O Fator Humano na Segurança de Informação nas Organizações

Telma Kidy da Conceição Tavares

Dissertação para a obtenção do grau de Mestre em:

Segurança de Informação e Direito no Ciberespaço

Orientador: Professor Doutor Carlos Manuel Costa Lourenço Caleiro

Júri

Presidente: Paulo Alexandre Carreira Mateus

Vogal: Fernando Ribeiro Correia

Dezembro 2017

“E disse o Senhor Deus à mulher: Por que fizeste isto? E disse a mulher: A serpente me enganou, e eu comi”.
Bíblia online: (Gênesis 3:13).

“Ao longo da história, o ser humano sempre buscou o controle sobre as informações que lhe eram importantes de alguma forma; isso é verdadeiro mesmo na mais remota antiguidade".
(Caruso; Steffen, 1999, p. 21).

Agradecimentos

À Deus todo poderoso, que através de sua bondade infinita, concedeu-me o potencial de concretizar mais uma conquista em minha vida. Também pela inspiração, sabedoria e por colocar no meu caminho pessoas que me auxiliaram e apoiaram nesta jornada;

À minha mãe - dona Filomena, e aos meus filhos - Emanuel e Ricardo, que são as pessoas mais importantes da minha vida,… é por eles, e para eles, que decidi abraçar mais este desafio;

Ao meu orientador, Prof. Dr. Carlos Caleiro, que abraçou esse projeto com o mesmo entusiasmo que eu, e que apesar de todas as dificuldades, fez o seu papel de orientador e motivador de uma maneira admirável;

A Universidade Utanga na pessoa do Engenheiro Gabriel Rufino, que financiou a bolsa de estudos tornando possível a realização deste sonho;

Aos meus irmãos - Victor e David, que nunca deixam de estar do meu lado;

A Eva Rodrigues, pelo carinho, atenção, força, cuidado, amizade, companheirismo, presença, preocupação, risadas, brincadeiras e que assim tanto me ajudou e contribuiu direta e indiretamente para a conclusão deste trabalho;

Aos funcionários do técnico, em especial Ana Barbosa, por toda a ajuda, carinho e atenção que me dedicou desde o início para tornar possível a conclusão desse trabalho;

Aos obstáculos no caminho, por terem sido os degraus que me levaram ao topo.

Resumo

Com a evolução das tecnologias, novas ameaças juntam-se as antigas, que geralmente estavam ligadas a vírus, DDos, vulnerabilidades em softwares etc, ou seja, ameaças que exploram vulnerabilidades técnicas, e não humanas. Isso faz com que janelas de oportunidades se abram nesta área, e sejam muito exploradas por malfeitores.

Uma das maiores ameaças à Segurança de Informação nos últimos anos é a Engenharia Social (SE), que tem colocado em risco muitas organizações. Segundo dados estatísticos, mais de metade das violações a dados concretizadas no ano passado, foram ocasionadas por ameaças internas, usando ou não meios tecnológicos no ataque.

Neste trabalho vamos analisar a influência do fator humano na segurança da informação de uma organização, e as consequências do comportamento inapropriado dos colaboradores, partindo do principio que no mecanismo de segurança, o homem é o único elemento que tem a opção de violar as regras.

Tendo em conta a questão da não territorialidade dos crimes informáticos, que faz com que nada e ninguém possa ser considerado seguro, em qualquer parte do mundo. O foco da pesquisa será abordar a importância da componente comportamental, na proteção da informação numa empresa prestadora de serviços públicos, num país Africano com uma economia em ascensão, explicando a pertinência do estudo no panorama internacional.

Os resultados obtidos serão utilizados para identificar as vulnerabilidades na segurança das informações desta instituição e propor soluções que permitam elimina-las e/ou mitiga-las.

Palavras-chave: Segurança de Informação; Componente Comportamental; Engenharia Social; Formação e Educação.

Abstract

With the evolution of technologies, new threats take the place of the old ones, which were usually linked to viruses, DDos, software vulnerabilities etc, ie threats exploiting technical rather than human vulnerabilities. This opens up windows of opportunity in this area, and is explored by evildoers.

The biggest threat to Information Security in recent years is Social Engineering (SE), which has put many organizations at risk. According to statistics, more than half of the data violations committed last year were caused by internal threats, using or not technological means in the attack.

In this work we will analyze the influence of the human factor on the information security of an organization, and the consequences of the inappropriate behavior of the employees, starting from the principle that in the security mechanism, the man is the only element that has the option to violate the rules.

Taking into account the non-territoriality of computer crimes, which makes nothing and nobody can be considered safe, anywhere in the world. The focus of the research will be on the importance of the behavioral component in the protection of information in a utility company in an African country with a rising economy, explaining the relevance of the study in the international scene.

The results obtained will be used to identify vulnerabilities in the security of the information of this institution and to propose solutions that allow to eliminate them and / or to mitigate them.

Keywords: Information Security; Social engineering; Behavioral Component; Training and education.

Indice

Lista de Figuras

Lista de Tabelas

Lista de Gráficos

Siglas e Acrónimos

Ameaça	Causa potencial de incidente indesejável que pode resultar em danos para uma organização ou qualquer sistema por ela utilizados. (CNSS, 2013).
Ataque	Qualquer tipo de atividade maliciosa que tenta recolher, perturbar, negar, degradar ou destruir recursos de sistema de informação ou a informação em si. (CNSS, 2013).
Ataque de força bruta	Uma estratégia de descoberta de senhas que tenta todas as combinações possíveis de caracteres alfanuméricos e símbolos especiais (Schneier, 2017b).
Autenticação de dois fatores	Uso de dois tipos diferentes de autenticação para verificar a identidade. (Schneier, 2017b).
Autenticidade	Num contexto informacional, propriedade de uma informação cuja origem e integridade são garantidas. (CNSS, 2013).
Backdoor	Um ponto de entrada oculto que fornece um caminho secreto para o computador e que é desconhecido do utilizador. (Oliveira, 2003).
Backup	Cópia extra dos dados e/ou programas, mantida em local seguro (Turban et al., 2004).
Cavalo de Tróia	Um programa que contém um código malicioso ou prejudicial, criado para gerir arquivos do computador da vítima ou para obter informações do computador ou da rede da vítima. (Oliveira, 2001).
Baiting	Uso de tecnologia de isca, ou mídia infetada e depende da curiosidade ou cobiça da vítima.
Cifrar	Transformar dados em código cifrado antes de sua transmissão. (Turban et al., 2004).
Decifrar	Transformação de código cifrado em dados legíveis, após a transmissão. (Turban et al., 2004).

Disponibilidade	Capacidade de uma unidade funcional permanecer em estado de realizar uma determinada função dentro de condições previamente determinadas, num dado instante ou num dado intervalo de tempo. (ISO/IEC 27000).
DKIM	Sistema de autenticação cifrada pelo remetente que aumenta a integridade do email ao ser entregue no destino.
DMARC	Conjunto de regras que permitem que os emissores e receptores coordenem seus esforços na detecção e tratamento de e-mails fraudulentos.
Dumpster diving	Vasculhar o lixo de uma empresa para encontrar informações descartadas que tenham valor ou que forneçam ferramentas e dados que podem ser usados num ataques da Engenharia Social. (Mitnick & Simon, 2002).
Engenharia Social	Técnicas utilizadas para obter informações importantes ou sigilosas através de ações que enganam ou exploram a confiança das pessoas. (CNSS, 2013).
Engenharia Social inversa	Ataque de Engenharia Social no qual o atacante cria uma situação, na qual a vítima tem um problema e entra em contato com ele para obter ajuda. (Mitnick & Simon, 2002).
Exposição	Dano, perda ou prejuízo que pode ocorrer, caso algo saia errado em um sistema de informação (Turban et al., 2004).
Firewall	Em tecnologias da informação e da comunicação, sistema informático concebido para proteger uma rede de computadores do acesso externo de utilizadores não autorizados. (CNSS, 2013).
Hacker	Pessoa que explora as falhas da segurança de um sistema com o intuito de violar a sua integridade, destruindo ou alterando a informação ali residente, ou ainda de copiar fraudulentamente os seus ficheiros. (CNSS, 2013).

Hardware	Totalidade ou parte dos componentes físicos de um sistema de processamento de dados (CNSS, 2013).
IETF	Internet Engineering Task Force, Grupo de Trabalho de Engenharia da Internet.
Incidente	Ações tomadas através da utilização de uma rede de computadores que resultam num efeito potencialmente adverso sobre um sistema de informação e/ou a informação aí armazenada (CNSS, 2013).
Informação	Dados que foram interpretados ou organizados de forma coerente e posteriormente comunicados, sendo então possível tirar conclusões do seu significado (CNSS, 2013).
Integridade	Garantia de que os dados ou a informação não sejam alterados de modo não autorizado (CNSS, 2013).
Malware	Programa de computador, tal como um vírus, um worm ou um Cavalo-de-Tróia, que executa tarefas prejudiciais (Oliveira, 2003).
Norma	Requisitos obrigatórios utilizados e impostos para atingir uma abordagem disciplinada e uniforme no desenvolvimento de software (CNSS, 2013).
Overflow	Uma condição de entrada de dados que permite que sejam introduzidos dados ou colocados em memória, para além da capacidade reservada para o efeito, provocando a escrita "por cima" de outra informação (CNSS, 2013).
Palavra-passe	Sequência de caracteres ou palavras que um sujeito apresenta a um sistema, como informação de autenticação (CNSS, 2013).
Patch	Código que quando colocado em um programa executável, corrige um problema (Oliveira 2003).
Persuasão	Arte de convencer alguém a entregar informação específica, para a qual se procura a respostas. Isto é possível porque as pessoas têm características comportamentais que as tornam vulneráveis à manipulação (Cialdini, 2006).

PGP	Programa de cifragem e decifra de dados, frequentemente utilizado para assinatura, cifragem e decifra de textos, e-mails, arquivos, diretórios e partições inteiras de disco.
Phishing	Mensagens de correio eletrónico com aparência de terem origem em organizações financeiras credíveis, mas com ligações para falsos sítios Web que replicam os originais, e nos quais são feitos pedidos de atualização de dados privados dos clientes (CNSS, 2013).
Privilégio Mínimo	Os privilégios e autorizações requeridos para o desempenho de determinada tarefa ou cumprimento de dever (CNSS, 2013).
Ransomware	O Ransomware é um tipo de ataque, que se caracteriza por infectar um computador e pedir um resgate para que este volte a estar operacional (CNSS, 2013).
Risco de Segurança	A probabilidade de as vulnerabilidades inerentes a sistemas de comunicação e informação serem exploradas por ameaças, levando ao comprometimento dos sistemas (CNSS, 2013).
Segurança da Informação	Proteção dos sistemas de informação contra o acesso ou a modificação não autorizada da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados (CNSS, 2013).
Software Malicioso	Programas informáticos destinados a perturbar, alterar ou destruir todos ou parte dos módulos indispensáveis ao bom funcionamento de um sistema informático. Exemplos: vírus, vermes, cavalos de Troia (CNSS, 2013).
SPAM	Mensagens de correio eletrónico não solicitadas, geralmente enviadas de uma forma massiva e indiscriminada, que, para além do incómodo provocado aos utilizadores do correio, podem comprometer o bom funcionamento dos sistemas informáticos (CNSS, 2013).
SPF	Protocolo que permite determinar que servidores de email têm permissão para o envio de mensagens a um determinado domínio.
Spoofing	Camuflagem do IP (IP spoofing), que consiste na utilização do endereço IP de outro utilizador; camuflagem do domínio (domain

	spoofing), que significa a utilização de um nome de domínio pertencente a outrem; camuflagem do endereço eletrónico (e-mail spoofing), que é a utilização de outro endereço eletrónico que não o próprio do utilizador (CNSS, 2013).
Spyware	Software usado para monitorizar de modo oculto as atividades do computador alvo como *Web sites* visitados e capturas do ecra (Oliveira, 2001).
TI (Tecnologias de Informação)	Integração de métodos, processos de produção, hardware e software, com o objetivo de proporcionar a recolha, processamento, disseminação, visualização e utilização de informação, de acordo com o interesse dos seus utilizadores. (CNSS, 2013).
Vírus	Software malicioso que tem a capacidade de se auto-replicar e "infetar" partes do sistema operativo ou outros programas, com o intuito de causar a perda ou alteração da informação (CNSS, 2013).
Vulnerabilidade	Ponto fraco que pode ser explorado por uma ou mais ameaças, podendo ser de natureza técnica, processual, material, organizativa ou operacional (CNSS, 2013).
Worm	Um programa autorreplicante, que se propaga utilizando mecanismos da comunicação em rede (CNSS, 2013).

Introdução

O fator humano tem sido encarado por muitas organizações, como um dos grandes desafios da segurança de informação, pois o facto dos utilizadores permitirem ou autorizarem que terceiros acedam a dados, lugares e/ou dispositivos, permitindo a pessoas não autorizadas acesso as informações importantes da organização, fragiliza a sua segurança.

O inicio da era tecnológica, permitiu automatizar as atividades nas organizações, reduzindo a quantidade de recursos físicos, lógicos e humanos outrora usados, aumentando a sua eficiência e produtividade. Essas vantagens, trouxeram consigo perigos, que fizeram com que nos últimos anos, as organizações tenham sofrido transformações para preservar a segurança de informação.

Questões ligadas ao aspeto comportamental dos colaboradores foram evidenciadas em estudos referenciados ao longo desta pesquisa, por serem reconhecidas como um dos grandes problemas atuais para a segurança de informação. O diferencial deste trabalho investigativo é mostrar que as pessoas importam tanto quanto, senão mais, do que a tecnologia, e podem causar elevados prejuízos as organizações.

Atualmente uma das técnicas mais utilizadas para influenciar os funcionários, a permitirem ou autorizarem o acesso de terceiros a informações privilegiadas, é a Engenharia Social, que será um dos pontos centrais do desenvolvimento deste estudo, tendo em conta a sua importância na mudança comportamental dos colaboradores.

Mitnick (2002) defendeu que a Engenharia Social usa a influência e a persuasão para enganar as pessoas ou convencê-las de algo, uma vez que o engenheiro social é alguém que se aproveita das pessoas para obter informações, com ou sem o uso da tecnologia. O autor sustenta ainda, que muitos profissionais da tecnologia da informação (TI) conservam a ideia errada de que suas empresas estão imunes a ataques por usarem *firewalls,* sistemas de deteção de intrusos (*IDSs*), dispositivos de autenticação como tokens ou cartões biométricos inteligentes, e adverte que as empresas que baseiam a sua segurança apenas em tecnologia, mais cedo ou mais tarde, serão vítimas de algum incidente de segurança.

A criminalidade informática é um fenómeno mundial que tornou as restrições territoriais irrelevantes no ciberespaço, pois o raio de alcance destes crimes vai alem das fronteiras físicas e geográficas. Os criminosos informáticos não precisam de proximidade física com seus alvos

para atacar, pois podem estar em diferentes cidades, Países ou continentes, e vitimar governos, empresas e pessoas em qualquer parte do mundo usando apenas um computador ligado a internet. Desta forma, um ataque a qualquer organização, é uma possibilidade sempre eminente, bastando apenas que o atacante tenha alguma motivação para desenvolver a ação.

A importância deste estudo para o panorama internacional, baseia-se no facto de termos escolhido como alvo de pesquisa, uma empresa que embora tenha consideráveis investimentos em meios materiais e humanos, está localizada no continente Africano, onde questões ligadas a segurança de sistemas informáticos ainda são matérias pouco aprofundadas, dadas as limitações técnicas e profissionais que a maioria dos Países Africanos vivem, em virtude do fraco desenvolvimento tecnológico do continente.

Neste contexto, vamos discutir o fator humano como elemento base para garantir a segurança de informação, pois os pilares da disponibilidade, integridade e confidencialidade da informação, se forem separados do fator humano, pouco contribuem para garantir a eficácia do sistema.

Nos próximos capítulos discutiremos a importância da segurança de informação para a continuidade do negócio, o papel do elemento humano neste processo, bem como o significado de Engenharia Social, e quais as técnicas mais usadas neste tipo de ataques, abordando ameaças internas como Phishing, Spyware, Baiting, Ransomware, e veremos também como evitar ataques desta natureza.

1 Capítulo - Enquadramento

1.1 Segurança Padrão

A incidência de ataques sistemáticos ao sistema informático das organizações, estão a fazer com que as mesmas passem a levar mais a sério a segurança dos seus activos, investindo enormes quantias em defesas sofisticadas, incluindo firewalls, anti-vírus, sistemas de identificação e detenção de intrusos, sistemas biométricos, cartões electrónicos de identidade e acesso. O impacto prejudicial de uma violação interna pode se estender além dos custos financeiros. Pode prejudicar a integridade da marca e afectar a segurança física dos próprios colaboradores (Stroz et al, 2016).

Para colmatar esta questão, está hoje disponível no mercado uma ampla gama de ferramentas eficientes contra os ataques considerados "técnicos", mas verifica-se que os problemas de segurança das informações e dos sistemas em rede nas organizações têm vindo a aumentar, em particular quando envolvem o fator humano.

Segundo Kevin Mitnick;

> "Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável".
>
> In Mitnick & Simon (2002), p.15.

Segundo a ideia do autor, mesmo tomando todas as precauções necessárias, ainda assim, nenhuma organização pode ser considerada 100% segura.

O lado da segurança envolvendo o fator humano, tem sido negligenciado pelos administradores e gestores das organizações, por confiarem e darem preferência aos sistemas padrão, ignorando que toda segurança poder ser quebrada se o inimigo estiver dentro da empresa, e tiver acesso ao sistema por uma conta autorizada. A maioria das organizações está mais preparada para responder a ameaças cibernéticas externas, por haver uma maior dificuldade em detectar e prevenir os ataques "*insiders*" (Stroz et al, 2016). Isso explica a crescente onda de ataques cibernéticos com origens internas sofridas por organizações em vários Países nos últimos anos.

1.2 Elo Mais Fraco

A maioria dos trabalhos de pesquisa sobre segurança de informação têm como alvo "defesas de perímetro", onde são usadas *firewalls, IDS,* métodos criptográficos e a área da Engenharia Social é deixada para trás, por não ser considerada crucial no processo de protecção dos sistemas de informação. Neste contexto, em a "Arte de Enganar", Mitnick afirmou que:

> *"...à medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes voltam-se cada vez mais para a exploração do elemento humano... Quebrar a "firewall humana" é quase sempre fácil, não exige nenhum investimento além do custo de uma ligação telefónica e envolve um risco mínimo" (Mitnick, 2002).*
>
> In Mitnick& Simon (2002), p.16.

Segundo Winnefeld (2015), há maiores chances de sucesso em ataques de Engenharia Social, quando as pessoas são ignorantes relativamente às práticas de segurança. Por esta razão, a característica mais comum nos ataques modernos é concentrarem-se no elo mais fraco na cadeia de segurança, ou seja, no ser humano.

1.3 Pilar Humano

Para Feleol (2012), o conceito de segurança de informação está sustentado em três pilares básicos: disponibilidade, integridade e confidencialidade da informação. Nesta perspectiva, o fator humano é descurado como decisivo para o sucesso do mecanismo de segurança.

No entanto, o crescimento dos índices de ataques bem-sucedidos nos últimos anos, tendo como alvos os utilizadores do sistema, apontam que, tal como a confidencialidade, a integridade e a disponibilidade, o pilar humano precisa de um tratamento equivalente, uma vez que a maior ameaça à Segurança de Informação nos últimos anos é a Engenharia Social (SE), que tem colocado em risco muitas organizações (Winnefeld et al, 2015).

Em testemunho num congresso, perante os senadores Lieberman e Thompson, Mitnick afirmou que:

> *"Motivado pela curiosidade, conseguiu entrar com sucesso em alguns dos sistemas de computadores mais protegidos que já foram desenvolvidos, e teve acesso não autorizado aos sistemas de computadores de algumas das maiores empresas do planeta, usando meios técnicos e não técnicos para obter o código-*

fonte de diversos sistemas operacionais e dispositivos de telecomunicações para estudar suas vulnerabilidades e seu funcionamento interno".

In Mitnick & Simon (2002), p.11.

Esta declaração revela o quanto é importante que os gestores, tomem consciência da dimensão real do problema "fator humano", e definam estratégias adequadas para lidar com a situação. Entende-se que a temática seja bastante delicada, dada a dificuldade de prever a probabilidade de um colaborador cometer actos ilegais, pois isso depende de fatores que estão fora da alçada da organização.

1.4 Definição do Problema

Qualquer organização, já sofreu algum tipo de ataque informático (ainda que não se tenha apercebido do facto), e o padrão mais denunciado pelas vítimas, é que em algum momento, esteve envolvida a interacção humana, sendo manipulada e direccionada para produzir os resultados desejados pelo atacante (Mitnick & Long, 2008).

Esta constatação despertou em nós o interesse de descobrir como é visto o "fator humano" numa das empresas Angolanas do sector privado, que mais investiu nos últimos anos em recursos materiais, humanos e tecnológicos, levando em conta que, até os mais caros e complexos sistemas de segurança de informação, podem ser violados da forma mais inesperada, expondo a informação aos atacantes.

1.4.1 Motivação

A maioria das soluções de segurança no mercado inclui apenas mecanismos técnicos para contra medidas de segurança usando *worms*, cavalo de Troia, *malwares, phishing, Spear phishing, Hijackers*, ataques de *bufferoverflow*, força bruta e outros, mas não se preocupa com os riscos causados pelo comportamento humano, descurando que as pessoas e suas escolhas são o que impulsionar uma organização para a frente ou sabotam o seu sucesso (Stroz et al, 2016 a) & (Winnefeld et al, 2015).

Acreditamos que uma abordagem diferente quanto a esta questão deve ser adoptada pelas organizações, tendo em conta a dependência do fator humano para manusear os sistemas. Para isso, foi definido um objecto de estudo e elaborados objectivos e questão de partida para fundamentar e argumentar possíveis práticas na prossecução desta questão eminente.

1.4.2 Objecto de Estudo

Foi escolhida para este estudo uma das maiores empresas do sector de transportes rodoviário no país. Por razoes de segurança, usaremos o nome fictício MATOX- Transportes, para não identifica-la, já que as informações que disponibilizaremos no estudo são de carater classificado.

Com uma frota operacional de 350 autocarros e capacidade de transportar diariamente 30 mil passageiros no serviço urbano e periurbano da capital, a MATOX conta para o efeito com 765 colaboradores. Nos últimos anos, a empresa investiu vários milhões de dólares norte-americanos em terminais rodoviários e aquisição de bens moveis e imóveis, alem de elevados investimentos em TI.

Estas razoes podem ser determinantes para que a empresa se torne alvo do tipo de ataques abordados nesta pesquisa, uma vez que estes, geralmente são motivados por fatores financeiros e competitivos (Puricelli, 2015).

1.4.3 Objectivo Principal

O nosso objectivo é analisar a influência que o comportamento humano pode ter na segurança da informação de uma dada organização. Com isso, pretendemos fornecer uma proposta que, por meio da demonstração dos diversos tipos de princípios psicológicos usados na manipulação dos utilizadores dos sistemas, torne os ataques de Engenharia Social mais claros para a organização e proporcione melhores contra medidas defensivas.

1.4.3.1 Objectivos Específicos

1) Identificar o nível de conhecimento dos colaboradores da empresa, sobre as principais questões que envolvem a segurança de informação, com realce para Engenharia Social bem como as técnicas de ataque mais usuais.
2) Averiguar se existem políticas, normas e procedimentos de segurança da informação implementadas na empresa. E se as mesmas terão sido dimensionadas de acordo com o nível académico dos colaboradores.
3) Propor práticas que contribuam para diminuir ou atenuar as vulnerabilidades identificadas.

1.4.4 Questão de Partida

Usando dados obtidos de fontes primárias de pesquisa, vamos tentar responder a seguinte questão de partida:

1) Em que medida o nível de conhecimento dos colaboradores bem como, a definição de politicas e procedimentos de segurança, contribuem para minimizar as violações de segurança que tenham como ponto de partida a interacção humana que resulta de actividades laborais?

