UNIVERSIDADE DO SUL DE SANTA CATARINA

JÚLIO GUAREZI

ENGENHARIA SOCIAL:
AVALIAÇÃO DE RISCOS E VULNERABILIDADES TENDO O FATOR HUMANO COMO O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

Palhoça

2019

JÚLIO GUAREZI

ENGENHARIA SOCIAL:
AVALIAÇÃO DE RISCOS E VULNERABILIDADES TENDO O FATOR HUMANO COMO O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistema da Informação da Universidade do Sul de Santa Catarina, como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Luiz Otavio Botelho Lento, Msc.

Palhoça

2019

JÚLIO GUAREZI

ENGENHARIA SOCIAL:
AVALIAÇÃO DE RISCOS E VULNERABILIDADES TENDO O FATOR HUMANO COMO O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Sistemas de Informação e aprovado em sua forma final pelo Curso de Graduação em Sistemas de Informação da Universidade do Sul de Santa Catarina.

Palhoça, 18 de novembro de 2019.

Prof. Orientador: Luiz Otavio Botelho Lento, Msc.
Universidade do Sul de Santa Catarina

Prof. Flávio Ceci, Dr.
Universidade do Sul de Santa Catarina

Prof. Rafael Lessa, Esp.
Universidade do Sul de Santa Catarina

Dedico este trabalho a minha esposa Franciele, minhas filhas Júlia e Alice, que está a caminho, por serem meu porto seguro.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, por me cuidar, ser meu alicerce e ter guiado meus caminhos até aqui.

Agradeço a minha esposa Franciele, por ser minha companheira, meu porto seguro e grande incentivadora. Nos momentos mais difíceis e cansativos do curso, foi ela quem me fez seguir em frente e não desistir.

Agradeço a minha amada filha Júlia, por ser paciente e entender as noites que precisei estar ausente e os momentos em que precisei ficar estudando em casa.

Um agradecimento a todos os amigos e familiares pelas palavras de incentivo e apoio desde o começo do curso. Em especial, a minha sogra Gessi e ao meu cunhado Fabricio.

Um agradecimento mais que especial ao professor Luiz Otávio, por toda sua paciência, conhecimento, por ser tão prestativo e atencioso em todos os momentos.

“Agora que já se ouviu tudo, aqui está a conclusão: Tema a Deus e obedeça os seus mandamentos, porque isso é o essencial ao homem. ” (ECLESIASTES 12:13).

RESUMO

Partindo do princípio que atualmente a informação é um dos ativos mais valiosos para uma organização, este trabalho visa demonstrar como a Engenharia Social pode ser utilizada para explorar características comportamentais do ser humano com o objetivo de obter benefícios ou informações sigilosas. Em toda organização o elo mais fraco da Segurança da informação é o ser humano. A maioria das empresas não está preparada ou não dá a devida atenção a este tema. Sendo assim, este trabalho tem como objetivos: analisar as principais técnicas e estratégias utilizadas pela Engenharia Social para explorar as vulnerabilidades e os riscos a que as organizações estão expostas; e, realizar um estudo de caso com a análise das vulnerabilidades e riscos ligados a Segurança da Informação. Para avaliar a proposta foi aplicado um teste de intrusão em uma empresa do ramo vidraceiro, com a aplicação de algumas técnicas de Engenharia Social. Foi possível constatar que a empresa não possui uma gestão eficiente de Segurança da Informação, e com isso, encontra-se vulnerável e um alvo fácil para que criminosos possam obter informações sigilosas e essenciais ao negócio.

Palavras-chave: Engenharia Social, Segurança da Informação, Informação, Organização, Ser Humano.

ABSTRACT

Assuming that information is currently one of the most valuable assets for an organization, this paper aims to demonstrate how Social Engineering can be used to exploit human behavioral characteristics in order to gain benefits or sensitive information. In every organization the weakest link in information security is the human being. Most companies are not prepared or do not give due attention to this topic. Thus, this work aims to: analyze the main techniques and strategies used by Social engineering to exploit the vulnerabilities and risks to which organizations are exposed; And, conduct a case study with the analysis of vulnerabilities and risks related to information security. To evaluate the proposal, an intrusion test was applied to a company in the glass industry, with the application of some techniques of Social engineering. It was possible to see that the company does not have an efficient management of information security, and thus is vulnerable and an easy target for criminals to obtain sensitive and essential information to the business.
Keywords: Social Engineering, Information Security, Information, Organization, Human.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas.

CID – Confidencialidade, Integridade, Disponibilidade.

GSI – Gerenciamento dos riscos de Segurança da Informação.

NBR – Norma Brasileira.

IEC – *International Electrotechnical Commission.*

ISO – *International Organization for Standardization.*

SGSI – Sistema de Gerenciamento de Segurança da Informação.

SUMÁRIO

1 INTRODUÇÃO

A informação é o ativo mais importante de uma organização. Quando uma organização perde sua propriedade intelectual, tem sua lista de clientes roubada ou seus projetos copiados, dificilmente esta organização conseguirá se recuperar. (MITNIK; SIMON, 2006).

As organizações precisam proteger suas informações mais relevantes ao mesmo tempo que precisam de eficiência e rapidez em suas tomadas de decisão. A disponibilidade de internet em praticamente todas as áreas e dispositivos, faz com que esta seja uma ferramenta estratégica para os negócios das empresas.

No entanto, assim como os inúmeros benefícios, as ameaças aos sistemas computacionais estão em constante evolução. Diariamente surgem novas formas de ataque, novas ameaças às vulnerabilidades que trazem riscos às informações das empresas.

Neste contexto, a Segurança da Informação busca diminuir possíveis riscos decorrentes utilização dos recursos da informação para as organizações, pois sendo roubada ou corrompida, pode gerar perdas irreparáveis para as organizações. (FONTES, 2001).

Segundo Maulais (2016, p.9):

> A Segurança da Informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, analisados criticamente, e melhorados quando necessário, para assegurar que os objetivos dos negócios e a Segurança da informação sejam alcançados.

No entanto, nenhuma política ou tecnologia aplicada à Segurança da Informação trará os resultados esperados se o fator humano for deixado de lado e não receber a atenção necessária. Uma das formas mais utilizadas e eficazes de se obter informações sigilosas, explorando as características humanas é o uso da Engenharia Social.

As pessoas que utilizam a Engenharia Social para obter informações geralmente falam com propriedade sobre determinados assuntos, adquirem a confiança da vítima e muitas vezes chegam a prestar algum favor ou oferecer algum benefício, criando assim, uma relação de confiança, o que facilitará alcançar o seu verdadeiro objetivo.

De acordo com Maulais (2016, p.11), “o fator humano deixado em segundo plano, é o ponto central de ataques de Engenharia Social que tem como propósito a exploração da fragilidade humana, necessitando medidas de segurança como mitigação desta fragilidade. ”

Geralmente as organizações maiores estão mais vulneráveis a ataques utilizando a Engenharia Social, por terem um número grande de funcionários e muitas vezes filiais espalhadas por outras cidades. Uma pessoa que deseja realizar o ataque pode se passar por um funcionário em viagem ou de uma outra filial, e assim, obter informações sigilosas.

A Engenharia Social é uma técnica muito utilizada por *crackers* que buscam obter acesso a sistemas, redes ou informações que possuam valor estratégico para as organizações. As pessoas que utilizam esta técnica para obter vantagens são chamadas de Engenheiros Sociais. (RAFAEL, 2013).

Com o uso de técnicas de Engenharia Social como: análise do lixo, análise das redes sociais, contato telefônico, contato pessoal e *phishing,* os engenheiros sociais buscam obter o acesso as informações estratégicas para o negócio das organizações.

Diante deste contexto, este trabalho tem o objetivo de analisar como as técnicas de Engenharia Social são utilizadas para obter informações consideradas sigilosas ou estratégicas para o negócio das organizações, explorando o fator humano que é o elo mais fraco numa estrutura de Segurança da Informação.

Para isso serão analisadas as técnicas de Engenharia Social mais utilizadas e os resultados de um teste aplicado em uma organização como estudo de caso.

1.1 PROBLEMÁTICA

A informação é um dos maiores ativos de uma organização, por isso é muito importante que os colaboradores saibam o valor que ela tem para a organização. É importante que todos os colaboradores estejam engajados e motivados em contribuir com as estratégias de Segurança da Informação estipuladas pela empresa.

No entanto, o fator humano é o mais crítico, é o elo mais fraco, pois possui traços comportamentais e psicológicos que o torna suscetível a falhas e que podem ser explorados pela Engenharia Social com o intuito de se obter informações estratégicas e sigilosas para determinada organização.

Diante deste contexto, surge a seguinte questão:

Como o fator humano pode ser explorado através da aplicação de técnicas de Engenharia Social para obter informações importantes e sigilosas para o negócio das organizações corporativas?

1.2 OBJETIVOS

Os objetivos do presente projeto estão descritos a seguir e dividem-se em objetivo geral e objetivos específicos.

1.2.1 Objetivo geral

Analisar a Segurança da Informação, sob o prisma do fator humano, sendo este estratégico dentro das organizações e identificar como a Engenharia Social é utilizada para encontrar vulnerabilidades, que são exploradas por criminosos com o objetivo de obter informações consideradas sigilosas e estratégicas para o negócio das organizações.

1.2.2 Objetivos específicos

Os objetivos específicos do projeto são:

- analisar as técnicas de Engenharia Social;
- analisar como a Engenharia Social é utilizada para obter informações privilegiadas;
- pesquisar as principais características comportamentais do ser humano que o torna suscetível a ataques de Engenharia Social;

- realizar uma análise de riscos e vulnerabilidades com foco em ataques de Engenharia Social em uma empresa do ramo vidraceiro no município de Palhoça;
- realizar um teste de intrusão, utilizando técnicas de Engenharia Social com os colaboradores da organização escolhida para o estudo de caso.

1.3 JUSTIFICATIVA

Por se tratar do ativo mais importante de uma organização, o processo de manter segura a informação requer mais que novas tecnologias. As organizações devem realizar um mapeamento contínuo das necessidades de aprimoramento de seus colaboradores, pois estes são o elo mais fraco da Segurança da Informação e podem ser explorados através de técnicas de Engenharia Social.

De acordo com Kim; Solomon (2014, pg. 28), "o usuário é o elo mais fraco da Segurança da Informação, e, até mesmo profissionais de segurança de sistemas de informação podem cometer erros. "

O erro humano é um risco alto e real, e uma grande ameaça às organizações corporativas. O comportamento do ser humano, suas características comportamentais e traços psicológicos não podem ser controlados. Sendo assim, as organizações precisam estar preparadas para usuários maliciosos, não treinados e descuidados

É necessário focar nas questões humanas e culturais, para que, em conjunto com processos e procedimentos bem estruturados, seja possível diminuir os riscos para o negócio a um nível considerado aceitável.

1.4 ESTRUTURA DA MONOGRAFIA

No primeiro capítulo deste trabalho é apresentado a introdução, a problemática, os objetivos e a justificativa.

O segundo capítulo apresenta o início da revisão bibliográfica sobre a informação e sobre os conceitos de Segurança da Informação, normas e sua importância dentro das organizações.

No terceiro capítulo ocorre a continuação da revisão bibliográfica, apresentando os conceitos de Engenharia Social, suas técnicas e como estas técnicas são aplicadas na tentativa de se obter informações privilegiadas.

Já no quarto capítulo, é apresentada a metodologia utilizada para alcançar os objetivos propostos neste trabalho.

No quinto capítulo apresentamos uma descrição do desenvolvimento de estratégias para aplicação das técnicas de ataque utilizados na Engenharia Social.

No sexto capítulo ocorre a descrição do estudo de caso realizado para validar as estratégias criadas no capítulo anterior, utilizando a aplicação de um teste de intrusão em uma empresa do ramo vidraceiro, localizada no município de Palhoça.

Já no sétimo e último, apresentamos as considerações finais e a conclusão do trabalho, bem como possíveis trabalhos e estudos futuros acerca do tema apresentado neste projeto.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão abordados os temas relevantes para o desenvolvimento do presente trabalho, apresentando o referencial teórico abordado por autores conceituados.

2.1.1 A Informação

No universo computacional, a informação pode ser definida como o resultado da análise e processamento de dados pelos computadores. (GALVÃO, 2015). "A informação é um ativo essencial para os negócios de uma organização, e necessita ser adequadamente protegida. " (ABNT, 2007, p.10).

Para uma organização, as informações auxiliam na tomada de decisões, aumentam a competitividade no mercado, servem como um fator motivacional e possibilitam o crescimento dos colaboradores. (JUNIOR, 2017).

É importante e necessário que toda organização, independentemente do tamanho ou segmento que atua, deve classificar as informações de acordo com o grau de importância.

Ainda neste contexto, Galvão (2015, p.5) diz que:

> A classificação das informações é o procedimento de diferenciar e determinar níveis e critérios de proteção, os quais devem zelar pela confidencialidade, integridade e disponibilidade das informações, sem deixar de lado sua relevância para a organização.

