharia Social pode ser aplicada nestes e buscar apresentar algumas soluções para o enfraquecimento da efetividade dos ataques. Além da pesquisa bibliográfica utilizamos como aspecto metodológico a metodologia OWASP, que é voltada para a análise de vulnerabilidades em aplicações *web*, com base nos pensamentos dos autores Meucci (2008), Harold (2010) e Basso (2010).

Ainda como parte do processo metodológico, apoiando-se em autores que tratem do aspecto não-técnico da Engenharia Social, pretende-se desenvolver uma mini cartilha que apresente os principais ataques realizados por um engenheiro social e seu possível combate.

Acredita-se que o presente trabalho possui relevância para a área Ciência da Computação uma vez que diferentemente dos modelos tradicionais com foco nos aspectos tecnológicos, este visa abordar a problemática da Engenharia Social a partir de uma visão do humano e do social, ou seja, de como esta exerce seu papel no roubo de informações. Dessa forma a pesquisa foi dividida em quatro principais capítulos, visando traçar um caminho seguro na abordagem dos temas propostos.

No primeiro capítulo, "*A segurança da informação em sistemas e na web*", serão abordados conceitos principais acerca da segurança da informação, primeiramente construindo a ideia de como a informação surge e quais são os fatores derivantes que originam a mesma. Em seguida, será utilizada a referenciação teórica para abordar os pilares de sustentação da segurança da informação não somente a nível tecnológico, mas procurando trazer o fator humano e social também como linha de defesa. E por fim será tratado quais as principais ameaças digitais que podem ocasionar a perda de informações.

No segundo capítulo, "*Falhas na segurança da informação exploradas pela Engenharia Social*", será abordado a temática de como se dá a realização das buscas por vulnerabilidades através da execução de testes de penetração ou *pentests*, baseados na metodologia OWASP, que aborda as aplicações *web*. Em seguida se buscará realizar um paralelo entre as principais vulnerabilidades nessas aplicações e como o uso da Engenharia Social pode ser utilizado para explorar essas falhas.

Já o terceiro capítulo, "*Engenharia Social – uma arte a ser explorada*", tem como foco mostrar quais os principais tipos de ataque que podem ser realizados por um engenheiro social. Dividindo-o de acordo com as suas características principais, bem como o "passo-a-passo" de um ataque. Como meio de ilustração serão trazidos casos reais das técnicas da Engenharia Social que foram utilizadas para burlar sistemas informáticos.

Por fim o quarto capítulo, "*Mitigação das vulnerabilidades*", trata propriamente dito das nossas contribuições para a área de estudo e pesquisa em questão. No qual foi realizada uma sintetização de métodos de prevenção a ataques relacionados a Engenharia Social, levando em consideração aspectos humanos e psicológicos para a mitigação das vulnerabilidades encontradas. O que se dá, nesse caso, através de técnicas específicas, como a criação de políticas de segurança da informação. Para concretizar o estudo, será produzida uma mini cartilha que exibe os principais questionamentos de como produzir efeitos positivos contra os ataques da Engenharia Social.

1. A SEGURANÇA DA INFORMAÇÃO EM SISTEMAS E NA *WEB.*

Neste capítulo serão abordadas algumas questões que envolvem a segurança da informação, em um primeiro momento será feita uma breve contextualização contemporânea de como a informação é construída e qual a sua importância para empresas e usuários. Em seguida será abordada a segurança da informação propriamente dita, em sistemas e na *web*, para em seguida discorrer sobre o uso da Engenharia Social como uma ferramenta para acesso a informações não autorizadas, bem como quais as principais ameaças digitais à segurança da informação.

A medida em que o tempo passa, a globalização cresce e gera efeitos quase que imediatos no que diz respeito a comunicação e a propagação da informação, em meio a essa nova conjuntura de distribuição dos dados, as empresas e organizações têm a sensação de que suas informações não estão sendo salvaguardadas de forma segura. Para que esse sentimento não seja transmitido e sentido, as empresas estão constantemente investindo em novas políticas de segurança para que os dados e informações mais relevantes se mantenham seguros em meio ao caos da Internet, que tem sido instaurado por diversos ataques.

A informação atualmente é um dos maiores patrimônios que uma empresa possui, deixar com que essas informações sejam acessadas indevidamente por terceiros preocupa a todos que estão envoltos e ligados a utilização do sistema falho. Com os dados expostos a qualquer um, a empresa perde confiança e credibilidade frente aos seus concorrentes. Mas que bem é esse e por que a sua segurança é tão importante?

Para melhor entender e compreender o que significa o termo informação e sua importância, primeiramente devemos conceituar o que são “dados”, uma vez que é a partir dos dados que surgem as informações. Para Chiavenato (2008), dados são apenas parte de um todo que precisam ser trabalhados para que sejam extraídas as informações, como se observa abaixo.

> Dados são os elementos que servem de base para a formação de juízos ou para a resolução de problemas. Um dado é apenas um índice ou um registro. Em si mesmo, os dados têm pouco valor. Todavia, quando classificados, armazenados e relacionados entre si, os dados permitem a obtenção da informação. Os Dados exigem processamento (classificação, armazenamento e relacionamento), para que possam

> ganhar significado e consequentemente informar. A Informação apresenta significado e intencionalidade, aspectos que a diferenciam do dado simples (*Ibid*. p. 505).

Dentro dessa mesma visão Bellinger (1996, p. 226), afirma que os "dados são apenas pontos inúteis, sem sentido no espaço e no tempo, sem referência a outro espaço ou tempo, enfim, um evento, uma carta, ou uma palavra, todos fora do contexto. "

Logo, é possível compreender que isoladamente o dado não tem nenhum valor substancial ou significativo, precisando assim ser processado (classificado, armazenado e relacionado) por alguma ferramenta, para que através do processamento desses dados sejam obtidas informações de relevância específica para as organizações. As informações obtidas sempre irão variar dependendo do contexto, seja ele cientifico, tecnológico, artístico etc.

Através dos dados é que são obtidas as informações necessárias e são elas que norteiam as estratégias e ações que serão tomadas pela empresa, dentro desse contexto de substancialidade e importância da informação Rezende e Abreu (2000) dizem que, "a informação tem valor altamente significativo e pode representar grande poder para quem a possui, indivíduos ou instituição", e completam afirmando que, "a informação e o conhecimento serão os diferenciais das empresas [...] que pretendem se destacar no mercado" (*Ibid.*), ou seja, sem informações consistentes e verídicas, as empresas perdem competitividade e poder de combate frente aos seus concorrentes por não saberem exatamente qual a necessidade dos seus clientes.

Segundo a ABNT. NBR ISO/IEC 27002:2005 (2005, p. 9), define informação como:

> É um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a grande variedade de ameaças e vulnerabilidades.

Tendo disponibilizado qual o valor e importância da informação para as empresas e organizações, surge então a necessidade de manter esses dados e informações seguros,

como uma derivação dessa necessidade surgem também os métodos de segurança da informação.

1.1 Segurança da informação: Conceitos principais

Como abordamos na introdução alguns aspectos gerais sobre segurança da informação, a partir de agora iremos nos aprofundar mais sobre esse tema de tão grande relevância tanto para as empresas quanto para as pessoas, para Beal (2005) segurança da informação é "a proteção dos itens de informação em combate a ameaças que comprometam a sua integridade, confidencialidade e disponibilidade".

Para Sêmola (2003), ela pode ser definida como uma área de conhecimento que se dedica a proteção dos ativos de informação contra o acesso não autorizado, alterações indevidas ou que de alguma forma tornem indisponíveis as informações. Já para a ABNT (2007), com a norma ISO/IEC 27002:2007 "a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio" e completa "a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade. ", para Nakamura (2007), a integridade, a confidencialidade e a disponibilidade das estruturas de redes são fundamentais para o bom funcionamento das organizações.

A preocupação com a segurança das informações não é desnecessária ou equivocada, pois a medida em que o tempo passa e com o advento das tecnologias que permitem cada vez mais mobilidade, as empresas se tornaram mais vulneráveis e o principal alvo dos ataques cibernéticos, caso medidas protetivas não sejam tomadas, a empresa corre sérios riscos do ponto de vista da proteção dos dados, como enfatiza Laureano (2005, p. 11),

> Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças (*Ibid*.).

É possível notar que ambos os autores possuem uma visão semelhante sobre a necessidade de existirem sistemas que garantam a segurança da informação, e para garantir que essa segurança seja de fato eficiente tem de estar alicerçada sobre três pilares principais: a integridade, a confidencialidade e a disponibilidade da informação.

Cada um destes três pontos tem sua importância e particularidade dentro de um sistema que garanta a segurança da informação, pois cada um deles exerce um papel diferente e fundamental na defesa e proteção da informação:

- **Integridade:** visa garantir que a informação transmitida entre o emissor e o receptor não foi modificada ou falsificada por usuários não-autorizados, mantendo assim, toda a sua condição original. (NAKAMURA, 2003)
- **Confidencialidade:** visa impedir que usuários não autorizados obtenham o acesso as informações sensíveis ou sigilosas, todas as informações devem ser protegidas. (CAMPOS, 2014)
- **Disponibilidade:** visa garantir que a informação necessária para o usuário ou para processos autorizados que precisem, estará disponível ou será gerada sempre que solicitada. (STALLINGS, 2010)

Alguns outros autores, porém, vão além dessas três características, como para Sêmola (2003), que acrescenta a estas:

- **Legalidade:** que visa garantir que a informação foi produzida de forma legal.
- **Autenticidade:** é a garantia que num processo de comunicação, os remetentes sejam quem dizem ser e que a mensagem transmitida ou informação não sofreu alteração após seu envio ou sua validação.

Quando se fala em manter seguros os dados e as informações, logo vem à mente a utilização de um *firewall* ou simplesmente a utilização de antivírus, antigamente era possível ter como afirmativa essa frase, como diz Piper (2011), ao indicar que até 1990, virtualmente, todos os ataques poderiam ser bloqueados apenas com o uso do *firewall*, porém com o transcorrer do tempo, os ataques estão se tornando cada vez mais sofisticados e esse modelo simplista não consegue manter a proteção adequada e necessária, assim, para manter um nível elevado de segurança na rede empresarial, é necessária a introdução de várias ferramentas distintas, entre elas está o próprio *firewall*, a criptografia, IDS (Sistema de Detecção d Intrusão) e/ou IPS (Sistema de Proteção de Intrusão), entre outros.

A grande diferença entre um *firewall* e um IDS/IPS é a forma como o pacote é tratado, para Piper (2011) no *firewall* a análise do pacote é feita identificando apenas o endereço e a sua porta de origem, independente do que venha a ser o conteúdo (*payload*), já os IDS/IPS, foram desenvolvidos para realizar a análise do conteúdo do pacote e dependendo da sua configuração que pode ser pré-estabelecida, emitir alertas, bloquear ou permitir o tráfego das informações, porém o *firewall* não é, em hipótese alguma descartável, ao contrário, ele é fundamental na busca pela segurança dos dados, afirma Nakamura (2007, p. 171) "*Firewalls* são a primeira linha de defesa, delimitando a organização virtual e impedindo uma exposição direta aos ataques de origem externa." Entretanto reconhecendo sua limitação, também afirma que, "*firewalls* não podem impedir todo tipo de ataque [...] O monitoramento é necessário para detectar eventuais sobreposições" (*Ibid.).*

Bace e Mell (2011) definem esses sistemas como a realização do processo de monitoramento de eventos que ocorrem em uma rede e analisa-los na busca sinais de intrusão, eventos esses que podem ser uma tentativa de comprometimento da integridade, confidencialidade e disponibilidade da informação, afetando diretamente o bom funcionamento da empresa. Nakamura (2007, p. 242) também afirma que "um Sistema de Detecção de Intrusão [...] é uma tecnologia essencial para a proteção de uma rede".

Os sistemas IDS são bem mais robustos que os tradicionais *firewalls*, uma vez que trabalham intensamente na busca de algum tipo de violação à rede, emitindo alertas de segurança ao reconhecer os primeiros sinais de um ataque, aplicando uma resposta coerente e assim minimizando os seus efeitos. Ele também é capaz de reconhecer problemas quando um dispositivo computacional está falhando e assim notificar o administrador ou responsável. Eles podem ser de três tipos, baseados em *Hosts* (HIDS), baseados em Redes (NIDS), ou podem ser híbridos, uma junção dos dois sistemas. Já os IPSs basicamente têm como objetivo reduzir a quantidade de alarmes falsos e prevenir ataques.

Além do *firewall*, dos IDSs/IDPs, uma outra ferramenta utilizada maciçamente para proteção da informação é a criptografia, sendo o seu papel principal, tornar inelegível uma mensagem para outros usuários que não sejam aqueles que estão se comunicando, é um processo de disfarce da mensagem original, ela serve de base para múltiplas tecnologias e protocolos, como a Infraestrutura de Chave Pública (PKI – *Public Key*

Infrastructure), Segurança de IP (IPSec - *IP Security*), Privacidade Equivalente ao Cabeado (WEP - *Wired Equivalent Privacy*) etc.

Uma definição formal do que seja a criptografia é dada pelo Comitê sobre Sistemas de Segurança Nacional (*Committee on National Security Systems* – CNSS) dos Estados Unidos, "é a arte ou ciência que se preocupa com os princípios, meios e métodos de tornar ininteligível um texto em claro e, inversamente, tornar legíveis informações criptografadas" (CNSS, 2006, p . 19). Já Para Nakamura (2007, p. 287), "é a ciência de manter as mensagens seguras", para o Instituto Nacional de Tecnologia da Informação (ITI) significa "a arte de escrever em códigos de forma a esconder a informação em um texto incompreensível" (Brasil, 2005). Ela possui diversas propriedades importantes como da garantia da integridade, da autenticidade, do não-repúdio e do sigilo.

A criptografia é uma das muitas maneiras encontradas para tornar possível a segurança da informação, porém ela sozinha, assim como o *firewall*, os IDSs, os IDPs, não são capazes de atender a todas as necessidades da empresa, contudo a medida em que são postas em conjunto, conseguem fornecer qualidade no mantimento da integridade, disponibilidade e confidencialidade da informação. Além desses existem atualmente um arsenal de ferramentas para proteger os ativos e dados sensíveis de uma empresa, tanto a nível de *software* quanto de *hardware*, porém todos eles ou a grande maioria estão submetidos a ação ou interferência humana.

1.2 Aspectos humanos na segurança da informação

Apesar das empresas e órgãos estarem constantemente investindo com a proteção e a segurança da informação com o uso de novas tecnologias, de nada adiantará se esse esforço também não for canalizado para a formação do corpo institucional, os funcionários. Estando cada vez mais expostas as ameaças externas, como as invasões, as empresas acabam esquecendo ou deixando de lado as ameaças internas, aquelas pessoas que lidam diretamente com o conhecimento e a manipulação das informações, caso não estejam treinadas, capacitadas e terem consciência nesse processo de proteção da informação, todo o investimento não surtará em benefícios para ela.

Para Mitnick e Simon (2003), uma empresa pode conseguir as melhores tecnologias compradas, *softwares*, *hardwares*, e ainda assim estarem vulneráveis, pois

por mais que o sistema em si seja seguro, ele ainda é administrado por pessoas e é sobre o fator humano que ocorrem inúmeros casos de vazamento de informação, seja por descontentamento, seja por técnicas de Engenharia Social. Mas o que é a Engenharia Social? Algumas definições formais sobre o termo podem ser encontradas, entre elas, podemos citar Peixoto (2006, p. 4), que diz:

> É a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos (*Ibid.*).

