FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Felipe do Santo Cavalcanti

A SEGURANÇA DAINFORMAÇÃO NAS REDES SOCIAIS

Americana, SP

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

Felipe do Santo Cavalcanti

A SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação do Prof. Me. Henri Alves de Godoy.

Área de concentração: Segurança da Informação

Americana, S. P.
2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS

Dados Internacionais de Catalogação-na-fonte

Cavalcanti, Felipe do Santo

C364s A segurança da Informação nas redes sociais. / Felipe do Santo Cavalcanti. – Americana: 2016.

56f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Me. Henri Alves de Godoy

1.Segurança em sistemas de informação I. Godoy, Henri Alves de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU:681.519

Felipe do Santo Cavalcanti

A SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 24 de junho de 2016.

Banca Examinadora:

Henri Alves de Godoy (Presidente)
Mestre
FATEC - Americana

Daniele Junqueira Frosoni (Membro)
Especialista
FATEC - Americana

Benedito Luciano Antunes de França (Membro)
Mestre
FATEC - Americana

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me dado saúde e força para superar as dificuldades. Agradeço também aos meus pais, irmão, tios, e à minha namorada pelo amor, incentivo e apoio incondicional.

Ao professor Henri Godoy, pela paciência na orientação e incentivo que tornaram possível a conclusão deste trabalho.

A esta universidade e seu corpo docente, direção e administração que tornaram possível a oportunidade de crescimento e aprendizado durante todo o período em que aqui estive.

RESUMO

As redes sociais na Internet, acessíveis através de mídias que possibilitam relacionamentos, possuem um grande número de informações dispostas e compartilhadas entre seus utilizadores, informações estas muitas vezes sensíveis e particulares. A maioria destes usuários não compreendem os riscos existentes neste meio assim como a importância da segurança da informação para proteger seus dados de diversos tipos de ataques presentes na Internet.

O presente trabalho visa mostrar os riscos envolvidos neste universo e suas respectivas formas de prevenção além disso, deseja mostrar que existem maneiras de acessar as redes sociais na Internet tendo a segurança da informação como foco principal. Utilizando-se das mídias sociais sem uma demasiada exposição, resguardando as informações por meio de técnicas e metodologias práticas.

Palavras-chave: Segurança da Informação; Internet; Redes Sociais.

ABSTRACT

Social networks on the Internet, accessible through the media que enable relationships; have a large number of willing and information shared among its users, information These Often sensitive and private. Most of These users do not understand the risks in this medium and the importance of information security to protect your data from various kinds of gifts attacks on the Internet.

This work AIMS to show the risks Involved in this universe and their ways of Preventing and further show que there are ways to access social networks on the Internet with information security as a main focus. Using social media without too much exposure, protecting the information through technical and practical methodologies.

Key words: *Information security; Internet; Social networks.*

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Diversas pessoas ao redor do mundo utilizam as redes sociais para manterem vários níveis de contato e compartilhamento de informações. Este fator é essencial nos dias de hoje devido ao encurtamento de distâncias e a facilidade do acesso.

Este evento tem tomado grandes proporções, por este motivo é indispensável a preocupação com a privacidade e com a segurança da informação de usuários e empresas que utilizam este tipo de rede.

O presente trabalho objetiva-se a resgatar os conceitos da segurança da informação nas redes sociais, mostrando o uso da tecnologia envolvida nas ferramentas disponíveis para que se evitem danos relacionados à disponibilidade, à integridade e à confidencialidade das informações na Internet.

Entre outros objetivos observar-se-á de que forma o compartilhamento de informações realizado de maneira incorreta pode afetar o usuário em diversos setores.

Avaliar e influenciar o leitor a respeito da conduta utilizada no acesso as redes sociais de modo geral.

O presente trabalho acadêmico também busca ser relevante para a comunidade ativa na Internet no que diz respeito aos riscos envolvidos nas redes sociais, além de gerar uma ótica fundamentada sobre os conceitos, ferramentas e metodologias de segurança da informação envolvidos.

Demonstrar de maneira prática e objetiva os riscos presentes nas mídias sociais com base em um ataque *Man In The Middle, e,* fixar a ideia de um uso consciente das redes, além de instruir a respeito da preservação da privacidade das informações compartilhadas.

Avaliar-se-ão ainda as questões relacionadas as vulnerabilidades que permitem que os ataques aconteçam, exibindo exemplos dos mesmos e as respectivas formas de prevenção.

2. SEGURANÇA DA INFORMAÇÃO

Segundo à Agência Brasileira de Normas Técnicas, ABNT.NBR ISO/IEC: 27002/2005 define-se segurança da informação como sendo um conjunto de métricas específicas de boa conduta e de ferramentas para que se tenha segurança no que se refere a informações digitais. Tem por objetivo proteger e restringir acessos indevidos e/ou não autorizados aos ativos das organizações ou usuários, sendo eles fornecedores, dados pessoais, produtos e clientes, entre outros.

A segurança da informação tem como principal finalidade proteger através do desenvolvimento e utilização de técnicas às informações intangíveis, mantendo, assim a continuidade do negócio.

Dantas (2011, p. 11-14) afirma que para que este objetivo seja alcançado deve-se utilizar os princípios básicos, entre eles:

Confidencialidade: Métrica que garante que a informação somente possa ser acessada por pessoa autorizada, tendo relação com o sigilo da informação, evitando acessos indevidos, garantindo a confiança da informação.

Integridade: Métrica que garante que a informação não seja modificada, ou seja, que a informação saia da origem e chegue a seu destino sem qualquer tipo de alteração ou danos.

Disponibilidade: Métrica que garante que a informação esteja sempre disponível quando se fizer necessária, utilizando-se de ferramentas tais como backup e alocação de um servidor de contingência em outra localidade.

Autenticidade: Princípio que se garante conhecer a identidade de um usuário ou sistema no momento em que está se comunicando, mantendo, assim, a originalidade das informações recebidas e enviadas. Para este fim a ferramenta mais utilizada atualmente são as assinaturas digitais.

2.1 O papel da segurança da informação nas redes sociais

O cenário das redes sociais é um lugar repleto de benefícios e bem atrativo devido à comodidade, encurtamento de distâncias, entre outros; entretanto, é preciso cuidado e vigilância com os fatores relacionados à segurança do usuário ou empresa que os utiliza.

A primeira diretriz para se manter seguro é definir a motivação para o uso, em segundo lugar, é necessário utilizar os critérios de acesso, utilizando os critérios como limitadores, inibindo, assim, riscos referentes a acessos ou postagens que possam ser realizadas.

As consequências e o impacto das redes sociais geraram novos desafios para a segurança da informação, tanto nos acessos domésticos quanto corporativos. No que diz respeito ao uso doméstico, pode-se dizer que cada dia mais as pessoas têm aberto mão da própria privacidade e isso torna-se um problema cultural de acesso. O usuário deve de maneira bem simples perguntar-se:

- Já realizou a busca de seu nome completo em algum mecanismo de pesquisa?
- Nas redes sociais, às quais participa, já revisou os requisitos de privacidade em todas elas?
- Já revisou a força de sua senha de acesso?

Tendo em vista os riscos para as corporações, sabem-se que os prejuízos de um ataque ou exposição são bem maiores e prejudiciais, afetando, além de tudo, a parte financeira, fazendo com que ocorra perda de dinheiro, clientes e de credibilidade.

Por estes motivos, foram desenvolvidos mecanismos de segurança para que se evite esse tipo de transtorno. Estes mecanismos subdividem-se em dois temos segundo artigo escrito por Yahya Mehdizadeh (2003) sendo:

Controle Físico: criação de barreiras físicas que impeçam a aproximação ou acesso de pessoas não autorizadas ou eventos que, por ventura, venham causar dano a infraestrutura tecnológica da corporação. Pode-se citar como controle físico os leitores biométricos, catracas de acesso portas e blindagens.

Controles Lógicos: Controles que barram acessos indevidos e não autorizados no que se diz respeito a danos no meio digital e eletrônico, impedindo acesso às informações e protegendo a integridade dos dados.

São exemplos de controles lógicos: Criptografia, assinatura digital, Firewall, autenticação de usuários.

2.2 Convergência entre controles de acesso

Segundo Yahya Mehdizadeh (2003), existe uma grande importância na fusão dos controles de acesso físico e lógico em que um complementa o outro, gerando mais segurança e confiabilidade às informações, como exemplo pode se imaginar um cenário que possua vigilância 24 horas por câmeras de segurança, em que os dados gravados não ficam armazenados para futuras consultas. Desta forma a medida se torna vã uma vez que caso necessário não se teria provas nem registros de algum fato ocorrido. Neste exemplo, uma maneira de se realizar esta convergência é o de adicionar um mecanismo que armazene os dados gravados, possibilitando futuras consultas a eles. É de extrema importância o alinhamento dos dois tipos de controle de acesso para que se tenha uma segurança da informação mais eficiente e para isso esses fatores devem estar devidamente alinhados, e, integrados aos processos da empresa que incluem:

- Uma política bem elaborada de segurança da informação;

- Provisionamento de ativos e pessoas;

- Monitoramento e auditoria;

- Plano de respostas a incidentes;

- Plano de continuidade de negócios.

Esta união é de grande valor para a inibição e a prevenção de ataques e para a detecção e correção caso eles aconteçam.

2.3 Senha

A cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil instrui que a senha é um mecanismo de segurança utilizado para gerar o acesso ao ambiente do usuário correspondente a ela, ou seja, ela verifica e certifica o quesito autenticidade de um acesso.

A criação de uma senha com nível alto de segurança deveria ser a principal preocupação dos usuários da Internet, afinal uma senha furtada pode liberar acesso a informações importantes por alguém não autorizado.

A importância da complexidade da senha escolhida é fundamental para que se evite não somente ataques de tentativas e erros que possam ser realizados por um indivíduo, mas também para coibir o sucesso de softwares, softwares os quais são desenvolvidos especificamente para este fim. Estes sistemas são capazes de testar diversas combinações por minuto intitulando um ataque de força bruta.

O levantamento realizado pela empresa Splash Data (2014) mostra a listagem contendo as 25 piores senhas do ano, estes dados podem ser vistos na Tabela 1:

Tabela 1. Piores senhas em níveis de segurança

Posição	Senha
1	123456
2	Password (Senha)
3	12345
4	12345678
5	Qwerty
6	123456789
7	1234
8	Baseball
9	Dragon (Dragão)
10	Football (Futebol americano)
11	1234567
12	Monkey (Macaco)
13	Letmein
14	abc123
15	111111
16	Mustang
17	Access (acesso)
18	Shadow (sombra)
19	Master
20	Michael
21	Superman
22	696969
23	123123
24	Batman
25	Trustno1 (Não confie em ninguém)

Fonte: SplashData (2014)

Os dados mostram a mínima importância dada por parte do usuário à senha de acesso, mostrando que esses preferem utilizar uma senha fraca invés da criação de uma senha complexa, portanto mais difícil de ser decifrada. Desta maneira a segurança da informação encontra sua principal dificuldade que é quando esse esbarra no fator humano.

Segundo à cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, existem três grupos básicos de mecanismos de autenticação: aquilo que você é (informações biométricas), aquilo que você possui (cartão de senhas bancárias) e aquilo que você sabe (informações como respostas a perguntas pessoais).

As métricas para se criar uma senha com nível de segurança elevado e de fácil memorização partem dos princípios:

- Não utilizar nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas (estes tipos de informações seriam facilmente descobertos por alguém próximo, com vínculo familiar ou de seu círculo de amizades)

- Não utilizar senhas associadas à proximidade entre os caracteres no teclado, como “1qaz2wsx” e “QwerTAsdfG” (estes caracteres podem ser facilmente visualizados por alguém próximo no momento da digitação).

- Não utilizar palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas etc. (estes tipos de senhas são comumente utilizados por sistemas de força bruta para tentativa de invasão).

- Use a mistura de letras, símbolos especiais e números;

- Use letras maiúsculas e minúsculas;

- Use uma quantidade de caracteres superior ao recomendado;

- Não use a opção de “lembrar senha” em computadores públicos.

3. RISCOS DO USO DA INTERNET

À cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, indica que o conceito de Internet é definido por um conjunto de diversas redes que se interligam fazendo uso de uma mesma linguagem, ou seja, utilizam o mesmo conjunto de regras ou protocolo para comunicação (TCP/IP). Trata-se de uma rede pública e descentralizada, sendo assim, não possui dono.

Com o crescimento desta rede foram aprimoradas ferramentas para facilitar, tornar ágil e agradável ao usuário os usos dos recursos disponíveis na rede, tratam-se de navegadores também chamados de *browsers*, programas para envio e recebimento de mensagens, distribuição de arquivos e compartilhamento de dados.

3.1 Navegadores

Á cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, instrui que o navegador, também chamado de programa cliente *web* ou *browsers*, o navegador é a mais utilizada e principal ferramenta para acesso da Internet. É responsável por solicitar o servidor *web* desejado as informações requisitadas e transmitir esses dados ao usuário.

Atualmente, existem diversos tipos de navegadores, e pode afirmar que nenhum deles é totalmente seguro. Á cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil ainda cita riscos relacionados ao uso de navegadores, dentre eles:

- *Coockies*: Trata-se de arquivos de texto de pequeno porte gravados na máquina durante o acesso, e que são reutilizados caso esse site volte a ser consultado são utilizados para manter informações sobre a visita realizada. Surgiram em 1994 para auxílio nas aplicações de sites de comércio eletrônico. São utilizados para lembrar suas referências, guardar nomes de usuários e até mesmo senhas.

Podem ser temporários, ou seja, são excluídos assim que o navegador é fechado ou permanentes, se alocando na máquina até o tempo determinado para expiração ou até ser removido. Também podem ser do tipo *first-party* definido pelo site visitado ou *thirtd-party* quando esse pertencente a outro domínio.

Os riscos que os *coockies* proporcionam, incluem compartilhamento de informações, exploração de vulnerabilidades, autenticação automática, coleta de informações pessoas e a coleta dos hábitos de navegação.