1.5 Metodologia de Investigação

Engenharia Social é uma temática pouco abordada em Angola, por não existirem muitos estudos nem relatos oficiais, de incidências dos mesmos na quebra de segurança dos sistemas informáticos no país. Este facto, fez com que inicialmente olhássemos a problemática a nível internacional, buscando informações em artigos, livros, relatórios e publicações de outros Países, para melhor entendermos o problema e suas implicações, e analisarmos que soluções já são aplicadas a nível internacional, para criarmos uma linha de orientação passível de ser aplicada em Angola.

A insuficiência de fontes escritas sobre este tema em Angola, fez com que fosse necessário basearmos a pesquisa em fontes primárias[1] em detrimento das secundárias[2], pelo que, foi realizada uma pesquisa de campo na empresa de transportes públicos angolana MATOX-Transportes, com uso de questionários para os colaboradores. As informações obtidas, serviram de base para a realização da pesquisa por constituírem uma importante fonte de informação.

O método adoptado foi o qualitativo, baseado num estudo exploratório, e as técnicas utilizadas foram as seguintes:

- Análise documental: livros, artigos, publicações, dissertações.
- Observação directa no local de trabalho dos colaradores.
- Aplicação de questionários.

Para tal, foram efectuadas perguntas específicas quando se interagia na sala com os colaboradores com o intuito de identificar as fragilidades do seu comportamento ao lidar com

[1]Consideram-se fontes primárias os inquéritos, questionários, entrevistas, observação de painéis, etc.
[2]Consideram-se fontes secundarias toda a bibliografia de referência utilizada para a realização desta pesquisa.

questões emocionais (fatores de influência comportamental), e técnicas (hardware e software). A informação conseguida na empresa foi utilizada de forma qualitativa como forma de reforço da investigação, o que permitiu uma abordagem através de um método misto de pesquisa (revisão de literatura e caso de estudo). (Hill & Hill, 1998).

A escolha deste método permitiu obter informações, tanto do comportamento humano em questões de segurança da informação no ambiente da organização, quanto de literaturas proeminentes relacionadas com o nosso estudo. Se recorrêssemos apenas a questionários, obteríamos conhecimento sobre o comportamento dos colaboradores, mas não teríamos como compara-los, dado que faltava a observação de campo. Assim sendo, é possível identificar potenciais comportamentos perigosos em colaboradores, e compara-los aos relatados por autores mencionados neste trabalho.

1.5.1 Delimitação do Estudo

Apesar de existirem várias ameaças e fatores que influenciam o comportamento humano, importa-nos abordar apenas as que resultem de Engenharia Social e tenham os colaboradores envolvidos, como participantes activos ou passivos dos ataques.

1.6 Síntese dos Capítulos

No capítulo 1, faremos o enquadramento do tópico de pesquisa abordando: o fator humano na segurança de informação; conceito de sistema de informação; definição do problema da pesquisa; motivações; objectivos; questões levantadas; metodologia usada; e delimitação do estudo.

No capítulo 2, com base na revisão da literatura, apresentaremos um mapa de conceitos, com os aspetos pertinentes do tema, incluindo os que hoje já não têm muita relevância para segurança de informação, mas que ainda possuem uma considerável importância histórica.

No capítulo 3, resumiremos importantes relatos de violações a dados usando técnicas de Engenharia Social (SE) para concretização do ataque. E faremos uma abordagem geral sobre a Engenharia Social como um aspecto importante da segurança de informação, onde tentaremos cobrir tanto o lado psicológico como o técnico da temática.

No capítulo 4, abordagem metodológica explicando os procedimentos adoptados para realização do estudo. Justificação do tipo estudo e metodologia adoptada, e aplicação de questionários ao grupo alvo da investigação.

No capítulo 5 faremos a análise e discussão dos resultados obtidos fornecendo propostas para solucionar os problemas identificados.

1.7 Resultados Esperados

Apos a analise dos objetivos estabelecidos, o estudo permitirá contribuir com melhores praticas ou mesmo propor medidas que englobem:

- ➔ Elaboração e implementação de políticas de segurança adequadas a realidade da empresa, assim como medidas punitivas para as infrações cometidas;
- ➔ Criação de um programa de educação e consciencialização dos colaboradores em segurança de informação;
- ➔ Implementação de mecanismos de segurança capazes de proteger a informação armazenada e ou em fluxo, de modo a garantir a continuidade do negocio;
- ➔ Fazer com que o corpo diretivo da empresa se consciencialize sobre a real importância da componente humana na segurança de informação e adote os mecanismos de prevenção e controlo para os diferentes tipos de ataques SE.

2 Capítulo - Segurança de Informação

2.1 Fundamentação Teórica

Segundo Mitnick & Simon (2002), em "A arte de enganar", a maior fraude de computadores registado pelo *Guiness Book* foi feita por Stanley Mark Rifkin, (sem o uso de computadores), usando Engenharia Social sobre os colaboradores do *Security Pacific National Bank*, de Los Angeles, fazendo-se passar por um consultor do banco.

Usando senhas e códigos de confirmação obtidos por telefonemas, Stanley ordenou a transferência de "dez milhões e duzentos mil dólares " para o Irving Trust *Company* de Nova York, a crédito do *Wozchod Handels Bank* de Zurique, Suíça, onde já havia aberto uma conta (Mitnick & Simon, 2002).

Histórias como estas acontecem com frequência. Se algo semelhante ainda não aconteceu na empresa onde trabalha, a questão não é se vai acontecer, mas sim, quando acontecerá. O autor de "*Segurança da Informação"*, Bruce Schneier declarou que, *"Se alguém acha que a tecnologia pode resolver seus problemas de segurança, então, ou não entende os problemas, ou não entende a tecnologia"* (Schneier, 2002). O que significa que por muito sofisticada que seja a tecnologia, terá sempre como vertente fundamental de suporte, o fator humano.

2.2 Dados Estatísticos

De acordo com a verizon (2016) foram encontrados indicadores estatísticos interessantes sobre as novas tendências de crimes informáticos, que mostram que a nova geração de ataques está a utilizar o factor humano para desencadear com frequência ataques a TI sem o uso de meios electrónicos.

O relatório de investigações de violação de dados da *Verizon*, reportou em 2016 mais de 100.000 incidentes de segurança relatados e 2.260 violações de dados confirmadas (Verizon, 2016).

Segundo a mesma fonte, os cibercriminosos continuam a explorar a natureza humana, pois dependem de padrões de ataque que jogam com a psicologia, como é o caso dos ataques de ransomware que aumentaram 16% em relação a 2015, onde os dados são cifrados e é exigido um resgate.

Os ataques de phishing são actualmente a forma mais usada, onde os utilizadores finais recebem um e-mail que sob algum pretexto aliciante para o alvo, pedem para o mesmo abrir determinado

arquivo ou clicar num link. O estudo aponta que cerca de 30% das mensagens *phishing* enviadas foram abertas, e que 13% dos utilizadores abriram o anexo malicioso ou o *link* (Verizon, 2016).

Uma constatação importante do relatório é a crescente tendência para envolver as pessoas uma vez que as organizações negligenciam a protecção das dezenas, centenas e até milhares de dispositivos como laptops, tablets e smartphones usados pelos colaboradores na empresa.

As ameaças internas perfazem 77% dos incidentes, sendo 26% erros que envolvem o envio de informações sensíveis a pessoas não autorizadas, e os restantes 51% incluem descarte inadequado de informações, má configuração de sistemas, e *laptops*/*smartphones* perdidos ou roubados. O método de invasão mais utilizado é o abuso de privilégios, já que o utilizador só precisa usar as ferramentas que a própria empresa disponibiliza (acesso aos dados). (Verizon, 2016).

O relatório Symantec[3] sobre ameaças à segurança na internet em 2016, apontou mais de um milhão de ataques diários contra utilizadores, onde os criminosos cibernéticos aproveitam-se das vulnerabilidades dos sites. A mesma fonte relatou que a quantidade de vulnerabilidades dia zero duplicou relativamente ao ano anterior, expondo cerca de 429 milhões de identidades (Symantec, 2017a).

O relatório da Intel Security em 2016 afirma que, entre as empresas que relataram violações de dados nos últimos anos, os colaboradores foram responsáveis por 43% da perda de dados, metade dos quais foi intencional e malicioso (Stroz et al, 2016). De onde se conclui que o erro humano, a falha em corrigir vulnerabilidades, configurações mal executas, e violações de procedimentos, constituíram a maioria de incidentes.

2.3 Conceito de Segurança de Informação

Os activos de informação são hoje considerados um dos principais patrimónios das organizações. Assim, o controlo de acesso as informações, é um requisito fundamental dada a sua importância para a continuidade do negócio. O conceito de Segurança de Informação, garante os mecanismos necessários para assegurar a sua preservação e integridade e prevenir os acessos não autorizados (Santos & Silva, 2013).

[3]Symantec Corporation, é uma empresa americana de software de segurança, armazenamento, e backup, que opera uma das maiores redes de inteligência cibernética do mundo. O relatório Symantec de ameaças à segurança na internet, oferece uma visão geral e análise das actividades de ameaças globais anualmente.

Para Beal (2005, p.71) a Segurança de Informação é "*o processo de proteger a informação das ameaças, para garantir a sua integridade, disponibilidade e confidencialidade*". Esta visão permite garantir que a informação existente em qualquer formato seja protegida contra o acesso por pessoas não autorizadas (confidencialidade), esteja sempre disponível quando necessária (disponibilidade), seja confiável (integridade) e autêntica (autenticidade).

Como conclusão podemos dizer que, a segurança de informação é o processo de proteger a informação de diversos tipos de ameaças internas e externas que coloquem em risco a continuidade do negócio e o retorno dos investimentos feitos. A adopção e implementação de um sistema de segurança é uma decisão particular de cada organização que é influenciada pelas necessidades e objectivos da empresa, requisitos de segurança, capital investido, tamanho e estrutura da organização. Assim sendo deve ser feita uma análise de risco que identifique as potenciais ameaças, apontando soluções que as eliminem, minimizem ou as transfiram a terceiros.

2.4 Ameaças à Segurança de Informação

Ameaças são acções de origem humana, que se exploradas, geram vulnerabilidades e permitem ataques, que têm como consequência a perda de confidencialidade, disponibilidade e integridade (Santos & Silva, 2013).

Para Teotônio (2013), ameaça é algo que provoca danos na segurança de informação, prejudicando acções da empresa e a sustentação do negócio, mediante a exploração de uma vulnerabilidade, e materializa-se na componente humana sob a forma de evento ou ideia capaz de causar danos a confidencialidade, integridade, disponibilidade.

Sêmola (2003) define ameaças como sendo, agentes ou condições que causam incidentes que comprometem as informações e seus activos, por meio de exploração de vulnerabilidades, o que provoca perdas de confidencialidade, integridade e disponibilidade e consequentemente, causa impactos aos negócios da organização.

Segundo Beal (2005), ameaças são expectativas de acontecimentos acidentais ou propositadas, causado por agente, que pode afectar um ambiente, sistema ou activo de informação.

Teotônio (2013) defende que, as ameaças podem surgir de uma variedade de eventos, e afectar os negócios de uma organização. Podendo estes ser eventos naturais, como terramotos, furacões, enchentes, descargas eléctricas, tsunamis, ou incidentes em instalações, como

incêndio, curto-circuitos, infiltrações; de incidentes de segurança, com roubo, furto, sabotagem e ataques terroristas.

Em todas as definições, uma ideia revela-se clara e preocupante, a automatização dos sistemas de processamento e armazenamento de informações, torna a própria informação mais susceptível às ameaças, uma vez que a mesma fica mais disponível.

2.4.1 Ameaças Internas vs Externas

A maioria das organizações se sentem vulneráveis ao lidar com ameaças internas, por ser mais difícil detectar e prevenir um ataque com privilégios do que um ataque cibernético externo (Stroz et al, 2016). As ameaças internas são iminentes estando a empresa ligada ou não à Internet, e podem causar desde leves incidentes, até a paralisação do sistema, apresentando como componente principal o jogo psicológico, considerado uma parte fundamental na preparação e execução do ataque. Este tipo de ameaça não tem êxito sem a participação do funcionário.

As ameaças externas, veem de fora, e visam aproveitar vulnerabilidades não corrigidas em softwares e dispositivos com acesso ao exterior, uma vez que, as vulnerabilidades sem patches são exploradas com mais frequência (Arora, 2006)

Estas ameaças incluem negação de serviço, exploração de vulnerabilidades em softwares, infecção de computadores por vírus, acesso não autorizado, entre outras. A negação de serviço destina-se a sobrecarregar os dispositivos de rede ou servidores por inundação, com falsas solicitações de serviço até que os mesmos não consigam dar resposta as solicitações e fiquem fora de serviço por incapacidade.

Os ataques de acesso não autorizado à rede são direccionados a violação da protecção externa para aceder ilegalmente a rede interna. As duas formas de ataques têm em comum o facto, dos colaboradores da organização encontrarem-se de alguma forma envolvidos.

2.5 Normas ISO/IEC 27000

Segundo Dantas (2011), "*a busca frenética por informações para a tão almejada vantagem competitiva é a grande responsável pelos actuais cuidados com a informação, uma vez que o sucesso dos negócios depende cada vez mais da competitividade*".

A norma padrão internacional denominada ISO/IEC 27000[4] foi criada para ajudar as organizações a manterem seus activos de informações protegidos de pessoas não autorizadas. A segurança de informação é padronizada por esta família de normas, que gerem informações financeiras, de propriedade intelectual, de colaboradores ou de terceiros, e podem ser adaptadas às necessidades de cada organização.

As normas ISO/IEC 27001 e 27002 fornecem os requisitos genéricos para a criação de um sistema de segurança de informação. Para maximizar seus benefícios, tais requisitos devem ser adequados e adaptados à realidade e necessidades de cada organização, já que os requisitos genéricos, são aplicáveis a todas organizações, independentemente do tipo, tamanho ou natureza. Os atributos básicos da segurança de informação confidencialidade, integridade e disponibilidade, são referidos como a Tríade da CIA (Harvey & Evans, 2016).

Esses atributos funcionam juntos para proteger os sistemas de informação da seguinte forma:

2.5.1 Integridade

A integridade é a garantia da exactidão da informação e dos métodos de processamento. Ela permite que a informação não seja modificada, alterada ou destruída sem autorização, que ela seja legítima e permaneça consistente, garantindo a sua protecção contra mudanças intencionais, indevidas ou acidentais.

Ocorre a quebra da integridade quando a informação é corrompida, falsificada, roubada ou destruída. Garantir a integridade é manter a informação na sua forma original.

Contribuem para a perda da integridade:

- ➔ Substituições, inserções ou exclusões de parte do conteúdo da informação;
- ➔ Alterações nos elementos de suporte onde ela está armazenada, ou quando são violadas as barreiras de segurança de uma rede de computadores.

2.5.2 Confidencialidade

Confidencialidade é a garantia de que a informação esteja disponível somente a pessoas autorizadas. Se uma informação é confidencial, ela deverá ser guardada com segurança, e não divulgada a pessoas não autorizadas.

[4]Normas ISO/IEC 27000, são normas internacionais que fornecem requisitos para o estabelecimento, implementação, manutenção e melhoria contínua de um sistema de gestão da segurança de informação.

Ocorre a quebra da confidencialidade quando se permite que pessoas não autorizadas tenham acesso ao seu conteúdo. Garantir a confidencialidade é evitar a sua divulgação indevida.

2.5.3 Disponibilidade

Disponibilidade é a garantia de que os utilizadores autorizados tenham acesso à informação quando necessário. Ocorre a quebra da disponibilidade quando a informação não está disponível ou ao alcance de seus utilizadores e destinatários quando necessário.

2.6 Classificações das Informações

A classificação das informações permite definir o nível de protecção das mesmas, por isso, é importante fazer uma classificação que permita preservar os requisitos fundamentais estabelecidos pela organização para a segurança das informações durante o seu ciclo de vida.

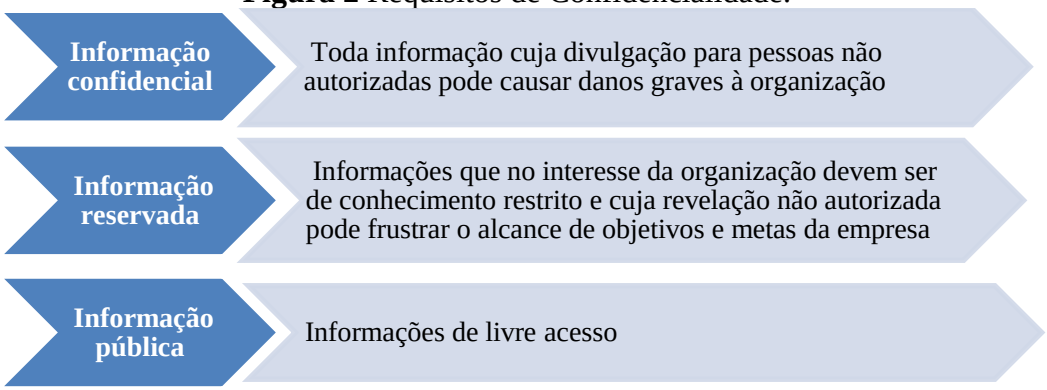
A classificação da informação proposta por Beal (2005), é demonstrada na figura 1:

Figura 1 Classificação da Informação.

Fonte: (Adaptado de Beal, 2005)

Na figura 2, Beal (2005) propõe uma classificação para os requisitos de confidencialidade:

Figura 2 Requisitos de Confidencialidade.



Fonte: (Adaptado de Beal, 2005)

Para os requisitos de disponibilidade, o mesmo autor orienta que a informação deva ser classificada de acordo com o impacto que sua falta possa provocar para a empresa, podendo ser estabelecidas categorias para o tempo de recuperação em caso de um evento ou desastre, de

minutos a semanas. Para os requisitos de integridade, classifica as informações em alta, média e baixa exigência de integridade.

2.7 Crimes Informáticos

Durante anos os crimes informáticos não tiveram regulamentação, fiscalização ou punição, e o anonimato da internet facilitava o encobrimento da autoria de atos ilícitos. A ausência de limites geográficos do espaço virtual, criou problemas relacionados à soberania nacional dos Estados, como nos casos em que dois ou mais Países estejam envolvidos numa situação de ciber espionagem ou utilizando técnicas de Engenharia Social, que levanta o problema do princípio da territoriedade, ou seja, definir se a jurisdição pertence ao país de onde partiram os ataques, de onde os dados estavam armazenados, ou do pais a quem pertencem os dados roubados (Gomes,2001).

Em "Arte da Guerra", Sun Tzu (1772) refere a espionagem como um ato só permitido entre nações e grupos guerrilheiros em guerra. Consiste na prática de obter informações de caracter sigiloso relativos a governos ou organizações sem autorização, para conseguir vantagem militar, politica, económica, cientifica, tecnológica ou social. Esta questão fez com que durante anos, malfeitores usassem ferramenta ilícitas para atingir a segurança nacional e prosperidade económica de organizações em vários Países.

Contudo hoje a realidade é completamente diferente, a maioria dos Países já possuem uma legislação especifica para crimes praticados com recurso a tecnologias de informação e comunicação (Oliveira, 2003). Em 2001 foi assinada em Budapeste a Convenção Internacional sobre a Cibercriminalidade (Convenção Sobre o Cibercrime, 2001), este foi o primeiro texto jurídico a debruçar-se sobre o assunto à escala internacional.

A convenção de Budapeste visa combater os crimes cibernéticos prevenindo e punindo crimes contra a disponibilidade, confidencialidade e a integridade de dados, como invasões a sistemas de computadores e crimes informáticos praticados com ou sem o uso de dispositivos eletrónicos. Trata-se de um tratado internacional, de vocação universal dirigido a todos os Países do mundo.

Urge realçar que a lei sobre a cibercriminalidade incentiva os Países a adotarem medidas legislativas que punam condutas que facilitem à introdução, alteração, eliminação não autorizada de dados informáticos, originando dados não autênticos que sejam tomados como autênticos.

3 Capítulo - Engenharia Social

3.1 Perspectiva Histórica

A história do cavalo de Tróia é uma das primeiras ocorrências documentadas de Engenharia Social, ela conta que depois de passar dez anos nos portões da cidade, os gregos fingiram conformar-se com a derrota, construíram um grande cavalo de madeira e o trouxeram como "presente" para a cidade de Tróia, enquanto fingiam ir para longe. Na verdade, foram seleccionados e escondidos dentro do cavalo os melhores soldados, que depois abriram as portas, permitindo a entrada ao exército grego que obteve uma vitória rápida e decisiva.

Ao contrário de outras ameaças da segurança de TI, a Engenharia Social ataca as pessoas responsáveis por operar, manter, supervisionar e proteger os sistemas, por isso a importância deste conto para a segurança de informação, revela uma importante mensagem de alerta, pois a técnica usada no conto foi inspiração para a criação de um programa malicioso de computador muito usado em ataques de SE.

3.1.1 Violações a Dados

3.1.1.1 Violação ao RSA SecurID

Em Março de 2011, a RSA Security, Inc. anunciou ter sido vítima de um ataque que resultou na divulgação de informações relacionado à sua solução de autenticação de dois factores (Coviello, 2016). A investigação subsequente descobriu que foi usada Engenharia Social para a entrada não autorizada aos sistemas dos colaboradores da RSA, a partir de um e-mail phishing de lança, que foi enviado para dois grupos de colaboradores da empresa.

Um colaborador foi enganado e abriu o e-mail que tinha como tema "Plano de Recrutamento 2011" e continha um anexo em Excel - "Plano de Recrutamento 2011.xls". Ao baixar e abrir o arquivo, ele explorou uma vulnerabilidade de dia zero no Adobe Flash e instalou um backdoor no PC da vítima. O custo total do ataque para a RSA foi de 66,3 milhões de dólares (RSA, 2011) & (Jarmoc, 2016).

3.1.1.2 Violação de dados no Fundo Monetário Internacional (FMI)

Em 2011 o Fundo Monetário Internacional sofreu um ataque cibernético em que alguns de seus sistemas foram comprometidos e utilizados para aceder dados internos. Uma investigação mostrou que um computador interno foi comprometido e usado para aceder a dados econômicos não públicos utilizados pelo FMI para promover a estabilidade da taxa de câmbio, apoiar o

comércio internacional equilibrado e fornecer recursos para remediar crises de balança de pagamentos dos membros (Wolf & Maclean, 2011) & (Guardian, 2011).

Não foi possível provar qual País esteve por trás do ataque, pois mesmo Países em desenvolvimento, poderiam falsificar sua posição geográfica e desencadear o ataque. Essa questão aumentou a preocupação mundial sobre a guerra cibernética realizada para fins de espionagem econômica e industrial.

3.1.1.3 Violações de Dados na Target Corporation.

Em Dezembro de 2013, a Target Corporation anunciou ter sido vitima de uma violação maciça de dados, afectando cerca de 40 milhões de cartões de crédito e débito de seus clientes. Depois de certo tempo, o número estimado de clientes afectados por este ataque foi aumentado para 70 milhões, tornando-se um dos maiores roubos de dados na história (Targetcorporate, 2013).

Embora tenham sido reveladas informações oficiais escassas sobre as consequências do incidente, o jornalista de segurança Brian Krebs relatou que o vector de ataque suspeito foi phishing de email enviado a um fornecedor do alvo de nome Fazio Mecânico. Esta informação foi parcialmente confirmada por Fazio que anunciou ter sido "vítima de uma sofisticada operação de ataque cibernético" (Krebs, 2014).

3.1.1.4 Violações de Dados na eBay Inc.

Um incidente semelhante aconteceu em Maio de 2014, quando a eBay Inc. publicou um artigo no site da empresa, admitindo que o seu banco de dados contendo o nome dos clientes, senha cifrada, endereço de e-mail, endereço físico, número de telefone e data de nascimento foi violado, e aconselhando seus clientes a alterar suas senhas.

O artigo também apontou que a violação não afectou os dados financeiros porque estes tinham sido armazenados separadamente, e em formato cifrado, mas que um pequeno número de credenciais de login de colaboradores foi comprometido, o que criou desconfianças de que o phishing foi o vector de ataque inicial (Trendmicro, 2014) & (Hunt, 2014).