Para Vargas (2002), a Engenharia Social pode ser definida de maneira simples, na habilidade de se obter alguma informação ou acesso não-autorizado a algum ambiente ou sistema utilizando técnicas de persuasão, Nakamura (2007) a define como, técnicas que tem como base a exploração de fraquezas humanas e sociais, no lugar das tecnológicas e "tem por objetivo enganar e ludibriar as pessoas assumindo uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização". (*Ibid.* p. 70), para Davis, Bodmer e Lemasters (2010), ela não é uma exclusividade da informática, sendo assim uma ferramenta onde se exploram as falhas humanas em organizações físicas ou jurídicas. De acordo com Ferreira (2009) têm-se os seguintes significados

> *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 (*Ibid.* p. 754). E *social*: da sociedade ou relativo a ela, sociável (*Ibid.* p. 1864).

Logo pode-se assim então defini-la como, a aplicação do conhecimento cientifico e empírico para se obter informações privilegiadas, onde a vítima é manipulada ou induzida a fornecer dados restritos a pessoas não-autorizadas. Esse tipo de ataque visa o elo mais fraco, o ser humano.

Os exemplos clássicos de Engenharia Social, consistem em uma pessoa se passar por um técnico que faz a manutenção da rede e para realizar o reparo, precisa de acesso remoto ao sistema. Um exemplo real pode ser encontrado na *America Online* (AOL) em

1998, onde um indivíduo obteve dados da AOL e fez a solicitação de mudança no registro de domínio DNS, modificando o trafego para um equipamento que não era o provedor.

Porém não é preciso ir tão longe, o uso da Engenharia Social está em todo canto e pode acontecer de muitas formas, por exemplo, quem nunca recebeu um *e-mail* de instituições bancárias da qual não possui nenhum vínculo? Ou algum anexo com a frase "veja nossas fotos como ficaram legais"? Um outro exemplo muito notório tempos atrás, era o recebimento de ligações de um falso sequestro onde o bandido simulava a voz do falso raptado com o intuito de enganar a vítima e solicitar uma recompensa pela libertação do "sequestrado", para Bosworth & Kabay (2002. p. 29) quando é tratado o tema da Engenharia Social afirma que, as falhas humanas são responsáveis pelos erros tecnológicos, dizendo, "o problema com as máquinas são as pessoas".

É possível então constatar, que por mais seguros que possamos nos sentir, não estamos de fato, como ditos, a Engenharia Social pode ser usada a qualquer instante e de muitas maneiras para se obter alguma informação, dentre inúmeras ferramentas podemos encontrar:

- ***Phishing Scan*:** São os falsos *e-mails*, que geralmente solicitam alguma mudança no cadastro de *login* e senha, também pode ser conhecido como *Fakemail.*
- ***Chats*:** Se passar por alguém que não é, se torna uma tarefa relativamente simples nas salas de bate-papo.
- **Telefone ou VoIP (Voz sobre IP):** Passar-se por uma vítima de um sequestro ou gerente de loja do qual se tem cadastro, é uma das clássicas ferramentas da Engenharia Social.
- ***Dumpster diving* (Mergulho no lixo):** Consiste em buscar informações em materiais que são descartados no lixo, como documentos, relatórios etc.
- ***Spyware*:** É um ***s**oftware* "espião" usado para o monitoramento oculto de atividades realizadas pelo computador.
- ***Footprint:*** É utilizado quando não se consegue obter as informações por meio de ligações, e-mails etc, então usa-se softwares maliciosos para se obter as informações necessárias ao ataque, ou seja, é a construção de perfil completo do alvo.
- **Redes sociais:** Dificilmente hoje, uma pessoa não possui uma conta no *Facebook, Twitter, Instagran*, fornecendo informações pessoais, como perfil, localização,

bens pessoais de forma pública. Essa é uma das principais armas utilizadas atualmente.

Além dessas, ainda é possível encontrar outras ferramentas que podem ser utilizadas, porém com menor relevância nos dias de hoje, como o uso de cartas, fax, “surfar nos ombros” que é bisbilhotar o que está sendo escrito sem que o outro perceba. Por mais que sejam ferramentas “fora da moda” ainda conseguem obter excelentes resultados dependendo do alvo.

A prevenção desse tipo de ataque é dificultoso, pois geralmente as empresas não estão preocupadas em direcionar recursos para treinamento e capacitação do capital humano, facilitando assim a ação de *hackers* que utilizam a Engenharia Social como arma inicial para um ataque. O ser humano é imperfeito, podendo tomar decisões precipitadas ou não comuns em situações de risco ou de um alto grau de criticidade e em função disso, sempre existirão brechas em relação ao caráter ou comportamento a serem exploradas eficazmente.

Para reduzir estes riscos é necessário que as empresas criem políticas de segurança normatizadas e bem divulgadas, para que aqueles que utilizam o sistema saibam como proteger as informações que estão ao seu alcance e em seu poder, também se faz necessário o treinamento periódico a todos da empresa, sem exceção, onde devem ser explorados os métodos comuns de intromissão, bem como as técnicas e estratégias de prevenção, por exemplo, ao detectar alguns sinais de ataque, a informação deve ser passada a todos, para que os outros não sejam ludibriados.

E mesmo com todo o treinamento e capacitação, a empresa estará sujeita a falhas, e elas ocorrerão, para isso, é necessário criar um plano de resposta a incidentes, que se trata de um documento que estão descritas as diretrizes gerais e quais os procedimentos para tratar os principais incidentes a segurança que podem ocorrer, fornecendo ao suporte, instruções sobre quais medidas tomar para a definição e correção das falhas, este plano também fornece a habilidade para a utilização dessas informações para reparar ou realizar a prevenção de ocorrências similares, aprimorando assim a segurança de uma forma geral nas empresas e organizações.

Como é possível perceber nem mesmo a mais eficiente segurança, é suficientemente perfeita e sempre estará sujeita a falhas, seja ela de cunho humano

explorada massivamente pela Engenharia Social, seja ela de cunho tecnológico, como as ameaças encontradas na *web*, os vírus, trojans entre outros que iremos abordar.

1.3 Ameaças digitais de maior relevância

Os profissionais que trabalham no âmbito da Segurança da Informação travam batalhas diárias contra as ameaças digitais, que na *web* são inúmeras e que podem causar imenso prejuízo as empresas. As batalhas travadas pelos profissionais de segurança da informação são trabalhosas, pois nesse meio, os invasores estão um passo à frente e esses profissionais atuam na reparação das falhas usadas por *hackers* e na prevenção contra novos incidentes.

Nakamura (2007) explica que a defesa das informações e das instituições é mais trabalhosa que o ataque, pois para o atacante, basta encontrar uma falha, e se não conseguir, tentar outras até atingir seu objetivo, já a defesa tem de explorar todos os pontos e caso apenas um ponto seja esquecido, todo esforço não será recompensado. A segurança contra essas ameaças varia de acordo com o porte de cada empresa, pois as empresas de pequeno e médio porte não possuem uma boa infraestrutura em TI, seja por falta de investimento financeiro ou por desconhecimento da sua necessidade para manutenção da qualidade dos serviços e produtos oferecidos, ou políticas de segurança que atuem na prevenção e proteção da rede contra *softwares* maliciosos.

Essas pragas virtuais ou *softwares* maliciosos são denominados como *malwares* (Manson, 1999) e atuam diversas maneiras, porém podemos elencar os principais objetivos que são: a perda ou alteração das informações, o roubo de senhas, a queda no desempenho ou paralisação do sistema, não somente de empresa, organizações e até mesmo usuários comuns, todos são diretamente ou indiretamente afetados por eles. Para Hardikar (2008), *malware* é um termo que caracteriza qualquer programa de computador cuja a finalidade seja maliciosa e é classificado em basicamente três tipos: Os vírus, os trojans e os *rootkits*.

Para o NIST (2005, p. ES-1):

> Malware [...] refere-se a um programa que, inserido em um sistema, normalmente de maneira secreta, com a intenção de comprometer com a confidencialidade, integridade, ou disponibilidade da informação da

> vítima, aplicações, ou sistema operacional (SO) ou de outra forma somente atrapalhar a vítima[1]. (Tradução nossa)

É possível entender que *malware*, é o termo aplicado a um programa que foi inserido no sistema de forma obscura e tem como intuito o comprometimento da integridade, da confidencialidade e da disponibilidade dos dados, aplicativos e até o próprio sistema da vítima infectada. As tentativas de violação da privacidade utilizando essas técnicas, elas se tornaram difundidas recentemente (MELL E KENT, 2005).

Entre os principais tipos de *malware*, pode-se classifica-los de acordo com a sua característica, os de ocultação como os *trojans horse*, os que infectam como vírus e *worms*, e os espiões (*spyware e adware*) eles não são os únicos. Assim como as ferramentas utilizadas na Engenharia Social são muitas, os *malwares* também cresceram em número e em formato. Algumas rápidas definições segundo Nakamura (2007) sobre os *malwares* podem ser fornecidas:

- **Vírus:** É um programa que destrói dados ou o sistema do computador, possuem a capacidade de replicação, porém estão limitados a ação do usuário, ou seja, precisa ser ativado por ele. Dentro dessa categoria existem ainda subcategorias como Vírus de Setor de *Boot*, Vírus de Arquivos Executáveis, Vírus de Macros e Vírus de *Scripts*.
- ***Worms:*** É similar ao vírus, sua diferença está na capacidade de auto replicação, espalhando-se rapidamente pela rede, ele pode então causar danos sem ser ativado pelo usuário.
- ***Trojan horse:*** São softwares legítimos que possuem códigos ocultos e realizam atividades não previstas, o usuário não percebe que está infectado e ao utilizar o programa, também está executando funções ilegais como o envio de imagens, abertura de portas etc.
- ***War Dialer*:** Programa que realiza a varredura de números telefônicos na tentativa de encontrar modens ou aparelhos de fax vulneráveis a ataques.

Existem vários desses *malwares* espalhados pela *web*, e pela sua alta disponibilidade e pela facilidade de ser criado ou modificado, aproveitando novas vulnerabilidades em programas ou no sistema, eles são utilizados aliados a outras

[1] *Malware […] refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim.*

ferramentas para realizar diversas formas de ataques, entre elas ataques coordenados, como o DDoS (Negação de Serviço Distribuído), DoS (Negação de serviço), entre outros. É preciso ressaltar que cada sistema possui um meio de ser burlado, por exemplo o Linux pode ser atacado por *worm*, e que o Windows é atacado basicamente por vírus.

As empresas sofrem constantes ataques diariamente e para sua proteção muitas deles acabam recorrendo a utilização do antivírus. Sua complexidade está no reconhecimento do vírus bem como a decifração do código malicioso, pois os vírus, podem se modificar a cada infecção, e a distribuição rápida e eficaz das vacinas não é simples. Ele é fundamental pois atua na primeira linha de defesa do sistema em questão, integrado a um *firewall* de configurações eficientes, evitam boa parte das infecções realizadas por vírus. Um exemplo empresarial de antivírus é o *Gateway* antivírus que fornece segurança integrada à rede, realizando a detecção na camada de aplicação de rede.

As vulnerabilidades encontradas em redes empresariais expostas à ação do uso não somente de *malwares*, como também da Engenharia Social, devem ser reconhecidas e informadas, porém não de qualquer forma. Para análise e mitigação das falhas encontradas pode ser realizada uma auditoria, usando não somente de tecnologias, mas também métodos utilizados pela Engenharia Social que podem influenciar e evidenciar falhas humanas. Essas devem ser direcionados a solucioná-las e podem ser realizadas por empresas específicas ou por *pentesters*[2]. Elas devem seguir um protocolo baseado nas leis vigentes de cada país sobre violação de dados e algumas organizações internacionais regulamentam as etapas a serem realizadas em uma análise ou *Pentest.*

[2] *Pentester*: Aquele que realiza um *pentest.*

2. FALHAS NA SEGURANÇA DA INFORMAÇÃO EXPLORADAS PELA ENGENHARIA SOCIAL.

Neste capítulo serão mostradas quais são as vulnerabilidades na segurança da informação, como essas vulnerabilidades podem ser exploradas a partir de ferramentas conhecidas, tendo como foco o uso do *pentest* como um dos métodos principais na busca por falhas, de maneira a buscar saber quais as políticas e instituições atuam na utilização do *pentest*. Dentre as metodologias que são frequentemente utilizadas no *pentest*, será dada atenção especial para a metodologia OWASP[3], pois ela tem como característica principal as buscas por vulnerabilidades em aplicações *web*. Sendo abordado quais são as principais vulnerabilidades e como o uso da Engenharia Social pode ser utilizada para facilitar o acesso e a exploração das falhas.

A busca por falhas tendo como característica a utilização de um *pentest* é interessante, pois atualmente existem metodologias que abarcam os principais cenários da segurança da informação, como os de aplicações *web*, de sistemas, entre outros.

O *pentest* ou o mundialmente conhecido teste de penetração, é um dos métodos para a realização de auditoria em redes, que tem como finalidade principal a procura por vulnerabilidades que forneçam informações que possibilitem a concretização e efetividade de um ataque externo ou interno, garantindo assim o acesso ao alvo desejado fornecendo-lhes informações privilegiadas as informações e aos sistemas (GIVAROTO e SANTOS, 2013).

Ele é então considerado como um espelho fidedigno de um ataque, pois busca a construção de um cenário real passível de uma atuação ofensiva contra a empresa. Para realização dos testes de penetração é necessário o seguimento de algumas etapas bem definidas, que são: o planejamento, execução e pós-execução, estas informações estão descritas e disponíveis no artigo NIST *Special Publication* 800-115 (Scarfone, et al., 2008). Eles também podem ser divididos em duas funções segundo Osborne (1998), uma com seu foco na gestão ou com seu foco na parte técnica.

[3] OWASP (*Open Web Application Security Project*) – Uma tradução livre dessa sigla é apresentada como Projeto de Segurança de Aplicações Abertas na *Web.*

Para a realização de um teste de penetração legal, é necessária a utilização de diversas ferramentas e métodos para que se obtenha um resultado satisfatório acerca das vulnerabilidades, erros e falhas encontradas. Para essa finalidade existem ferramentas tecnológicas, como os sistemas operacionais voltados para segurança e auditoria em redes. Em sua maioria sistemas operacionais baseados em Linux, como o *Kali Linux, BackTrack, Matrix, Deff* entre outros. Se destacando no cenário atual tem-se o *Kali Linux*, que é definido pelo próprio *site* https://www.kali.org/[4] como, "uma avançada distribuição especializada em Testes de Intrusão e auditoria de segurança".

Sua larga utilização se dá pelo fato de possuir qualidades como a utilização de cerca de trezentas ferramentas de intrusão. De acordo com Givaroto e Santos (2013) e a *Offensive Security*, ele é uma distribuição completa, robusta e atualizada. O *Kali Linux* é uma atualização de um outro sistema baseado em Linux conhecido como *BackTrack*. Sua facilidade de uso não se dá somente pela quantidade de ferramentas que podem ser utilizadas, o fato de ser gratuito e que pode ser utilizado sem a estrita necessidade de instalação no disco rígido, usando-o por exemplo por um *pen drive* ou um *Live* CD, possuir um ambiente gráfico limpo e bem organizado, o torna bastante atrativo e eficiente para complexidade das atividades que podem ser realizadas. A Figura 1 mostra a área de trabalho do Kali Linux.