- *Códigos Móveis*: São códigos criados por desenvolvedores com a finalidade de aprimorar a experiência de navegação, melhorando a funcionalidade e aparência das páginas da Internet. Oferecem riscos que incluem programas e *applets* Java, Java *Scripts* e controle *Activex*.

- *Pop-up*: Definem janelas que são executadas automaticamente sem a permissão do usuário possuem riscos relacionados à, mensagens indesejadas, vínculo com links mal-intencionados.

- *Plug-ins*: São pequenos programas desenvolvidos por terceiros para adicionar funções auxiliares ao navegador que o mesmo não possui originalmente, os riscos referentes a esses programas dizem respeito ao controle sobre o local onde é armazenado. Podem, também, incluir códigos maliciosos que serão executados pelo usuário acreditando se tratar de uma aplicação benéfica.

- *Links Patrocinados*: Trata-se de propagandas acordadas entre o anunciante e o site que a divulgará, o lucro é gerado através de cada acesso dos usuários com base em um valor pré acordado. Os riscos desse tipo de *link* estão em um redirecionamento malicioso para páginas de *phishing,* em que o usuário insere dados de conta e senhas, acreditando estar no site original.

- *Banners*: São espaços disponibilizados em páginas da *web* com o intuito de divulgar informações sobre produto ou comércio, o método de lucratividade funciona da mesma maneira, que para os *links* patrocinados. O risco desta ferramenta está na criação de anúncios mal-intencionados apresentando publicidades em diversas páginas simultaneamente.

- Programas Compartilhamento de Arquivos P2P (*peer to peer*): São programas que permitem o compartilhamento de arquivos máquina a máquina sem o intermédio de uma segurança especial ou servidor que gerencie a troca de informações, os riscos desse uso estão no acesso indevido a diretórios e arquivos, obtenção de arquivos maliciosos contidos no computador de outrem e a violação de direito autorais de músicas, livros e artigos.

3.2 VULNERABILIDADES

As vulnerabilidades em segurança da informação caracterizam erros de programação, má configuração ou falha humana durante processos de *hardware* e *software*. Este fator cria espaços que podem tornar ataques, ou acesso às informações bem-sucedidas, sendo assim, as vulnerabilidades são pontos fracos de qualquer estrutura física ou lógica dentro da tecnologia da informação.

Comumente ocorrem casos de falhas em *softwares* ou sistemas operacionais em que as vulnerabilidades são expostas, como por exemplo um sistema operacional com uma brecha de segurança em determinada porta que poderia permitir uma invasão por parte de um atacante, liberando acesso a toda uma rede e comprometendo informações corporativas.

A Tabela 2 exibe uma listagem de vulnerabilidades disponíveis para consulta em levantamento de 20 itens realizado pela Sans Istitute:

Tabela 2. Vulnerabilidades

	CIS Critical Security Controls - Version 6.0
1	Inventory of Authorized and Unauthorized Devices
2	Inventory of Authorized and Unauthorized Software
3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Administrative Privileges
6	Maintenance, Monitoring, and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols, and Services
10	Data Recovery Capability
11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on the Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Appropriate Training to Fill Gaps
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

Fonte: Sans.org, 2000 - 2016

Além destas, é um ato comum das empresas fabricantes do *hardware* ou *software* disponibilizarem informações sobre as vulnerabilidades que esses possuem, assim como atualizações (*patches*, *hotfix*, pacotes de serviços), para que essas sejam corrigidas. Sendo assim o processo de manter as atualizações em dia é a principal ferramenta no combate a ataques a em decorrência das vulnerabilidades.

3.2.1 Serviços de mensagens instantâneas

Á cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, remete ao entendimento de que os maiores riscos que envolvem serviços de mensagem instantânea, estão vinculados ao próprio conteúdo do diálogo. Existem técnicas de engenharia social que em sua essência é a arte de enganar pessoas, que geralmente possuem pouco conhecimento dos métodos de segurança disponíveis para uso. Está técnica pode ser executada de maneira direta e pessoal através de um diálogo estabelecido ou fazendo uso de recursos tecnológicos tais como *e-mail*, telefone, *chats*.

O objetivo deste tipo de técnica é utilizar o poder de persuasão através de uma conversa comum e amigável e obter informações importantes e pessoais como, por exemplo, senhas e números de cartões de crédito.

No meio tecnológico, a engenharia social, primeiramente coleta as informações fazendo uso de redes sociais ou por troca de *e-mails*, após, desenvolve um relacionamento com a vítima, para depois começar a extrair as informações necessárias para a execução de um ataque utilizando de ferramentas como:

- Envio de mensagens com conteúdo falso;

- Criação de perfis falsos em redes sociais;

- Envio de arquivos vinculados a códigos maliciosos (*backdoor*).

A utilização destes meios e softwares fornece ao atacante o IP do computador da vítima, dando total acesso para que vulnerabilidades sejam exploradas.

Programas de comunicação instantânea como *Whatsapp*, *Facebook Messenger*, *Skype*, ICQ estão constantemente expostos a ataques de vulnerabilidades deste tipo, a prevenção contra isso pode ser realizada através de:

- Manter o software constantemente atualizado minimizando as vulnerabilidades;
- Utilizar um bom software de antivírus, seja em microcomputadores ou em dispositivos móveis, assim como verificar as atualizações de vacinas e versões dos mesmos;
- Restringir assuntos de conteúdo confidenciais e pessoais, principalmente com pessoas desconhecidas;
- Restringir a exibição do endereço IP no software a ser utilizado, caso esta opção já não venha configurada por padrão.

3.2.2 Programas compartilhadores de arquivos

Á cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, indica que dentre milhares de programas disponíveis na Internet uma das categorias mais usadas é a dos que compartilham arquivos tais como músicas, filmes, fotos e até mesmo *softwares;* estes programas levam o nome de P2P (*peer to peer*) sendo a solução mais prática e popular aos usuários. Esta popularidade gerou o interesse de *hackers* que utilizam estes *softwares* como meio de disseminação de vírus.

Os riscos envolvendo este tipo de *software* além das ameaças a violação de direitos autorais são:

- *Malwares*: Quando se utiliza softwares P2P torna-se difícil a identificação da fonte do *download* e isso gera a incerteza de que se a mesma é ou não confiável. Esta incerteza é utilizada por hacker para inserção de códigos malicioso em arquivos a serem baixados, com o agravante de que alguns deles não necessitam nem de ser executados para que torne o computador cliente vulnerável.

- *Exposição a informações*: A má configuração de um software P2P pode expor voluntária ou involuntariamente, informações confidenciais do usuário. Este fator pode

expor informações financeiras, corporativas e pessoais a um utilizador mal-intencionado.

- *Facilitação a Ataques*: Praticamente todas as instalações de programas P2P necessitam de uma alteração, desbloqueio ou liberação de alguma porta no firewall, para que não a transferência dos arquivos não seja prejudicada. Alguns programas alteram estas configurações sem o consentimento do usuário. Estas alterações tornam o computador vulnerável a futuros ataques que por ventura possam utilizar as portas liberadas na configuração.

Os métodos preventivos para impedir ataques vinculados a programas P2P consistem em possuir um software de antivírus atualizado e bem configurado; manter o *firewall* ativo, evitando, assim, a exposição de porta; evitar a instalação de complementos que vem acoplados ao pacote instalador do programa P2P, pois podem conter *spywares*, evitar a exposição de informações pessoais, assim como não compartilhar diretórios importantes, por fim, utilizar servidores de renome, descartando assim servidores menos populares e inseguros.

4. SEGURANÇA NA INTERNET

Como todas as ambiguidades existentes, a Internet é um campo fértil para fraudes e quebras de segurança, afinal qual o tamanho dos riscos do mundo virtual? São dois mundos próximos e que se espelham a vida real e a virtual. Como andam juntas estão sujeitas a todos os tipos de violações, como fraudes e furtos.

Com o passar do tempo os *hackers* têm evoluído conhecimentos e com novas tecnologias, desenvolveram ferramentas com maior poder de dano, que faz com que a segurança também tenha que ser aprimorada com novas ferramentas, recursos e procedimentos.

4.1 Antivírus

São programas desenvolvidos para manter o computador ou dispositivo móvel seguro, protegendo-o contra ameaças. Eles têm por função impedir, detectar e remover programas que contenham códigos mal-intencionados.

Os vírus são adquiridos por diversos meios como, por exemplo, *pen drive*, *e-mail*, visita a *sites* ou *downloads* de arquivos infectados, entre outros. Estes têm a missão de furtar informações confidenciais, financeiras, causando danos a usuários domésticos e empresas.

Os antivírus foram evoluindo com o passar do tempo e com o avanço tecnológico e, hoje, se apresentam junto a um pacote de ferramentas complementares que podem variar de acordo com o tipo de licença adquirida (gratuita ou paga).

Á cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil instrui que para que se tenha um antivírus eficaz é necessário:

- Manter atualizações constantes de assinaturas e vacinas;

- Configurá-lo para averiguar automaticamente anexos de *e-mails* e arquivos baixados;

- Configurá-lo para averiguar automaticamente mídias externas tais como CD, DVD, *Pen drive*, cartões de memória;

- Configurá-lo para verificar todo tipo de extensão de arquivos.

É importante lembrar que nenhum antivírus garante 100% à segurança de um computador ou dispositivo contra explorações a vulnerabilidades nem que haverá invasões via *backdoor* que, por ventura, já estejam alojados.

4.2 Firewall

Firewall, baseado na cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, é um mecanismo de extrema importância para a segurança da informação em uma rede, seja ela privada ou doméstica. Este mecanismo tem como função verificar e filtrar informações oriundas da Internet ou de outra rede permitindo ou barrando a entrada ou saída dessas informações conforme configuração de regras e instruções.

Existem no mercado, dois tipos de *firewall* e sua aplicação varia de acordo com a necessidade do usuário ou empresa.

O *firewall* em forma de aplicação geralmente vem incluso no próprio sistema operacional ou em equipamentos que o trazem como complemento de segurança. Este é o caso dos roteadores domésticos, que permitem, por exemplo, a criação de listas contendo computadores conectados a ele, que serão impedidos de acessar a Internet.

Os *firewalls* em forma de *hardware* são equipamentos desenvolvidos única e exclusivamente com a finalidade de se tornar um guardião da rede e gerenciar pacotes destinados aos diversos equipamentos contidos nela. Essa solução é voltada ao meio corporativo, tornando o mecanismo dedicado e, assim mais eficiente.

O *firewall* funciona como uma barreira que impede que atacantes ou códigos maliciosos adentrem a rede causando danos ao usuário ou corporação. Uma de suas vantagens é a criação de logs para consulta de eventos ocorridos na rede o que permite a realização de análises para se saber sua origem assim, além do trabalho em conjunto com o antivírus aumentando o nível da segurança.

Como toda ferramenta, o *firewall* atuando sozinho não garante 100% da segurança, é importante ter em mente que uma base estruturada de segurança da

informação não pode fundar-se apenas um mecanismo e, sim em um elo trabalhando em conjunto.

4.3 Proxy

Segundo à cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, *Proxy* é o nome que recebe o servidor que faz o intermédio entre o usuário solicitante e o servidor requisitado.

O intuito é aumentar o desempenho dos acessos *web* armazenando uma cópia das páginas já acessadas e utilizadas com mais frequência. Quando o navegador realiza a requisição de uma página já acessada anteriormente ela é disponibilizada pelo servidor *proxy,* que, por sua vez, já possui este conteúdo armazenado em sua memória cache, encurtando o caminho e o tempo de se fazer novamente o acesso direto.

O Servidor *Proxy* também exerce papel importante na segurança dos acessos filtrando conteúdos que possam conter *softwares* mal-intencionados. Um *Proxy* mal configurado pode gerar riscos no que diz respeito a ataques, tornando anônimas algumas ações na Internet. Esse mecanismo é utilizado por corporações, em geral usuários comuns não utilizam *proxy* em seus acessos domésticos.

4.4 Backup

O conceito de *Backup,* conforme à cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, consiste na redundância de dados com foco na restauração em caso de perda dos dados originais decorrentes de exclusão, vírus ou perca destes dados em caso de invasão.

Um *backup* eficiente minimiza os impactos da perda e possibilita a restauração de dados e serviços dentro de um tempo tolerável de indisponibilidade e com o mínimo de desatualização das informações. Podem ser influenciados pela natureza dos dados, necessidade do negócio e infraestrutura disponível. Podem ser uma simples cópia de dados para um *pen drive* ou disco rígido externo no caso de usuários comuns

ou mais complexos, envolvendo equipamentos e rotinas definidas em casos corporativos.

A escolha dos dados a serem salvos varia de acordo com a política da corporação, sempre com foco nas informações que possuem maior valor para a organização e no prejuízo gerado, caso esses dados se percam. É importante manter salvos somente dados confiáveis, protegendo-os de qualquer tipo de vírus ou algum outro tipo de ameaça.

A periodicidade com que o procedimento de *backup* é executado também varia de acordo com a frequência com que é alterado esse fator parte de um alinhamento entre a tecnologia da informação e a organização.

Segundo à cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil os dispositivos mais utilizados para realização de *backups* são:

- Mídia ótica;

- Fitas magnéticas;

- Discos rígidos.

As topologias de backup podem ser:

- Centralizado;

- Descentralizado;

- Armazenamento em nuvem.

Visando evitar a sobrecarga da rede pelo fato de existirem menos usuários ativos e quantidade reduzida de arquivos abertos, os *backups* geralmente são realizados no período noturno.

O local de armazenamento das mídias deve ser climatizado e com acesso restrito a pessoas não autorizadas. Um dos fatores que aumenta a segurança é manter o local de armazenamento em locais diferentes ou até mesmo contratar uma empresa conceituada que preste esse tipo de serviço.

Dados com informações sigilosas requerem uma segurança diferenciada dentro de uma rotina de *backup*, e caso deve se aplicar tipos de algoritmos de criptografia visando manter a segurança destes dados.