"O objetivo de se estabelecer um padrão de classificação de dados, é oferecer uma definição consistente de como uma organização deve tratar e proteger diferentes tipos de dados. " (KIM; SOLOMON, 2014, p.32). Ainda de acordo com os autores citados, é necessário que existam controles e procedimentos que definam como as organizações devem tratar cada tipo de informação.

Cada organização deve implementar políticas de classificação da informação, baseadas em suas estratégias de negócios e na importância que as informações têm dentro da organização. Quanto maior for a organização, mais níveis de classificação devem ser

implementados. Organizações de médio porte, geralmente classificam suas informações com três níveis de confidencialidade e um nível público. (KOSUTIC, 2014).

As informações podem ser classificadas de acordo com seu grau de confidencialidade, integridade e disponibilidade. As organizações devem preocupar-se em o quanto a informação é importante, levando em conta que o custo de sua manutenção, é menor que o custo de não a manter de forma adequada. (LENTO, 2011).

Os padrões de classificação dos dados normalmente incluem as seguintes categorias:

a) dados confidenciais: o mais alto nível de confidencialidade. São informações ou dados de propriedade da organização. Podem ser propriedade intelectual, lista de clientes, informações de patentes e preços são alguns exemplos.
b) dados privados: nível médio de confidencialidade. Dados sobre pessoas que precisam ser mantidos privados. As organizações precisam usar controles de segurança apropriados para garantir a privacidade destes dados. (GALVÃO, 2015).
c) uso interno: nível mais baixo de confidencialidade. São informações ou dados compartilhados internamente por uma organização. Essas comunicações não devem sair da organização, mesmo que não incluam dados ou informações confidenciais. (KIM; SOLOMON, 2014)
d) domínio público: todos podem ver a informação. Geralmente são informações ou dados compartilhados com o público, como conteúdo de *web site* ou informações oficiais.

A informação é considerada um ativo valioso e importante para as estratégias de negócio das organizações, por isso, deve se ser gerenciada, protegida, preservada e mantida em ambientes seguros. Galvão (2015, p. 13) confirma esta importância ao afirmar que " a informação é um dos maiores patrimônios de uma organização, sendo vital para quaisquer níveis hierárquicos e para qualquer organização que deseja manter-se competitiva no mercado. "

De acordo com Sêmola (2003), todas as organizações, independente do segmento de mercado que atuam, das estratégias de negócio que seguem, do tamanho e quantidade de

funcionários, utilizam as informações como objetivo de aumentar sua competitividade, reduzir custos, melhorar a produtividade, apoiar em seu planejamento e tomada de decisão.

Deve-se procurar diminuir os riscos, ameaças e vulnerabilidades que a informação está exposta, sem perder a competitividade e o rendimento necessários para que a organização tenha sucesso. Uma maneira de realizar isso é indicada por Fontes (2001, p. 01), "a informação deve ser protegida por meio de políticas e regras, da mesma forma que os recursos financeiros e materiais da organização, pois é um recurso crítico para a realização do negócio e execução da missão da organização. "

2.2 SEGURANÇA DA INFORMAÇÃO

Cada vez mais as organizações buscam novas tecnologias e recursos para aumentar sua produtividade, eficiência e auxiliar no planejamento e desenvolvimento de suas estratégias de negócio. No entanto, torna-se um desfio cada vez maior manter as informações seguras, evitando vazamento, roubo, espionagem ou destruição de informações consideradas vitais para o negócio.

De acordo com Fontes (2001, p. 10), "Segurança da Informação é o conjunto de orientações, normas, procedimentos e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão alcançada. "

A Segurança da Informação tem o objetivo de mitigar os riscos para as organizações, pois o mal gerenciamento das informações pode acarretar perdas, afetar o desempenho e em situações mais estremas levar a falência. (KIM; SOLOMON, 2014).

Lento (2011, p. 20), define a Segurança da Informação como:

> A garantia que as informações (em qualquer formato: mídias eletrônicas, papel, e até mesmo em conversações pessoais ou por telefone) estejam protegidas contra o acesso por pessoas não autorizadas (confidencialidade), estejam sempre disponíveis quando necessárias e que sejam confiáveis (que não tenham sido corrompidas ou adulteradas por atos de pessoas mal-intencionadas).

É necessário desenvolver um planejamento para a Segurança da Informação, buscando mapear, identificam e organizar as informações com o objetivo de mantê-las seguras. (GALVÃO, 2015),

As organizações precisam criar políticas e metodologias de segurança que englobem controles, processos, procedimentos, estruturas organizacionais, funções de *software* e *hardware* e os colaboradores. Para que os objetivos da Segurança da Informação sejam alcançados, é necessário que sejam estabelecidos controles, e que estes, possam ser monitorados, revisados e melhorados quando necessário. (HINTZBERGEN et al., 2018).

2.3 CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Quando se fala em Segurança da Informação, alguns conceitos importantes e a relação entre eles devem ser entendidos, para que se torne possível obter uma visão mais profunda do que e de quem a informação deve ser protegida.

Um programa de Segurança da Informação deve ser capaz de atender objetivos estipulados pelas políticas da organização, e principalmente garantir que os princípios mais importantes: Confidencialidade, Integridade e Disponibilidade. Confirmando isso, Lento (2011, p. 143), diz que "a Segurança da Informação tem como objetivo garantir o uso adequado da informação, evitar que ela seja perdida ou corrompida, isto é, garantir a confidencialidade, integridade e disponibilidade dessa informação. "

A Segurança da Informação faz a gestão dos riscos que podem comprometer um ou todos os princípios citados anteriormente. Estes princípios de Segurança da Informação podem ser vistos na figura 1:

Figura 1 – Princípios da Segurança da Informação.

Fonte: Lopes (2017).

A figura anterior mostra como os princípios da Segurança da Informação estão diretamente ligados e que todos os controles de segurança e mecanismos de proteção devem ser implementados, para evitar o comprometimento desses princípios.

Os três princípios da Segurança da Informação podem ser definidos da seguinte maneira:

a) confidencialidade: se refere aos limites em termos de quem pode obter que tipos de informação. Assegura que o nível de sigilo adequado seja aplicado em cada elemento de processamento de dados e impede a divulgação não autorizada. O nível de confidencialidade deve permanecer enquanto as informações residirem em sistemas e dispositivos de rede, quando forem transmitidos e quando chegarem ao seu destino. Busca prevenir a divulgação intencional ou não de uma mensagem. (HINTZBERGEN et al., 2018).
b) integridade: se refere a ser correto e consistente com o estado ou a informação pretendida. Qualquer modificação não autorizada é uma violação a integridade dos dados. Devem ser prevenidas modificações não autorizadas ao *software* ou *hardware,* que não sejam realizadas modificações não autorizadas aos dados, e que as informações sejam internamente e externamente consistentes. (LENTO, 2011).

c) disponibilidade: a informação deve ser acessível e utilizável sob demanda por quem for autorizado. Assegura o acesso confiável e em tempo oportuno a dados ou recursos de computação por pessoas autorizadas. Em outras palavras, garante que os sistemas estejam ativos e funcionando quando necessário. Hintzbergen et al. (2018) cita ainda algumas características como: oportunidade, a informação deve estar disponível quando necessário; continuidade, é possível utilizar a informação em caso de alguma falha no sistema; robustez, existe capacidade suficiente para que todas as pessoas autorizadas a utilizar as informações ou sistemas possam operar ao mesmo tempo, quando necessário.

Alguns autores como Galvão (2015), Hintzbergen et al. (2018) e Kim; Solomon (2014), citam outras duas características que são associadas a Segurança da Informação:

d) autenticidade: "garante a legitimidade da transação, acesso, comunicação e da própria informação, assegurando a veracidade da fonte anunciada e que a informação não sofreu modificação não autorizada. " (GALVÃO, 2015, p. 17).
e) não repudio ou irrevogabilidade: este princípio existe para garantir que não seja possível negar uma ação. Garante que uma informação existente e autêntica, seja irrevogável, e que um indivíduo que realizou uma transação ou modificação, não possa negar sua autoria. (SÊMOLA, 2003).

2.3.1 Riscos, ameaças e vulnerabilidades

Os riscos podem ser definidos para Lento (2011, p. 27), "como o potencial de uma determinada ameaça explorar vulnerabilidades, proporcionando perdas ou danos a ativos de forma direta ou indireta para uma organização. "

Uma ameaça é qualquer evento que possa causar impacto na capacidade das organizações atingirem seus objetivos de negócio. Pode-se dizer ainda que é a probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização ou um evento indesejável que remove, desabilita ou destrói um recurso ou uma

informação. As ameaças aproveitam as falhas de segurança da organização. Possibilidade de um agente explorar uma vulnerabilidade. (OLIVEIRA, 2018).

De acordo com Lento (2011) e Galvão (2015), as ameaças dividem-se em: ameaças ativas, quando o agente interage diretamente com o sistema e; ameaças passivas, cujo objetivo é a coleta de informações, não alteram o sistema.

Os autores citados, declaram ainda que as ameaças podem ser naturais e físicas: quando relacionadas à estrutura física da organização; não intencionais: quando relacionadas às falhas por falta de conhecimento e; intencionais: quando os atos são praticados com a intenção de destruir, roubar ou adulterar as informações.

As ameaças podem assumir diversas formas desde furto de mídia, documentos e equipamentos, forjamento de direitos, espionagem a distância, escuta não-autorizada, até fenômenos climáticos, incêndio.

Para Cicco (2018, pg. 2), "as consequências dessas ameaças podem ser traduzidas por vários impactos nos negócios das organizações como, perdas financeiras, paralisação de serviços essenciais, perda de confiança dos clientes e falhas de telecomunicações. "

Além das ameaças e dos riscos, as organizações podem estar expostas a vulnerabilidades. Uma vulnerabilidade pode ser causada por uma falha em um procedimento ou sistema utilizado pela organização.

Tratando de vulnerabilidades, Oliveira (2018) afirma que "vulnerabilidade pode ser uma falha ou fraqueza de procedimento, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada. " Essa vulnerabilidade pode gerar uma brecha de segurança ou uma violação nas políticas de Segurança da Informação.

Ainda falando sobre vulnerabilidade, pode-se dizer são fraquezas relacionadas a um conjunto de ativos de informação e acabam reduzindo a manutenção dos princípios da Segurança da Informação. (GALVÃO, 2015; OLIVEIRA, 2018).

Como já citado anteriormente, um dos maiores patrimônios de uma organização á a informação, e faz toda a diferença no a maneira como a Segurança da Informação é tratada. É o que afirma Oliveira (2018), quando diz que "é importante que toda empresa ao lidar com a informação avalie os riscos, vulnerabilidades e as ameaças que ela pode sofrer. "

É necessário identificar os pontos vulneráveis dos ativos de informação e buscar condições de repará-los para garantir que não permitam que uma ameaça possa atingir os sistemas de informação das organizações.

De acordo com Galvão (2015, p. 25), “a gestão de Segurança da Informação eficiente deve se preocupar com a vulnerabilidade de seus ativos de informação, com as ameaças às quais as informações estão sujeitas e com os possíveis ataques que podem sofrer. "

A figura 2 mostra as principais ameaças que exploram as vulnerabilidades das organizações.

Figura 2 – Ameaças e vulnerabilidades das organizações.

Fonte: Oliveira (2018).

De acordo com a figura 2, pode-se perceber que as ameaças e vulnerabilidades contra a Segurança da Informação nas organizações vão além de problemas com invasões de hackers, é preciso além de proteger o setor de TI, criar regras para criação de senhas e restringir o acesso a espaços físicos e a informações importantes.

As organizações precisam levar em consideração que os custos para segurança são muito menores do que os custos causados por perda ou roubo de informações. É necessário que as ameaças, riscos e vulnerabilidades sejam avaliados, monitorados e tratados.

2.4 SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

As organizações estão constantemente correndo riscos. “Seus negócios, processos, ativos físicos, tecnológicos e humanos são alvos de investidas de ameaça de toda ordem, que

buscam identificar um ponto fraco, uma vulnerabilidade capaz de potencializar a ação. ” (SÊMOLA, 2003, p.18).

A área de Segurança da Informação é a responsável por proteger as organizações de todos os tipos de ameaças que possam afetar sua existência. Um bom sistema de Segurança da Informação deve diminuir os riscos a que a organização está exposta, gerar oportunidades, colaborar para o crescimento da organização. (GALVÃO, 2015).

Os ativos de informação devem ser protegidos, pois possuem um alto valor para as organizações. A proteção desses ativos e de todo o sistema em que estas informações circulam e estão disponíveis é de extrema importância. (LAUDON; LAUDON, 2012).

Quando uma organização não tem a devida preocupação com a segurança de seus sistemas de informação, coloca em risco informações de clientes, fornecedores e parceiros comerciais. Ter estas informações roubadas pode trazer graves problemas financeiros, de reputação e até decretar o fim da organização.

