CST0206-Arte de Enganar: Parte 1 - Conceitos básicos de Engenharia Social

Data do Post	@July 29, 2022 9:00 AM
Status	Next
Palavras-chave	Engenharia Social
Fonte	
Pronto	Preparado
IG post	☑
Publicado	☐

Post-Linkedin

Engenharia social é um ataque não técnico de um criminoso obter acesso a informações importantes ou sigilosas de pessoas, organizações ou sistemas por meio do engano, ou exploração da confiança, ou negligência das pessoas.

Leia o artigo na íntegra.

Siga-me e veja outros posts no meu Instagram https://www.instagram.com/idaleciosilvatech/

Deixe o like para medirmos a repercussão do conteúdo.
Guarde para rever noutro momento.
Compartilha o conteúdo com os amigos e não só
Comente o que acha do conteúdo e da iniciativa e deixe sugestões.
#cybersecurity #technology #linux #ataquescibernéticos #hacking #socialengineering

Introdução

Engenharia social é um ataque não técnico de um criminoso obter acesso a informações importantes ou sigilosas de pessoas, organizações ou sistemas por meio do engano, ou exploração da confiança ou negligência das pessoas.

A engenharia social é usada para ultrapassar meios técnicos de segurança de uma organização sem o uso de força bruta. Ela permite explorar as falhas de segurança originadas pelas pessoas devido à falta de treinamento e conhecimento de como se defender contra esses tipos de ataques.

Engenheiro Social

Um engenheiro social é uma pessoa que datada com excelentes habilidades de comunicação e bom domínio de técnicas de persuasão que permitem utilizar gatilhos emocionais para seduzir ou aliciar pessoas a aceitarem uma sugestão deles, ou realizar uma acção que lhes favorece. Para atingir seu objectivo, o “engenheiro social” pode se passar por outra pessoa, assumir outra personalidade, procura conhecer os seus alvos para saber se esse, por sua vez, possui as informações que ele deseja.

Os engenheiros sociais frequentemente dependem da boa vontade das pessoas para ajuda, mas também miram nos pontos fracos. Por exemplo, um invasor pode chamar um funcionário autorizado com um problema urgente, que requer acesso imediato à rede. O invasor pode recorrer à vaidade do funcionário, valer-se de autoridade usando técnicas que citam nomes ou apelar para a ganância do funcionário.

Técnicas de Engenharia social

Engenheiros sociais utilizam várias tácticas. As tácticas de engenharia social incluem:

- **Autoridade** – As pessoas são mais propensas a cooperar quando instruídas por "uma autoridade".

- **Intimidação** – Os criminosos intimidam a vítima a realizar uma acção
- **Consenso/prova social** – As pessoas realizarão essa acção se pensarem que as outras pessoas aprovarão
- **Escassez** – As pessoas realizarão essa acção se pensarem que existe uma quantidade limitada
- **Urgência** – As pessoas realizarão essa acção se pensarem que existe um tempo limitado
- **Familiaridade/gosto** – Os criminosos criam empatia com a vítima para estabelecer um relacionamento

Confiança – Os criminosos criam uma relação de confiança com uma vítima, que pode precisar de mais tempo para ser estabelecida

Tipos de ataques

O “ataque” do engenheiro social pode acontecer através de uma conversa amigável, ao telefone ou até mesmo por meio da sedução. A técnica mais utilizada na engenharia social é a habilidade de lidar com pessoas, convencedo-lhes a fornecer informações necessárias ou executar acções em prol do ataque.

Existem diversos ataques, mas todos sempre procurar explicar a elo mais fraco de qualquer sistema de segurança – as pessoas. A maioria das técnicas de engenharia social consiste em obter informações confidenciais enganando os usuários de um determinado sistema através de identificações falsas, empatia ou até mesmo ganhando a confiança da vítima.

Phishing

Nesse tipo de ataque de engenharia social utiliza a estratégia do e-mail falso que o engenheiro social cria uma mensagem convincente que pode ser de uma instituição com boa reputação como empresas, bancos, lojas ou até mesmo de departamentos do governo.

Nessa mensagem o atacante cria uma situação que pode suscitar o interesse do receptor, pode ser um problema na sua conta bancária que para resolver esse problema, deve aceder a um link ou baixar um arquivo em anexo no e-mail.

Após acessar o link ou baixar o arquivo, pode ser instalado um ‘malware’ no computador que pode ser o acesso concedido ao atacante para os dados pessoais do usuário ou da rede que o computador ou dispositivo está conectado.

Pretexting

Pretexting em português “Pretexto” é quando um criminoso chama uma pessoa e mente-lhe na tentativa de obter acesso a dados confidenciais.

