Anais do Conic-Semesp. Volume 1, 2013 - Faculdade Anhanguera de Campinas - Unidade 3. ISSN 2357-8904

TÍTULO: VICTIM PROFILE: SOFTWARE DE DETECÇÃO DAS VULNERABILIDADES MEDIANTE O PERFIL DAS VÍTIMAS DA ENGENHARIA SOCIAL

CATEGORIA: EM ANDAMENTO

ÁREA: ENGENHARIAS E TECNOLOGIAS

SUBÁREA: COMPUTAÇÃO E INFORMÁTICA

INSTITUIÇÃO: FACULDADE DE CIÊNCIAS APLICADAS DOUTOR LEÃO SAMPAIO

AUTOR(ES): RAYANNE OLIVEIRA BARBOSA, AMANDA LUIZA FERREIRA DUDA, CHRISTIANNE DE OLIVEIRA PINHEIRO, FRANCISCA DÉBORA ALVES DE FREITAS, PEDRO NATALINO SANTOS DA SILVA

ORIENTADOR(ES): RENATA KALINA DE PAULO ALVES

Realização: SEMESP Apoio: Anhanguera

1. RESUMO

O presente artigo analisa os possíveis meios de ataques de Engenheiros Sociais (ES) tendo como estudo, usuários de diversas culturas organizacionais em ambientes corporativos. Embasado nessa análise, será traçado o nível da vulnerabilidade individual ou em conjunto para ser aplicada uma medida de prevenção, e assim informar agilmente a organização responsável sobre os vazamentos de informações, para que se possa resolver rapidamente o problema e evitar futuras invasões de intrusos com intenções maléficas buscando capturar informações sigilosas.

2. INTRODUÇÃO

Com o crescente aumento de ataques realizados por ES, muitas organizações estão preparando seus colaboradores aplicando treinamentos considerando o fator humano (conscientização dos ataques) e técnico (configuração de antivírus, firewall etc).

O usuário vítima, geralmente tem pouca ou nenhuma experiência sobre segurança da informação, as pessoas revelam informações mais do que o necessário.

Sendo assim propõem-se a seguinte problemática, como identificar perfis de vítimas da engenharia social a partir da análise de comportamentos contínuos em ambientes corporativos utilizando um software de detecção de vulnerabilidades?

3. OBJETIVOS

3.1 GERAL

A pesquisa pretende desenvolver um software que detecte as vulnerabilidades de usuários em empresas corporativas, com o intuito de definir o perfil de vítimas à ataques de engenheiros sociais, propondo uma reeducação quanto à postura dos funcionários possuidores de informações, para saberem como prevenir-se das tentativas intrusas de pessoas com más intenções.

3.2 ESPECÍFICOS

- Desenvolver um software que identifique vítimas da engenharia social;
- Identificar vulnerabilidades dos funcionários nos sistemas da organização;
- Ajudar ao usuário identificar seu perfil a partir das vulnerabilidades quanto as invasões de ES;
- Informar ao departamento de T.I. (Tecnologia da Informação) da organização mostrando o resultado da avaliação, e em paralelo para o usuário;
- Apresentar métodos de prevenção de ataques de ES.

4. METODOLOGIA

Será realizada uma pesquisa qualitativa com entrevista para coletar informações precisas quanto a rotina da empresa. Os entrevistados serão os responsáveis do sistema da empresa alvo, que supervisionam e controlam o fluxo das informações que circulam entre os funcionários. A partir dessa pesquisa será possível traçar os diferentes perfis e o nível de vulnerabilidade, tendo como meta a reeducação dos usuários (funcionários da corporação) no que diz respeito à segurança da informação envolvendo o fator humano.

5. DESENVOLVIMENTO

Qualquer indivíduo deveria ter a garantia da segurança, principalmente no que se trata das informações intrínsecas de cada um em particular. As informações estão cada vez mais acessíveis, pois a frequência do uso da Internet permite realizar diversas ações no dia a dia. Esse tráfego de informações gera muitas vulnerabilidades, estando assim a mercê da engenharia social. Santos (2013) define a engenharia social como sendo “as práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação com mentiras e blefes ou exploração da confiança das pessoas”.

O treinamento em segurança da informação é essencial em qualquer tipo de ambiente, muitas pessoas só se preocupam quando sofrem o primeiro

ataque ou golpe. Um treinamento deve ser tanto de forma técnica com o uso de antivírus e *firewal*l, mas principalmente um treinamento considerando o fator humano.

Ainda para os autores Mitnik e Simon (2003, p. 22) “uma política de segurança bem desenvolvida, combinada à educação e treinamento adequados, aumenta bastante a consciência do empregado sobre o tratamento correto das informações comerciais corporativas”.

É a compreensão da importância desse treinamento e a aplicação do mesmo que fará toda a diferença para a política de segurança da organização. Toda medida de segurança só será eficiente se houverem pessoas conscientes e comprometidas com o seu meio.

6. RESULTADOS PRELIMINARES

Considerando que todos os passos do ser humano tornaram-se praticamente públicos, garantir a integridade, proteger a imagem de si mesmo como também do ambiente corporativo em que se está inserido é uma questão de sobrevivência. Essencialmente todos precisam entender que a segurança não é especificamente apenas responsabilidade dos profissionais de T.I. envolve a equipe como um todo, onde cada um agindo corretamente coopera para que toda a organização seja protegida.

7. REFERÊNCIAS

MITNICK, Kevin D. e SIMON, William L . **A arte de enganar:** ataques de hackers, controlando o fator humano na segurança da informação, São Paulo : Pearson Prentice Hall, 2003

SANTOS. Ellian Mendonça Cardoso dos. **Engenharia Social**: atualmente e o combate para a segurança. Disponível em: <http://www.fatecriopreto.edu.br/Storage/Projetos%20de%20Graduacao/Informatica%20para%20Negocios/Turma%2009%20(12-2010)/Engenharia%20Social%20%20atualmente%20e%20o%20combate%20para%20a%20seguranca.pdf> Acesso em: 02 de dezembro de 2012.