RODRIGO DA COSTA SILVA

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UMA ANÁLISE SOBRE AS TÉCNICAS DE ENGENHARIA SOCIAL APLICADAS PARA OBTER INFORMAÇÕES.

Ji-Paraná
2019

RODRIGO DA COSTA SILVA

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UMA ANÁLISE SOBRE AS TÉCNICAS DE ENGENHARIA SOCIAL APLICADAS PARA OBTER INFORMAÇÕES.

Monografia apresentada à Banca Examinadora do Centro Universitário São Lucas de Ji-Paraná, como requisito de aprovação para obtenção de grau acadêmico de Bacharel em Sistemas de Informação. Sob orientação do professor Jose Rodolfo Milazzotto Olivas.

Ji-Paraná
2019

Dados Internacionais de Catalogação na Publicação
Gerada automaticamente mediante informações fornecidas pelo(a) autor(a)

S586s Silva, Rodrigo da Costa.

Segurança da informação no ambiente corporativo: uma análise sobre as técnicas de engenharia social aplicadas para obter informações. / Rodrigo da Costa Silva.-- Ji-Paraná, RO, 2019.

77 p.

Orientador(a): Prof. José Rodolfo Milazzoto Olivas

Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) - Centro Universitário São Lucas

1. Segurança corporativa. 2. Sistemas de segurança. 3. Engenharia Social. I. Olivas, José Rodolfo Milazzoto. II. Título.

CDU 004.45

Bibliotecário(a) Alex Almeida CRB 11.8537

SÃO LUCAS
EDUCACIONAL

ATA Nº 05/2019 DE TRABALHO DE CONCLUSÃO DE CURSO EM SISTEMAS DE INFORMAÇÃO

No segundo dia do mês de dezembro de 2019, das 17h as 22h reuniram-se na sala de Inovação Tecnológica 7 o(a) professor(a) orientador(a) José Rodolfo Milzzotto Olivas e os(as) professores(as) Hailton Cezar Alves dos Reis e Thyago Bohrer Borges para comporem Banca Examinadora de Trabalho de Conclusão de Curso em Sistemas de Informação sob presidência do(a) primeiro(a), para analisarem a apresentação do trabalho "Segurança da informação no ambiente corporativo: uma análise sobre as técnicas de engenharia social aplicadas para obter informações.". Após as arguições e apreciação sore o trabalho exposto foi atribuída à menção como nota do Trabalho e Concluso do curso do Acadêmico(a) Rodrigo da Costa Silva.

OBS: Trabalho de Conclusão de Curso (X) Aprovado ou (__) Reprovado com nota total de 8,2, atribuídos o valor de 7,6 (sete vírgula seis pontos) para o trabalho escrito e o valor de 8,8 (oito vírgula oito pontos) para a apresentação oral.

Rodrigo da Costa Silva
Rodrigo da Costa Silva

Prof. Esp. Hailton Cezar Alves dos Reis

Prof. Me. Thyago Bohrer Borges

Prof. Esp. José Rodolfo Milzzotto Olivas
Orientador

Prof. Me. Thyago Bohrer Borges
Coord. Sistemas de Informação

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, que é meu guia e força nos momentos difíceis, a minha mãe Tereza que sempre me motivou a estudar e buscar o conhecimento, ao meu Pai Paulo que sempre fez de tudo por mim. Dedico também a minha namorada Karol que sempre me apoiou em todas decisões e esteve do meu lado nos momentos difíceis e felizes. Por fim, quero dedicar a todos os professores que estiveram presentes na minha vida acadêmica, pois graças à partilha de seus conhecimentos, pude me desenvolver neste caminho de estudos.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me dar sabedoria e me tornar capaz de concluir mais uma etapa em minha vida.

Aos meus pais por terem me ajudado e apoiado em todos momentos da vida, por me ajudar a sempre buscar o caminho do conhecimento e a querer crescer na vida.

Ao meu orientador Jose Rodolfo por me ajudar, e orientar no desenvolvimento deste trabalho.

A minha Namorada Karol, uma pessoa incrível, inteligente, minha fonte de inspiração nos estudos. Sem ela nada disso seria possível, desde que comecei a faculdade ela sempre acreditou no meu potencial, me apoiou nos momentos difíceis e me incentivou a sempre buscar mais e realizar meus sonhos, não importa o tamanho do sonho que eu tenho ela sempre diz que eu sou capaz e sabe de um jeito único me motivar a conquistar tudo. Graças a ela hoje eu sou completo e feliz.

“O trabalho vai preencher uma grande parte da sua vida. A única maneira de ser realmente feliz é fazer o que você acredita ser um ótimo trabalho. E o único jeito de fazer um ótimo trabalho é amar o que você faz.”
Steve Jobs

RESUMO

O presente trabalho foi desenvolvido por meio de pesquisas bibliográficas e artigos científicos sobre o tema da segurança da informação no ambiente corporativo:
uma análise sobre as técnicas de engenharia social aplicadas para obter informações, cuja problemática se refere a preparação das organizações para saber lidar com tipos de ataques relacionados a engenharia social, tendo em vista que o referido assunto é um tema que muito se tem discutido atualmente e motivo de grande preocupação por parte dos empresários. Percebe-se no decorrer deste estudo que embora seja um fator que vem ocorrendo com grande frequência nas organizações, as mesmas ainda não estão devidamente preparadas para lidar com esses tipos de ataques, haja vista que por vezes a organização, na tentativa de evitar novos gastos, ou até mesmo economizar, passam a contratar serviços de menor qualidade, contratam serviços não licenciados e produtos não originais. Assim, procura-se demonstrar que a melhor forma de combate à engenharia social ainda é através da prevenção, onde pequenas atitudes podem evitar que a organização seja alvo de um ataque, seja através de treinamentos adequados aos funcionários, através da utilização de produtos genuínos e serviços licenciados, combinado com a contratação de um serviço de TI adequado.

Palavras-Chave: Segurança. Engenharia social. Organizações.

ABSTRACT

The present work was developed through bibliographical research and scientific articles on the theme of information security in the corporate environment:
an analysis of the social engineering techniques applied to obtain information, whose problematic refers to the preparation of organizations to deal with types of attacks related to social engineering, considering that this subject is a subject that has been much discussed today and cause for great concern on the part of businessmen. It is clear from this study that although it is a factor that is occurring very frequently in organizations, they are not yet adequately prepared to deal with these types of attacks, since sometimes the organization, in an attempt to avoid new expenses , or even save money, start hiring lower quality services, hiring unlicensed services and non-original products. Thus, we seek to demonstrate that the best way to combat social engineering is still through prevention, where small attitudes can prevent the organization from being attacked, either through appropriate employee training, through the use of genuine products and licensed services combined with hiring an appropriate IT service.

Keywords: Security. Social engineering. Organizations

LISTA DE ABREVIATURAS E SIGLAS

TI – Tecnologia da Informação

DDOS- Distributed Denial of Service

IP- Internet Protocol address

ISO- International Organization for Standardization

NBR- Norma Técnica

ISFS- Information Security Foundation

CRM- Customer Relationship Management

SCM- Supply Chain Management

CPF- Cadastro de pessoa física

RG- Registro Geral

FBI- Federal Bureau of Investigation

SUMÁRIO

1. INTRODUÇÃO

Trata-se de um trabalho, cujo assunto está relacionado à área do conhecimento pertencente a segurança da informação, onde serão abordados os conceitos relacionados ao ambiente corporativo, mostrando como a Engenharia Social é aplicada para obter dados de empresas e vantagens de forma ilícita.

Com relação ao objetivo do presente trabalho, constitui em diversas pesquisas em livros, artigos científicos pertinentes ao assunto, a fim de desenvolver o caminho para a produção do tema em questão.

Propõe-se no presente projeto, uma investigação acerca das técnicas mais utilizadas na engenharia social, como a Análise de lixo, Internet e Rede Social, Contato Telefônico, Abordagem Pessoal, Phishing e Falha Humana e as formas de proteção mais eficazes, como evitar abrir e-mail recebido de pessoas/empresas desconhecidas, não passar dados privados relacionados à empresa por telefone, bem como se atentar com extensões de arquivos e programas ao fazer instalações nos computadores e sempre que houver dúvida de terminada solicitação procurar pelo supervisor.

No primeiro capítulo será abordado acerca da segurança da informação nas empresas, através de uma conceituação de segurança e informação, bem como será analisada a história das organizações ao longo do tempo, referente a organização dos seus dados, será abordado também sobre os aspectos da segurança da informação de modo geral, analisar-se-á por fim as vulnerabilidades das organizações e o fator humano.

No tocante ao segundo capítulo analisar-se-á especificamente acerca da Engenharia Social nas empresas, sua história ao longo do tempo, sua definição e a definição de engenheiro social, bem como suas principais técnicas utilizadas para obtenção de dados, será também realizada uma comparação da engenharia social, com os demais métodos utilizados para captar dados e por fim será estudada a nova tendência de fraude de engenharia social.

Por fim, no terceiro capítulo será solucionada a problemática suscitada no projeto de pesquisa, analisando-se às vulnerabilidades das empresas frente a engenharia social. As características da vulnerabilidade humana que são exploradas pelo engenheiro social. As formas mais comuns de segurança utilizadas atualmente, o uso de International Organization for Standardization (ISOS), traduzido na língua portuguesa, significa Organização Internacional para Padronização, bem como será realizada uma análise acerca da preparação das empresas para se defender desse tipo de ataque, e por fim serão elencados meios preventivos de combate a ataques e invasão.

A solução da problematização levantada no presente trabalho é de suma importância para o estudo da luta e combate a engenharia social, haja vista que ataques como os da engenharia social têm crescido cada vez mais, uma vez que o fator de manipulação humana é mais vulnerável para ser quebrado dentro de uma organização, sendo assim mais fácil obter dados e vantagens.

Deste modo, o presente trabalho será produzido a partir da questão gerada com o aumento do número de empresas que vem sofrendo os referidos ataques.

Por fim, busca-se efetuar uma pesquisa detalhada para descobrir se as empresas estão preparadas para se protegerem dessa técnica utilizada para captar dados, bem como analisar se existem medidas de segurança nas organizações que busquem de forma efetiva evitar determinados ataques.

1.1 PROBLEMATIZAÇÃO

De acordo com dados fornecidos pelas empresas Kaspersky e Ecoit, que são especialistas no ramo da segurança da tecnologia da informação, durante muito tempo as organizações vêm sofrendo inúmeros ataques tanto por meio de suas redes de computadores internas, como também na internet, e com o decorrer dos anos, passaram a ter uma evolução significativa no que tange a segurança da informação.

De acordo com o Referencial Teórico elaborado no Projeto de Pesquisa, embora as organizações atualmente possuam um preparo maior para se defender dos inúmeros ataques proporcionados pelos crackers, termo designado a pessoas que se utilizam de meios árduos para invadir sistemas e coletar informações, estes estão se evoluindo cada vez mais ao longo do tempo, se utilizando de inúmeras técnicas para coletar dados das organizações, tal como a engenharia social utilizada para influenciar as pessoas a fim de coletar dados, passando desta forma a serem conhecidos como engenheiros sociais, que se utilizam da persuasão para aproveitar-se da ingenuidade ou falta de conhecimento das pessoas.

Desta forma, surge a seguinte problemática em torno do tema em questão: As organizações estão preparadas para esse novo tipo de técnicas utilizadas para coletar dados?

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Analisar as técnicas mais comuns utilizadas na engenharia social para coletar dados das organizações.

1.2.2 Objetivos Específicos

- Compreender o histórico das organizações no que tange a organização dos seus dados;
- Identificar as principais técnicas utilizadas através da engenharia social para obter dados na empresa;
- Analisar as formas de segurança que as organizações têm utilizado para se prevenir de ataques relacionados à segurança da informação no que tange a engenharia social;
- Analisar as ameaças mais comuns direcionadas às organizações;
- Identificar meios preventivos de combate a ataques e invasões que estão sendo uteis atualmente;
- Avaliar se as empresas estão preparadas para se defender desse tipo de ataque de engenharia social no seu cotidiano.

2. REFERÊNCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS

A questão em torno da segurança da informação nas organizações é um tema que há muitos anos vem sendo discutido pela sociedade e alvo de inúmeras controversas. Diante disso, os profissionais da área de tecnologia da informação passaram a se interessar cada vez mais por esse tema, haja vista que com os grandes avanços da tecnologia, surgiram também avanços na tentativa de burlar a segurança da informação.

Com o passar do tempo as empresas começaram a se preocupar mais com à segurança de suas informações e dados, e em virtude disso, estão criando métodos eficazes de proteção, como por exemplo, a utilização de firewall, antivírus, proxy, dentre outros. Em contrapartida, os invasores também estão se aperfeiçoando a cada dia e aprendendo técnicas avançadas na tentativa de coletar dados e informações de forma ilegal das organizações.

Pode-se dizer que a segurança da informação possui três princípios essenciais para seu norteamento, sendo a confidencialidade, integridade e disponibilidade. Enquanto o primeiro tem o objetivo de impedir que informações confidenciais e críticas não sejam obtidas por meio de ataques criminosos como por exemplo, Ciberataques, espionagem, etc; o segundo visa a qualidade da informação, visto que esta precisa ser integra, ou seja, não pode sofrer alterações e por fim o terceiro visa que esteja sempre disponível o acesso à informação à pessoas que possuam o acesso autorizado.

> A Segurança da Informação, em geral, é entendida pela garantia de seus três aspectos fundamentais: a confidencialidade, que é a propriedade de a informação ser acessada por quem tenha autorização e não seja acessada por aqueles que não possuem autorização; a integridade, que é a propriedade de a informação não ter sido alterada por qualquer agente desautorizado; a disponibilidade, que é o aspecto da segurança que garante que a informação estará disponível para todos os autorizados e que precisem dela sempre que necessário (SOUZA, 2015, p.69).

