INTERFACE TECNOLÓGICA

ENGENHARIA SOCIAL: vulnerabilidade à segurança da informação

SOCIAL ENGINEERING: vulnerability do information security

Alder Leandro Garbin Minatel – alder@process.com.br
Guilherme Augusto Malagolli – guilherme.malagolli@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (FATEC) – SP – Brasil

RESUMO

A informação tornou-se um recurso essencial na sociedade contemporânea. Para fortalecer sua segurança as organizações investem cada vez mais em equipamentos de alta tecnologia. Neste contexto, com a dificuldade de atacar e fraudar dados em servidor de instituição bancária ou comercial, os golpistas vêm concentrando seus esforços na exploração de fragilidades dos usuários. Utilizando técnicas de engenharia social e por diferentes meios e discursos, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações relevantes ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas. Com o crescimento das redes de computadores e o surgimento da tecnologia da informação, os ataques de Engenharia Social têm sido uma ameaça atual aos sistemas de informação em ambientes organizacionais. Com o intuito de minimizar ou evitar essa ameaça, é necessário entender o comportamento do indivíduo malicioso, ou seja, identificar as principais ações tomadas para alcançar os objetivos desejados. A solução para combater esse problema é a conscientização e o conhecimento adquirido com treinamentos. O presente artigo pretende apresentar e analisar uma das técnicas da Engenharia Social de grande preocupação e prejuízos para as organizações e conceituar as melhores práticas para se prevenir contra esses ataques, evitando assim danos irreparáveis.

Palavras-chave: Segurança da Informação. Engenharia Social. Vulnerabilidade. Organização. Informação.

ABSTRACT

Information has become an essential resource in contemporary society. To strengthen their safety, organizations are continuously investing in high technology equipments. In this context, due to the challenges of attacking and defrauding data from banking or commercial servers, scammers have been concentrating their efforts on exploiting users' weaknesses. Through social engineering techniques and by different means and speeches, hackers deceive and persuade potential victims to provide relevant information or take actions, such as executing malicious codes or accessing false pages. Along with the expansion of computer networks, and the emergence of information technology, Social Engineering attacks have been a recurrent threat to information systems in organizational environments. In order to minimize or avoid these threats, it is necessary to understand the behavior of the malicious individual, that is, identify their main approaches for achieving their goals. The solution to combat these frauds is awareness and knowledge gained from training. Therefore, the present article intends to present and analyze one of the techniques of Social Engineering of greatest

concern and impact to the organizations; as well as conceptualize the best practices in preventing the aforementioned attacks, thus avoiding irreparable damages.

Keywords: Information security. Social engineering. Vulnerability. Organization. Information.

1 INTRODUÇÃO

Atualmente, as empresas tem considerado a informação como um dos principais recursos para tomada de decisões no meio corporativo. Deste modo, pode-se afirmar que, sem informação, acarreta grandes dificuldades em se manter competitivo no mercado.

Sendo a informação um ativo importante na sociedade contemporânea, estas precisam ser protegidas contra as ameaças que podem pôr em risco sua adulteração, divulgação não autorizada e até mesmo perda (BEAL, 2008).

Existem diversos mecanismos de proteção, tais como: antivírus, firewalls, intranet, sistemas de autenticação, token, dentre outros. Essas tecnologias têm função importante para manter os dados em segurança. Contudo, ainda não é o suficiente para garantir a confidencialidade dos dados. Um ponto extremamente relevante e que não pode ser negligenciado na segurança da informação, é a forma de se proteger de ataques provenientes de engenharia social.

> A Engenharia Social é uma técnica antiga e muito popular, que poderia ser traduzida, grosso modo, como “enganar pessoas”. A ideia é que o engenheiro social, como são conhecidos aqueles que praticam esse ato, possa manipular pessoas para que elas revelem informações importantes ou, então, para que elas façam algo que facilite o trabalho dele. Além disso, ela também pode ser encarada como uma maneira de tirar proveito em benefício próprio, por meio de truques psicológicos, ao manipular a tendência que as pessoas possuem de confiar umas nas outras. Autoconfiança, facilidade de comunicação, aptidão profissional e grande capacidade de persuasão são características de um engenheiro social. (GUIMARÃES & JESUS, 2017, p. 8)

Sendo assim, diversas são as organizações que em algum momento se tornam vítimas de aplicações de golpes elaborados por engenheiros sociais. Dentre elas, as instituições bancárias, objeto dessa pesquisa, que tendem a ser alvos dos engenheiros sociais em decorrência de sua atividade estar relacionada a grandes movimentações financeiras.