Para Lento (2011, p. 27), “a existência de riscos em uma organização exige a adoção de medidas de proteção, reduzindo a probabilidade de as ameaças explorarem vulnerabilidades existentes, garantindo que os ativos da organização exerçam tarefas para que foram criados. ”

As informações relacionadas ao tipo de negócio, estratégias de mercado, produtos e serviços de uma organização podem ser o seu bem mais valioso. “Uma simples falha pode custar todo o futuro da corporação, em que, cada vez mais, as pessoas estão comprando na internet, dados estão sendo migrados para a nuvem e a transição deles é constante. ” (INOVE DADOS, 2018).

Para Dawel (2005, p. 55), “a informação vale dinheiro, portanto, as organizações precisam não só proteger seus ativos reais, mas principalmente seu capital intelectual e suas informações. ”

Considerada um fator crítico para o negócio das organizações, é necessário que sejam aplicadas políticas e soluções e que os usuários sejam conscientizados da importância de manter as informações seguras. (LENTO, 2011).

Infelizmente, a realidade para a maioria das empresas não permite que sejam aplicadas soluções que possibilitem um cuidado maior com a segurança de suas informações. Pequenas e médias empresas são um dos principais alvos de ataques cibernéticos. Essas empresas se tornam alvos lucrativos e relativamente fáceis para os cibercrimonosos. Diferentemente de grandes empresas, não tratam com a devida atenção a segurança das informações ou não dispõem de orçamento para se proteger adequadamente.

De acordo com Galvão (2015, p. 90), “a Segurança da Informação não é um assunto puramente tecnológico, pois para obtê-la, as organizações precisam de um gerenciamento, e como consequência, alguns preceitos da administração. ”

Existem normas que tratam como a gestão da Segurança da Informação deve ser tratada pelas organizações, afirmando que “a adoção de um Sistema de Gerenciamento de Segurança da Informação (SGSI) deve ser uma decisão estratégica para uma organização. O design e a implementação do SGSI de uma organização são influenciados por suas necessidades e objetivos, requisitos de segurança, processos e tamanho e estrutura da organização. ” (ABNT, 2010, p.5).

A norma ABNT ISO/IEC 27001 “foi preparada para fornecer requisitos para o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria de um Sistema de Gerenciamento de Segurança da Informação. ” (SCGI) (ABNT, 2010, p.5).

Para Hintzbergen et al. (2018), a norma ABNT ISO/IEC 27001, “é a norma para os requisitos do Sistema de Gerenciamento de Segurança da Informação, trata-se de uma especificação formal para os requisitos. ”

Outra norma que rege a gestão da Segurança da Informação é a ABNT ISO/IEC 27002. Esta norma “estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de Segurança da Informação em uma organização. Os objetivos definidos nessa norma provêm diretrizes gerais sobre as metas aceitas para a gestão da Segurança da Informação. ” (ABNT, 2005, p.5).

A norma ABNT ISO/IEC 27002 pode ser considerada como o código de práticas para controles de Segurança da Informação. Ela descreve os controles e objetivos referentes às boas práticas que as organizações precisam seguir para estabelecer uma política de Segurança da Informação.

“Os objetivos de controle e os controles da norma ABNT ISO/IEC 27002 têm como finalidade ser implementados para atender aos requisitos identificados por meio da avaliação de riscos. Serve como um guia prático para desenvolver os procedimentos da gestão da Segurança da Informação. ” (ABNT, 2005, p.5).

2.5 ANÁLISE DE VULNERABILIDADES E GERENCIAMENTO DE RISCOS

Ataques cada vez mais frequentes e em constante evolução exigem respostas rápidas das organizações. Soma-se ainda novas legislações de proteção de privacidade e governança cooperativa, tudo isso gerando a necessidade de as organizações serem mais efetivas no gerenciamento de seus ativos humanos e tecnológicos. Confirmando isso, Bezerra (2013, p. 11) afirma que:

> Para enfrentar essas novas ameaças e demandas as organizações devem desenvolver uma atitude mais proativa, antecipando-se em conhecer suas fraquezas e vulnerabilidades. Isto pode ser obtido através da adoção de um processo formal de gerenciamento de riscos de Segurança da Informação, que permita a organização estabelecer um nível aceitável de risco.

As organizações necessitam realizar análises de vulnerabilidade, para que possam identificar, quantificar e priorizar o que há de mais importante em seus sistemas de informação. Isso se faz necessário para tornar a segurança mais robusta. (ALERTA SECURITY, 2018).

A análise das vulnerabilidades pode detectar as possíveis falhas e aponta o caminho para a correção e para garantir que a organização tenha um nível de Segurança da Informação eficiente. Sobral (2018), confirma isso quando fala que "o objetivo da análise de vulnerabilidade é reduzir o risco em relação aos incidentes de segurança, tanto na rede interna quanto na rede externa. "

De acordo com Galvão (2015, p. 93), "a Segurança da Informação de qualquer organização, independentemente do ramo de atuação, possui riscos. " A análise de vulnerabilidade é uma das melhores ferramentas que uma organização pode empregar para aumentar a Segurança da Informação.

Segundo Sêmola (2003, p. 109):

> Diagnosticar o risco envolve a análise de variáveis endógenas que extrapolam os aspectos tecnológicos; portanto, devem considerar, também, os aspectos comportamentais dos recursos humanos, os aspectos físicos, legais e, ainda, um grande leque de variáveis exógenas que interferem direta ou indiretamente na proteção do negócio.

A análise de vulnerabilidades é fundamental para diagnosticar a real situação da Segurança da Informação da organização, através do entendimento dos desafios e do relacionamento entre os processos do negócio com os ativos humanos e tecnológicos.

A norma ABNT ISO/IEC 27005 fornece as diretrizes para o Gerenciamento dos riscos de Segurança da Informação (GSI). Tem o objetivo de auxiliar a implementação correta da Segurança da Informação com base em uma abordagem no gerenciamento dos riscos.

De acordo com Bezerra (2013, p. 9):

> Esta norma descreve todo o processo necessário para a gestão de riscos da Segurança da Informação e as atividades necessárias para a perfeita execução da gestão. Apresenta também, práticas para a gestão de riscos da Segurança da Informação. As técnicas nela descritas seguem o conceito, o modelo e os processos globais especificados na norma ABNT NBR ISO/IEC 27001, além de apresentar a metodologia de avaliação e tratamento dos riscos requerido pela mesma norma.

Cabe a cada organização definir sua abordagem ao gerenciamento de riscos, dependendo, por exemplo, do escopo do SGSI, do contexto de gerenciamento de riscos ou setor de atuação. (ABNT, 2011, p.5).

A análise de vulnerabilidade para Galvão (2015) e Alerta Security (2018), compreende algumas etapas, citadas a seguir:

- definição dos objetivos: nessa etapa se defini qual será o objetivo desse processo, é definido se o gerenciamento será para minimizar riscos, falhas de sistemas ou custos.
- identificação dos riscos: cada organização deve conhecer e identificar os riscos que podem afetar seus sistemas de informação. Para identificar os riscos, devem ser aplicadas algumas técnicas, como por exemplo, o mapeamento de todo processo computacional da empresa.
- análise de riscos: deve-se identificar quais informações a organização armazena e seu valor, descobrir ameaças que pode sofrer e suas vulnerabilidades, distinguir o grau de impacto de cada risco e estimar os custos de um incidente. Deve ser vista como um instrumento importante para diagnosticar a atual situação da Segurança da Informação dentro da organização.
- planejamento do tratamento de risco: a gestão de riscos de uma organização nem sempre se preocupa em eliminar totalmente os riscos, pois em algumas situações, é necessário um alto custo para isso. A organização deve fazer o possível para mitigar as vulnerabilidades detectadas. Conhecendo os sistemas que estão sob risco e identificando a importância de cada um deles, é possível enumerar as ameaças que devem ser atacadas primeiro. Se há

vulnerabilidades nos controles existentes, por exemplo, elas devem ser corrigidas o quanto antes. A organização deve entender como o tipo de risco que o negócio corre pode ser evitado e quais são as ferramentas mais eficazes para isso.

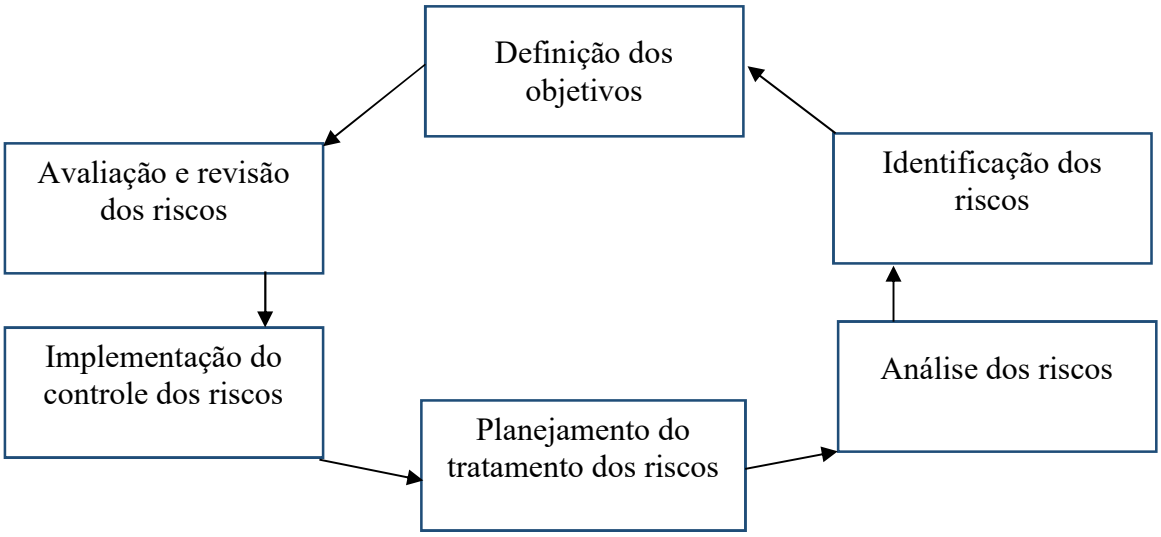
- implementação do controle de risco: na implementação deve-se executar todo o planejamento do tratamento dos riscos através de algumas políticas como o engajamento dos gestores e funcionários, monitoramento da implementação, comunicação entre os gestores e funcionários e comprometimento de todas as áreas.
- avaliação e revisão dos riscos: O gerenciamento dos riscos deve estar sempre avaliando e revisando os riscos existentes, assim como estar atento a novos riscos que possam surgir e afetar a organização.

Para Sêmola (2003, p. 109), "existem duas linhas metodológicas para orientar uma análise de riscos: uma quantitativa e outra qualitativa. "

Galvão (2015) e Sêmola (2003) descrevem que a análise de riscos quantitativa mensura os impactos financeiros provocados por uma quebra de segurança a partir da valorização dos próprios ativos. Já a análise qualitativa, permite estimar os impactos provocados no negócio provocados por exploração de uma vulnerabilidade através de uma ameaça.

De acordo com Galvão (2015, p. 98), "o gerenciamento de riscos é um processo cíclico, pois ao chegar a última etapa, é necessário verificar se novos riscos surgiram. " A figura 3 apresenta as etapas desse processo.

Figura 3 – Etapas do gerenciamento de riscos.



Fonte: Adaptada pelo autor de Galvão (2015).

É evidente que a análise de vulnerabilidades deve atingir os ativos tecnológicos das organizações, analisando e identificando possíveis falhas em computadores, servidores, redes internas e sistemas. Porém, existem outros fatores que somados aos citados anteriormente, que são relevantes e sensíveis e podem comprometer o negócio.

Cada organização possui características, objetivos e estratégias próprias, e precisa encontrar o nível de risco aceitável para operar. É necessário incentivar uma cultura de segurança que seja colaborativa, estruturada e incorporada por todos os processos e pessoas da organização.

De acordo com Cisco (2018, tradução nossa):

> O comprometimento executivo é vital para uma cultura consciente da segurança. Quando a conscientização da segurança é enfatizada pelos principais níveis de gerenciamento, os funcionários tendem a ver a segurança como um facilitador de negócios, em vez de um obstáculo à produtividade.

Uma das maneiras de uma organização analisar suas vulnerabilidades é através de testes de invasão, conhecidos também como *Pen Test*. O *Pen Test* é um conjunto de técnicas e ferramentas utilizadas para identificar falhas de segurança em sistemas e redes corporativas.

"Através dessas técnicas, o profissional de Segurança da Informação irá identificar as vulnerabilidades existentes na arquitetura da empresa, explorá-las e entregar um relatório à empresa, que deverá então tomar as devidas ações para corrigir as falhas de segurança. " (PROFISSÃO HACKER, 2018).