[4] Site: https://www.kali.org/

Figura 1 – Área de trabalho Kali Linux
Fonte: https://www.kali.org/downloads/

Para que qualquer auditoria aconteça, é necessário seguir uma série de protocolos e regras estabelecidos, não somente por órgãos internacionais, mas também pelas leis vigentes e as políticas de acesso a informação, estas devem ser respeitadas e estritamente executadas, para que todo o processo seja considerado legal e para que não haja transtornos judiciais as empresas ou organizações solicitadas para a realização do processo.

2.1 Políticas e instituições ligadas à realização de *pentests.*

Como dito anteriormente, os testes de penetração realizados numa auditoria, devem seguir todo o processo legal. Os crimes cibernéticos, ou CiberCrimes são ataque a redes corporativas ou pessoais utilizando de técnicas ilegais para obtenção de privilégio

de acesso a informação restrita. Para Wendt (2013), os CiberCrimes são aqueles que têm a característica da prática de delito por intermédio do meio cibernético, ou seja, da Internet.

Dentro desse contexto de excessivos ataques, os testes de penetração mostram como ferramentas fundamentais e eficientes, pois ao simularem um ambiente real de ataque, eles exploram as vulnerabilidades que podem ser encontradas, desde as falhas de origem tecnológica a nível de *hardware* e *software*, como as falhas a nível operacional, cometidas pelos usuários, que lidam diariamente e constantemente com o sistema. Os *pentests* geram resultados consistentes, informando quais medidas devem ser tomadas e quais políticas de segurança devem ser implementadas para sanar as falhas.

Atualmente, no Brasil não se possui um conjunto de leis específicas para o tratamento dos crimes envolvendo toda a diversidade de violações de dados pessoais e empresariais por meio da utilização de ferramentas ilícitas. Entretanto, alguns passos foram dados em relação a tipificação da criminalidade tendo como base os meios informáticos. Um exemplo disso é a lei 12737/12 do código penal brasileiro no artigo 154-A que pode ser encontrado no site: http://www.planalto.gov.br/[5], que expressa:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, tendo como pena detenção de 3 (três) meses a 1 (um) ano, e multa.

Por não existir no cenário atual um conjunto de leis que abarque diferentes meios para a violação de dados protegidos e o acesso ilegal a informação, faz da *Internet* um ambiente propício ao ataque, tornando assim, impunes os invasores e até mesmo dentre os tipos de violações que se enquadram na lei, a pena aplicada bastante branda dada a gravidade da ação e das consequências resultantes desta ação, se torna um agravante e um convite à impunidade. Para explorar as brechas deixadas, evitando assim o desperdício de capital financeiro e o desprestígio da empresa, o *pentest* torna-se uma saída confiável para o fortalecimento da segurança das informações das instituições.

[5] Site: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm#art154a

Os *pentests* são realizados com base em estudos feitos por instituições internacionais, que a partir de dados coletados e informados pelas empresas, são listados os principais tipos de ataques existentes em um determinado espaço de tempo. Foram essas instituições que criaram as principais metodologias na padronização para se realizar uma auditoria. Segundo Fonseca, Vieira e Madeira (2010), pode-se citar algumas de maior relevância como a OSSTMM (*Open Source Security Testing Methodology Manual*), ISSAF (*Information Systems Security Assessment Framework*), OWASP Testing Guide (*Open Web Application Security Project*) e NIST SP800-115 e SP800-042 (*National Institute of Standards and Technology*).

A OWASP por exemplo, é uma fundação que se define como "aberta, dedicada a capacitar as organizações a desenvolver, adquirir e manter aplicações confiáveis" e todos os anos exibe uma lista com os dez principais tipos de ataques em aplicações *web* (OWASP, 2013), (HAROLD, 2010). Ela também indica que as empresas que estão almejando a busca de uma segurança efetiva e de qualidade a não se limitarem ao top 10, incentivando que busquem sempre estar atualizados. Essa lista com os principais ataques será abordada de forma completa no próximo tópico, que aponta os principais métodos de ataque, bem os ataques e a utilização da Engenharia Social.

É possível verificar que a incidência de ataques às redes empresariais sofreu enormes avanços, devido à alta disponibilidade de métodos de invasão, que podem ser encontradas facilmente em uma pesquisa rápida no *Google*. Essa alta incidência pode ser constatada na Figura 2, onde é mostrada uma tabela disponibilizada pela CERT.br (Centro de Estudo, Resposta e Tratamento de Incidentes de segurança no Brasil) e nesse *site* podem ser encontrados dados quantitativos e qualitativos sobre ataques. É possível verificar que entre os anos de 1999 a 2015, houve um aumento de quase 2.300.000,00% (dois milhões e trezentos mil por cento), é possível constatar também que entre os anos de 2014 e 2015, houve uma redução na quantidade de ataques em cerca de 31%.

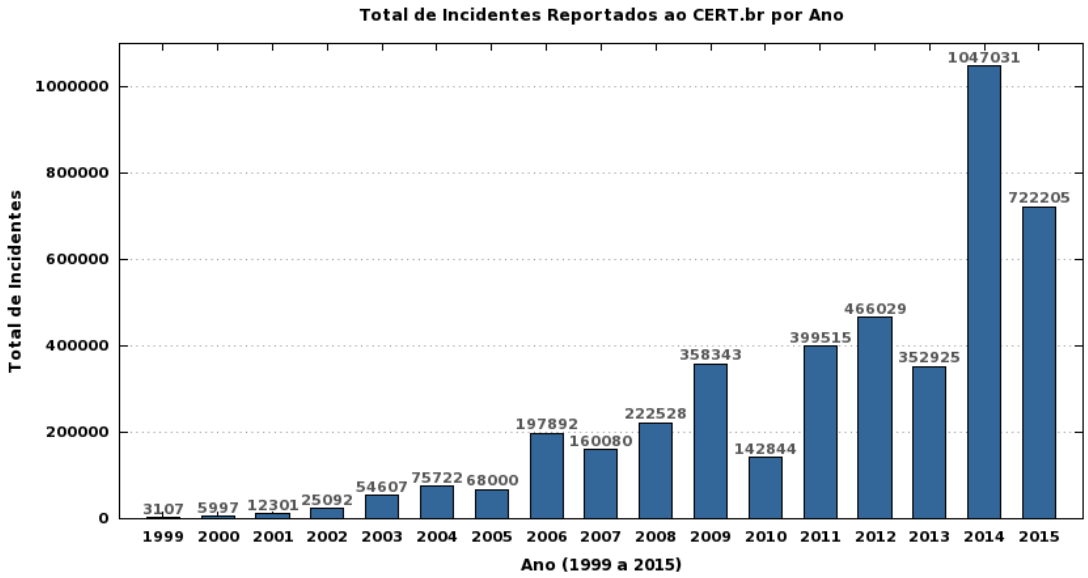

Figura 2 – Incidência de ataques entre os anos de 1999 a 2015.

Fonte: http://www.cert.br/stats/incidentes/

A Figura 3, mostra quais são os principais tipos de ataques reportados ao CERT.br no ano de 2015. Estando em primeiro lugar o *scan*, que é uma varredura de um IP ou domínio a busca de se obter informações técnicas sobre o alvo, em segundo lugar podemos encontrar as fraudes, que são as tentativas de enganar ou obter alguma vantagem, em terceiro lugar apare a *web* que são os ataques que visam o comprometimento de servidores ou a desfiguração das páginas de Internet, em quarto temos o DoS (negação de serviço) quando se utiliza um computador ou vários deles deixar um serviço *offline*, em quinto e sexto lugar, temos as invasões e outros tipos de ataque respectivamente. Todas as definições e demais informações podem ser encontradas no *site* www.cert.br[6].

Frisando que esses dados são apenas de ataques que foram reconhecidos e notificados, não incluindo ataques que as empresas não recorreram a qualquer órgão de segurança por medo de exposição negativa da marca. Também é importante atentar que os dados têm como base os ataques ou tentativas de ataque somente no Brasil.

[6] http://www.cert.br/stats/incidentes/

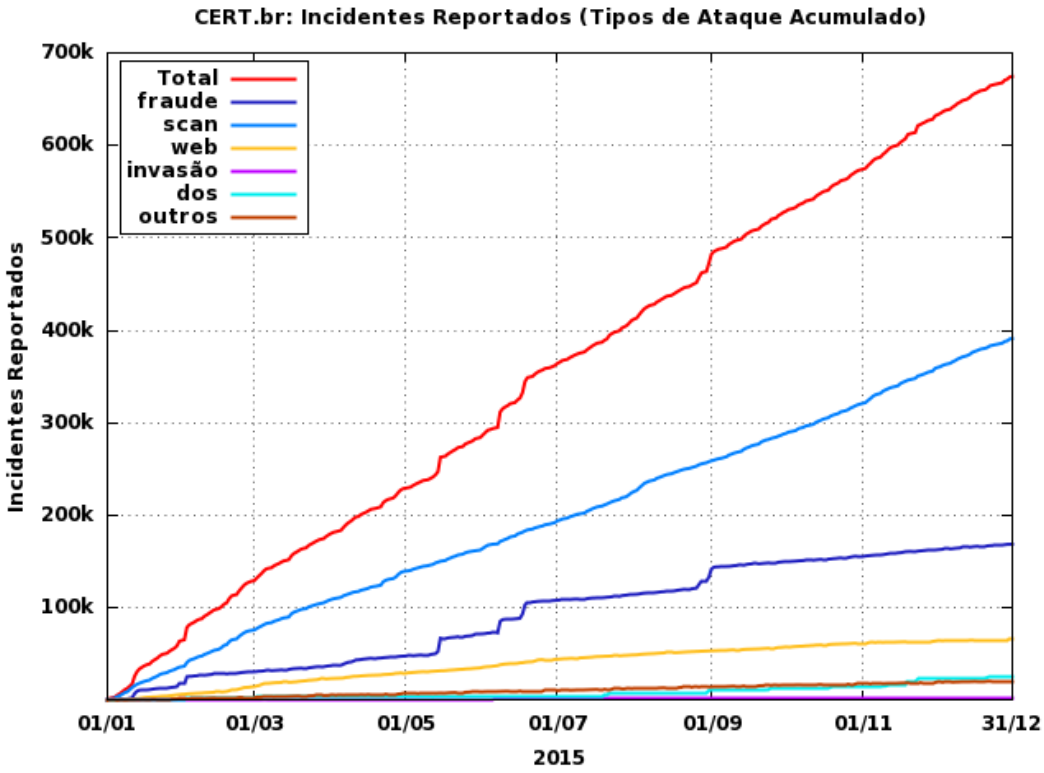

Figura 3 – Principais tipos de ataques reportados ao CERT.br em 2015.

Fonte: http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque-acumulado.html

Portanto, é possível concluir que na medida em que a modernidade avança e que as empresas precisam estar cada vez mais conectadas à rede, elas acabam se inserindo em campo desconhecido e envoltas em um meio perigoso e arriscado para a manutenção da privacidade dos seus dados, pois a cada ano o número de ataques a redes corporativas se mostra elevado e que a dinamicidade dos métodos utilizados põe em risco os modelos de segurança existentes.

Para se proteger devem ser adotadas medidas que tornem a empresa resistente a ataques, porém, como se proteger daquilo que não se conhece? Para responder a essa pergunta, serão abordados os métodos de ataque mais conhecidos baseados na metodologia OWASP, buscando mostrar que o aspecto humano dentro da busca por vulnerabilidades torna-o mais eficaz.

2.2 Principais tipos de ataques baseados na metodologia OWASP

Como foi dito, essa metodologia para a realização de testes de penetração ou *pentest*, abarca principalmente e enfaticamente quais são os dez tipos de ataques que ocorrem com frequência realizados na *web*, de maneira que cada ataque atua de uma forma diferente e necessita de ferramentas diferentes para que seja executado com sucesso. Em alguns será possível observar algumas semelhanças entre um tipo de ataque e outro e que também uma falha pode permitir a abertura para outras.

A metodologia OWASP leva esse nome pois possui o mesmo nome da entidade fundante, tendo como objetivo principal efetivar o encontro e combate a causa da insegurança nos aplicativos *web.* De acordo com Oliveira (2012, p. 49), "os projetos OWASP são divididos em duas categorias: desenvolvimento e documentação" e Meucci (2008) cita alguns dos principais projetos desenvolvidos pela entidade, tais como:

- ***Development Guide:*** é a documentação que tem seu foco na segurança no desenvolvimento do projeto.
- ***Testing Guide:*** é um guia que aborda as principais questões de por que se proteger aplicações na *web*.
- ***Code Review Guide:*** é um guia que aborda as principais práticas para revisão segura de códigos em busca de vulnerabilidades.
- ***Top Ten:*** é o seu guia mais popular, é basicamente um documento que traz as referências e explica as dez principais vulnerabilidades das aplicações na *web* bem como as consequências geradas por essas vulnerabilidades.

Basso (2010, p.20) afirma que, através da OWASP, "é possível encontrar informações sobre as vulnerabilidades e explicações sobre como funcionam os ataques a elas", entretanto para Carvalho (2014). Esse documento não realiza a listagem das vulnerabilidades mais críticas e sim daquelas que ocorrem com maior frequência, pois à medida em que o tempo passa, a lista vai adquirindo novos itens e excluindo outros. A periodicidade em que a lista é atualizada é entre dois e três anos, pois algumas vulnerabilidades novas surgem e outras perdem a sua eficácia ou até mesmo deixam de existir. O último comparativo foi realizado entre os anos de 2010 e 2013 e a Figura 4 mostra essa comparação. Até a finalização desta pesquisa não foi divulgado o comparativo entre os anos de 2013 e 2016.

Nessa figura é apresentada a listagem das vulnerabilidades que são classificadas segundo a quantidade de ocorrências notificadas à organização e são enumeradas de A1

a A10. É possível observar que, no período comparativo da imagem e como afirmam Muniz e Lakhani (2013), a injeção de código (A1) permaneceu no topo da lista, pois continua sendo a que ocorre com maior frequência a ser encontrada em aplicações *web*.

OWASP Top 10 – 2010 (Anterior)	OWASP Top 10 – 2013 (Novo)
A1 – Injeção de código	A1 – Injeção de código
A3 – Quebra de autenticação e Gerenciamento de Sessão	A2 – Quebra de autenticação e Gerenciamento de Sessão
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos	A4 – Referência Insegura e Direta a Objetos
A6 – Configuração Incorreta de Segurança	A5 – Configuração Incorreta de Segurança
A7 – Armazenamento Criptográfico Inseguro – Agrupado com A9 →	A6 – Exposição de Dados Sensíveis
A8 – Falha na Restrição de Acesso a URL – Ampliado para →	A7 – Falta de Função para Controle do Nível de Acesso
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<Removido do A6: Configuração Incorreta de Segurança>	A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos	A10 – Redirecionamentos e Encaminhamentos Inválidos
A9 – Proteção Insuficiente no Nível de Transporte	Agrupado com 2010-A7 criando o 2013-A6

Figura 4 – Comparativo das vulnerabilidades na web entre 2010 e 2013.
Fonte: www.owasp.org/images/9/9c/OWASP_Top_10_2013_PT-BR.pdf.