Diante dos prejuízos gerados pela Engenharia Social, as empresas precisam aplicar um trabalho de conscientização aos seus colaboradores através de treinamentos, a fim de minimizar as vulnerabilidades de segurança pelo fator humano e reduzir os efeitos negativos nos negócios corporativos.

Neste contexto, este artigo tem por objetivo apresentar e analisar uma das técnicas da Engenharia Social de grande preocupação e prejuízos para as organizações e conceituar as melhores práticas para se prevenir contra esses ataques, evitando assim danos irreparáveis.

2 ENGENHARIA SOCIAL

Com o surgimento da Tecnologia da Informação há um aumento contínuo na quantidade de informação, em especial, no ambiente corporativo. Essas informações são armazenadas em diferentes componentes tecnológicos, os quais necessita que o usuário seja prudente quanto ao seu manuseio. É indispensável que sejam elaborados e aplicados métodos para prevenção de fraudes e erros, pois afetam diretamente os processos das organizações.

A maioria das empresas se concentra nas novas ferramentas de proteção tecnológicas, dentre elas: firewalls, antivírus, biometria e outros que proporcionam segurança de suas informações. Entretanto, esquecem-se de outras técnicas aplicadas por indivíduos mal-intencionadas que tem como alvo direto outras pessoas, sem ao menos ter que passar pelos dispositivos tecnológicos.

O ato de persuadir ou influenciar pessoas para obtenção de informações sigilosas ou confidenciais é uma atividade conhecida como engenharia social e é um dos principais desafios da segurança.

Engenharia social é um conjunto de práticas utilizadas para a obtenção de informações relevantes ou sigilosas de uma organização ou indivíduo, por meio da persuasão, manipulação e influência das pessoas, seja com o uso ou não da tecnologia (MITNICK & SIMON, 2003).

Pode-se também definir a engenharia social como sendo a arte de obter informações ou vantagens através de armadilhas psicológicas, persuasão ou qualquer técnica que explore a fraqueza do elemento humano.

Conforme Mann (2008), a segurança humana é a conexão que falta entre segurança de TI e segurança física. O maior risco para a Segurança da Informação em uma organização não está relacionado à tecnologia, mas sim na omissão ou ação de funcionários da organização que, consequentemente, leva a incidentes de segurança.

Dentre as várias definições para o termo, o ponto comum entre todas as interpretações é que a engenharia social utiliza técnicas que pretendem controlar o comportamento humano como um meio para a concretização de um objetivo que, muitas vezes, só é atingido depois da aplicação de diferentes técnicas (HENRIQUES, 2016).

Com o intuito de reduzir ou até mesmo eliminar esses problemas, a solução mais eficaz é a conscientização e o conhecimento dos funcionários ou indivíduos através de treinamentos.

2.1 Conscientização e Treinamento

Primeiramente, para a construção de um programa bem-sucedido de conscientização de segurança é entender o conceito de conscientização, como definir a conscientização de segurança e como isso afeta o negócio de uma forma que faça sentido apoiá-la.

Conscientização é a percepção individual das consequências de uma ação, aliada à habilidade de avaliar sua intenção e seu impacto. A consciência de Segurança da Informação (SI) antecede treinamentos em SI e é um estímulo à participação nestes treinamentos (SANTARCANGELO, 2010).

Muitas pessoas não tem a consciência de que essa ameaça existe e também acham que nunca serão manipuladas, enganadas, persuadidas ou influenciadas. Acreditam que isso só acontece com os outros e, quando menos esperam, são apanhadas desprevenidas por um ataque de engenharia social.

O principal objetivo de um programa de conscientização em Segurança da Informação é fazer com que as pessoas mudem seu comportamento, motivar o empregado a querer fazer parte do programa. Explicar como a participação das pessoas vai beneficiar a empresa e os empregados de forma individual. Os colaboradores precisam estar conscientes de que as informações, sejam elas pessoais ou corporativas, são ativos de muito valor e que seu papel na proteção desse ativo é muito importante (FONSECA, 2009).

