
CYBER
ACADEMY
FEBRABAN

MÓDULO 3

Engenharia Social

Conceito

É a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo. Cabe destacar que geralmente os criminosos simulam fazer parte de determinada instituição confiável, como bancos, sites de grandes lojas, órgãos do governo ou outros órgãos públicos para que a vítima confie nos falsos dados apresentados, o que, na verdade, será a isca para que sejam fornecidas as referidas informações.

Utilização

Enquanto certas ameaças cibernéticas utilizam vulnerabilidades localizadas em uma rede ou servidor, na engenharia social o criminoso concentra-se nas vulnerabilidades que porventura a vítima possa ter e/ou apresentar frente a determinadas situações do seu cotidiano. Nestas situações o ponto nevrálgico é a falta de conscientização do usuário de computador sobre os perigos de acreditar em todas as informações que chegam até ele. Também, são as informações que podem ser coletadas pelo criminoso no âmbito da Internet e que são disponibilizadas pelos usuários em suas redes sociais (nomes de familiares, colégios, idade, datas importantes etc.).

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), a engenharia social é Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. Neste contexto, é considerada uma prática de má-fé, usada por golpistas para tentar explorar a ganância, a vaidade e a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes. O popularmente conhecido “conto do vigário” utiliza engenharia social. A Cartilha do CERT.Br apresenta inúmeros exemplos deste tipo de atividade criminosa na Internet, envolvendo ataques,

golpes e códigos maliciosos. Uma característica deste tipo de ação é que não possui procedimentos definidos sendo utilizados; trata-se principalmente da criatividade do autor destas ações e da sua capacidade para persuadir a vítima a oferecer as informações desejadas. Nestes termos, a engenharia social pode ser vislumbrada sob o aspecto físico e psicológico. No físico, exploram o local de trabalho, vasculham lixeiras, e por telefone se passam por outra pessoa. No psicológico, exploram o lado sentimental das pessoas. No Brasil ainda não há uma legislação específica que puna estes tipos de crimes; então, além da conscientização e treinamentos constantes, as empresas devem possuir um plano de contingência para eventuais ataques e assim garantir a continuidade dos negócios.

A engenharia social pode também ser utilizada no âmbito da investigação criminal. Um exemplo muito comum se apresenta nas situações em que o policial se infiltra em uma organização criminosa para coletar indícios sobre a prática de crimes. Nesses casos são utilizadas técnicas de engenharia social para que seja coletado o maior número de informações. É, dentre outros termos, a engenharia social contra o crime. Existem diversas ferramentas na Internet que facilitam a utilização da engenharia social e passam a buscar, de modo automatizado, informações sobre os alvos de interesse dos eventuais cibercriminosos. O tema do uso de fontes abertas é explorado em outras obras.

Exemplos de Procedimentos Preventivos

Segundo Kevin Mitnick, são necessários alguns procedimentos preventivos para evitar ser vítima de engenharia social. Dentre as técnicas, o mais famoso hacker da história apresenta as seguintes:

- Desenvolver protocolos claros e concisos que sejam cumpridos consistentemente em toda a organização;
- Organizar um treinamento em consciência da segurança;
- Criar regras simples que definam quais são as informações confidenciais;
- Elaborar uma regra simples segundo a qual sempre que alguém solicitar uma ação restrita (ou seja, uma ação que envolva a interação com um equipamento relacionado a um computador, cujas consequências não sejam conhecidas), a identidade do solicitante seja verificada de acordo com a política da empresa;
- Desenvolver uma política de classificação de dados;
- Treinar funcionários para resistir a ataques de engenharia social;
- Testar a suscetibilidade de seu funcionário a ataques de engenharia social, conduzindo uma avaliação de segurança.

O aspecto mais importante do programa é estabelecer protocolos de segurança adequados e, então, motivar os funcionários para que assimilem esses protocolos.

Exemplos de técnicas de engenharia social

As principais técnicas utilizadas pelos engenheiros sociais são baseadas na manipulação da emoção de seus "alvos". Assim, trabalham principalmente com o medo, a ganância, a simpatia e, por último, a curiosidade. O usuário de Internet, motivado por essas circunstâncias, acaba prestando informações que não devia ou clica em links que direcionam a sites de conteúdo malicioso e/ou para execução de algum código maléfico em sua máquina. Outro aspecto a destacar sobre a engenharia social é a utilização do chamado efeito saliência: quando o criminoso usa, para chamar a atenção de suas potenciais vítimas, algum assunto que está em destaque na mídia mundial, nacional e/ou regional, como a morte de um ator famoso, um acidente de grandes proporções etc. Por último, procurando traçar didaticamente o tema, outra característica da engenharia social é a ancoragem, quando os criminosos virtuais utilizam, para dar credibilidade aos seus atos, imagens de empresas de mídia, de bancos, de órgãos públicos etc., usando assim, por exemplo, imagens das Polícias Civis, Polícia Federal, Supremo Tribunal Federal, Ministério Público Federal, Globo, Record, SBT etc.

Referências Bibliográficas:

Capeletti, Lucas. Fundamentos de Gestão de Acesso e Identidade (IAM) (Portuguese Edition).
Lisboa Melo, Jefferson; Vieira de Oliveira, Alexandre; Mauser, Daniel. Do Iniciante ao Profissional em Segurança Cibernética. SF Editorial e AcademiaTI.
Fernandes, Victor. Inteligência Artificial para Leigos (Portuguese Edition).
Wendt, Emerson; Jorge, Higor Vinicius Nogueira. Crimes Cibernéticos 3a edição: Ameaças e procedimentos de investigação (Portuguese Edition). BRASPORT.
Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 (Portuguese Edition). BRASPORT.
R., Raphael. Segurança Cibernética: Protegendo Infraestruturas e Dados (Portuguese Edition).

CYBER
ACADEMY

FEBRABAN