Serão abordados os três principais riscos em aplicações *web*, pois eles são aqueles que ocorrem mais frequentemente e que são mais estudados, são eles:

- **Injeção de Código (A1)**: É o processo de envio de informações que não são confiáveis, enviados ao interpretador *web*, na maioria das vezes por meio de requisição ou consulta, podendo executar comandos inesperados pelo uso de dados maliciosos enviados pelo atacante e tendo como consequência a permissão de acesso a dados não autorizados. Essa vulnerabilidade também tem como característica o alto impacto em sistemas computacionais, como aplicações em *datacenters*. Ela pode surgir em qualquer lugar da aplicação *web* onde se possa realizar a alteração e fornecer dados maliciosos, tendo como principal alvo as funcionalidades de: Comandos executados no sistema operacional, SQL (*Structured Query Language*), Analisadores XML (*Extensible Markup Language*), Cabeçalhos SMTP (*Simples Mail Transfer Protocol*).
- **Quebra de Autenticação e Gerenciamento de Sessão (A2)**: É um dos resultados da vulnerabilidade anterior. Silva et. al. (2014) afirmam que onde existe a quebra

de autenticidade, é onde o invasor consegue obter acesso ao sistema sem precisamente ter descoberto o *login* e a senha. Páginas que contenham injeção SQL são exemplos de quebra de autenticidade. Já as sessões são maneiras de se continuar o acesso do usuário pelo período de tempo de uso da aplicação e quando há um gerenciamento das sessões mal planejado, permitem ao invasor o comprometimento de informações como os identificadores de sessão ou as senhas de acesso a aplicação. Uma outra possibilidade é sequestrar a sessão com intuito de se passar por outro usuário.

- **Falsificação de *Script* (*Cross-Site Scripting*) (A3):** Esse tipo de falha de falsificação de *script* ou XSS, acontece quando o navegador recebe dados que não são confiáveis e em seguida realiza a devolução das informações ao navegador do usuário sem usar qualquer tipo de filtro ou de validação, permitindo ao invasor a execução de dados em *javascript* no navegador da vítima e que ele execute ações maliciosas como por exemplo o sequestro de sessão. É então possível perceber que o XSS está diretamente ligado à quebra de autenticação e o gerenciamento de sessão. A XSS pode ser de dois tipos segundo Torres (2014): Armazenado (*Stored*) e Refletido (*Reflected*), sendo a tipo Armazenado mais perigosa pois o código *javasript* pode ser inserido dentro do site, infectando todos aqueles que acessarem o *site*, enquanto que o do tipo Refletido é uma URL enviada para a vítima potencial, infectando assim, apenas aqueles que clicarem a URL, tendo assim um alcance mais limitado.

As outras vulnerabilidades são: **Referência insegura e Direta** a objetos que mostra que uma referenciação errônea abre brechas para intrusões e acesso não autorizado a terceiros; as **Configurações incorretas de segurança**, que basicamente todo problema de segurança que tenha efeitos sobre um elemento de *software* que não seja a aplicação *web* se enquadra nessa categoria; a **exposição de dados sensíveis**, são as aplicações que não protegem por meio de criptografia as informações dos usuários, como CPF, RG, telefone etc.; **Falta de função para controle de acesso**, que são basicamente aplicações que não verificam os direitos de acesso em nível de função, pode ser uma modificação em uma URL; **Cross-Site Request Forgery (CSRF)**, essa falha ocorre quando um invasor consegue enviar requisições maliciosas forçando o navegador a executar tarefas no qual esteja logado, pois este entenderá ser autêntico uma vez que o usuário é autêntico; **Utilização de Componentes Vulneráveis Conhecidos**, são causados pela exploração de

falhas não corrigidas em atualizações de *software* como *plugin* ou *framework*; e por fim os **Redirecionamentos e Encaminhamentos Inválidos**, essas falhas ocorrem quando os usuários são redirecionados para outros sites que são falsos através da manipulação das funções que analisam os dados dentro do *site* original.

É possível compreender que uma falha tem como resultado a abertura de brechas para falhas maiores, podendo ser entendido como uma espécie de "bola de neve" ou um efeito cascata, e como pode ser observado, uma falha de Injeção de código pode ter como consequência direta a geração de falhas de Quebra de autenticidade e Gerenciamento de sessão, essa por sua vez pode gerar a falhas de Falsificação de *script*. Mesmo sendo uma lista com as dez vulnerabilidades que ocorrem em aplicações *web*, a análise de um "*top tree"* se torna suficiente diante do objetivo final deste capítulo, que é a utilização da Engenharia Social como fator potencializante para a obtenção de informações privilegiadas e acesso não autorizadas.

2.3 Utilização da Engenharia Social em um *pentest.*

Para a realização de um *pentest*, é necessária a ação realizada por uma empresa ou por algum *hacker*, ou *cracker*. A diferença substancial entre um e outro é que, ao se contratar uma empresa ou um *hacker*, há o entendimento de que o mesmo seguirá todo o processo legal, não utilizando ferramentas ilícitas na descoberta das vulnerabilidades a serem encontradas e exploradas na rede e nas aplicações que a empresa possui. Esse mesmo entendimento não pode ser fornecido no caso dos *crackers*, quando a rede ou as aplicações são invadidas sem estrito conhecimento do proprietário da empresa, estes utilizam métodos criminais para a obtenção de dados de forma ilegal.

Mesmo aqueles que atuam fora da legalidade tem um papel importante na descoberta de vulnerabilidades, pois alguns acabam por descobrir as falhas e reportá-las ao proprietário ou gerente da empresa. Para Wilheslm (2009), eles se dividem em dois grupos: os *White hats* também conhecidos como *Hackers* do bem, ou *hackers* éticos, são aqueles que utilizam os seus conhecimentos na descoberta de vulnerabilidades e aplicar as correções necessárias, agindo de forma profissional. Já os *Black hats* também conhecidos como *full flaged* ou *crackers* que utilizam o seu conhecimento para invadir e roubar informações sensíveis da organização e em muitos casos tentam vender a

informação novamente ao proprietário. Para Kimberly (2010), uma terceira categoria é adicionada, são os *Gray hats*, que são aqueles que trabalham tanto como um *hacker* quanto como um *cracker*, dependendo da situação, eles são aqueles que estão na linha divisória entre o "bem e o mal".

Para alguns autores, como Hadnagy (2011) e Peixoto (2006) fica claro que a utilização da Engenharia Social leva em consideração apenas o aspecto da enganação, não considerando a engenharia como uma técnica criminal, porém Mann (2008) considera que seu uso pode ser encarado tendo em vista atividades ilegais, como o roubo de informações.

Em um *pentest*, o ataque realizado para obtenção das informações pode ser de cunho tecnológico ou não, e a utilização desses meios tem como finalidade enganar os funcionários, afim de persuadi-los a entregar informações que forneçam acesso ao sistema ou às aplicações desse sistema. A Engenharia Social é primeiro passo a ser dado na coleta de informações sobre o alvo pretendido e existem atualmente diversas ferramentas e técnicas que podem auxiliar o *tester*[7] a obter informações sensíveis e importantes.

Com o advento das novas tecnologias de informação e comunicação que geraram a revolução tecnológica, a conectividade entre aparelhos móveis e a geração de informações constantemente, a troca de informações vem se tornando impactante para as empresas, pois na *web*, por exemplo, há um leque de informações a disposição de todos aqueles que desejarem acessá-la ou conhecê-la. O levantamento das informações e a criação de perfis dos alvos selecionados se tornou fácil para o atacante e consequentemente difícil de ser detectado, pois como a busca de informações é livre, não há como saber quando e como um alvo será selecionado, muito menos quando será atacado. Como se sabe, o uso da Engenharia Social é uma das ferramentas essenciais para realizar o *footprint* e consequentemente realizar o ataque. Um dos criminosos mais conhecidos nessa área Kevin Mitnick que utilizava a Engenharia Social em mais de 80% dos seus ataques, segundo Nakamura (2007). A engenharia é muito eficiente e extremamente poderosa, pois une três áreas do conhecimento: ciência, arte e psicologia (BATISTA, 2015).

Um invasor, seja ele *hacker* ou *cracker*, na maioria dos casos irá buscar informações sobre a empresa, o sistema ou a aplicação a ser testada. Desde informações

[7] Tester: profissional responsável por realizar os testes.

básicas como por exemplo endereço, telefones de contato, e-mails, horários de funcionamento da empresa, até informações técnicas como provedores de e-mail, tipo do sistema operacional, qual o *host*, qual o servidor que roda a aplicação, o tipo de banco de dados, telefone e e-mail do administrador do servidor da rede, tentando assim criar um perfil sobre a vítima. O nome dado a essa ferramenta é *footprinting.*

A utilização de técnicas de Engenharia Social, dentro de um *pentest*, tendo como base a metodologia OWASP, que aponta que em aplicações *web* a injeção de código é a falha que ocorre mais frequentemente, leva em consideração não somente as características tecnológicas, como as sociais. No tocante às características técnicas os engenheiros sociais possuem à sua disposição uma grande soma de conhecimento e de recursos tecnológicos, como por exemplo a utilização de *softwares*, tais como:

- ***Whois*[8]:** que pode ser utilizado para a descoberta de contatos e servidores DNS que estejam associados a um domínio ou a um endereço de IP (*Internet Protocol*),
- ***Scanners ou Port Scanning*:** Ferramenta largamente utilizada, conhecidos *scanners*, eles têm como objetivo principal fornecer informações sobre os serviços que estão disponíveis através do *scan* das portas TCP/UDP. Um dos *scanners* mais conhecido e mais poderoso é NMAP[9], pois ele realiza uma varredura completa detectando o estado do *host*, a detecção de portas abertas, se existe algum *firewall* para filtragem ou não das portas, e em alguns casos a detecção do sistema operacional, a sua versão, com uma precisão de 100%.

Existem muitas outras técnicas que são utilizadas no *footprint* a nível tecnológico, não sendo o objetivo deste trabalho abordar todas as técnicas, que vão além do *footprint*, mas abordar um conjunto de ferramentas e técnicas para a utilização do *pentest*, tendo como fonte de busca de informações a Engenharia Social. Já no que diz respeito aos aspectos humanos, eles podem e são utilizados quando o atacante não obtém todas as informações que necessita. O engenheiro social utiliza técnicas baseadas na psicologia para influenciar a tomada de decisões, pois elas são realizadas, segundo Conheady (2014), em função das limitações humanas como a confiança, medo das autoridades, desejo de ser útil e despreocupação com a segurança da informação, como algumas das razões que

[8] WHOIS é um protocolo baseado em TCP para ser usado num modelo pedido/resposta. O nome não é um acrônimo, mas sim a junção das palavras *who is.*

[9] NMAP: ferramenta que apresenta um rol alargado de opções para operações de reconhecimento de rede e análise de portas e serviços, sendo largamente usada para auditar a segurança de computadores.

fazem com que a Engenharia Social possa ser utilizada em qualquer pessoa, em qualquer lugar do mundo. As principais técnicas utilizadas pelo engenheiro social são:

- **Coleta de informações:** Para o engenheiro social, nenhuma informação é irrelevante e qualquer detalhe pode ser decisivo para que o ataque tenha o resultado desejado. Além das ferramentas tecnológicas citadas acima, uma simples conversa pode fornecer dados importantes que posteriormente serão agrupadas e organizadas para montar a estratégia de ataque. Dentro da coleta de informações, também é possível agregar ferramentas tecnológicas como o *Google*, o qual tem papel fundamental pois essa "ferramenta", se assim pode ser chamada, consiste na utilização do motor de busca do Google para obter informações necessárias acerca do alvo que se pretende atacar, como endereço, provedores de e-mail, telefones. Utilizando tipos específicos de busca de informações é possível até a identificação de falhas referentes à segurança, e podendo assim traçar um perfil genérico do alvo e utilizar através das informações colhidas, técnicas específicas para o ataque.
- **Elicitação:** É uma das técnicas mais importantes e críticas usada pelo engenheiro social, pois ela pode fornecer todas as informações relevantes ou fracassar completamente. Elicitação é o saber conversar, ser educado, se vestir adequadamente, para conseguir prender a atenção e conquistar sua confiança. Ela é uma ferramenta poderosa por se tratar de uma simples conversa, onde o atacante segura a vítima sem utilizar uma linguagem maliciosa. Hadnagy (2011, p. 59) diz os três elementos principais da arte da conversação são: Relaxe, Eduque-se, Controle-se.
- **Pretexto:** Para muitos, é somente uma história ou alguma mentira a ser apresentada, mas dentro do contexto da Engenharia Social, é como uma história de fundo, com atitudes e personalidades diferentes da realidade utilizadas no intuito de enganar a vítima. O pretexto irá maquiar tudo o que o engenheiro social é na realidade, com um bom pretexto, fica praticamente impossível de detectar quem o engenheiro é realmente, ou seja, é uma espécie de arte onde se cria um cenário no intuito de persuadir alguém a conseguir alguma informação.

Assim é possível perceber que o engenheiro social, é aquela pessoa que busca através de uma mentira, muitas vezes criando um perfil falso de si mesmo para obter uma informação que ele não possui, explorando principalmente falhas humanas. Vargas,

(2002) *apud* Popper; Brignoli, (2003, p. 7) afirmam que “Os seres humanos são seres imperfeitos e multifacetados. Além disso, situações de risco modificam seus comportamentos, e, decisões serão fortemente baseadas em confiança e grau de criticidade da situação” e dentro de um *pentest* as técnicas de Engenharia Social são largamente utilizadas para que o invasor trace as principais diretivas para o ataque.

É preciso compreender que cada ataque de Engenharia Social é único, pois leva em consideração múltiplas fases e ciclos, tornando-o assim imprevisível (ALLEN, 2006), e que as organizações e empresas investem anualmente milhares de dólares em recursos financeiros para a proteção dos seus dados, pois muitas vezes há equivocadamente o entendimento de que um eficaz sistema antivírus e a utilização de um *firewall* poderoso atrelado aos sistemas de detecção e prevenção de intrusão (IDS/IDP), serão capazes de proteger tecnologicamente suas informações. Para Mitnick e Simon (2003), desconsiderando a Engenharia Social, até mesmo os melhores programas, utilizados pelos mais bem treinados profissionais e protegidos pela melhor segurança do mundo, ainda assim a informação estará vulnerável e passível de ataque, e “a verdade é que não existe uma tecnologia no mundo que evite o ataque de um engenheiro social” (MITNICK; SIMON, 2003, p. 195).

3. ENGENHARIA SOCIAL – UMA ARTE A SER EXPLORADA

A Engenharia Social é utilizada como fator potencializante em um ataque a uma rede pessoal ou coorporativa, pois como dito, o engenheiro social utiliza diversos meios de dinamização para conseguir a maior quantidade de informações possíveis, para assim modelar a forma adequada de se obter o acesso privilegiado a informações das quais ele está impedido de obter. Para entender a natureza de um ataque de um engenheiro social e como ele pode ser desastroso, dependendo do contexto em que se aplique, serão explicitados quais são os tipos de ataque de um engenheiro social, como também alguns casos reais que a Engenharia Social foi aplicada e utilizada como meio para se atingir determinados objetivos.