Segundo Ferreira & Araújo (2008) relata que para um bom programa de conscientização e treinamento deve-se realizar o planejamento, implementação, manutenção e avaliações periódicas do programa. Alguns pontos devem ser considerados ao se elaborar um programa de treinamento e conscientização contra ataques de engenharia social e, assim tornar a organização menos vulnerável:

a) Definir escopo, metas e objetivos: o escopo deve contemplar todos os profissionais que interagem com os sistemas e com as informações sensíveis para a organização;

b) Identificar os instrutores: é importante que os profissionais dominem as técnicas e os princípios de segurança;
c) Identificar o público-alvo: Identificar e separar os grupos de profissionais que receberão o treinamento. Somente os conceitos necessários devem ser apresentados para obter o melhor resultado;
d) Motivação dos funcionários e da alta administração: O apoio dos funcionários e da alta administração é fundamental para que o programa tenha efetividade e é responsabilidade da alta administração assegurar que todos os usuários dos sistemas de informação saibam como proteger seus ativos;
e) Continuidade: dar atenção às mudanças tecnológicas e de segurança de informação. um programa desenvolvido hoje pode tornar-se obsoleto e ineficaz quando houver mudança no ambiente tecnológico;
f) Avaliação: a avaliação dos funcionários após a realização do treinamento é uma boa opção para verificar o aprendizado dos conceitos e avaliar o nível de conscientização e no direcionamento do reforço necessário.

2.2 Phishing

Diante de diversas técnicas existentes, o Phishing é um tipo de ataque de engenharia social extremamente comum e de grande potencial nocivo para as pessoas e organizações, principalmente no tocante ao prejuízo financeiro.

Em um ataque de phishing, os usuários podem ser coagidos a instalar um software malicioso em seus dispositivos ou a compartilhar informações pessoais, financeiras ou de negócio.

Lee et al 2007 afirma que a técnica consiste, basicamente, no envio de um e-mail à vítima como sendo de uma entidade confiável. Nesse e-mail contêm um link de uma página web fraudulenta, uma imitação perfeita da página oficial, contendo os mesmos logotipos e conteúdos. Como forma de obter informação existe um formulário de cadastro, no qual solicita a introdução de informação confidencial, como: o número da conta, número fiscal, códigos de acessos, dados do cartão de crédito, entre outros. A vítima na sua ingenuidade devido ao desconhecimento ou descuido das políticas de segurança fornece a informação requerida, facilitando os trabalhos do engenheiro social.

O engenheiro social não escolhe horário para o ataque, tem como único objetivo retirar informações sigilosas ou informações pessoais de suas vítimas em potencial, sem ao menos que as percebam que estão contribuindo com o envio dessas informações.

A Federação Brasileira de Bancos (FEBRABAN) tem, constantemente, alertado a população sobre os ataques de phishing. Informa que este ataque tem o objetivo de roubar os dados sigilosos de usuários de computadores como dados bancários, senhas e informações pessoais. E, afirma que esses ataques são provenientes de e-mails que carregam vírus ou links que direcionam o usuário a sites falsos e que, normalmente, possuem remetentes desconhecidos ou falsos. As mensagens contidas nesses e-mails exploram as emoções do destinatário (medo, curiosidade, oportunidades únicas, entre outras), fazendo com que o mesmo clique nos links ou arquivos anexados.