4.4.1 Seleção de Dados

As cópias a serem salvas devem conter somente arquivos de confiança dos usuários, não contendo vírus ou qualquer outro tipo de ameaça. Arquivos de sistemas que façam parte da instalação dos *softwares* contidos no computador não devem fazer parte do *backup* devido ao risco que podem trazer. Esses arquivos podem ser alterados ou substituídos por arquivos contaminados com códigos mal-intencionados que podem trazer riscos a rede e ao computador em uma possível restauração. *Softwares* e sistemas de computador devem seguir o processo de instalação por mídia fornecida pelos fabricantes.

4.4.2 Mídia de Backup

A escolha da mídia de armazenamento do *backup* é de extrema importância pois define a vida útil que a cópia dos dados terá. O tipo de mídia a ser utilizado define a capacidade e a segurança do *backup* cada uma com suas particularidades e limitações.

A forma mais simples para a realização do *backup* é através de mídias físicas fazendo uso de CDs e DVDs. Esse tipo de mídia se torna o mais utilizado por usuários domésticos por terem um baixo custo. Entretanto, possuem a desvantagem de pouco espaço para armazenamento, sendo necessária a utilização de um número maior de mídias caso o volume do *backup* seja grande. Outra desvantagem desse tipo de mídia é o desgaste da vida útil com o passar do tempo e a fragilidade a danos tais como riscos e quebras.

Outra maneira bastante utilizada para a realização de *backups* é através de mídias externas, são elas, disco rígido externo ou *pen drive*. Trata-se de dispositivos mais versáteis para se armazenar uma cópia de segurança de arquivos importantes uma vantagem é o fácil manuseio, que garante ao usuário facilidade no deslocamento

uma vez que pode ser levado para qualquer lugar. Esses tipos de dispositivos podem guardar uma grande quantidade de informação dependendo de sua capacidade de armazenamento.

Atualmente, existem diversos meios que permitem o armazenamento de arquivos em nuvem, termo este utilizado para o armazenamento *on-line*, fazendo se desnecessário, o uso de qualquer tipo de mídia física. Existem planos gratuitos para usuários simples, com limitações de espaço e planos corporativos para empresas que necessitam de grande espaço para armazenamento; neste caso, cobrados pela empresa prestadora do serviço.

Backups realizados na nuvem permitem não somente a maior segurança dos dados como também a facilidade de acesso de qualquer outro computador ou dispositivo. O armazenamento em nuvem permite a realização da cópia de segurança tanto de computadores quanto de dispositivos móveis (*tablets*, *smatphones*).

4.4.3 Local de Armazenamento

Para definição do local de armazenamento das mídias de *backup* deve-se segundo à cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, considerar três pontos primordiais:

- Pedidos simples de restauração de usuários;
- Grandes recuperações de dados;
- Resgates de arquivos com pouca probabilidade de uso.

Independentemente de qual seja a necessidade, o *backup* deve atender às regras bases da segurança da informação e estar disponível seguindo uma política predefinida pela empresa que gerencia o recurso.

As cópias devem ser mantidas em local condicionado e seguro, de modo que somente pessoas autorizadas possam ter acesso, atendendo às diretrizes do controle de acesso físico.

Existem empresas que se utilizam de locais diferentes para o armazenamento, ou seja, guardam a cópia em outra localidade, o que é bastante útil em casos de catástrofes que por consequência causem danos à estrutura da informação.

5. REDE SOCIAL: CONCEITO

O conceito de redes sociais, transmitido por Marteleto (2001, p.72) indica a ideia de compartilhamento de valores e interesses que, para promover o fortalecimento da rede, dependem do compartilhamento da informação e do conhecimento.

Em resumo, são páginas da Internet em que pessoas e organizações se encontram, criam redes de amigos e grupos com interesses comuns, tais como música, trabalho, meio ambiente ou simplesmente com o intuito de conhecer gente nova.

Marteleto (2001, p.72) sobre as redes sociais, afirma:

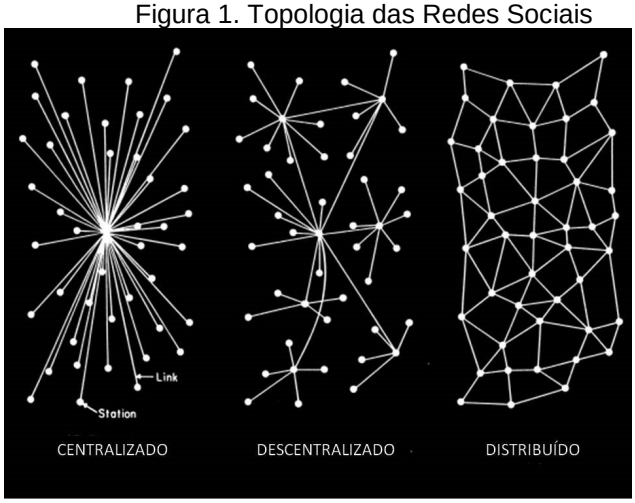
> [...]um conjunto de participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados [...].

Uma rede social tem como base o indivíduo e a sua necessidade de socialização. Desta maneira, pode se dizer que as redes sociais sempre existiram, tomaram forma, ganharam potencial e se expandiram após o surgimento da Internet.

A necessidade de socialização vem se aprimorando com o passar do tempo, e não é por acaso que esse evento é tão impactante na sociedade contemporânea. De fato, as redes sociais chegaram para ficar e não podem ser consideradas como “moda passageira”, pois representam uma grande revolução na ótica da sociedade de como conviver, conhecer pessoas e de compartilhar momentos.

As redes sociais podem ser definidas entre três topologias distintas. A ilustração apresentada na Figura 1, foi criada por Paul Baran, no ano 1964 e demonstra graficamente essas topologias para um melhor entendimento.

Figura 1. Topologia das Redes Sociais



Fonte: Baran (1964)

Um grande problema encontrado em todas às topologias é relacionado ao conhecimento das conexões estabelecidas.

Este tipo de problema está diretamente ligado as atitudes tomadas pelos membros nesse meio e na forma com que expõem a intimidade e informações particulares, tornando-os presas fáceis para criminosos virtuais.

A falta de moderação no conteúdo publicado influi diretamente no aumento desses riscos. É necessário, também, atenção a *links* vinculados a códigos mal-intencionados que são camuflados em fotos e outros arquivos que redirecionam o usuário das redes a *sites* maliciosos.

5.1 Distinção entre mídia social e rede social.

Palavras utilizadas para definir nomenclaturas no mundo da Internet surgem todos os dias e torna-se difícil saber a diferença entre esses termos que por muitas vezes parecem definir a mesma coisa. É o que acontece com os termos “mídia social” e “rede social” que apesar de parecidos são independentes.

Tratando-se de “rede social”, Kaplan e Michael (2010) referem-se sobre basicamente a criação de relacionamentos com pessoas compartilhando objetivos e valores comuns. Isso se faz tanto conectado à Internet quanto no dia a dia nos relacionamentos interpessoais. Levando o termo para o mundo conectado, *sites* de

relacionamentos têm como objetivo facilitar e viabilizar, de forma rápida essas conexões.

Kaplan e Michael (2010) definem as “mídias sociais” como um grupo de aplicações para a Internet construídas com base nos fundamentos ideológicos e tecnológicos da *web*, e que permitem a criação e a troca do conteúdo gerado pelo utilizador.

Em resumo, mídia social é o ambiente virtual para compartilhamento de informações, cada uma com suas particularidades e características.

5.2 Tipos de mídias sociais

Existem diversos tipos de mídias sociais, sendo as redes sociais as mais conhecidas. Os dois termos chegam a causar alguma confusão em relação ao conceito e chegam a ser considerados equivalentes, porém, são distintos. As redes sociais fazem parte do grupo de mídias sociais. As redes sociais, como o próprio nome sugere, destinam-se à criação de relacionamentos em forma de rede gerando interação interpessoal. Por sua vez, mídia social tem o foco no compartilhamento de conteúdo. Outras ferramentas também compõem este universo entre elas pode se citar: ferramentas de editoração, *blogs*, *livecastings*, jogos etc.

5.2.1 Facebook (facebook.com)

Segundo o Grupo de Estudos sobre Adições Tecnológicas (2012), esta mídia social foi criada em 2004, inicialmente, era utilizado somente por estudantes da Universidade de Harvard expandindo sua fama para muitas outras universidades. É uma rede gratuita e tem sua receita proveniente de publicidade, incluindo *banners* e grupos patrocinados. O acesso é liberado mediante a criação de uma conta por parte do usuário. Suas versões estão disponíveis também para dispositivos móveis. Tem como objetivo principal a interação e o relacionamento entre pessoas por meio de chats, grupos, eventos e aplicativos que permitem esta interação.

Outro recurso disponibilizado pelo Facebook é a de parceria com outras mídias sociais. Esse recurso consiste na integração entre os dados de cadastro e acesso por

meio do próprio Facebook, ou seja, não é necessário o preenchimento de um formulário ou criação de nova conta para o acesso a essas mídias, uma vez que o vínculo é estabelecido, sua página inicial é exibida na Figura 2.

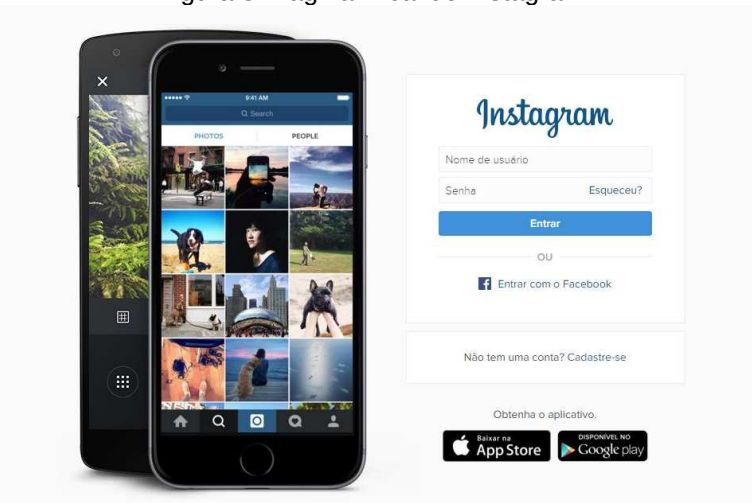
Figura 2. Página inicial do Facebook

Fonte: Facebook, 2016

5.2.2 Instagram (instagram.com)

Segundo o Grupo de Estudos sobre Adições Tecnológicas (2012), a mais famosa rede social *on-line* para compartilhamento de fotos e vídeos é exibida na Figura 3. Foi criada em outubro de 2010 e disponibilizada, inicialmente, como aplicativo para *smartphones*. Após, foi expandida a versão *web* do aplicativo que permite apenas a visualização das fotos e vídeos postados pelos usuários. O aplicativo permite a interação com outras mídias sociais, estabelecendo vínculo entre as postagens e marcações de pessoas.

Figura 3. Página inical do Instagram



Fonte: Instagram,2016

5.2.3 Twitter (twitter.com)

A Figura 4 exibe a tela inicial do *twitter*, conforme o Grupo de Estudos sobre Adições Tecnológicas (2012), à mídia social que se destaca na categoria de *microblogging* permite aos usuários enviar e receber atualizações pessoais com texto que contenham até 140 caracteres. Os textos são conhecidos como *tweets* e podem ser recebidos e enviados pelo *site*, ou pelo aplicativo para *smartphone*. As atualizações são exibidas e enviadas a seguidores através da linha do tempo do usuário e salvas em ordem cronológica. Além das mensagens o *twitter* permitiu recentemente o compartilhamento de fotos e vídeos através de *links* inseridos à página.

Figura 4. Página inicial do *Twitter*

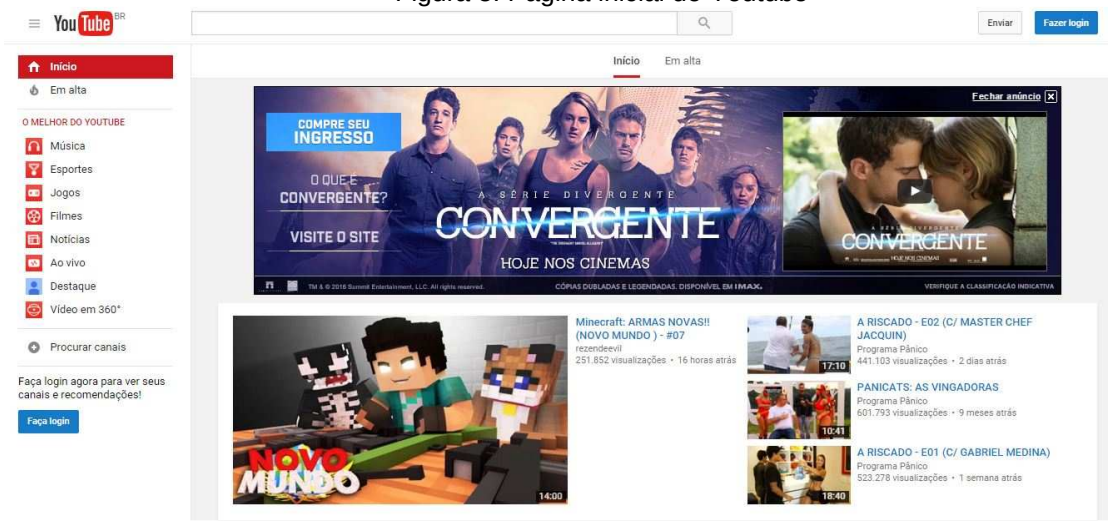
Fonte: Twitter, 2016

5.2.4 Youtube (youtube.com)

Na Figura 5 é demonstrada a página inicial do Youtube, segundo o Grupo de Estudos sobre Adições Tecnológicas (2012), à rede social tem foco em compartilhamento e acessos a vídeos. A ideia parte do mesmo princípio que a TV, em que existem diversos canais disponíveis, a diferença está em que ao contrário da TV, os canais são criados pelos próprios usuários que os utilizam para compartilhar vídeos dos mais variados temas.

Os vídeos ficam disponíveis para qualquer pessoa e permitem ou não a inserção de comentários, conforme parâmetros definidos pelos proprietários. O destaque de alguns vídeos caseiros, musicais ou eventos em que exista algum talento ou diferencial podem levar as pessoas à fama, sendo consideras “celebridades instantâneas”.