Dentro de um cenário como o da a realização de um *pentest*, que tenta burlar os sistemas de segurança da informação, a Engenharia Social ganha de forma e força por ser uma área completamente desconhecido ou parcialmente conhecido. Por não ser uma área aprofundada dos gestores responsáveis pelo desenvolvimento e manutenção desses sistemas, a Engenharia Social se torna mais complexa, abrangente e consequentemente perigosa para as organizações, empresas e usuários vítimas de um ataque de um engenheiro social, uma vez que o desconhecimento tem como resultado direto as brechas de segurança, vazamento de informações confidenciais e de dados sensíveis.

Bons engenheiros sociais são pessoas que são especialistas em analisar o comportamento dos seres humanos, segundo a *Social Engineer*, Inc. O fator decisivo para o sucesso de um ataque de Engenharia Social, como citado anteriormente, segundo Conheady (2014) está fundamentado em quatro características:

- **Confiança:** É da natureza humana a confiança, pois a sociedade é baseada na confiança, porém ela não é simples de ser obtida. Na Internet há dificuldade em encontrar casos que pessoas são vítimas de alguma fraude, mas para o engenheiro social, essa não é uma tarefa complicada, pois como ele monta um teatro e encena perfeitamente uma situação ilusória, a detecção da mentira se torna extremamente difícil, principalmente em ambientes compartilhados com a vítima, tais como locais de trabalho, em estádios de futebol, supermercados etc. Um estudo denominado "*Project Wizard*" realizado pela Universidade da Califórnia, São Francisco, coordenada pelos psicólogos Paul Ekman e Maureen O'Sullivan,

durante mais de 20 anos, com mais de 15 mil pessoas e detectou que a maioria das pessoas só consegue identificar cerca de 50% das mentiras, e apenas 50 indivíduos conseguiram identificar mais de 80% e nenhum chegou aos 100%.

- **Medo de autoridades:** Desde o nascimento estamos condicionados a autoridade de alguém, dos pais, professores, policiais e geralmente também de pessoas que utilizam uniforme, onde na grande maioria das vezes age-se de forma tendenciosa a obedecer uma autoridade quase que de forma inquestionável. Pessoas tendem a obedecer a ordens de outros que possuem cargo superior ao seu e um engenheiro social sabendo disso, em um ataque se passa por um funcionário com cargo maior, pois muito provavelmente seu pedido será atendido. Alguns fatores como autoridade, pressão e justificativa aumentam as chances das pessoas atenderem a ordem.
- **Desejo de ser útil:** As pessoas se sentem naturalmente bem ao ajudar alguém, ainda que estranhas, principalmente em ambientes de trabalho. Um dos principais alvos dos engenheiros sociais são os *call centers*, recepcionistas, pois eles têm como função principal informar. Carnegie (2012) afirma que:

> Faça a outra pessoa sentir-se importante, e faça-o com sinceridade. Um engenheiro social quando pede ajuda para alguém e consegue provar para essa pessoa que ela o ajudar ele irá considera-la uma pessoa importante é quase certo que essa pessoa irá o ajuda sem pensar duas vezes. Carnegie (2012, p. 139).

- **Falta de preocupação com a segurança:** Também é um fator importante na aplicação da Engenharia Social, porque as pessoas não sabem o valor da informação e até quando percebem algo fora do normal, acham que "não é nada demais", um exemplo disso é ampla publicação de informações em redes sociais como o Facebook. As pessoas não sabem o que é a Engenharia Social e mesmo quando sofrem algum tipo de ataque não sabem especificar o que é um ataque desse tipo. Como citado anteriormente, o *phishing* fez e faz inúmeras vítimas todos os anos. Não há nada pior para um profissional de segurança do que ouvir uma pessoa falando que não se preocupa, pois não tem nada a perder.

Essas ferramentas à disposição do engenheiro, o torna praticamente invisível, o tornando quase imune quanto ao descobrimento da sua real identidade e de quais são os seus verdadeiros objetivos. Assim, tendo uma visão alargada sobre os pontos que tornam

a Engenharia Social tão efetiva, abre-se o caminho para conhecer quais são os tipos de ataque de um engenheiro social.

3.1 Tipos de ataques de Engenharia Social.

Tendo como um de seus objetivos, impressionar o alvo, tentando subtrair a informação desejada, o engenheiro social que tem que ser uma pessoa detalhista, tem a capacidade de estuda-lo por um período de tempo indeterminado, tentando mostrar domínio sobre assuntos conhecidos da sua vítima, para então atacá-la. Um ataque de um engenheiro social, se resume basicamente em dois tipos: o direto e o indireto.

3.1.1 Ataque direto e indireto

Esse modelo de ataque é considerado o mais ousado e arriscado para o engenheiro social, pois ele entra em contato com seu alvo, seja pessoalmente ou via telefone, e-mail etc., em geral não realizado por iniciantes, pois requer experiência para conseguir as informações que são necessárias e para se conseguir realizar esse tipo de ataque o engenheiro segue alguns passos, que para Dolan (2004) são:

- **Escolha do alvo e a aproximação:** O alvo em questão pode ser qualquer um, pessoas próximas ou não, vai variar com objetivo do atacante. Sua aproximação e a forma como se dará, tem como influência direta a escolha do alvo, e ao mesmo tempo em que se aproxima, não pode se deixar ser notado até o momento certo.
- **Estudo da vítima:** Frequentar os mesmos lugares, observação do alvo, escuta de conversas e conseguir o máximo de informações possíveis de fontes variadas fazem parte desta fase.
- **Aclimatação:** São os contatos iniciais, realizados através de conversas despretensiosas, procurando se inserir no meio ao qual a vítima está de forma natural e espontânea.
- **Confiança e cumplicidade:** Explora a confiança da vítima através de situações como carência afetiva, dificuldades financeiras, sempre demostrando boa-fé. Aqui o engenheiro mesmo pode expor a vítima em situação, e ajuda-la para ganhar sua

confiança, dominando-a assim inconscientemente, essa técnica é conhecida como Engenharia Social Reversa.

- **Criação do pretexto:** Aqui é onde o engenheiro começa a sua atuação, criando histórias e encarnando um personagem.
- **Execução:** O engenheiro torna-se o pivô da tomada de decisões da vítima, ainda que pareça mal-intencionada, mostra-se como uma pessoa sincera e segura, cativando a vítima e envolvendo-a no golpe.
- **Finalização:** É quando por fim, o alvo descobre que foi enganado, porém em muitas vezes, o engenheiro social já se encontra em situação privilegiada, e repentinamente desaparece do contato com a vítima.

Existem exemplos que se encaixaria esse tipo de ataque, Mitnick (2003) em seu livro "A arte de enganar" e Mitnick (2006) com a "Arte de Invadir", trazem inúmeros destes exemplos, de pessoas que fingem ser outras, e após longa análise e estudo, aplicam o ataque e quando obtém sucesso, costumam desaparecer do círculo pessoal da vítima. Essa, porém não é a única forma de ataque de um engenheiro social, apesar de ser a mais usada.

Diferentemente do ataque direto, o ataque indireto consiste na utilização das ferramentas tecnológicas para se obter informações sobre o alvo. Na Internet, mais especificamente as redes sociais, se mostram como a forma fácil de se conseguir essas informações, clonando-se sites, utilizando vírus, formulários de cadastro falsos, o *phishing scan*, entre outros. Nesse método, por não ter o contato diretamente com a vítima, pode ser considerado como menos arriscado que o ataque direto.

Com isso pode-se adentrar no conhecimento de casos reais que a Engenharia Social se fez presente e consequentemente gerou inúmeros prejuízos não somente financeiros, mas prejudicou a imagem e a reputação da empresa frente a empresas do mesmo segmento.

3.2 Caso Kevin Mitnick

Pode-se constatar que nenhum trabalho sobre ataques de Engenharia Social estaria completo sem citar Kevin Mitnick (Goodell, 1996), ele é o autor de grandes obras literárias sobre Engenharia Social como: a arte de invadir, a arte da invisibilidade e a arte de enganar. Diferentemente de outros engenheiros sociais, Kevin usava a engenharia

como um *hobbie* (Mitnick; Simon, 2006), se é possível falar assim. Além do caso citado no tópico 1.2 sobre a AOL, ele realizou muitos outros ataques dos quais não se conhece, porém em julho 1994, o *New York Times* publicou uma capa que o considerava como "o mais procurado do ciberespaço por ter enganado o FBI e ter invadido a rede do NORAD (Comando de Defesa Aeroespacial da América do Norte) e grampeado o FBI. Entre os ataques mais famosos realizados por Mitnick podemos citar um em especial, que teve como resultado a sua prisão.

Ao tentar invadir a rede pessoal de Tsutomu Shimomura, especialista em segurança de redes, através do uso da Engenharia Social para a descoberta sobre os detalhes envolvendo a rede, realizando um *scan*, ele obteve informações como o endereço de IP, DNS, etc. da rede de Tsutomu e ao descobrir essas informações, realizou um ataque chamado de *IP Spoofing*, que tem como finalidade a clonagem do endereço de IP, fazendo com que o servidor de Tsutomu considerasse o computador que acessava a rede de forma remota de Mitnick como um computador que estava dentro da rede local e não em uma rede externa.

Por ter sido invadido por um *hacker*, teve início a caçada ao "Condor" (apelido utilizado por Kevin) e os problemas começaram quando Tsutomu Shimomura conseguiu refazer os últimos passos de Mitnick e resolveu descobrir quem tinha passado pela sua segurança. Tendo então a informação de qual era a origem do IP atacante, passou a monitora-lo e juntamente com a ajuda entre Tsutomu Shimomura e os provedores de redes locais como WELL e em seguida a Netcom conseguiram, através de uma varredura de rede, descobrir pelo IP qual o real endereço de Kevin Mitnick.

Comunicaram então ao FBI e conseguiram um mandado de prisão e após dois dias de interceptação das conversas e do telefone, Kevin foi preso em casa em 1995. Sua condenação gerou a pena de ter de passar cinco anos preso em regime fechado e mesmo após o cumprimento da pena, teve de ficar mais três anos sem poder ter nenhuma espécie de contato com computadores.

Após o período estabelecido pela justiça norte-americana, Mitnick criou uma empresa de segurança de informação chamada Mitnick Secutiry, possui um site para maiores aprofundamentos, https://mitnicksecurity.com/.[10]

[10] O *site https://mitnicksecurity.com/ é da empresa de segurança da informação criada por Kevin Mitnick.*

É possível identificar a utilização da Engenharia Social dentro desse processo de invasão, pois a falsificação do endereço de IP ou *Ip Spoofing* não era uma técnica muito conhecida na época e sua realização não é possível sem o prévio conhecimento de elementos específicos da rede. A obtenção dessas informações pode ser adquirida através da utilização de um *software*, o *port scanning* ou escaneamento de portas, como citado no capítulo anterior, no tópico 2.3, que mostra que essa ferramenta identifica setores, portas que se encontram abertas e estão passiveis de ataque.

3.3 Caso Wells Fargo e Bank of América.

Esse foi um dos casos que ganharam repercussão internacional, um dos *sites* que se pode encontrar a notícia é no http://portalimprensa.com.br/[11], foi uma fraude realizada em dois dos maiores Internet Bankings dos Estados Unidos, o *Bank of America* e o *Wells Fargo*. Os clientes desses bancos foram vítimas de um ataque de Engenharia Social denominado *phishing* e realizado por um *insider*[12], esse modelo consiste basicamente na criação de uma página falsa para a obtenção de dados como *login* e senha de uma conta de rede social ou especificamente nesse caso, de um banco. Nesse ataque o *phisher*[13], enviou por e-mail para os clientes do banco uma solicitação de atualização de informações da sua conta, quando clicavam, os clientes eram redirecionados para uma página fraudulenta, para tornar mais verídico o e-mail, foi utilizado um senso de urgência para atrair mais facilmente as vítimas.

O ataque foi realizado em múltiplas fases que incluíam o uso de ferramentas *Open Source*, obtenção de um emprego em caráter temporário, corrupção de responsabilidades de funcionário temporário, abuso de acesso físico, *hacking* interno, facilitação de *hackers* externos e *hacking* externo. Os resultados dessa invasão foram impactantes, em cerca de vinte quatro horas, mais de 1 milhão de dólares em informação foram roubados. Enquanto por meio do *firewall* o acesso externo se tornava praticamente impossível, o comprometimento da informação foi feito quase que livremente por um usuário dentro da

[11] Site: http://portalimprensa.com.br/noticias/ultimas_noticias/28913/operacao+binacional+desmantela+quadrilha+de+roubo+de+informacoes+via+web
[12] Insider – Hacker ou Cracker que trabalha dentro das instituições.
[13] Phisher – Ator que realiza o *phishing*

organização. Essa ação foi realizada em bancos que possuíam os melhores sistemas de segurança interno que existiam. Esse ataque gerou um estudo de caso e seu resumo pode ser encontrado no site Social-engineer.org[14] e o artigo completo pode ser visto em Social-engineer.org[15].

Atualmente diversos casos que envolvem o uso de *phishing* atrelados a Engenharia Social são informados à imprensa, como afirmam Moore, Clayton e Anderson (2009), no *phishing* as pessoas recebem o estímulo para fornecer dados tendo como meio as mensagens eletrônicas, onde os remetentes usam de personificação de identidades ou de organizações, com o intuito de inspirar a confiança ou o receio de ser atacado, segundo Sony, Firake e Meshram (2011).

Apesar de hoje já existir um grande esforço da comunidade mundial no combate a esse tipo de fraude (Fette et al. 2007, Kumaraguru et al. 2007, Bergholz et al. 2010), é possível observar que o *phishing* é resistente, o que leva a acreditar que à medida em que o tempo passa, as técnicas do *phisher* também vão se atualizando, anulando técnicas anteriores de prevenção.

Compreendendo que a natureza de um ataque de Engenharia Social pode ocorrer tanto dentro das próprias instituições como fora, torna o engenheiro social um profissional que possui a capacidade de penetrar nos mais restritos espaços na busca informação desejada, utilizando ou não meios eletrônicos e computacionais. Também é possível visualizar que as perdas referentes a informação, não são ruins somente do ponto de vista da reputação da empresa, as perdas financeiras são gigantes e constantemente empresas multinacionais, órgãos governamentais sofrem com a constante ação dos engenheiros sociais. Um dos casos recentes envolvendo a perda de informações foi a do Yahoo.com, que divulgou ter sofrido um ataque que afetou 1 bilhão contas de usuários em 2014, como noticiado no site olhardigital.uol.com.br[16]

Para realizar a prevenção do vazamento das informações são necessárias ações que impossibilitem ou ao menos dificultem ao máximo a ação de um engenheiro social, essas ações serão abordadas no próximo capítulo.

---

[14] http://www.social-engineer.org/framework/general-discussion/categories-social-engineers/penetration-testers/

[15] http://social-engineer.org/wiki/archives/PenetrationTesters/Pentest-Winkler.html

[16] http://olhardigital.uol.com.br/fique_seguro/noticia/yahoo-anuncia-que-1-bilhao-de-usuarios-tiveram-suas-contas-hackeadas/64675.

4. MITIGAÇÃO DAS VULNERABILIDADES

Tendo em vista toda a discussão promovida nos capítulos anteriores, com base nos autores aqui evidenciados, torna-se perceptível que a amplitude da Engenharia Social não é o fator determinante para o seu sucesso. Por ser uma técnica, possui falhas e limitações. Mesmo os melhores engenheiros também erram, acreditamos assim que as brechas deixadas por eles podem ser utilizadas para impedir sua boa execução, permitindo então a mitigação do ataque.

