Ataques de Engenharia Social

12
jan,2016

1 (https://www.auzac.com.br/ataques-de-engenharia-social/)

(https://www.auzac.com.br/ataques-de-engenharia-social/)
(https://www.auzac.com.br/ataques-de-engenharia-social/)

(https://www.auzac.com.br/ataques-de-engenharia-social/)

(https://www.auzac.com.br/author/admin/) por admin (https://www.auzac.com.br/author/admin/)

Engenharia social (https://www.auzac.com.br/tag/engenharia-social/)

Ataques de Engenharia Social (https://www.auzac.com.br/ataques-de-engenharia-social/)

A engenharia social, no contexto de segurança da informação, refere-se a manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança.

Um ataque clássico na engenharia social é quando uma pessoa se passa por um funcionário de alto nível dentro da organização e diz que o mesmo possui problemas urgentes de acesso ao sistema, conseguindo assim o acesso a locais

restritos. Existem também outras técnicas utilizadas como ataques de engenharia social das quais podemos listar:

E-mail Falso

Sem dúvidas esta é a técnica mais utilizada para conseguir um acesso na rede alvo. Conhecido como ***phishing***, que pode ser traduzido como “pescaria” ou “e-mail falso”, são e-mails manipulados e enviados com o intuito de aguçar algum sentimento de seus destinatários, para que o usuário aceite o e-mail e realize as operações solicitadas.

Análise do Lixo

Provavelmente poucas organizações tem o cuidado de verificar o que está sendo descartado da empresa e de que forma é realizado este descarte. O lixo é uma das fontes mais ricas de informações para os Engenheiros Sociais. Existem muitos relatos e matérias publicadas na Internet abordando este tipo de ataque, visto que através das informações coletadas no lixo podem conter nome de funcionários, telefone, e-mail, senhas, contato de clientes, fornecedores, transações efetuadas, entre outros, ou seja, este é um dos primeiros passos para que se inicie um ataque direcionado à empresa

Contato Telefônico

Utilizando de uma ligação telefônica, seja se passando por um funcionário da empresa, fornecedor ou terceiros, é possível que o ***hacker*** consiga nomes e e-mail de gerentes, coordenadores, até colaboradores da área de TI, informações de ***hardwares*** e de ***softwares*** e até mesmo endereços de IP, diretamente dos próprios funcionários da empresa alvo nesse tipo de ataque.

Internet e Redes Sociais

Atualmente muitas informações podem ser coletadas através da Internet e Redes Sociais sobre o alvo. Quando um ***hacker*** precisa conhecer melhor seu alvo, esta técnica é utilizada, iniciando um estudo no site da empresa para melhor entendimento, pesquisas na Internet e uma boa consulta nas redes sociais na qual é possível encontrar informações interessantes de funcionários da empresa, cargos, amizades, perfil pessoal, entre outros.

Como esse tipo de ataque depende do fator humano para obter êxito, esse último se caracteriza como um dos principais tipos de vulnerabilidade. Neste link você encontrará algumas das mais exploradas que favorecem um ataque hacker (http://www.auzac.com.br/o-que-favorece-um-ataque-hacker/).