3.1.1.5 Violações de Dados ao Escritório de Gestão de Pessoal dos EUA

Em 2015, o Escritório de Gestão de Pessoal (OPM) dos Estados Unidos em Pequim, sofreu o roubo de dados digitais mais extenso na história, que resultou na perda de 21,5 milhões de registros de pessoal. A escala dessa violação teve como consequência a retirada do pessoal de inteligência dos EUA dos escritórios de Pequim como medida de segurança. O OPM declarou

que *"dos 21,5 milhões de indivíduos cujos Números de Segurança Social e outras informações confidenciais foram afetados pela violação, aproximadamente 5,6 milhões tiveram as impressões digitais roubadas* "(Harvey & Evans, 2016). Outros ataques como os que ocorreram na RSA SecurID, Target Corporation e no Fundo Monetário Internacional, têm provado cada vez mais a tendência dos cibercriminosos para roubo de identidade ou fraude que exploram o erro humano.

3.1.2 Ataques Recentes

3.1.2.1 Ransomware "WannaCry" Attack

Em Maio de 2017, houve um ciberataque mundial de ransomware visando computadores com sistema operativo Windows. O ataque cifrou os dados dos computadores infectados e exigiu o pagamento de resgate em Bitcoin. Este ataque num único dia, infectou mais de 300 mil computadores em mais de 150 Países (Thompson & Mullen, 2017), (Schallhorn, 2017) & (Newman, 2017).

O ciberataque Wannacry, é um programa malicioso que codifica os arquivos do computador alvo, tornando-os reféns para pedir resgate financeiro. Trata-se de um ataque *ransomware*, no qual as telas exibem uma mensagem exigindo dinheiro como resgate para decifrar as informações sequestradas (Eurotux. 2017) & (Parsons, 2017).

A figura 3 é ilustrativa da forma de ataque:

Figura 3 Mensagem de Ecrã do Sistema Atacado.

Fonte: (Adaptado de Parsons, 2017)

Este vírus infectou desde os equipamentos de 16 hospitais e centros de saúde no Reino Unido, computadores do Ministério do Interior na Rússia, a Renaul em França, e centenas de milhares de ocorrências em sites de vários Países. A seguir listamos algumas das principais ocorrências divulgadas pelo mundo:

No Brasil: O Instituto Nacional de Segurança Social (INSS) após o ataque, desligou os servidores e suspendeu o atendimento ao público (Elpais, 2017).

Na China: A empresa de segurança da internet Qihoo360 emitiu um "alerta vermelho" dizendo que um grande número de faculdades e estudantes no país tinha sido afectado pelo ransomware WannaCrypt. A imprensa estatal informou que os sistemas de pagamento digital em alguns postos de combustível ficaram *offline*, obrigando os clientes a pagar em dinheiro (Thompson & Mullen, 2017).

Na Alemanha: A empresa ferroviária alemã Deutsche Bahn (DB), informou ter sofrido um "ataque com cavalos-de-troia" na rede, mas que não alterou o tráfego dos comboios.

Na França: A Renault suspendeu a produção em várias fábricas devido à onda de ciberataques. A suspensão, "integra as medidas de protecção adoptadas para evitar a propagação do vírus".

Em Londres: O ransomware paralisou temporariamente os hospitais e instalações do Serviço Nacional de Saúde no Reino Unido, bloqueando as salas de emergência, atrasando os procedimentos médicos vitais e criando caos para muitos pacientes britânicos (Newman, 2017) & (Wolff, 2017).

Na Espanha: Dezenas de empresas espanholas sofreram o ciberataque. A companhia mais atingida foi a Telefónica, com a infecção de várias centenas de computadores de sua sede central, no Distrito C de Madrid (Thompson & Mullen, 2017), (Elpais, 2017a).

Nos Estados Unidos: A FedEx *corporation* admitiu ter sofrido "interferências" nos equipamentos usando o sistema operativo Windows devido a "um *malware*" (Thompson & Mullen, 2017).

No Japão: Cerca de 600 empresas japonesas, entre elas a Hitachi e a Nissan, foram afectadas pelo ciberataque mundial. A Hitachi confirmou que o seu serviço de e-mail foi invadido deixando alguns colaboradores com problemas para aceder arquivos, enviar e receber mensagens (Elpais, 2017).

Na Rússia: O Ministério do Interior admitiu que seus computadores foram afectados, e que o vírus infectou cerca de 1.000 computadores do ministério. A empresa ferroviária, telefonia MegaFon e o Banco Central da Rússia estão entre as várias entidades sofreram ataque (Schallhorn, 2017).

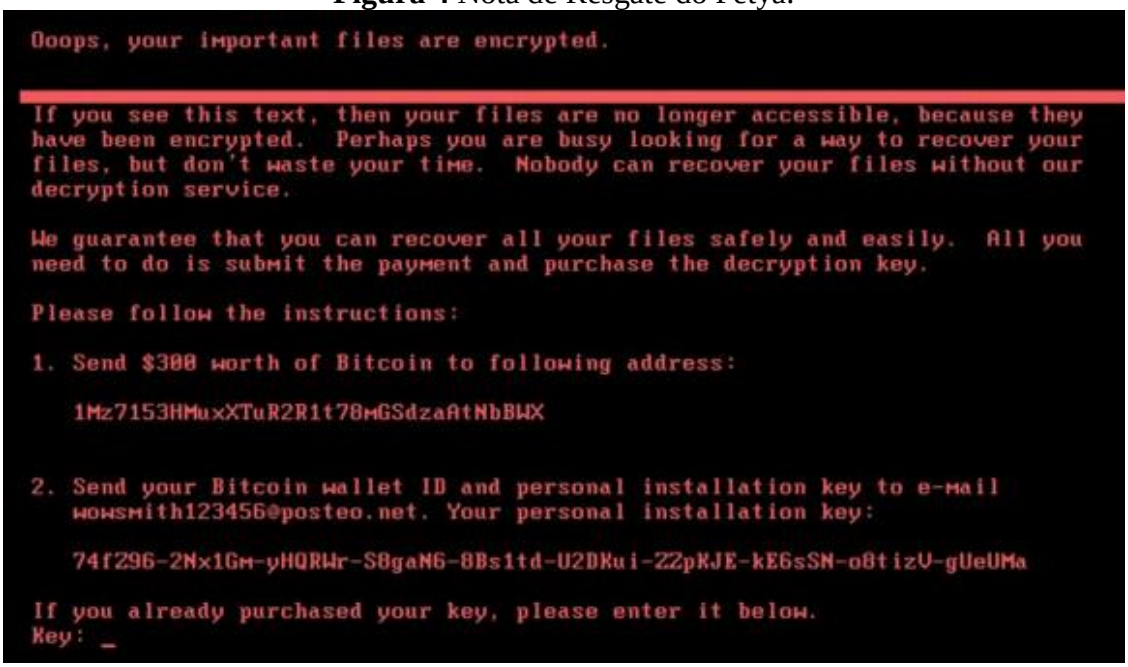
Embora as empresas atacadas não tenham dado muitas informações sobre os ataques sofridos, uma característica comum em todas, é o facto de ter sido usada pelo menos uma técnica de Engenharia Social no ataque. Os relatos dos mesmos, demonstram que nenhum sistema por mais sofisticado que seja, pode ser considerado 100% seguro.

3.1.2.2 Ransomware "Petya" Attack

Em Junho deste ano, uma nova estirpe de ransomware denominada "Petya" começou a espalhar-se no mundo com uma velocidade alarmante. Segundo a empresa de segurança Symantec, esta ameaça explora a vulnerabilidades "Eternal Blue" do Windows, podendo recolher senhas e credenciais dos computadores afectados. Os ataques Ransomware tornaram-se uma pestilência tão comum, que muitas empresas como medida preventiva, têm armazenando Bitcoins caso precisem desbloquear rapidamente os arquivos que forem afetados (Krebs, 2017) & (Boozallen, 2017) & (Eset, 2017).

A figura 4 mostra a imagem apresentada na tela dos computadores Microsoft Windows infectados com Petya.

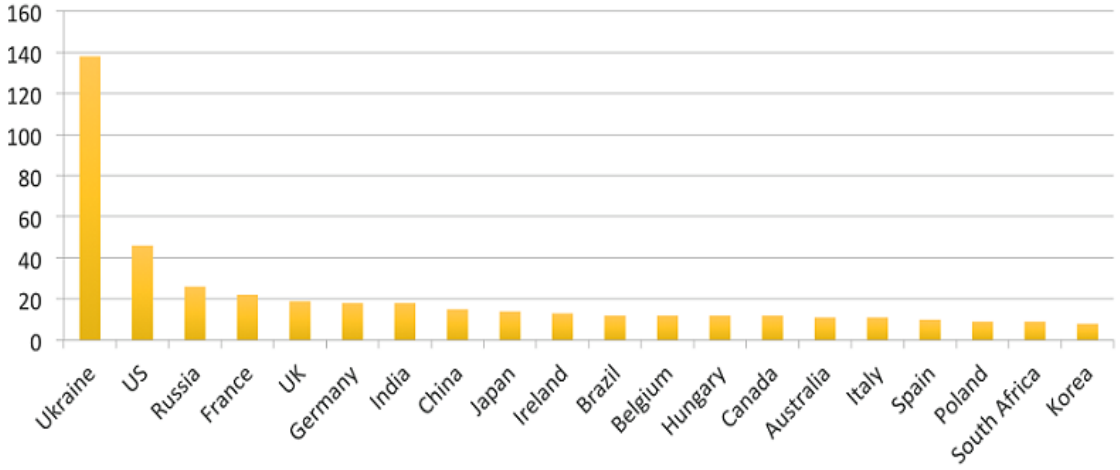
Figura 4 Nota de Resgate do Petya.



Fonte: (Adaptado de Krebs, 2017).

A Symantec (2017b) confirmou que um pacote de software de contabilidade (MEDoc), foi usado para a inserção inicial na rede da organização. O MEDoc é muito utilizado na Ucrânia, indicando que as organizações desse país eram o principal alvo. Conforme mostra o gráfico da figura 5, onde a Ucrânia aparece no topo dos Países afetados.

Figura 5 Os 20 Países com Maiores Números de Organizações Afectadas.



Fonte: (Adaptado de Symantec, 2017b).

Depois de entrar no sistema, o Petya usa uma variedade de métodos para se espalhar na rede da organização. Como por exemplo criar uma lista de IPs da rede local (LAN), e IPs remotos para se espalhar para esses destinos e criar listas de nomes de utilizadores e senhas que poderão ser usadas para vários fins (Symantec, 2017b).

Tanto o *WannaCry* quanto o *Petya* são duas formas maliciosas de software que usa criptografia para manter refém os dados até um resgate ser pago. O *Petya*, no entanto, apresenta uma forma mais destrutiva, pois alem de cifrar os dados, também destrói o sistema. Após a criptografia, as vítimas dos dois tipos de *malware* são informadas do ataque através da tela de seus computadores infetados, onde é exigido um resgate a ser pago em bitcoin para recuperar os dados.

3.2 Conceito de Engenharia Social (SE)

O maior problema na segurança são as pessoas, que pelas suas características psico-emocionais podem facilmente serem manipuladas, induzidas, coagidas, ou forçadas a violar aspecto de segurança para conceder acesso ou privilégios a alguém, dai que, a maior protecção contra a Engenharia Social, continua a ser a educação e consciencialização. Treinar o pessoal sobre como agir e relatar todas as acções anormais ou estranhas são as contra medidas mais eficazes contra a Engenharia Social (Jones, 2004) & (Filho, 2004).

Embora existam muitas definições para Engenharia Social no contexto da segurança de informação, podemos dizer informalmente, que a Engenharia Social descreve um fenómeno em que as pessoas são influenciadas a ter determinadas atitudes, que podem ser até, contra seu próprio interesse.

A Engenharia Social é definida no contexto das ciências sociais como uma disciplina que visa influenciar as crenças, atitudes, acções e comportamentos sociais em larga escala, (Wikipedia, 2016). No contexto da Segurança de Informação, tem um objectivo semelhante, pois visa ajudar o atacante a atingir seus objectivos, manipulando as pessoas e não a tecnologia (Baker et al, 2005)

Mitnick (2002) afirma que "…*para anular as medidas de segurança, o atacante ou engenheiro social deve encontrar um modo de enganar um utilizador para que ele revele as informações, ou ... forneça o acesso"*. Quando um colaborador é enganado, influenciado ou manipulado a revelar informações ou executar acções que criem uma lacuna na segurança, nenhuma tecnologia do mundo pode proteger a empresa. Reforçando esta ideia, outros autores deram a sua definição sobre Engenharia Social.

Christopher Hadnagy nas primeiras páginas de "Engenharia Social: A Arte do Hacking Humano", diz que "*A Engenharia Social é o ato de manipular uma pessoa para tomar uma acção que pode ou não estar no melhor interesse do alvo ".*

Hadnagy reforça que as técnicas de Engenharia Social são frequentemente usadas na nossa vida quotidiana por pessoas de vários estratos sociais como por exemplo, os médicos que influenciam o comportamento dos pacientes com o objectivo de melhorar sua saúde, ou pelos pais que influenciam comportamento dos filhos para que façam a coisa certa (Hadnagy, 2010).

Foozy argumenta que:

> *"O propósito dos ataques de Engenharia Social, é obter o acesso directo a informação, usando o acesso físico ou digital ao sistema de informação de uma organização".*

In Foozy (2011).

Mouton argumenta que:

> *"A Engenharia Social refere-se a várias técnicas utilizadas para obter informações, a fim de contornar os sistemas de segurança, através da exploração da vulnerabilidade humana".*

In Mouton et al, (2010).

Huber argumenta que:

> *"A Engenharia Social é a arte de explorar o elo mais fraco dos sistemas de segurança da informação: as pessoas que os usam".*

In Huber (2009).

Long argumenta que:

> *"A Engenharia Social não confia numa peça defeituosa de equipamentos de alta tecnologia para montar o ataque; Em vez disso, ele usa um ataque hábil na psique do adversário ".*

In Mitnick &Long (2008).

Evans argumenta que:

> *"Os ataques de Engenharia Social têm o objectivo de recolher uma certa quantidade de dados para serem usados posteriormente num ataque técnico".*

In Evans (2009).

Mitnick argumenta que:

> *"Usando a influência e a persuasão para enganar as pessoas, convencendo-as por manipulação de que é alguém que na verdade não é, o engenheiro social é capaz de tirar proveito das pessoas para obter informações ou persuadi-las a executar uma acção, com ou sem o uso da tecnologia ".*

In Mitnick & Simon (2002).

Analisando as opiniões destes autores, uma coisa torna-se óbvia, todos concordam que o alvo primário e único de um ataque de Engenharia Social é o homem, que é considerado pela maioria deles como o elo mais fraco do sistema. E quase todos mencionam a existência de alguma forma de manipulação ou influência do atacante sobre o alvo.

Outra retirada importante dessas definições, é a ausência ou menção de dispositivo computacional. Ao analisarmos as ferramentas da Engenharia Social, vemos que elas não dependem do uso de computadores e podem ser aplicadas também no contexto de uma organização que gere sua informação totalmente em papel.

Por outro lado, se excluirmos totalmente as TI da Engenharia Social, perderemos elementos importantes muito usados pelos atacantes, como é o caso dos ataques de phishing e outros, que usam meios computacionais.

Foozy (2011) definiu um modelo conceitual de ataques de Engenharia Social que abarca as componentes técnicas e humanas. No modelo podemos ver as técnicas utilizadas para

influenciar ou manipular psicologicamente o alvo sem o uso de tecnologias, e as técnicas utilizando meios tecnológicos, que através da acção de um colaborador, conseguem explorar vulnerabilidades no sistema.

3.3 Técnicas Utilizadas

O ser humano possui várias vulnerabilidades facilmente exploradas pelos engenheiros sociais, tais como, confiança, medo, curiosidade, instinto de querer ajudar, ingenuidade, ganância e culpa. A maioria dos especialistas em segurança concorda que a educação dos utilizadores é essencial para uma estratégia eficaz de segurança da informação. (Mitnick & Simon,2002). Porém, a maioria destas formações se baseia apenas em ameaças electrónicas, de como detectar um *phishing* ou *spear phishing* ataque ou como evitar o download e instalar *malware*.

Embora essas ameaças também sejam Engenharia Social devido ao seu elemento enganoso, os colaboradores não têm sido treinados a suspeitar de telefonemas aparentemente benignos de pessoas que pareçam acima de suspeitas.

Lidar com a Engenharia Social baseada em meios electrónicos é relativamente mais fácil porque, como acontece mais regularmente, os utilizadores podem ser ensinados a não abrir e-mails de alguém que não reconhecem, nem fazer downloads em sites duvidosos. Mas a Engenharia Social baseada em influência, como telefonemas de pessoas aparentemente confiáveis, ou permitir a entrada na empresa de uma pessoa estranha, se baseando na sua boa aparência, uniforme de uma empresa conhecida, ou por ter contado uma história muito convincente, pode se caracterizar numa séria ameaça (Mouton, 2014).

Os ataques de Engenharia Social baseados em influência, são muito mais subtis e difíceis de detectar porque envolvem os cenários mais complexos e ilimitados que surgem a partir da interacção do dia-a-dia entre seres humanos (Cialdini, 2005) & (Peltier, 2006). A maioria das organizações não treina seus colaboradores para reconhecer esses perigos potenciais que são explorados pela característica inata dos seres humanos confiarem, quererem ser úteis e serem vistos como "boas pessoas".

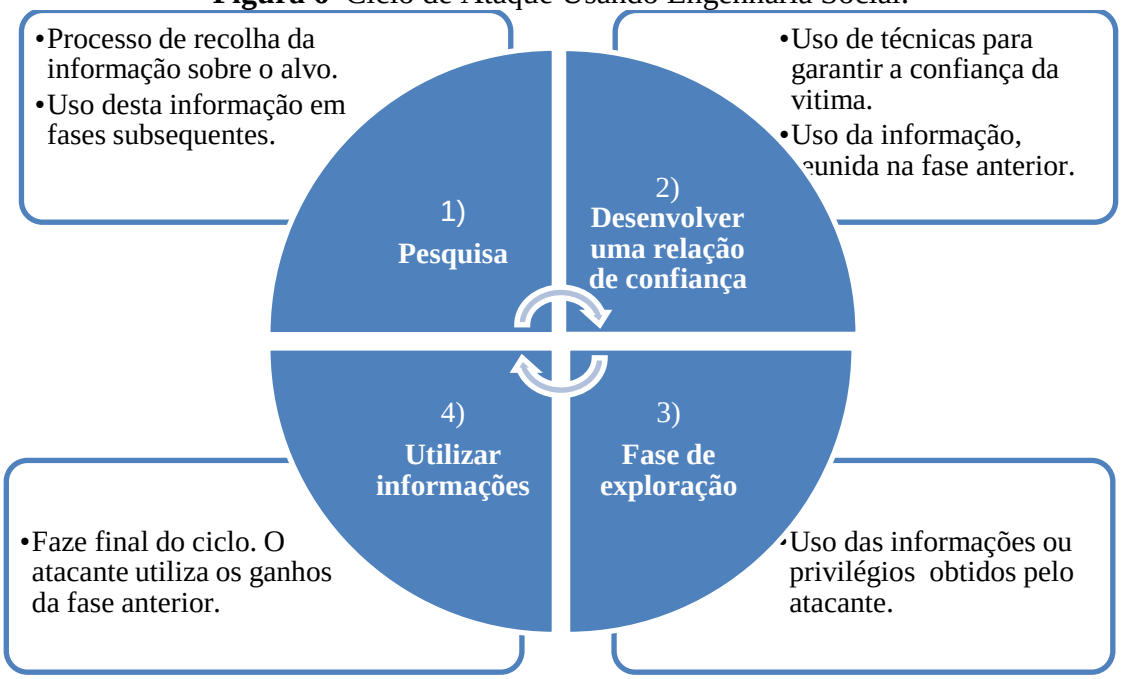
De acordo com esta constatação, Mitnick e Simon (2002), baseiam a Engenharia Social em 6 tendências humanas básicas.

1. Gosto
2. Consistência e compromisso
3. Escassez

4. Reciprocidade
5. Tendência natural a ser útil
6. Autoridade

Existem vários modelos de ataques de Engenharia Social (Mouton, 2016), mas o modelo mais conhecido é o ciclo de ataque de Kevin Mitnick descrito no livro "A Arte de Enganar" (Mitnick e Simon 2002). A figura 6 mostra as quatro fases deste ciclo de ataque de Engenharia Social:

Figura 6 Ciclo de Ataque Usando Engenharia Social.



Fonte: (Adaptado de Mitnick & Simon, 2002)

Segundo Cialdini (2006) & (Mouton, 2014), as seis "tendências" humanas *"podem mudar as nossas atitudes, comportamento ou crenças devido à pressão externa que pode ser real ou imaginaria"*. E descrevem estas influências ou princípios de comportamento humano como apresentamos na figura 7*:*

Figura 7 Seis Princípios de "Influências".

Fonte: (Adaptado de Cialdini, 2006 & Mouton, 2014)

Amizade ou Gosto: reflecte a ideia de que as pessoas estão dispostas a "fazer o impossível" pelas pessoas que gostam, ou seja, a vítima estará mais disposta a cooperar com o atacante se este for considerado amigo.

Compromisso e Consistência: reflecte a ideia de que as pessoas tendem a cumprir compromissos e agir em consistência com suas opções, mesmo que suas escolhas sejam inconsistentes e até mesmo ilógicas.

Escassez: reflecte a ideia de que as pessoas irão alterar seu comportamento em busca de um recurso escasso, independente do seu real valor.

Reciprocidade: reflecte a ideia de que as pessoas estão dispostas a pagar bondade com bondade, ou "devolver o favor". As pessoas estão predispostas a serem cordiais com quem os trate bem.

Aprovação Social: reflecte a ideia de que as pessoas tendem a comportar - se de maneiras que consideram socialmente aceitável para ganhar a aprovação das pessoas com quem se relacionam (amigos, vizinhos, colegas, familiares, etc).

Autoridade: reflecte a ideia de que as pessoas vão cumprir os pedidos feitos por figuras de autoridade, pois têm mais dificuldade em negar pedidos que vêm de pessoas com autoridade percebida sobre elas.

Os engenheiros sociais usam inúmeras maneiras de obter acesso a informações confidenciais. Mas o elemento comum em todas as técnicas é o engano. Seja enviando um e-mail *phishing* ou se passando por um técnico de suporte informático ou ficando do lado de fora da empresa usando um uniforme de alguma empresa de entregas ou mensageiro, para enganar um alvo e conseguir dele informações sensíveis (Ashford, 2016).

Antes de citarmos as diversas técnicas de ataques existentes, o ideal é descrever quem podem ser os atacantes, uma vez que erradamente algumas pessoas pensam que os ataques só são feitos por hackers.

A tabela 1, mostra alguns tipos de intrusos e seus principais objetivos:

Tabela 1 Tipos de Atacantes e Principais Objectivos
(Adaptado de Ashford, 2016)

Atacantes	Objetivos
Estudantes	Invadir sistemas para bisbilhotar mensagens de correio electrónico por diversão.
Hackers	Testar sistemas de segurança, roubar informações, como senhas e números de cartões de crédito, desfalques financeiros.
Concorrentes	Descobrir planilhas de preços, cadastro de clientes, plano estratégico, etc.
Ex-colaboradores	Sabotagem por vingança.
Corretores de valores	Distorcer informações para lucrar com o valor das ações.
Espiões	Descobrir informações estratégicas (pessoais/financeiras/comerciais /politicas/militares, etc).
Terroristas	Causar a paralisação do sistema, espalhar o pânico pela rede e roubar de informações confidenciais.

Os métodos de ataque mais usados por engenheiros sociais se enquadram nas categorias abaixo descritas.

3.4 Métodos de Ataque

3.4.1 Recolha de Informações

A fase mais importante dos ataques de Engenharia Social é o reconhecimento. O reconhecimento lida com a aquisição de informações a partir de uma infinidade de fontes, que vão permitir ao atacante adaptar o ataque. Um ataque personalizado tem a vantagem de ser menos reconhecível, deixar menos vestígios e ser menos detectável (Russell, 2009).

A figura 8 demostra o tipo de informações geralmente recolhidas nesta fase de preparação:

Figura 8 Informações Recolhidas na Fase de Preparação do Ataque.

Fonte: (Adaptado de Russell, 2009)

A seguir demonstraremos algumas das ferramentas de pesquisa mais usadas nesta fase, com dados relacionados a empresa "estudada", para descobrirmos que informações um atacante encontraria, fazendo a mesma pesquisa, e o quanto a sua revelação poderá comprometer a segurança.