A Engenharia Social está diretamente ligada a falhas comportamentais do ser humano, baseada em situações distintas: como o medo, o desconforto, a necessidade de ajudar. Como ela pode ser usada contra qualquer membro de uma organização ou empresa, desde o cargo inicial até o cargo de mais alto escalão, ela se torna uma ferramenta imprescindível para ataques como o terrorismo empresarial, e como já afirmado por Mitnick (2003), não existe nenhuma tecnologia no mundo capaz de deter um ataque vindo de um bom engenheiro social, até por que muitas vezes, o ataque de um engenheiro social não leva em consideração ferramentas tecnológicas.

Todos estão susceptíveis a um ataque de Engenharia Social, e conhecer como se precaver é o primeiro passo a ser dado para se minimizar a eficiência desses ataques e mesmo em casos onde um ataque de Engenharia Social for efetivo se faz necessária a tomada de medidas para a correção o mais rapidamente das vulnerabilidades.

Essa preocupação com a proteção e segurança das informações se mostra necessária, pois “ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes” (BRASIL, 2003, p. 9). As brechas deixadas de lado, podem justamente ser o motivo do vazamento das informações, uma vez que os engenheiros sociais podem estar tanto dentro da empresa quanto fora, eles podem ser estudantes, executivos, representantes comerciais e até mesmo ex-funcionários. A Engenharia Social deve ser levada especialmente em consideração quando se fala sobre a segurança da informação, porque a comunicação pode ser imaginada e usada com a finalidade de influenciar ou controlar as pessoas (BERLO, 2003), levando então o outro a tomar atitudes, agir ou servir a um determinado propósito que vai além da concepção muitas vezes do próprio atacante.

De acordo com Marcelo e Pereira (2005), existem dois tipos de engenheiros, os denominados ‘formados’ que são aqueles que passam por algum tipo de treinamento ou formação para executar tarefas como engenheiros sociais, são eles policiais, detetives, espiões etc. Também existem os chamados de ‘notório-saber’ que são aqueles frutos da própria sociedade, são aqueles que conseguem olhar para uma situação de várias formas distintas, eles não chamam a atenção pelas ações, mas pelo carisma, dois exemplos conhecidos são Frank Abgnale Junior e Kevin Mitnick.

Quando pessoas vulneráveis são colocadas a ataques de engenheiros sociais, se torna inviável as restrições de segurança somente dentro da área da tecnologia da informação, por isso a importância de se possuir uma nova mentalidade onde a segurança da informação não engloba somente aspectos tecnológicos, mas aspectos sociais de toda a organização.

4.1 Identificação e Mitigação dos ataques

Para se defender de um ataque de um engenheiro social, é necessário segundo Dolan (2004), a criação de rotinas de treinamento, que visem principalmente os esclarecimentos sobre como agir de forma segura diante das principais técnicas da Engenharia Social bem como uma sólida política de segurança. Concordando com Dolan, Gragg (2002) define que, a defesa da organização deve acontecer em um modo multinível, que são abordados os gatilhos psicológicos e os níveis de defesa definidos pelas políticas de segurança, através de treinamento e conscientização sobre a segurança, treinamentos de resistência, lembretes, minas terrestres para Engenharia Social (SELM) e de resposta a incidentes.

Em resumo, é preciso conhecer como o engenheiro social age e mitigar a sua eficiência, se faz então necessário o conhecimento das atitudes tomadas pelo engenheiro, e saber reconhecer quando se está sendo vítima de um ataque. Para se obter esse nível de conhecimento, é necessária a implantação de políticas de segurança e através delas, um plano de treinamento e conscientização que aborde não somente as técnicas, mas as ferramentas a favor da Engenharia Social e como ela afeta diretamente cada membro da empresa, levando em consideração os aspectos técnicos e psicológicos.

Um outro ponto abordado nas políticas de segurança, é a utilização de um Plano de Resposta a Incidentes (PRI), evitando assim a propagação das falhas e vulnerabilidades pela empresa, corrigindo os erros e respondendo de forma rápida e objetiva para saná-los, conquistando assim um nível de excelência em relação a segurança da informação.

A mitigação das vulnerabilidades e a defesa de ataques da Engenharia Social se tornam complicadas porque são direcionadas diretamente ao elo mais fraco da segurança, o operador do sistema. Nós humanos, não podemos simplesmente ser configurados a nos defender, não existe um *patch* contra as falhas humanas (Marcelo; Pereira, 2005), que fazemos o *download* e nos tornamos imunes a ataques dos engenheiros sociais.

A primeira observação que deve ser feita é a identificação daqueles que são os alvos mais fáceis de serem atacados, esses devem se colocar na postura do engenheiro social, de como ele age, como ele faria se estive do outro lado. Além disso, existem outras formas de identificar o engenheiro social, pois existem categorias que podem ajudar a encontrar ou identificar um ataque e Engenharia Social antes que ele se concretize, concordando com Hadnagy (2011), essas categorias são:

- **Atitude:** os engenheiros sociais podem ser pessoas com um extremo bom humor, muito educada, que buscam ajudar em demasiado, ou o oposto, pessoas extremamente rudes com pedidos autoritários, ou ainda pessoas sentimentais demais.
- **Tentativa de Conexão:** Os engenheiros sociais buscam se conectar às suas vítimas, isso é fundamental para eles, usando nomes de pessoas conhecidas, sendo que ela nunca te falou sobre o atacante.
- **Pequenos erros:** Engenheiros sociais menos experientes tendem a ser mais descuidados quanto aos detalhes, pois a Engenharia Social exige prática e experiência. Esses erros a olhares comuns são imperceptíveis, mas para profissionais treinados, pequenas falhas podem se tornar gatilhos de defesa evitando o ataque.

Levando-se em consideração esses fatores preliminares como ponto de partida, outras maneiras de se evitar o ataque de um engenheiro social, podem ser definidas através da documentação de políticas de segurança, que devem ser conhecidas por todos aqueles que constituem o quadro de funcionários da empresa.

4.2 Políticas de segurança

As políticas de segurança dentro de uma empresa são imprescindíveis, pois elas visam proteger a empresa bem como os seus principais bens, as informações que podem ocasionar ataques, Mitnick (2003) afirma:

> Como diz o ditado; até mesmo os verdadeiros paranoicos [sic] provavelmente têm inimigos. Devemos assumir que cada empresa também tem os seus — os atacantes que visam a infraestrutura [sic] da rede para comprometer os segredos da empresa. Não acabe sendo uma estatística nos crimes de computadores; está mais do que na hora de armazenar as defesas necessárias implementando controles adequados por meio de políticas de segurança e procedimentos bem planejados. (MITNICK; SIMON, p. 23).

Para que se consiga de fato estabelecer um ambiente seguro, é fundamental que haja uma série de procedimentos claros e bem estabelecidos em qualquer ambiente em que essa informação venha a transitar. Mas por que não deve ser restrito apenas às máquinas e equipamentos tecnológicos? Schwartau, (2010, p. 1) responde afirmando que, "nós não tocamos em redes, nós tocamos nas pessoas. Porque, no fim, o elo mais fraco em todas essas coisas é a pessoa que está à frente da tela".

Esses procedimentos são denominados Políticas de Segurança, e nesse caso está inserido no âmbito da informação. Segundo Fonseca (2009), as políticas de segurança podem ser determinadas como um conjunto de instruções claras com o objetivo de preservar as informações. Logo, é possível entender que um dos meios de se estar dando os passos corretos no sentido de fornecer à empresa um ambiente seguro, é a adoção de regras que de forma conjunta busquem combater e prevenir ameaças e ataques, estando elas entre as mais efetivas evitando e detectando ataques da Engenharia Social.

O objetivo das políticas de segurança não é eliminar todo e qualquer risco dos ataques de Engenharia Social, mas minimiza-los a níveis aceitáveis, pois, mesmo com todo o treinamento dado a funcionários e que todos esses sigam rigorosamente as regras documentas, ainda assim, estão passiveis e vulneráveis a um ataque.

Segundo Fonseca (2009), as políticas de segurança da informação, deve prioritariamente começar com a avaliação dos riscos envolvidos e buscando responder alguns questionamentos:

- Que informações ou quais os tipos de informação precisarão ser protegidos e qual nível de proteção se enquadrará cada informação?
- Quais são as ameaças ou quais tipos de ameaça a empresa pode sofrer?
- Qual seria o prejuízo caso uma dessas ameaças fosse explorada e um ataque viesse a acontecer?

Naturalmente se observa que o objetivo desse levantamento inicial é a avaliação de riscos imediatos e que sabidamente precisam de proteção mais urgente. O segundo passo a ser dado nas políticas de segurança é obter a relação custo/benefício, com o intuito de se fazer um levantamento de quanto custará a empresa, a informação a ser protegida. Nesse ponto é fundamental o apoio irrestrito da gerência, pois assim estará demonstrando que realmente se preocupa com o bom funcionamento da empresa e quer vê-la segura para os funcionários de menor escalão.

Como as políticas de segurança são regras claras e bem definidas, estas devem ser entendidas por todos, levando em consideração que existem funcionários que não possuem entendimento da linguagem técnica, logo, os bordões e jargões técnicos devem ser abolidos, visando o entendimento por qualquer funcionário. Também é necessário deixar claro o porquê de se estar utilizando essas políticas, para que não sejam encaradas como algo chato, desnecessário ou perda de tempo.

Elas devem ser criadas de preferência em dois documentos distintos, que um abordará o caráter das políticas e o outro os procedimentos, pois os procedimentos tendem a mudar mais constantemente do que as políticas em si. Além disso, na redação das políticas é necessária a análise da tecnologia que será usada para implanta-las, se o custo/benefício realmente existe e devendo assim manter o foco para que as políticas adotadas sejam adequadas ao ambiente de trabalho, uma vez que cada empresa possui o seu jeito de funcionar, uma cultura organizacional própria e que os requisitos necessários para a segurança da informação devem atender as demandas da empresa.

Por fim, é preciso entender que essas políticas e procedimentos não devem ser enrigidecidos, pois a medida que o tempo passa, novos ataques são criados e/ou métodos antigos são atualizados baseados nas próprias políticas de segurança. É fundamental a

abertura a atualizações, estabelecendo sempre novos procedimentos para combater novos meios de invasão e que sempre esses documentos devem estar em locais acessíveis e de boa visibilidade, facilitando seu acesso e consulta a todos os funcionários da empresa.

4.2.1 Plano de conscientização e treinamento

O plano de conscientização e treinamento tem como foco principal a busca por mudanças de posturas e atitudes, tentando em primeiro lugar conscientizar e influenciar os funcionários a uma mudança de hábitos, mostrando que dentro do processo da segurança da informação, eles são peças fundamentais e diante de um ataque eles serão aqueles que sofrerão os primeiros impactos.

À medida em que os treinamentos forem acontecendo, é primordial que haja gatilhos e técnicas para prender a atenção e buscar entusiasmar os funcionários, caso contrário, em vez de benéfico para empresa, o resultado poderá ser o oposto. O treinamento e a educação consciente acerca da preservação de que a informação precisa ser protegida e como os funcionários devem protegê-la é essencial, pois somente assim, eles estarão aptos a identificar um ataque de Engenharia Social.

Um outro detalhe de grande importância nos treinamentos é que eles devem acontecer periodicamente pois, como dito, os modelos utilizados pelos engenheiros sociais vão se sofisticando com o tempo e é preciso estar atualizado, para que o combate se dê de forma efetiva, uma vez que funcionários sem treinamento constante, correm um risco muito maior de serem vítimas do engenheiro social porque ao passo em que o tempo passa algumas partes do treinamento vão ficando esquecidas, sendo necessário um reforço deste aspecto.

Para motivar os funcionários de que a segurança da informação não é importante somente para empresa, mas também para ele, é fazê-lo conhecer e entender que ao deixar as informações expostas e sob risco de ataque, os próprios dados particulares dos funcionários também estão em risco. A utilização de analogias é extremamente válida, usando como um exemplo de que a informação da empresa é semelhante a senha do banco para ele. Outra boa forma de exemplificação é mostrar ataques reais de Engenharia Social, através de vídeos educativos, reportagens, de modo que seja educativo e instrutivo ao mesmo tempo, assim o funcionário irá compreender e saber que ele tem papel

fundamental na segurança da empresa, que essa segurança passa por ele e não é algo sem importância, que ele está a parte ou exerce um papel inferior.

Para ressaltar a importância da administração com a segurança, a empresa como fator motivador, também pode oferecer recompensas a aqueles funcionários que cumprirem todas as medidas de segurança estabelecidas, pois o incentivo é motivador por si próprio. Um outro fator motivador e estimulante para o funcionário se manter sempre alerta, segundo Mitnick (2003) é a mostra de casos onde se houve a tentativa de um ataque a segurança e o funcionário atuou da maneira correta e evitou danos a empresa.

Outro aspecto importante que os treinamentos devem abordar é de que cada setor da empresa lida com a informação de maneira diferente, naturalmente os treinamentos devem se adequar às características particulares de cada empresa em cada setor, por exemplo, os funcionários que lidam diretamente com a entrada de dados nos sistemas, cargos de chefia, técnicos da informação da empresa precisam passar por um treinamento distinto daqueles aplicados a funcionários que não utilizam computadores, *notebooks* etc. Já para os funcionários que mudarem de cargo, devem ser oferecidos treinamentos específicos para a nova a função, já aqueles que perderam alguma parte do treinamento por motivos diversos, devem ser estimulados a realizar o restante através de vídeo-aula, cursos *on-line*, material escrito, entre outros.

A melhor maneira de se resolver um problema é evitando-o, quando adentramos no universo da empresa, é fácil constatar que a tarefa de prevenção não é das mais simples, pois ainda que a mentalidade hoje esteja mudando, o investimento nessa área é limitado, ao passo que investem muitos nos sistemas, investem o mínimo em treinamentos para evitar ataques que usam como fator principal a Engenharia Social. Não que eles sejam desnecessários, mas ao contrário, ligando fatores tecnológicos como o uso da *intranet* para divulgação das informações, de novas políticas de segurança, a utilização dos *e-mails* para criar vínculos e divulgar vídeos, cursos para melhor se conseguir a segurança, são fundamentais e excelentes ferramentas, uma vez que as falhas humanas são tão comuns como as falhas técnicas.

Como o objetivo do processo de conscientização e treinamento é criar novos hábitos acerca da segurança da informação, concordando com Fonseca (2009), alguns tópicos não podem ser deixados de lado, como:

- Descrever as táticas empregadas e as formas que os engenheiros sociais as utilizam para manipular suas vítimas e assim cumprir seus objetivos.
- Como se realiza a identificação de um engenheiro social.
- Como responder de forma correta ao desconfiar de uma solicitação suspeita.
- Questionar as solicitações de informação, independente do cargo.
- A quem deve-se informar as tentativas de ataque ou ataques que aconteceram.
- Desconfiar de pessoas que fazem solicitações sem informar sua real importância.
- Como proceder para a proteção de informações sensíveis.
- Como encontrar as políticas de segurança e a sua importância na proteção da informação.
- Explicar e sintetizar o sentido de cada política adotada.
- Como realizar a divulgação de material ou de alguma informação restrita.
- Adoção de melhores práticas de uso de *e-mails*, evitando ataques de Engenharia Social.
- Questões de ordem física, como a utilização de crachás, senhas biométricas etc.
- Eliminação de documentos confidenciais de forma correta, seja de natureza física ou eletrônica.
- Parabenizar de forma pública os funcionários que cumprirem as regras e políticas de segurança.