Figura 5. Página inicial do Youtube



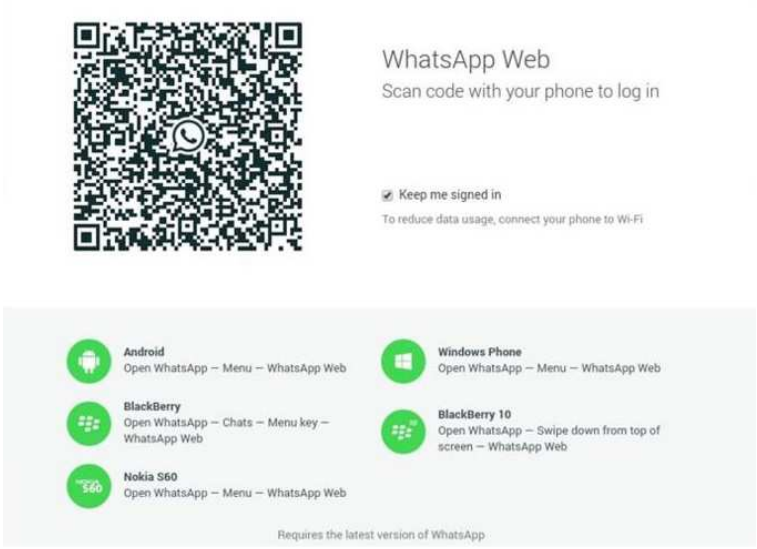
Fonte: YouTube, 2016

5.2.5 WhatsApp Messenger (web.whatsapp.com)

A Figura 6 exibe a página inicial do whatsapp em sua versão *web*. Segundo o Grupo de Estudos sobre Adições Tecnológicas (2012), o Aplicativo multi-plataforma de mensagens instantâneas e chamadas de voz para *smartphones* com suporte a sistemas operativos *IOs*, *android*, *Windows*, *BlackBarry* e Nokia. Além da mensagem de texto o aplicativo compartilha também fotos, vídeos, arquivos e áudios entre os usuários. O grande destaque do aplicativo se dá à associação dos contatos já salvos na agenda de contatos, ou seja, o usuário não necessita de um cadastro para a

utilização, uma vez que o próprio aplicativo associa os contatos da agenda com usuários que também possuam o aplicativo. Permite também, a criação de grupos de contatos criados com algum propósito ou assunto em comum. O WhatsApp é visto como o sucessor do SMS, por ser mais prático e econômico e também por não ter custo no envio das mensagens. Recentemente ganhou a versão para utilização *web*, em que a autenticação se dá através de um *QR Code* exibido na tela inicial, trazendo mobilidade e a não necessidade de se estar com o *smartphone* em mãos.

Figura 6. Página inicial do WhatsApp *Web*



Fonte: WhatsApp, 2016

O universo das mídias sociais vai além das citadas acima as quais são as mais utilizadas atualmente, cada uma com seu objetivo e particularidades diferentes.

5.3 Reputação e valores da sociedade digital

Recuero (2009) transmite a ideia de que a sociedade digital é um meio vinculado a ativos intangíveis, ou seja, é um universo em que não se tem somente o bem corpóreo e físico; sendo assim, existem valores a serem preservados, tais como o conhecimento e a reputação.

É necessário ter ciência da importância das opiniões que são expressas através das redes sociais, pois essas influenciam de maneira quase imperceptível na vida dos usuários refletindo, de maneira positiva ou negativa na vida real destes.

Alguns fatores são de extrema relevância para à identificação do perfil de um usuário da rede, postagens, conteúdo, termos utilizados são itens que facilitam esse processo que hoje em dia é muito utilizado por empresas, como por exemplo, para requisito de classificação ou não de um funcionário.

As redes sociais abrem espaço para que se observe através delas a vida privada de seus usuários. Dessa forma pode se analisar lugares frequentados, tipos de vestimentas, fotos vulgares com poses que exaltem a sensualidade, consumo excessivo de álcool ou substâncias que podem comprometer o rendimento do colaborador na empresa, preconceitos, agressões e julgamentos, colocando, assim, o membro em uma linha de análise negativa.

Outro fator importante ao se inserir em uma rede social é avaliar o termo de uso e privacidade. Esses termos são apresentados ao usuário de início e inviabiliza a criação do perfil caso haja discordância por parte do usuário.

Segundo Recuero (2009), um dos valores a serem construídos dentro de uma rede social é a reputação e isso é oriundo das impressões emitidas pelo indivíduo. Esse fator, em grande parte, não depende somente dos atos do indivíduo, mas, sim, do membro que vê, avalia e julga o ato.

Recuero (2009), remete ao pensamento de uma responsabilidade imposta a todos os usuários e não a determinados grupos ou pessoas, afirmando que a reputação pode ser criada através de um controle sobre as impressões deixadas, e que a reputação é extremamente influenciada pelas ações, porém não única e exclusivamente por elas.

Segundo à cartilha de segurança para internet Cert.Br (2006) do Comitê Gestor da Internet no Brasil, chama à atenção para os cuidados com os dados pessoais, uma vez que essas informações podem ser utilizadas de maneira ilícita por terceiros.

O ponto primordial é manter restritos os números dos documentos tais como: RG, CPF, CNH etc. Possivelmente, *sites* de compras *online* vão exigir essas numerações, pois fazem parte do processo. Nesse caso é necessária atenção sobre a segurança e a reputação do site escolhido.

O fornecimento do nome completo, assim como nomes de pais, filhos ou de outros membros da família também é um risco, uma vez que esses dados podem ser utilizados para afirmar nomes conhecidos em ligações ou em possíveis fraudes. Da mesma maneira, é contraindicado marcar fotos ou indicar laços familiares nas redes sociais, este tipo de informação privilegiaria alguém mal-intencionado, no caso de um trote ou até mesmo no intuito de buscar informações pessoais do usuário.

É necessária cautela no uso das informações pessoais na Internet. O maior trunfo é se manter seguro e restringir ao máximo as informações que possam ser úteis às pessoas mal-intencionadas. É preciso bom senso na hora da divulgação dos dados e divulgá-los somente quando e a quem for necessário, conhecendo sempre o destino e a forma com que estas informações serão utilizadas.

5.4 Ataques em redes sociais

À cartilha de segurança para internet Cert.Br (2006, p.29) do Comitê Gestor da Internet no Brasil, define engenharia social:

> [...]O termo é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

As bases da engenharia social estão firmadas na manipulação de pessoas com o intuito de conseguir informações pessoais. Nesse caso, o atacante utiliza o relacionamento humano (habilidades sociais e psicológicas) para conseguir comprometer o sistema, perfil ou a rede do alvo.

Geralmente os atacantes induzem a vítima a executar algum tipo de software malicioso que abre o acesso a senhas bancárias e informações pessoais.

Durante o ataque, o criminoso se mostra íntegro e confiável, podendo fornecer credenciais, *e-mails* ou utilizando de um falso cargo em uma empresa para sustentar sua identidade. Através de perguntas ele, pode ser capaz de reunir dados para concluir a invasão.

O elo mais fraco da segurança da informação consiste no fator humano, sendo assim é extremamente nulo o investimento em equipamentos e sistemas se isso não estiver alinhado a conscientização do pessoal.

À cartilha de segurança para internet Cert.Br (2006, p.6) do Comitê Gestor da Internet no Brasil, demonstra alguns exemplos de engenharia social:

> [..]Exemplo 1: você recebe uma mensagem e-mail, onde o remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado a mensagem. A execução deste aplicativo apresenta uma tela idêntica aquela que você utiliza para ter acesso a conta bancaria, aguardando que você digite sua senha. Na verdade, este aplicativo este preparado para furtar sua senha de acesso a conta bancaria e enviá-la para o atacante.
> Exemplo 2: você recebe uma mensagem de e-mail, dizendo que seu computador está infectado por um vírus. A mensagem sugere que você instale uma ferramenta disponível em um site da Internet, para eliminar o vírus de seu computador. A real função desta ferramenta não é eliminar um vírus, mas sim permitir que alguém tenha acesso ao seu computador e a todos os dados nele armazenados.
> Exemplo 3: algum desconhecido liga para a sua casa e diz ser do suporte técnico do seu provedor. Nesta ligação ele diz que sua conexão com a Internet está apresentando algum problema e, então, pede sua senha para corrigi-lo. Caso você entregue sua senha, este suposto técnico poderá realizar uma infinidade de atividades maliciosas, utilizando a sua conta de acesso à Internet e, portanto, relacionando tais atividades ao seu nome. (Cert.Br – Pág. 6) [...]

5.4.1 Técnicas de invasão

Com a popularização da Internet e suas ferramentas golpistas virtuais desenvolveram técnicas que utilizam os meios de comunicação *online* tais como as mídias sociais, *e-mail* e *links* para colherem informações ou manipular usuários desatentos.

Existe uma evolução no que diz respeito a *malware* e esse fator anda lado a lado com a engenharia social. Há pouco tempo, qualquer tipo de infecção virtual passaria a ser óbvia ao usuário pela simples forma em que era apresentada. Os ícones, mensagens, imagens eram bem descarados e ressaltavam por muitas vezes o criador do malefício.

Atualmente, os códigos maliciosos são camuflados em ferramentas idênticas às que o usuário utiliza normalmente e fica oculto até o momento em que seja necessário agir.

5.4.2 Social - Phishing

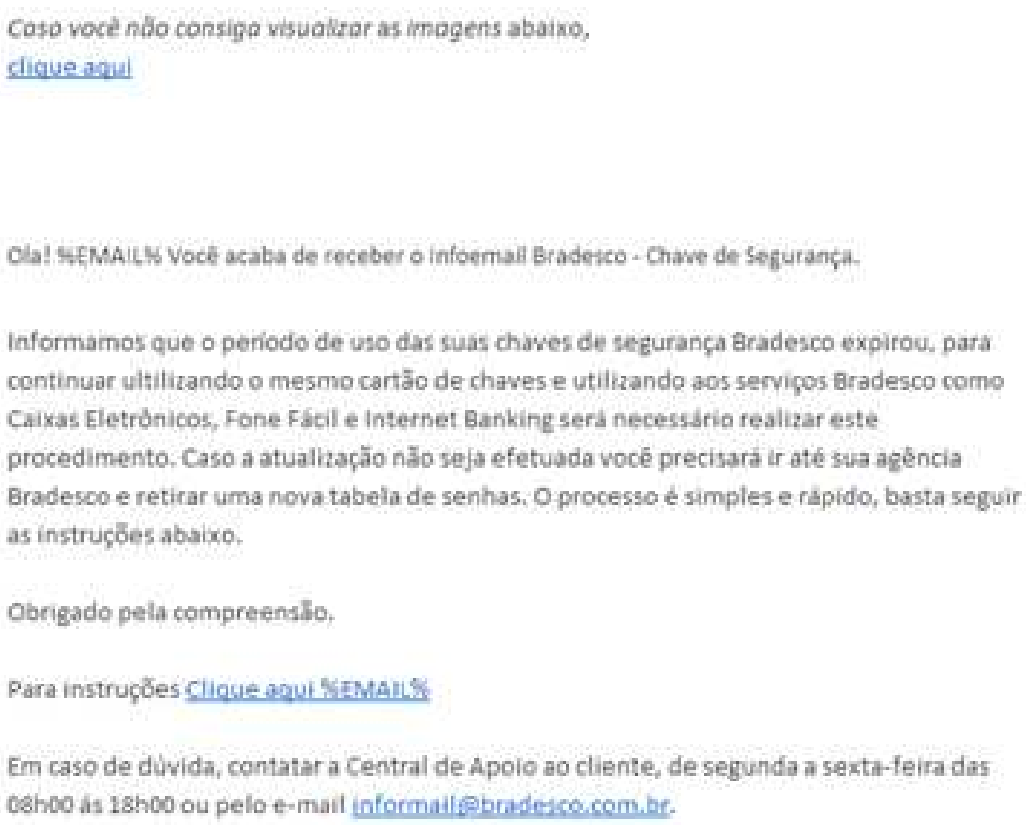
À cartilha de segurança para internet Cert.Br (2006, p.35) do Comitê Gestor da Internet no Brasil, define o termo *phishing*:

> Phishing, também conhecido como phishing scam ou phishing / scam, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.

O social *Phishing* utiliza a combinação de vários fatores para que o ataque tenha sucesso, desde um evento cotidiano até fatores relacionados ao sentimento humano, e podem abordar duas situações diferentes: ou são enviados através de mala direta para um grande número de vítimas, ou utiliza uma situação específica e é direcionada a determinada pessoa, contendo informações reais colhidas anteriormente para que o ataque tivesse embasamento.

A Figura 7 demonstra o método utilizado pelo atacante para tentar passar credibilidade a vítima, inserindo um e-mail corporativo para contato. Ao clicar no *link* é realizado um redirecionamento a uma página falsa que solicitará número de agência, conta e senha. Desta maneira, as informações pessoais são expostas ao atacante.