Por outro lado, a segurança da informação ainda possui alguns aspectos importantes para sua prática, quais sejam, a autenticação, que é a disponibilização da informação apenas a aqueles que possuem autorização para acessar, e a conformidade que está relacionada dentro do regulamento e princípios éticos.

2.1.1 CONCEITO DE SEGURANÇA

De acordo com o dicionário tradicional, o conceito de Segurança é basicamente uma ação de tornar algo seguro, ou seja, estabilidade e firmeza. A segurança visa proteger algo ou alguém contra alguma coisa perigosa. Assim, quando dizem que algo está seguro, significa que a ameaça está longe.

No que tange especificamente à segurança voltada a informação pode-se dizer que essa é imprescindível dentro de uma organização, haja vista que a maioria dos dados e informações de uma empresa, são sigilosos e para tanto precisam estar seguros.

Pode-se afirmar que o conceito básico de segurança da informação é a proteção de dados e informações sigilosos de uma organização, na tentativa de coibir o acesso a pessoas não autorizadas.

Marcos Sêmola (2014, p. 41) define segurança da informação como “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Marcos Sêmola (2014) ainda explica que a segurança pode ser utilizada como “meio” e como “fim”. Enquanto no primeiro a segurança visa proteger os três princípios básicos, quais sejam a confidencialidade, integridade e disponibilidade, ou seja, a segurança neste caso é utilizada como um meio de proteção, já o segundo visa a padronização dos processos em que a informação é utilizada, ou seja, ela é utilizada com o objetivo de proteger as informações.

2.1.2 CONCEITO DE INFORMAÇÃO

A informação se dá a partir da organização de dados de forma coesa que atribua um sentido lógico a uma determinada coisa.

Nas palavras de Marcos Sêmola a informação nada mais é que,

> Conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ ou máquinas em processos comunicativos (isto é, baseados em troca de mensagens) ou transacionais (isto é, processos em que sejam realizadas operações que envolvam, por exemplo, a transferência de valores monetários. (2014, p. 43).

Assim, a informação é um conjunto de dados que podem ser uteis para o ser humano de alguma maneira, podendo ser armazenado ou transferido.

No entanto, é importante diferenciar a informação dos dados, pois dado é todo conteúdo que não relacionado a outro conteúdo, não agrega valor algum e a informação são todos os dados relacionados e organizados que geram algum valor, tornando-se assim uma informação.

De acordo com Peixoto (2006) as informações se subdividem-se em públicas ou internas, confidencial ou particular. As públicas são aquelas que estão disponíveis ao público em geral, sem restrições, como por exemplo sites na internet, revistas, artigos, jornais, etc; já as internas são aquelas que são específicas da organização, somente permitido seu acesso a pessoas autorizadas, sendo estas o alvo principal do engenheiro social. As confidenciais são aquelas também específicas de uma empresa, no entanto, estas informações são restritas a um número específico de funcionários. Por fim as informações particulares são aquelas informações que envolvem a vida privada de um funcionário, como conta bancária, histórico financeiro, etc.

Importante ressaltar que há diversos tipos de informações em uma organização, podendo ser pública, restrita, sigilosa, secreta e ultra secreta, assim cada uma merece uma atenção individual por parte dos colaboradores.

A informação pública é aquela que está disponível para todos, podendo assim qualquer pessoa ter acesso a ela, sem prejuízo a organização, considerando ser de interesse público, no entanto é necessário um cuidado com relação a estas em garantir que não sejam alteradas.

O autor Lyra assim explica,

> Essas informações não precisam de controle de acesso e de distribuição. Apenas deve-se cuidar para que elas não sejam danificadas ou alteradas. São exemplos de informações de nível 1: Dados do balanço de empresas de capital aberto; Lista de produtos; Notícias sobre a empresa. (2015, p.2)

As informações restritas são específicas a um número de pessoas, geralmente são aquelas em que apenas as pessoas que possuem algum tipo de interesse podem ter acesso.

> Essas informações, se vazadas, podem comprometer a imagem da organização mas não sua operação. São exemplos de informações de nível 2: Relatórios de consultoria sobre empresas concorrentes; Dados pessoais dos funcionários e executivos da empresa; Relatos de defeitos de produtos e serviços. (LYRA, 2015, p. 2)

As informações sigilosas são aquelas informações de muita importância para o crescimento da empresa, uma vez vazadas estas podem ser cruciais para uma crise financeira, haja vista que podem ser uteis a concorrência, assim elas são sigilosas e apenas os envolvidos nessa informação podem ter acesso a elas.

> Essas informações, se vazadas ou danificadas, podem gerar decisões erradas e prejudiciais para a operação da empresa ou inviabilizar o lançamento de um novo produto ou serviço. São exemplos de informações de nível 3: Relatórios de investigação de práticas concorrenciais ilegais; Detalhes sobre campanhas de lançamento comercial; Detalhes sobre planos de fusão, aquisição ou fechamento de empresas. (LYRA, 2015, p. 2)

Já as informações secretas são aquelas que dizem respeito a fabricação de produtos novos, decisões significativas ou detalhes de produtos e serviços que estão em lançamentos, sendo de suma importância para a empresa que tais informações permaneçam secretas aos envolvidos, vez que caso sejam vazadas podem levar a concorrência a se utilizar de tais informações e lançar o referido produto ou serviço antes.

> Essas informações, se vazadas ou danificadas, podem comprometer o protagonismo no lançamento de um novo produto ou ainda permitir que

> concorrentes o lancem antes da empresa. Podem ainda inviabilizar fusões ou aquisições de empresas ou, pior, leva a empresa a ser alvo de investigação por parte da CVM. São exemplos de informações de nível 4: Detalhes de produtos e serviços em desenvolvimento; Detalhes sore a negociação de compra ou venda de empresas ou filiais; Relatórios sobre falhas graves, em produtos, serviços ou processos internos, que podem afetar o valor das ações da empresa na bolsa de valores. (LYRA, 2015, p. 2).

Por fim, as informações ultra secretas são aquelas em que somente a alta cúpula da empresa consegue ter acesso, caso sejam vazadas podem levar a empresa a responder a grandes processos judiciais e até mesmo ocasionar uma falência não premeditada.

> Essas informações, se vazadas, podem levar a ações judiciais à empresa ou a seus executivos e acionistas. Compreendem ainda informações sobre segredos industriais que diferenciam a empresa de seus concorrentes. São exemplos de informações de nível 5: Detalhes sobre operações ilícitas ou de alto risco jurídico; Segredos industriais sobre componentes, insumos ou processos de produção dos principais produtos da empresa ainda não patenteados ou protegidos por lei. (LYRA, 2015, p. 3).

Percebe-se então a importância das informações e de sua segurança devida para uma organização, visto que caso sejam conhecidas por pessoas má intencionadas, podem causar inúmeros prejuízos para a organização.

2.1.3 HISTÓRICO DAS ORGANIZAÇÕES NO QUE TANGE A ORGANIZAÇÃO DOS SEUS DADOS

Na década de 90, com o advento da era da informação, as organizações saíram do modelo tradicional vindo da era industrial e passaram a encarar novos desafios nos negócios. A partir desse momento as organizações tiveram que acompanhar o ritmo das inovações daquela época, de tal modo que acabou por ocasionar um cenário no mundo dos negócios mais dinâmico e com fácil potencial de mudanças, porque a tecnologia teve como importante papel estimular essas mudanças conforme as necessidades organizacionais.

Conforme explica Marcos Sêmola,

> Se resgatarmos a história, veremos diversas fases, desde as revoluções industrial e elétrica, a abertura de mercado e o aumento da competitividade proporcionado pela globalização, passando pelos momentos relacionados à reengenharia de processos, à terceirização, à virtualização e, mais recentemente, aos efeitos da tecnologia da informação aplicada ao negócio de forma cada vez mais abrangente e profunda. (2014, p. 1).

Com tantas mudanças acontecendo e tornando-se cada vez mais competitivo o mundo dos negócios, era imprescindível que as organizações tivessem que reestruturar a sua forma de gerir o negócio, tanto na estrutura da parte de gestão, quanto na relação com os clientes.

O autor Chiavenato (2010) aborda em um quadro os quatros componentes da função de organizar assim denominados por ele de tarefas, pessoas, órgãos e relações.

Dessa forma, a parte de relações é voltada para adesão de sistemas de informações com foco para aproximar as organizações com o cliente e os fornecedores, utilizando o CRM (Customer RelationShip Management) para armazenar os dados dos clientes e futuramente utilizar desses dados para gerirem informações importantes para o negócio e o SCM (Supply Chain Management) para guardar dados de seus fornecedores.

Com a evolução da tecnologia nos anos 90, esta começou a ter um avanço mais rápido ainda, não somente nas organizações, mas também para o uso de usuários em suas residências com a utilização da internet.

De acordo com Silva (2015) a tecnologia evoluiu tanto ao ponto que o acesso a essas informações são feitas por meio de dispositivos eletrônicos que possuem diversos sistemas de informações, tendo como objetivo organizar os dados e transformá-los em informações. Assim, as organizações começaram a utilizar o sistema para melhorar o relacionamento com seus clientes e fornecedores, hoje em dia esse processo pode ser organizado de maneira mais prática por meio de smartphones, notebooks, computadores e demais dispositivos eletrônicos.

Conforme defendido por Silva (2015) o objetivo da segurança da informação é garantir que os dados das organizações sejam guardados de forma segura, logo pessoas que não tenham autorização para ter acesso a esses dados, não poderão utilizá-los sem permissão.

Desta forma, o fácil acesso à informação por meio de diversos dispositivos eletrônicos, trouxe também algumas preocupações para as organizações em proteger seus dados.

2.1.4 ASPECTOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação possui dois aspectos fundamentais, sendo a autenticação e a conformidade. No entanto, de acordo com Sêmola (2014) ela possui também alguns aspectos que merecem destaque, como autorização, auditoria, autenticidade, severidade, relevância do ativo, relevância do processo de negócio, criticidade e irretratabilidade.

A autorização é um aspecto de extrema importância no que tange a segurança da informação, pois estabelece que somente usuários autorizados tenham acesso a uma informação.

Já a auditoria é um processo que visa identificar a origem e o destino das informações repassadas, com o objetivo de identificar as pessoas envolvidas na movimentação das informações.

Por outro lado, a autenticidade é um processo que visa assegurar que as pessoas que trocam informações são realmente quem dizem ser, e que a informação repassada seja verídica e não tenha sido alterada de nenhuma forma.

A severidade diz respeito ao tamanho do dano que um bem pode sofrer em razão da exploração de um ponto fraco de alguma organização. Assim, já se enquadra a relevância do ativo, haja vista que o ativo possui uma grande importância para os negócios, que por sua vez há a relevância do processo de negócio, tendo em vista a importância que esse processo tem para uma organização.

Por fim, a criticidade é a gravidade do impacto que a ausência de ativo traz para uma organização e a irretratabilidade é quando uma informação vem com a autenticidade do seu emissor.

2.1.5 VULNERABILIDADES

É importante frisar que quando se fala em vulnerabilidade da informação, significa dizer que há uma ausência de proteção com relação a esta informação, ou seja, há uma ameaça eminente que possa explorar essa vulnerabilidade. Essas ameaças tanto podem ser naturais, voluntárias ou involuntárias, mas ambas se concretizadas trazem um enorme prejuízo para uma organização.

Dantas afirma que,

> Observa-se que as vulnerabilidades estão relacionadas com situações de fragilidade existentes no ambiente ou nos ativos, e que elas estão relacionadas com um incidente indesejado que, em decorrência daquela, pode vir a provocar algum dano. (2011, p. 31)

Na maioria dos casos vulnerabilidade é causada por uma falta de proteção maior de uma informação sigilosa, logo em decorrência desta falta de segurança, pessoas mal-intencionadas podem se utilizar dessa fragilidade na proteção para se beneficiar ilicitamente de tais informações.

De acordo com uma pesquisa trazida por Dantas as principais ameaças à segurança da informação são:

> Vírus, worm, cavalo de tróia (trojan horse);
> Phishing, pharming e spyware; Adware; spam;
> Roubo de dados confidenciais da empresa e de cliente, da propriedade da informação e da propriedade intelectual;
> Acesso não autorizado à informação;
> Perda de dados de clientes;
> Roubo de laptop, portáteis e de hardware;
> Má conduta e acesso indevido à network por funcionários e gerentes, bem como abuso de seus privilégios de acesso e utilização indevida da rede wireless;
> Ataque de negação de serviço, invasão de sistemas e da network;
> Acesso e utilização indevida da internet e dos recursos dos sistemas de informação;
> Degradação da performance, destruição e/ou desfiguramento da network e do web site;
> Software de má qualidade, mal desenvolvido e sem atualização;
> Fraude financeira e de telecomunicações;
> Interceptação de telecomunicação (voz ou dados) e espionagem;
> Sabotagem de dados e da network;
> Desastres naturais;
> Cyber-terrorismo; (2011, p. 36-37)

O autor Sêmola (2014) traz alguns exemplos de vulnerabilidades, sendo elas físicas, naturais, hardware, software, mídias, comunicação e humanas.

As físicas e as naturais são semelhantes, pois enquanto a primeira diz respeito a instalação da organização em mal estado, as naturais dizem respeito a proximidade de equipamentos eletrônicos com locais onde possam ocorrer desastres naturais.

O Hardware pode ter exemplos de vulnerabilidade quando submetido a ambientes com umidade, sujeira, calor ou quando mal manuseado, instalado com os demais componentes, podendo assim gerar falhas. Quanto ao Software, a sua programação pode ser um problema de vulnerabilidade, uma vez que ao deixar falhas no código ou até mesmo na regra de negócio do sistema, isso faz com que pessoas não autorizadas consigam facilmente acessar um sistema ou aplicativo.

Com relação a mídia, a sua fragilidade pode ser um fator de vulnerabilidade, pois podem acabar sendo danificados com descarga de energia ou fator alheio ao ambiente físico, fazendo com que seus dados possam vir a se perder. Já a comunicação é um fator sensível, uma vez que pode ser rastreado por programas diversos, como por exemplo escutas telefônicas, ataques em aplicativos, programas de mensagens e etc.