3 ENGENHARIA SOCIAL

Atualmente, as vulnerabilidades que cercam os sistemas de informação são muito discutidas e amplamente combatidas. No entanto, as vulnerabilidades humanas que são as emoções e sentimentos que cada indivíduo possui, muitas vezes são deixadas de lado.

Mitnick; Simon (2003) declaram que a Engenharia Social é a arte ou a ciência de influenciar ou enganar as pessoas. Com o auxílio de informações privilegiadas, obtidas por meios escusos, o engenheiro social engana para obter vantagens.

A Engenharia Social é utilizada para ludibriar as pessoas, se tornou muito popular e utilizada nos últimos anos com o surgimento de novas formas de comunicação e o crescimento das redes sociais. (PONTIROLI, 2013).

Segundo Fontes (2006, p. 119), "Engenharia Social é o conjunto de procedimentos, e ações utilizados para adquirir informações de uma organização ou pessoa por meio de contatos falsos sem uso de força ou arrombamento físico. "

Este termo é usado para referenciar as técnicas que criminosos virtuais utilizam para manipular seus alvos, tendo como objetivo obter informações ou fazer com que executem alguma ação que danifique os sistemas utilizados.

A Engenharia Social ainda pode ser definida de acordo com Pavão (2018), "como um método de ataque em que uma pessoa mal-intencionada faz uso da manipulação psicológica para induzir alguém a fazer ações específicas, como divulgar informações pessoais, baixar aplicativos falsos ou abrir links maliciosos. "

Pode se ainda definir a Engenharia Social, como "qualquer estratégia usada pelos *hackers* que, em grande parte, dependem da interação humana e geralmente envolvem iludir o usuário para desrespeitar práticas de segurança padrão. " (PROOF, 2018).

Com o conceito de Engenharia Social em mente, um ponto muito importante a ser ressaltado, é que independente do sistema, do *hardware* ou *software* utilizados, o fator de maior vulnerabilidade em qualquer organização, é o humano.

O sucesso dos ataques de Engenharia Social depende da habilidade atacante em manipular as vítimas para que executem certas ações ou ofereçam informações. Para isso, exploram as emoções e sentimentos das pessoas, descobrindo e explorando suas fragilidades e vulnerabilidades.

Segundo Proof (2018), “como não envolve nenhum aspecto técnico que possa ser reconhecido pelas ferramentas de segurança tradicionais, os ataques de engenharia social estão entre as maiores ameaças às empresas atualmente. ”

O engenheiro social procura convencer as pessoas por meio de persuasão e manipulação, tenta se passar por outra pessoa para obter vantagens ou informações privilegiadas utilizando ou não algum tipo de tecnologia. (MITNICK; SIMON, 2003).

Os seres humanos possuem traços psicológicos e comportamentais que o tornam vulneráveis a ataques que utilizam a Engenharia Social. Os engenheiros sociais conseguem descobrir estas características e acabam explorando-as para obter vantagens, acessos privilegiados ou informações sigilosas.

Para Mitnick; Simon (2003, p.26), “é de natureza humana confiar nas pessoas, particularmente quando a solicitação parece ser razoável. Os engenheiros sociais usam esse conhecimento para explorar suas vítimas e atingir seus objetivos. ” Os engenheiros sociais geralmente confiam na disposição das pessoas para ajudar. Eles também atacam as fraquezas das pessoas.

Junior (2006), e Silva (2012, p. 2) descrevem algumas destas características que são exploradas pela Engenharia Social:

- vontade de ser útil: O ser humano, geralmente, age com cortesia, procura ajudar os outros quando necessário;
- busca por novas amizades: O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a fornecer informações.
- propagação de responsabilidade: O ser humano considera que ele não é o único responsável por um conjunto de atividades.
- persuasão: é a capacidade de convencer as pessoas a realizarem ações, acreditarem em determinadas ideias ou acredite em determinada pessoa.
- vaidade: Pode ser pessoal ou profissional. A identificação com argumentos que corroboram com a avaliação pessoal ou profissional gera aceitação espontânea e há uma receptividade e aceitação maior;
- autoconfiança: Necessidade que os seres humanos têm de falar sobre o quanto é bom em realizar determinadas tarefas e ações, o quanto entende determinados assuntos;

- formação profissional: o ser humano busca valorização de suas habilidades, procura demonstrar domínio na comunicação, execução ou apresentação profissional.

Estas são as principais características humanas exploradas por pessoas mal-intencionadas que utilizam a Engenharia Social para obter vantagens indevidas ou informações sigilosas.

Para Galvão (2015, p. 99), "a Engenharia Social pode causar falhas em sistemas de informação computacionais. Na maioria das vezes, consegue informações necessárias para realizar seu objetivo por meio da observação de hábitos e estudo de traços comportamentais. "

3.1 ATAQUES UTILIZANDO ENGENHARIA SOCIAL

A Engenharia Social serve de ferramenta para explorar falhas em empresas, órgãos do governo e pessoas físicas, pode ser aplicada em praticamente todas as áreas e situações.

É o que ressalta Silva (2012), quando afirma que "informações pessoais e conhecimentos empíricos são parte de um sistema que possui características comportamentais e psicológicas, no qual a Engenharia Social necessita do auxílio de algumas técnicas específicas. "

Os engenheiros sociais estudam técnicas de linguagem corporal, grafologia e outras, para obter as informações que procuram. Estudam o comportamento de seus alvos, buscando descobrir suas rotinas, círculos sociais e seus hábitos, procurando coletar o máximo de informação para realizar o ataque. (MAULAIS, 2016).

Para Mitnick; Simon (2003, p. 85):

> Os engenheiros sociais habilidosos são adeptos do desenvolvimento de um truque que estimula emoções como o medo, agitação ou culpa. Eles fazem isso utilizando gatilhos psicológicos, que são mecanismos automáticos que levam as pessoas a responderem às solicitações sem uma análise cuidadosa das informações disponíveis.

Os ataques podem ser realizados por diversos meios. Os mais comuns são através de telefonemas, e-mail falso, verificação de lixo, abordagem pessoal e mapeamento das redes sociais. Para Silva (2012), "os ataques podem ser direcionados a um indivíduo específico dentro

de uma organização ou através de terceiros, que possuam maior grau de vulnerabilidade e maior acesso ou confiança do alvo principal. ”

O engenheiro social consegue representar um papel, como se fosse um personagem de um filme. Em determinadas situações, assume o papel de um funcionário de alguma organização conhecida, em outras, afirma ser funcionário da mesma organização, porém de outro setor ou outra filial.

De acordo com Mitnick; Simon (2006, p. 188), “o engenheiro social usa a arte de enganar como uma das armas de seu kit de ferramentas, procura explorar traços comportamentais da natureza humana. ”

Quando realizam ataques “físicos”, procuram escolher roupas e acessórios que transmitam credibilidade e confiança. Mitnick; Simon (2006, p. 198) afirmam que “a força desse método se deve ao fato que, ao aceitarmos alguém, fazemos inferências e atribuímos outras características a essa pessoa. ”

Na maioria dos ataques de Engenharia Social, o primeiro passo é obter credibilidade e a confiança da vítima. Para isso, o engenheiro social geralmente utiliza três métodos para alcançar o objetivo. No primeiro, faz algo que parece ir contra seu interesse, como por exemplo, dizer para a vítima inserir uma senha, mas alertá-la em não falar em voz alta, passando uma imagem de confiança. (MITNICK; SIMON, 2006).

O segundo e terceiro método geralmente são utilizados juntos. Neles, o atacante faz uma advertência de um evento a vítima. Este evento será provocado pelo atacante, sem que a vítima saiba. Em seguida, após o evento ter ocorrido, o atacante informa a vítima que consegue corrigir o problema. (MITNICK; SIMON, 2006). Assim, consegue a confiança e gratidão da vítima.

Atualmente os engenheiros sociais têm uma grande facilidade para obter informações: as redes sociais. Estas são acessadas normalmente pelo mesmo smartphone que o usuário utiliza para suas tarefas corporativas, muitas vezes acessando redes *wi-fi* públicas.

As redes sociais podem ser utilizadas pelos engenheiros sociais para conhecer melhor seu alvo, pois nelas é possível encontrar gostos pessoais, círculo de amizades e outras informações que serão uteis para traçar o perfil do alvo e utilizar as melhores técnicas de Engenharia Social.

Para Dawel (2005, p.72), “as técnicas da Engenharia Social podem ser divididas em duas categorias diferentes, no que diz respeito ao modo de atuação: física e psicológica. ”

Procurar informações no lixo, em papéis ou mídias eletrônicas; entrar em uma empresa oferecendo algum tipo de serviço, para ter acesso a algum tipo de informação; escutar conversas telefônicas, estes são alguns exemplos de ações físicas da Engenharia Social.

Em relação as questões psicológicas, o engenheiro social busca explorar o comportamento humano e sua tendência a confiar nas pessoas, a ser prestativo, curioso, solidário. (DAWEL, 2005).

Para Mitnick; Simon (2003, p.27), "os trapaceiros de informações experientes não têm escrúpulos em ligar para os governos federal, estadual ou municipal para saber os procedimentos da aplicação das leis. " Sendo assim, com a informação necessária, o engenheiro social pode contornar as verificações de segurança padrão de organizações ou de qualquer outro alvo.

3.2 FATOR HUMANO: O ELO MAIS FRACO DA SEGURANÇA

Com frequência, a segurança é apenas uma ilusão, que às vezes piora quando entram em jogo a credulidade, inocência ou a ignorância. Ataques da engenharia social podem ter sucesso quando as pessoas em geral, apenas desconhecem as boas práticas da segurança. (MITNICK; SIMON, 2006, p.3).

Com o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os ataques se voltam cada vez mais para a exploração do elemento humano. (MITNICK; SIMON, 2006).

Explorar falhas humanas geralmente exige pouco investimento e esforço, como por exemplo, uma ligação telefônica, e envolve um risco mínimo. Explorando traços psicológicos e comportamentais, o atacante consegue informações importantes.

Os engenheiros sociais têm alvos bem-definidos e são motivados pelo ganho financeiro. Concentram-se em um alvo de cada vez e não são como os amadores, que tentam se infiltrar no maior número possível de sistemas. "Enquanto intrusos amadores de computadores apenas buscam quantidade, engenheiros sociais visam as informações de qualidade e valor. " (MITNICK; SIMON, 2003, p. 6).

Ataques de Engenharia Social são pessoais. Os hackers entendem que os funcionários costumam ser o elo mais fraco de um sistema de segurança - eles são suscetíveis

a truques e suas respostas variadas podem oferecer aos invasores muitas oportunidades de sucesso. (CISCO, 2018. Tradução nossa).

Os atacantes exploram vulnerabilidades e privilégios de usuários para ter acesso a informações privilegiadas. Eles exploram o elo mais fraco dentro de qualquer sistema de Segurança da Informação, o ser humano. (BARKER, 2018. Tradução nossa).

A grande maioria das violações de segurança cibernética, se devem a negligência dos colaboradores ou ações maliciosas conscientes. Uma vez no interior, os atacantes usam acesso privilegiado para explorar a rede, assumindo o controle de mais ativos e dados críticos.

Um dos maiores perigos da Engenharia Social é que os ataques não precisam funcionar contra todos. Uma única vítima bem-sucedida pode fornecer informações suficientes para acionar um ataque que afetará toda a organização. (CISCO, 2018. Tradução nossa).

Independentemente de saber se os usuários de uma organização são negligentes, descuidados, ou simplesmente desinformados, é importante implementar os controles de segurança.

Os riscos de segurança da Engenharia Social são significativos e as organizações necessitam estar preparadas para lidar com ameaças de Engenharia Social como parte de uma estratégia geral de gerenciamento de riscos.

Pode-se afirmar que “a melhor maneira de mitigar o risco apresentado pelos métodos de Engenharia Social em rápida evolução é através de um compromisso organizacional com uma cultura consciente da segurança. ” (CISCO, 2018. Tradução nossa).

O treinamento contínuo fornece aos funcionários as ferramentas necessárias para reconhecer e responder às ameaças de Engenharia Social, e o apoio da equipe executiva criará uma atitude de propriedade e responsabilidade que incentiva a participação ativa na cultura de segurança.

A melhor forma de evitar problemas não intencionais ligados à Segurança da Informação é fornecer a todos os funcionários um treinamento regular de conscientização da importância da segurança. “Esse treinamento deve informar os funcionários sobre novas ameaças e atualizar sua compreensão sobre como identificar e evitar ataques de Engenharia Social. ” (CISCO, 2018. Tradução nossa).

Com treinamentos adequados, os funcionários podem assimilar as medidas de segurança implantadas, podem saber como manipular informações sigilosas e reconhecer possíveis ataques de Engenharia Social.

Dentro de uma organização, alguns funcionários podem estar mais expostos aos ataques de Engenharia Social, como administradores de redes, por exemplo. Esses, devem ter acesso a treinamentos mais específicos.