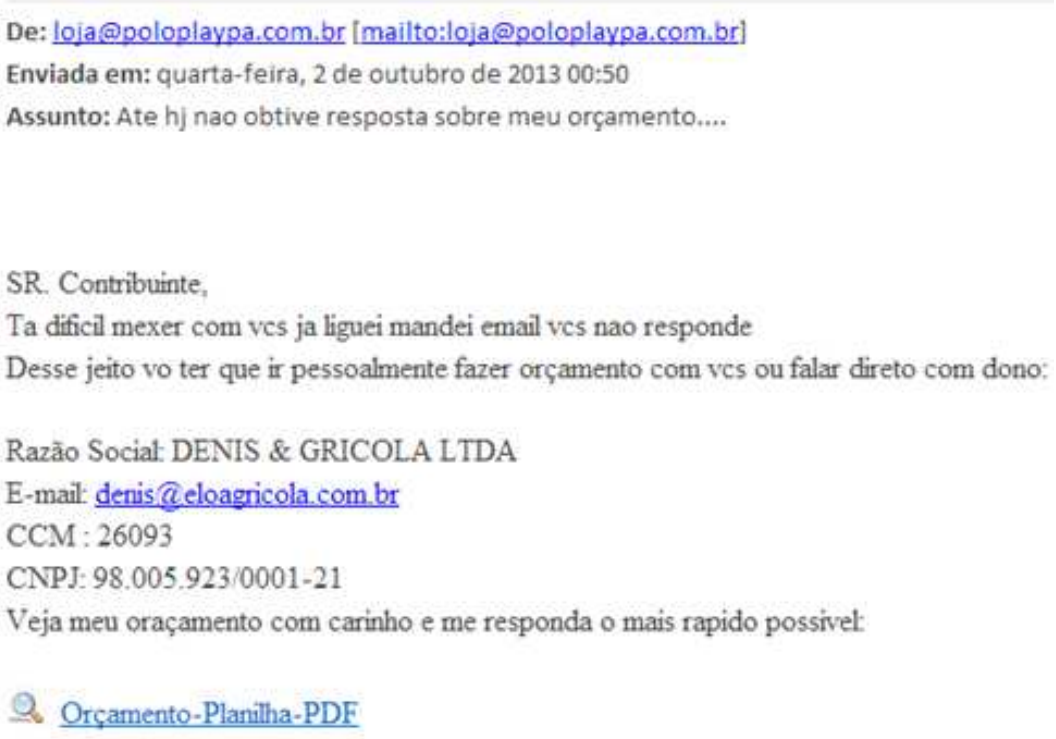
Figura 7 – Exemplo de *e-mail phishing*



Fonte: Autoria própria

É exibido na Figura 8 o exemplo em que o atacante utiliza o fator humano relacionado ao medo para promover o ataque, alegando uma possível conversa pessoal com o proprietário do negócio caso, o orçamento não seja enviado.

Figura 8 – Exemplo prático de Social Phishing


De: loja@poloplaypa.com.br [mailto:loja@poloplaypa.com.br]
Enviada em: quarta-feira, 2 de outubro de 2013 00:50
Assunto: Ate hj nao obtive resposta sobre meu orçamento....

SR. Contribuinte,
Ta dificil mexer com vcs ja liguei mandei email vcs nao responde
Desse jeito vo ter que ir pessoalmente fazer orçamento com vcs ou falar direto com dono:

Razão Social: DENIS & GRICOLA LTDA
E-mail: denis@eloagricola.com.br
CCM : 26093
CNPJ: 98.005.923/0001-21
Veja meu oraçamento com carinho e me responda o mais rapido possivel:

Orçamento-Planilha-PDF

Fonte: Autoria própria

À cartilha de segurança para internet Cert.Br (2006, p.38) do Comitê Gestor da Internet no Brasil, recomenda algumas maneiras de como ficar livre deste tipo de ameaça:

> [...]• leia atentamente a mensagem. Normalmente, ela conterá diversos erros gramaticais e de ortografia;
> • os fraudadores utilizam técnicas para ofuscar o real *link* para o arquivo malicioso, apresentando o que parece ser um *link* relacionado `a instituição mencionada na mensagem. Ao passar o cursor do mouse sobre o *link*, será possível ver o real endereço do arquivo malicioso na barra de status do programa leitor de *e-mails*, ou *browser*, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este link será diferente do apresentado na mensagem;
> • qualquer extensão pode ser utilizada nos nomes dos arquivos maliciosos, mas fique particularmente atento aos arquivos com extensões “.exe”, “.zip” e “.scr.”, pois estas são as mais utilizadas. Outras extensões frequentemente utilizadas por fraudadores são “.com”, “.rar” e “.dll”;
> • fique atento as mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa;
> • acesse a página da instituição que supostamente enviou a mensagem, e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, você vai observar que não e política da instituição enviar *e-mails* para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados [...].

5.4.3 Cyberstalking

Segundo Truzzi (2012), o termo *cyberstalking* consiste no uso das redes tecnológicas com o intuito de perseguir e ameaçar o indivíduo.

Utilizando meios psicológicos e mentais de forma inconveniente e opressora, gerando um assédio que pode resultar em danos muito grandes. Os ataques podem ser baseados em demonstrações de afeto em demasia e causam desconforto, ultrapassando, assim, os limites de uma convivência saudável.

Diversas ações fazem parte do conjunto de intromissão à vida alheia. A maioria dos *cyberstalkers* têm um comportamento padrão iniciando uma colheita de informações relevantes sobre seu alvo. Essas reuniões de informações podem vir de conhecidos, parentes, visitas aos perfis em redes sociais seguindo os passos da pessoa a fim de monitorar seus atos.

Truzzi (2012) afirma, que os sentimentos que motivam um *cyberstalker* são geralmente o ciúme, inveja e a baixa tolerância a frustrações, e, em sua grande parte, são compostos por pessoas que já mantiveram algum tipo de relacionamento com a vítima ou têm interesse nesse sentido, aproveitando-se da intimidade proporcionada pelo relacionamento e de rastros e interações deixados nas redes sociais que possam ser úteis para chantagens e ameaças.

Recuero (2009, p.30) define estas evidências deixadas nas redes sociais:

> [...] Essas interações, na Internet, são percebidas graças à possibilidade de manter os rastros sociais dos indivíduos, que permanecem ali. Um comentário em um weblog, por exemplo, permanece ali até que alguém o delete ou o weblog saia do ar. Assim acontece com a maior parte das interações na mediação do computador. Essas interações são, de certo modo, fadadas a permanecer no ciberespaço, permitindo ao pesquisador a percepção das trocas sociais mesmo distante, no tempo e no espaço, de onde foram realizadas [...].

Sem dúvida o anonimato proporcionado pela Internet é de grande ajuda para que esse tipo de ataque seja concretizado e encoraja essa ação por parte do atacante, todavia é possível reduzir as chances restringindo os acessos a essas informações utilizando a proteção de arquivos, fotos, vídeos, e não compartilhando estes itens em grande escala com pessoas desconhecidas ou que tenham pouco contato.

À cartilha de segurança para internet Cert.Br (2006, p.33) do Comitê Gestor da Internet no Brasil, indica o bom senso para evitar ataques por meio de engenharia social.

> [...] Em casos de engenharia social o bom senso é essencial. Fique atento para qualquer abordagem, seja via telefone, seja através de um e-mail, onde uma pessoa (em muitos casos falando em nome de uma instituição) solicita informações (principalmente confidenciais) a seu respeito [...].

5.5 Ataques baseados em localização geográfica

Redes sociais baseadas em localização são serviços móveis que crescem em larga escala e incentivam o compartilhamento da localização atual com amigos e seguidores. Entretanto, um fator esquecido pelos utilizadores desse tipo de serviço é o risco e a exposição gerada por ele no que diz respeito a lugares frequentados e a ausência da residência com detalhes referentes ao horário e distância.

Esses dados publicados sem nenhum critério podem ser de grande valia para assaltantes e sequestradores e colocar em risco o usuário e seus familiares. As coordenadas geográficas existentes nestas localizações devem ser utilizadas com cautela e levando em consideração os riscos que esse tipo de atividade pode gerar.

Quando um usuário realiza um *check-in*, ou publicações de fotos com coordenadas geográficas, automaticamente esse dispositivo está indicando o local onde está e estas informações podem ser úteis para um *cyberstalker* ou até mesmo a um ladrão que aproveita dessa ausência para realizar furtos.

O fascículo sobre redes sociais da cartilha de segurança para internet Cert.Br (2015) do Comitê Gestor da Internet no Brasil, sugere alguns critérios para segurança nas redes sociais baseadas em geolocalização:

> [...] Cuidado ao divulgar fotos e vídeos, pois ao observar onde eles foram gerados pode ser possível deduzir a sua localização não divulgue, sem autorização, imagens em que outras pessoas apareçam
> Não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência
> Ao usar redes sociais baseadas em geolocalização, procure fazer *check-in* apenas em locais movimentados e, de preferência, ao sair do local
> Cuidado ao confirmar sua presença em eventos públicos organizados via redes sociais [...].

5.6 Crimes e redes sociais

Assim como os crimes tradicionais, os crimes realizados na Internet podem ter diversas formas e ocorrer a qualquer momento. Os criminosos cibernéticos utilizam métodos diferentes com base nos objetivos a serem alcançados, e a expansão das redes sociais e seus recursos possibilitam o desenvolvimento de um sistema que facilita o anonimato.

Pozzebon (2016) cita em artigo que os criminosos virtuais utilizam na maioria das vezes, a inocência das vítimas para realizarem suas ações e acreditar que as configurações de segurança das redes sociais são infalíveis é um erro. Na Internet, seja usando um computador seja outro dispositivo nada é plenamente seguro e a possibilidade de invasão é sempre presente e está ao alcance de qualquer pessoa. Portanto não é necessário ser um especialista no assunto para praticar atos ilícitos.

Os sites de relacionamento estão entre os vilões da Internet, neles existem muitos perfis falsos criados para realização de ações de má fé. Esses farsantes utilizam habilidades na coação, e, no jogo de palavras, são envolventes e dizem exatamente o que a vítima quer ouvir, criando, assim, um vínculo e conquistando total confiança, assim conseguindo roubar, extorquir, ameaçar, chantagear e até cometer crimes sexuais, abaixo são exibidos exemplos de crimes e situações ocorridas neste tipo de ambiente:

*Roubos de identidade***:** Os piratas virtuais enganam os internautas e se apoderam de suas informações pessoais para fazer compras on-line ou realizar transferências financeiras indevidamente. Segundo o IPDI (Instituto de Peritos em Tecnologias Digitais e Telecomunicações), pessoas que usam a informática para roubar identidades podem responder por estelionato, furto mediante fraude, intercepção de dados, quebra de sigilo bancário e formação de quadrilha.

Pedofilia: Internautas criam sites ou fornecem conteúdo (imagens e vídeos) relacionado ao abuso sexual infantil;

Calúnia e difamação: Divulgação de informações muitas vezes mentirosas que podem prejudicar a reputação da vítima. Esses crimes tornaram-se mais comuns com a popularização do site de relacionamentos Orkut;

Ameaça: Ameaçar uma pessoa envia e-mail ou posts, por exemplo, afirmando que ela será vítima de algum mal;

Discriminação: Divulgação de informações relacionadas ao preconceito de raça, cor, etnia, religião ou procedência nacional. Também se tornou mais comum com a popularização do Orkut;

Espionagem industrial: Transferência de informações sigilosas de uma empresa para o concorrente. A tecnologia facilita esse tipo de ação, já que um funcionário pode copiar em um palmtop ou *memory stick*, por exemplo o equivalente a quilos de documentos.

Existem atualmente delegacias e órgãos judiciais que tratam especificamente de crimes virtuais, entre eles:

São Paulo: DIG-DEIC – 4ª Delegacia – Delitos praticados por Meios Eletrônicos. Presta atendimento presencial, por telefone e via Web. Endereço: Av. Zack Narchi, 152, Carandiru – São Paulo (SP) Fone: (11) 2224-0721 ou 2221 – 7030. Para denunciar qualquer espécie de delito virtual anonimamente, utilize o e-mail: 4dp.dig.deic@policiacivil.sp.gov.br;

Rio de Janeiro: Delegacia de Repressão aos Crimes de Informática (DRCI). Rua Professor Clementino Fraga, nº 77 (2º andar), Cidade Nova (prédio da 6ª DP), Rio de Janeiro/RJ (CEP: 20230-250), telefones (0xx21) 2332-8192, 2332-8188 e 23328191 e e-mails drci@pcivil.rj.gov.br;

Espírito Santo: Delegacia de Repressão a Crimes Eletrônicos (DRCE) – Av. Nossa Senhora da Penha, 2290, Bairro Santa Luiza, Vitória/ES (CEP: 29045-403), telefone (0xx27) 3137-2607 e e-mail drce@pc.es.gov.br;

Minas Gerais: DEICC – Delegacia Especializada de Investigações de Crimes Cibernéticos – Av. Nossa Senhora de Fátima, 2855 – Bairro Carlos Prates – CEP: 30.710-020, Telefone (33) 3212-3002, e-mail dercifelab.di@pc.mg.gov.br;

Paraná: Nuciber da Polícia Civil do Paraná – Rua José Loureiro, 376, 1º andar – sala 1 – Centro – 80010-000 – Curitiba-PR, Tel:(41) 3323-9448 – Fax: (41) 3323-9448, e-mail cibercrimes@pc.pr.gov.br;

Rio Grande do Sul: Delegacia de Repressão aos Crimes Informáticos (DRCI/DEIC) – Av. Cristiano Fischer, 1440, Bairro Jardim do Salso em Porto Alegre, na mesma sede do DEIC. O telefone de contato é (0xx51) 3288-9815, e-mail drci@pc.rs.gov.br;

Distrito Federal: Divisão de Repressão aos Crimes de Alta Tecnologia (DICAT) – Não atende diretamente ao público, neste caso a vítima pode procurar a delegacia mais próxima para efetuar registro de ocorrência, A DICAT é uma Divisão especializada em crimes tecnológicos que tem como atribuição assessorar as demais unidades da Polícia Civil do Distrito Federal, o telefone é (0xx61) 3462-9533 e e-mail dicat@pcdf.df.gov.br;

Pará: Delegacia de Repressão aos Crimes Tecnológicos – Travessa Vileta, n° 1.100, Pedreira. Belém-PA. CEP: 66.085-710, com telefone de contato (91) 4006-8103, e-mail drct@policiacivil.pa.gov.br. A DRCT é vinculada à Diretoria de Repressão ao Crime Organizado.

6. AMBIENTE DE TESTE PRÁTICO – ESTUDO SOBRE A CAPTURA DE CREDENCIAIS EM REDES SOCIAIS.

As redes sociais permitem que seus utilizadores forneçam diversas informações pessoais, tais como, interesses profissionais, contatos e atividades diárias. Essas informações podem ser de grande interesse a pessoas mal-intencionadas na rede que têm por objetivo o furto e o mal-uso destas, com o intuito de obter lucros financeiros ou simplesmente prejudicar uma pessoa ou organização no que diz respeito à reputação e autoria de ações.