Estas informações geralmente são conseguidas executando um ou mais procedimentos de recolha de informações que passaremos a descrever:

3.4.1.1 Google Hacking

Esta ferramenta permite pesquisar e refinar os resultados. O mecanismo de busca do Google é ágil e agressivo na sua indexação, o que às vezes resulta em informações indexadas sem o conhecimento da organização alvo. Um atacante pode usar as informações indexadas pelo Google para preparar ou adaptar o seu ataque (Mitnick & Long, 2008).

As pesquisas do Google que podem facilitar um invasor incluem:

Site da empresa: exemplo < MATOX.com > (este tipo de pesquisa dá-nos o domínio da empresa alvo).

Procura pelo domínio: Site: <MATOX.com> @ MATOX.com (Pode revelar endereços de e-mail e nomes de colaboradores).

Extensões de documentos: Podem revelar entradas de calendário indexadas para o domínio < MATOX.com >. Exemplo: Site: < MATOX.com > ext: xls (pode revelar arquivos do Excel que contenham informações do directório, nomes de utilizadores, e-mails).

3.4.1.2 Redes Sociais

O uso massificado das redes sociais por um público cada vez maior, tem vindo a favorecer ataques de Engenharia Social (Hadnagy, 2012). Informações que outrora eram privadas e difíceis de adquirir, são agora voluntariamente compartilhadas pelos seus proprietários, facilitando a fase de reconhecimento para os engenheiros sociais (Verizon, 2016).

Os atacantes usam as redes sociais para obter informações das vítimas sobre:

- ➔ Qualificações (cargo ou funções).
- ➔ Interesses.
- ➔ Rede profissional e de amigos.
- ➔ Ausência e presença em áreas específicas (eventos que participa).

3.4.1.3 Contacto Telefónico

Com as informações recolhidas na fase anterior, o Engenheiro Social pode fazer uma abordagem telefónica fazendo-se passar por um assessor, cliente/fornecedor ou prestador de serviços, para obter acesso não autorizado a empresa. Fazendo-se passar por outra pessoa (de preferência alguém que a vítima conheça), o engenheiro social consegue acesso a informações necessárias para concretizar o ataque.

Segundo Rafael (2013),"*a maior vantagem do uso desta técnica é que a maioria das pessoas pensam que são imunes a tais truques por serem de alguma forma mais inteligentes ou mais conscientes que os outros*". Os primeiros alvos destes ataques são as secretárias, recepcionistas, seguranças e pessoal de limpeza, pois esses colaboradores estão sempre em contacto (directo ou indirecto) com as pessoas que detém cargos de poder dentro da empresa, os verdadeiros alvos.

3.4.1.4 Abordagem Pessoal

É uma técnica arriscada onde o atacante tem de ir fisicamente a empresa alvo. Esta abordagem pode ser feita, passando-se por um fornecedor de equipamentos, técnico de manutenção, amigo do director, prestador de serviço, ou outros. Usando o poder de persuasão e contando com o

desconhecimento dos colaboradores (segurança, secretária, recepcionista ou outros), o atacante tenta conseguir acesso a áreas onde possa recolher informações (Rafael, 2013).

3.4.1.5 Análise do Lixo

A maioria das empresas não têm o cuidado de verificar o que os colaboradores deitam fora e como deitam. O lixo das empresas é uma das melhores fontes de informações para os engenheiros sociais. Existem muitos relatos de ataques usando informações recolhidas no lixo, que continham nomes de colaboradores, telefones, e-mail, senhas, contacto de clientes, fornecedores e transações efetuadas.

Em a arte de enganar, Mitnick (2002) relata que "*procurando nas lixeiras dos terminais dos autocarros, conseguia encontrar blocos de passagens parcialmente usados, que eram jogados fora pelos próprios motoristas no final de seus turnos*". Com aqueles blocos de passagens em branco e um furador, ele falsificava suas próprias passagens e viajava para qualquer parte de Los Angeles aonde fossem os autocarros. Hoje esta técnica já é pouco útil, uma vez que as informações outrora procuradas no lixo são agora obtidas usando pesquisas electrónicas.

3.4.2 Engenharia Social Inversa

Nesta abordagem o atacante cria uma situação que influencia a vítima a iniciar o contacto, pedindo uma solução para uma questão técnica. A principal vantagem desta técnica é que os utilizadores nunca duvidam da autenticidade da comunicação que eles próprios iniciaram, devido à ilusão de controle da situação, por terem sido eles que iniciaram a conexão.

3.5 Uso de Ferramentas

3.5.1 SET

O Social-Engineer Toolkit (SET) é uma ferramenta projectada para realizar ataques contra o elemento humano e rapidamente se tornou muito utilizada para testes de invasão (SCO, 2012).

Esta ferramenta permite explorar o alvo através de vulnerabilidades em aplicativos, recolhendo informações confidenciais como senhas e conta de utilizador. *Os* métodos mais eficientes de ataque do SET são o phishing e-mails com anexo malicioso, ataques applet Java em navegadores, roubo de credenciais em Websites, criação de USB /DVD/CD infectados, e outros vectores semelhantes . No menu principal da ferramenta (tabela 2), apresentaremos os principais métodos de ataque (Miércoles, 2012).

Tabela 2 Opções do Menu Inicial do SET.
(Adaptado do Menu Principal da Ferramenta SET)

Opções do Menu Inicial
1) Ataques de Engenharia Social
2) Teste de Invasão Rápida
3) Módulos de Terceiros
4) Atualizar o Metasploit Framework
5) Atualizar o Social-Engineer Toolkit
6) Atualizar Configurações SET
7) Ajuda e Créditos Sobre…
8) ...

Na tabela 3, opções que permitem a criação de vectores de ataque:

Tabela 3 Opções dos Principais Módulos de Ataque do SET.
(Adaptado do Menu Principal da Ferramenta SET)

Seleccione no menu
1) Vectores de ataque Spear-Phishing
2) Vetores de Ataque de Website
3) Criar Mídia Infectada
4) Criar uma carga útil e Ouvinte
5) Ataque de Mail em Massa
6) Ataque Baseado em Vetor Arduino
7) Vetor Ataque SMS Spoofing
8) Vetor de Ataque do AP Sem Fio
9) Vetor do Ataque do Gerador de QRCode
10) Vetores de Ataque de PowerShell
11) Módulos de Terceiros

Utilidade da Ferramenta:

1) O ataque de phishing leva a cabo ataques de correio electrónico dirigidos contra uma vítima.

2) O ataque Web utiliza fragilidades em páginas Web para comprometer o computador da vítima que aceda a eles.

3) O gerador de mídia infectada permite infectar dispositivos de armazenamento por meio do arquivo autorun.inf que é auto executável.

4) O ataque de Mail em massa, permitir enviar correios electrónicos a muitas vítimas com mensagens personalizadas, entre outras utilidades.

3.5.1.1 Sites Falsificados

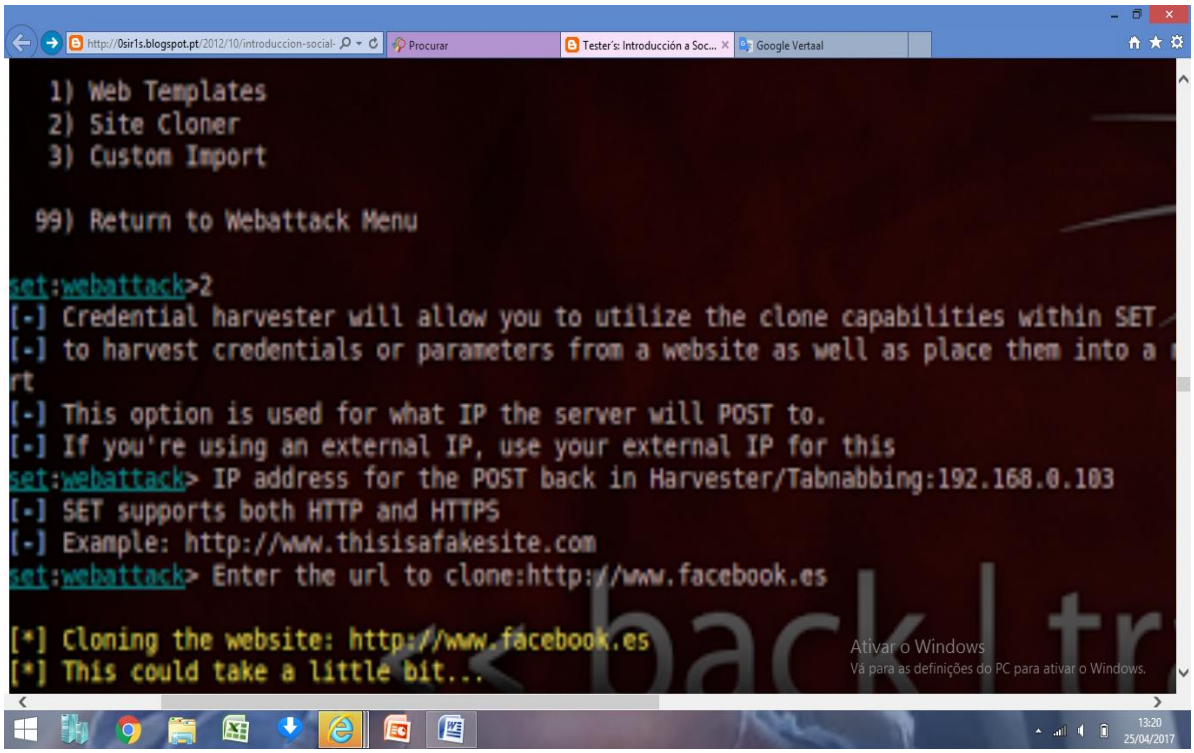
Um método muito utilizado para recolha de credenciais de utilizadores é através de sites falsificados fazendo-se passar pelo legitimo. A falsificação do site facebook é uma técnica muito usada, que permite ao atacante obter rapidamente o e-mail e senha do alvo (figura 9). Este é o tipo de ataque que a maioria das pessoas caiem constantemente, pois dificilmente as pessoas prestam atenção ao "URLs" da página antes de colocarem suas credenciais (HackingArticles, 2016).

Figura 9 Pagina do Facebook Falsificada pela Ferramenta SET.

Fonte: (Adaptado de Guiadoti, 2013)

Para obter a pagina falsificada mostrada na figura 9, basta clicar na opção 2 do menu do SET (de clonar o site), e preencher os campos pedidos, como podemos ver na figura 10. Após alguns segundos, temos o site copiado em http: // localhost, (com o URLs indicando o computador local!). (Guiadoti, 2013).

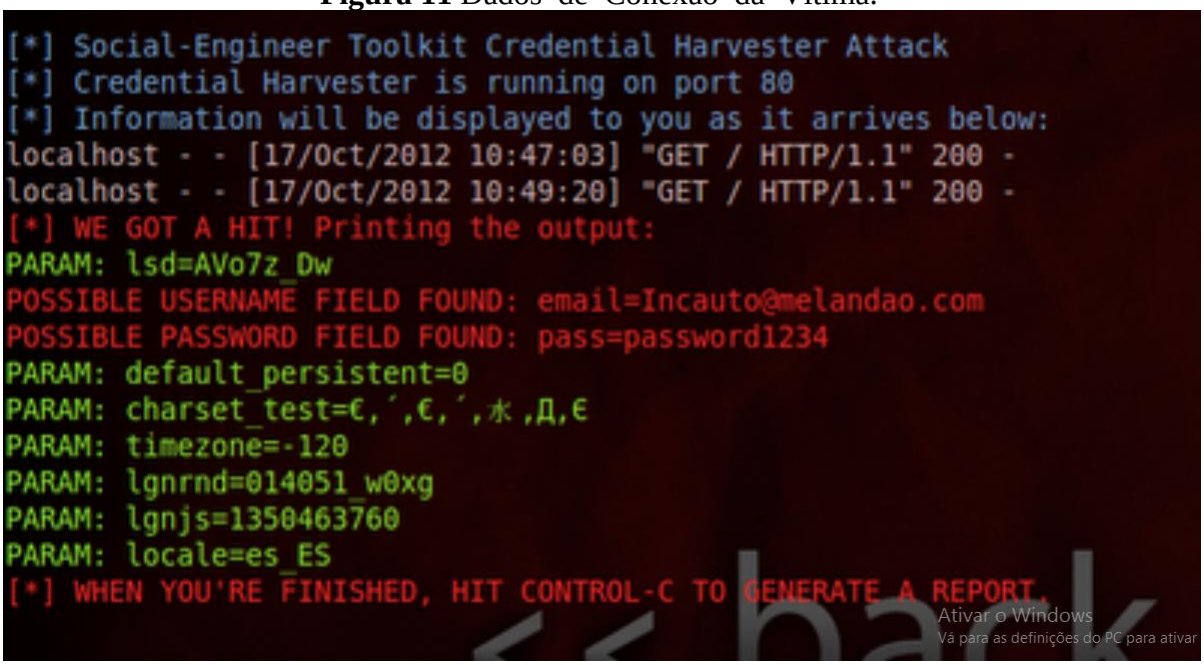
Figura 10 Falsificação do Site.



Fonte: (Adaptado de Guiadoti, 2013)

De seguida, é feito um DNS-spoofing para obter os dados de conexão da vítima (figura 11).

Figura 11 Dados de Conexão da Vitima.



Fonte: (Adaptado de Guiadoti, 2013)

Como pudemos demonstrar, o SET é uma ferramenta muito fácil, ágil, precisa e não exige muita perícia para usa-la, o que explica o facto de ser bastante utilizada por malfeitores em ataques exploratórios.

3.5.2 MALTEGO

Maltego é uma aplicação forense de mineração de dados que consulta várias fontes de dados públicas e descreve graficamente as relações entre entidades, como pessoas, empresas, sites e documentos. Ele oferece uma interface para recolha e mineração das informações, e as representa num formato fácil de perceber (Socialengineer, 2017).

Através da sua biblioteca de gráficos, o Maltego identifica as principais relações entre as informações e as relações anteriormente desconhecidas entre elas. A ferramenta funciona como um banco de dados relacional, encontrando links entre bits de informação tratados como entidades dentro da aplicação, isso é óptimo para o engenheiro social, pois simplifica o seu trabalho de estudar as tendências e gostos da vítima.

A mineração de informações, permite relacionar endereços de e-mail, sites, endereços IP e informações de domínio, além de procurar por qualquer endereço de e-mail dentro de um domínio de destino. Isso permite descobrir, que sites determinado endereço de e-mail visitou, e com isso criar um perfil do alvo.

3.5.3 FOCA

O FOCA faz testes de invasão que analisam metadados em qualquer documento disponibilizado na Web. A sua utilização é muito simples, basta usar o aplicativo no site da empresa alvo, e clicar no botão "procurar todos", e o FOCA exibirá todos os documentos *PDF, Microsoft Office, Open Office* e outros no site da empresa que foram indexados pelo Google ou outro motor de busca (Elevenpaths, 2017).

A ferramenta também permite baixar esses documentos, e extrair deles metadados como nomes de utilizador, pastas de rede, nomes de impressora, endereços de e-mail, e detalhes sobre o software que foi usado para criar os arquivos.

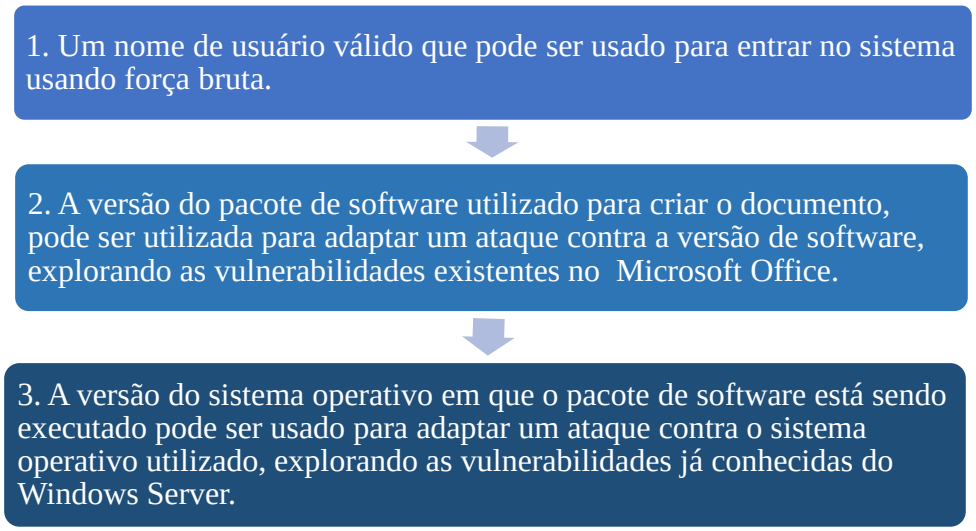
Principais funções:

1. Obtém informações dos metadados de arquivos.
2. Analisa arquivos *online* e *offline*.

3. Da informação de hábitos de navegação de utilizadores de um servidor DNS.
4. Faz um mapa de rede com todos os dados extraídos.

Como mostra a figura 12, dos metadados, o invasor pode retirar informações importantes como:

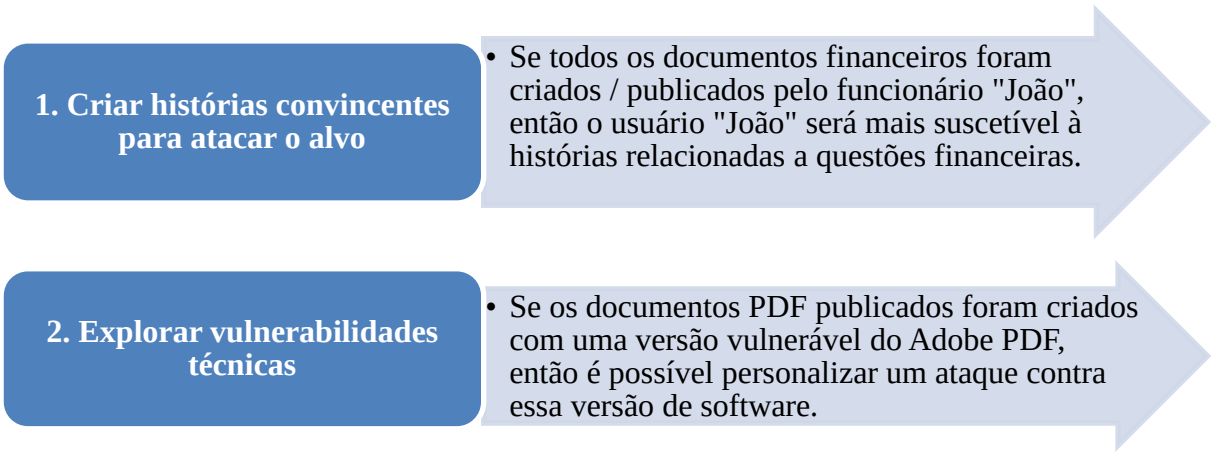
Figura 12 Informações dos Metadados.



Fonte: (Adaptado de ElevenPaths, 2017)

O invasor pode usar as informações extraídas dos metadados num dos dois cenários da figura 13:

Figura 13 Uso das Informações Extraídas dos Metadados.



Fonte: (Adaptado de ElevenPaths, 2017)

No Defcon[5] 18, os hackers José Palazon Palatko e Chema Alonso, utilizaram o FOCA 2.5 no site da casa branca e mostraram credenciais de utilizadores internos não acessíveis na Internet, o que comprovou a eficácia da ferramenta (Hadnagy & Maxwell, 2012).

3.6 Uso de e-mails

3.6.1 Worms

Alguns vírus possuem a característica de se espalharem facilmente, por isso recebem o nome de worms (vermes). Este tipo de vírus, são usados em emails e paginas Webs para se propagarem mais rapidamente, mas isso requer que o utilizador ao receber o e-mail ou visitar determinada pagina, execute o arquivo em anexo ou clique em determinado link para que seu computador seja contaminado, para isso, os atacantes usam textos que despertem o interesse ou curiosidade do alvo.

Os engenheiros sociais aproveitam esta particularidade do vírus infectar dezenas ou centenas de utilizadores rapidamente, enviando para vários endereços um e-mail com *worm*, usando como tema cartões virtuais de amizade. O alvo ou alvos que forem enganados pela mensagem vão contaminar seus computadores, e o worm para se propagar vai enviar cópias da mesma mensagem para a lista de contactos das vítimas com o endereço de e-mail da vítima como remetente (Rafael, 2013). A táctica de engenharia social neste caso, explora um assunto sensível a qualquer pessoa, "a amizade" .

3.6.2 Spyware

São programas espiões que reúnem informações do utilizador supervisionando o seu comportamento e preferências enquanto o mesmo navega na internet. Eles podem ser instalados no computador como troianos, que são instalados sem o consentimento dos utilizadores quando o mesmo visita sites que contêm códigos maliciosos que exploram vulnerabilidades no navegador da Web, ou como softwares livres ou freeware, que incluem *spyware* no pacote de instalação (Rafael, 2013).

O *spyware* pode ser instalado sem a aprovação do utilizador, e o tipo mais comum de informação recolhida é o endereço dos sites visitados, os sites de motores de busca

[5]DEF CON (também escrito como Defcon, ou DC) é uma das maiores convenções anuais de hackers do mundo, realizada anualmente em Las Vegas. O encontro inclui concursos e competições de hackers onde equipes tentam atacar e defender computadores e redes usando softwares e estruturas de redes.

usados, a versão do sistema operativo, os softwares usados no computador infectado e endereços de e-mail.

3.6.3 Phishing

Phishing é derivado da palavra pesca em inglês, e é intencionalmente mal escrito para mostrar a facilidade de confundirmos palavras similares, fazendo uma comparação com a facilidade de confundir um domínio ligeiramente errado. Neste caso, a vítima é o peixe que morde a isca.

Os ataques típicos de phishing incluem e-mails não autênticos, mensagens em redes sociais (Facebook, Twitter, etc.), ou plataformas de mensagens instantâneas e sites falsificados, imitando o verdadeiro, mas geralmente possuindo um nome de domínio ligeiramente diferente (Higbee, 2016).

E-mails falsos são enviados a organizações e pessoas para aguçar a curiosidade ou algum outro sentimento que faça com que o utilizador realize as operações solicitadas. Os casos mais comuns de *Phishing* são e-mails dizendo que o utilizador pode receber algum prémio (telemóvel, computador, promoções) se clicar na ligação abaixo. A maioria dos *Phishings* possuem algum anexo ou l*inks* dentro do e-mail que direccionam a situação desejada pelo atacante (Baker et al 2005) & (Rafael, 2013). Este tipo de ataque muitas vezes é precedido por um estudo sobre os gostos e tendências da vítima.

Também podem ser utilizadas mensagens intimidatórias dizendo que determinado programa deixará de funcionar se não fizer o *download* de actualização do link abaixo, ou dezenas de outras histórias semelhantes com as situações mais absurdas, mas que muitas pessoas ainda caem por falta de conhecimento.

3.6.3.1 Spear Phishing

O *spear* ao contrário dos padrões de ataque *Phishing* é direccionado a um único alvo. A ideia principal é fazer com que o alvo acredite que a fonte do e-mail é alguém dentro da empresa e com algum tipo de autoridade. Enquanto o objectivo de *Phishing* é roubar informações, o do *Spear Phishing* é obter acesso não autorizado (Baker et al 2005) & (Rafael, 2013).

3.6.4 Ransomware

O ransomware é um vírus que infecta o computador do alvo cifrando os arquivos até que a vítima pague um resgate. Os criminosos fornecem instruções as vítimas sobre como comprar *bitcoin* e pagar o resgate. O preço do resgate é definido de acordo com a condição financeira da vítima, e podem chegar a centenas de milhares de dólares (Schneier, 2017a) & (GReAT, 2017).

De 2005 à 2016, o *Internet Crime Complaint Center* (IC3) do departamento de justiça americana, revelou que recebeu perto de 7,700 queixas de ransomware, com perdas de 57.6 milhões de dólares. As perdas incluem pagamentos de resgates entre 200 e 10,000 dólares, e custos de lidar com os ataques. Este ano, um ataque de ransomware conhecido como WannaCry (*Win32/Filecoder.WannaCryptor.D*) espalhou-se rapidamente por todo o mundo e afectou sistemas em mais de 150 Países (Eset, 2017).