Uma avaliação de risco contínua que testa a resistência dos funcionários às tentativas e técnicas de Engenharia Social ajuda a avaliar a validade do programa de treinamento e das políticas de segurança implantadas, e pode aumentar ainda mais a conscientização sobre a Segurança da Informação dentro da organização.

3.3 AS PRINCIPAIS TÉCNICAS DE ATAQUE DE ENGENHARIA SOCIAL

Os ataques realizados através da Engenharia Social normalmente são feitos através do envio de e-mails falsos, telefonemas, pessoalmente, através de investigação das redes sociais.

De acordo com Coimbra (2010), “outras técnicas muito utilizadas na Internet são os sites anônimos que prometem muitas coisas com acesso grátis, bastando você fornecer a eles seu nome de usuário e senha. ”

O impacto dos ataques contra empresas geralmente é alto, pois os riscos e ameaças não são totalmente conhecidos. Um artigo do site Inove Dados (2017) mostra os perigos que as organizações correm, ao afirmar que “a Engenharia Social não é apenas um método de ataque digital para obter acesso a computadores e dados computacionais, essa técnica pode ser aplicada através do telefone, internet ou até pessoalmente. ”

Os tipos mais comuns de ataques de Engenharia Social de acordo com os sites Proof (2018) e Inove Dados (2017) incluem *phishing, baiting*, *pretexting*, *spear phishing* entre outras.

A seguir serão descritas algumas técnicas mencionadas pelos autores citados anteriormente.

3.3.1 Phishing

O principal objetivo é induzir a vítima a inserir informações pessoais ou confidenciais, nome, número de documentos, senhas, informações de conta e cartões.

O phishing é atualmente, de acordo com Cisco (2018, tradução nossa), "a técnica de ataque de Engenharia Social mais utilizada e possui algumas variações. Normalmente os agentes de ameaças utilizam para enviar e-mails falsos, que parecem ser de alguma organização conhecida. "

Nesta técnica são produzidas mensagens, comunicações ou informações fraudulentas com a intenção de fazer os alvos a acreditarem que são verdadeiras. Dessa maneira, acabam instalando *malwares* em seus dispositivos ou a compartilham informações pessoais, financeiras ou de negócio. (PROOF, 2018).

De acordo com artigo do site Canaltech (2018), trata-se de "ação fraudulenta caracterizada por tentativas de adquirir ilicitamente dados pessoais de uma pessoa ou organização - senhas, dados financeiros, dados bancários, números de cartões de crédito. "

Algumas das variações deste tipo de ataque são citadas a seguir:

Watering hole - Este ataque determina primeiro sites que um grupo-alvo visita regularmente. Em seguida, o agente de ameaça tenta comprometer esses sites, infectando-os com malwares que podem identificar e segmentar apenas membros do grupo-alvo.

Vishing - Este é um ataque de phishing usando voz e sistema de telefone em vez de e-mail.

Smishing - Este é um ataque de phishing usando mensagens de texto SMS em vez de e-mail.

3.3.2 Baiting

Esta técnica ocorre quando o engenheiro social deixa à disposição de um usuário, algum dispositivo infectado com *malware,* como por exemplo, um pen-drive. O objetivo é despertar a curiosidade do indivíduo, para que insira o dispositivo em um computador a fim de checar seu conteúdo.

Para obter sucesso, esse ataque depende de três ações do indivíduo: encontrar o dispositivo, abrir seu conteúdo e instalar o *malware* sem perceber. Após instalado, o *malware* permite que o atacante tenha acesso aos sistemas que o usuário utiliza.

Essa tática necessita de pouco trabalho, pois tudo que ele precisa fazer é "infectar um dispositivo e ocasionalmente deixá-lo à vista do alvo, seja na entrada ou no interior dos escritórios. " (INOVE DADOS, 2017).

3.3.3 Pretexting

O atacante precisa apenas encontrar um alvo e investigar seu perfil em redes sociais, por exemplo, buscando informações que auxiliem o ataque. Com as informações necessárias, basta realizar um contato com o alvo criando alguma situação para obter o que deseja.

"Nesse tipo de ataque, falsas circunstâncias coagem a vítima a oferecer acesso a informações e sistemas críticos. Os *hackers* assumem uma nova identidade ou papel para fingir que são alguém de confiança da vítima. " (PROOF, 2018).

3.3.4 Spear phishing

É uma variação do *Phishing*. Nesta técnica, é disparado um e-mail direcionado a um grupo, uma pessoa ou uma organização específica. Tem o objetivo único de obter acesso não autorizado aos dados sigilosos. Após obter acesso, busca roubar propriedade intelectual, dados financeiros, segredos comerciais ou militares e outros dados confidenciais. (KASPERSKYLAB, 2018).

No caso de ataque a uma organização, o engenheiro social pode se passar por um executivo ou membro de outro setor e aborda funcionários com intuito de obter informações sensíveis. (PROOF, 2018).

Através das redes sociais, pode-se obter informações sobre o alvo e o quadro organizacional da organização. "Com essas informações em mãos, basta enviar uma

comunicação fingindo ser, por exemplo, um executivo da empresa com uma demanda urgente que requer uma transação financeira imediata para uma conta específica. ” (PROOF, 2018).

Como a maioria das pessoas não percebe pequenos indícios de fraude, normalmente esse tipo d ataque tende a atingir sucesso no convencimento de funcionários, para que estes executem ações específicas ou revelem informações importantes e sigilosas.

3.3.5 Pharming

Este tipo de ataque também é uma variação do *Phishing* e de acordo com Inove Dados (2017), “é a combinação de técnicas avançadas de invasão com Engenharia Social, o *pharming* visa envenenar o servidor DNS da vítima que é responsável por redirecionar os sites acessados para o endereço correto. ”

Esta técnica direciona todo tráfego para sites falsos, por exemplo, é possível fazer com que quando o usuário acessar o site de um banco, ele seja direcionado para um servidor falso, que tem uma cópia perfeita da tela do site original. (PROOF, 2018). Com isso, se consegue informações como senha, número de cartão e número de documentos pessoais.

3.3.6 Visual hacking

É aqui que um agente de ameaça observa fisicamente a vítima inserindo credenciais, como um *login* na estação de trabalho, um PIN do caixa eletrônico ou a combinação em um bloqueio físico. Esta prática é também referida como “surfar no ombro”. (CISCO 2018, tradução nossa).

3.3.7 Algo para algo (*Quid pro quo*)

A tática mais comum envolve se passar por alguém da TI e abordar diversas vítimas encontrar alguém com um problema real de TI. “Sob instruções do *hacker*, a vítima então dá acesso a códigos, desabilita programas vitais e instala *malware* achando que conseguirá resolver seu problema. (PROOF, 2018).

“Um ataque de quid pro quo ocorre quando um hacker requer informações privadas de alguém em troca de algo. “*Quid pro quo*” basicamente significa “isso por aquilo”, em que o atacante oferece algo à vítima em troca de informações sensíveis. ” (PROOF, 2018).

3.3.8 Análise de lixo

Este tipo de ataque é bastante utilizado, visto que as informações coletadas no lixo podem conter nome de funcionários, telefone, e-mail, senhas, contato de clientes, fornecedores, transações efetuadas, entre outros. Quando um engenheiro social pretende realizar um ataque direcionado à uma organização, este pode ser um dos primeiros passos.

“Provavelmente 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. ” (AUZAC, 2015).

4 MÉTODO

Neste capítulo serão apresentados os fundamentos metodológicos utilizados para a realização do presente trabalho.

A escolha do método correto para realizar qualquer pesquisa, pode ser comparada com a escolha do melhor caminho a se seguir. Para Motta et al. (2013, p.84), “o método é o ponto de ligação entre a dúvida e o conhecimento. ”

4.1 CARACTERIZAÇÃO DO TIPO DE PESQUISA.

De acordo com Motta et al. (2013, p. 104), “a pesquisa é um processo de investigação que se interessa em descobrir as relações existentes entre os aspectos que envolvem os fatos, fenômenos, situações ou coisas. ”

“Para se desenvolver uma pesquisa, é indispensável selecionar o método de pesquisa a utilizar. De acordo com as características da pesquisa, poderão ser escolhidas diferentes modalidades de pesquisa. ” (GERHARDT; SILVEIRA, 2009, p. 36).

O presente trabalho tem como sua principal base a pesquisa bibliográfica, pois de acordo com Motta et al. (2013, p. 114), “se desenvolve tentando explicar um problema a partir das teorias publicadas em diversas fontes: como livros, artigos científicos, artigos publicados em site especializados, manuais. ”

Quanto aos objetivos de estudo, a pesquisa realizada é uma pesquisa aplicada, pois pode gerar conhecimentos para aplicações práticas e voltadas a solução de problemas específicos, no caso do presente trabalho, as ameaças ligadas a ataques de Engenharia Social.

Quanto a abordagem, este trabalho utiliza a pesquisa qualitativa. De acordo com Gerhardt; Silveira (2009, p. 32), “A pesquisa qualitativa preocupa-se, portanto, com aspectos da realidade que não podem ser quantificados, centrando-se na compreensão e explicação da dinâmica das relações sociais. ” Os principais focos da abordagem são analisar os riscos e vulnerabilidades ligados a ataques de Engenharia Social dentro de uma organização.

Sendo assim, pode se enquadrar na classificação quanto ao nível, como uma pesquisa exploratória, que, de acordo com Motta et al. (2013, p. 106), “proporciona maior familiaridade com o objeto de estudo. ”

Para validar os resultados será aplicado um teste de intrusão (*Pen Test*) de Engenharia Social. O teste de intrusão consiste em um processo de análise detalhada do nível de Segurança da Informação pela perspectiva de um invasor.

O *Pen Test* é um conjunto de técnicas e ferramentas utilizadas para identificar falhas de segurança em sistemas e redes corporativas. Assim é possível identificar as vulnerabilidades existentes na arquitetura da empresa, explorá-las e entregar um relatório à empresa, que deverá então tomar as devidas ações para corrigir as falhas de segurança. (PROFISSÃO HACKER, 2018).

4.2 ETAPAS METODOLÓGICAS

Para se alcançar o objetivo principal será realizado um estudo de caso em uma organização corporativa de pequeno porte da área vidraceira, no município de Palhoça. Estas atividades são descritas abaixo:

- definição dos objetivos;
- identificação dos riscos:
- análise de riscos e vulnerabilidades;
- definição das estratégias;
- aplicação das técnicas de Engenharia Social;
- análise dos resultados.

O período de realização destas etapas está descrito no cronograma apresentado no Apêndice A que se encontra no final do presente trabalho.

4.3 DELIMITAÇÕES

Toda pesquisa científica precisa de uma delimitação, para Motta et al. (2013, p.139), “delimitar é indicar a abrangência do estudo; é estabelecer os limites conceituais do tema. ”

O presente trabalho aborda a Segurança da Informação, delimitado apenas aos ataques relacionados à Engenharia Social aplicados ao elo mais fraco de todo e qualquer sistema de Segurança da Informação: o usuário. O trabalho se desenvolverá através de um estudo de caso.

O objetivo é realizar uma avaliação de riscos e vulnerabilidades relacionados à Engenharia Social em um ambiente corporativo, aplicando algumas técnicas para explorar essas vulnerabilidades, e encontrar maneiras de mitigar os riscos.

Não será desenvolvido nenhum *software* ou sistema para dar suporte a análise dos riscos e vulnerabilidades, nem para realizar as simulações de ataque.

5 ESTRATÉGIAS DE ENGENHARIA SOCIAL

Este capítulo tem como objetivo apresentar as etapas que serão realizadas para o desenvolvimento de uma auditoria de Segurança da Informação com foco em ataques de Engenharia Social.

Em um processo de auditoria se verifica se tudo funciona como planejado. Através de auditorias é possível examinar se as políticas de Segurança da Informação estão em conformidade com os padrões exigidos pelas normas técnicas vigentes. (KIM; SOLOMON, 2014).

Para Lento (2011), toda auditoria é dividida em três fases: planejamento, onde são identificados os instrumentos necessários para sua realização; a execução, onde são reunidas evidências confiáveis, relevante e úteis para o alcance dos objetivos; relatório, onde serão apresentados os resultados e análises obtidos pela auditoria.

Para realizar esta auditoria serão efetuadas algumas etapas de avaliação de riscos e vulnerabilidades ligadas exclusivamente a ataques de Engenharia Social. Realizar uma análise de riscos e vulnerabilidades é fundamental para diagnosticar a real situação da Segurança da Informação da organização.

1ª etapa: planejamento

A primeira etapa desta avaliação de riscos e vulnerabilidades consiste em definir seu objetivo. No caso do presente trabalho, será mitigar os riscos causados por ataques de Engenharia Social.

Em seguida, deve-se identificar os riscos que podem afetar a organização. Os principais vetores de ataques de Engenharia Social são: online, telefone, gerenciamento de lixo, abordagens pessoais e Engenharia Social Reversa. É necessário também saber o que o atacante deseja conseguir. Geralmente, os principais objetivos são financeiros e informações sigilosas.