Nesse tipo de ataque, o engenheiro social pode utilizar vários métodos para convencer o usuário a dar informações sigilosas sobre ele ou a empresa. Pode ser uma pesquisa falsa ou um perfil falso de rede social que crie uma relação de amizade e utilize essa proximidade para extrair algum dado útil para a invasão.

Something for Something (Quid pro quo)

Ocorre quando um invasor solicita informações pessoais de uma pessoa em troca de algo, como um presente. Isso pode acontecer quando um engenheiro social liga para diversos números de uma empresa para prestar um serviço ou ligou para resolver um problema para a pessoa.

Outros criminosos, vão mais longe. Aliciam as pessoas, oferecendo presentes, dinheiro, pequenos agrados em troca de informações sobre a empresa ou sobre outra pessoa para ela poder montar um perfil e, consequentemente, desferir um ataque.

Shoulder Surfing

Um criminoso observa, ou navega no ombro, para obter PINs, códigos de acesso ou números de cartão de crédito. Um atacante pode estar na proximidade da sua vítima ou o atacante pode usar binóculos, ou câmeras de circuito fechado para descobrir as informações. Esta é uma razão pela qual uma pessoa apenas pode ver o ecrã de uma ATM de certos ângulos. Estes tipos de salvaguardas tornam o surf no ombro muito mais difícil.

“O lixo de um homem é o tesouro de outro homem”. Esta frase pode ser especialmente verdadeira no mundo do mergulho de lixo, o processo de passar pelo lixo de um alvo para ver que informação uma organização deita fora.

Considere proteger o caixote do lixo. Qualquer informação sensível deve ser devidamente eliminada por trituração ou utilização de sacos de queima, um recipiente que guarda os documentos classificados ou sensíveis para posterior destruição por queima.

Imitação e Hoaxes

A imitação ou representação é a acção de fingir ser outra pessoa. Por exemplo, um golpe comum que temos visto são feitos por pessoas que fingem-se passar por outras pessoas, normalmente representam ser funcionários de instituições financeiras ou promotores de sorteios. Esses criminosos, aliciam as pessoas com diversos prémios e no final dizem que as solicitam que as vítimas façam algum depósito ou transferência bancaria para activar esses prémios. No final, não passa de uma trapaça que eles usam para extorquir dinheiro das pessoas.

Uma hoax, ou fraude por mentira, ou boato, é um ato destinado a enganar ou iludir. Uma fraude cibernética deste tipo pode causar tanta interrupção quanto uma violação real causaria. Ela provoca uma reacção do utilizador. A reacção pode criar medo desnecessário e comportamento irracional. Os utilizadores passam estas fraudes por e-mail e nos meios sociais.

Piggybacking e tailgating

Piggybacking ocorre quando um criminoso acompanha uma pessoa autorizada para conseguir entrar num local seguro ou numa área restrita. Os criminosos usam vários métodos para realizar o piggybacking:

- Eles podem dar a aparência de ser escoltados pelo indivíduo autorizado
- Eles podem juntar-se a uma grande multidão fingindo ser um membro
- Eles podem ter como alvo uma vítima descuidada sobre as regras do estabelecimento

Tailgating é outro termo que descreve a mesma prática.

Disfarce on-line, no e-mail e na Web

Encaminhar ou reencaminhar e-mails engraçados, memes de fontes questionáveis, GIFs e e-mails desconhecidos, não relacionados com o trabalho, no local de trabalho podem violar a política de uso aceitável da empresa e resultar em processos disciplinares. Isso porque os criminosos, hoje em dia, esses meios para se esconderes e desferir ataques disfarçados que podem colocar em risco uma organização.

Muitos desses criminosos utilizam sites de conteúdo imoral, publicidades de descontos únicos e imperdíveis para criar gatilhos emocionais nas pessoas e, consequentemente, acederem aos seus sites. Após acederem pode ser que seja um site malicioso com algum tipo de malware que pode comprometer a rede em que o computador do usuário está conectada.

Conclusão

O elemento mais vulnerável de qualquer sistema de segurança é o ser humano, pois possui traços comportamentais e psicológicos que a torna susceptível a ataques de engenharia social. O objectivo dos criminosos é obter acessos não autorizados, espiar e/ou roubar dados e identidades. Muitas das organizações atacadas nem percebem que foram alvos de um ataque, pois esses criminosos usam métodos sorrateiros para deixarem poucos ou rastos falsos, para dificultar que suas acções sejam identificadas.

Embora os profissionais da segurança da informação sejam as pessoas com mais possibilidades de cuidar desses tipos de ataques, deve ser preocupação de todos ter muito cuidado com os riscos da engenharia social, pois todos possuímos dados e eles podem ser usados para cometerem crimes, apoiar campanhas terroristas e muito mais.