O "*WannaCry*" é baseado numa vulnerabilidade desenvolvida pela Agência de Segurança Nacional dos Estados Unidos (NSA), contra versões do sistema operativo *Windows* (Eurotux, 2017). A Microsoft corrigiu estas vulnerabilidade um mês antes do ataque, mesmo assim, o ataque afectou versões antigas do Windows que a Microsoft já não suporta, assim como versões recentes não actualizadas (Schneier, 2017a).

3.6.5 Man-in-the-Middle (PRMitM)

Pesquisadores do *Cyberpion* e *College of Management Academic Studies* de Israel descreveram um *"Password Reset Man-in-the-Middle Attack*" também conhecido como ataque PRMitM onde os hackers conseguem roubar a conta de e-mail de um utilizador, fazendo com que ele se inscreva noutro site, mesmo estando protegido por autenticação de dois fatores 2FA (Gelernter, et al, 2017). Segundo estes pesquisadores, o ataque é desenvolvido da seguinte forma:

Utilizando Engenharia Social, o atacante leva o utilizador a se inscrever numa conta aliciante para a vítima, como sites de jogos, filmes, testes de personalidade gratuitos, sorteios ou outros. O processo de inscrição apresenta uma série de prompts começando com o endereço de e-mail da vítima.

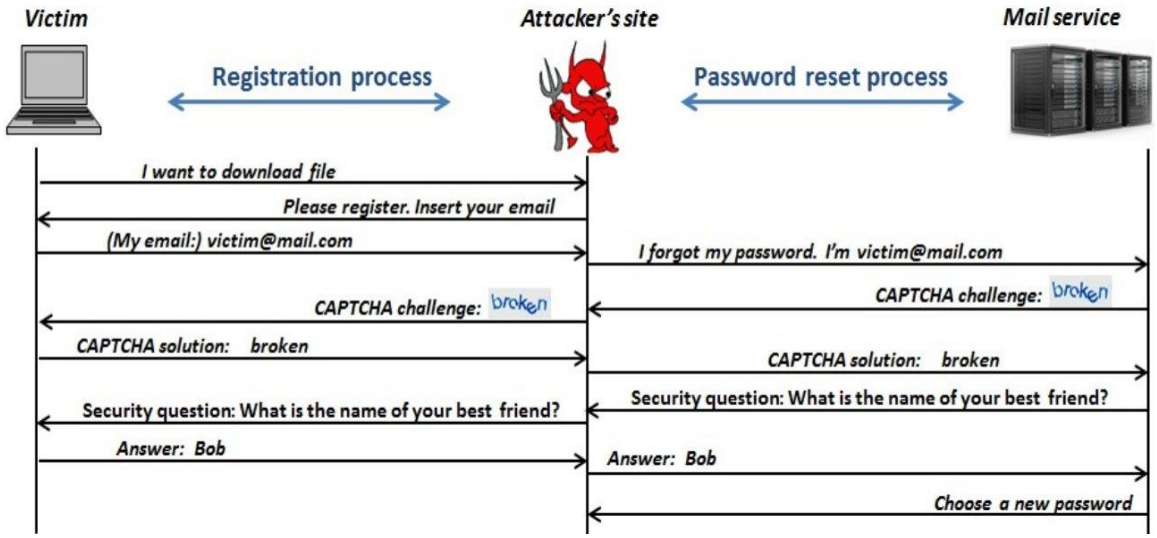
Em posse do endereço de e-mail, o atacante inicia um processo de redefinição de senha clicando em "Eu perdi acesso ao meu email". A partir dai, cada pergunta no processo de inscrição da vítima para o serviço do invasor será uma questão de redefinição de senha do provedor de e-mail da vítima. Por exemplo, se o provedor de e-mail enviar um PIN para o telefone da vítima como parte do processo, o invasor solicita o seu número de telefone e diz: "Acabei de lhe enviar

um PIN, insira-o agora". A vítima insere o PIN e o atacante repassa esse PIN para o seu provedor de e-mail.

O mesmo acontece para "perguntas de segurança" como "em que rua viveu quando criança?" O provedor de e-mail faz ao invasor essas perguntas, e ele faz as mesmas perguntas para o processo de inscrição da vítima, e usa as respostas para representar a vítima para o provedor de e-mail (Gelernter, et al, 2017).

Esta representação de ataque é bem ilustrada na figura 14:

Figura 14 - Roubo de Credenciais de E-Mail com Autenticação 2FA.



Fonte: (Adaptado de Gelernter, et al, 2017)

Trata-se de um ataque que revela fragilidades no padrão de redefinição de senha vulneráveis ao ataque PRMitM. Esta vulnerabilidade permite que até um atacante fraco assuma contas de muitos sites, incluindo Google e Facebook (Schneier,2017b), por isso os colaboradores devem ter bastante consciência dos riscos que correm quando utilizam seus e-mails em sites.

3.7 Baiting

O baiting é semelhante aos ataques de *phishing*, so que o atacante utiliza algum item como isca para atrair vítimas. Exemplos de *baiters* são sites que oferecem músicas/filmes/jogos livres para downloads desde que o utilizador forneça suas credenciais de login para o site ou aplicativo (Thornton, 2017).

Baiting ataques são também usados para explorar a curiosidade humana através do uso de dispositivos como Cds e *pendrives* que são deixados em lugares estratégicos para que possam servir de isca para algum colaborador.

Um desses ataques foi documentado por Steve Stasiukonis, fundador da *Secure Network Technologies*, em 2006. Para avaliar a segurança de um cliente financeiro, Steve e sua equipe infectaram dezenas de USBs com um vírus Trojan e dispersaram os dispositivos infectados em torno do estacionamento da organização. Mesmo com todos conhecimentos sobre segurança, muitos colaboradores pegaram os USBs e os ligaram aos seus computadores, activando um *logger* chave que deu a Steve acesso as credenciais de login dos colaboradores (Johansson, 2008).

Os colaboradores da empresa, mesmo tendo consciência dos riscos que corriam, preferiram ignorar o perigo que expunham a sua organização para saciar o seu instinto de curiosidade ou ganância.

A Engenharia Social joga com um elemento básico e elementar do ser humano, "seus instintos", por isso é tão eficaz. Uma característica interessante nos ataques desta natureza, é que eles dependem do nível de especialização do Engenheiro Social, que pode ser baixo (com técnicas fáceis), a alto, para ataques que precisam de habilidades sociais e /ou técnicas substanciais.

Nestes ataques, a interacção com o alvo pode ser nenhuma (inexistente), virtual (usando um meio) ou física (pessoalmente), conforme mostrado na tabela 4:

Tabela 4 Especialidades do Engenheiro Social e Técnicas Correspondentes. (Adaptado de Johansson, 2008)

Nível de especialização do engenheiro social	Meios de interacção	Técnicas de engenharia social
Baixo	**Nenhum**	✓ Reconhecimento físico ✓ Identificação de pessoas ✓ Dumpster diving ✓ Pesquisa na Web
	Virtual	✓ Personificação virtual
Médio	**Nenhum**	✓ Análise forense ✓ Phreaking ✓ Análise de perfis
	Virtual	✓ Mail-outs ✓ Phishing ✓ Engenharia social inversa ✓ Software mal-intencionado
	Físico	✓ Abordagem direta ✓ Tailgating ✓ Piggybacking ✓ Office snooping ✓ Desk sniffing ✓ Deixar cair Itens como iscas
Alto	**Virtual**	✓ Roubo de identidade
	Físico	✓ Personificação física ✓ Roubo de dados

Acredita-se que hoje, mais de 46% do *malware* implantado nos sistemas organizacionais venha de ataques de Engenharia Social como *phishing*, *Baiting*, actividades em rede social ou propagandas enganosas em sites falsificados (Baker et al, 2005).

4 Capítulo - Abordagem Metodológica

4.1 Enquadramento

Angola é um país Africano com uma economia emergente, elevado nível de pobreza, e os indicadores sociais mais baixos do mundo, onde 70% da população é analfabeta (CIA World Factbook, 2017).

Embora existam poucos relatos de ataques cibernéticos explorando vulnerabilidades humanas no país, não significa que ocorram com reduzida frequência, significa apenas que são pouco relatados devido a escassa informação sobre o assunto. Este motivo, levou-nos a recolher informações que identifiquem possíveis vulnerabilidades de segurança no comportamento dos colaboradores de uma das três empresas que operam no país no setor de transportes rodoviários, que levem a concretização de um ataque, e prever soluções de mitigação das mesmas.

4.2 Validade do Estudo

Para respondermos aos objetivos e questão de partida predefinidos, foi efetuado um inquérito através de questionários numa empresa de média dimensão do sector de transportes rodoviários Angolano, com filiais em todas as províncias. Optamos por direccionar a recolha de dados apenas ao escritório sede localizado na capital do país, porque por imperativos de tempo, técnico e financeiro, não foi possível deslocarmo-nos as demais províncias. A sede da empresa conta com um total de 210 colaboradores, dos quais 100 são técnicos e administrativos com acesso a computador ou sistema digital de dados.

Segundo Aaker et al. (2001), não existem procedimentos que garantam que os objectivos de um questionário (responder as questões feitas no início da pesquisa), sejam alcançados, uma vez que a natureza das pessoas é uma condição crítica, que influencia a interpretação dos resultados. Os inquiridos ou tentam adivinhar o motivo das questões para responder o que a pesquisa quer, ou respondem sem ter certeza, pois têm medo de não ter opinião (Galvão, 2013).

Este motivo, fez com que, de acordo com Carmo (2013), formulássemos as questões usando uma comunicação simples, sem ambiguidades e evitando:

- ➔ Perguntas que sugeriam a resposta;
- ➔ Perguntas com sentimento de aprovação ou reprovação;
- ➔ Necessidade do inquerido fazer cálculos para responder;
- ➔ Perguntas com alternativas longas;

- ➔ Mudanças bruscas de temas;
- ➔ Contágio de respostas;

As questões selecionadas para o questionário foram criadas de acordo com os objetivos, a questão de partida, e trabalhos similares já realizados por outros pesquisadores. Foi tido como exemplos os questionários usados por Matthew Spinapolice, com o tema “Mitigando o risco de ataques de Engenharia Social”, do mestrado em ciências de redes e administração do sistema - Instituto Rochester de Tecnologia (Spinapolice, 2011), e Bernard Oosterloo, com o tema “Gestão social e riscos de engenharia - tornar a Engenharia Social transparente”, da tese de mestrado em engenharia e gestão industrial (Oosterloo, 2008).

Ao longo do questionário procedeu-se ao rastreio das questões, apresentando-as de diferentes formas, de modo a distrair a atenção dos participantes do tópico real, para não influenciar as respostas (Hill& Hill, 1998) & (ExcelWorld, 2017). O termo "Engenharia Social" e “Segurança de Informação " foram várias vezes mencionados intencionalmente, pois verificamos no pré-teste, um total desconhecimento sobre o assunto.

As perguntas foram concebidas especificamente para averiguar:

1. O nível de conhecimento sobre segurança de informação, Engenharia Social e técnicas mais utilizadas.

2. A existência de políticas de segurança e planos de resposta a incidentes.

3. A existência de programas de formação em Segurança de Informação.

4. O comprometimento dos colaboradores com a protecção do Sistema de Informação.

Para garantir que o questionário cumprisse com o objectivo da pesquisa, foi realizado um pré-teste, através de entrevista aos directores dos recursos humanos e departamento de informática da empresa, para prever todos os problemas e/ou dúvidas que pudessem surgir durante a aplicação do mesmo (Mattar, 1994).

4.3 População e Amostra

Embora o mercado angolano conte com três empresas operando no sector de transportes públicos rodoviário, a definição do método de amostragem, foi baseado na conveniência ou intenção de estudar a empresa com maior dimensão, por possuir mais recursos materiais, financeiros e humanos para garantir os objectivos da pesquisa.

Não obstante tratar-se de um método não probabilístico, que não permite a generalização dos resultados obtidos, o mesmo garante uma análise estratégica da realidade da empresa, permitindo que os resultados obtidos, possam servir para identificar situações de risco, e apontar soluções para os problemas. No entanto, temos consciência que esta impossibilidade de generalizar os resultados, para além do contexto criado, constitui uma limitação da investigação.

4.3.1 Validade da amostra

Uma amostra válida é um subconjunto representativo da população alvo. A amostragem não probabilística de conveniência, permite obter respostas de pessoas que pertencem a grupos definidos (Kitchenham e Pfleeger, 2002a). Por isso foi seleccionado o grupo de colaboradores que respondia aos interesses do estudo.

A amostra em causa foi constituída por pessoal administrativos e técnico, composto por directores de áreas, recursos humanos e finanças, supervisores de turnos, secretárias, recepcionistas, e pessoal de TI. Obtivemos uma amostra aleatória de 80 participantes, escolhidos num universo de 100 colaboradores destas áreas, na sede da empresa. De acordo com a Tabela 5, a margem de erro e nível de confiança da nossa amostra reflectidos nos resultados obtidos é de 5% e 95% respectivamente.

Tabela 5 Margem de Erro e Nível de Confiança mais Utilizados em Pesquisas.

População	Margem de erro			Nível de confiança		
	10%	5%	1%	90%	95%	99%
100	50	80	99	74	80	88
500	81	218	476	176	218	286
1.000	88	278	906	215	278	400
10.000	96	370	4.900	264	370	623
100.000	96	383	8.763	270	383	660
1.000.000+	97	384	9.513	271	384	664

Fonte: (Adaptado de Surveymonkey, 2017).

Assim as amostras seleccionadas para a pesquisa foram:

a) Colaboradores administrativos, com acesso ao sistema informático da empresa.

b) Colaboradores técnico/operacionais, com ou sem acesso ao sistema informático da empresa, mas que manipulam ou tomam conhecimento de informações da empresa no decorrer de suas actividades laborais.

4.4 Aplicação de Questionários aos Colaboradores da Empresa.

Foi elaborado um questionário misto, com questões dicotómicas[6] e múltipla escolha, mas sempre respeitando a confidencialidade dos participantes. Foi concedido aos inqueridos, o tempo necessário para a leitura e compreensão das questões de modo a responderem adequadamente as mesmas. O questionário foi respondido exclusivamente por via presencial, com recurso ao documento impresso em folha de papel A_4, entre os dias 10 a 14 de Julho de 2017, tendo sido recolhidas 80 respostas completas.

O questionário que consubstancia o presente estudo foi composto por 50 perguntas e estruturado em cinco grupos de questões. Os primeiros dois grupos caracterizaram os dados demográficos e perfil dos participantes no estudo. O terceiro caracterizou as medidas de segurança existentes e implementadas na empresa. Por fim, o quarto e quinto caracterizaram o nível do conhecimento, opinião e atitude dos colaboradores face à Segurança de Informação e Engenharia Social.

Devido à escassez de tempo, não foi possível fazer entrevistas pessoais as chefias sobre o tema, embora saibamos que poderíamos ter obtido informações mais valiosas fazendo-as.

O primeiro dado apurado no questionário tem a ver com o nível de escolaridade do nosso alvo.

Tabela 6 Dados Demográficos.

Dados demográficos				
Nível acadêmico do colaborador	**Ensino médio incompleto**	**Ensino médio completo**	**Superior incompleto**	**Superior completo**
	25%	44%	17%	14%

A caracterização dos participantes do estudo revelou que cerca de 25% dos colaboradores têm o ensino médio incompleto, 44% o ensino médio concluído, 17% frequentam o ensino superior, e apenas 14% têm o ensino superior concluído (mostrado no gráfico 1). Essa informação revela

[6]Questões com caráter bipolar, do tipo sim/não; concordo/ não concordo; gosto/não gosto. Por vezes, uma terceira alternativa é oferecida, indicando desconhecimento ou falta de opinião sobre o assunto.

que deve haver um especial cuidado na adequação das políticas, normas e procedimentos de segurança da empresa.

Gráfico 1 Dados Demográficos.

Os dados da tabela 7 têm a ver com procedimentos que envolvem o colaborador.

Tabela 7 Procedimentos que Envolvem o Colaborador.

Sobre o Colaborador				
Já teve acesso as políticas de segurança da informação?	**Sim, quando assinei o contrato de trabalho**	**Tenho acesso periodicamente**	**Está sempre disponível**	**Nunca tive acesso**
	28%	9%	0%	62%
Assinou algum termo de responsabilidade e/ou confidencialidade sobre as informações da empresa?	**Sim**	**Não**		
	15%	85%		
Qual a área mais vulnerável do sistema de informação?	**Fator Humano**	**Hardware/Software**		
	11%	89%		
Existe algum procedimento para uso de telemoveis e tablets na empresa?	**Sim**	**Não**		
	19%	81%		

Verificamos que 28% dos colaboradores afirmaram terem lido as políticas de segurança de informação quando assinaram o contrato de trabalho, e 9% ter acesso a ela periodicamente. Segundo o departamento de informática da empresa, as políticas de segurança não são dadas a conhecer aos colaboradores sendo as restrições de segurança, directamente aplicadas no sistema impedindo-os de executarem ações que não tenham a ver com suas atividades laborais. O que

confirma a margem de 62% que afirmou nunca ter tido conhecimento de nenhuma política, ao contrário do que seria desejável.

No gráfico 2, vimos que a opinião dos inquiridos sobre o lado mais vulnerável do sistema de informação, foi de 75% para o hardware/software, deixando o fator humano em segundo plano. Pode-se considerar que a falta de conhecimento da real importância do fator humano para o sistema de segurança, propiciou essa margem de respostas.

Gráfico 2 Informações Sobre o Colaborador.

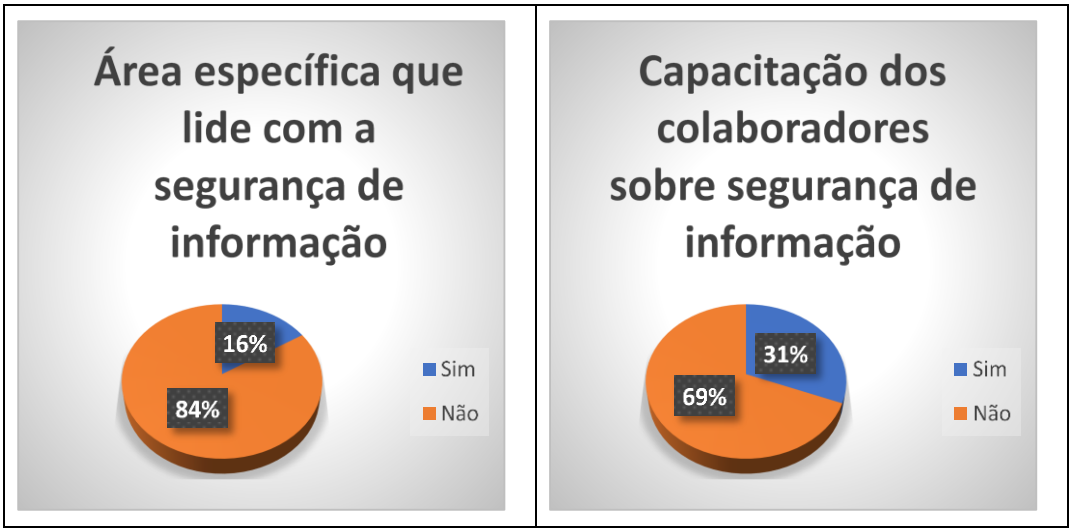
Os dados apurados na tabela 8 têm a ver com os procedimentos de segurança da empresa.

Tabela 8 Procedimentos de Segurança da Empresa.

SOBRE A EMPRESA			
A empresa disponibiliza informação sobre a classificação da informação?	**Sim**	**Não**	
	38%	63%	
Existe alguma estrutura que responde aos incidentes de segurança?	**Sim**	**Não**	
	19%	81%	
Existem critérios para descarte da informação?	**Sim**	**Não**	
	6%	94%	
É feita alguma capacitação dos colaboradores sobre segurança da informação?	**Sim**	**Não**	
	31%	69%	
Existe uma área específica que lide com a segurança da informação ?	**Sim**	**Não**	
	16%	84%	

Embora 31% dos colaboradores afirmaram que a empresa os capacita sobre questões ligadas a segurança de informação, 69% garante nunca ter recebido nenhuma informação do gênero. Cerca de 16% afirma existir uma área específica que lida com a segurança de informação, e 84% garante que esta área não existe (gráfico 3).

Gráfico 3 Segurança da Empresa.



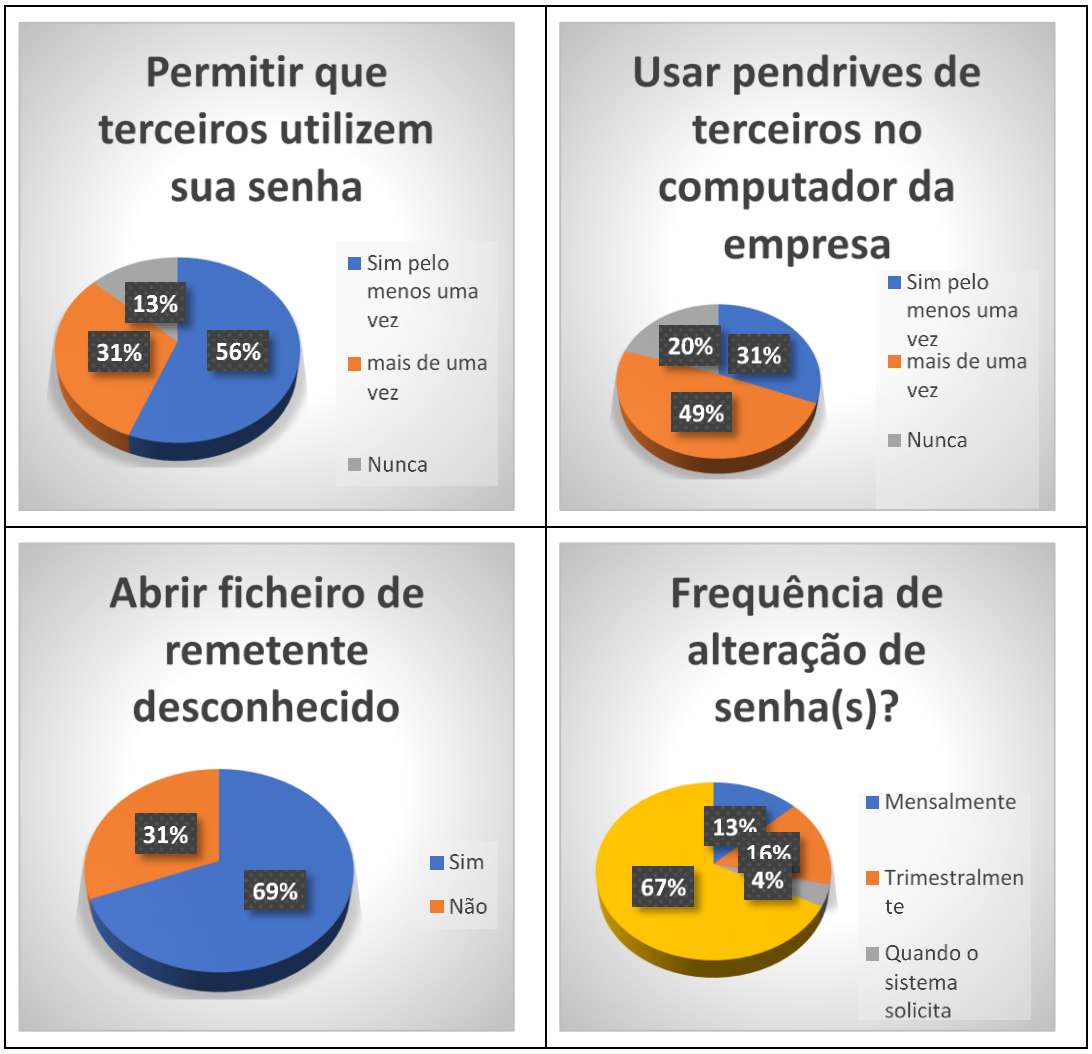
Os dados apurados na tabela 9 têm a ver com a segurança de informação.

Tabela 9 Segurança de Informação.