Por fim, o fator humano está relacionado com o treinamento do colaborador dentro de uma organização, pois uma vez que mal preparado, pode vir ocasionar problemas no ambiente físico ou até mesmo no ambiente lógico referente as informações, este será discutido afundo no decorrer dos próximos tópicos.

2.1.6 FATOR HUMANO

Conforme explica Sêmola (2014) o fator humano é um dos maiores causadores na quebra do sigilo das informações, haja vista que este vem tornando-se cada vez mais alvo de ataques por parte dos criminosos.

Ainda de acordo com Sêmola (2014) um dos principais motivos para que o fator humano seja um alvo fácil de ataques é exatamente a falta de preparação, uma vez

que um novo colaborador muitas vezes não possui um tempo hábil para aprender as normas e regras da empresa antes de começar a exercer suas funções.

É importante ressaltar que um ex-funcionário de uma organização representa um grande fator de risco, haja vista que por diversas vezes ao término de um contrato de trabalho, há desavenças entre o funcionário e o dono da empresa, logo aquele pode por motivos de insatisfação e até mesmo por vingança, divulgar informações sigilosas da empresa.

Peixoto (2006), assim explica que como o funcionário que trabalha na empresa, o ex-funcionário representa um grande fator de risco em se tratando de informações confidenciais. Funcionários insatisfeitos ou revoltados por uma demissão devem ser sempre pontos de suspeita em casos às vezes inexplicáveis de perdas de documentos importantes, entrega de informações que somente aquele setor deveria saber, dentre inúmeros outros problemas quanto à seguridade de informações internas da empresa.

Ocorre que nem sempre a divulgação de informações sigilosas acontece de forma proposital, em alguns casos ela ocorre por acidente, ou seja, negligência ou falta de atenção de algum funcionário, deste modo entra a figura dos insider threat, mais comumente conhecidos como ameaças internas, uma vez que essas pessoas podem ser os próprios colaboradores, ex-funcionários, associados de negócios que por motivos desconhecidos acabam tendo acessos a setores ou terminais que não possuem autorizações, não sendo uma ameaça de imediato, mas podendo se tornar uma, devido as informações privilegiadas que ele possa vir a obter.

Adachi (2004 apud NETTO; SILVEIRA, 2007, p. 280) explica que a camada humana é formada por todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos da Tecnologia da Informação (TI), seja para manutenção ou uso. São aspectos importantes desta camada: a percepção do risco pelas pessoas: como elas lidam com os incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes no uso da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social.

Como explanado, a ausência da segurança da informação nas empresas, nem sempre ocorre por má-fé dos colaboradores, muitas vezes ocorre simplesmente pela falta de um treinamento apropriado, assim eles acabam não sabendo lidar com algumas situações, daí advém a necessidade das organizações treinarem adequadamente seu quadro de colaboradores.

Eliézer Pereira (2018) assim explica

> Surge então a necessidade de investir em treinamento e conscientização à cerca de como proteger a informação. Pessoas necessitam saber o valor desta informação, e assim participar efetivamente de processos além de operar mecanismos para que ela seja protegida. Pessoas, processos e tecnologias são de vital importância para a manutenção da segurança da informação, e no que consiste às pessoas, algumas vulnerabilidades podem ser exploradas, como é o caso da engenharia social. (Disponível em: <https://www.lexmachinae.com/2018/01/04/fator-humano-em-seguranca-da-informacao/ >. Acesso em 18 de agosto de 2019 às 12:00)

Desta feita, é essencial que ao fazer parte da organização, todo colaborador seja devidamente treinado acerca da segurança da informação, bem como é imprescindível que eles possuam um conhecimento adequado no que tange às formas de ataque e vulnerabilidades da empresa, para que assim, caso ocorra alguma situação de ameaça, consigam lidar com elas da melhor forma possível e menos prejudicial à organização.

2.2 ENGENHARIA SOCIAL NAS EMPRESAS

Atualmente, muito se tem discutido acerca das formas mais comuns de ataques à segurança da informação nas organizações, dentre as quais destacam-se a engenharia social que é uma técnica muito utilizada para influenciar as pessoas através da persuasão.

De acordo com Rosa, Silva e Silva (2012) o termo Engenharia Social ficou conhecido nos anos noventa, em decorrência do famoso Hacker americano Kevin Mitnick, que ficou conhecido mundialmente após invadir o sistema do Comando de Defesa Aérea dos Estados Unidos, ele se utilizava desta técnica para coletar dados que pudessem ser úteis para suas invasões.

A Engenharia Social está relacionada ao fato de alguém persuadir uma pessoa com o objetivo de ganhar a confiança desta, a fim de obter informações privilegiadas e a partir disso conseguir acessos não autorizados a computadores ou informações.

2.2.1 HISTÓRICO DA ENGENHARIA SOCIAL

Estando agora as organizações inseridas em um contexto tecnológico onde toda sua informação gerida por meio dos seus sistemas de informações é tão valiosa, surgem pessoas mal-intencionadas conhecidas como crackers. Para Ferreira a definição de cracker é:

> Não muito conhecido pelas pessoas, o cracker, ou black hat (chapéu preto), é praticamente o hacker do mal. Os crackers são indivíduos também com amplo conhecimento em informática, mas que usam esse conhecimento para quebrar sistemas de segurança a fim de obter vantagens ilícitas. (2014, p.4).

Os crackers têm como objetivo captar dados sigilosos, se utilizando de novos meios de roubar dados, como ataques às redes de computadores, enviando vírus e outros ataques.

Em contrapartida, com o passar do tempo, no intuito de se protegerem, as organizações foram adotando técnicas para evitar tais ataques como a utilização de Antivírus, que é um software para proteção contra invasores e ameaças e Firewall, sendo uma proteção utilizada para rede interna do ambiente, entre outros meios de segurança da informação.

Com a evolução na parte de segurança da informação por meio das organizações, novas técnicas começaram a surgir, como por exemplo, a “Engenharia Social”, conforme define Nakamura e Geus,

> A engenharia social é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização. (2003, p. 70).

A Engenharia Social, técnica utilizada para influenciar pessoas por meio da persuasão, é destinada para roubar dados de organizações e pessoas, conforme tais dados sejam coletados. Os autores Mitnick e Simon afirmam que

> A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia. (2003, p.8).

Assim, tais pessoas que fazem uso dessa técnica para captar dados ficaram conhecidas como Engenheiros Sociais. Peixoto (2006) afirma que o Engenheiro Social na maioria das vezes são pessoas agradáveis.

O efeito que o uso dessa técnica pode ter em uma organização é imensurável, visto que o Engenheiro Social trabalha diretamente com a manipulação humana na organização, não apenas em ataques diretos a softwares e a rede, sendo assim qualquer pessoa em uma organização pode ser alvo de ataques da Engenharia Social a qualquer momento e qualquer lugar, não necessariamente estando dentro da organização.

2.2.2 DEFINIÇÃO DE ENGENHARIA SOCIAL

No decorrer dos anos, diversos foram os conceitos trazidos para explicar essa técnica mundialmente conhecida, que é a Engenharia Social, assim faz-se necessário destacar algumas delas.

Os autores Rosa, Silva e Silva (2012) definem Engenharia Social como “o termo utilizado para identificar um conjunto de técnicas cujo objetivo é a obtenção de informações relevantes a respeito de um determinado indivíduo ou organização.”

Para Nakamura e Geus a definição de Engenharia Social é:

> [...] a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização. (2003, p. 70).

Já Jeremy (2015, apud MAULAIS, 2016, p.23) atribui o seguinte conceito

> A Engenharia Social, no contexto da Segurança da Informação é a manipulação de pessoas para levá-las inconscientemente a executar ações que causam danos à confidencialidade, integridade e disponibilidade de recursos da organização, incluindo a informação, os sistemas de informação e os sistemas financeiros.

Mister destacar ainda o conceito trazido por Nicholas Ferreira

> Engenharia social é a prática de conseguir informações sigilosas com outras pessoas, ou fazer com que elas façam o que você quer, sem perceber, usando a argumentação e persuasão a seu favor. (2014, p. 06)

Rosa, Silva e Silva (2012) acreditam que as informações podem ser obtidas por ingenuidade, persuasão, dissimulação ou confiança.

Assim, o Engenheiro social, que é o nome dado a pessoa que pratica a Engenharia Social, se utiliza da ingenuidade da sua vítima, até mesmo por falta de conhecimento da mesma acerca da sua vulnerabilidade, podendo empregar também a persuasão, que é muito comum, onde utiliza meios de chantagem para alcançar seus objetivos, ou ainda o Engenheiro social pode fazer uso da dissimulação, fingindo ser uma pessoa que não é, com o objetivo de ganhar a confiança da vítima e fazê-la fornecer informações importantes da empresa.

Desta feita, a principal técnica utilizada pela pessoa que pratica a Engenharia social é a manipulação, ou seja, ela age com frieza e todo o ataque é premeditado, se utilizando de alguma vulnerabilidade da vítima em questão, logo ela leva a mesma a praticar alguma conduta (ainda que inconscientemente) que prejudique de alguma forma a segurança da organização.

2.2.3 QUEM É O ENGENHEIRO SOCIAL

O Engenheiro social, na maioria dos casos é uma pessoa aparentemente bem vestida, carismática, possui uma boa conversa e sem qualquer tipo de dúvida, é uma pessoa inteligente e manipuladora.

Turban (2004, apud BALDIM, 2007, p. 45) traçou um perfil básico do engenheiro social, como por exemplo, na maioria dos casos são homens brancos entre 19 e 30 anos, sem antecedentes criminais, costumam ser programadores de aplicativos, usuários de sistema, pessoal administrativo, estudantes ou gerentes. Geralmente possuem um QI elevado, é inteligente e tem boa aparência, além de ser criativo, aparentemente autoconfiante, ambicioso, dinâmico e gosta de aventuras, e sempre está disposto a aceitar desafios tecnológicos, por ser altamente motivado.

Então, pode-se entender que o engenheiro Social se utiliza da arte da enganação para fazer com que a vítima em questão forneça informações importantes da organização que lhe possam ser úteis de algumas formas.

Em se tratando dos ataques realizados por Engenheiros Sociais, Gartner (2002, apud BALDIM, 2007, p.47) define um ciclo de ataque, sendo este: coletar informações, desenvolvimento da relação, explorando a relação e executando o ataque.

Primeiramente, o Engenheiro Social se utiliza de técnicas para obter informações básicas sobre a vítima, para se utilizar futuramente, como por exemplo obtenção de dados pessoais, CPF, RG, nome completo, data de nascimento e dados físicos como a característica da pessoa, etc.

Logo, ele se utiliza do desenvolvimento de relação, que é o fato de ganhar a confiança por meio de ataques onde possa explorar a fraqueza humana e assim vir a criar um laço afetivo com a vítima, tal método pode demorar dias, semanas ou até meses para se concretizar.

A partir de então, surge a exploração de relações, onde o Engenheiro Social sonda a vítima, a fim de obter informações importantes, as quais esta não revelaria em qualquer momento, como por exemplo senha de bancos, período de férias, etc. Ocorrem casos também em que o engenheiro social obriga a vítima a praticar determinadas ações.

Já na fase de execução do ataque, o Engenheiro Social utiliza de todas as outras fases abordadas anteriormente, reunindo as informações conseguidas a fim de colocar em prática seu ataque de maior proporção direcionado a empresa.

Kevin Mitnick identifica algumas das atitudes mais comuns dos Engenheiros sociais tais como

> Na maioria dos ataques de engenharia social, o atacante assume certos acessórios do 'papel' que está representando para fazer com que o alvo infira

> outras características e aja de acordo com o esperado. Esse papel pode ser o de um técnico de TI, o de cliente, o de um novo contratado ou de qualquer um que requeira o cumprimento de uma solicitação. Táticas comumente usadas são mencionar o nome do chefe do alvo ou de outros funcionários, usar terminologia ou jargão da empresa ou do setor. Para ataques 'físicos', os atacantes podem escolher roupas, jóias (um alfinete da empresa, um relógio de atleta, uma caneta cara, um anel de formatura) ou modos de se arrumar (por exemplo, o estilo do penteado), também acessórios que podem conferir credibilidade ao papel desempenhado pelo atacante. A força desse método deve-se ao fato de que, ao aceitarmos alguém (como um executivo, cliente ou funcionário), fazemos inferências e atribuímos outras características a essa pessoa (um executivo é rico e poderoso; um desenvolvedor de software têm conhecimentos técnicos, mas pode ser socialmente inibido; um funcionário é digno de confiança). (2005, p.198).

Desta forma, dentro de uma empresa independente do setor em que os colabores atuem, estes podem correr o risco de ataques voltados a Engenharia Social, independente do setor, função ou cargo, uma vez que o Engenheiro Social busca roubar informações para que futuramente venham a ser utilizadas como meio de extorsão.

2.2.4 PRINCIPAIS TÉCNICAS UTILIZADAS ATRAVÉS DA ENGENHARIA SOCIAL PARA OBTER DADOS NA EMPRESA

De acordo com Maulais (2016) as principais técnicas utilizadas em um ataque de Engenharia Social para obter informações de sistemas, redes de computadores das organizações são: a Análise de lixo, Internet e Rede Social, Contato Telefônico, Abordagem Pessoal, Phishing e Falha Humana, as quais serão devidamente definidas a seguir:

A análise de lixo é tudo aquilo que é descartado pelas organizações, assim, estes dados contidos em papéis que são jogados em lixos comuns, podem vir a ser utilizados por um engenheiro social para obter mais informações futuramente.

Para Rafael (2013) a análise de lixo para os Engenheiros Social tem importância devido

> [...] poucas organizações têm o cuidado de verificar o que está sendo descartado da empresa e de que forma é realizado este descarte. O lixo é uma das fontes mais ricas de informações para os Engenheiros Sociais. (Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em 01 de setembro de 2019 às 18:00).

