9º FEPEG FÓRUM DE ENSINO, PESQUISA, EXTENSÃO E GESTÃO
TRABALHOS CIENTÍFICOS APRESENTAÇÕES ARTÍSTICAS E CULTURAIS DEBATES MINICURSOS E PALESTRAS
23 A 26 SETEMBRO DE 2015
Campus Universitário Professor Darcy Ribeiro
ISSN 1806-549X
A HUMANIZAÇÃO NA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Engenharia Social – Uma abordagem geral sobre a "Arte de Enganar"

João Paulo Pereira Nery, Christine Martins de Matos, Thalles Miguel Tavares, Lucas Araújo Borges, Luanna Ferreira Neves, Joana Gabriela Ribeiro de Souza

Introdução

Com o advento do desenvolvimento tecnológico, um grande volume de dados passou a ser processado, armazenado e compartilhado e, levando-se em conta que se vive a Era da Informação, a proteção desses dados tornou-se essencial. Assim como apregoa a Ciência da Informação, a informação corresponde aos dados processados e dotados de um significado e, dentro da Era da Informação, esta tornou-se diferencial competitivo e componente do principal ativo das organizações, sendo a sua perda motivo de graves danos. A proteção do ativo informacional, levantada no contexto anteriormente exposto, é obtida por meio da Segurança da Informação.

A Segurança da Informação é definida como a proteção do ativo informacional, obtido por meio da adoção de um conjunto de controle adequados, e que visa, entre outras coisas, a continuidade dos negócios de uma organização [1]. A Segurança da Informação possui três pilares essenciais, sendo tecnologias, processos e pessoas. Entretanto, este último pilar é o principal responsável pelas perdas, danos e vazamentos de informações das organizações. Ciente disso, uma prática se aproveita da vulnerabilidade humana na Segurança da Informação: a Engenharia Social. Fazendo uso da manipulação dos sentimentos e comportamentos das pessoas, a prática citada desperta a atenção de profissionais da área de segurança e merece o destaque aqui oferecido.

Material e métodos

A. Conceito e características da Engenharia Social

O termo Engenharia Social ganhou destaque na década de 90 com o ex-*hacker* e atualmente consultor de segurança, Kevin Mitnick. A prática é definida por Mitnick e Simon [2], bem como por Peixoto [3] como a "A arte de enganar" e como uma ciência que faz uso do comportamento humano com a finalidade de induzir alguém a atuar segundo o seu desejo. É uma técnica que não se utiliza necessariamente de grandes conhecimentos técnicos, mas sim um bom planejamento e uma boa conversa [2].

Apesar de Engenharia Social ter ganho notoriedade na década de 90, esta prática é antiga, e ao contrário do que o termo possa indicar, ela não tem nada a ver com ciências exatas ou sociologia. Segundo Santos [4] o uso do termo "engenharia", utilizado para se referir à prática aqui estudada, ocorre pelo fato desta se construir a partir de informações e táticas para acessar informações sigilosas. Em complemento, o autor afirma que o uso do termo "social" se deve ao fato desta prática envolver pessoas que vivem e trabalham em grupos organizados.

Os ataques da Engenharia Social se diferenciam quanto às abordagens, alcances, canais, estratégias e alvos. Os engenheiros sociais, pessoas que fazem uso da Engenharia Social, adaptam seus ataques ao contexto encarado e as suas vítimas, sendo a efetividade das investidas, condicionada ao planejamento feito pelo engenheiro social e pelo conhecimento e suporte comportamental e psicológico de suas vítimas.

Com o fim de melhor caracterizar os ataques da Engenharia Social, é adotada a metodologia utilizada por Câmara [5] ao dividir os ataques da Engenharia Social segundo suas abordagens, alcances, canais, estratégias e alvos.

B. Abordagens utilizadas

Os ataques da Engenharia Social ocorrem por meio de duas abordagens: a abordagem direta e a abordagem reversa.

A abordagem direta condiz com a investida tradicional da Engenharia Social, onde o engenheiro social entra em contato com suas vítimas, por meio de telefone, fax e até pessoalmente. A obtenção de informações por meio dessa abordagem faz com que seja necessário um bom planejamento prévio por parte do atacante.

A abordagem reversa, ou simplesmente Engenharia Social Reversa (Inversa), representa a abordagem utilizada em ataques onde a vítima é quem entre em contato com o atacante. Nestes ataques é comum que o engenheiro social crie uma situação-problema através de sabotagem e, que acometerá uma vítima. O engenheiro social ganha a confiança da vítima e se apresenta como a pessoa capaz de solucionar o infortúnio ocorrido. Em um terceiro momento, a vítima sofrendo os efeitos da sabotagem, entra em contato com o engenheiro social pedindo informações ou solicitando que este resolva o problema. Outra forma de Engenharia Social Reversa é aquele onde a vítima, identificando que está sofrendo uma ofensiva da Engenharia Social, utiliza desta mesma prática para acometer o atacante.

C. Alcances

Ainda fazendo uso do enfoque utilizado por Câmara [5], destaca-se que a Engenharia Social tem duas formas de alcance: o alcance físico e o alcance psicológico.