O próximo passo deve ser analisar os riscos, identificando quais informações a organização armazena e o seu valor. Assim, é possível identificar quais ameaças pode sofrer e distinguir o grau de impacto de cada risco, estimando também os custos de um incidente.

Após realizar estas etapas, será possível realizar um planejamento do tratamento dos riscos, enumerando as ameaças que devem ser atacadas primeiro, buscando mitigar as vulnerabilidades encontradas.

2ª etapa: execução

Com os riscos e vulnerabilidades identificados, será analisado, através da auditoria se o planejamento do tratamento dos riscos está sendo executados e se as políticas de Segurança da Informação voltadas para ataques de Engenharia Social estão surtindo o efeito esperado.

Os riscos devem ser monitorados e analisados constantemente, pois a todo instante novas ameaças podem surgir e explorar vulnerabilidades já existentes ou que também possam surgir. O processo de monitorar e controlar riscos deve focar na identificação e análise de novos riscos e controle daqueles já identificados.

Para validar o resultado da proposta apresentada, foi aplicado um teste de intrusão (*Pen Test*) de Engenharia Social.

3ª etapa: apresentação dos resultados

Nesta etapa são apresentados os resultados obtidos através do estudo de caso. Após utilizar as técnicas de Engenharia Social escolhidas pode-se ter uma visão da situação atual na organização.

A seguir apresentamos as técnicas de Engenharia Social que serão utilizadas no estudo de caso escolhido.

5.1 ATAQUES UTILIZANDO VISHING E SMISHING

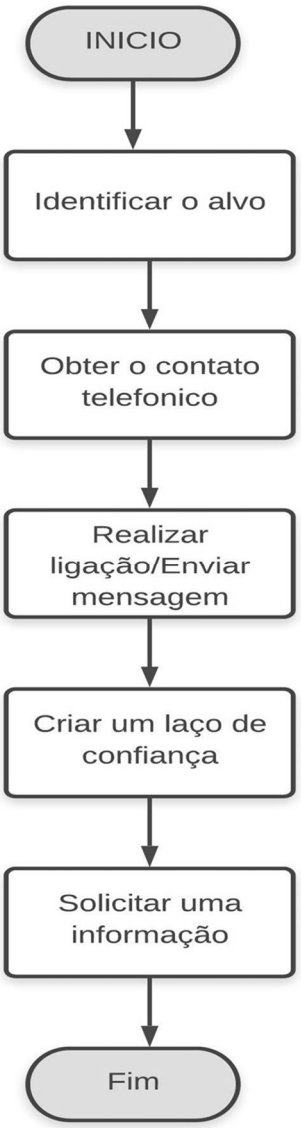
Como mencionado anteriormente, essas técnicas utilizam ligações e mensagens telefônicas. Utiliza-se esta técnica com o objetivo de obter dos funcionários da organização alguma informação importante para o negócio da empresa.

O estudo de caso foi realizado em uma organização que atua na indústria e comercio de vidros e será detalhada no capítulo 6. Utilizando a informação que atua no comércio de vidros, iremos realizar ligações para o setor comercial nos passando por clientes, com a intenção de obter informações que nos sejam valiosas.

Uma ferramenta muito utilizada atualmente por praticamente todas as pessoas é o *whatsapp*. Essa ferramenta nos permitirá enviar mensagens para alguns setores da organização, buscando obter informações que possam ser utilizadas a nosso favor.

A figura 4 apresenta um fluxograma que mostra os passos para utilizar esta técnica.

Figura 4 – Fluxograma de um ataque utilizando *vishing/smishing.*



Fonte: elaborado pelo autor, 2019.

5.2 A TÉCNICA DE *BAITING*

De acordo com o que já foi citado anteriormente neste trabalho, *baiting* é uma técnica antiga, mas que já foi muito utilizada. Esta técnica explora a curiosidade do alvo, durante o teste se oferece ou esquece propositalmente um dispositivo de armazenamento em algum local estratégico, geralmente onde existe a circulação de muitos funcionários.

Nessa parte do teste, iremos inserir um arquivo com o nome “salário funcionários” em um *pen drive*. O *pen drive* será deixado próximo a alguns computadores no escritório.

A intenção é fazer com que algum funcionário morda a isca e insira o dispositivo em sua estação de trabalho, acessando os arquivos. O nome do arquivo chama a atenção e explora a curiosidade das pessoas.

Para se obter sucesso com esta técnica, o ataque dependerá de algumas ações do indivíduo que sofrerá o ataque: ele deve encontrar o dispositivo, em seguida deve sentir a curiosidade de conectar em seu computador e abrir seu conteúdo.

Em uma outra estratégia para utilizar esta técnica, iremos criar uma situação e entregar o dispositivo de armazenamento para o funcionário alvo. Essa situação pode ser pedir para o alvo copiar músicas, fotos ou filmes a partir do dispositivo, e colocar o malware dentro de um desses arquivos, levando o alvo a abrir sem perceber. O intuito aqui é explorar a boa vontade e a curiosidade das pessoas.

A figura 5 mostra um fluxograma apresentando as etapas que serão realizadas para realizar o ataque utilizando esta técnica.

Figura 5 – Fluxograma de um ataque utilizando a técnica de *baiting*.

Fonte: elaborado pelo autor, 2019.

5.3 A TÉCNICA DE ANÁLISE DE LIXO

A maioria das organizações não tem o cuidado de verificar o que é descartado da empresa e de que forma é realizado este descarte. O lixo de uma empresa é uma das fontes mais ricas de informações para os Engenheiros Sociais.

Iremos analisar as estações de trabalho da empresa e como são descartados seus papeis. A intenção será coletar informações que podem conter nome de funcionários, telefone, e-mail, senhas, contato de clientes, fornecedores, transações efetuadas, entre outros.

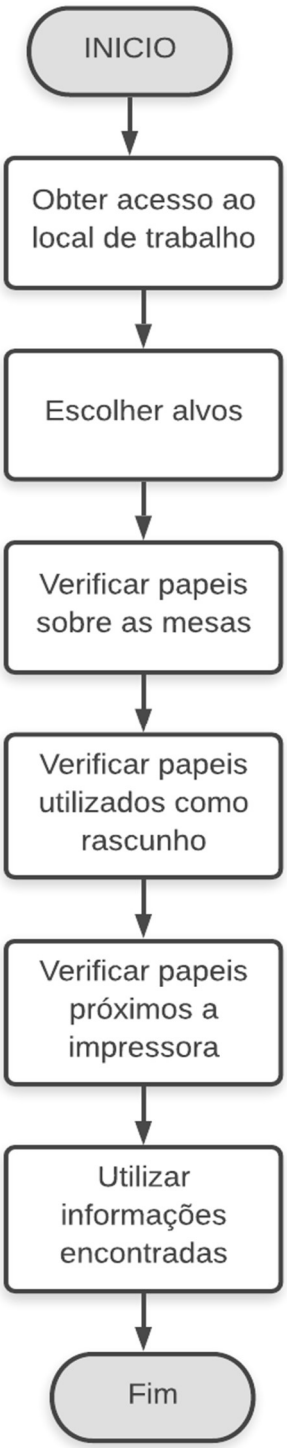
A grande maioria das empresas acaba reaproveitando folhas impressas de documentos ou e-mails que são de circulação interna. Muitos funcionários acabam utilizando relatórios, demonstrativos de operações bancárias ou pagamentos como rascunho. Esses rascunhos podem conter informações sigilosas. (ARRUDA, 2011).

Vamos tentar encontrar papéis que possam conter informações aparentemente simples, como o nome ou o telefone de pessoas e departamentos. Esses papéis costumam ficar próximo as impressoras e muitas vezes nas mesas dos funcionários.

Esta técnica será utilizada junto com a técnica conhecida como surfar sobre os ombros. Nós ficaremos próximo de outros funcionários para olhar o que digitam no teclado, olhar os papéis sobre a mesa de trabalho, tentar identificar o que está sendo realizado no computador. Tudo será realizado para tentar buscar o máximo de informações sem que o alvo escolhido perceba.

A figura 6 apresenta um fluxograma que mostra os passos para utilizar esta técnica.

Figura 6 – Fluxograma de um ataque utilizando a técnica de análise de lixo.



Fonte: elaborado pelo autor, 2019.

5.4 A TÉCNICA DE *PHISHING*

Como mencionado no presente trabalho, uma das técnicas mais utilizadas em ataques envolvendo Engenharia Social é o *phishing.* Será realizado um teste com um ataque de *phishing* contra os funcionários da empresa Tudo Vidro. Este teste é um dos processos que pode auxiliar os responsáveis pela Segurança da Informação a fazer um diagnóstico mais preciso, e assim, identificar quais são os colaboradores mais vulneráveis e suscetíveis as ameaças.

O primeiro passo a ser dado será realizar a identificação dos possíveis alvos, utilizando para isso contatos diretos com o intuito de identificar as características comportamentais dos colaboradores e a posição que ocupam dentro da empresa, o que facilitará o acesso as informações sensíveis, caso o alvo escolhido acabe caindo na armadilha.

Para realizar esta experiência, utilizou-se a ferramenta online *Sophos Phish* para realizar uma simulação de ataques de phishing. Esta ferramenta possui modelos de e-mails pré-definidos, mas também permite criar e-mails personalizados. A ferramenta cria relatórios e informa quais contatos abriram e clicaram no link do falso e-mail.

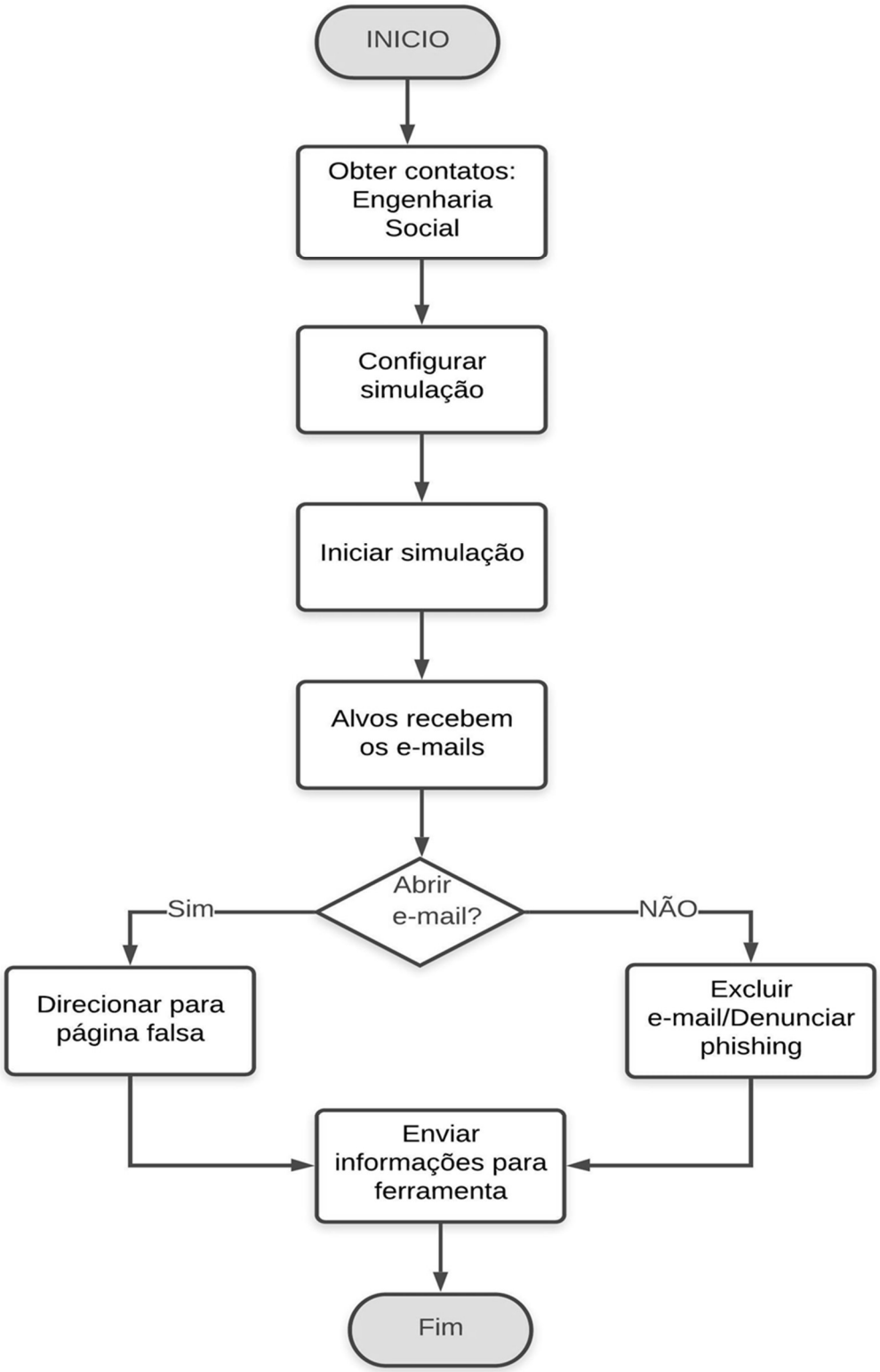
É possível ainda configurar para que envie um e-mail automático informando ao funcionário que ele foi alvo de um teste ou direcioná-lo para um treinamento online sobre os riscos de ataques de phishing. A escolha por esta ferramenta deu-se pelo fato de ser gratuita e por ser uma boa opção para realizar o trabalho acadêmico.