Deste modo é possível ver a importância que até mesmo os dados descartados pelas organizações têm, uma vez que o Engenheiro Social pode se utilizar destes como finalidade para realização de novos ataques ou até mesmo obter vantagens privilegiadas dentro da organização com a forma de manipulação do colaborador.

A Internet como um todo é uma grande ferramenta para encontrar dados públicos de organizações, o que acaba sendo prejudicial, haja vista que por muitas vezes o uso de redes sociais na internet pode acabar prejudicando uma organização, quando seu uso acaba sendo exagerado e expondo informações importantes que por sinal deveriam ser privadas apenas aos colaboradores.

De acordo com Townsend (2019) a motivação de ataques online na internet se faz frente a oportunidade de

> O maior e mais comum motivador dos ataques de engenharia social online é obter acesso aos dados confidenciais da vítima. Os dados pessoais são um dos bens mais valiosos na internet e são negociados entre empresas e também no mercado negro. (Disponível em: <https://blog.avast.com/pt-br/social-engineering-hacks >. Acesso em 19 de setembro de 2019 às 21:30).

O contato telefônico geralmente é utilizado quando combinado com outras técnicas já previamente utilizadas e com algum resultado obtido, a partir disso o Engenheiro Social pode se utilizar do contato telefônico para tentar roubar mais dados ou manipular para que alguma ação importante seja tomada pelo alvo.

A Abordagem pessoal é a técnica em que o Engenheiro Social pode ir até a empresa se passando por um fornecedor ou alguém interessado em conhecer a organização, os produtos, serviços e etc. A partir disso se aproveita para coletar mais informações importantes para seu ataque.

Para Rafael (2013) a utilização da abordagem pessoal consiste em

> Abordagem Pessoal: Está técnica consiste do Engenheiro Social realizar uma visita na empresa alvo, podendo se passar por um fornecedor, terceiro, amigo do diretor, prestador de serviço, entre outros, no qual através do poder de persuasão e falta de treinamento dos funcionários, consegue sem muita dificuldade convencer um segurança, secretária, recepcionista a liberar acesso ao datacenter onde possivelmente conseguirá as informações que procura. (Disponível em:

> <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em 01 de setembro de 2019 às 20:35).

A utilização dessa técnica é importante para a Engenharia Social de modo que a partir dela é possível não somente conhecer o ambiente que pretende efetuar um ataque de Engenharia Social, como também obter algumas informações mediatas.

Nos dias atuais a Rede Social tem sido uma grande aliada para a Engenharia Social, visto que as pessoas estão cada vez mais tornando público seus dados, fotos e vídeos, por meio das redes sociais e aplicativos. Isso pode ter fator decisivo para um Engenheiro Social, uma vez que pode utilizar desse meio para influenciar um colaborador de uma determinada organização.

De acordo com Rafael (2013) o Engenheiro Social utiliza da Rede Social quando necessita

> [...] conhecer melhor seu alvo, esta técnica é utilizada, iniciando um estudo no site da empresa para melhor entendimento, pesquisas na Internet e uma boa consulta nas redes sociais na qual é possível encontrar informações interessantes de funcionários da empresa, cargos, amizades, perfil pessoal, entre outros. (Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em 01 de setembro de 2019 às 18:01).

Deste modo é possível ver a importância dessa técnica para o Engenheiro Social, uma vez que é possível conhecer a vítima com antecedência, saber seus pontos fracos e descobrir meios para influenciar a mesma.

A Falha Humana acaba sendo por muitas vezes utilizada para contribuir com ataques sociais, se aproveitando de fraquezas humanas, como medo, bondade, insegurança e muitos outros fatores.

Para Rafael (2013) sobre os fatores humanos que são mais suscetíveis estão

> Falhas Humano: O Ser Humano possui várias vulnerabilidades que são exploradas pelos Engenheiros Sociais, tais como, confiança, medo, curiosidade, instinto de querer ajudar, culpa, ingenuidade, entre outros. (Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>. Acesso em 01 de setembro de 2019 às 01:08).

A técnica de Phishing mais utilizada no dia a dia, em sua tradução literal significa “pescaria”, utilizada através de e-mails falsos enviados para as organizações, tendo por objetivo fazer com que algum colaborador abra tal e-mail e realize os procedimentos solicitados neste.

De acordo com Müller (2012) a técnica de phishing ocorre

> O phishing pode ocorrer de diversas formas. Algumas são bastante simples, como conversas falsas em mensageiros instantâneos e emails que pedem para clicar em links suspeitos. Fora isso, existem páginas inteiras construídas para imitar sites de bancos e outras instituições. Todas essas maneiras, no entanto, convergem para o mesmo ponto: roubar informações confidenciais de pessoas ou empresas. (Disponível em <https://www.tecmundo.com.br/phishing/205-o-que-e-phishing-.htm>. Acesso em 30 de setembro de 2019 às 20:00)

Deste modo é preciso ficar atento as diversas formas de ataques que essa técnica pode propor, para evitar cair em suas armadilhas e ter seus dados e segurança comprometidos.

2.2.5 COMPARAÇÃO DA TÉCNICA DE ENGENHARIA SOCIAL COM OS DEMAIS MÉTODOS UTILIZADOS PARA ROUBAR DADOS

Como explanado, a engenharia social é uma técnica de ataque voltada à manipulação de pessoas, ou seja, o engenheiro social, que na maioria dos casos é uma pessoa aparentemente confiável, se utiliza dessa possível confiança para manipular as pessoas e conseguir informações que lhe possam ser uteis de alguma maneira.

Entretanto, inúmeros são os métodos além da engenharia social, que são utilizados para captar dados de uma organização, tais como Backdoor, Ataque DDoS, Eavesdropping, Spoofing entre outros que serão devidamente definidas a seguir:

De acordo com a empresa de tecnologia Psafe em uma matéria publicada por Novaes (Disponível em <https://www.psafe.com/blog/botnet-x-backdoor-sao-como-prevenir/>. Acesso em 01 de outubro de 2019) o backdoor é direcionado a obter controle de apenas uma máquina, como seu foco é específico isso faz com que este

ataque seja mais prejudicial ao usuário, uma vez que obtém o controle do computador é possível ter acesso a todos dados da máquina.

Logo, o método acima citado é bem parecido com as técnicas relacionada a Engenharia Social, onde é possível selecionar um alvo e estudar ele de modo que seja possível preparar a melhor abordagem para capturar os dados da vítima.

Os ataques DDoS tem por finalidade sobrecarregar um servidor ou computador, de modo que seu processamento e memória fiquem esgotados e isso deixe o mesmo inacessível, fazendo com que o usuário não tenha acesso a internet ou em determinado sistema.

Conforme publicado pela empresa Hostinger o objetivo de um ataque DDoS é:

> Um ataque DDoS é geralmente motivado por hackers que, por algum motivo especial, tenham um objetivo malicioso em comum, fazendo de tudo para que um alvo fique indisponível na internet e o prejudique de várias maneiras diferentes. (Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-ddos-e-como-se-proteger-de-ataques> Acesso em 02 de outubro de 2019 ás 20:15).

Ficar inacessível a internet ou a sua própria rede pode ser prejudicial de diversas formas, uma vez que isso faz com que sua segurança lógica seja prejudicada e a empresa ou usuário sejam um alvo fácil.

Outra técnica bem utilizada para roubar informações é a Eavesdropping utilizada para violar a confidencialidade, tendo por objetivo fazer uma varredura sem autorização em todo dispositivo que esteja sendo alvo do ataque.

A técnica de Spoofing é utilizada para falsificar IP, isso faz com que a comunicação entre os dispositivos seja comprometida, visto que aplicada essa técnica é possível fazer com que um dispositivo falsificado se passe por outro, o qual seria a fonte confiável da comunicação.

2.2.6 UMA NOVA TENDÊNCIA: A FRAUDE DE ENGENHARIA SOCIAL

O Controle de um sistema de informação em uma determinada organização deve ser mantido com um nível de segurança alto, visto que todos os dados utilizados por uma organização, que são gerados dentro de um sistema de informação, possuem tanto os dados dos seus clientes como também dos seus colaboradores, sócios, produtos e toda lógica de negócio utilizados pela empresa, e isso é o que um Engenheiro Social busca para fazer de refém uma determinada organização.

Uma nova tendência é a utilização de fraudes combinadas com a Engenharia Social, considerando que essa técnica está crescendo e causando prejuízos as organizações, Zoldi explica a utilização dessa nova abordagem

> Fraudes baseadas em engenharia social estão em ascensão, com abordagens cada vez mais ousadas e manipuladoras que as anteriores. Um ataque deste tipo refere-se a qualquer transação na qual a vítima é levada a revelar detalhes financeiros confidenciais ou transferir dinheiro de suas contas para fraudadores. Exemplos comuns incluem e-mails falsos (phishing) e mensagens de texto." (2018. Disponível em **<**https://computerworld.com.br/2018/10/17/machine-learning-contra-fraudes-de-engenharia-social/> Acesso em 23 de outubro de 2019 às 03:15)

Como explicado acima, a utilização da Engenharia Social se dá por meio de técnicas já existentes, como por exemplo phishing, onde a vítima recebe um e-mail falso ou mensagem de texto e acredita na veracidade do conteúdo recebido e acaba caindo no golpe.

De acordo com Comer (2011) dentro de uma organização pode existir 3 tipos de fraudes sendo essas as Fraudes Internas, Externas, de Funcionários e da Gerência.

As fraudes Internas ocorrem por meio de um criminoso que tenha acesso a organização, podendo ser este um funcionário ou alguém que teve seu acesso liberado ao local, assim poderá ter acesso a vários dados da instalação física e até mesmo sistemas de informações utilizados na organização.

As fraudes externas acontecem quando o criminoso em parceria com o funcionário utiliza de dados da organização, como por exemplo, quem são os

fornecedores, os clientes, contas a receber e entre outros dados para conseguir fraudar e obter vantagem.

Por fim, as fraudes de funcionários e da Gerência estão voltadas para a parte da Ganância, onde são motivadas pelo poder ou vontade de receber salários maiores, fazendo com que o próprio colaborador venha cometer tal ato para prejudicar a organização.

Conforme exposto por Laudon e Laudon (2004) alguns dos problemas relativos à qualidade dos dados armazenados em sistemas de informação dentro de uma organização, tem como exemplo a organização Royal Bank of Canada que por meio de uma fraude sofreu um determinado ataque onde o banco de dados continham strings ‘frias’ assim relatado, tais fraudes eram feitas de modo que registrava o código de endereçamento postal, quando o funcionário não tinha o endereço correto dos clientes e isso fez com que fosse gerado um código postal para promover empréstimo em uma determinada área geográfica.

Laudon e Laudon (2004) ainda relatam que diversos estudos confirmam que 5 a 12 por cento das vendas que são realizadas por meio do código de barras em supermercados de varejo estão erradas, tal fator está relacionado à fraudes que são voltadas aos sistemas de informações, podendo ser por meio de hackers ou Engenheiro social. Até mesmo o próprio FBI em um estudo realizado descobriu que 54,1 por cento dos registros do National Crime Information Center System eram imprecisos por conta de fraudes.

A fraude dentro das organizações tem crescido e com ela a utilização da Engenharia Social está se tornando um fator essencial, como visto acima, por meio de técnicas de Engenharia Social é possível criar caminhos mais fáceis para chegar ao resultado esperado.

Comer (2011) elaborou um quadro abordando a frequência relativa dos meios de ataques mais comuns nas organizações, mostrando em qual tipo de organização ocorre com mais frequência, a forma que acontece e sua frequência relativa.

De acordo com o quadro trazido por Comer (2011) nos escritórios das empresas, consultores e nas residências dos diretores, os ataques ocorrem através do furto de lixo, entrevistas de pretexto, infiltração de agentes, roubo e vigilância, ocorrendo com muita frequência. Já nas salas de conselho e conferências e hotéis, são realizados por meio de escuta e vigilância, ocorrendo com média frequência, as linhas telefônicas, interruptores e celulares também ocorrem pelo mesmo meio, no entanto estas ocorrem com bem mais frequência.

2.3 VULNERABILIDADE DAS EMPRESAS FRENTE A ENGENHARIA SOCIAL

Sabe-se que as empresas vêm se preocupando cada vez mais com a sua segurança da informação e com o passar dos anos foram criando inúmeros métodos de proteção contra as diversas formas de ataques, dentre elas a engenharia social.

No entanto, apesar do grande avanço conseguido pelas empresas no que tange a proteção de seus dados e informações, ainda continua grande o número de ataques sofridos pelas empresas em decorrência da engenharia social, que vem sendo a técnica mais utilizada pelos cibercriminosos.

De acordo com Robert McMillan (Disponível em <https://www1.folha.uol.com.br/tec/2018/09/hackers-obtem-segredos-de-empresas-com-engenharia-social.shtml>. Acesso em 03 de outubro de 2019 às 07:20), hoje cerca de um terço dos ataques começam por engenharia social e há cinco anos, a proporção era de 19%. Esses ataques já causaram R$ 51,12 bilhões em prejuízos, com base nas informações do FBI.

Os dados são alarmantes de acordo com Fritzen (2018)

> A edição semestral do Relatório de Ameaças Cibernéticas 2018 da SonicWall, traz dados preocupantes em relação ao número de malwares, ataques de Ransomware e demais ameaças existentes. De acordo com o relatório, a quantidade de ataques vem crescendo em nível recorde desde 2017 e não mostrou sinais de redução no primeiro semestre de 2018. Somente nos dois primeiros meses de 2018 foram registrados 5,99 bilhões de ataques de malware em todo o mundo. Em relação aos ataques de Ransomware, que haviam reduzido entre 2016 e 2017, voltaram a crescer: somente no primeiro semestre de 2018 tivemos a quantia de 181,5 milhões de ataques, o que representa um crescimento de 229% em relação ao mesmo período de 2017.No Brasil, o número de ataques cibernéticos praticamente

> dobrou nos primeiros 6 meses de 2018. Nesse período foram detectados 120,7 milhões de ataques, o que representa um aumento de 95,9% em relação ao ano anterior. O Brasil também concentra 55% de todos ataques de Ransomware da América Latina, onde o principal foco são empresas. Em 2017 foram registrados 134 mil incidentes de Ransomware em empresas brasileiras. E como a maioria dos ataques de segurança não são relatados, estima-se que os incidentes fiquem perto de 350 mil. (Disponível em < https://www.profissionaisti.com.br/2018/10/seguranca-da-informacao-protecao-da-rede-sistemas-atualizados-e-educacao-dos-usuarios/>. Acesso em 02 de outubro de 2019 às 12:01).