Para o alcance físico, Granger [6] afirma ser aquele em que os ataques se concentram em ambientes físicos. Nesse sentido a autora cita o uso do local de trabalho, telefone, meio *on-line* e até o lixo. Um exemplo de ataque que faz uso do alcance físico, pode ser aquele em que um engenheiro social, caminhando por escritórios e se passando por uma pessoa autorizada, busca senhas que mais tarde o dará acesso aos sistemas e computadores de uma organização.

Para o alcance psicológico entende-se como aquele que se concentra no ponto de vista psicológico dos ataques, ou seja, a manipulação de sentimentos e comportamentos das pessoas. Para esse alcance da Engenharia Social, Mitnick e Simon [2] tratam sobre a utilização de gatilhos psicológicos, os quais definem como "os mecanismos automáticos que levam as pessoas a responderem às solicitações sem uma análise cuidadosa das informações disponíveis". Granger [6] identifica a utilização de métodos básicos de persuasão como a bajulação, simpatia, transmissão de responsabilidades, intimidação, entre outros.

D. Canais

Entre os vários meios utilizados pelos engenheiros sociais para a realização de ataques, Câmara [5] destaca 4: em pessoa, telefonia, *on-line* e periféricos. Destaca-se que os meios de ataques se adaptam ao desenvolvimento tecnológico.

Os ataques que ocorrem pessoalmente, assim como os demais utilizados na Engenharia Social, visam a persuasão da vítima. Nesses casos os engenheiros sociais vão de encontro às suas vítimas, colocando em risco seus possíveis disfarces, para obterem informações sigilosas, terem acesso às redes e áreas críticas da organização. O contato pessoal, normalmente é evitado pelos atacantes.

Os ataques via telefone são caracterizados pelo roubo de informações por meio de uma simples conversa ou um grampo telefônico. Ataques utilizando este canal são possibilitados pela falta de cuidado das empresas e de funcionários na exposição de ramais da organização e telefones pessoais, bem como pelo conhecimento técnico dos engenheiros sociais na área da telefonia. Nesses ataques, o telefone serve como uma espécie de escudo para o atacante.

Já o meio *on-line* é considerado um terreno fértil para a coleta de senha e informações que serão utilizadas pelos engenheiros sociais. Os atacantes utilizam-se de *sites*, redes sociais, e-*mails* e formulários falsos para a obtenção de informações. Geralmente os atacantes buscam assuntos de interesse de determinada vítima, e enviam, através e-*mails*, *links* ou anexos que quando clicados redirecionam à *sites* falsos que capturarão dados das pessoas, ou farão o *download* de arquivos que quando executados, infectarão o computador da vítima com vírus ou cavalos de tróia, que podem se ocultar e transmitir informações como senhas e números de cartão de crédito para os invasores.

Quanto ao uso de dispositivos periféricos para ataques, Mitnick e Simon [2] apresentam casos de ataques indiretos, em que os *crackers* ou engenheiros sociais instalam códigos maliciosos em CD-ROM, disquetes ou outras mídias removíveis, as rotulam como algo irresistível e colocam diversas cópias em áreas que empregados das organizações têm acesso. Ao acessar o conteúdo destas mídias em computadores, o código malicioso desenvolvido pelos atacantes será executado e, a vítima poderá ter seu computador ou rede da organização afetada.

E. Estratégias utilizadas por engenheiros sociais

Além da escolha de um meio para a realização de seus ataques, os engenheiros sociais adotam determinadas estratégias para acometerem seus alvos. Neste sentido, os atacantes podem fazer uso da persuasão, intimidação, coerção e extorsão para atingir seus alvos.

A persuasão é tratada por Hadnagy [7] como uma arte e a define como o processo de fazer com que as pessoas queiram, façam, reajam, pensem e acreditem da maneira como você deseja. Mitnick e Simon [2] complementam esta definição informando que a Engenharia Social utiliza da persuasão para convencer a vítima de que o atacante é, quem na verdade ele não é. Já a intimidação é conceituada como o ato de intimidar, ou seja, tornar tímido, temeroso. Hadnagy [7] informa que a intimidação não é uma técnica que deve ser utilizada dentro da Engenharia Social no seu sentido tradicional e, ainda afirma que ela é/deve ser usada de maneira sutil.

Por coerção é utilizada a definição de uma força que se observa no campo psicológico, levando alguém a cumprir determinada regra, a ter uma certa conduta, somente devido à pressão "abstrata" que o sujeito emissor da norma impõe. Por último, a extorsão é tida como um crime e é abordada no Art. 158 do Código Penal Brasileiro, como o ato de

ISSN 1806-549X

constranger alguém por meio de violência ou ameaça com o intuito de se obter vantagem econômica, a fazer, tolerar que se faça ou deixar fazer alguma coisa.