Com a aplicação deste teste, é possível identificar os colaboradores mais cuidadosos, aqueles que seguem as recomendações de Segurança da Informação e tem consciência do que não deve ser acessado, principalmente dentro da organização.

Também é possível identificar os colaboradores que não seguem essas recomendações, com isso, a organização pode trabalhar na conscientização sobre a proteção das informações e o cuidado que cada colaborador deve ter ao acessar a internet.

Uma forma de exemplificar os passos a serem seguidos para realizar o ataque utilizando a técnica de phishing pode ser vista em um fluxograma que está na figura 7.

Figura 7 – Fluxograma de um ataque utilizando a técnica de *phishing*.



Fonte: elaborado pelo autor, 2019.

6 ESTUDO DE CASO

O presente capítulo apresenta um estudo de caso onde descreve a aplicação das estratégias descritas no capítulo anterior. Este estudo de caso tem como objetivo analisar as vulnerabilidades de Segurança da Informação, com foco em ataques de Engenharia Social em uma organização do ramo vidraceiro no município de Palhoça.

6.1 FERRAMENTAS UTILIZADAS

Para realizar o estudo de caso desenvolvido no presente trabalho de conclusão de curso foram utilizadas algumas ferramentas, que são apresentadas a seguir, na figura 8.

Figura 8 – Ferramentas utilizadas.

Fonte: elaborado pelo autor, 2019.

Para realizar as pesquisas bibliográficas foram utilizados livros disponibilizados na biblioteca virtual da Unisul. Utilizou-se o Meu Pergamum, um sistema integrado da biblioteca. Foram realizadas pesquisas em sites e blogs que abordam o tema escolhido, utilizando para

isso, o navegador Chrome. Para o desenvolvimento do trabalho escrito foi utilizada a ferramenta Word. Os fluxogramas foram desenvolvidos na ferramenta online Lucidchart.

Para a realização do estudo de caso, e aplicação das técnicas de Engenharia Social foram utilizadas as seguintes ferramentas: *whatsapp*, para realizar contatos com os funcionários, buscando coletar informações; a ferramenta online *Sophos Phish,* que possibilita criar simulações personalizadas de ataques de *phishing*.

A ferramenta *Sophos Phish* permite a criação de simulações personalizadas de ataques de phishing, e assim, avaliar como os usuários alvo do ataque respondem as simulações. É possível também distribuir treinamentos *anti-phishing* aos colaboradores da empresa.

6.2 DESCRIÇÃO DA ORGANIZAÇÃO

A organização corporativa utilizada no estudo de caso atua na área vidraceira há aproximadamente 25 anos. É uma empresa de médio porte, possui aproximadamente 40 funcionários, sendo cerca de 12 na parte do escritório, distribuídos nos setores administrativo, financeiro e comercial. A sede da empresa é localizada no munícipio de Palhoça e possui uma filial, somente com escritório comercial em Porto Alegre, no Rio Grande do Sul.

Foi solicitado que não se divulgue o nome da empresa nem informações que são consideradas estratégicas para organização, por isso foi atribuído um nome fictício: Tudo Vidro.

A empresa Tudo Vidro contava com um funcionário que atuava exclusivamente na área de TI, prestando suporte aos sistemas internos e *hardwares* da organização. Atualmente, esta função é exercida por uma empresa terceirizada.

A realização deste estudo de caso foi autorizada por um dos diretores e apenas ele e uma funcionária do setor administrativo estão cientes do processo que foi realizado. Utilizou-se o nome fictício de Maria. Durante o processo, foram realizadas algumas visitas a empresa Tudo Vidro e contamos com o apoio de Maria em algumas ações.

A escolha da organização para realizar este trabalho foi motivada pelo fato de o autor deste trabalho conhecer a forma como as informações são tratadas pelos colaboradores e pela direção.

É de conhecimento do autor do presente trabalho que a empresa sofreu dois ataques ao seu sistema nos últimos 12 meses. No primeiro ataque, a empresa ficou sem operar por 3 dias. Foi exigido o pagamento de um valor para liberar acesso ao sistema. Nessa época, a empresa estava trocando o sistema, e, só conseguiu voltar a operar, porque conseguiu o *backup* do novo sistema, perdendo informações do sistema antigo.

No segundo ataque, a empresa já operando totalmente pelo novo sistema, conseguiu realizar um backup, e, no mesmo dia voltou a operar novamente. A suspeita da direção, é que, ambos os ataques ocorreram por falha de algum colaborador da empresa, porém, não conseguem comprovar.

6.3 IDENTIFICAÇÃO DAS VULNERABILIDADES E ANÁLISES DOS RISCOS

Através de conversas com o diretor e com a funcionária foi possível levantar algumas vulnerabilidades existentes no tratamento das informações dentro e fora da empresa. Pode-se verificar que não possui nenhuma política de gestão ou gerenciamento de Segurança da Informação e que os funcionários estão sujeitos a todo tipo de ataques.

A empresa Tudo Vidro possui um sistema que integra todos os setores, incluindo a produção. Cada setor tem um *login* e senha que permite acesso ao sistema e apenas o líder do setor deveria saber. No entanto, constatou-se que outros funcionários também têm acesso a essas informações.

Em duas ocasiões, a empresa foi alvo de ataques que causaram grandes transtornos e prejuízo financeiro. O primeiro ataque ocorreu quando era realizada a troca do seu sistema de gerenciamento.

O ataque bloqueou todo o acesso ao sistema antigo e exigiu o pagamento de uma quantia em dinheiro para a liberação. Constatou-se que foi acessado dentro da empresa, um *e-mail* falso contendo o código malicioso em anexo. Até então, os funcionários não haviam recebido nenhuma orientação ou treinamento no que diz respeito ao acesso de *e-mails*.

Nesse primeiro ataque, a empresa Tudo Vidro ficou 3 dias parada, pois não conseguiram acesso ao backup também. Só foi possível recuperar o que já havia migrado para o novo sistema. O diretor calcula que houve um prejuízo de aproximadamente R$ 200.000,00 reais nesse período.

O segundo ataque que a empresa sofreu, deixou o sistema fora de operação por um dia, pois a fornecedora do novo sistema possuía *backup*. O diretor não soube informar como ocorreu esse ataque.

6.4 APLICAÇÃO DAS TÉCNICAS E RESULTADOS OBTIDOS

Com o objetivo de validar as estratégias utilizadas em ataques de Engenharia Social em organizações corporativas, o autor procurou aplicar algumas técnicas na empresa escolhida. É bom ressaltar que a empresa Tudo Vidro não possui políticas de gerenciamento de Segurança da Informação e os gestores não tinham ideia do que se trata a Engenharia Social, nem dos estragos que pode causar. A empresa terceirizada contratada para dar suporte na área de TI faz apenas a manutenção de *hardwares* e *softwares* da organização.

Nas visitas realizadas na Tudo Vidro pode-se constatar que os funcionários não dão o devido fim aos papeis utilizados no escritório. Foram encontrados sobre as mesas dos funcionários do setor administrativo, papeis contendo o balancete dos meses de julho, agosto e setembro de 2019.

Outra situação que foi percebida, em conversas com as funcionárias, é que algumas utilizam esses papeis como rascunho no escritório ou levam para casa, com a justificativa que é para seus filhos desenharem. Segundo o diretor da empresa, esse hábito sempre existiu, e até então, não havia percebido que esses atos podem gerar grandes problemas para a empresa.

Como mencionado no item 6.3, a empresa possui um sistema que integra todos os setores e que cada líder de setor deveria ser o único a possuir o acesso. No entanto, pode-se constatar também que na prática não é assim que funciona. Em uma das visitas ao escritório, podemos ver uma funcionária do setor administrativo solicitou o *login* e a senha de acesso do setor comercial a uma das vendedoras e essa prontamente atendeu. O detalhe aqui é que essa informação deveria ser de conhecimento apenas da gerente comercial.

No decorrer do estudo de caso, obtivemos acesso ao celular de uma funcionária. Utilizando seu *whatsapp*, solicitamos ao gerente da filial que nos enviasse um relatório de vendas por *e-mail* e que nos encaminhasse seu *login* e senha ao sistema na filial pelo aplicativo. O gerente prontamente atendeu, enviando primeiro as informações de acesso ao sistema e mais

tarde o relatório. Em nenhum momento houve contestação ou alguma ligação par confirmar se realmente era a funcionária quem estava solicitando.

Nesse caso foi apenas uma situação controlada, que faz parte de um trabalho acadêmico. As informações foram deletadas assim que recebidas. Porém, mais uma vez mostrou-nos a falta de zelo e o mínimo de preocupação com as informações da empresa, pois em nenhum momento cogitou-se que o aplicativo *whatsapp* pudesse ter sido clonado.

Pode-se constatar também que em algumas ocasiões utilizam seus *e-mails* pessoais para tratar de assuntos da empresa. Alguns funcionários também utilizam seus celulares particulares, com o aplicativo de troca de mensagens no aplicativo *whatsapp* para tratar de assuntos ligados a empresa.

Outro ponto levantado refere-se a facilidade que clientes tem em acessar algumas salas do escritório. Através de uma visita a empresa Tudo Vidro e de conversas com uma funcionária do setor administrativo, pode-se perceber que por possuírem uma certa confiança, alguns clientes mais antigos têm livre acesso ao setor administrativo.

Os riscos que essa atitude oferece são enormes, pois constatou-se que a empresa não possui cuidados com papeis impressos, e esses geralmente ficam sobre as mesas. Esses papeis contem balancetes, planilhas de venda e faturamento e algumas informações que deveriam ser resguardadas, como contas de banco de fornecedores e até da própria empresa.

Em relação a facilidade que os clientes têm em entrar no escritório, foi relatado pelo diretor, que em uma ocasião, uma pessoa veio fazer uma negociação de compra de uma grande quantidade de vidro. Após algum tempo de conversa e de ter conseguido a confiança de um dos sócios da, essa pessoa foi convidada a conhecer toda a fábrica, incluindo máquinas, processos da produção e projetos.

Ainda de acordo com o diretor, essa pessoa saiu sem realizar a compra. Algum tempo depois, após uma conversa com um antigo cliente, os sócios ficaram sabendo que aquela pessoa trabalhava para uma empresa do mesmo segmento, localizada no Rio Grande do Sul. Isso deixa claro que a falta de cuidados básicos com sua segurança, seja a do espaço físico, ou da Informação.

Durante as visitas realizadas, verificou-se que a empresa que presta serviços de TI para a Tudo Vidro, fez o bloqueio das portas USB dos computadores utilizados. Com isso, não foi possível utilizar a técnica de *baiting*. Verificou-se também que a empresa utiliza antivírus e *firewall* atualizados.

Através da análise nos papeis não descartados e de uma ligação feita para o setor comercial, foi possível obter o endereço de *e-mail* de oito funcionários. Utilizando a ferramenta *Sophos Phish,* foi realizado uma simulação de ataque de *phishing.* Foram escolhidos dois modelos criados pela ferramenta: um *e-mail* simulando um comunicado do Banco do Brasil, e outro, simulando uma solicitação de amizade do *Facebook*. O ataque foi configurado com duração de uma semana, durante o mês de outubro deste ano.

Pode-se verificar que dos oito funcionários alvos do ataque, cinco abriram os *e-mails*. Destes cinco, três abriram o *e-mail* com o comunicado do Banco do Brasil, sendo que dois acabaram clicando no *link*. Por se tratar de um trabalho acadêmico, esse *link* direcionava para uma página com informação de erro. O *e-mail* contendo uma solicitação de amizade do Facebook também foi aberto por três funcionários.

Como já descrito no trabalho, a maioria das empresas não dá a devida atenção aos ataques de Engenharia Social. Este estudo de casa demonstra essa condição, pois foi possível verificar que 62, 5% dos funcionários que foram alvo do ataque acabaram abrindo os *e-mails*, e, 40 % destes, clicaram no *link* que o *e-mail* trazia. Isso torna a situação preocupante, pois demonstra que estão suscetíveis a caírem em ataques de Engenharia Social, e com isso, acabam colocando a segurança das informações da empresa Tudo Vidro em risco.

Com a aplicação de algumas técnicas de Engenharia Social, pode-se constatar que, sem uma gestão eficiente de Segurança da Informação, que englobe os meios físicos e digitais, aliados a implementação de uma cultura de conscientização e treinamento dos funcionários, é improvável que a empresa possa garantir a confidencialidade, integridade, disponibilidade de suas informações.