Assim, em decorrência do crescente aumento do número de empresas vítimas de ataques de engenharia social, elas vêm investindo milhares de dólares na proteção de seus dados e informações, bem como têm se preocupado mais com esse tipo de situação e dificultando a atuação dos engenheiros sociais.

Robert McMillan (Disponível em <https://www1.folha.uol.com.br/tec/2018/09/hackers-obtem-segredos-de empresas-com-engenharia-social.shtml>. Acesso em 03 de outubro de 2019 às 07:30) conta que empresas como a Apple e a Microssoft investiram bilhões de dólares na melhoria da segurança de seus produtos e por outro lado os consumidores têm transferido grande parte de seus dados em serviços de computação em nuvem, dificultando assim a ação dos hackers.

De acordo com dados fornecidos pela TrendMicro (Disponível em <https://www.trendmicro.com/pt_br/business.html>. Acesso em 04 de outubro de 2019 às 13:04), empresa internacional voltada para a proteção da segurança da informação de outras empresas, os ataques de engenharia social tem aumentado a cada ano, assim os URL relacionados à phishing (técnica da engenharia social) bloqueados aumentaram ao longo dos anos, sendo que em 2015 o número era de 8.164,348, em 2016 subiu para 35.081,648, já em 2017 aumentou para 73.063,493 e em 2018 elevou-se ainda mais o número de URL bloqueados para 210.479,026.

Dessa forma, apesar do grande avanço conseguido no decorrer dos anos pelas organizações na proteção de seus dados e informações, pode-se dizer que ainda há uma grande vulnerabilidade das mesmas no que tange à ataques da engenharia social.

2.3.1 CARACTERÍSTICAS DA VULNERABILIDADE HUMANA EXPLORADAS PELO ENGENHEIRO SOCIAL

É cediço que o engenheiro social explora inúmeras vulnerabilidades humanas a fim de conquistar seu objetivo, logo, se ele encontra qualquer tipo de brecha, ele sabe usá-la da melhor forma para cumprir seu objetivo.

Gartner (2002, apud BALDIM, 2007, p.46) afirma que

> A Engenharia Social compreende em entender o comportamento humano, e nas habilidades de persuadir os outros para conseguir informações ou fingir que é outra pessoa. Persuasão por si mesma é uma arte e uma ciência; estudos mostram que humanos tem certas tendências de comportamento que são exploráveis por uma cuidadosa manipulação. Alguns indivíduos têm uma habilidade natural de manipular, enquanto outros desenvolvem essa habilidade através de prática usando reforços positivos, e negativamente.

Assim, o engenheiro social, que é um manipulador nato, sabe compreender como ninguém e entender o comportamento humano, logo, se ele percebe qualquer tipo de fraqueza humana, sabe se utilizar dela com maestria.

Gartner (2002, apud BALDIM, 2007, p.47) elaborou algumas características da vulnerabilidade humana que podem ser exploradas pelo Engenheiro Social**,** tais como a reciprocidade, coerência, aceitação social, simpatia, autoridade e escassez.

Quando se fala em reciprocidade, pode-se compreender que é a troca, ou seja, o engenheiro social instiga sua vítima fazendo com que esta se sinta obrigada a fazer alguma coisa com relação a isso.

Há a coerência quando o Engenheiro social faz algum tipo de pergunta a vítima que lhe possa ser útil em seu ataque, e a mesma vê-se coagida a responder.

Já a aceitação social é aquilo que todo mundo faz e por isso alguém se sente obrigado a fazê-lo também, assim se a vítima percebe que alguns colaboradores estão repassando informações importantes ao engenheiro social, ela vê-se obrigada a também repassar o que sabe.

Com relação a simpatia, essa é uma grande característica de vulnerabilidade, pois quando há uma pessoa simpática, geralmente ninguém consegue dizer não a essa pessoa, assim é o engenheiro social, uma pessoa aparentemente tão simpática que todos dizem sim ao que lhe pedem.

A autoridade é um fator que influencia muito, haja vista que se o Engenheiro social demonstra ter algum tipo de autoridade na organização, todos os colaboradores tendem a fazer o que ele manda.

Por fim, a escassez, que é um fator onde o Engenheiro Social se utiliza da escassez humana, ou seja, da falta de algo para a vítima, para apelar e fazer com que ela lhe entregue informações importantes.

2.3.2 FORMAS MAIS COMUNS DE SEGURANÇA QUE AS ORGANIZAÇÕES TÊM UTILIZADO ATUALMENTE PARA SE PREVENIR DE ATAQUES

Como explanado, as organizações com o passar do tempo vêm se preocupando mais com a proteção de seus dados e informações e para tanto, se utilizam de inúmeros métodos de segurança para se prevenirem de ataques.

Assim, algumas formas de prevenção são utilizadas frequentemente pelas organizações, tais como o uso de firewalls, assinatura digital, utilização da nuvem e uma maior preocupação com o hardware e software.

O uso de firewall é bastante utilizado pelas empresas, haja vista que visa assegurar o adequado funcionamento da comunicação, com o objetivo de impedir que sejam adulterados através de qualquer tipo de intrusão a comunicação entre a rede interna e externa.

As organizações também estão utilizando a assinatura digital para garantir integridade aos seus arquivos, uma vez que um arquivo é assinado digitalmente não pode ser alterado, sendo assim é uma forma de combater alterações maliciosas até a entrega do seu destinatário.

Hoje em dia o backup nas organizações tem se tornado algo rotineiro, cada empresa utiliza de meios diversos para fazer o backup de seus dados, uma maneira utilizada é a de salvar o backup de seus arquivos em nuvem, por meio de empresas que oferecem estes serviços, garantindo assim segurança de seus dados e a disponibilidade dos mesmos sempre que preciso. Assim as organizações estão evitando problemas como por exemplo: perder dados em servidores locais por causa de erro do usuário, vírus e entre outros motivos, perda de servidores por problemas físico do ambiente, incêndio, água e entre outros.

Cada vez mais as empresas estão buscando se adequar em um cenário mais tecnológico, buscando por melhorias em seus computadores, utilização de serviços de terceiros e isso só tem a tornar tanto o hardware e software de seus computadores mais eficazes no dia a dia. Essas medidas adotadas pelas empresas ainda são pouco seguras em comparação a ataques proporcionados por crackers e engenheiros sociais, assim, no decorrer do projeto será abordado meios alternativos e mais eficazes para se prevenir destes ataques.

2.3.3 A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO ATRAVÉS DO USO DE ISOS NAS ORGANIZAÇÕES

A organização Internacional de Normalização mais conhecida atualmente como ISO é uma entidade que busca reunir padronização/normalização, seus benefícios podem ser vários desde a gestão de qualidade, garantia de qualidade, segurança da informação e entre vários outros benefícios conforme a ISO utilizada.

A NBR ISO/IEC 27002 trata-se de um código de Prática para a Gestão de segurança da informação, tendo em vista que seu objetivo é voltado para implementar diretrizes e princípios de segurança da informação dentro de uma organização.

De acordo com o artigo publicado por Faria (Disponível em <https://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-1/>. Acesso em 06 de outubro de 2019 às 14:00) a NBR ISO/IEC 27002 – Código de Prática para a Gestão de Segurança, são distribuídas em 11 seções voltadas para a segurança da informação, sendo assim, as mais importantes voltadas para o controle

começam a partir da seção 5 até a seção 9 abordado em seu artigo, sendo essas: Seção 5 – Política de Segurança da Informação , Seção 6 – Organizando a Segurança da Informação, Seção 7 – Gestão de Ativos, Seção 8 – Segurança em Recursos Humanos, Seção 9 – Segurança Física e do Ambiente.

Ao tratar de segurança da informação dentro da organização, com a utilização da ISO supracitada, é importante olhar para essa seção apresentada com mais responsabilidade, porque são voltadas diretamente para a parte dos colaboradores e a organização sendo assim mais efetiva na questão de proteção se trabalhada de maneira correta.

Conforme apresentado pelo portal Seginfo (disponível em: https://seginfo.com.br/certificacoes-em-seguranca-da-informacao/. Acesso em 10 de outubro de 2019 às 20:00) em uma matéria publicada sobre certificação, existe uma certificação ministrada pela EXIN sendo a ISFS (Information Security Foundation) baseada na ISO 27002, ela é essencial em se tratando de segurança da informação, estando assim dividida em 10% no quesito de informação e segurança, 30% em ameaças e riscos, 10% em abordagem e organização, 40% em medidas e 10% em legislação e regulamentação.

Tanto a certificação ISFS (Information Security Foundation) quanto a ISO 27002 são essenciais para manter o padrão de segurança em uma organização, quando o assunto é a utilização de ISOS voltadas para segurança da informação em uma organização ou certificação de segurança da informação é uma opção excelente para adotar no ambiente da organização, sendo assim de extrema necessidade para as organizações nos dias atuais a utilização destas ou outras ISOS/Certificações para combater invasões e ataques.

2.2.4 PREPARAÇÃO DAS EMPRESAS PARA SE DEFENDER DESSE TIPO DE ATAQUE

Durante muito tempo, as organizações vêm sofrendo inúmeros ataques tanto por meio de suas redes de computadores, como também na internet, e com o decorrer

dos anos, elas passaram a ter uma evolução significativa no que tange a segurança da informação.

Assim, embora as organizações atualmente possuam um preparo maior para se defender dos inúmeros ataques proporcionados pelos crackers, termo designado a pessoas que se utilizam de meios árduos para invadir sistemas e coletar informações, estes estão se evoluindo cada vez mais ao longo do tempo, se utilizando de inúmeras técnicas para coletar dados das organizações, tal como a engenharia social utilizada para influenciar as pessoas a fim de coletar dados, passando desta forma a serem conhecidos como engenheiros sociais, que se utilizam da persuasão com o objetivo de aproveitar-se da ingenuidade ou falta de conhecimento das pessoas.

De acordo com uma pesquisa realizada por Rodrigues através da Kaspersky, empresa especialista em segurança da informação (Disponível em: <https://www.kaspersky.com.br/blog/brasil-ataques-phishing/11826/>. Acesso em 10 de outubro de 2019 às 17:00) o Brasil foi o país que mais sofreu em relação a ataques de phishing no primeiro trimestre de 2019 chegando a 22% se levado em comparação ao 1º trimestre de 2018 com 19%. Outros países também são apresentados também como a Austrália com 17% e Espanha 17%.

Conforme a pesquisa supracitada, esse aumento de ataques de phishing é derivado de anúncios falsos na internet de oferta de emprego, sendo assim uma maneira fácil de pessoas caírem nesse tipo de ataque, as vítimas podem ser até mesmo pessoas já empregadas em busca de novas condições de trabalho.

A Ecoit empresa de segurança digital (Disponível em: <https://ecoit.com.br/3-casos-de-empresas-que-sofreram-por-nao-ter-backup-profissional-em-nuvem/>. Acesso em 10 de outubro de 2019 às 12:40) aborda em seu artigo que a empresa Uber em outubro de 2016 teve dados e mais de 56 milhões de usuários do aplicativo roubados, tais dados incluíam nomes, e-mail, número e celular. O ataque deu origem por meio de colaboradores que trabalhavam na empresa.

É possível ver que ataques relacionados a engenharia social são realizados de diversas maneiras, como por exemplo ataques voltados para usuários no dia a dia, podendo ser estes os colaboradores de uma determinada organização quando utilizam seus computadores pessoais a fim de obter informações importantes relacionadas à organização, ou até mesmo a própria organização por meio de pessoas infiltradas, utilizando de técnica da engenharia social como a abordagem pessoal para facilitar ataques de maiores proporções para roubar informações.

Percebe-se então, que os ataques de engenharia social vêm se tornando cada vez mais comuns, principalmente dentro das organizações, haja vista a facilidade encontrada na disponibilidade da internet para todos, logo ocorre também uma maior dificuldade por parte das empresas em se protegerem de ataques.

Com a popularização da internet atualmente é mais fácil a realização de ataques de Engenharia social, o que dificulta ainda mais a proteção por parte das organizações, por isso é preciso a adoção de normas de proteção e a utilização de meios para se prevenirem de tais ataques.

Por mais que ataques como estes estejam crescendo cada vez mais, são poucas as empresas que adotam a utilização de Firewall, antivírus, Proxy, servidores de backup entre outros meios de prevenção dentro da organização.

Assim, embora as empresas atualmente com o crescente número de ataques relacionados a engenharia social tenham um maior conhecimento acerca dos meios de proteção, muitas vezes elas acreditam que não serão uma provável vítima, e só realmente passam a se preocupar após o primeiro ataque.

Para Balloni, (2014, apud MAULAIS, 2016, p. 51),

> Os especialistas acreditam que mais de 90% dos ataques cibernéticos bem-sucedidos poderiam ter sido evitados usando a tecnologia disponível no momento em que ocorreram. Foi a atenção humana inadequada que possibilitou que prevalecessem com Engenharia Social.

Dessa forma, destaca-se que a maior parte das empresas que possuem proteções eficazes contra os ataques de engenharia social, são aquelas que já

sofreram algum tipo de ataque, e na tentativa de se protegerem de posteriores ataques, criam métodos eficazes de proteção.

Uma das maiores dificuldades encontradas pelas organizações no que tange a proteção de seus dados é exatamente pelo grande custo econômico que essa proteção acrescenta à empresa, haja vista que como é cediço, serviços e assinaturas eficazes possuem um custo econômico maior.