F. Alvos

Como abordado, a Engenharia Social aproveita-se de sentimentos e comportamentos humanos para realizarem seus ataques. Mitnick e Simon [2], Câmara [5] e outros autores identificam alguns fatores alvos desta prática:

- medo:, os engenheiros sociais usam o medo das vítimas como alvo, principalmente quando este é relacionado com autoridade. As vítimas obedecem aos comandos dos atacantes para evitarem consequências negativas;
- gratidão: a gratidão das pessoas é constantemente visada pelos engenheiros sociais. Mitnick e Simon [2] identificam o fato das vítimas ficarem agradecidas quando, ao se depararem com um problema, alguém se mostra disponível para ajudar. Um engenheiro social cria um problema, para depois oferecer ajuda e, a partir daí faz uso da gratidão da vítima para extrair informações das quais ele necessita;
- curiosidade: um dos modos utilizados pelos engenheiros sociais para manipularem a curiosidade humana são os *e-mails.* Os atacantes, para convencerem suas vítimas a fazerem o *download* de anexos contaminados, utilizam-se de mensagens chamativas que se referem a conteúdo sexual, notícias, interesses pessoais da vítima, entre outros;
- negligência: conforme apontam Mitnick e Simon [2], as vítimas por razões de descuido, preguiça, desatenção, ou por ignorarem a importância da proteção de determinadas informações, negligenciam as práticas de segurança propostas e colocam as informações pessoais e o ativo informacional das organizações em risco.

Além destes alvos, a Engenharia Social se utiliza da ansiedade, impulsividade, conformismo, culpa, ingenuidade, etc.

Resultados e Discussão

A partir da pesquisa bibliográfica realizada para a construção deste artigo, verificou-se que a Engenharia Social se apresenta como real ameaça à Segurança da Informação. Apesar da exposição sobre como os atacantes fazem uso desta prática, ainda ocorrem muitos episódios de danos ou perda de informações por meio de ataques da Engenharia Social.

Foi identificado que pessoas e organizações continuam a priorizar investimentos na melhoria de aparatos tecnológicos para a segurança das informações e, acabam deixando em segundo plano o cuidado com o fator humano. Este fato, dentre outros, é responsável pela falta de conhecimento das pessoas sobre medidas de Segurança da Informação e dificuldade dos mesmos identificarem ataques de Engenharia Social.

Considerações Finais

Mediante os resultados levantados anteriormente, conclui-se a necessidade de um melhor equilíbrio no tratamento sobre os pilares da Segurança da Informação, enfatizando o treinamento e conscientização das pessoas para o melhor cuidado com o ativo informacional e principalmente, o cumprimento das medidas definidas em Políticas de Segurança da Informação adotadas pela organização. Também, torna-se necessário um maior estudo sobre a influência de fatores ambientais, comportamentais e sentimentais nas pessoas envolvidas no processo de Segurança da Informação, cabendo identificar a intensidade desta influência e criar mecanismos que minimizem seus efeitos durante a proteção do ativo informacional.

Referências

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799**: tecnologia da informação: técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p. Disponível em: < http://xa.yimg.com/kq/groups/21758149/952693400/name/ABNT+NBR+ISO+IEC+17799+-+27001-2005+-+Tecnologia+da+Informa%C3%A7%C3%A3o+- +T%C3%A9cnicas+de+Seguran%C3%A7a+-+C%C3%B3digo+de+Pr%C3%A1tica+para+a+Gest%C3%A3o>. Acesso em: 10 maio 2015.

[2] MITNICK, Kevin; SIMON, William L. **A arte de enganar:** Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

[3] PEIXOTO, Mário C. P. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa**. Rio de Janeiro: Brasport, 2006 apud FONSECA, Paula F. Gestão de Segurança da Informação: O Fator Humano. 2009. 16 f. Artigo (Especialização) – Curso de Pós-Graduação em Redes e Segurança de Computadores, Pontifícia Universidade Católica do Paraná, Curitiba, 2009. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf>. Acesso em: 22 maio 2015.

[4] SANTOS, Luciano A. L. **O impacto da engenharia social na segurança da informação**. 2004. 82 f. Monografia (Especialização em Redes de Computadores) – Curso de Pós-Graduação em Redes de Computadores, Universidade Tiradentes, Aracaju, 2004. Disponível em: <http://search.4shared.com/q/1/O+impacto+da+engenharia+social+na+Seguran%C3%A7a+da+Informa%C3%A7%C3%A3o>. Acesso em: 23 maio 2015.

[5] CÂMARA, Marcelo Ribeiro. **Engenharia Social**: A Psicologia da Aplicação e sua Prevenção. 2009. p. 52. Slide. Disponível em: <http://www.iccyber.org/2009/uploads/trabalhos/20090923/Bradesco_Marcelo_Camara.pdf>. Acesso em: 20 maio 2015.

[6] GRANGER, Sarah. **Social Engineering Fundamentals, Part I**: Hacker Tatics. Disponível em: <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>. Acesso em: 25 maio 2015.

[7] HADNAGY, Christopher. **Social Engineering:** The Art of Human Hacking. Nova Jersey: Wiley, 2010. Disponível em: <http://bookdl.com/9781118906712/>. Acesso em: 20 maio 2015.