7 CONCLUSÕES E TRABALHOS FUTUROS

Neste capítulo, apresentamos a conclusão deste trabalho, bem como a possibilidade de continuar explorando o assunto e o desenvolvimento de possíveis trabalhos relacionados ao tema.

7.1 CONCLUSÃO

Este trabalho permitiu realizar uma análise da Segurança da Informação em uma empresa, focando os estudos na utilização da Engenharia Social e em como esta é utilizada para explorar o elo mais fraco de todos os sistemas de segurança, o ser humano.

A informação é vista como um ativo valioso para todas as organizações empresariais, por isso, sistemas de Gerenciamento de Segurança da Informação são essenciais para a preservação deste ativo. No entanto, muitos criminosos utilizando técnicas de Engenharia Social conseguem burlar até os mais avançados sistemas de Segurança da Informação, pois, atacam os usuários desses sistemas, explorando características comportamentais.

Com a aplicação de algumas técnicas de Engenharia Social foi possível verificar a fragilidade e o pouco cuidado que a empresa alvo do estudo de caso apresenta ao tratar de suas informações. Os funcionários demonstraram estar despreparados para lidar com ameaças geradas pela Engenharia Social. Até a realização deste trabalho, a administração não tinha conhecimento sobre este tema.

Realizando ações simples, foi possível obter informações sigilosas e importantes para o negócio da empresa. Pode-se demonstrar para os diretores que a empresa se encontra vulnerável a ataques que utilizam Engenharia Social, e, que é necessário implementar uma política de treinamentos e de conscientização dos funcionários.

Foi possível compreender que de nada adianta um bom sistema de segurança, se os usuários não estiverem cientes do seu papel dentro do sistema de Segurança da Informação e da ameaça que a Engenharia Social representa.

Para que a informação seja protegida e que os critérios de confidencialidade, integridade e disponibilidade sejam atendidos, é necessária uma política de Segurança da

Informação que adote estratégias de capacitação e constantes campanhas de conscientização dos funcionários, aliado a um conjunto de instrumentos que possam implementar, operar, controlar e analisar ameaças, com o objetivo de mitigar os riscos para empresa.

7.2 TRABALHOS FUTUROS

O presente trabalho permitiu verificar as vulnerabilidades e os riscos que a empresa Tudo Vidro está sujeita em relação a ataques de Engenharia Social. Uma sugestão para trabalhos futuros, é desenvolver dentro da empresa, uma política de segurança focada em ataques de Engenharia Social, criando diretrizes baseadas nas principais normas de Segurança da Informação, visando mitigar os problemas encontrados.

REFERÊNCIAS

ALERTA SECURITY. **Análise de vulnerabilidade: o que é e como fazer?** 2018. Disponível em: <https://www.alertasecurity.com.br/analise-de-vulnerabilidade-o-que-e-e-como-fazer/> Acesso em: 27 out. 2018.

ARRUDA, Felipe. **Engenharia Social: o malware mais antigo do mundo.** Tecmundo, 2011.
Disponível em: < https://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm> Acesso em:03 mai. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 27001: Técnicas de segurança - Sistemas de gerenciamento de segurança da informação.** Rio de Janeiro, p. 27. 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 27002: Código de prática para a gestão da segurança da informação.** Rio de Janeiro, p. 140. 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 27005-2011: Gestão de riscos de segurança da informação** Rio de Janeiro, p. 76. 2011.

AUZAC. **Ataques de Engenharia Social.** 2015. Disponível em: <http://www.auzac.com.br/ataques-de-engenharia-social/> Acesso em: 08 nov. 2018.

BANNWAR, Claudio. **Engenharia Social nas Redes Sociais: a inteligência usada para o mal.** Canaltech. 2013. Disponível em:< https://canaltech.com.br/seguranca/Engenharia-Social-nas-Redes-Sociais/> Acesso em: 20 mai. 2019.

BARKER, Jessica. **Security Controls that Mitigate the Human Factor in Cyber Risk**. 2018.
Disponível em:
<https://info.beyondtrust.com/110718webinar.html?utm_campaign=WebinarBarker20181107&utm_medium=email&utm_source=btdbemea&mkt > Acesso em: 29 out. 2018.

BEZERRA, Edson Kowask. **Gestão de riscos de TI: NBR 27005.** Escola Superior de Redes. Rio de Janeiro, 2013. Disponível em: <https://www.portalgsti.com.br/2012/07/ebook-nbr-iso-27005.html> Acesso em: 03 nov. 2018.

CANALTECH. **O que é phishing?** 2018. Disponível em: <https://canaltech.com.br/seguranca/O-que-e-Phishing/> Acesso em: 16 set. 2018.

CICCO, Francesco De. **A nova norma internacional ISSO 27005 de Gestão de Riscos de Segurança da Informação.** Disponível em: <https://www.qsp.org.br/artigo_27005.shtml> Acesso em: 27 out.2018.

CISCO. **Protect Against Social Engineering.** Disponível em: <https://www.social-engineer.org/wiki/archives/AttackersMightUse/Ciscosocial-engineering.html> Acesso em: 07 nov.2018.

COIMBRA. **Engenharia Social: tipos comuns de ataque.** PROJETOS&TI. 2010. Disponível em: < https://projetoseti.com.br/engenharia-social-tipos-comuns-de-ataque/> Acesso em:23 out. 2018.

DAWEL, George. **A Segurança da Informação nas empresas.** Ciência Moderna. Rio de Janeiro, 2005.

FONTES, Edison. **Segurança da informação - 1ª edição**. Saraiva, 12/2001. [Minha Biblioteca]. Disponível em: <https://integrada.minhabiblioteca.com.br/books/9788502122185/pageid/29> Acesso em: 09 set. 2018.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação.** Pearson. 2015. Disponível em: <http://unisul.bv3.digitalpages.com.br/users/publications/9788543009452/pages/-6> Acesso em: 30 set. 2018.

GEER, David. **Conheça seis técnicas de Engenharia Social muito eficazes.** CIO, 2017. Disponível em: <http://cio.com.br/tecnologia/2017/04/09/conheca-seis-das-tecnicas-de-engenharia-social-muito-eficazes/> Acesso em: 23 out. 2018.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Método de pesquisa.** Universidade Federal do Rio Grande do Sul. Porto Alegre, 2009. Disponível em: <http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf> Acesso em: 04 nov. 2018.

HINTZBERGEN, Jule; HINTZBERGEN, Kees; SMULDERS, André; BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISSO 27001 e na ISO 27002.** Brasport, 2018. Disponível em: <http://unisul.bv3.digitalpages.com.br/users/publications/9788574528670> Acesso em: 04 out. 2018.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social.** Disponível em: <https://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social> Acesso em: 14 out. 2018.

KASPERSKYLAB. **O que é *spear phishing*?** 2018. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/spear-phishing> Acesso em: 23 out. 2018.

KOLBE JUNIOR, Armando. **Sistemas de Segurança da Informação na era do conhecimento.** Intersaberes, 2017. Curitiba. Disponível em: <http://unisul.bv3.digitalpages.com.br/users/publications/9788559723038/pages/5> Acesso em: 08 out. 2018.

KIM, David; SOLOMON, Michael G. **Fundamentos de Segurança de Sistemas de Informação.** LTC, 01/2014. [Minha Biblioteca]. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788521635284/cfi/6/16!/4/14@0:6.86> Acesso em: 30 set. 2018.

KOSUTIC, Dejan. **Classificação da informação de acordo com a ISSO 27001.** 2014. Disponível em: <https://advisera.com/27001academy/pt-br/blog/2014/05/14/classificacao-da-informacao-de-acordo-com-a-iso-27001/> Acesso em: 06 out. 2018.

KSECURITY**. Engenharia Social: os perigos das redes sociais para as empresas**. 2018. Disponível em: <https://www.ksecurity.com.br/single-post/2018/07/03/Engenharia-social-os-perigos-das-redes-sociais-para-empresas> Acesso em: 21 out. 2018.

INOVE DADOS. **Qual a importância da segurança da informação para as empresas?** 2018. Disponível em: <https://inovedados.com.br/importancia-da-seguranca-da-informacao> Acesso em: 20 out. 2018.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de informação gerenciais.** Pearson. São Paulo, 2010. Disponível em: <http://unisul.bv3.digitalpages.com.br/users/publications/9788576059233/pages/_7> Acesso em: 18 out. 2018.

LENTO, Luiz Otávio Botelho. **Segurança em redes de dados:** Livro Didático. 4. ed. Unisul Virtual. Palhoça, 2011.

LOPES, Petter. **Política de Segurança da Informação**. 2017. Disponível em: <https://periciacomputacional.com/psi-politica-de-seguranca-da-informacao/> Acesso em: 06 out. 2018.

MARTINS, Elaine. **O que é cracker?** 2012. Disponível em:< https://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm> Acesso em: 16 set. 2018.

MAULAIS, Claudio N. dos Santos. **Engenharia Social: técnicas e estratégias de defesa em ambientes virtuais vulneráveis.** 2016. 79f. Tese (Mestrado em Sistemas de Informação) – Faculdade de Ciências Empresariais, Belo Horizonte, 2016.

MITNIK, Kevin D.; SIMON, William L. **A arte de invadir.** Pearson. São Paulo, 2006. Disponível em: < https://archive.org/details/lilicamy_aline_hotmail_Mais> Acesso em: 09 set. 2018.

MITNIK, Kevin D.; SIMON, William L. **A arte de enganar.** Pearson. São Paulo, 2003. Disponível em: <https://drive.google.com/file/d/0B-eg6n_xOIehZXE5ZGY3NUFOQ2c/view> Acesso em: 14 out.2018.

MOTTA, Alexandre de Medeiros et al..**Universidade e Ciência: livro didático.** Unisul Virtual. Palhoça, 2013.

MULLER, Marney. **Quais são e para que servem as normas de Segurança da Informação?** 2017. Disponível em: <https://www.anyconsulting.com.br/normas-de-seguranca-da-informacao/> Acesso em: 29 out. 2018.

OLIVEIRA, Waldes **Riscos, ameaças e vulnerabilidades em Segurança da informação.** 2018. Disponível em: <https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/ >Acesso em: 21 out.2018.

PAVÃO, Samantha. **Tudo o que você precisa saber sobre Engenharia Social.** 2018. Disponível em: <https://www.psafe.com/blog/rp-o-que-e-engenharia-social/> Acesso em: 14 out.2018.

PONTIROLI, Santiago. **A Engenharia para enganar pessoas.** 2013. Disponível em: <https://www.kaspersky.com.br/blog/engenharia-social-hackeando-humanos/1845/> Acesso em: 14 out 2018.

PROFISSÃO HACKER. **Pen Test: Os testes de intrusão.** 2018. Disponível em: <http://profissaohacker.com/pentest/> Acesso em: 07 nov. 2018.

PROOF**. Engenharia Social.** 2018. Disponível em: <https://www.proof.com.br/blog/ataques-de-engenharia-social/> Acesso em: 14 out.2018.

RAFAEL, Gustavo de Castro. **Engenharia Social: as técnicas de ataque mais utilizadas.** 2013. Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/>
Acesso em: 15 set. 2018.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva.** 2003. Editora Campus. Rio de Janeiro, 2003.

SILVA, Pedro A. Lemes da. **Análise de redes sociais aplicada à Engenharia Social**. 2012. Disponível em: <http://rabci.org/rabci/sites/default/files/Artigo_ARS_e_ES.pdf> Acesso em: 14 out.2018.

SOBRAL, Bosco. **Análise de vulnerabilidades.** Disponível em: <http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5630/material-seg-redes/Analise-de-Vulnerabilidades.pdf> Acesso em: 27 out. 2018.

SYMANTEC. **O que é Engenharia Social?** Disponível em: <https://br.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html> Acesso em: 14 out. 2018.

APÊNDICES

APÊNDICE A

Cronograma TCC – Aluno: Júlio Guarezi – Orientador: Luiz Otávio Botelho Lento

ATIVIDADE	Outubro-				Novembro				Dezembro - Fevereiro	Agosto				Setembro				Outubro				Novembro				Dezembro	
Semanas	1	2	3	4	1	2	3	4		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2
Leitura bibliografia	X	X	X	X																							
Redação Revisão bibliográgica	X	X	X	X																							
Entrega Cap. 2 e 3				X																							
Elaboração método				X	X	X																					
Entrega Cap. 4						X																					
Entrega Av Externo							X																				
Correções				X	X	X	X	X																			
Início redação Cap. 5						X	X	X		X	X	X															
Entrega início Cap. 5													X														
Redação Cap. 6												X	X	X	X	X											
Entrega Cap. 6																			X								
Conclusões Cap. 7/Resumo																		X									
Entrega Monog.																					X						
Poster e Resumo																						X	X				
DEFESA																								X			
Correções																								X	X		
Entrega versão final																										X	