Algumas outras questões podem ser abordadas, porém esses exemplos se tornam suficientes na explanação de como criar boas políticas de segurança através do treinamento e conscientização do bom uso das informações e como ela deve ser protegida. É assim, possível comprovar a eficiência do programa de treinamento quando todos aqueles que fazem parte da empresa participam e se empenham e põe em prática as normas estabelecidas.

Além da consciência sobre a importância da segurança da informação, os treinamentos também devem englobar as medidas tomadas em caso de não comprimento das políticas de segurança da empresa, bem como as consequências das normas e procedimentos estabelecidos, sendo divulgado amplamente. Estando assim os funcionários bem motivados, entusiasmados e conscientes do seu papel, eles buscarão cumprir o seu papel na manutenção do bem mais precioso da empresa, a informação.

Mas não há como evitar em 100% dos casos que uma invasão ou vazamento de informações aconteça, para esses casos se faz necessário o emprego não somente medidas protetivas de segurança da informação, mas também medidas corretivas e essas medidas estão explicitadas no Plano de Resposta a Incidentes.

4.2.2 Plano de resposta a incidentes

Concordando com Cabral (2015) quando diz que, não existem sistemas 100% seguros e complementando com Wadlow (2000) que diz que "a segurança é processo" e justamente por ser um processo, tem de ser executado todos os dias, pois caso contrário vulnerabilidades aparecerão e comprometerão a empresa. As falhas acontecerão, independente do sistema, ou das pessoas que operem esse sistema, portanto é necessário que as empresas estejam preparadas para realizar o conhecimento, a análise e por fim responder os incidentes de segurança o mais brevemente possível.

Por isso é fundamental a criação de um plano de resposta a incidentes, pois eles atuam de forma a amenizar os estragos advindos de um ataque ou a redução dos custos na sua manutenção, tendo em vista que as experiências anteriores servem de base para ocorrências futuras e para aprimorar a segurança como um todo.

O plano de resposta a incidentes segundo Popper (2003), é um documento que possui os procedimentos e diretivas a serem tomadas para a solucionar, agir de forma corretiva ou realizar o contorno de incidentes, onde o tratamento de cada incidente irá variar de acordo com alguns fatores, como a sua magnitude e os riscos que envolvem a empresa. Como abordado anteriormente, cada empresa possui uma cultura organizacional e particularidades próprias, logo o tratamento de resposta a incidentes também possui especificidades daquela empresa. Um mesmo tratamento de incidentes pode ser aplicado em outra empresa? A resposta é sim, porém não há certeza sobre os resultados que serão alcançados pela segunda empresa serão semelhantes ao da empresa primeira.

Como é observável, é de fundamental importância que cada empresa possua o seu próprio Plano de Resposta a Incidentes, independentemente do seu porte, pequeno, médio ou grande, ou do ramo de atividade seja ele comercial, industrial, etc. Sobre as medidas que serão aplicadas no Plano de Resposta a incidentes, concordando ainda com Popper (2003), elas não podem excluir como resultados:

- A identificação de autoria do ataque, sua seriedade, os danos que foram causados e quais são os responsáveis pelo incidente.
- Realizar a divulgação de forma urgente o evento ocorrido, para que não haja ataques semelhantes em outras áreas da empresa.
- Realizar os procedimentos necessários para reestabelecer aquilo que foi diretamente ou indiretamente afetado pelo ataque, como por exemplo, a mudança de senha, troca de funcionários, etc.
- Contatar os órgãos ou instituições de segurança, reportando o fato, para que fique registrado, bem como deve haver a tentativa de entrar em contato com os responsáveis pela realização dos ataques.

De acordo com o explicitado, é perceptível que os pontos principais levados em consideração pelo Plano de Resposta a Incidentes são constituídos como uma espécie de *timeline*[17], no primeiro momento é a realização da descoberta de quem efetivou o ataque e qual a sua dimensão, em seguida comunicar a todos que fazem parte da empresa sobre o ataque, prevenindo-se explicitamente de outros ataques parecidos, no terceiro passo é solucionar as falhas que foram exploradas e por fim e não menos importante realizar a reportação aos órgão competentes que tratam ou abordam a segurança da informação.

Neste capítulo foram apresentados alguns procedimentos que dentro do contexto da segurança da informação se mostram fundamentais para a criação de políticas de segurança objetivas e eficientes, tendo como ponto de vista principal a abordagem com da utilização da Engenharia Social. A lista de procedimentos abordados neste trabalho, mostra pontos comuns de defesa das organizações e de forma alguma buscam mostrar todas as maneiras possíveis de se evitar um ataque de um engenheiro social. Pois primeiramente, como para cada empresa esses procedimentos variam, a lista de procedimentos também tende a mudar de acordo com as especificidades da empresa, já que de acordo com Mitnick & Simon (2003); Cabral (2015), não há como se defender em todos os casos. A mitigação das vulnerabilidades, torna a empresa mais resistente e menos propícia a um ataque real e torna os danos causados mais fáceis de serem contornados.

[17] *Timeline*: linha do tempo, utilizada em muitas redes sociais.

4.3 Cartilha – Engenharia Social: Sua empresa está protegida?

Como maneira de contribuir de forma concreta e palpável, realizou-se o desenvolvimento de uma cartilha sobre a segurança da informação, tendo como foco os métodos de prevenção de ataques da Engenharia Social, os quais foram vistos nos tópicos anteriores. O seu objetivo é responder a alguns pontos explorados na criação das políticas de segurança da informação, no entanto de forma didática e resumida.

A cartilha será constituída de capa, sumário, introdução, definições sobre o que é a segurança da informação, Engenharia Social etc. Ela tem como foco, alcançar as empresas para que exista uma conscientização sobre a importância da segurança da informação dentro delas, abordando o fator humano como mais deficiente e que naturalmente precisa de investimentos. Será produzida e diagramada no aplicativo Adobe Photoshop CS6.

Os questionamentos levantados para a responder como se obtém uma política de segurança informação firme, tem como pilares os autores Conheady (2014), Hadnagy (2011), Fonseca (2009) e Popper (2003). Os dois primeiros autores levam em consideração os aspectos psicológicos, os dois últimos levam em consideração aspectos humanos de como mitigar e se recuperar de um ataque.

Esta cartilha não busca alcançar apenas as empresas, mas através da conscientização, espalhar esse método também a usuários comuns, como meio de se proteger e consequentemente conseguir proteger as suas informações pessoais, que por não perceberem o risco que correm, acabam deixando suas informações ao acesso de todos. Para melhor entendimento e visualização, é possível visualizar as páginas da cartilha no APÊNDICE I.

Devido a sua importância para a segurança da informação tendo como meio preventivo para ataques de Engenharia Social, são indicados para trabalhos futuros um estudo de caso, aplicando essa cartilha ou adaptando-a de acordo com as especificidades em uma empresa. Também é possível a aplicação em duas empresas e verificar então os pontos fortes e fracos, realizando uma comparação explanando onde e porque a cartilha obteve maior sucesso em sua aplicabilidade.

CONSIDERAÇÕES FINAIS

Diante do que foi exposto neste trabalho torna-se possível verificar que no que compete a Engenharia Social, a mesma não está estritamente ligada a métodos computacionais, sendo estes apenas um meio de se obter a informação desejada. Apesar deste trabalho evidenciar apenas alguns casos que envolvem o uso direto e determinante da Engenharia Social na ocorrência de um ataque, sabe-se que existem inúmeros outros, que se configuram nesse mesmo modelo. As razões para um ataque de um engenheiro social podem ser infinitas e distintas em cada caso.

Foi possível reconhecer o porquê desse modelo ser extremamente eficiente, pois tendo como foco o ser humano e suas limitações, o engenheiro se utiliza da percepção e analise, aproveitando todas as ferramentas a sua disposição e reconhecendo, portanto, um padrão nas ações de suas vítimas e estabelecendo diretrizes para o ataque. Sendo assim de difícil reconhecimento por parte do alvo.

No primeiro capítulo intitulado, "*A segurança da informação em sistemas e na web"*, chegou-se a percepção de que a utilização de sistemas computacionais, atuando como linha de defesa, são de extrema importância, porém se estes forem manuseados por usuários sem o devido treinamento, estarão susceptíveis a ataques e as ameaças digitais. Tornando todos os esforços para os investimentos nestes equipamentos de segurança da informação inúteis.

Já no segundo capítulo, "*Falhas na segurança da informação exploradas pela Engenharia Social"*, foi possível constatar que um dos modelos mais eficientes de busca por vulnerabilidades se dá através da utilização de um *pentest* e que dentre várias metodologias existentes, a OWASP que trata de aplicações *web* se enquadrou melhor diante da pesquisa. Também foi possível observar que na busca por vulnerabilidades em aplicações *web*, a utilização da Engenharia Social acontece de forma efetiva, utilizando meios tecnológicos como as ferramentas WHOIS e o *Port Scanning* em conjunto com os meios sociais através das técnicas de coleta de informações, elicitação e pretexto. No fim, foi possível compreender que a amplitude das ferramentas utilizadas, torna a Engenharia Social, efetiva de fato quanto a quebra da segurança da informação.

No terceiro capítulo, "*A Engenharia Social – uma arte a ser explorada*", foi possível entender que a Engenharia Social é utilizada como um fator que potencializa a

quebra da segurança. Para isso, constatou-se que o engenheiro social pode possuir nomenclaturas diferentes, cada uma baseada no tipo de engenheiro que se é, e que os ataques acontecem de forma direta ou indireta. Como forma de exemplificação foram trazidos os casos de Kevin Mitnick e do *Wells Fargo & Bank of America*, onde a Engenharia Social teve papel fundamental nas fraudes apontadas que geraram prejuízos não somente financeiros, mas a sua credibilidade no mercado.

Por fim no quarto capítulo intitulado, "*Mitigação das vulnerabilidades*", chegou-se a constatação de que a Engenharia Social, por explorar falhas humanas, e ser realizada por humanos que também possuem falhas, e podendo influenciar na mitigação dos ataques. No primeiro momento foi preciso entender que só é possível se defender de um ataque quando se conhece como se pode ser atacado, para isso foi abordado no tópico 4.1 como os engenheiros exploram as vulnerabilidades. Após isso nos tópicos seguintes foram analisados os métodos de prevenção de ataques, como a criação das políticas de segurança, e dentro delas estão o plano de treinamento e conscientização que buscam dar ao funcionário uma nova visão sobre a proteção dos dados. E nos casos onde já existem as brechas na segurança, se faz necessário a criação de um plano de resposta a incidentes que visa fechar as brechas existentes.

Sendo assim, como uma das contribuições do presente trabalho, criou-se uma mini cartilha sobre como se prevenir de um ataque de Engenharia Social, na qual contém os principais questionamentos acerca da proteção das informações da empresa e usuários, e como soluciona-los.

Sabendo, contudo, que o assunto não se encerra neste trabalho, tendo em vista que a Engenharia Social se utiliza de diversas áreas do conhecimento para desenvolver-se. Acredita-se que a presente pesquisa servirá de base para a criação e desenvolvimento de trabalhos futuros como nas áreas de segurança da informação, Engenharia Social, *pentests* etc.

REFENCIAS BIBLIOGRÁFICAS

ALLEN, Malcolm. **Social Engineering: A Means to Violate a Computer System**. SANS Institute InfoSec Reading Room. june/dec. 2006. Disponível em: <http://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT) – **Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 17799:2001**. Rio de Janeiro: ABNT,2003.

BACE, R.; MELL P. **Intrusion Detection Systems**. 2011. Disponível em: http://cryptome.org/sp800-31.htm. Acesso 03 de novembro de 2016.

BASSO, Tania. **Uma abordagem para avaliação da eficácia de scanners de vulnerabilidades em aplicações web**. Dissertação e Apresentação de Mestrado, 2010.

BATISTA, L. Felippe. **Métodos e práticas utilizadas em engenharia social com o intuito de obstar o roubo de informações sensíveis.** Projeto de TCC. Centro Universitário de Brasília, 2015.

BEAL, Adriana. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações - São Paulo: Atlas, 2005.

BELLINGER, G. **Knowledge Management. Consortium benchmarking study. Final report.** American Productivity & Quality Center, 1996.

BERLO, D. **O processo de comunicação: introdução à teoria e à prática**. São Paulo: Martins Fontes, 2003.

BOSWORTH, S.; KABAY, M. E. **Computer security handbook**. 4.ed. USA: Wiley, 2002.

BRASIL. Presidência da República. **Decreto Nº 7.724, de 16 de maio de 2012**. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do §3 do art. 37 e no §2 do art. 216 da Constituição. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm>.

CABRAL, Carlos; CAPRINO, William. **Trilhas em Segurança da Informação:** Caminhos e ideias para a proteção de dados. Rio de Janeiro. Braspot, 2015.

CAMPOS, André. **Sistema de Segurança da Informação**. 3 ed. Florianópolis: Visual Books, 2014.

CARVALHO, Alan Henrique Pardo. **Segurança de aplicações web e os dez anos do relatório OWASP Top Ten: o que mudou?** Fasci-Tech – Periódico Eletrônico da FATEC-São Caetano do Sul, São Caetano do Sul, v.1, n. 8, Mar./Set. 2014, p. 6 a 18.

CHIAVENATO, Idalberto. **Gestão de Pessoas.** 3ª edição, Editora Elsevier – campus, 2008.

COMMITTEE ON NATIONAL SECURITY SYSTEMS – CNSS. **Instruction No. 4009**. National Information Assurance (IA) Glossary. EUA: CNSS, 2006.

CONHEADY, Sharon. **Social Engineering in IT Security**: Tools, Tactics, and Techniques. Estados Unidos: McGraw-Hill Education, 2014.

DAVIS, M. A.; BODMER, S.; LEMASTERS, A. (2010). **Hacking exposed malware & rootkits: malware & rootkits security secrets & solutions**. New York, McGraw Hill.

DOLAN, A. **Social engineering**. [S.l.]: Sans Institute. 2004.

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

FETTE, I., Sadeh, N., e Tomasic, A. (2007). ***Learning to detect phishing emails***. Em Proceedings of the 16th International Conference on World Wide Web, WWW, 2007.

FONSECA, Jose; VIEIRA, Marco; MADEIRA, Henrique. **The web attacker perspective - a field study**. In: Software Reliability Engineering (ISSRE), 2010. IEEE 21st International Symposium on. IEEE, 2010. P .299-308.

FONSECA, Paula F. **Gestão da segurança da informação:** O fator humano. 2009. 16 f. Monografia (Especialização) – Redes e Segurança de Computadores, Pontifica Universidade Católica do Paraná (PUC-PR), Curitiba, 2009. Disponível em: http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf. Acesso em 22/11/2016.

GIAVAROTO, Silvio César Roxo. SANTOS, Gerson Raimundo dos. **Backtratrack Linux: auditoria e teste de invasão em redes de computadores**. Rio de Janeiro, Ciência Moderna Ltda., (2013).

HADNAGY, Cristopher. **Social Engineering: The Art of Human Hacking. Indianapolis**, IN: Wiley Publishing, 2011.