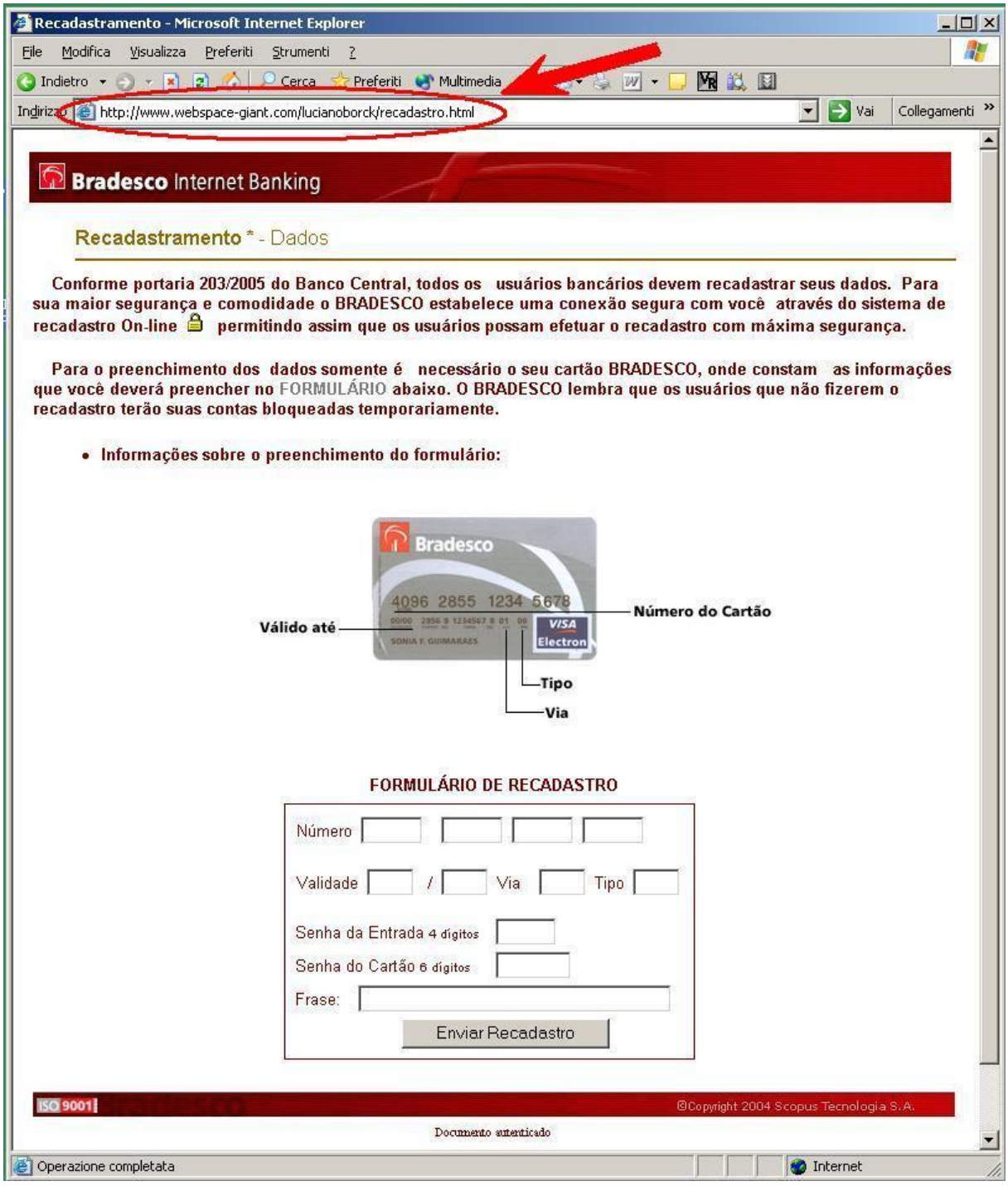
A Figura 1 mostra um exemplo desta técnica de enganar os usuários e convencê-lo ao preenchimento de um formulário para posterior atuação insana do golpista.

3 PROCEDIMENTOS METODOLÓGICOS

Para a construção desse artigo, foi realizada uma pesquisa descritiva e exploratória. A pesquisa descritiva procura observar, registrar, analisar, classificar e interpretar os fatos ou fenômenos (variáveis), sem que o pesquisador interfira neles ou os manipule. Este tipo de pesquisa tem como objetivo fundamental a descrição das características de determinada população ou fenômeno. Por fim, as pesquisas exploratórias são usadas quando pouco se conhece o assunto. Assim, o objetivo de uma pesquisa exploratória é compreender um assunto ainda pouco estudado. Por ser um tipo de pesquisa muito específica, quase sempre assume a forma de um estudo de caso (GIL, 2006). Neste artigo, o caso que ilustra a pesquisa exploratória é o Phishing.