SEGURANÇA DE INFORMAÇÃO				
Já permitiu que outras pessoas utilizassem sua senha?	**Sim pelo menos uma vez**	**Sim, mais de uma vez**	**Nunca**	
	56%	31%	13%	
Já usou pendrives de terceiros no computador da empresa?	**Sim pelo menos uma vez**	**Sim, mais de uma vez**	**Nunca**	
	31%	49%	20%	
Já abriu algum ficheiro de email de remetente desconhecido?	**Sim**	**Não**		
	69%	31%		
Com que frequência você altera sua(s) senha(s)?	**Mensalmente**	**Trimestralmente**	**Quando o sistema solicita**	**Nunca**
	13%	16%	4%	67%

Cerca de 56% dos colaboradores admite ter cedido sua senha a um colega, chefe ou suporte técnico. 44% admitem já ter conectado pendrives ou outro dispositivo USB de terceiros em computadores da empresa, e ainda 69% reconhecem já ter aberto algum ficheiro de remetente desconhecido. Quanto a alteração de senhas, 67% afirmou nunca ter trocado a sua senha se acesso ao sistema.

Gráfico 4 Segurança de Informação.



Os dados apurados na tabela 10, têm a ver com a Engenharia Social.

Tabela 10 Engenharia Social e Técnicas de Ataque.

ENGENHARIA SOCIAL		
Já ouviu falar em Engenharia Social?	**Já ouvi falar**	**Nunca ouvi falar**
	34%	66%
Conhece alguma medida de prevenção contra Engenharia Social?	**Sim**	**Não**
	6%	94%
Sabe verificar as informações de autenticação nos certificados de segurança dos sites?	**Sim**	**Não**
	5%	95%
Conhece que informações são vitais para o negócio da empresa?	**Sim**	**Não**
	18%	82%
Se sente responsável pela segurança de informação da empresa?	**Sim**	**Não**
	21%	79%

Em relação a Engenharia Social e suas técnicas (gráfico 5), o estudo revelou que 66% nunca ouviu falar no termo, e 94% desconhecem as existência de medidas preventivas contra este tipo de ataques. Verificamos que a maioria dos inquiridos, mesmo os que trabalham com TI demonstraram pouco conhecimento sobre o tema. Quanto a proteção das informações da empresa, 79% dos inqueridos revelou que apenas é responsável pelo seu trabalho, e apenas 21% considera importante garantir esta proteção (gráfico 4).

Gráfico 5 Medidas Preventivas Contra Ataques de Engenharia Social.

Mesmo usando TI como vector de operação do negócio, a empresa não tem um plano de investimento na formação e consciencialização dos colaboradores, e os procedimentos de segurança implementados apenas contemplam o uso de firewalls, anti-vírus, sistemas de identificação e detenção de intrusos, ignorando as ameaças provenientes da imprudência ou desconhecimento dos próprios colaboradores.

Constatamos que os utilizadores não sabem analisar os indicadores de segurança na "*Web explorers*" nem verificar informações de autenticação dos certificados de segurança dos sites, (facto compreensível, uma vez que nunca foram informados nem orientados a este respeito).

A partir destes resultados, identificamos a lista de vulnerabilidades descritos na tabela 11, que utilizaremos como ponto de partida para propor um conjunto de boas práticas que englobem a criação de políticas adequadas, bem como, programas de educação e formação permanente dos colaboradores, plano de resposta a incidentes e aplicação de medidas de punição.

Tabela 11 Lista de Vulnerabilidades.

Questões Selecionadas no Questionário Tendo em Conta os Objetivos Traçados	Filtro de Dados Estatísticos
Nível Acadêmico do Colaborador.	69% dos colaboradores têm um nível de escolaridade abaixo do ensino superior.
Acesso as políticas de segurança de informação.	64% nunca tiveram acesso.
Vulnerabilidades do sistema de informação da empresa.	89% considera o Hardware/Software os principais perigos a segurança de informação.
Uso de telemoveis e tablets para trabalho na empresa.	81% utilizam dispositivos pessoais em serviço sem uso de controle de acessos.
Informação sobre a classificação da informação.	63% dos que lidam com as informações da empresa desconhecem a sua classificação.
Estrutura que responde aos incidentes de segurança.	81% desconhece existir nenhuma estrutura que responde aos incidentes de segurança.
Capacitação sobre segurança de informação.	69% nunca recebeu nenhuma capacitação sobre o assunto.
Ceder a terceiros a senha de acesso ao sistema.	87% já cederam.
Uso de pendrives de terceiros no computador da empresa.	80% já utilizaram.
Abrir email de remetente desconhecido no computador da empresa.	69% já abriram.
Alteração de senhas.	67% utilizam sempre a mesma senha.
Engenharia Social.	66% nunca ouviram falar.
Prevenção contra Engenharia Social.	94% desconhecem.
Verificar informações de autenticação de segurança dos sites.	95% desconhecem.
Responsabilidade pela segurança de informação da empresa.	79% acredita não fazer parte de suas atribuições garantir esta segurança.

4.4.1 Práticas a Propor

Depois de identificadas as principais vulnerabilidades comportamentais nos colaboradores da empresa, propomos como solução, a implementação de quatro níveis de contramedidas. O primeiro, visa a criação de políticas e procedimentos de segurança contra ataques a segurança de informação com realce para Engenharia Social. O segundo, a educação, formação e consciencialização dos colaboradores em questões de segurança. O terceiro, para ataques técnicos onde os colaboradores sejam o alvo principal. E por último, a criação de um plano de resposta a incidentes de segurança, e medidas de punição que desencorajem a pratica de atos ilícitos.

5 Capítulo - Análise e Discussão de Resultados

Com o objetivo de responder as vulnerabilidades identificadas no capítulo anterior, propomos a implementação das seguintes contramedidas:

- ➔ Projetar uma política de segurança que leve em conta o nível intelectual, cultural e social dos colaboradores da empresa.
- ➔ Desenvolver um programa de educação, formação e consciencialização em segurança, que torne os utilizadores conscientes do importante papel que desempenham na segurança da informação da empresa.
- ➔ Adotar e implementar soluções que criem uma barreira lógica contra ataques efetuados por meios eletrônicos.
- ➔ Criar um plano de resposta a incidentes de segurança, que identifique e reaja rapidamente a um ataque ou tentativa de ataque, prevendo medidas punitivas que desincentivem a prática ou colaboração em tais crimes.

5.1.1 Primeira Etapa - Concepção da Política de Segurança Certa

Políticas são regras que orientam o comportamento dos colaboradores de como proteger os sistemas de informação e as informações sensíveis. Elas devem basear-se em normas e procedimentos padrão, mas também devem estar adequadas a realidade e necessidades de cada empresa (Barman, 2001). A criação e implementação da política, deverá ser precedida e acompanhada por campanhas de consciencialização e educação sobre a política de segurança e procedimentos a adotar no decorrer das atividades laborais.

Política de Segurança é definida por Bosworth & Kabay (2002), como "*As regras e regulamentos estabelecidos pela organização, em conformidade com a legislação aplicável, regulamentos da indústria e decisões dos líderes da empresa".*

Tendo em conta o nível acadêmico e intelectual da maioria dos colaboradores da empresa, a política criada deverá ser fácil de ler, interpretar e aceder. Deve-se evitar palavras complexas e de significado ambíguo. As regras e processos devem ser bem detalhados e se possível ilustrados, para evitar diferentes interpretações de diferentes leitores (Blank & Gallagher, 2013). Isto significa que a política deverá poder ser lida e percebida por todos colaboradores nos vários níveis da organização, não só pelo pessoal administrativo ou de TI.

5.1.1.1 Defesa a Nível de Políticas

Segundo Peixoto (2006), "*a consciencialização deverá ser combinada à política de segurança, e complementada com educação dos utilizadores. Uma política de segurança desatualizada ou surrealista leva os utilizadores a burlá-la.*".

As práticas recomendadas de segurança de informação exigem que uma organização tenha uma política formal e sólida para o pessoal. Para Bosworth & Kabay (2002), algumas sugestões incluem:

- ➔ Implementar uma política de "privilégios mínimos" para proteger os utilizadores de ataques. É importante que os colaboradores tenham consciência disso, para não gerar insatisfações que aumentem o risco de ataques associado a colaboradores descontentes.
- ➔ Implementar o uso de scripts para cada fluxo de informações quando os colaboradores estão se comunicando por telefone/e-mail.
- ➔ Sempre que possível usar a autenticação de dois fatores, isso tem como vantagem evitar que o roubo de credenciais tenha efeitos muito danosos.
- ➔ Classificar a informação consoante a sua importância e a informação considerada sensível, deverá ter procedimentos de tratamento que imponham maiores requisitos de segurança.
- ➔ Identificar algum responsável para lidar com as tentativas de Engenharia Social. Isso fará com que os colaboradores se tornem mais proactivos na defesa da organização.

5.1.1.2 Gestão de Senhas

Deve-se desenvolver na empresa uma política de mudança frequente de senhas, e educar os colaboradores a nunca darem suas senhas ou outras informações confidenciais. Deve-se força-los a criarem senhas fortes e a usa-las conscientemente, alterando-as periodicamente, e não digitá-las na presença de outras pessoas (Baldim, 2007).

As senhas aleatórias são facilmente esquecidas, e quando armazenadas, geralmente são guardadas em lugar vulnerável. As datas significativas, nomes dos animais de estimação, números de telemóvel, nomes do membro da família, podem ser descobertos muito rapidamente. As possibilidades alternativas incluem:

- ➔ Combinar nomes dos personagens de filmes, livros ou televisão não relacionados;
- ➔ Usar parte de uma citação popular;
- ➔ Combinar palavras, nomes, números e datas significativas, não relacionadas entre si;

➔ Escrever intencionalmente errada uma palavra aleatória.

5.1.1.3 Senhas como Fator de Autenticação

As senhas ainda são e continuarão a ser por bastante tempo uma peça importante na segurança dos sistemas de TI. No entanto, elas podem ser uma faca de dois gumes como fator de autenticação no contexto em que é muito fácil comprometê-las (Martins, 2013).

Uma questão relevante a ter em conta, é a necessidade de usar senhas diferentes para cada provedor de serviços. Memorizar senhas para todas as contas dos diferentes prestadores de serviços, é uma tarefa difícil do ponto vista psicológico. Por este motivo, muitos utilizadores optam por ignorar esta prática de segurança.

Vale ressaltar que, o roubo de senhas é muitas vezes a principal finalidade de um ataque SE, por isso, substituí-las por um mecanismo alternativo não propenso a roubo, aliviaria automaticamente a pressão sobre os seres humanos em preservar a confidencialidade dos seus fatores de autenticação.

5.1.2 Autenticação Biométrica

O uso de características biológicas físicas para identificação e autenticação dos utilizadores dos sistemas reduz esse problema, já que características pessoais como impressão digital, geometria da mão e padrão ocular, não podem ser roubadas, mas esta solução requer um alto investimento na aquisição de equipamentos de autenticação telebiométricos (TAO), como leitores e câmaras, que façam a leitura das caraterísticas físicas das pessoas (Griffin, 2016). Estes dispositivos alem de caros, podem ser enganados por programas que simulam estas características.

Sobre isso, há uma pesquisa interessante sobre o uso de "*hacking* leitores de impressão digital mestre" para enganar leitores biométricos. A pesquisa mostra que estes programas são capazes de abrir cerca de dois terços dos iPhones com essas impressões mestre, (Schneier, 2017b).

Uma alternativa ao uso da biometria física ou convencional, é a biometria comportamental, que usa algoritmos de Análise de Componentes Principais (PCA) e Análise de Discriminação Linear (LDA) no tratamento das caraterísticas comportamentais como timbre de voz, escrita à mão, assinatura, dinâmica da digitação, e outras, para identificar um indivíduo (Schwartz, 2016) & (Gavrilova, 2014). Esta abordagem é mais barata, eficiente e simples de implementar, pois usa algoritmos comportamentais e linguagem máquina para autenticar um utilizador.

5.1.2.1 Combinação de Dois Fatores de Autenticação (2FA)

A adoção de métodos de autenticação biométricos, ainda apresenta muitas questões não triviais, como é o caso de fatores biométricos poderem mudar para num indivíduo e causar a rejeição de um utilizador autorizado. Uma alternativa para este problema é a adoção do sistema biométrico multimodal que incorpora dois ou mais traços biométricos do individuo aumentando a taxa de reconhecimento do sistema. Isso permanece verdadeiro mesmo na presença de dados errados, incompletos ou ausentes (Nicholson, 2016).

É aconselhável que mais de uma técnica de autenticação sejam combinadas para aumentar a segurança dos sistemas. A combinação de técnicas biométricas multimodais com métodos de autenticação tradicionais (cartões com chips e senhas), é chamada autenticação multi-fator ou em vários níveis, e garantem um nível de segurança mais eficiente, pois autentica o utilizador pelo que sabe (palavra-chave), pelo que têm (dispositivo ou certificado) e pelo que é (características biológicas, físicas e comportamentais) (Martins, 2013) & (Nicholson, 2016).

Um grande número de sistemas multimodais tem sido desenvolvido para encontrar a melhor combinação de características biométricas que minimize erros de reconhecimento. O PCA e LDA já têm sido utilizados no reconhecimento visual e análise de características principais, permitindo que a combinação de aprendizagem de máquinas e sistemas multimodais reduzam a incidência de intrusos no sistema. (Gavrilova, 2014), (Nicholson, 2016) & (Schwartz, 2016).

Investir na adoção e implementação desta forma de autenticação na empresa poderá ser uma medida de segurança aceitável pois reduziria consideravelmente os índices de violações de segurança causados por perdas, roubos ou cedência intencionais de dados de autenticação por parte dos colaboradores.

5.2 Segunda Etapa - Consciencialização e Formação do Colaborador

Para Sêmola (2003), "*O ser humano é uma máquina complexa, dotada de iniciativa, criatividade e que sofre interferência de fatores externos, provocando comportamentos imprevisíveis".*

Partindo deste ponto de vista, a ideia será incutir a consciência de segurança nos colaboradores como ferramenta contra ataques de Engenharia Social. O objetivo será torna-los conscientes das técnicas utilizadas pelos atacantes, e mais importante, convencê-los de que a segurança da informação é parte de seu papel na empresa.

5.2.1 Educação e Consciencialização

Uma tática defensiva muito sugerida em ataques de Engenharia Social, é garantir que todos os colaboradores, independente das suas funções recebam instruções em reconhecer e lidar com este tipo de ataques. Atenção especial deve ser dada às redes sociais (tendo em conta a sua prevalência), uma vez que, os utilizadores não percebem a quantidade de informações confidenciais que compartilham publicamente, identificando-os como colaboradores da organização.

Outra medida relevante é estratificar os colaboradores consoante o nível hierárquico e intelectual (Kee, 2008). Sendo os dirigentes o grupo-alvo prioritário do engenheiro social, devem estar muito conscientes das consequências para a empresa de um ataque de Engenharia Social bem-sucedido.

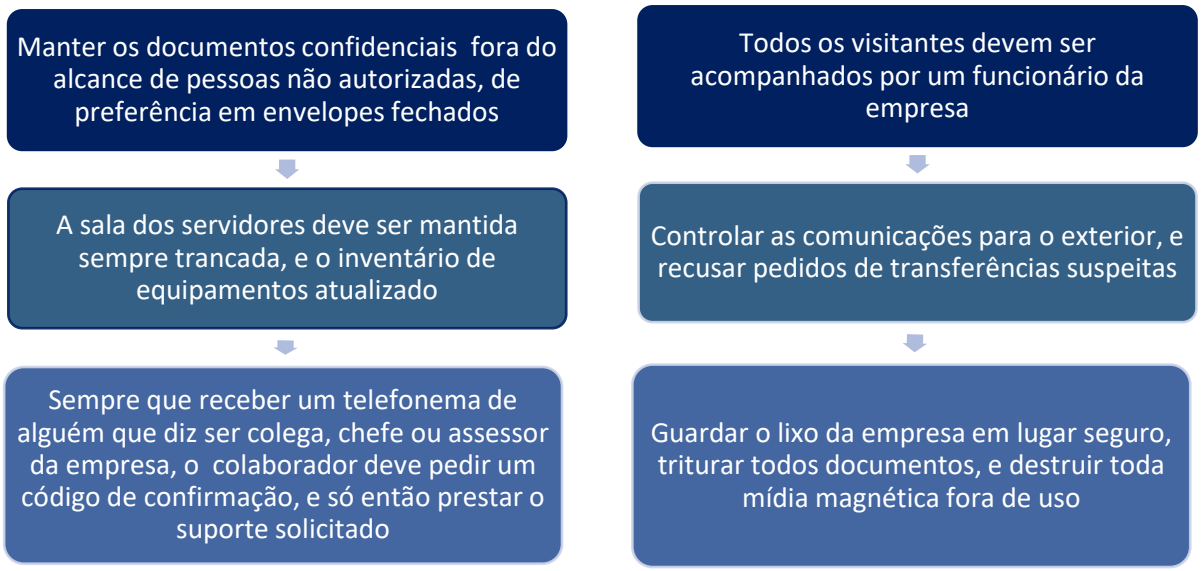
5.2.2 Formação em Técnicas de Engenharia Social

O primeiro a garantir neste programa de formação é que todos na organização percebam o valor das informações da empresa. Todos colaboradores devem ser instruídos sobre quais informações precisam ser protegidas e como protegê-las (Alves, 2007).

A formação deve abranger toda a empresa desde diretores, gerentes, supervisores, técnicos e demais colaboradores, todos deverão ser treinados. Também deverão ser explicadas as táticas mais comuns de ataques e formas de prevenção. Deve ser orientado que sempre que se perceber algum sinal de ataque, os demais colegas devem ser logo alertados.

Na figura 15 estão expostas algumas estratégias de prevenção que poderão ser adotadas:

Figura 15 Estratégias de Prevenção Contra Ataques SE.



Fonte: (Adaptado de Alves ,2007)

Para Baldim (2007), *"um programa de formação bem-sucedido, passa por perceber a razão da vulnerabilidade das pessoas, identificando seus pontos fracos*". Um fator de motivação para os colaboradores, é fazer com que saibam o quanto sua colaboração beneficiará a empresa, e que o contrário também é verdadeiro. Isso faz com que sintam a responsabilidade pelo sucesso ou fracasso da empresa.

O programa deve criar neles a consciência de que a empresa pode estar sob ataque a qualquer momento, e em consequência disso os seus empregos se encontram em risco.

De acordo com Mitnick & Simon (2002), um programa que vise a segurança de informações e contenha também aspetos do comportamento humano deve incluir:

- ➔ Como reconhecer um ataque de Engenharia Social;
- ➔ Relato das tentativas de SE e os ataques bem-sucedidos;
- ➔ Procedimentos para lidar com uma solicitação suspeita;
- ➔ Instruir cada colaborador a criar uma senha difícil de adivinhar;
- ➔ Conhecer o sistema de classificação das informações e as principais políticas de segurança;
- ➔ Questionar todos que fazem uma solicitação suspeita, independente da importância que a pessoa alegar ter;
- ➔ Uma descrição do "*modus operandi*" dos atacantes e métodos usados para atingir seus objetivos;

- ➔ Verificar a identidade e autoridade de quem faça uma solicitação;
- ➔ Não confiar em terceiros sem uma verificação adequada. Isso significa nunca dar o benefício da dúvida;
- ➔ Obrigar todo colaborador a cumprir às regras e implementar consequências ao não-cumprimento.

A criação deste programa, deverá ser sedimentado com a construção de uma cultura de segurança. A este respeito, Sêmola (2003) apresenta algumas propostas de medidas a adotar:

Seminários: Realizar seminários abertos que divulguem os riscos associados às atividades da empresa, e o impacto para o negócio se alguma ameaça se concretizar.

Campanha e Divulgação: Dar à conhecer a todos, as diretrizes, normas, procedimentos e instruções, apresentando-os a cada grupo com perfil de atividade semelhante. Assim, cada colaborador perceberá suas responsabilidades dentro do modelo de segurança, motivando-o a colaborar.

Envolvimento do Diretor da Empresa: É conveniente que o Diretor, Presidente, CEO ou CIO manifeste oficialmente seu envolvimento no processo, através de um documento disponibilizado ou encaminhado a cada colaborador, dando caráter formal ao procedimento.

Termo de Responsabilidade e Confidencialidade: Serve para formalizar o compromisso do colaborador diante de suas responsabilidades com à proteção das informações que manipula. Além disso, este termo se encarrega de divulgar as punições cabíveis por desvios de conduta, e esclarecer que a empresa é a legítima proprietária dos ativos de informação temporariamente custodiadas pelas pessoas.

Cursos de Capacitação e Certificação: Uma motivação para que o colaborador aplique as medidas de segurança, é por exemplo, promover certificados pela conclusão e acompanhamento dos programas de formação, e dar brindes ou prêmios ao colaborador por ajudar a diminuir os ataques sofridos, ou por evita-los.

Para Peixoto (2006), é importante fazer com que o colaborador assine algum termo de comprometimento quanto ao seguimento das políticas e princípios de segurança ministrados pelo programa. Geralmente quando as pessoas assinam algo, as chances de se esforçarem para cumprir os procedimentos aumentam.

5.3 Terceira Etapa - Defesas Técnicas

5.3.1 Soluções de Segurança de E-mail

Sendo o *phishing* de e-mail o vetor de ataque mais comum em Engenharia Social, apontaremos algumas soluções eficazes que permitem fazer a autenticação dos e-mails recebidos. Existem pelo menos três soluções técnicas que podem ser adotadas pela empresa para fornecer autenticação e segurança nas comunicações de e-mails, são elas:

- ➔ Padrão OpenPGP para cifrar e assinar mensagens (Callas,2007).
- ➔ Protocolo S/MIME com tratamento de chaves públicas (Ramsdell, 2010).
- ➔ Protocolos SPF / DKIM / DMARC, baseados em DNS (Kucherawy, 2015).

O OpenPGP é um programa que cifra e decifra dados fim-à-fim usando um padrão aberto baseado no PGP[7]. A cifra de chave pública fornece autenticação e privacidade criptográfica em comunicações de mensagens de e-mail. Cada utilizador gera no seu computador um par de chaves pública e privada. A pública é distribuída livremente e permite que o utilizador cifre seus dados e só quem possuir a chave privada correspondente poderá decifrar.

A chave privada além de decifrar, também assina os dados. Quando uma mensagem é assinada com uma chave privada, a chave pública correspondente pode verificar se o remetente é verdadeiro e se o conteúdo não foi adulterado depois de assinado.

Apesar de sólido, este padrão é mais direcionado para indivíduos, e não para organizações, uma vez que, a tarefa de verificar a autenticidade dos remetentes ou da chave pública do emissor é do utilizador e não de uma autoridade central que lida com a PKI[8] (Green, 2014). A solução não deixa de ser uma opção válida, uma vez que os emails são sempre direcionados a indivíduos, neste caso, aos colaboradores da empresa.

O protocolo S/MIME *(Secure/Multipurpose Internet Mail Extensions)* é semelhante em *design* e objetivos ao padrão OpenPGP, mas utiliza o modelo de confiança dos certificados X.509, usados em conexões TLS[9] . Isso traz como vantagem a integração com PKI, fazendo com que

[7]O PGP é muito utilizado para assinatura, cifra e decifra de textos, e-mails, arquivos, diretórios e partições inteiras de disco e segurança de comunicações via e-mail.

8PKI (Infraestrutura de Chaves Públicas), é um órgão público ou privado que emite chaves públicas, baseando-se no princípio da terceira parte confiável, oferecendo uma mediação de credibilidade e confiança em transações entre partes que utilizam certificados digitais.

[9]TLS (Transport Layer Security), assim como o seu antecessor *Secure Sockets Layer* (*SSL*),é um protocolo de segurança desenvolvido pela *IETF TLS Working Group*, para proteger as telecomunicações via internet em serviços de e-mail (SMTP), navegação por páginas (HTTPS) e outros tipos de transferência de dados.

seja mais usado em empresas que o OpenPGP. O protocolo é usado para o envio de mensagens de email assinadas e cifradas digitalmente, fazendo com que a pessoa que recebe a mensagem tenha a certeza que o que está em sua caixa de entrada é a mensagem exata que partiu do remetente, e que o remetente é quem diz ser, e não um impostor (Ramsdell, 2010).

Os protocolos SPF, DKIM e DMARC, garantem a autenticação dos utilizadores de um domínio usando o DNS[10]. É um método apropriado para empresas com várias filiais espalhadas geograficamente como é o nosso estudo de caso.