HAROLD F. Tipton. **Official (Isc) 2 Guide to the SSCP Cbk, Second Edition (2nd ed.)**. Auerbach Publications, Boston,MA, USA, 2010.

HARDIKAR, A. M. **Malware 101 – Viruses**. SANS Institute, 2008. Disponível em: https://goo.gl/kY1bcc.

KIMBERLY, Graves. Ceh **Certified Ethical Hacker Study Guide**. USA. Wiley Publishing, 2010.

LAUREANO, Marcos Aurélio Pchek. **Gestão de Segurança da Informação**. 1/06/2005. Disponível em: http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em: 26/10/2016.

MANN, Ian. **Engenharia Social**. São Paulo: Edgar Blücher, 2008.

MANSON, M. **Estudio sobre vírus informáticos**, 1999. Disponível em: <http://www.monografias.com/trabajos/estudiovirus/estudiovirus.shtml?monosearch. Acesso em: 12 set. 2016.

MARCELO, Antonio; PEREIRA Marcos. **A arte de hackear pessoas.** Rio de Janeiro: Brasoft, 2005, p. 4-26-30- 5.

MELL, P. and karen Kent, N. J. (2005). **Guide to Malware Incident Prevention and Handling Recommendations of the National Institute of Standards and Technology**, volume 800-83. Department of Homeland Security, Gaithersburg, 800-83 edition.

MEUCCI, M. **Owasp testing guide version 3.0**. OWASP Foundation. 2008.

MITNICK, KEVIN D.; SIMON, WILLIAM L. **A arte de enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 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.

MOORE, T; CLAYTON, R; ANDERSON, R. ***The Economics of Online Crime.*** *In: Journal of Economics Perspectives*, v.23, n. 3, P. 3-20, 2009.

MUNIZ, Joseph; LAKHANI, Aamir. **Web Penetration Testing with Kali Linux**. Birmingham: Packt. 2013.

NAKAMURA, Emilio Tissato. **SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS**. Novatec 2007.

NIST. **Guide to Malware Incident Prevention and Handling**. Recommendations of the National Institute of Standards and Technology, 2005. Disponível em: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf. Acesso em 07/10/2016.

NIST Special Publication 800-115: **Technical Guide to Information Security Testing and Assessment** (Scarfone, Souppaya, Cody, Orebaugh, 2008).

OLIVEIRA, Túlio. **Testes de Segurança em Aplicações Web segundo a metodologia OWASP**. Projeto de TCC. Universidade Federal de Lavras. 2012.

OSBORNE, K. Auditing The IT Security Function. **Revista Computers & Security**, 17, 1998. p.34-41.

PEIXOTO, Mário C. P. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

PIPER, S. **Intrusion Prevention Systems for Dummies**. New Jersey: Wiley Publishing, Inc, 2011.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. **ENGENHARIA SOCIAL**: Um Perigo Eminente. [2003]. 11 f. Monografia (Especialização) – Gestão Empresarial e Estratégias de Informática, Instituto Catarinense de Pós-Graduação – ICPG, (2003).

PRESIDÊNCIA DA REPÚBLICA. Instituto Nacional de Tecnologia da Informação – ITI.CRIPTOGRAFIA. In: **O que é Certificação Digital?** Brasília: ITI/PR, 2005. Disponível em: < http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf>.

REZENDE, D.A.; ABREU, A. F. de. **Tecnologia da informação aplicada a sistemas de informações empresariais**: o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2000.

SÊMOLA, M. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus Elsevier, 2003.

SCHWARTAU, Winn. **Engenharia social: pessoas ainda são elo mais fraco**. [S.l.:s.n.], 2010. Disponível em: http://www.modulo.com.br/comunidade/noticias/1281-engenharia-social-pessoas-ainda-sao-elo-mais-fraco-diz-especialista

SILVA, Rodrigo; LIMA, Rommel; LEITE, Cicilia; SILVA, Romero. **Investigação de segurança no moodle**. Renote, v. 12, n. 2, 2014.

SOCIAL ENGINEER, INC. **The Social Engineering Framework**. Disponível em: http://www.social-engineer.org/framework/general-discussion, acesso em 17/11/16.

SONY, P.; Firake, S.; Meshram, B. B. "***A phishing analysis of web based systems***". *In: International Conference on Communication Computing & Security.* Redmond, EUA, (2011).

STALLINGS, William. **Criptografia e segurança em redes**. 4.ed. São Paulo: Person Prentice Hall, 2008.

TORRES, André Felipe F. **Os referenciais de segurança da informação e a melhoria contínua: um caso exploratório.** Dissertação e Apresentação de Mestrado. 2014.

VARGAS, Alexandre. **Ameaça além do Firewall. Porque as empresas devem se preparar contra a Engenharia Social,** [mensagem pessoal]. Acesso em 05/11/2016.

WADLOW, Thomas A. **Segurança de Redes:** projeto e gerenciamento de redes seguras. Tradução: Fábio Freitas da Silva - Rio de Janeiro: Campus, 2000.

WENDT, Emerson; NOGUEIRA, Higor Vinicius. **Crimes Cibernéticos ameaças e procedimento de investigação**. 2. Ed. Rio de Janeiro; Brasport, 2013.

WILHELM, Thomas. **Professional Penetration Testing**. Burlington, Syngress, 2009.

APÊNDICES

UNIVERSIDADE DO ESTADO DO RIO GRANDE DO NORTE – UERN
FACULDADE DE CIÊNCIAS NATURAIS E EXATAS - FANAT
DEPARTAMENTO DE INFORMÁTICA – DI

VINNÍCIUS LUAN DOS SANTOS COSTA

SEGURANÇA DA INFORMAÇÃO: USO DA ENGENHARIA SOCIAL COMO MÉTODO DE ATAQUE E COMO MITIGAR SEUS EFEITOS.

CARTILHA – ENGENHARIA SOCIAL: SUA EMPRESA ESTÁ SEGURA?

SUMÁRIO

CONSIDERAÇÕES:

Esta cartilha, tem como foco abordar a temática da engenharia social dentro da segurança da informação. Possui como fonte de pesquisa autores nacionais e internacionais que tratam do tema. Trazendo as principais ferramentas de ataques da engenharia social, bem como conseguir construir uma defesa sólida e mitigando vulnerabilidades através de pontos específicos.

Este trabalho foi realizado como parte da Monografia do dicente Vinnícius Luan dos Santos Costa, graduando do curso de Ciência da Computação, através do Departamento de Informática (DI), pela Universidade do Estado do Rio Grande do Norte (UERN).

INTRODUÇÃO

No mundo atual as empresas estão cada vez mais conectadas e à Internet consequentemente mais expostas a ataques, sejam a nível técnico ou humano. Os ataques podem ocorrer tanto de dentro, quanto do lado de fora. Dentro das organizações o fator humano muitas vezes é desconsiderado quando se fala em "segurança da informação". Esta cartilha tem como objetivo alertar para a importância desse poderoso agente, mostrando como ele pode ser explorado.

A motivação para a criação desta cartilha, em um primeiro momento é, alertar empresas e funcionários sobre o risco no qual eles estão envolvidos e sujeitos. Bem como a tentativa de diferentemente de outros pesquisadores que possuem a visão sobre o aspecto tecnológico, alargar a visão sobre a problemática.

As falhas humanas estão diretamente ligadas a perda e roubo de informações sensíveis, através de um meio denominado "engenharia social", e que é preciso estar preparado para possíveis ataques.

DEFINIÇÕES

Para melhor compreender a importancia da segurança da informação e sobre como a engenharia social é perigosa, é preciso defini-las:

- Segurança da Informação: É uma área de estudo que visa proteger a informação de ameaças, que em sua finalidade buscam comprometê-la ou de algum modo torná-la inacessivel.

- Engenharia Social: É uma técnica que tem como finalidade enganar pesoas, a fim de obter acesso a uma informaçaão ou conjunto de informações das quais não posui, comprometendendo assim a segurança da informação.

Em uma analogia rápida, a engenharia social é como uma chave-mestre capaz de abrir qualquer porta, por mais segura que esta seja.

4

FATORES PSICOLÓGICOS

A engenharia social é realmente efitiva, porque diferente de um ataque a um sistema, o engenheiro social foca o ser humano que o controla. Ele utiliza o fator psicológico para enganar as vitimas a fornecerem os dados necessários. Entre os fatores podemos citar:

(1) Confiança: Uma das melhores armas utilizadas pelo engenheiro social, pois ele se beneficia de que a maioria das pessoas não é capaz de identificar uma mentira.

(2) Medo de Autoridade: Todos possuem o entendimento de que se deve obedecer a ordem de autoridades. Nessa tentativa, o engenheiro se passa por algum chefe que precisa de uma informação urgente.

(3) Desejo de ser útil: A bondade é própria do ser humano, com isso o engenheiro social se utiliza dessa arma tornando a vítima importante por ajuda-lo em algo.

(4) Falta de preocupação com a segurança: Por não saberem o valor da informação, os funcionários acabam espalhando em diversos meios informações próprias da empresa.

UERN

5

FATORES PSICOLÓGICOS

Como Mitigar?

(1) Procure sempre estar atualizado sobre as informações básicas sobre a empresa e ao ser questionado sempre desconfie da real intenção de quem o pergunta, se possivel questione-o.

(2) Como os engenheiros costumam se passar quem não são de fato, ao ser questionado por alguma autoridade que não se conhece, busque checar se as informações fornecidas são as mesmas que você possui sobre a pessoa em questão.

(3) Ao ajudar alguem dando alguma informação, mesmo que desconhecido, avalie se a informação é realmente necessária de ser dada.

(4) A informação é o bem mais preciso da empresa, então evite falar ao celular ou telefone informando senhas, nomes de pessoas, bem como compartilhar fotos, vídeos de forma pública, informando localização e divulgando o ambiente interno da empresa.

UERN

6

MITIGAÇÃO DA ENGENHARIA SOCIAL

Algumas categorias podem ser usadas para ajudar a encontrar ou identificar um ataquie de engenharia social, entre elas podemos citar:

- Atitude: Os engenheiros sociais, sao pessoas educadas, com muito bom humor, ao perceber a atitude do atacante é possivel evitar um ataquer.

- Tentativa de conexão: Eles buscam se conectar as suas vítimas, muitas vezes utilizam os nomes de pesoas conhecidas, é preciso verificar a autenticidade da informaçao antes de dar um próximo passo, como informar dados etc.

- Pequenos erros: Eles assim como outros seres humanos possuem limitaçoes, principalmente os menos experientes, nenhum detalhe pode passar despercebido por quem está sendo atacado. Um treinamento é uma excelente opção para aguçar as barreiras individuais da informação.

UERN

7

MITIGAÇÃO DA ENGENHARIA SOCIAL

Para criar uma defesa sólida contra os ataques de engenharia social, é preciso saber que existem documentos que servem de modelo para estruturar uma boa defesa.

Entre esses documentos, o principal deles são as Políticas de segurança da informação, sabe por que elas são tão importantes?

- Através delas, a empresa criar protocolos de defesa evitando ataques.
- Porque Identificam quais as informações que devem ser guardadas.
- Faz o reconhecimento de quais são as principais ameaças as empresas.
- Avalia os riscos em casos onde a informação foi corrompida.
- Cria medidas para evitar nos ataque e para solucionar os efeitos de ataques mais frequentes.

UERN

8

MITIGAÇÃO DA ENGENHARIA SOCIAL

Dentro das políticas de segurança da informação, estão tambem descritos dois pontos para se construí-la, são as Poiticas de Treinamento e Conscientizaçao e a Política de Resposta a Incidentes.

As Políticas de Treinamento e Conscientização visa dar aos funcionários o entendimento do valor da informação para a empresa, através de treinamento e cursos, motivando-os a agirem corretamente na divulgação de dados, bem como alertando sobre as sanções em caso de não cumprimento.

As poíticas de Resposta a Incidentes visam sanar as falhas ocorridas de forma rapida e objetiva e evitar que falhas recorrentes aconteçam frequentemente. Permitindo tambem através do erro, a aprendizagem.

UERN

9

POLÍTICAS DE TREINAMENTO E CONSCIENTIZAÇÃO

Aqui, alguns pontos são abordados para melhorar e eficiência da defesa da empresa, podemos citar:

• Como responder de forma correta ao desconfiar de uma solicitação suspeita?

- Comunicar ao setor de segurança, e dizer que não pode fornecer a informaçao solicitada.

• Questiono as solicitações de informação, independente do cargo?

- Sim, Se não conhecer quem solicita as informações, verificara quem de fato é a pessoa que pede e questionar sua finalidade.

• Como proceder para a proteção de informações sensíveis?

- A!tenção, verifique a identifcação de quem pede as informações, cheque se são autenticas. Os erros só sao perceptiveis com um olhar atento as brechas deixadas pelo engenheiro social e com treinamento específico.

UERN

10

POLITICA DE RESPOSTA A INCIDENTES

Existem alguns outros pontos que devem ser levantados quando os ataques ja foram realizados, são as políticas de Resposta a Incidentes, são eles:

• A identificação de autoria do ataque, sua seriedade, os danos que foram causados e quais são os responsáveis pelo incidente.

- Em caso de não haver um setor de TI voltado pra isso, pode ser contratada uma empresa para realizar uma auditoria através de um *Pentest*. Pois ele identificará a autoria, os danos e quem foi diretmaente afetado.

• Realizar a divulgação de forma urgente o evento ocorrido.

- Isso se faz necessário para alertar todos os setores da empresa para que não sejam também prejudicados.

• Contatar os órgãos ou instituições de segurança, reportando o fato.

- É imprescidível essa reportação, pois fornecerá subsídios de informação para outras empresas sobre ataques semelhantes.

UERN

11

COINCLUSÃO

Apesar de ter seu foco para órgãos e empresas, as informações aqui apresentadas, também podem ser direcionadas para usuários comuns, para que compreendam quão valioso é o bem da informação.

Por se tratar de uma cartilha, esta não leva em consideração todos os pontos para o combate da sngenheria social, mas busca apresentar uma visão mais ampla sobre como realizar a defesa.

Cada empresa possuí especificidades e a modelagem das politicas de segurança da informação, devem atentar para uma nova modelagem a cada empresa diferente.

Para mais informações sobre o tema, é recomendada a leitura do trabalho de conclusão de curso:

- Segurança da informação: uso da engenharia social como método de ataque e como mitigar seus efeitos.

UERN

12

REFERÊNCIAS BIBLIOGRÁFICAS

CONHEADY, Sharon. Social Engineering in IT Security: Tools, Tactics, and Techniques. Estados Unidos: McGraw-Hill Education, 2014.

FONSECA, Paula F. Gestão da segurança da informação: O fator humano. 2009. 16 f. Monografia (Especialização) – Redes e Segurança de Computadores, Pontifica Universidade Católica do Paraná (PUC-PR), Curitiba, 2009. Disponível em: http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf. Acesso em 22/11/2016.

HADNAGY, Cristopher. Social Engineering: The Art of Human Hacking. Indianapolis, IN: Wiley Publishing, 2011.

POPPER, Marcos Antonio; BRIGNOLI, Juliano Tonizetti. ENGENHARIA SOCIAL: Um Perigo Eminente. [2003]. 11 f. Monografia (Especialização) – Gestão Empresarial e Estratégias de Informática, Instituto Catarinense de Pós-Graduação – ICPG, (2003).

UERN