O presente estudo objetiva-se a demonstração de um ataque *Man in The Middle*, tipicamente utilizado por *hackers* que utilizam ferramentas como *phishing* ou *malwares* para induzir a vítima a *sites* clonados, colocando se assim no meio da conexão com o intuito de interceptar as informações inseridas.

O gráfico exibido na Figura 9 demonstra um levantamento realizado pelos laboratórios da Breach Security Inc. e numeram ataques realizados de acordo com a instituição alvo, é notável o maior percentual relacionado à *web* 2.0 sendo esses atribuídos, em grande, parte às redes sociais.

Figura 9. Classificação de Ataques Por Organização

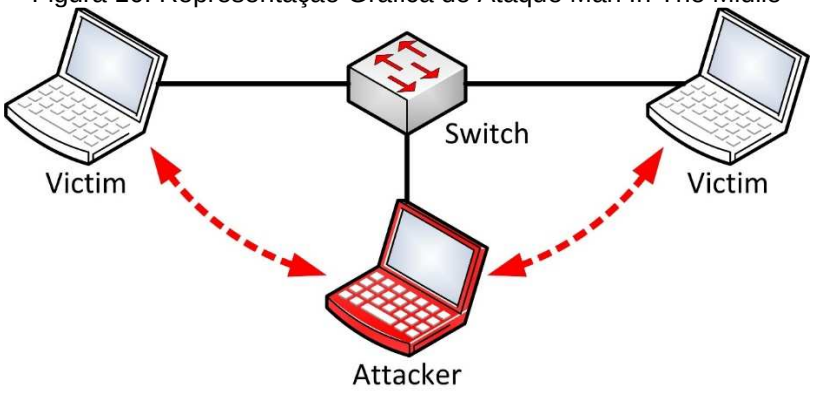
Fonte: Breach Security Inc. (2009)

O facilitador desses ataques é o próprio usuário da rede social que pode estar interessado tanto em contatos pessoais quanto profissionais, tornando-o, assim, suscetível a aceitação de convites e mensagens enviadas por pessoas desconhecidas.

A exploração de um ARP *spoofing* é o meio mais eficaz de se estabelecer um elo entre a comunicação cliente/servidor e interceptar requisições e informações compartilhadas entre ambas, gerando acesso a dados confidenciais, senhas e dados de tráfego. A ilustração deste tipo de ataque é exibida na Figura 10.

O método a ser utilizado se aplica somente à rede interna, sejam elas empresariais, residenciais ou de livre acesso como é o caso de estabelecimentos comerciais que liberam ao cliente o acesso à Internet.

Figura 10: Representação Gráfica de Ataque Man In The Midlle



Fonte: Weber (2013)

Este tipo de rede funciona com base em dois endereços de identificação: o MAC *Address* e o IP. O endereço MAC é o endereço físico contido em todo dispositivo de rede, sendo único e exclusivo para cada um destes dispositivos. A rede envia pacotes de dados divididos em frames e os cabeçalhos de identificação desses *frames* retornam o endereço MAC para a identificação entre clientes e servidores durante a troca de informações.

O IP (Internet Protocol) é o endereço lógico atribuído à placa de rede independentemente da operação, seja por meios estáticos ou dinâmicos.

Os dois endereços trabalham juntos para o envio, fragmentação e reconhecimento dos frames na rede e para o repasse à porta de destino mapeadas anteriormente e identificadas pelo MAC e IP.

Ferreira (2008) em artigo escrito para o Universo Online afirma, que a sigla DNS significa *Domain Server Name* (Sistema de Nomes de Domínios). Trata-se de uma base de dados distribuída que armazena informações de mapeamento entre nomes de domínios e informações referentes a eles. Também exerce a função de ser um protocolo de comunicação entre cliente e servidor. O DNS define o processo de interrogação e atualização da base de dados. Os mecanismos de replicação da informação entre servidores e a organização da informação na base de dados, sendo assim responsável pelo funcionamento de outros serviços relacionados à Internet.

A necessidade do uso do DNS vem do fato de que na Internet, os computadores são identificados por IP (*Internet Protocol*), e não por nomes. Desta maneira quando se digita um *site* no navegador, na realidade está-se realizando a requisição a um IP vinculado a este nome e é função do DNS fazer a procura deste endereço nos servidores, e retornar à página em questão.

O ataque realizado neste estudo mostrará o redirecionamento do servidor DNS para o *site* clonado, ou seja, a partir da alteração realizada na tabela ARP faremos com que o DNS desvie as rotas das requisições ao site do Facebook para o computador do atacante criado especificamente para isso, retornando, assim, a página clone para captura das credenciais.

O ARP *(Address Resolution Protocol)* é um protocolo de resolução de nomes dentro da rede. Tem como função atrelar um endereço lógico (IP) ao endereço físico (MAC). Quando um pacote chega da Internet o *gateway* fará a leitura do cabeçalho de requisição, fará a busca do MAC responsável e o encaminhamento para o IP de destino.

Será realizado um *spoofing* na rede confundindo o cache do protocolo ARP e fazendo com que o cliente e servidor redirecionem os pacotes trafegados à máquina do atacante.

Dessa maneira, todas as requisições ao site do Facebook, serão automaticamente desviadas, fazendo com que o usuário confie suas credenciais acreditando estar utilizando o site original.

A demonstração realizada a partir de agora exibe a situação de um ataque MITM, em que o invasor se posiciona entre duas partes que tentam se comunicar, interceptando dados de trafego se passando por uma das partes envolvidas.

Ataques MITM são uma grande ameaça para a segurança da informação, pois cede ao atacante a possibilidade de capturar e manipular informações em tempo real, como conversas, senhas e dados importantes.

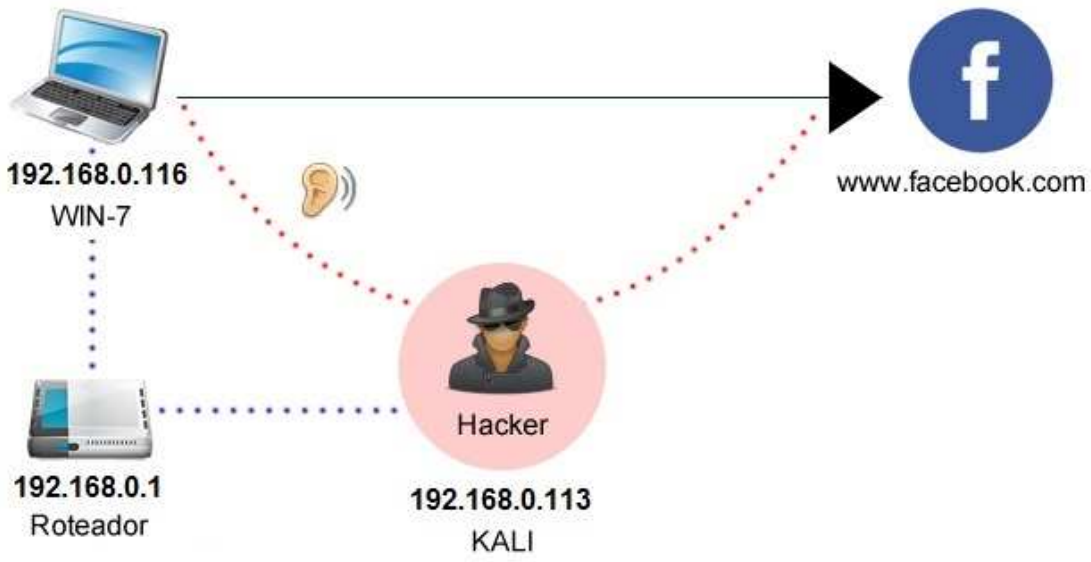
Foram criados para a execução do trabalho o ambiente contendo a seguinte estrutura:

Máquina Atacante: Será o interceptador da comunicação, ou seja, será o host inserido entre o trafego de dados e receberá os dados desviados da rota original.
Sistema Operacional: Kali Linux 2.0
Identificação Lógica: 192.168.0.113
Roteador: Receberá as requisições da máquina alvo e através das configurações realizadas para o ataque, fará a busca do endereço www.facebook.com na máquina atacante, retornando assim uma página clonada para a máquina alvo, ao invés da original.
Modelo: TL-WR740N
Identificação Lógica: 192.168.0.1

Máquina Alvo: Receberá os pacotes da página clonada retornados pelo roteador, e realizará a inserção das credenciais a serem capturadas.
Sistema Operacional: Windows 7 Professional
Identificação Lógica: 192.168.0.116

Na prática a interceptação dos dados funcionará conforme o escopo exibido na Figura 11:

Figura11: Escopo do ataque MITM



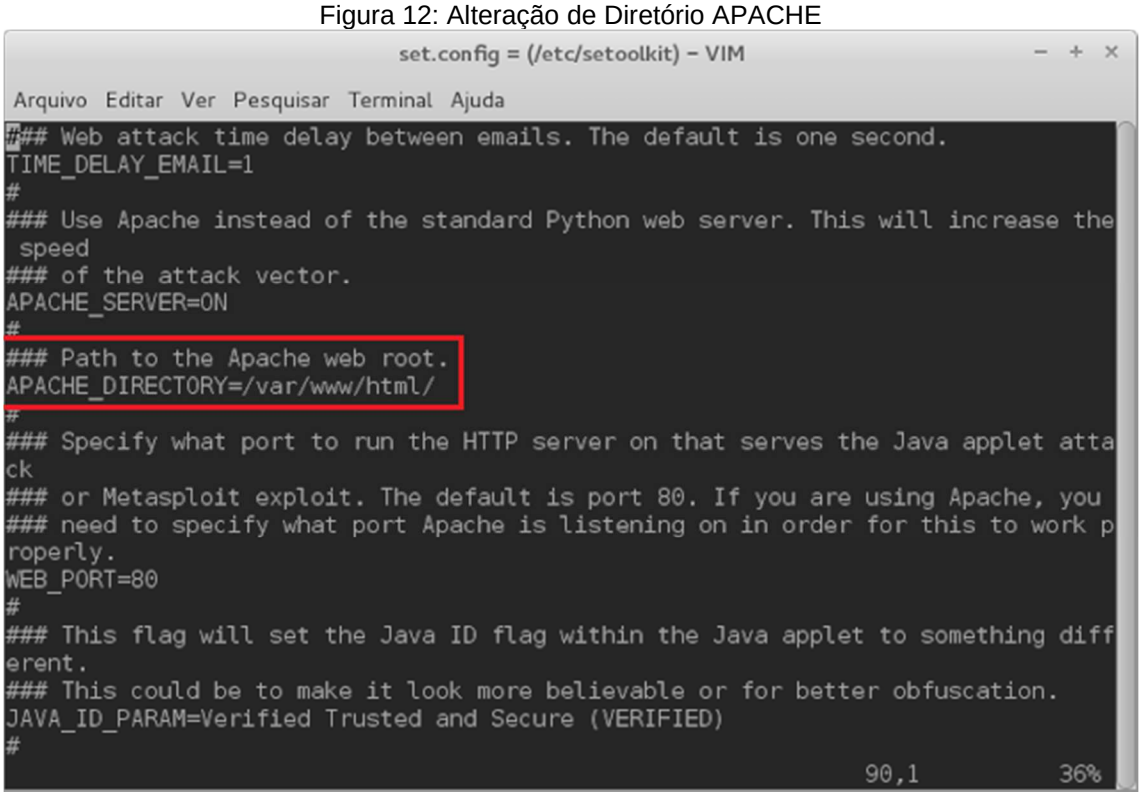
Fonte: Autoria própria

Utilizando SET (Social Engineer Toolkit), que tem por objetivo auxiliar testes de penetração e trazer consciência para ataques que envolvem engenharia social. Disponibiliza um pacote de ferramentas com foco nos alvos relacionados a fraqueza humana, credibilidade e curiosidade. A ferramenta utiliza *e-mails*, *sites* falsos e outros vetores para que a vítima seja enganada e assim comprometer informações sensíveis.

A Figura 12 demonstra a edição do arquivo /etc/setoolkit/set.config alterando o diretório do root do apache, pois por padrão o SET grava os *sites* clonados no diretório /var/www/ isto é realizado através dos comandos:

Iniciando o apache: # service apache2 start
Editando o diretório root: # vim /etc/settoolkit/set.config
Alterar o parâmetro apache_directory para o valor /var/www/HTML

Figura 12: Alteração de Diretório APACHE

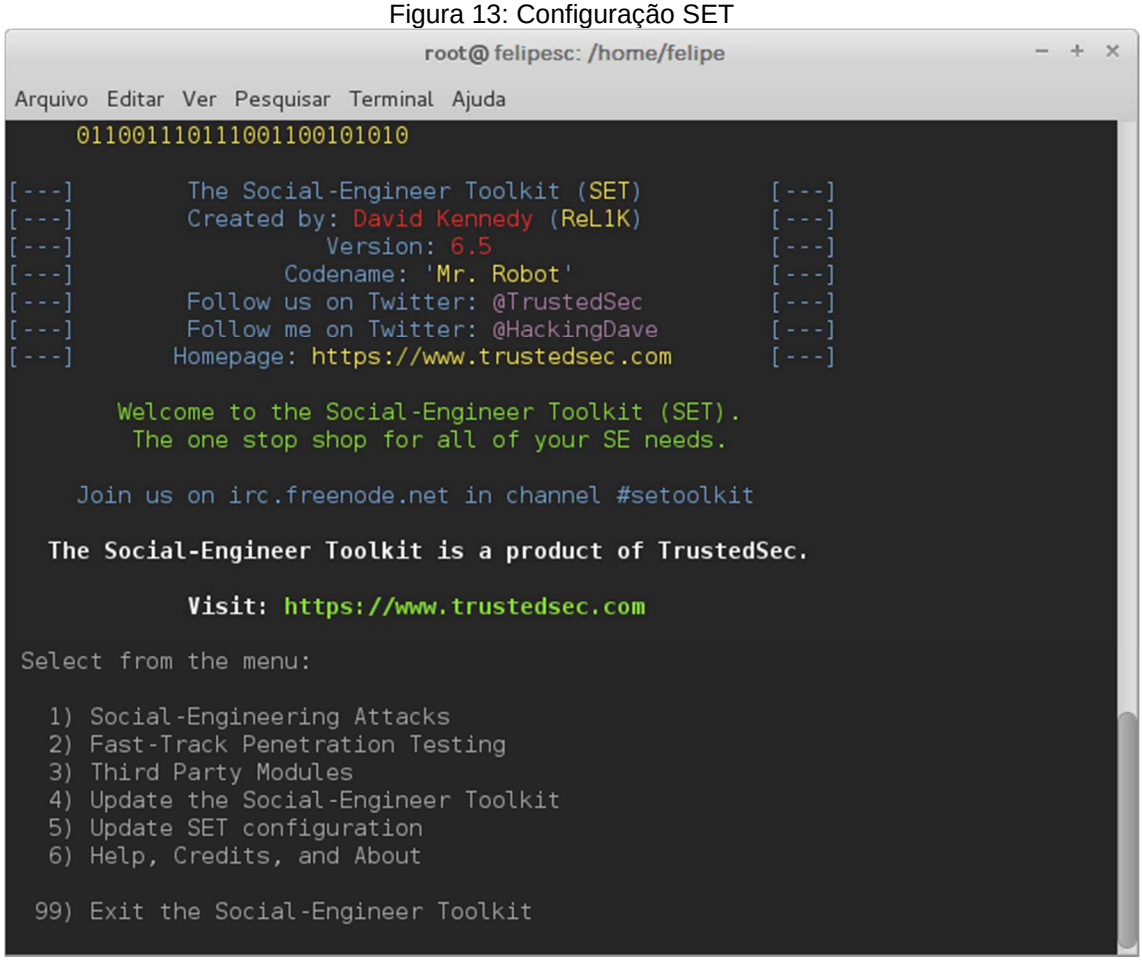


Fonte: Autoria própria

A Figura 13 ilustra a utilização do SET através do comando #setoolkit que retorna a imagem exibida, em que serão aplicadas as seguintes configurações:

- Selecionada opção 1 “*Social-engineering Attacks*”
- Selecionada opção 2 “*Website Attack Vectors*”
- Selecionada opção 3 “*Credential Harvester Attack Method*”
- Selecionada opção 2 “*Site Cloner*”

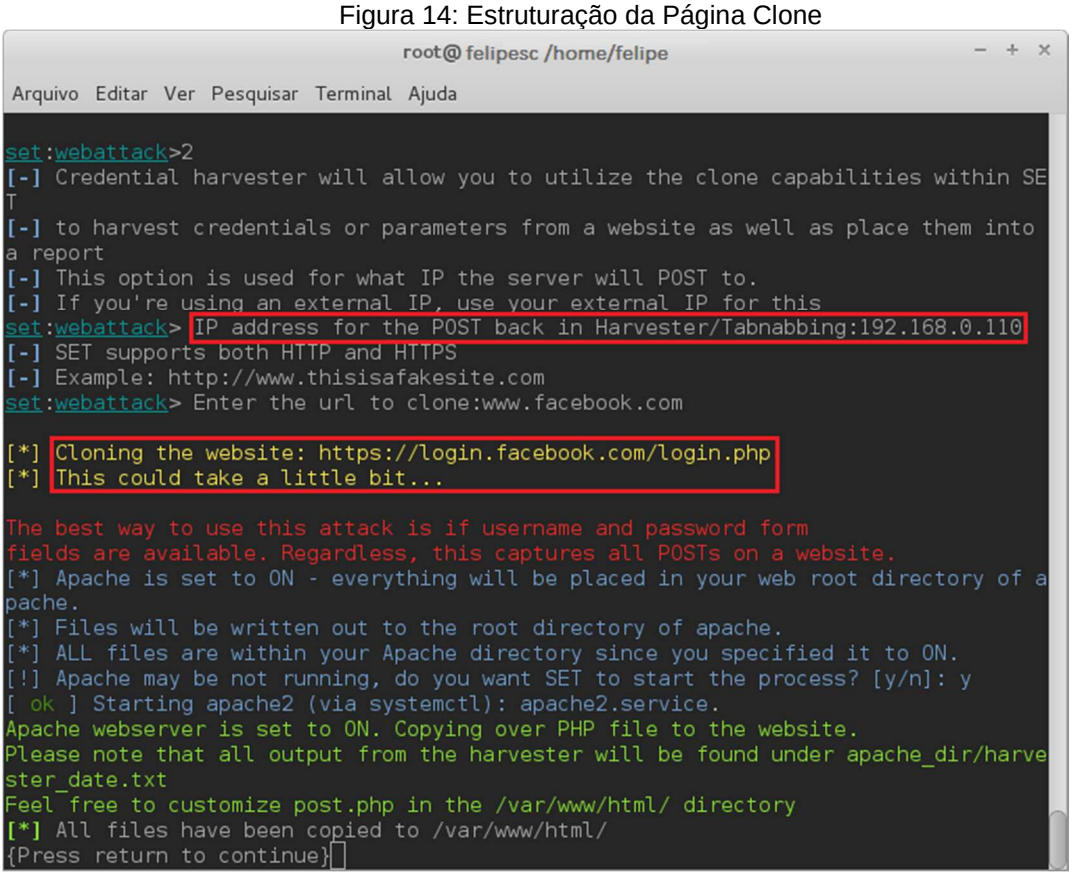
Figura 13: Configuração SET



Fonte: Autoria própria

É visto na Figura 14 o passo realizado para definição da página clone por meio da alteração do endereço IP do micro que fará o papel do servidor e que receberá os dados do ataque. A gravação do *site* clone será salva na pasta /var/www/html.

Figura 14: Estruturação da Página Clone



Fonte: Autoria própria

A Figura 15 mostra a validação das alterações que foram efetuadas com sucesso. Ao digitar *localhost* na barra de endereços do navegador, com as definições ativas a página definida como clone deverá ser exibida.

Figura 15: Validação da Página Clone

Fonte: Autoria própria

Definidas as alterações de pasta e do arquivo em que ficarão salvas as informações capturadas no ataque, assim como o clone do *site* foi necessário também a edição do arquivo /etc/ettercap/éter.dns para a inserção das seguintes linhas:

Acessando e editando o arquivo pelo comando: #vim /etc/ettercap/etter.dns

facebook.com A 192.168.0.113
m.facebook.com A 192.168.0.113
*.facebook.com A 192.168.0.113
www.facebook.com PTR 192.168.0.113
https://www.facebook.com A 192.168.0.0.113

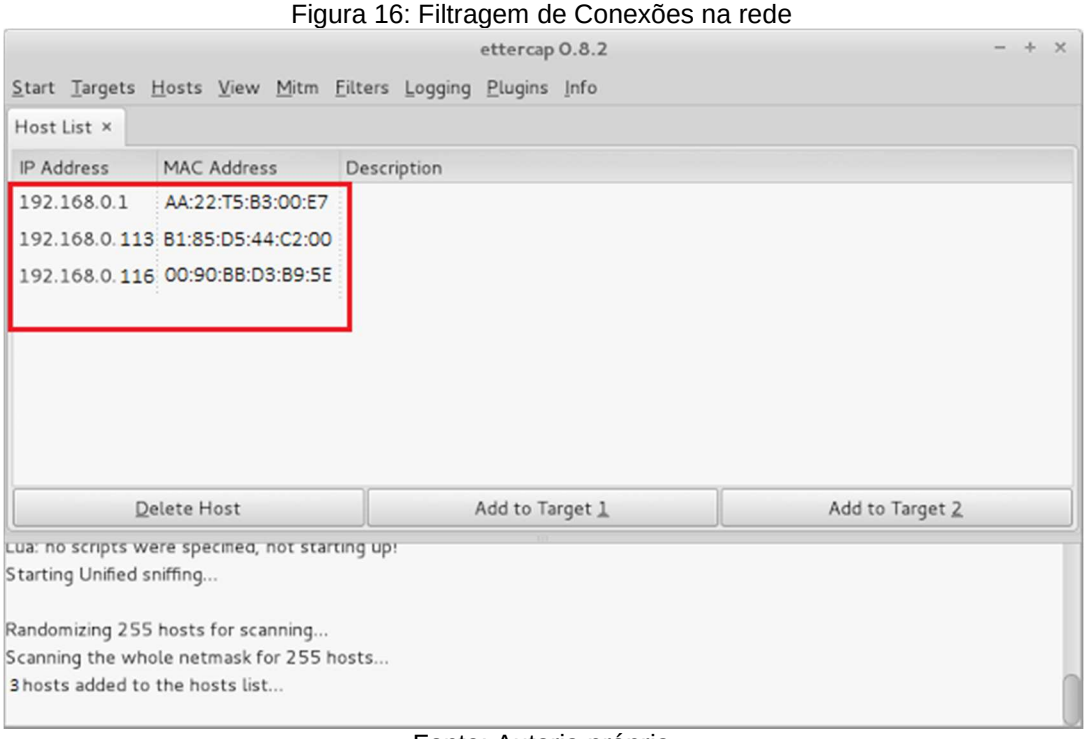
Esse passo tem como objetivo fazer com que o DNS se confunda e através deste parâmetro e redirecione o tráfego enviado ao *site* do Facebook para a máquina atacante.

O próximo passo executado é a abertura do Ettercap, que é um programa classificado como *sniffer*, pois realiza a captura do tráfego de dados em uma rede local, possibilitando, assim, a captura de senhas digitadas por usuários desta rede.

Na aba *Sniff* foi selecionada a opção "*Unified Sniff*"
Na aba *Host*, selecionada a opção "*Scan for hosts*"
Novamente na aba "*hosts*" selecionada a opção "*Host List*"

A Figura 16 demonstra as informações relacionadas aos computadores e dispositivos que fazem parte desta rede, realizadas através de uma filtragem dos endereços conectados:

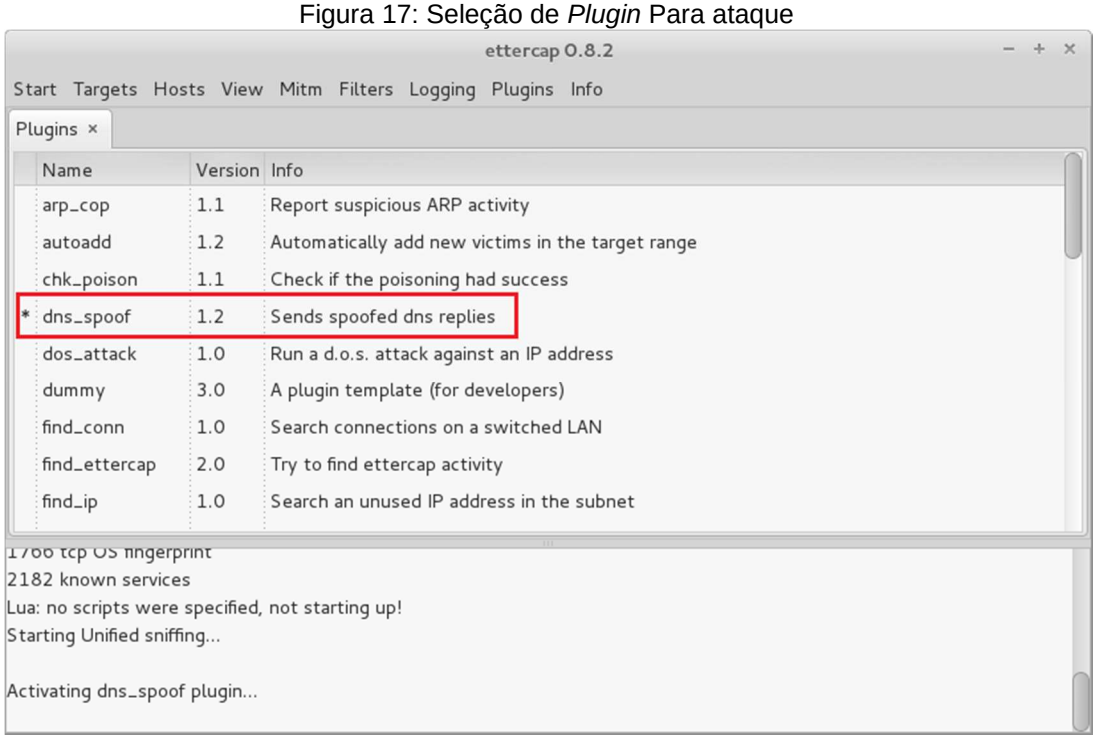
Figura 16: Filtragem de Conexões na rede



Fonte: Autoria própria

A Figura 17 exibe a seleção do *plugin* a ser utilizado após a seleção do *gateway* e do endereço IP do host escolhido, para que tenha o tráfego de dados capturado.

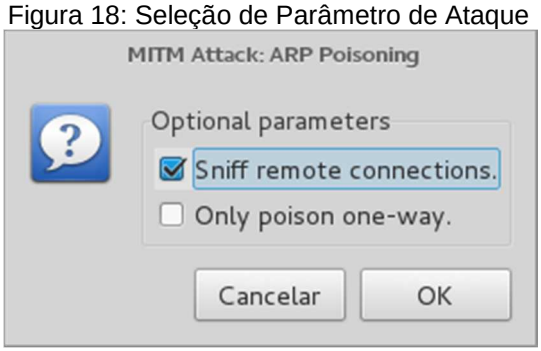
Figura 17: Seleção de *Plugin* Para ataque



Fonte: Autoria própria

Sendo assim, pode se ver na Figura 18 a seleção do "*Sniff remote connections*" a ser aplicado na captura.