De acordo com Sêmola

> Há casos em que o custo de implementação de medidas de segurança para evitar ou reduzir determinado risco é maior do que o valor da informação a ser protegida, desaconselhando que essa ação seja efetuada (2014, p. 47).

Desta feita, as empresas por vezes contratam serviços mais baratos ou até mesmo gratuitos, acreditando está fazendo a escolha certa, no entanto, os prejuízos após os ataques são bem maiores que o custo de um serviço de proteção eficaz, caso tivesse sido contratado anteriormente.

Allison Souza explica que

> Muitas empresas ainda não seguem parâmetros adequados da Segurança da Informação e, por esse motivo, sofrem com diversos tipos de ameaças virtuais - tão nocivas quanto a engenharia social. Para isso, existem muitas soluções e métodos aconselháveis que cabem perfeitamente no ambiente corporativo. (2017. Disponível em: <https://ostec.blog/geral/engenharia-social-impactos>. Acesso em 21 de outubro de 2019 às 08:00)

Nos serviços de proteção de dados são cobrados assinaturas mensais e as empresas na tentativa de “economizarem” e evitarem ter um débito a mais todo mês, acabam contratando serviços ou produtos piratas.

Um bom exemplo disso é a assinatura de firewall, disponibilizada por empresas do ramo, manutenção de um serviço de assistência técnica mensalmente por uma empresa especialista, ter antivírus licenciados, windows genuínos, haja vista que se uma empresa possui computadores com windows não genuínos ou outros programas não licenciados corre sérios riscos de ter sua segurança comprometida por facilitar a entrada de invasores no seu sistema operacional.

Outro fator crucial para que as empresas não estejam devidamente preparadas é com relação ao fator humano, visto que por vezes as empresas investem muito dinheiro em tecnologias de segurança da informação e acabam se esquecendo da sua principal vulnerabilidade, que é o fator humano. Costa explica que,

> Apesar de grandes investimentos na área de segurança, grande parte das empresas ainda não está preparada para lidar com este tipo de problema. Independentemente do sistema de segurança adotado, há sempre um elemento mais vulnerável e principal alvo destes procedimentos criminosos, o ser humano. (2017. Disponível em < http://micreiros.com/engenharia-social-nas-empresas/ > Acesso em 21 de outubro de 2019 às 19:40)

O ser humano tende a ser falho e na maioria das vezes o engenheiro social se utiliza dessas fraquezas humanas para aplicar seu golpe, e como por vezes a organização não investe no treinamento adequado dos funcionários, estes tornam-se as vítimas perfeitas.

Logo, pode-se compreender que as organizações ainda não estão completamente preparadas para se protegerem desse tipo de ataque, embora já estejam no caminho certo, ainda falta um longo caminho a ser percorrido para conseguirem diminuir ainda mais o número de ataques de engenharia social.

Para tanto, é importante todas as organizações terem consciência dos inúmeros prejuízos que ataques relacionados a engenharia social podem causar em uma empresa, assim é importante ter em vista que a melhor forma de combate a engenharia social ainda é a proteção dos dados, assim recomenda-se o uso de produtos originais e programas licenciados.

2.2.5 MEIOS PREVENTIVOS DE COMBATE A ATAQUES E INVASÕES

É cediço que a maior forma de combate a ataques e invasões relacionados a engenharia social é através da prevenção, pois através da mesma há uma maior proteção dos dados e informações de uma organização.

Maulais afirma que,

> Estar seguro é uma necessidade na atualidade. Seja segurança física, material e digital. Sobretudo a digital, pois hoje as organizações dependem dos computadores e da Internet para atividades cotidianas, como buscar

> informações de clientes e fornecedores em sites, acessar homepages de bancos e até mesmo sistemas de gestão empresarial disponibilizado para funcionários acessarem externamente. (2016, p. 51)

Um dos maiores meios de prevenção que podem ser eficazes no combate a engenharia social são as medidas de segurança, que visam impedir ataques e invasões, ou até mesmo reduzir o prejuízo, caso ocorra algum tipo de ataque.

De acordo com Sêmola,

> As medidas de segurança são as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, reduzir essas vulnerabilidades, limitar a probabilidade ou o impacto de sua exploração, minimizando ou mesmo evitando os riscos. (2014, p.47)

Assim, entende-se que as medidas de segurança são uma forma de controle, bem como uma forma de evitar a exploração de vulnerabilidades das organizações ou reduzir o impacto causado com a descoberta de tais vulnerabilidades.

Marcos Sêmola (2014) explica que há três características das medidas de segurança que podem ser eficazes para uma organização, sendo elas as preventivas, que são aquelas que visam evitar que ameaças venham a ocorrer, realizada através de campanhas de conscientização, palestras, etc; as detectivas, que são aquelas que visam identificar indivíduos ou condições que possam vir a ser uma ameaça, ocorrendo através de câmeras de segurança, alarmes, etc; as corretivas, que são as ações voltadas a correção das estruturas para o fim de se adaptar com as formas de segurança, realizada através de equipes para emergências e plano de recuperação de desastres.

É importante ter em vista que quando se fala em prevenção, não basta somente a organização procurar meios de segurança através das tecnologias, mas também é muito importante que invistam em treinamento de seus funcionários, pois em muitos casos a engenharia social ocorre por meio de alguém que trabalhe na empresa. Para Maulais

> A segurança tecnológica deve ser utilizada, tanto quanto possível para proteger o hardware, software e redes. Isso pode incluir criptografia, protocolos de segurança, firewalls e software antivírus. (2016, p. 52)

O primeiro passo para evitar que ataques de engenharia social ocorram é a empresa se conscientizar de que nenhuma empresa está imune a ataques desse tipo e estes estão ocorrendo cada vez com mais frequência. Após essa conscientização por parte do dono da empresa, é importante que ocorra uma conscientização por parte do quadro de funcionários, que pode ser feito através de palestras frequentes, reuniões mensais e informações necessárias para que entendam do que se trata.

Uma importante forma de combate à engenharia social é através do treinamento presencial, o qual é realizado de forma interativa e dinâmica de modo a treinar os funcionários para saberem lidar e se prevenir de ataques relacionados à engenharia social.

Assim explica Mann,

> Reunir um grupo de funcionários para uma sessão de treinamento presencial e interativa é uma das maneiras mais eficazes de desenvolver sua segurança da informação. Isso, obviamente, presumindo-se que o conteúdo seja interessante e relevante e também que a maneira como é passado seja divertida e criticamente memorável. (2011, p. 194)

Importante ressaltar, que as novas tecnologias também ajudam muito no combate a engenharia social, seja através de antivírus adequados, firewall, proxy, uso de biometria e sistemas que detectam invasores.

Outra importante forma de prevenção é através da conexão segura e da criptografia, haja vista que esta tem como objetivo proteger os dados de uma forma segura que somente a pessoa que utilizou da criptografia consiga saber o real conteúdo por traz da mesma, impedindo assim que o Engenheiro social obtenha tais dados sigilosos para se utilizar contra a vítima.

Conforme explica Braga,

> Um comportamento simples, mas eficiente no combate à Engenharia Social é a atenção a segurança da conexão e o não envio de dados sigilosos em uma conexão insegura. Uma conexão criptografada impede que um terceiro obtenha dados de uma vítima e use-os contra ela em um posterior ataque de Engenharia Social. (2010, p. 7)

Esse também é o entendimento de Terada,

> Algoritmos criptográficos basicamente objetivam “esconder” informações sigilosas de qualquer pessoa desautorizada a lê-las, isto é, de qualquer pessoa que não conheça a chamada chave secreta de criptografia. (2008, p.18)

Atualmente a maioria dos navegadores, informam se a conexão do usuário é segura ou não, e nos casos em que são seguras, informam o tipo de criptografia utilizada.

Assim informa Braga,

> Para auxiliar o usuário a maioria dos navegadores atuais mostra se a conexão é criptografada e, caso positivo, o tipo da criptografia empregado. Também é recomendado o uso de protocolos seguros no referente ao acesso remoto, como por exemplo o uso do SSH em detrimento do TELNET, uma vez que esse último não garante por padrão a segurança da conexão. (2010, p. 7)

Outra forma de prevenção é através da visitação em sites com certificação digital, visto que quando uma página possui um certificado digital válido, o próprio navegador indica se esta é válida ou não, caso seja positiva a validade, é sinal de que o site é confiável, caso contrário há uma grande chance de o site ser uma fraude.

Braga explica que

> Entidades certificadoras são instituições responsáveis pela emissão de certificados digitais que identificam sites na Internet e seus respectivos proprietários. Ao assinar digitalmente os certificados que emite, a entidade certificadora relaciona a identidade do portador do certificado, e portanto da chave privada, à chave pública existente no certificado. A maioria dos navegadores exibem se a página visitada possui um certificado digital válido, caso não possua, o site provavelmente é uma fraude. (2010, p. 7)

Nota-se a importância de os empresários e os funcionários terem bom senso, responsabilidade e atenção, haja vista que a maior parte dos ataques de engenharia ocorrem por negligência do quadro de colaboradores, que por algum deslize acabam repassando informações importantes da empresa que possam ser uteis nos ataques do engenheiro social.

Um bom conselho dado por especialistas na área de proteção à segurança da informação é para que os empresários e funcionários usem senhas fortes e extensas, difíceis de serem acertadas, como por exemplo senhas com letras maiúsculas, minúsculas e contendo números.

Nas palavras de Braga,

> Jamais use senhas constituídas de informações pessoais que possam ser descobertas por um engenheiro social. Números de CPF ou RG, datas de aniversário, nomes de amigos ou familiares, endereços, o nome de um time de futebol e o próprio *login* são exemplos de senhas que um atacante descobrirá rapidamente. Prefira senhas extensas, com letras em caixa-alta e baixa, números e caracteres especiais. (2010, p. 8)

Assim, algumas simples atitudes realizadas pelas organizações podem ser muito eficazes na tentativa de combate a engenharia social, tais como a realização periódica de palestras aos funcionários, treinamentos adequados, realizar testes de invasão com frequência, enfim, ter uma rígida política de segurança e uma maior atenção por parte dos colaboradores.

É importante destacar também que as empresas devem se atentar ao uso de produtos originais, serviços devidamente licenciados, realizar a avaliação de TI com uma maior frequência, utilizar antivírus adequados, dentre outras medidas que podem ser muito eficazes.

Mister ressaltar que o processo de conscientização dos colaboradores no combate a engenharia social ocorre de forma lenta e minuciosa, e que todo esse processo de prevenção não irá ocorrer de um dia para o outro, mas sim ocorrerá aos poucos, através da participação de todos os colaboradores, haja vista que ainda não há uma solução imediata contra a engenharia social, mas sim há diversas formas de prevenção que podem ser eficazes se usadas corretamente.

METODOLOGIA

Em razão das peculiaridades da problematização e dos objetivos que se pretendem alcançar; a pesquisa monográfica referente a este projeto tem como proposta o seu desenvolvimento mediante o método dedutivo, tendo em vista que oferece uma base lógica ao tema em questão, partindo primeiramente do histórico das organizações no que tange a organização dos seus dados, conceito de dados, informações e engenharia social, bem como suas principais técnicas utilizadas e consequências em uma empresa que sofre esse tipo de ato, como também as formas de segurança que as organizações têm utilizado, levando a uma conclusão acerca da preparação ou não das organizações com relação a tais ataques. Os resultados serão apresentados de forma qualitativa, baseada em informações e dados.

O estudo será realizado a partir de pesquisas bibliográficas, através de autores como Idalberto Chiavenato, Marcos Sêmola, Mário Cesar Pintaudi Peixoto e Kevin D. Mitnick, bem como através de buscas por artigos científicos e revistas especializadas, visando analisar o problema em torno da engenharia social.

Nesse sentido, ter-se-á o desenvolvimento da pesquisa sob as do tipo bibliográfica, tendo em vista que para o processo de conhecimento proposto na metodologia supracitada, referente ao tema e a problematização discorridos neste trabalho, será necessário fazer uma pesquisa nas leituras de textos bibliográficos.

3. CONSIDERAÇÕES FINAIS

Como explanado, com o surgimento da era da informação, as empresas tiveram que encarar novos desafios, haja vista que a tecnologia passou a ter um maior avanço, facilitando o acesso não tão somente as organizações, mas também aos usuários.

Assim, com esse avanço, começaram a surgir também algumas vulnerabilidades que passaram ser utilizadas por pessoas de má fé, na tentativa de captar dados e informações de uma organização. Dessa forma, surgiu a engenharia social que é a técnica para obtenção de informações importantes, e esta passou a ser utilizada com cada vez mais frequência, trazendo inúmeros prejuízos às empresas.

O engenheiro social é uma pessoa manipuladora, por isso ele consegue tão facilmente captar dados que lhe possam ser úteis nos seus ataques, haja vista que ele consegue ganhar a confiança de todos e por vezes o engenheiro social é o próprio funcionário da empresa.

Os ataques mais comuns que ocorrem atualmente são através do phishing, por meio telefônico ou eletrônico, análise de lixo, abordagem pessoal e por meio da internet.

A engenharia social traz inúmeros prejuízos para uma organização, haja vista que muitas empresas após sofrerem algum tipo de ataque, não conseguem se reerguer, ocasionando assim o fechamento da mesma.

Diante de todo o exposto no presente trabalho conclui-se que a Engenharia social está ocorrendo com grande frequência, onde inúmeras organizações estão tendo seus dados e informações roubados e expostos.

Pode-se dizer que apesar de esta ocorrendo com grande frequência, muitas empresas ainda não estão preparadas para se defender desse tipo de ataque, pois muitas acreditam que não são uma vítima em potencial, no entanto é importante frisar que ninguém está imune a esses tipos de ataques.