O SPF (Sender Policy Framework) define um formato de registros TXT de DNS para o domínio da empresa e cria uma lista de endereços IP autorizados a enviar e-mails para aquele nome de domínio. O servidor de e-mail verifica a presença de registros DNS no domínio do remetente e rejeita e-mails que são enviados de endereços não autorizados.

O DKIM (*Domain Keys Identified Mail*) é um protocolo que autentica as partes envolvidas numa comunicação, inserindo um cabeçalho na mensagem de e-mail, com uma assinatura cifrada do conteúdo do e-mail. A parte receptora recupera a chave pública correspondente através de registros TXT de DNS e verifica a assinatura (Kucherawy, 2015).

Antes da mensagem ser enviada o DKIM cria uma assinatura digital única para cada corpo e cabeçalho da mesma. Ao receber o e-mail, o servidor de destino pesquisa o DNS do domínio do remetente e verifica se no campo "De", a assinatura DKIM está configurada. Se sim, ele recebe a chave pública do domínio e a usa para decifrar a assinatura do cabeçalho e corpo da mensagem do e-mail.

O DMARC é um protocolo de normatização que garante a autenticidade de e-mails, adotado por empresas como a Google e Microsoft. Ele baseia-se no DKIM, mas agrega a função de relatórios que permite supervisionar o comportamento dos e-mails (Kucherawy, 2015) & (Steve, 2016).

Uma questão importante nas três propostas é a necessidade da organização convencer as organizações com as quais tem regular comunicação, a adotar as mesmas soluções de segurança, pois assumindo uma implementação completa e correta dessas tecnologias, o aspeto técnico do *phishing* pode ser atenuado (Steve, 2016) & (Crocker & Zink, 2008).

[10]DNS (Domain Name System) é um sistema de gestão de nomes hierárquico distribuídos a computadores, serviços ou qualquer recurso conectado à internet ou rede privada. O servidor DNS resolve nomes para os endereços IP e endereços IP para nomes respetivos, permitindo a localização de hosts num determinado domínio.

5.3.1.1 Soluções Anti-Phishing

Além das propostas acima apresentadas, o mercado hoje oferece várias tecnologias que detectam tentativas de phishing e advertem o utilizador. A pesquisa de Calvin Ardi e John Heidemann (2016), com o tema "Detecção Personalizada de Phishing Baseada em Conteúdo", desenvolvida no Instituto de Ciências da Informação (USC), apresenta algumas sugestões que poderão ser adotadas:

- ➔ *Carnegie Mellon Anti-phishing* é uma ferramenta de análise de rede (CANTINA[11]). Esta ferramenta detecta com sucesso 95% dos sites de *phishing* combinando a análise DOM[12]com os resultados dos motores de busca para detectar sites de *phishing*.
- ➔ *CodeShield* usa uma *Whitelist* de Aplicação Personalizada (*PAW*) para bloquear automaticamente sites que não estejam na lista de permissões.
- ➔ Alerta de senha do Google é uma extensão do navegador que detecta quando um utilizador insere as credenciais da conta do Google em outro site e o avisa para alterar imediatamente a senha do Google.
- ➔ *AuntieTuna* é um navegador *Web Plug-in* que usa a personalização e algoritmos de detecção para decidir se uma página é ou não uma tentativa de *phishing*.

5.3.1.1.1 Simulações de Phishing

A "simulação de *phishing*" é hoje muito usada para mitigar estas ameaças. A abordagem consiste em realizar um ataque de phishing a um grupo de colaboradores num ambiente controlado e fornecer feedback aos participantes, com base no desempenho pessoal. A técnica inclui inicialmente educação e recomendações de atenção contínua neste sentido aos participantes (Phishme, 2015). Estas simulações devem ser repetidas periodicamente, até que seja fácil para os colaboradores identificá-las.

5.3.2 Auditorias e Testes de Invasão

Para Randell (2013),"*as formações e campanhas de consciencialização têm tendência a falhar se não houver supervisão*". Esta medida de defesa visa a realização periódica de auditorias externas e testes com vetores de ataque de Engenharia Social. Estes testes beneficiam a

[11]CANTINA analisa assinaturas com base no ranking mais alto do conteúdo da página através de mecanismos de busca e assume que o conteúdo válido será o que for altamente classificado nos resultados.

[12]O DOM (Modelo de Objeto de Documento) é uma convenção multiplataforma independente de linguagem para representação e interação com objetos em documentos HTML, XHTML e XML, onde os nós de cada documento são organizados em uma estrutura de árvore, chamada árvore DOM.

organização, dando uma visão geral das vulnerabilidades existentes, para ajudar a direção a implementar um plano de soluções adequadas a organização, e alcançar um nível de segurança aceitável.

5.4 Quarta Etapa - Resposta a Incidentes

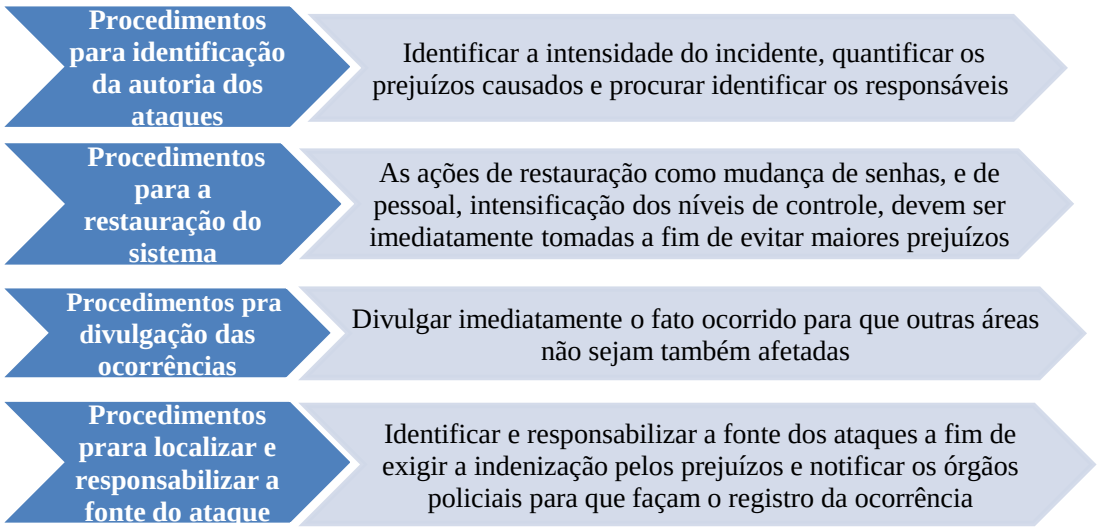
Mesmo tomando todas as precauções cabíveis, ainda existe a chance de que um incidente de segurança ocorra, pelo que, a organização deverá ter meios para responder a esse evento. A rapidez com que a organização reconhece, analisa e responde a um incidente de segurança, pode minimizar os estragos e diminuir as perdas.

O plano de resposta a incidentes é um documento que descreve as diretrizes gerais e procedimentos para tratamento dos principais incidentes de segurança que podem ocorrer na organização, dando ao pessoal técnico suporte e instruções sobre as medidas a adotar para a rápida resolução dos mesmos (Blank & Gallagher, 2013).

O tipo de tratamento dado aos incidentes de segurança varia de acordo com a sua intensidade e risco. As ações pertinentes podem envolver a intervenção de entidades externas (como parceiros, provedores de serviços, etc) ou mesmo órgãos policiais.

Para Medeiros (2001), os principais pontos a considerar num plano de resposta a incidentes são os mencionados na figura 16:

Figura 16 Elaboração de um Plano de Resposta a Incidentes.



Fonte: (Adaptado de Medeiros, 2001)

5.4.1 Punições para Crimes de Engenharia Social

A Engenharia Social é uma prática sustentada no roubo de informações com ou sem o uso de dispositivos eletrónicos no processo, o que torna difícil a sua descoberta e enquadramento legal. A maioria das organizações que sofreram ataques dessa natureza nem desconfiam que suas informações foram expostas, e as que tomam consciência dos ataques optam por não divulga-los publicamente para não expor suas falhas de segurança.

Em Angola não são conhecidos relatos oficiais da ocorrência de crimes de Engenharia Social, nem existe um ordenamento jurídico-penal relacionado a crimes desta natureza, apesar de haver legislações que permitem tipificar algumas condutas ilícitas inerentes a estas práticas criminosas, nomeadamente:

- ➔ Constituição da República de Angola;
- ➔ Código Penal Angolano;
- ➔ Lei nº 22/11, de 17 de junho, Lei da proteção de dados pessoais.
- ➔ Lei nº 23/11, de 20 de julho, Lei das Comunicações Eletrónicas e dos Serviços da Sociedade da Informação;
- ➔ Decreto presidencial nº225/11 de 15 de agosto, o regulamento geral das comunicações eletrónicas;
- ➔ Decreto presidencial nº 202/11 de 22 de julho, o regulamento das tecnologias e dos serviços da sociedade de informação;
- ➔ Lei nº71/11 de 12 de setembro, livro branco das tecnologias de informação e comunicação- "Angola rumo a sociedade da informação e do conhecimento";
- ➔ Lei nº244/12 de 6 de dezembro, Estatuto orgânico do Ministério das telecomunicações e tecnologias de informação;
- ➔ Lei nº 27/17, de 16 de fevereiro, Lei de proteção das redes e sistemas informáticos.

Estas leis versam sobre crimes como a falsidade e a sabotagem informáticas, danos relativos a dados ou programas, acesso ilegítimo a sistemas ou redes, viciação ou destruição dos dados pessoais, dano utilizando um meio informático, interceção ilegítima e reprodução de programas, mas não existem regras específicas no que toca aos crimes cibernéticos, matéria que dada a sua complexidade e especificidade merece pelo legislador um tratamento em diploma autónomo.

A lei Angolana para Proteção das Redes e Sistemas Informáticos, define como roubo informático qualquer apropriação indevida de uma rede, sistema informático, base de dados,

equipamento ou programa informático, usando a violência, ameaça, e acesso ilegítimo, com vista a estruturação incorreta de programa ou sistema informático (Lei de Proteção das Redes e Sistemas Informáticos, 2017).

Nesta lei apenas são previstas situações em que a apropriação indevida seja feita de forma explicita (pelo uso da força), mas nada está previsto sobre a cedência consciente ou inconscientemente dos mesmos por parte do utilizador autorizado sob a influência de manipulação, persuasão ou má fé do atacante.

Como exemplo, podemos destacar atos que nem sequer são considerados crimes, como a manipulação psicológica de funcionários para obtenção de informações classificadas, olhar informações expostas sobre mesas ou écrans, vasculhar o lixo da empresa em lugar público, e outros delitos cometidos para a obtenção de informações que posteriormente servirão para concretização do ataque.

No entanto a nível local, a empresa deverá criar mecanismos sancionatórios que desincentivem a participação ou conivência dos colaboradores neste tipo de atos, implementando medidas que vão desde a advertência e censura registada à demissão do colaborador.

6 Conclusão e Recomendações

Com base na bibliografia de referência utilizada, observou-se que a maioria das empresas acredita que a solução, unicamente técnica garante a segurança dos sistemas. Embora esta solução seja necessária, e não deva ser descartada, ao longo do trabalho vimos que ela por si só não é suficiente. É preciso também considerar o componente humano no sistema de segurança de informação a fim de minimizar as vulnerabilidades dos sistemas.

Concluímos que a maior parte dos desastres e incidentes com a segurança das informações tem como fator predominante a intervenção humana, e que a segurança tem primeiro a ver com pessoas e processos, antes de ver com a tecnologia. De acordo com alguns especialistas em segurança de informação citados nesta pesquisa, a Engenharia Social é uma das maiores ameaças à continuidade dos negócios da nossa era, pelo que, de nada valerão os milhões investidos em tecnologia, se o fator humano for deixado em segundo plano.

Através da pesquisa realizada na empresa MATOX- Transportes (com a aplicação do questionário e constatação "*in locus*" da realidade da empresa), podemos verificar que cerca de 69% dos funcionários das áreas técnica e administrativa da empresa, têm um nível de escolaridade abaixo do ensino superior, situação que influencia na forma como deverão ser abordadas as questões ligadas a segurança das informações da empresa.

Este facto aliado a ausência de um plano de formação e consciencialização permanente dos colaboradores que defina clara e concisamente quais os procedimentos de segurança a adotar para cada situação inerente a suas atividades laborais, politicas e normas de segurança bem divulgadas e conhecidas por todos os elementos da organização, e planos de resposta a incidentes que descrevam as diretrizes e procedimentos que a área de suporte técnico deverá adotar para a rápida resolução dos incidentes de segurança que possam ocorrer na organização, foram os pontos que mereceram principal destaque neste estudo.

Concluímos ser imperioso proporcionar formação adequada aos colaboradores sobre questões de segurança, e ter em atenção suas condições de trabalho e de remuneração, pois se não são oferecidas boas condições de trabalho, e for exigida uma eficácia incompatível com sua preparação e competências, a tendência é que isso favoreça o desenvolvimento de um clima de insatisfação e *stress* no colaborador, e abra espaço para à execução de atos ilegais que coloquem em risco a segurança da informação.

A sensibilização, formação e educação dos colaboradores é uma arma valiosíssima que nunca deverá ser descartada mesmo que se presuma que todos tenham consciência dos perigos e conheçam a forma correta de agir. O objetivo da sensibilização e educação dos colaboradores não é fazer com que as pessoas se tornem paranoicas, mas que estejam sempre alertas às solicitações que recebam, e que saibam o valor das informações pelas quais são responsáveis.

É recomendável que se crie e implemente uma política de segurança adequada a realidade e necessidades da empresa, e que seja bem divulgada por todos os meios disponíveis na instituição, para que todos saibam como se defender e a quem recorrer em caso de necessidade.

Também recomendamos a adoção da biometria comportamental para a autenticação contínua do utilizador com sessão iniciada no sistema, avaliando fatores como a dinâmica de digitação e do movimento do mouse, tempo e duração em que a tecla é mantida pressionada, frequência e correções de erros de digitação, pressão exercida sobre as teclas, entre outras, por serem características únicas em cada indivíduo, o que reduziria significativamente a incidência de violações usando senha de funcionários.

Punir os responsáveis por ataques de Engenharia Social não é uma tarefa fácil, porque muitos dos delitos utilizados na persecução de ataques nem sequer são considerados crimes nos diplomas jurídicos em vigor no país. No entanto, ações punitivas locais devem ser tomadas pela empresa para desincentivar a prática ou a facilitação de tais crimes por parte de colaboradores, que de forma intencional ou não, possam fornecer ou facilitar aos atacantes a obtenção de informações confidenciais da empresa.

Já a nível nacional, ainda não é possível combater alguns desses delitos, pelo que é necessária uma legislação que defina bem esses crimes, por isso, esta pesquisa recomenda vivamente que a legislação Angolana de crimes informáticos possa prever no futuro, punições específicas para crimes de Engenharia Social como uma forma de desencorajar a prática de tais crimes no país.

O que se espera com este trabalho é que, tendo-se diagnosticado o problema da segurança dos sistemas de informação na empresa, se providenciem as medidas cabíveis aqui sugeridas para que os profissionais de Engenharia Social tenham mais dificuldade para obter e divulgar informações sigilosas da empresa.

Referências

Aaker, et al (2001) “Marketing Research” (7th Ed.), New York: John Wiley & Sons, Inc

Ante projeto da Lei das Comunicações Eletrónicas e dos Serviços da Sociedade da Informação- Lei nº23/11 de 17 de 20 de Julho. (s.d.). Assembleia da republica, Luanda, Angola.

Ardi, C. & Heidemann,J.(2016). AuntieTuna- Personalized Content-based Phishing Detection. NDSS Usable Security Workshop. Disponível em: <https://www.isi.edu/~calvin/papers/Ardi16a.pdf>.acedido aos: 12/02/17

Arora, A. Et al. (2006). Does Information Security Attack Frequency Increase With Vulnerability Disclosure. Disponível em: <https://cyber.harvard.edu/cybersecurity/Does_Information_Security_Attack_Frequency_Increase_With_Vulnerability_Disclosure> acedido aos 21/07/17

Ashford, W.(2016). Social Engineering is top Hacking Method, Survey Shows. ComputerWeekly.com. Disponível em: <http://www.computerweekly.com/news/4500272941/Social-engineering-is-top-hackingmethod-survey-shows> acedido aos: 12/02/17

Baker et al, (2005).“The Impact of Social Engineering Attacks on Organizations: A Differentiated Study”. Information Systems Security, vol. 4320, pp. 1–21.

Baldim, N.(2007). Engenharia Social e Segurança da Informação no Ambiente Corporativo: Uma análise focada nos profissionais de Secretariado Executivo. Universidade Federal de Viçosa.

Barman, S.(2001). “Writting Information Security Policies”.1st Ed. Indianapolis, New Riders.

Beal, A.(2005).Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo. Atlas.

Bíblia online. Gênesis 3:13. Disponível em:https://www.bibliaon.com/versiculo/genesis_3_13/>acedido aos 31/08/17

Blank, R. & Gallagher, P. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations.* nvlpubs.nist.gov. U.S. Department of Commerce. National Institute of Standards and Technology. Disponível em: < nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> acedido aos: 24/03/17

Boozallen.(2017).The malware outbreak may have hidden other network intrusions. Disponível em< https://www.boozallen.com/s/insight/thought-leadership/was-petya-a-cover-up-for-prior-attacks.html >acedido aos 31/08/17

Bosworth, S.& Kabay,M. (2002). Computer Security Handbook, 4th ed. New York. John Wiley.

Callas, J. & Donnerhacke, L.(2007). OpenPGP Message Format. Network Working Group.RFC 4880. IETF. Disponível em: < https://tools.ietf.org/html/rfc4880 > acedido aos: 05/05/17

Carmo, V. (2013). O Uso de Questionários em Trabalhos Científicos. Disponível em: <http://www.inf.ufsc.br/~vera.carmo/Ensino_2013_2/O_uso_de_questionarios_em_trabalhos_cient%edficos.pdf. > acedido aos 03/08/17

Caruso,C. Steffen, F. (1999). Segurança Em Informática e de Informações. São Paulo. Senac.

Cia World Factbook; 2014. Taxa de alfabetização Mundo, disponível em: <http://www.indexmundi.com/map/?v=39&l=pt> acedido aos: 23//11/16

Cialdini, R. (2006).Influence- The psychology of persuasion, Revised. New York. USA. HarperCollins.

Cialdini, R..(2005).Guadagno R., "Online Persuasion and Compliance: Social Influence on the Internet and Beyond," The social net. Human behavior in …, pp. 1–35.New York. HarperCollins.

CNSS (2013). *National Information Assurance (IA) Glossary CNSSI Nº4009.* Disponível em: <http://www.ncsc.gov/publications/policy/docs/CNSSI_4009.pdf> acedido aos: 07/05/17

Constituição da Republica de Angola. (Fevereiro de 2010). Angola.

Convenção Sobre o Cibercrime. 2001. Budapeste. Série de Tratados Europeus / 185**.** Disponível em<http://www.cicdr.pt/documents/57891/128776/Conven%C3%A7%C3%A3o+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c> acedido aos 09/09/17

Convenção Sobre o Cibercrime. 2001. Budapeste. Série de Tratados Europeus / 185**.** Disponível em<http://www.cicdr.pt/documents/57891/128776/Conven%C3%A7%C3%A3o+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c> acedido aos 09/09/17

Coviello, A.(2011), Open Letter to Customers, RSA Security, Inc., hosted on "Network Computing Architects.", disponível em: < http://www.ncanet.com/resources/pressreleases/91-2011-06-08-art-coviello-rsa-open-letter-customers.html > acedido aos: 16//05/17

Crocker, D.&Zink,.T.(2008). M3AAWG Trust in Email Begins with Authentication. M3AAWG. Disponível em:< https://www.m3aawg.org/sites/default/files/document/M3AAWG_Email_Authentication_Update-2015.pdf> acedido aos: 25/01/17

Dantas, M. (2011). Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos, Olinda. Livro Rápido.

ElevenPaths(2017). Fingerprinting Organizations with Collected Archives, disponível em: <https://www.elevenpaths.com/labstools/foca/index.html> acedido aos: 02//04/17

Elpais(2017). Ataque afeta quase cem Países, de Renault na França a bancos russos, disponível em<http://brasil.elpais.com/brasil/2017/05/13/internacional/1494668788_755982.html?rel=mas> acedido aos 21//05/17

Eset.(2017). ESET protects against Petya ransomware and WannaCry. Wannacry Ransomware. Disponível em <https://www.eset.com/pt/home/wannacry/?gclid=Cj0KEQjwmcTJBRCYirao6oWPyMsBEiQA9hQPbr7jxdeNuWm2oN1jIh_j7o8q2sI4ycJxEiI_aZTa1csaAl218P8HAQ> acedido aos: 25/05/17

Eurotux.(2017). Wannacry Ransomware .Protect your business from this digital threat. Disponível em < https://eurotux.com/servicos/seguranca/ransomware-malware?gclid=Cj0KEQjwmcTJBRCYirao6oWPyMsBEiQA9hQPbjXuVYrPf7W5XMkpbvmz-1T7R7CcLscxWNIkv5W0BZgaAlA08P8HAQ> acedido aos: 22//05/17

Evans, N.(2009). "Information technology social engineering: an academic definition and study of social engineering-analyzing the human firewall". Disponível em: <http://lib.dr.iastate.edu/etd/cgi/viewcontent.cgi?article=1701&context=etd · PD> acedido aos: 10//05/17

ExcelWorld,(2017). Planilha de Excel para um questionário. Disponível em: <https://pt.excelworld.net/download/questionario> acedido aos 03/04/17

Feleol, A.(2012). Os três pilares da segurança da informação. Disponível em: <https://alexfeleol.wordpress.com/2012/06/23/os-tres-pilares-da-seguranca-da-informacao/> acedido aos 21/07/17

Filho, A. (2004). Entendendo e Evitando a Engenharia Social: Protegendo Sistemas e Informações in Revista Espaço Acadêmico nº 43; Disponível em <http://www.espacoacademico.com.br/043/43amsf.htm > acedido aos: 23//05/17

Foozy, C. et al (2011). "Generic Taxonomy of Social Engineering Attack," Malaysian Technical Universities International Conference on Engineering & Technology. MUiCET, pp. 527–533.

Galvão, B.(2013). Apresentação Questionários - Como analisar respostas. slideshare. Disponível em: <https://pt.slideshare.net/galvaobianca/apresentacaosurveysbiancagalvo. > acedido aos 03/08/17

Gavrilova, M. (2014). Biometric-Based Authentication for Cyberworld Security: Challenges and Opportunities. Computer Science, University of Calgary. Disponível em: < http://docplayer.net/1130729-Biometric-based-authentication-for-cyberworld-security-challenges-and-opportunities-by-m-l-gavrilova.html> acedido aos 30/08/17

Gelernter, N.et al.(2017). How hackers can steal your 2FA email account by getting you to sign up for another Website/ IEEE Security, disponível em: <https://boingboing.net/2017/06/22/security-questions-suck.html> acedido aos 25/06/17

Gomes, A.(2001).A Criminalidade Cibernética e suas Conseqüências Legais. Security Magazine. Revista de Segurança em Informática. São Paulo.

GReAT, (2017). WannaCry ransomware used in widespread attacks all over the world. Disponível em <https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/> acedido aos: 27//05/17

Green, M.(2014). What's the matter with PGP?, A Few Thoughts on Cryptographic Engineering. Disponível em: <https://blog.cryptographyengineering.com/2014/08/13/whatsmatter-with-pgp/. > acedido aos: 16//05/17

Griffin, P. (2016). Biometric-Based Cybersecurity Techniques- In book: Advances in Human Factors in Cybersecurity. Disponível em: < https://www.researchgate.net/publication/305082243_Biometric-Based_Cybersecurity_Techniques> acedido aos 30/08/17

Guardian, (2011).Cyber-attack of the IMF led by hackers seeking "inside information" . Disponível em< https://www.theguardian.com/business/2011/jun/12/imf-cyber-attack-hack>acedido aos 09/09/17

Guiadoti. (2013). Clonando Páginas com SET (Toolkit de Social-Engineer) + DNS Spoofing. Disponível em: < http://guiadoti.blogspot.pt/2013/02/clonando-paginas-com-set-toolkit-de.html > acedido aos: 16//05/17

Hacking Articles,(2016). Hack Remote PC using PSEXEC Injection in SET. Disponível em: < Toolkit, http://www.hackingarticles.in/hack-remote-pc-using-psexec-injection-set-toolkit/ > acedido aos: 16//05/17

Hadnagy, C. (2010).Social Engineering: The Art of Human Hacking. Indianapolis. Whiley.