Figura 18: Seleção de Parâmetro de Ataque

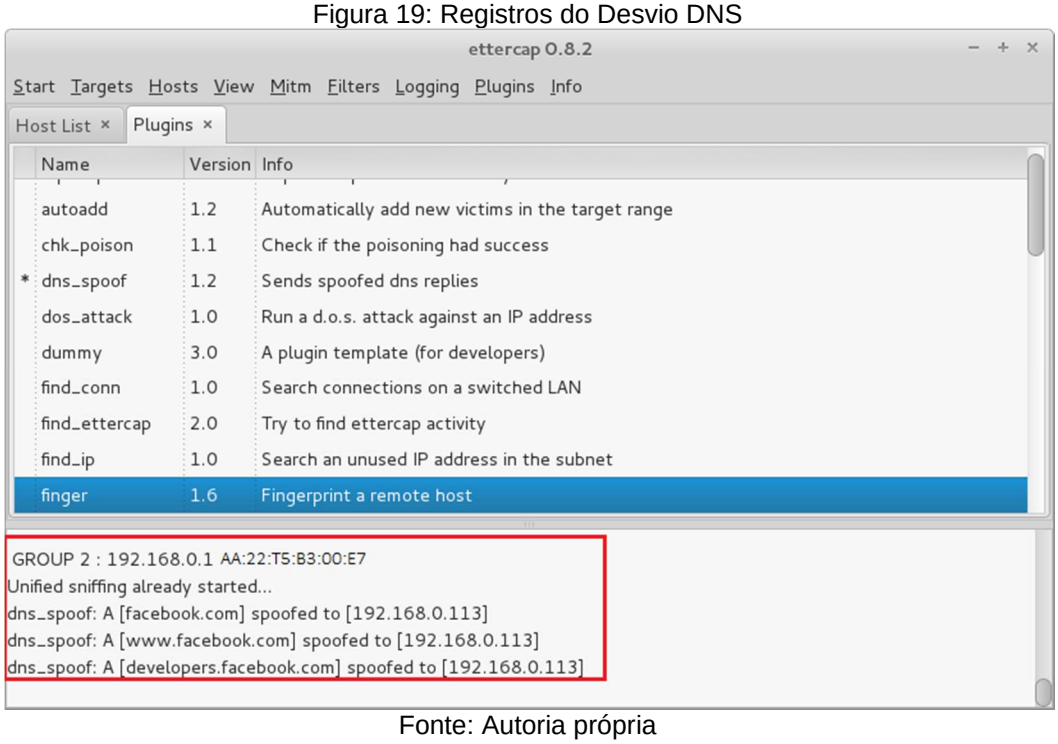


Fonte: Autoria própria

Deixando o protocolo ARP da rede confuso esse passa a atender aos nomes de domínio vinculados a máquina atacante em vez dos DNS padrões, que levariam o usuário a página original. Sendo assim, quando o próximo usuário do micro 192.168.0.116 realizar o acesso a página www.facebook.com a rota será desviada, fazendo com que a máquina atacante (192.168.0.113) funcione como o servidor retornando a ele a página clonada anteriormente.

A figura 19 apresenta os registros capturados pelo Ettercap deixando claro que o *plugin* DNS *spoof* desviou o acesso ao Facebook para o IP 192.168.0.113.

Figura 19: Registros do Desvio DNS



Fonte: Autoria própria

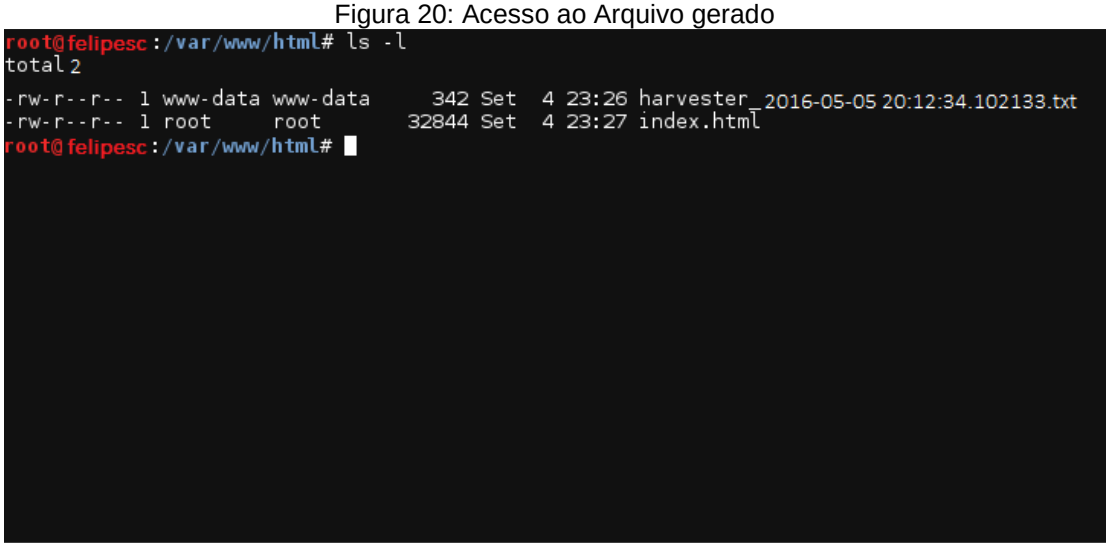
A figura 20 exibe o procedimento de acesso ao arquivo chamado “harvest_2016-05-05 20:12:34.102133.txt”, que é gerado no diretório do apache definido anteriormente para ser salvo em /etc/var/www/html:

Exibindo o arquivo:

#cd /var/www/html

#ls –l

Figura 20: Acesso ao Arquivo gerado



Fonte: Autoria própria

6.1 Resultados Obtidos

É demonstrado na Figura 21 os dados de captura ao final do processo, notam-se que as credenciais de acesso ao site do Facebook foram inseridas ao arquivo, possibilitando, assim, o acesso ao atacante.

Figura 21: Exibição de dados Capturados

Fonte: Autoria própria

O ataque apresentado neste exemplo prático ocorre na tentativa de comunicação da vítima com alguma entidade financeira, *sites* de compras e redes sociais.

Existem fatores que facilitam a interceptação de dados pelo atacante tornando possível, assim, o ataque, alguns destes fatores são:

- Brechas na criptografia;
- Códigos maliciosos em *sites*;
- *Phishing* enviado via *e-mail*.

Para que se evite um ataque MITM é necessário além da atenção com relação a engenharia social, medidas relacionadas aos equipamentos e conexões.

Manter roteadores, servidores e *switches* com *firmwares* sempre atualizados é uma medida essencial para prevenir ataques desse tipo, além da preocupação com a segurança na definição de senhas desses dispositivos.

É necessário, também, usar técnicas que utilizem criptografia de alto nível na comunicação entre cliente e servidor, reforçando assim a segurança na comunicação de ponta a ponta.

A utilização de *plug-ins* no navegador a fim de identificar conexões duvidosas também é outro meio de se manter imune aos ataques

É importante dizer que nenhum tipo de ferramenta ou configuração é confiável em sua totalidade e que o bom senso na hora de se conectar a alguma rede livre é essencial.

7. CONCLUSÃO

Realizando a análise dos assuntos dispostos e atividades desenvolvidas neste trabalho, percebem-se que as redes sociais existem a partir do momento em que grupos de pessoas possuem e possam compartilhar interesses e objetivos em comum, e que esse fator vai além das mídias digitais dispostas na Internet. Os meios dispostos pela grande rede permitem e oferecem ferramentas e mídias para facilitar essa conexão em tempo real e absoluto por intermédio de dispositivos móveis e *smartphones*, porém é importante atentar-se quanto à segurança envolvida neste setor.

Ficou claro que por se tratar de mídias utilizadas na Internet existem fatores a serem levados em consideração em seu uso, que remetem a segurança da informação. A demonstração de métodos eficazes para que se mantenham os dados dos usuários protegidos como, por exemplo, a utilização de um software de antivírus ativo e atualizado, a utilização de *firewall*, entre outras ferramentas demonstradas com o intuito de assegurar a integridade e disponibilidade dos dados, evitando, assim, que esses sejam modificados por algum código mal-intencionado ou invasor.

As redes sociais se tornaram uma febre mundial desde seu surgimento, e o número de utilizadores cresce diariamente, assim como a quantidade e a diversidade das informações compartilhadas neste meio. Ao levantar-se a questão dos riscos relacionados à privacidade do compartilhamento público de informações, ficou evidente a intenção de instruir cautela aos usuários, no que diz respeito ao compartilhamento da localização evitando assim ataques baseados neste tipo de informação.

Adicionalmente é levantado o alerta sobre os valores existentes na sociedade digital e os cuidados que deve se ter para que as redes sociais não afetem diretamente a vida real, no que se refere a reputação e as consequências de publicações compartilhadas.

Exemplos cotidianos de ataques a redes sociais são expostos de maneira a conscientizar sobre as falhas que levam a ocorrência destes ataques, assim como a descrição de cada um e seus respectivos métodos de prevenção.

Por fim chega-se a conclusão de que existem inúmeras vantagens na utilização da Internet como meio de interação, e socialização através das mídias sociais que dispõem além do entretenimento a busca de informações e o estreitamento de relações, e demonstra-se que o principal desafio está em manter a consciência em sua utilização, com relação ao conteúdo recebido e enviado à rede, tendo em mente as consequências que estes fatores podem acarretar.

Espera-se que esta monografia sirva como apoio para a criação de um nível de consciência mais elevado, visando a melhor utilização das informações que são dispostas nas redes sociais, e o propósito incluído em cada uma delas, aproveitando assim dos benefícios proporcionados por este ambiente de maneira segura.

REFERÊNCIAS

ACADEMIA DO MARKETING. **Redes sociais horizontais e redes sociais verticais:** Qual a diferença? Disponível em: http://www.academiadomarketing.com.br/redes-sociais-horizontais-e-verticais/. Acesso em 07 nov. 2015.

AHAVA SOLUÇÕES EM INFORMÁTICA. **Os perigos dos programas P2P.** Disponível em: http://www.ahavainformatica.com.br/2014/02/os-perigos-dos-programas-p2p.html. Acesso em 13 nov. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – **ISO/IEC NBR 27002**: Tecnologia da informação: Técnicas de segurança: Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005. 120p.

BARAN, Paul. **On distributed communications**: Introduction to distributed communications networks. In: Memorandum RM-3420-PR, August 1964. Santa Mônica: The Rand Corporation, 1964.

CARTILHA DE SEGURANÇA PARA INTERNET; Versão 3.1 (CGIB) – São Paulo: COMITÊ GESTOR DA INTERNET NO BRASIL, 2006.

DEPENDÊNCIA DE TECNOLOGIA. **Redes Sociais mais populares.** Disponível em: http://dependenciadetecnologia.org/a-familia-e-a-tecnologia/conhecendo-melhor-os-jogos-e-as-redes-sociais/redes-sociais-mais-populares/. Acesso em 10 jul. 2015.

DANTAS, Marcus Leal. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

DUARTE, Fábio.; FREI, Klaus.; QUANDT, Carlos.; SOUZA, Queila. **O Tempo Das Redes.** Perspectiva Editora – 2008.

PORTAL G1. **Crimes praticados pela Internet são cada vez mais comuns na região.** Disponível em http://g1.globo.com/sao-paulo/sorocaba-jundiai/noticia/2012/03/crimes-praticados-pela-internet-sao-cada-vez-mais-comuns-na-regiao.html. Acesso em 14 abr. 2016.

MARTELETO, Regina Maria. **Análise de redes sociais:** aplicação nos estudos de transferência da informação. Ciência da Informação. Brasília - 2001.

MICHAELHAENLEIN. **Users of the world, unite:** The challenges and opportunities of Social Media. KAPLAN, Andreas; HAENLEIN, Michael. Disponível em: http://michaelhaenlein.eu/Publications/Kaplan,%20Andreas%20-%20Users%20of%20the%20world,%20unite.pdf. Acesso em 02 mar. 2016.

MICROSOFT. **O que é software antivírus?** Disponível em: https://www.microsoft.com/pt-br/security/resources/antivirus-whatis.aspx. Acesso em 05 out. 2015.

OFICIAL DA NET. **Quais são os crimes virtuais mais comuns?** Disponível em: https://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns. Acesso em 05 dez. 2015.

PAPER, White. **BREACH SECURITY INC:** The web hacking incidents database 2009. Agosto, 2009.

PR WEB. **Maintains the Top Spot on SplashData's Annual.** Disponível em: http://www.prweb.com/releases/2015/01/prweb12456779.htm. Acesso em 10 nov. 2015.

RECUERO, Raquel. **Redes sociais na internet.** Cidade: Sulina. Editora – 2009.

RIPE NCC. **IPv6 Segurança - Uma Visão Geral.** Disponível em: https://www.google.com.br/?gws_rd=ssl#q=tradutor+on+line. Acesso em 15 nov. 2015.

SANS. **Critical Security Controls;** 2000-2016. BETHESDA, Maryland. USA. Disponível em: https://www.sans.org/critical-security-controls/. Acesso em 11 nov. 2015.

SANS INSTITUTE INFOSEC READING ROOM. **Convergence of Logical and Physical Security**. MEHDIZADEH, Yahya (p.4). Disponível em: http://www.sans.org/reading_room/whitepapers/authentication/convergence_of_logical_and_physical_security_1308. Acesso em 28 out. 2015.

SYMANTEC. **Minimizando os Riscos das Mensagens Instantâneas.** Disponível em: http://www.symantec.com/region/br/home_homeoffice/library/im_risks.html. Acesso em 26 out. 2015.

TEAMSID. **Piores senhas de 2014.** Splash Data (2014). Disponível em https://www.teamsid.com/worst-passwords-of-2014/. Acesso em 20 out. 2015.

TECNOLOGIA. **Postagens com localização e apps terceiros colocam usuário do Twitter em risco.** Disponível em: http://tecnologia.ig.com.br/dicas/2016-03-04/check-in-e-aplicativos-integrados-podem-afetar-seguranca-de-usuario-do-twitter.html. Acesso em 13 abr. 2016.

TECNOLOGIA**. O que é DNS e o que ele tem a ver com a minha conexão com a Internet?** Disponível em: http://tecnologia.uol.com.br/dicas/ultnot/2008/07/24/ult2665u363.jhtm. Acesso em 10 out. 2015.

TRUZZI. **Cyberbullying, Cyberstalking e Redes Sociais.** LIMA, Gisele Truzzi (2010). Disponível em: http://www.truzzi.com.br/pdf/artigo-cyberbullying-cyberstalkingredes-sociais.pdf. Acesso em: 18 nov. 2014.

VIVA O LINUX. **Set (Social Engineer)**. Disponível em: https://www.vivaolinux.com.br/dica/SET-(Social-Engineer). Acesso em 25 abr. 2016.