UNIVERSIDADE FEDERAL DE ALAGOAS

INSTITUTO DE COMPUTAÇÃO

EDUARDO ANTÔNIO DE LUCENA LISBOA

ERYCLES DA SILVA SANTOS

MARCOS FABRICIO DE OLIVEIRA SILVA

THALYSSA DE ALMEIDA MONTEIRO

CIBERSEGURANÇA: PREVENINDO ATAQUES BASEADOS EM ENGENHARIA SOCIAL

Maceió - AL

2018

EDUARDO ANTÔNIO DE LUCENA LISBOA

ERYCLES DA SILVA SANTOS

MARCOS FABRICIO DE OLIVEIRA SILVA

THALYSSA DE ALMEIDA MONTEIRO

Projeto de Pesquisa apresentado à disciplina de Metodologia de Pesquisa e do Trabalho Científico do curso de Ciência da Computação da Universidade Federal de Alagoas

Maceió - AL

2018

SUMÁRIO

1 INTRODUCÃO . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

1.1 Abordagem do tema . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

1.2 Justificativa. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

1.3 Hipóteses . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

2 OBJETIVOS DE PESQUISA . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

2.1 Objetivo Geral . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

2.2 Objetivos Específicos. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

3. FUNDAMENTAÇÃO TEÓRICA. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

3.1 Segurança da informação . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

3.2 Engenharia social. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6

4 METODOLOGIA DA PESQUISA . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7

REFERÊNCIAS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8

**1. INTRODUÇÃO**

**1.1 Abordagem do tema:**

Atualmente as grandes empresas guardam informações cada vez mais importantes e sigilosas, mantendo sob sua responsabilidade dados pessoais de milhões de pessoas. Nesta perspectiva, a preocupação de assegurar quem deve ou não acessá-las se torna imprescindível para a manutenção dos três pilares da segurança da informação: Confidencialidade, integridade e disponibilidade (ANDRESS, 2014).

Muito dinheiro tem sido gasto em tecnologias e treinamento de funcionários para garantir que as informações não sejam acessadas de forma indevida, mas ainda assim uma empresa pode estar completamente vulnerável a ataques por ignorar o elo mais fraco da cadeia: O fator humano (MITNICK, 2002).

Não somos treinados para desconfiar uns dos outros e muitas vezes vivemos como se todos fossem dotados de um caráter distinto, este comportamento, apesar de ser uma vulnerabilidade evidente, nos condiciona a uma “ilusão de segurança”. O atacante se aproveita desta ilusão por meio de um contato simples e plausível, de forma que a pessoa nem ao menos perceba o que está se passando (MITNICK, 2002).

Ataques contra a segurança da informação podem ser divididos genericamente em quatro categorias: Intercepção, interrupção, modificação e fabricação (ANDRESS, 2014). Todos eles podem ser um risco à uma empresa caso um engenheiro social bem treinado consiga acesso à dados indevidos, logo, torna-se importante um treinamento específico nas empresas para garantir que seus funcionários estejam conscientes e treinados contra o tipo de ameaça que podem enfrentar.

**1.2 Justificativa:**

De acordo com o site português It Channel (2015), os casos de fraudes e roubos por causa de engenharia social só estão aumentando com o passar do tempo, à medida que as tecnologias de segurança aumentam, tornando o fator humano um elo cada vez mais fraco, sendo o mais fácil de ser corrompido ou atacado. Isto torna, portanto, imprescindível um preparo de todos, para minimizar ao máximo essa vulnerabilidade.

**1.3 Hipóteses:**

Serão necessárias diversas palestras e panfletos informativos com todos os funcionários da empresa, independente do seu nível na mesma, demonstrando as diversas maneiras que os engenheiros sociais maliciosos podem atacar, mostrando que eles utilizarão toda e qualquer informação que esteja ao alcance deles. Phishing, vishing, cavalos de tróia, emails infectados, links falsos e até maneiras mais drásticas como “dumpster diving”, onde o malfeitor literalmente vasculha o lixo da vítima a procura e documentos com informações sensíveis.

**2. OBJETIVOS**

**2.1 Objetivo geral:**

Desenvolver um treinamento presencial para minimizar os cyber-ataques focados na engenharia social, diminuindo a taxa de ataques bem sucedidos e fortalecendo as redes das empresas participantes do projeto.

**2.2 Objetivos específicos:**

Desenvolver um programa geral de mudança e fortalecimento da rede, a partir do levantamento das áreas mais vulneráveis no sistema e o comportamento de cada usuário dele.

**3. FUNDAMENTAÇÃO TEÓRICA**

**3.1 Segurança da Informação:**

A segurança da informação é definida como "proteger os sistemas de informação do acesso, uso, divulgação, interrupção, modificação ou destruição", de acordo com a lei dos EUA. Em essência, isso significa que queremos proteger nossos dados e nossos sistemas daqueles que tentam minimizá-los.

De um modo geral, segurança significa proteger nossos ativos. Isso pode significar protegê-los de invasores invadindo nossas redes, desastres naturais, condições ambientais adversas, falhas de energia, roubo ou vandalismo ou outros estados indesejáveis. Em última análise, tentaremos nos proteger contra as formas mais prováveis ​​de ataque, na medida em que razoavelmente pudermos, dado nosso ambiente (ANDRESS, 2014).

**3.2 Engenharia Social:**

Segundo o Oxford English Dictionary, o termo “engenharia social” tem dois significados distintos (social engineer, social engineering, n. 2017). Primeiro, é “o uso do planejamento centralizado em uma tentativa de gerenciar a mudança social e regular o futuro desenvolvimento e comportamento de uma sociedade”. Segundo, é “o uso do engano para induzir uma pessoa para divulgar informações privadas ou involuntariamente fornecer acesso não autorizado a um sistema de computador ou rede.”Embora ambas envolvem um ou mais indivíduos indutores de comportamento por parte de outros, o primeiro encontra explicitamente sua aplicação no domínio da gestão política e económica, enquanto o segundo encontra sua casa exclusivamente no domínio do ciberespaço. (HATFIELD, 2018).

**4. METODOLOGIA DA PESQUISA**

Inicialmente será escolhida uma empresa disposta a participar do projeto, depois disso haverá o levantamento de dados acerca das vulnerabilidades corporativas e a apresentação delas para a gerência.

Após isso será feito um plano de ação, de forma a fornecer soluções possíveis e auxiliar na implementação das mesmas.

**REFERÊNCIAS**

ANDRESS, Jason. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2. ed. EUA: Elsevier, 2014. 240 p.

Social engineering in cybersecurity: The evolution of a concept. Hatfield, J. M. Elsevier, 2017.

MITNICK, Kevin D. A Arte de Enganar. 1. ed. Estados Unidos da América: Pearson, 2002. 304 p.

CHANNEL, IT. Ataques de engenharia social estão a aumentar – porque é importante proteger-se?. Disponível em: <https://www.itchannel.pt/news/seguranca/ataques-de-engenharia-social-estao-a-aumentar--porque-e-importante-proteger-se>. Acesso em: 28 maio 2018.