Hadnagy, C.& Maxwell, E. (2012). "Social Engineering Capture the Flag Results 2012," in Defcon. USA.

Harvey, S. & Evans, D. (2016). Defending Against Cyber Espionage: The US Office of Personnel Management Hack as a Case Study in Information Assurance. Proceedings of the National Conference On Undergraduate Research (NCUR) . University of North Carolina Asheville. Disponível em< http://ncurproceedings.org/ojs/index.php/NCUR2016/article/view/1764/982>acedido aos 09/09/17

Higbee A.(2016). Phishing and Ransomware Threats Soared in Q1 2016, PhishMe, disponível em: <http://phishme.com/phishing-ransomware-threats-soared-q1-2016/. > acedido aos: 27/04/17

Hill, M. & Hill, A. (1998). A construção de um questionário. Disponível em: < https://repositorio.iscte-iul.pt/bitstream/10071/469/4/DINAMIA_WP_1998-11.pdf> acedido aos 21/07/17

Huber, M. et al.(2009). "Towards Automating Social Engineering Using Social Networking Sites".in International Conference on Computational Science and Engineerin. vol. 3, pp. 117–124.

Hunt,T.(2014).The eBay breach: answers to the questions that will inevitably be asked. Disponível em: <https://www.troyhunt.com/the-ebay-breach-answers-to-questions/.> acedido aos: 10//05/17

ISO/IEC 27000. Information technology -Security techniques - Information security management systems. Overview and vocabulary. Disponível em: < http://www.dcag.com/images/ISO_IEC_27000.pdf> acedido aos: 22/02/17

ISO/IEC 27001. Information technology -Security techniques - Information security management systems. Requirements. Disponível em: <http://www.vazzi.com.br/moodle/pluginfile.php/135/mod_resource/content/1/ISOIEC-27001.pdf> acedido aos: 22//01/17

Jarmoc, J.(2016). RSA compromise: Impacts on SecurID, SecureWorks, Inc. Disponível em: <https://www.secureworks.com/research/rsacompromise. > acedido aos: 15//03/17

Johansson,J.(2008). Island Hopping. The Infectious Allure of Vendor Swag. Technet Magazine. Disponível em: <https://technet.microsoft.com/en us/magazine/2008.01.securitywatch.aspx > acedido aos: 17/03/17

Jones, C. (2004). "Social Engineering: Understanding and Auditing".GSEC. SANS Institute.

Kee, J.(2008). Social Engineering: Manipulating the Source. SANS Institute. Disponível em: <https://www.sans.org/reading-room/whitepapers/engineering/social-engineeringmanipulating-source-32914> acedido aos: 23//03/17

Kitchenham, B. & Pfleeger, S. (2002). Principles of survey research: part 2: Designing a survey. ACM SIGSOFT Software Engineering Notes, 27(1):44–45.

Krebs, B. (2014). Email Attack on Vendor Set Up Breach at Target, February 12, 14. Disponível em: <https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/. > acedido aos: 05/01/17

Krebs, B. (2017). 'Petya' Ransomware Outbreak Goes Global. Disponível em: <https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/> acedido aos 21/07/17

Kucherawy, M.(2015). Domain-based Message Authentication, Reporting, and Conformance (DMARC), RFC 7489. IETF.disponível em: <https://tools.ietf.org/html/rfc7489. > acedido aos: 05/01/17

Lei de Proteção das Redes e Sistemas Informáticos. 2017. Diário da republica de Angola. 16 Fevereiro de 2017. I serie, nº 27.

Lei de Proteção das Redes e Sistemas Informáticos. 2017. Diário da republica de Angola. 16 Fevereiro de 2017. I serie, nº 27.

Lei sobre a Criminalização das Infrações Subjacentes aos Branqueamentos de Capitais- Lei nº 3/14 de fevereiro. (s.d.). Luanda, Angola.

Martins, H. (2013). Identificação biométrica e comportamental de utilizadores em cenários de intrusão. Universidade do Minho Escola de Engenharia. Disponível em: <

http://mei.di.uminho.pt/sites/default/files/dissertacoes/eeum_di_dissertacao_pg21039.pdf> acedido aos 30/08/17

Mattar, F. (1994) Pesquisa de Marketing. Metodologia, Planejamento, Execução e Análise, 2a. ed. São Paulo. Atlas.

Medeiros, C. (2001). Implementação de Medidas e Ferramentas de Segurança da Informação. Joinville. Universidade da Região de Joinville.

Miércoles,(2012).Introducción a Social-Engineering Toolkit (SET), disponível em: <http://0sir1s.blogspot.pt/2012/10/introduccion-social-engineering-toolkit.html > acedido aos: 07//05/17

Mitnick, K. & Long, J.(2008).No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Burlington, MA. Syngress.

Mitnick, K.& Simon, W.(2002). The art of deception: Controlling the human element of security. New York. John Wiley & Sons.

Mitnick, K.(2012).Ghost in the Wires. My Adventures as the World's Most Wanted Hacker. Little. Brown and Company.

Mouton, et al, (2010). "Social engineering attack detection model. SEADM" in Information Security for South Africa, pp. 1–8.

Mouton, F.(2014) Social Engineering Attack Framework, Information Security for South Africa. Disponível em: <https://www.researchgate.net/publication/263588935_Social_Engineering_Attack_Framework> acedido aos: 08//02/17.

Mouton, F.(2016). Towards an Ontological Model Defining the Social Engineering Domain, IFIP Advances in Information and Communication Technology 431, disponível em: <https://link.springer.com/chapter/10.1007/978-3-662-44208-1_22> acedido aos: 08//02/17.

NCSC,(2014). *Cyber Security Assessment Nethrleands CSAN-4.* NCTV.NL. Disponível em: <https://english.nctv.nl/Images/cybersecurityassessmentnetherlands2014_tcm92-580598.pdf?cp=92&cs=65035 > acedido aos: 23//02/17

Newman, L. (2017). The Biggest Cybersecurity Disasters Of 2017 So Far. Security. Disponível em: <https://www.wired.com/story/2017-biggest-hacks-so-far/> acedido aos 03/08/17

Nicholson, D. (2016). Advances in Human Factors in Cybersecurity. Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity. Walt Disney World®. Florida. USA. Disponível em: < http://www.springer.com/gp/book/9783319419312> acedido aos 30/08/17

Oliveira, W. 2001. Segurança da Informação – Técnicas e Soluções. Sociedade da Informação. 1ª edição. Lisboa. Centro Atlântico.

Oliveira, W.(2003). Técnicas para Hackers - Soluções para Segurança. Sociedade da Informação. 2º edição. Lisboa. Centro Atlântico.

Oosterloo, B. (2008). Managing Social Engineering Risk - Making social engineering transparent. Disponível em: <http://essay.utwente.nl/59233/1/scriptie_B_Oosterloo.pdf> acedido aos 21/07/17

Parsons, J. (2017). A potentially virus derived from the CryptoLocker malware crippled NHS trusts across the UK. A look at the ransomware that brought down the NHS. Disponível em <http://www.mirror.co.uk/tech/what-wanna-decryptor-look-ransomware-10410236> acedido aos: 25//05/17

Peixoto, M. (2006).Engenharia Social & Segurança da Informação na Gestão Corporativa. 1ª ed. Rio de Janeiro. Brasport.

Peltier,T.(2006). Social Engineering: Concepts and Solutions. Information Systems Security. Disponível em:<https://www.researchgate.net/publication/220450160_Social_Engineering_Concepts_and_Solutions> acedido aos: 08//02/17

Phishme,(2015).Enterprise Phishing Susceptibility Report, PhishMe. Disponível em: <https://phishme.com/project/enterprise-phishing-susceptibility-report/.> acedido aos: 03//01/17

Puricelli, R. (2015). The Underestimated Social Engineering Threat in IT Security Governance and Management. ISACA Journal. CISM. Disponível em: < https://www.isaca.org/Journal/archives/2015/Volume-3/Pages/the-underestimated-social-engineering-threat-portuguese.aspx> acedido aos 03/04/17

Rafael,G.(2013) Engenharia Social: as técnicas de ataques mais utilizadas, disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/> acedido aos: 13//11/16

Ramsdell, B.(2013). Why security awareness campaigns fail, MWR InfoSecurity.disponível em: <https://www.mwrinfosecurity.com/our-thinking/why-security-awareness-campaignsfail> acedido aos: 31//05/17

Ramsdell,B.(2010). Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. RFC 5751. IETF. Disponível em: <https://tools.ietf. org/html/rfc5751> acedido aos: 03//12/16

RSA.(2011). Anatomy of an attack. RSA FraudAction Research Labs. Disponível em ; http://blogs.rsa.com/anatomy-of-an-attack/. > acedido aos: 03//03/17

Russell, R., Mullen, T. & Long, J.(2009). Stealing the Network: The Complete Series Collector's Edition. Burlington, MA: Elsevier Inc.,

Santos, D.& Silva. R.(2013).Segurança da Informação. Norma ISO/IEC 27000 e ISO/IEC 27001.disponível em: <https://Web.fe.up.pt/~jmcruz/seginf/seginf.1314/trabs-als/final/G4-ISO.27000.final.pdf > acedido aos: 23//11/16

Schallhorn, K. (2017). WannaCry ransomware attack: A look at other major cyber breaches hackings. Disponível em: <http://www.foxnews.com/tech/2017/07/10/wannacry-ransomware-attack-look-at-other-major-cyber-breaches-hackings.html> acedido aos 21/07/17

Schneier B.(2017a). WannaCry Ransomware. Criminals go where the money is, and cybercriminals are no exception. On security. Disponível em<https://www.schneier.com/blog/archives/2017/05/wannacry_ransom.html> acedido aos 23//05/17

Schneier, B. (2002). *Secrets & Lies.* Indianapolis, IN: Wiley Publishing. p.22.

Schneier, B.(2007). Social Engineering Diamond Theft, “Schneier on Security” blog, disponível em<https://www.schneier.com/blog/archives/2007/03/social_engineer_3.html. > acedido aos: 15/05/17

Schneier, B.(2017b) A Man-in-the-Middle Attack against a Password Reset System, disponível em: <https://www.schneier.com/blog/archives/2017/07/a_man-in-the-mi.html> acedido aos 23/06/17

Schwartz, J. (2016). Machine Learning Is No Longer Just for Experts. Analytics. Disponível em: < https://hbr.org/2016/10/machine-learning-is-no-longer-just-for-experts?referral=03759&cm_vc=rr_item_page.bottom> acedido aos 30/08/17

SCO.(2012).The Social Engineering Toolkit's Evolution. Goals.disponível em: <http://www.csoonline.com/article/2131550/social-engineering/the-social-engineering-toolkit-s-evolution--goals.html > acedido aos: 03//03/17

Sêmola, M. (2003).Gestão da segurança da informação.visão executiva da segurança da informação. Rio de Janeiro. Campus.

SocialEngineer,(2017).The Social Engineering Framework; disponível em: < http://www.social-engineer.org/framework/se-tools/computer-based/maltego/ > acedido aos: 23//02/17

Spinapolice, M.(2011). " Mitigating the Risk of Social Engineering Attacks". Rochester Institute of Technology. Disponível em: < http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1397&context=theses> acedido aos 03/04/17

Steve, L.(2016). Domain-Based Message Authentication Reporting and Conformance. InfoSec Institute, disponível em: <http://resources.infosecinstitute.com/domain-basedmessage-authentication-reporting-and-conformance/.> acedido aos: 23//03/76

Stroz, E. et al (2016). Psychology Is the Key to Detecting Internal Cyberthreats. Disponível em: <https://hbr.org/2016/09/psychology-is-the-key-to-detecting-internal-cyberthreats> acedido aos 30/08/17

SurveyMonkey, (2017). How to analyze the results of the survey. Disponível em: <https://help.surveymonkey.com/articles/en_US/kb/How-to-analyze-results.> acedido aos 03/08/17

Symantec, (2017b).Petya Ransomware Outbreak: Here's what you need to know. Symantec Security Response. Disponível em: < https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know> acedido aos 21/07/17

Symantec. (2017a). 2017 Internet Security Threat Report. The 2017 Internet Security Threat Report (ISTR) details how simple tactics and innovative cyber criminals led to unprecedented outcomes in global threat activity. Disponível em: < https://www.symantec.com/security-center/threat-report > acedido aos: 22//04/17

TargetCorporate, (2013). Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores. Target Brands. Inc. Corporate. Disponível em: <https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car. > acedido aos: 23/04/17

TargetCorporate, (2014).Target Provides Update on Data Breach and Financial Performance. Target Brands. Inc. Corporate.disponível em: <https://corporate.target.com/press/releases/2014/ 01/target-provides-update-on-data-breach-and-financia. > acedido aos: 07/04/17

Teotônio, D.(2013). Entendendo os Fundamentos da Segurança da Informação; disponível em: <https://www.profissionaisti.com.br/2013/10/entendendo-os-fundamentos-da-seguranca-da-informacao/> acedido aos: 21//11/16

Thompson, M & Mullen, J. (2017). World's biggest cyberattack sends countries into 'disaster recovery mode'. Disponível em: <http://money.cnn.com/2017/05/14/technology/ransomware-attack-threat-escalating/index.html> acedido aos 21/07/17

Thornton, K. (2017). What Is Social Engineering. Five types of Social Engineering Attacks. Disponível em: <http://www.datto.com/blog/5-types-of-social-engineering-attacks > acedido aos: 27//04/17

Trendmicro, (2014). Social engineering attacks on the rise, part 1. eBay breach. Trend Micro.disponível em: <http://blog.trendmicro.com/social-engineering-attacks-rise-part-1-ebay-breach/. > acedido aos: 25//01/17

Turban et al (2004). Tecnologia da Informação para Gestão. Transformando os Negócios na Economia Digital. 3ª ed. Porto Alegre. Bookman.

Tzu, Sun. (1772). Em S. B. Cassal, & L. &. Pocket (Ed.), A Arte da Guerra (Vol. 207, pp. 12, 13). Porto Alegre.

Verizon, (2016). Data Breach Investigations Report finds cybercriminals are exploiting human nature.disponível em:<http://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-0> acedido aos: 10//11/16

Wikipedia, (2016). Social engineering (political science). Wikipedia.disponível em: <http://en.wikipedia.org/wiki/Social_engineering_(political_science). > acedido aos: 23//02/17

Winnefeld, J. et al (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. SECURITY & PRIVACY. Disponível em: < https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon> acedido aos 21/07/17

Wolff, J. & Maclean, W. (2011). The IMF cyber attack aimed to steal privileged information. Disponível em< http://www.reuters.com/article/us-imf-cyberattack/imf-cyber-attack-aimed-to-steal-insider-information-expert-idUSTRE75A20720110612>acedido aos 09/09/17

Wolff, J.(2017). Digital Health Harvard. Holding Hospitals Hostage- From HIPAA to Ransomware. Disponível em< https://cyber.harvard.edu/events/digitalhealth/2017/04/Wolff> acedido aos 30/08/17

Apêndices

Questionário sobre segurança da Informação na empresa de transportes públicos angolana MATOX- Transportes

Por favor assinale **X** no quadrado da opção verdadeira.

I BLOCO

Dados Demográficos

1. **Qual seu Sexo?**

☐ Masculino ☐ Feminino

2. **Qual seu nível acadêmico?**

☐ Ensino médio incompleto ☐ Ensino médio completo

☐ Superior incompleto ☐ Superior completo

3. **Em que área da empresa você trabalha?**

☐ Administração ☐ Técnica ou Operacional

4. **Quanto tempo você trabalha na empresa?**

☐ Menos de 1 ano ☐ De 1 a 5 anos

☐ De 6 a 10 anos ☐ Acima de 10 anos

II BLOCO

Sobre o Colaborador

5. **O setor em que trabalha, possui informações consideradas confidenciais?**

☐ Sim ☐ Não

6. **Ao sair, deixa seu computador bloqueado ou desligado?**

☐ Sim ☐ Não

☐ As vezes ☐ Nunca reparei

7. **Deixa sua mesa limpa, sem papéis importantes?**

☐ Sim ☐ Não

☐ Nunca reparei

8. **Neste momento, existe algum papel com informações da empresa sobre sua mesa?**

☐ Sim ☐ Não

9. **Seus colegas conhecem a importância das informações da empresa?**

☐ Sim ☐ Não

10. **A informações da empresa estão facilmente acessíveis as pessoas externas a organização?**

☐ Sim ☐ Não

11. **Já teve acesso as políticas de segurança da informação?**

☐ Quando assinei o contrato de trabalho ☐ Tenho acesso periodicamente

☐ Está sempre disponível ☐ Nunca tive acesso

12. Assinou algum termo de responsabilidade e/ou confidencialidade sobre as informações da empresa?

☐ Sim ☐ Não

13. Recebeu alguma formação sobre segurança da informação?

☐ Sim ☐ Não

14. Conhece os mecanismos de segurança para tratamento de dispositivos eletrônicos?

☐ Sim ☐ Não

☐ Sim, porém desatualizados

15. Conhece os mecanismos de segurança de correio eletrônico?

☐ Sim ☐ Não

☐ Sim, porém desatualizados

16. Na sua opinião, qual o lado mais vulnerável da segurança?

☐ Hardwares e Softwares ☐ As pessoas

III BLOCO

Sobre a Empresa

17. A empresa possui Política de Segurança da Informação?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

18. Essa política é divulgada aos novos contratados?

☐ Sim ☐ Não

19. A empresa disponibiliza orientação sobre o manuseamento da informação?

☐ Sim ☐ Não

20. A empresa possui um departamento de Informática?

☐ Sim ☐ Não

21. A empresa possui requisitos de segurança para contratos com terceiros?

☐ Sim ☐ Não

22. A empresa possui controles de segurança específicos para prestadores de serviço?

☐ Sim ☐ Não

23. Existe alguma estrutura que responde aos incidentes de segurança?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

24. Existe alguma gestão de acessos do utilizador?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

25. Existe controle de acesso à rede informática da empresa?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

26. É feito o controle de acesso às aplicações ou diretórios?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

27. É feito o controle de acesso e uso da rede?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

28. Existem critérios de uso de dispositivos pessoais no trabalho ou remotamente?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

29. A empresa estabelece critérios de seleção e política de pessoal?

☐ Sim ☐ Não

☐ Sim, porém desatualizada

30. É feita a capacitação ou educação dos colaboradores sobre segurança da informação?

☐ Sim ☐ Não

31. Existe uma área específica que lide com a segurança da informação ou incidentes de segurança?

☐ Sim ☐ Não

IV BLOCO

Sobre a Segurança da Informação

32. Alguém mais, além de você, conhece a(s) sua(s) senha(s)?

☐ Sim ☐ Não

33. Já utilizou a senha de alguém para aceder a informações da empresa?

☐ Sim, do meu chefe ☐ Sim, de um colega

☐ Não

34. Onde anota suas senhas de acesso?

☐ Próximo ao computador ☐ Na agenda

☐ No telemóvel ☐ Nenhum

35. Com que frequência você altera sua(s) senha(s)?

☐ Mensalmente ☐ Trimestralmente

☐ Quando o sistema solicita alteração ☐ Nunca

36. Como procede para fornecer informações solicitadas por telefone ou email?

☐ Forneço a informação, pois não há nada confidencial em minha área

☐ Forneço a informação, após identificar o solicitante

☐ Forneço somente quando a informação não for confidencial

☐ Forneço informações somente aos gerentes da empresa

☐ Só forneço informações por escrito e com autorização do meu superior

☐ Não forneço, independente de quem for

37. Já deu sua senha por telefone a um colega, chefe ou suporte técnico?

☐ Sim, pelo menos uma vez ☐ Nunca

☐ Sim, mais de uma vez

38. Já usou pendrives de terceiros no computador da empresa?

☐ Sim, pelo menos uma vez ☐ Nunca

☐ Sim, mais de uma vez

39. Já abriu algum ficheiro de email de remetente desconhecido?

☐ Sim, pelo menos uma vez ☐ Nunca

☐ Sim, mais de uma vez

V BLOCO

Sobre a Engenharia Social

40. Já ouviu falar de Engenharia Social?

☐ Já ouvi falar ☐ Nunca ouvi falar

☐ Já ouvi falar, mais não sei do que se trata

41. Conhece alguma medida de prevenção contra Engenharia Social?

☐ Sim, conheço ☐ Nunca ouvi falar

☐ Já ouvi falar, mais não sei do que se trata

42. Já identificou algum ataque de Engenharia Social?

☐ Sim ☐ Não

43. Tem acesso a informações que posam interessar um engenheiro social?

☐ Sim ☐ Não

44. Conhece as técnicas dos engenheiros sociais obterem informações?

☐ Sim ☐ Não

45. Sabe verificar as informações de autenticação nos certificados de segurança dos sites?

☐ Sim ☐ Não

46. Conhece que informações são vitais para o negócio da empresa?

☐ Sim ☐ Não

47. Acredita que possa ser alvo da manipulação de um engenheiro social ?

☐ Sim ☐ Não

48. Saberia se alguém tentasse obter de si informações confidenciais da empresa?

☐ Sim ☐ Não

49. Alguém já utilizou má-fé para obter as informações que tem acesso?

☐ Sim ☐ Não que eu saiba

50. Se sente responsável pela segurança da informação da empresa?

☐ Sim ☐ Não

☐ Sou responsável somente pelo meu trabalho

Informação na Empresa de Transportes Públicos

Matox Transportes

DADOS DEMOGRÁFICOS				
Nível acadêmico do colaborador	**Ensino médio incompleto**	**Ensino médio completo**	**Superior incompleto**	**Superior completo**
	25%	44%	17%	14%

SOBRE O COLABORADOR				
Já teve acesso as políticas de segurança da informação?	**Sim, quando assinei o contrato de trabalho**	**Tenho acesso periodicamente**	**Está sempre disponível**	**Nunca tive acesso**
	28%	9%	0%	62%
Assinou algum termo de responsabilidade e/ou	**Sim**	**Não**		
	15%	85%		
Qual a area mais vulneravel do sistema de informação	**homens**	**Hardware/Software**		
	11%	89%		
Existem critérios de uso de dispositivos pessoais no	**Sim**	**Não**		
	19%	81%		

SOBRE A EMPRESA		
A empresa disponibiliza informação sobre a	**Sim**	**Não**
	38%	63%
Existe alguma estrutura que responde aos incidentes de	**Sim**	**Não**
	19%	81%
Existem critérios para descarte da informação?	**Sim**	**Não**
	6%	94%
É feita alguma capacitação dos colaboradores sobre	**Sim**	**Não**
	31%	69%
Existe uma área especifica que lide com a segurança da	**Sim**	**Não**
	16%	84%

SEGURANÇA DA INFORMAÇÃO				
Já permitiu que outras pessoas utilizassem sua senha?	**Sim pelo menos uma vez**	**Sim, mais de uma vez**	**Nunca**	
	56%	31%	13%	
Já usou pendrives de terceiros no computador da empresa?	**Sim pelo menos uma vez**	**Sim, mais de uma vez**	**Nunca**	
	31%	49%	20%	
Já abriu algum ficheiro de email de remetente	**Sim**	**Não**		
	69%	31%		
Com que frequência você altera sua(s) senha(s)?	Mensalmente	Trimestralmente	Quando o sistema solicita	Nunca
	13%	16%	4%	67%

ENGENHARIA SOCIAL		
Já ouviu falar em engenharia social?	**Já ouvi falar**	**Nunca ouvi falar**
	34%	66%
Conhece alguma medida de prevenção contra engenharia	**Sim**	**Não**
	6%	94%
Sabe verificar as informações de autenticação nos	**Sim**	**Não**
	5%	95%
Conhece que informações são vitais para o negócio da	**Sim**	**Não**
	18%	83%
Se sente responsável pela segurança da informação da	**Sim**	**Não**
	21%	79%