Embora as empresas atualmente possuam um maior preparo para lidar com esses tipos de ataques, percebe-se que ainda não tem sido suficientes para a proteção de seus dados, haja vista que por muitas vezes as empresas acham muito grande o custo para manter uma medida de segurança e acabam usando produtos não licenciados ou optando por serviços gratuitos sem segurança, o que acaba ocasionando inúmeros prejuízos, haja vista que estes não são eficazes no combate a engenharia social.

Dessa forma, faz-se cada vez mais necessário uma maior precaução por parte das organizações, através da conscientização tanto dos diretores como também do quadro de funcionários.

Assim, os meios mais eficazes de proteção dos dados são através do treinamento adequado dos funcionários, realização de palestras, uso de firewall, uso de produtos genuínos, serviços devidamente licenciados ou por meio da contratação de serviços de empresas especializadas na área da tecnologia da informação, realização periódica de palestras aos funcionários, treinamentos adequados, realizar testes de invasão com frequência, enfim, ter uma rígida política de segurança e uma maior atenção por parte dos colaboradores.

REFERÊNCIAS

AURELIO. **O mini dicionário da língua portuguesa**. 4ª ed. Revista e ampliada do mini dicionário Aurélio. 7ª impressão. Rio de Janeiro, 2002.

BALDIM, Natália Pimenta. **Engenharia social e segurança da informação no ambiente corporativo: uma análise focada nos profissionais de secretariado executivo.** 2007. Trabalho de Conclusão de Curso - Universidade Federal de Viçosa, Minas Gerais: 2007.

BRAGA, Pedro Henrique da Costa. **Técnicas de Engenharia social**. 2010. Trabalho de Conclusão de Curso - Universidade Federal do Rio de Janeiro, Rio de Janeiro: 2010.

CHIAVENATO, Idalberto. **Iniciação a sistemas, Organizações e métodos: So&m**. São Paulo: Manoele, 2010.

COMER, Michael J. **Fraudes corporativas**. São Paulo: Blucher, 2011.

COSTA, Everton Junior da Silva. **Engenharia social nas empresas**. Disponível em <http://micreiros.com/engenharia-social-nas empresas/?fbclid=IwAR2yGTKRRu7H36S-0_7W-LdPsmSE8khL7AuyPaGngY5_xVJZUzjP4n6Z598>. Acesso em: 30 outubro 2019.

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

ECOIT, Segurança Digital. **3 casos de empresas que sofreram por não ter backup profissional em nuvem**. Disponível em:< https://ecoit.com.br/3-casos-de-empresas-que-sofreram-por-nao-ter-backup-profissional-em-nuvem/>. Acesso em: 06 outubro 2019.

FARIA, Alexia Lage de. **Conheça a NBR ISO/IEC 27002 – Parte 1**. Disponível em:< https://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-1/>. Acesso em: 06 outubro 2019.

FERREIRA, Nicholas. **O Guia do Hacker**. [S.I.:s.n.], 2014.

FRITZEN, Cledson Eduardo. **Segurança da informação nas empresas: proteção da rede, sistemas atualizados e educação dos usuários**. Disponível em:< https://www.lumiun.com/blog/seguranca-da-informacao-nas-empresas-protecao-da-rede-sistemas-atualizados-e-educacao-dos-usuarios/>. Acesso em: 23 agosto 2019.

HOSTINGER, Hospedagem de Sites. **DDoS: o que é, como funciona e como se proteger de ataques maliciosos na internet**. Disponível em <https://www.hostinger.com.br/tutoriais/o-que-e-ddos-e-como-se-proteger-de-ataques?fbclid=IwAR2NuzOq4Kac9Guwrl0DA6yFDdQgr46B8k9J0CJxZxqip75FuvOKgkvgpE0>. Acesso em: 22 setembro 2019.

LAUDON, Kennth C; LAUDON, Jane P. **Sistemas de informação gerenciais: administrando a empresa digital**. 5ª ed. São Paulo: Prentice Hall, 2004.

LYRA, Mauricio Rocha. **Governança da Segurança da Informação**. Brasília:[s.n.], 2015.

MANN, Ian. **Hacking the human**. São Paulo: Blucher, 2011.

MAULAIS, Claudio Nunes dos Santos. **Engenharia social: técnicas e estratégias de defesa em ambientes virtuais vulneráveis**. 2016. Projeto de pesquisa - Universidade FUMEC, Belo Horizonte:2016.

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

MITNICK, Kevin D.; SIMON, William L. **A Arte de invadir: As verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos**. São Paulo: Pearson Prentice Hall, 2005.

MÜLLER, Léo. **O que é Phishing?.** Disponível em: <https://www.tecmundo.com.br/phishing/205-o-que-e-phishing-.htm>. Acesso em: 26 setembro 2019.

MCMILLAN, Robert. **Hackers obtêm segredos de empresas com engenharia social.** Disponível em: < https://www1.folha.uol.com.br/tec/2018/09/hackers-obtem-segredos-de-empresas-com-engenharia-social.shtml>. Acesso em: 29 setembro 2019.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Futura, 2003.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. **Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas**. 2007. Trabalho de conclusão de Curso - Universidade Municipal de São Caetano do Sul, São Caetano do Sul: 2007.

NOVAES, Rafael. **Botnet x Backdoor: o que são e como se prevenir**. Disponível em:< https://www.psafe.com/blog/botnet-x-backdoor-sao-como-prevenir/>. Acesso em: 15 setembro 2019.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

PEREIRA, Eliézer. **Fator humano em segurança da informação**. Disponível em: <https://www.lexmachinae.com/2018/01/04/fator-humano-em-seguranca-da-informacao/ >. Acesso em: 18 agosto 2019.

RODRIGUES, Renato. **Brasil é o País com mais usuários atacados por phishing**. Disponível em:<https://www.kaspersky.com.br/blog/brasil-ataques-phishing/11826/>. Acesso em: 06 outubro 2019.

RAFAEL, Gustavo de Castro. **Engenharia Social: as técnicas de ataques mais utilizadas**. Disponível em: < https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/ >. Acesso em: 01 setembro 2019.

REVISTA DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO. São Caetano do Sul: [s.n.], v.4,n.3, ago./out.2007. ISSN 1807-1775.

ROSA, Adriano Carlos; SILVA, Bruno Donizete da; SILVA, Pedro Lemes da. **Análise de redes sociais aplicada à engenharia Social.** In: Anais do I SINGEP. São Paulo, SP, Brasil,2012. Disponível em <https://repositorio.uninove.br/xmlui/handle/123456789/163>. Acesso em: 20 outubro 2019.

SEGINFO, Portal, Podcast e Evento sobre Segurança da Informação. **Certificações em Segurança da Informação**. Disponível em:< https://seginfo.com.br/certificacoes-em-seguranca-da-informacao/>. Acesso em: 06 outubro 2019.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva da segurança da informação.** Rio de Janeiro: Elsevier, 2014.

SILVA, Carlos Alberto. **Elo mais fraco da segurança da informação: Pessoas representam o maior desafio**. Minas Gerais: Amazon, 2015.

SOUZA, Raul Carvalho. **Prevenção para ataques de engenharia social.** Tese de Doutorado - Universidade de Brasília, Brasília: 2015.

SOUZA, Állison. **Engenharia social e os impactos no meio corporativo**. Disponível em <https://ostec.blog/geral/engenharia-social-impactos?fbclid=IwAR3Bc26I1IwpSzgrDoSmX9okSjGaXPLc_2jlVSrFwnAvrdaIS5gg53AY7eE> Acesso em 30 outubro 2019.

TERADA, Routo. **Segurança de dados: criptografia em redes de computador**. 2 ed. São Paulo: Blucher, 2008.

TOWNSEND, Kevin. **Quando os cibercriminosos usam fraudes para invadir sua própria mente.** Disponível em: < https://blog.avast.com/pt-br/social-engineering-hacks >. Acesso em: 10 setembro 2019.

TRENDMICRO, Incorporated. Dealing With Pervasive and Persistent Threats. Disponível em:< https://www.trendmicro.com/pt_br/business.html>. Acesso em: 26 agosto 2019.

ZOLDI, Scott. **Machine learning contra fraudes de engenharia social**. Disponível <https://computerworld.com.br/2018/10/17/machine-learning-contra-fraudes-de-engenharia-social/> Acesso em 30 outubro 2019.

APÊNDICE- A PROJETO DE PESQUISA

RODRIGO DA COSTA SILVA

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UMA ANÁLISE SOBRE AS TÉCNICAS DE ENGENHARIA SOCIAL APLICADAS PARA OBTER INFORMAÇÕES.

Ji-Paraná
2019

RODRIGO DA COSTA SILVA

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE CORPORATIVO: UMA ANÁLISE SOBRE AS TÉCNICAS DE ENGENHARIA SOCIAL APLICADAS PARA OBTER INFORMAÇÕES.

Projeto de pesquisa apresentado ao Centro Universitário São Lucas Educacional, para obtenção de grau na disciplina Trabalho de Conclusão de Curso I, no curso de Sistemas de Informação, sob orientação do Professor especialista Jose Olivas Jose Rodolfo Milazzotto Olivas.

Ji-Paraná
2019

SUMÁRIO

1 INTRODUÇÃO

Trata-se de um projeto de pesquisa, cujo assunto está relacionado à área do conhecimento pertencente à segurança da informação, onde serão abordados os conceitos relacionados ao ambiente corporativo, mostrando como a Engenharia Social é aplicada para roubar dados de empresas e obter vantagens de forma ilícita.

No tocante ao objetivo do presente trabalho, constituirão em inúmeras pesquisas em livros, artigos científicos pertinentes ao assunto em questão, a fim de desenvolver o caminho para a produção do tema em questão.

Propõe-se no presente projeto, uma investigação acerca das técnicas mais utilizadas na engenharia social, como a Análise de lixo, Internet e Rede Social, Contato Telefônico, Abordagem Pessoal, Phishing e Falha Humana e as formas de proteção mais eficazes, como evitar abrir e-mail recebido de pessoas/empresas desconhecidas, não passar dados privados relacionados à empresa por telefone, bem como se atentar com extensões de arquivos e programas ao fazer instalações nos computadores e sempre que tiver dúvida de terminada solicitação procurar pelo supervisor.

A solução da problematização levantada no presente projeto é de suma importância para o estudo da luta e combate a engenharia social, haja vista que ataques como os da engenharia social têm crescido cada vez mais, uma vez que o fator de manipulação humana é mais vulnerável para ser quebrado dentro de uma organização, sendo assim mais fácil obter dados e vantagens.

Deste modo, o seguinte projeto será produzido a partir da questão gerada com o aumento do número de empresas que vem sofrendo os referidos ataques.

Por fim, com este projeto busca-se efetuar uma pesquisa detalhada para descobrir se as empresas estão preparadas para se proteger dessa técnica utilizada para roubar dados, bem como analisar se existem medidas de segurança nas organizações que busquem de forma efetiva bloquear determinados ataques.

2 PROBLEMATIZAÇÃO

Durante muito tempo, as organizações vêm sofrendo inúmeros ataques tanto por meio de suas redes de computadores, como também na internet, e com o decorrer dos anos, as mesmas passaram a ter uma evolução significativa no que tange a segurança da informação.

Assim, embora as organizações atualmente possuam um preparo maior para se defender dos inúmeros ataques proporcionados pelos crackers, termo designado a pessoas que se utilizam de meios árduos para invadir sistemas e coletar informações, estes estão se evoluindo cada vez mais ao longo do tempo, se utilizando de inúmeras técnicas para coletar dados das organizações, tal como a engenharia social utilizada para influenciar as pessoas a fim de coletar dados, passando desta forma a serem conhecidos como engenheiros sociais, que se utilizam da persuasão com o objetivo de aproveitar-se da ingenuidade ou falta de conhecimento das pessoas.

Desta forma, surge a seguinte problemática em torno do tema em questão: As organizações estão preparadas para esse novo tipo de técnicas utilizadas para coletar dados?

3- HIPÓTESES

- É possível que se conclua, numa primeira hipótese, após o desenvolvimento monográfico, que as organizações não estão preparadas para esse novo tipo de técnicas utilizadas para coletar dados, haja vista que a engenharia social visa atacar diretamente o fator humano dentro de uma organização sendo assim imprevisível medir o quão seguro uma organização pode estar, pelo fato de que nem todos colaboradores podem seguir as medidas de segurança interna da organização.

- Numa segunda hipótese é possível que se conclua que no decorrer dos anos, as empresas conseguiram sim criar mecanismos de combate a esse tipo de técnicas, visto que cada vez mais organizações tem adotado medidas internas de segurança visando não só na parte de softwares, mas também medidas voltadas para parte humana, restringindo acesso em determinados sites, não passar informações sigilosas por telefone, evitar abrir links por e-mail que não seja conhecidos e etc.

4 Objetivos

4.1 Geral

Analisar as técnicas mais comuns utilizadas na engenharia social para coletar dados das organizações.

4.2 Específicos

- Compreender o histórico das organizações no que tange a organização dos seus dados;
- Compreender o que é dado e o que é informação;
- Identificar as principais técnicas utilizadas através da engenharia social para obter dados na empresa;
- Analisar as formas de segurança que as organizações têm utilizado para se prevenir de ataques relacionados à segurança da informação no que tange a engenharia social;
- Analisar as ameaças mais comuns direcionadas às organizações;
- Identificar meios preventivos de combate a ataques e invasões que estão sendo uteis atualmente;
- Comparar a técnica de engenharia social utilizada para roubar informações com os demais métodos utilizados para roubar dados dentro de uma organização;
- Analisar a politica de segurança da informação através do uso de ISOS nas Organizações;

- Avaliar se as empresas estão preparadas para se defender desse tipo de ataque de engenharia social no seu cotidiano.

5 Justificativa

O presente trabalho justifica-se tendo em vista o crescente aumento de coleta de dados de forma ilegal nas organizações, através da técnica de engenharia social, que acabam por gerar inúmeras consequências à aquelas, dentre as quais se destacam a descoberta de dados sigilosos e a utilização de tais dados para obtenção de recursos financeiros.