Como qualquer pesquisa, ela depende também de uma pesquisa bibliográfica, pois mesmo que existam poucas referências sobre o assunto pesquisado, nenhuma pesquisa hoje começa totalmente do zero. Para isso, o foco da pesquisa bibliográfica é o conceito de Engenharia Social, como delimitador da pesquisa e que fornece um suporte acadêmico de confiabilidade e veracidade aos fatos e informações descritos. Segundo Gil (2006) uma pesquisa bibliográfica é feita com o auxílio de material já existente, que permite ao pesquisador reconhecer o passado histórico e os aspectos atuais da área pesquisada.

Figura 1. Exemplo prático de Phishing



Fonte: Cartilha de Segurança Digital (2019)

4 RESULTADOS E DISCUSSÃO

Pode-se observar na Figura 1 uma falha grotesca de segurança, isto é, o link está direcionado para uma página de protocolo “http” e os bancos utilizam somente o protocolo de segurança “https”. Outro detalhe importante é que os usuários devem sempre suspeitar do link

recebido por e-mail, visto que as instituições financeiras não se comunicam dessa forma com seus clientes. Outro motivo de desconfiança é que este spam é enviado para várias pessoas e nem todas essas pessoas possuem conta neste banco. As instituições financeiras, por questão de segurança, não solicitam quaisquer que seja informação via e-mail. Muitas pessoas mesmo sabendo dessas informações básicas ainda acabam clicando para analisar e preencher a proposta de recadastramento, onde são submetidas a este tipo de golpe.

A FEBRABAN informa que os bancos, de maneira geral, não enviam e-mails não solicitados com anexos para serem instalados ou links para serem abertos. Alertam que deve-se confiar em um link enviado em mensagens de e-mail somente com o remetente de um banco. No caso de dúvida, o próprio órgão regulamentador pede para o usuário contatar o seu gerente ou sanar as dúvidas com a Central de Atendimento do seu banco.

5 CONSIDERAÇÕES FINAIS

A engenharia social é um dos maiores desafios de segurança para os profissionais de Segurança da Informação. Para uma boa gestão de segurança é necessário que os responsáveis, conheçam as práticas de segurança, bem como acompanhar a evolução da tecnologia e das formas de ataques, além de apresentar habilidades de reconhecer as características de um engenheiro social mal intencionado.

Entretanto, para que as organizações consigam se defender contra esses ataques devem-se estabelecer políticas e procedimentos que definam papéis e responsabilidades para todos os usuários e não somente aos profissionais responsáveis na área de segurança. Enquanto a aplicação somente dê soluções técnicas de software e hardware, que estão bem avançados, estas não são suficientes para o processo de Segurança da Informação, pois a engenharia social ataca o elo mais fraco: os seres humanos.

Por fim, conclui-se que as organizações devem reforçar sua postura de segurança não apenas de forma técnica, mas com uma perspectiva humana da segurança.

REFERÊNCIAS

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção
dos ativos de informação nas organizações.** São Paulo: Atlas, 2008. 175 p.

FEBRABAN. Federação Brasileira de Bancos. Disponível em: https://portal.febraban.org.br/paginas/81/pt-br/. Acesso em: 03 mar. 2019.

FERREIRA, Fernando Nicolau Freitas.; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação** - Guia Prático para Elaboração e Implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FONSECA, Paula Fernanda. FONSECA, Paula F**. Gestão de Segurança da Informação**. 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/PaulaFernandaFonseca-Artigo.pdf>. Acesso em: 25/01/2017.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Editora Atlas 2006

GUIMARÃES, M. V. P.; JESUS, G. L. A. **Engenharia social em nosso cotidiano**. p. 15, 2017.

HENRIQUES, F. A. F. **A influência da Engenharia Social no fator humano das organizações**, p. 112, Universidade Federal de Pernambuco, Recife. 2016.

LEE, D. H., CHOI, K. H., & KIM, K. J.. Intelligence Report and the Analysis Against the Phishing Attack Wich Uses a Social Engineering Technique. Springer-Verlag. 2007.

MANN, Ian. **Hacking the human:** social engineering techniques and security countermeasures. Aldershot, England ; Burlington, VT: Gower, 2008. ISBN 978-0-566-08773-8.

MITNICK, Kevin D.; SIMON, William L**. A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education, 2003.

SANTARCANGELO, Michael. **Why the definition of security awareness matters.** 2010. Disponível em: <https://securitycatalyst.com/why-the-definition-of-security-awarenessmatters/>. Acesso em: 31/01/2017.