Diante disso, faz-se de extrema necessidade o estudo acerca desse tema, com o principal objetivo de analisar como as organizações vêm se comportando durante o passar do tempo, e quais meios estas estão utilizando como forma de prevenção e combate a estes tipos de ataques, que acabam por deixar as organizações desprotegidas e vulneráveis a novos ataques, tendo em vista que uma vez que ocorreu o primeiro ataque, esta passa a se tornar um alvo fácil a próximos ataques, bem como passa a ter sua imagem manchada perante os clientes e colaboradores.

Portanto, o presente trabalho visa ajudar as organizações que já sofreram ou possam vir a sofrer ataques desse tipo, com o objetivo de ajudá-las a se prevenir, se utilizando de técnicas abordadas no presente trabalho e como estas podem ter eficácia no combate à engenharia social.

6 Referencial teórico

Na década de 90, com o advento da era da informação, as organizações saíram do modelo tradicional vindo da era industrial e passaram a encarar novos desafios nos negócios. A partir desse momento as organizações tiveram que acompanhar o ritmo das inovações daquela época, de tal modo que acabou por ocasionar um cenário no mundo dos negócios mais dinâmico e com fácil potencial de mudanças, porque a tecnologia teve como importante papel estimular essas mudanças conforme necessidades organizacionais.

Com tantas mudanças acontecendo e tornando cada vez mais competitivo o mundo dos negócios na época, era imprescindível que as organizações tivessem que reestruturar a sua forma de gerir o negócio, tanto no que tange a estrutura voltada para parte de gestão, quanto para a parte de relação com os clientes.

Chiaventato (2010, p.97) aborda em um quadro os quatros componentes da função de organizar assim denominados por ele na época, sendo estes as tarefas, pessoas, órgãos e relações.

Dessa forma, a parte de relações é voltada para adesão de sistemas de informações com foco para aproximar as organizações com o cliente e os fornecedores, utilizando o CRM – Customer RelationShip Management para armazenar os dados dos clientes e futuramente utilizar desses dados para gerir informações importantes para o negócio e o SCM – Supply Chain Management para guardar dados de seus fornecedores.

Com a evolução da tecnologia nos anos 90 não somente nas organizações, mas também para o uso de usuários em suas residências com a utilização da internet, a tecnologia começou a ter um avanço mais rápido ainda.

De acordo com Silva (2015) hoje em dia a tecnologia evoluiu tanto ao ponto que o acesso a essas informações são feitas por meio de dispositivos eletrônicos que possuem diversos sistemas de informações, tais sistemas tem como objetivo organizar os dados e transformar em informações assim como antigamente as

organizações começaram a utilizar sistema para melhorar o relacionamento com seus clientes e fornecedores hoje em dia esse processo pode ser organizado de maneira mais prática por meio de smartphones, notebooks, computadores e demais dispositivos eletrônicos.

Desta feita, o fácil acesso a informação por meio de diversos dispositivos eletrônicos trouxe também algumas preocupações para as organizações em proteger seus dados.

Conforme defendido por Silva (2015) o objetivo da segurança da informação é garantir que os dados das organizações, sejam guardados de forma segura, assim pessoas que não tenha autorização para ter acesso a esses dados não poderão utilizá-los sem permissão.

Pode-se dizer então, que dado é todo conteúdo que não relacionado a outro conteúdo, não agrega valor algum e a informação é todos os dados relacionados e organizados que gera algum valor tornando assim uma informação.

Estando agora as organizações inseridas em um contexto tecnológico onde toda sua informação gerida por meio dos seus sistemas de informações é tão valiosa, surgem pessoas mal-intencionadas conhecidas como crackers. Para Ferreira a definição de cracker é:

> “Não muito conhecido pelas pessoas, o cracker, ou black hat (chapéu preto), é praticamente o hacker do mal. Os crackers são indivíduos também com amplo conhecimento em informática, mas que usam esse conhecimento para quebrar sistemas de segurança a fim de obter vantagens ilícitas.” (Ferreira, 2014, p.4).

Os crackers têm como objetivo captar dados sigilosos, novos meios de roubar dados começou a ser utilizados, como ataques às redes de computadores das mesmas, enviando vírus e outros ataques.

Em contrapartida, com o passar do tempo, no intuito de se protegerem, as organizações foram adotando técnicas para evitar tais ataques como a utilização de Antivírus, Firewall entre outros meios de segurança da informação.

Com a evolução na parte de segurança da informação por meio das organizações, novas técnicas começaram a surgir, como por exemplo, a “Engenharia Social”, conforme define Nakamura e Geus,

> “A engenharia social é a técnica que explora as fraquezas humanas e sociais, em vez de explorar a tecnologia. Ela tem como objetivo enganar e ludibriar pessoas assumindo-se uma falsa identidade, a fim de que elas revelem senhas ou outras informações que possam comprometer a segurança da organização” (2003, p. 70).

A Engenharia Social, técnica utilizada para influenciar pessoas por meio da persuasão, é destinada para roubar dados de organizações e pessoas, conforme tais dados sejam coletados. MITNICK afirma que:

> “A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado,o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.” (2003, p.8).

Assim, tais pessoas mal-intencionadas que fazem uso dessa técnica para roubar dados ficaram conhecidas como Engenheiro Social. Peixoto (2006) define que o Engenheiro Social na maioria das vezes são pessoas agradáveis.

O efeito que o uso dessa técnica pode ter em uma organização é imensurável, visto que o Engenheiro Social trabalha diretamente com a manipulação humana na organização, não apenas em ataques diretos a softwares e a rede das mesmas, sendo assim qualquer pessoa em uma organização pode ser alvo de ataques da Engenharia Social a qualquer momento e qualquer lugar, não necessariamente estando dentro da organização.

De acordo com Maulais (2016) as principais técnicas utilizadas em um ataque de Engenharia Social para obter informações de sistemas, redes de computadores das organizações são: a Análise de lixo, Internet e Rede Social, Contato Telefônico, Abordagem Pessoal, Phishing e Falha Humana.

Deste modo, podemos entender que a Análise de lixo é tudo aquilo que é descartado pelas organizações, assim, estes dados contidos em papéis que são

jogados em lixos comuns, podem vir a ser utilizados por um engenheiro social para obter mais informações futuramente.

A Internet como um todo é uma grande ferramenta para encontrar dados públicos de organizações, o que acaba sendo prejudicial, haja vista que por muitas vezes o uso de redes sociais na internet pode acabar prejudicando uma organização, quando seu uso acaba sendo exagerado e expondo informações importantes que por sinal deveria ser privada apenas aos colaboradores.

O contato telefônico geralmente é utilizado quando combinado com outras técnicas já previamente utilizadas e com algum resultado obtido, a partir disso o Engenheiro Social pode se utilizar do contato telefônico para tentar roubar mais dados ou manipular que alguma ação importante seja tomada pelo alvo.

Baldim (2007) expõe em sua monografia que um dos métodos utilizados em ataque de engenharia social é justamente o de se passar por uma pessoa de autoridade dentro da organização, combinado com ataques por ligação é possível que um colaborador seja facilmente influenciado.

A Abordagem pessoal é a técnica em que o Engenheiro Social pode ir até a empresa se passando por um fornecedor ou alguém interessado em conhecer a organização, os produtos, serviços e etc. A partir disso se aproveita para colher mais informações importantes para seu ataque.

A técnica de Phishing mais utilizada no dia a dia, em sua tradução literal significa “pescaria”, utilizada através de e-mails falsos enviados para as organizações, tendo por objetivo, fazer com que algum colaborador abra tal e-mail e realize os procedimentos solicitados nesse e-mail.

E por fim a Falha Humana acaba sendo por muitas vezes utilizada para contribuir com ataques sociais, se aproveitando de fraquezas humanas, como medo, curiosidade, vontade de querer ajudar o próximo, ingenuidade e muitos outros fatores.

Tendo em vista as diversas técnicas utilizadas pelo Engenheiro Social para roubar dados nas organizações, alguns meios de prevenções começaram a ser adotados para combater tais técnicas, uma vez que a adoção dos métodos de prevenções utilizadas anteriormente para combater meios de ataques tradicionais já não é mais tão eficaz para combater as referidas técnicas.

Para Mendes (2004) com a adoção de algumas medidas é possível evitar ataques de engenharia social, tais medidas são voltadas para a educação e treinamento de funcionários, mostrando o real valor da informação dentro da organização.

Freitas propõe em seu artigo algumas instruções para evitar ataque de Engenharia Social:

> - Ficar atento com ligações que solicitem muitas informações via telefone ou e-mails de pessoas perguntando a respeito de funcionários e/ou outras informações internas da empresa.
> - Não passar dados pessoais ou dados a respeito da sua empresa, incluindo a estrutura física.
> - Não informar dados pessoais ou financeiros em e-mail e muita cautela ao responder e-mails com esses tipos solicitações, procurar sempre averiguar a veracidade da pessoa que enviou o e-mail. Com relação aos links enviados por e-mail, na dúvida, não clique no mesmo.
> - Verificar a grafia do domínio solicitado na URL. Sites falsos costumam parecer idênticos a um original. Prestar atenção no está digitado no seu navegador
> - Se não tem certeza da veracidade de uma solicitação via e-mail, entre em
> - Ficar atento com e-mails cujo conteúdo contenha algo não solicitado por você, geralmente o mesmo possui um link mal intencionado ou um arquivo para ser executado.
> - Não acessar conta bancária por meio de links contidos em e-mails. Digitar o endereço do site em seu navegador. Os e-mails com remetentes desconhecidos / ou duvidosas podem conter links que direcionem para páginas fraudulentas.
> - E-mails com ofertas extraordinárias que circulam pela Internet, não dê credibilidade
> - Atenção com os arquivos com extensões, anexados no email ".exe", ".zip" e ".scr"..
> - Fazer uso de firewall e manter o antivírus atualizado. (2015, p. 27).

Deste modo é possível observar que a organização no cenário atual não depende somente do fator software no que tange segurança da informação, pois agora com a engenharia social, o fator humano acaba sendo muito mais importante e decisivo para obter informações dentro das organizações.

Para Freitas (2015) por mais que existam meios de prevenção, não é possível afirmar que os mesmos são totalmente eficazes, pois uma vez que a engenharia social agindo por nível em relação aos seus ataques é preciso realizar métodos de prevenção do mesmo jeito, visando à preocupação com a segurança física, dados, softwares, host e a rede interna.

Deste modo adotando normas voltadas para segurança física, dados, softwares, host e rede interna, o nível de segurança aumenta bastante dentro de uma organização, mas será que as organizações no cenário atual estão preocupadas em adotar determinadas normas? Ou se instruções abordadas anteriormente para proteção contra ataque de Engenharia Social estão sendo aplicadas dentro das organizações.

É notável que ataques de Engenharia Social cada vez mais está crescendo em todo mundo e só vai ser possível reduzir tais ataques a partir do momento que as organizações e pessoas começarem a entender mais sobre o assunto e trazerem para o cotidiano da organização tal conceito.

7 Metodologia

Em razão das peculiaridades da problematização e dos objetivos que se pretendem alcançar; a pesquisa monográfica referente a este projeto tem como proposta o seu desenvolvimento mediante o método dedutivo, tendo em vista que oferece uma base lógica ao tema em questão, partindo primeiramente do histórico das organizações no que tange a organização dos seus dados, conceito de dados, informações e engenharia social, bem como suas principais técnicas utilizadas e consequências em uma empresa que sofre esse tipo de ato, como também as formas de segurança que as organizações têm utilizado, levando a uma conclusão acerca da preparação ou não das organizações com relação a tais ataques. Os resultados serão apresentados de forma qualitativa, baseada em informações e dados.

O estudo será realizado a partir de pesquisas bibliográficas, através de buscas doutrinas, artigos científicos e revistas especializadas, visando analisar o problema em torno da engenharia social.

Nesse sentido, ter-se-á o desenvolvimento da pesquisa sob as do tipo bibliográfica, tendo em vista que para o processo de conhecimento proposto na metodologia supracitada, referente ao tema e a problematização discorridos neste projeto, será necessário fazer uma pesquisa nas leituras de textos bibliográficos.

8 Recursos

TIPO DE MATERIAL	QUANTIDADE	VALOR DO PRODUTO
PAPEL SULFITE	2 resmas	R$ 32,00
LIVROS	3	R$ 150,00
TINTA/IMPRESSORA	1 recarga tonner	R$ 45,00
INTERNET	Valor mensal	R$ 80,00

10. REFERÊNCIAS

BALDIM, Natália Pimenta. **Engenharia social e segurança da informação no ambiente corporativo: uma análise focada nos profissionais de secretariado executivo**. 2007. Trabalho de Conclusão de Curso- Universidade Federal de Viçosa, Minas Gerais, 2007.

CHIAVENATO, Idalberto. **Iniciação a sistemas, Organizações e métodos: So&m**. São Paulo: Manoele, 2010.

FERREIRA, Nicholas**. O Guia do Hacker**. 1° ed, 2014.

FREITAS, Cibelle. **Tratando de segurança na Engenharia Social**. Disponível em : <https://www.devmedia.com.br/tratando-de-seguranca-na-engenharia-social/33770> Acesso em : 02 abr. 2019.

MAULAIS, Claudio Nunes dos Santos. **Engenharia social: técnicas e estratégias de defesa em ambientes virtuais vulneráveis.** 2016. Projeto de pesquisa- Universidade FUMEC, Belo Horizonte, 2016.

MENDES, Antônio da Silva Filho. **Entendendo e Evitando a Engenharia Social:** protegendo Sistemas e Informações. Revista Espaço Acadêmico N°43 dez. 2004 - Mensal-ISSN1519. 6186 (Ano IV).

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

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. **Segurança de Redes em Ambientes Cooperativos.** São Paulo: Futura, 2003.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa**. 1ª ed. Rio de Janeiro: Brasport, 2006.

SILVA, Carlos Alberto. **Elo mais fraco da segurança da informação: Pessoas representam o maior desafio**. Minas Gerais: Amazon, 2015.

.