TAG: Engenharia Social

“Faça um relatório explicando um ataque de engenharia social. Explique nele como você faria para conseguir uma informação explorando as falhas humanas (foque em fugir de algo técnico aqui) e depois mostre como você usaria ferramentas para aprimorar este ataque.”

Nome: Gabriel Silva Pereira

Data: 15/02/2020

Relatório:

- Introdução

Considero que o alvo da engenharia social é uma empresa, uma organização ou uma entidade, ou seja, um alvo genérico. Partindo dessa premissa, irei descrever um ataque de maneira ampla dado o meu entendimento de vulnerabilidade social que tenho em minha mente, ou seja, tal entendimento é uma visão com pouco embasamento estatístico e muito embasamento anedótico.

- 1º passo (Geolocalização)

Partindo do princípio que tal alvo deve possuir uma ou mais localidades físicas e virtuais, o primeiro passo é entender a geolocalização e a dinâmica logística. As localidades físicas podem ser prédios, casas, shoppings e afins. As localidades virtuais são os servidores que podem estar conectados a rede mundial de computadores ou ser uma fisicamente rede privada. Bem feita essa análise, servirá de base para os passos seguintes.

- 2º Passo (Cara-Crachá)

Saber sobre as pessoas que circulam tal alvo é crucial. Elas são a chave que decripta uma entrada humana em lugares indevidos. Saber não apenas as localidades

centrais do alvo, ou seja, onde provavelmente estará os dados pelo qual se quer roubar ou danificar, também é importante. O endereço dos que circulam podem deixar brechas para explorar redes e afins. Pesquisas avançadas no Google, ou em base dados públicas, podem revelar informações que podem ser relevantes como : pessoas pelo qual aquela pessoa está relacionada, telefone, idade, gênero, CPF, RG, locais de circulação e etc.

- 3º Passo (Planos)

Coletado informações pré-condicionais, se faz uma triagem das mesmas pra elaboração de planos. Os ataques podem ser simples técnicas de fraude social como : Phishing, Tailgating, Quid Pro Quo, Pretext, Baiting ou utilizando ferramentas de cunho tecnológico como Maltego, SET (Social Engineering Toolkit), entre outras. Mas importante ressaltar que esses planos são feitos com base em informações obditas anteriormente através de meios legais, como pesquisa no Google e pesquisa em base dados abertas.

Algumas noções anedóticas salientarei a seguir :

◦ Dados gerais como a proporção de idade, proporção de geração - idoso, adulto, jovem - é importante para saber em qual técnica focar e como utilizá-la. Idosos caem mais em Phishing, Adultos caem mais em Quid Pro Quo, e Jovens caem mais em Pretext, por exemplo;
◦ A maioria dos funcionários, por mais que recebam o código de conduta ou a política de privacidade, não leem tais documentos e consequentemente não os seguem;
◦ Dificilmente, hoje em dia, pessoas irão cair em golpes envolvendo e-mail e assim passarão dados por conta disso, a não ser que a proporção de idosos seja maior;
◦ Mais provável de se usar ataques relacionados a criar Pretext, Baiting, ou Quid Pro Quo, considerando a faixa etaria da população no geral;
◦ Tailgating talvez seja a base para obter acesso físico. Se passar por funcionário da limpeza, entregador, técnico de conserto (eletricista, mecânico, etc);

◦ Pessoas ainda anotam senhas em papeis, vide exemplo da minha mãe que trabalhava na operação de atualização de um sistema hospitalar e de um posto de gasolina cujo vi a senha anotada no balcão;

- 4º Passo (Aplicação e Replanejamento)

Feito o arcabouço teórico, é hora da prática. Considerando as circunstâncias da realidade os planos podem falhar. Desta forma é importante elaborar vários destes e documentar o progresso. Caso obtenha sucesso em algum nível, que seja obter alguma informação parcial, a partir de novas informações se volta ao 3º Passo. Assim se faz um laço de repetição até conseguir o objetivo central do ataque.

- Finalização

Se após seguir tais passos cumpriu-se com o objetivo, ou se é muito bom em tais técnicas ou a empresa é muito ruim e mal orientada para tal aspecto de sua segurança. E pelo parágrafo 1.2 do códito de ética e conduta profissional da ACM (Association for Computing Machinery) - organização que representa internacionalmente os profissionais de TI -, para evitar danos deve relatar a empresa caso observe alguma falha nesse aspecto e caso tenha sido contratado documentar bem, ser profissional e cuidadoso referente a aplicação do ataque.

- Fraudes sociais citadas

Phishing

Obter nome, endereço, RG, CPF Redirecionar a vítima para um site que requisita informações relevantes Colocar ameaças para a resposta ser rápida;

Pretext

Criar um cenário plausível, utilizando informações falsas, para induzir as vítimas a passar informações sigilosas ou seduzi-las a abusar da segurança da organização permitindo entrada;

Baiting

Promete um presente a vítima, na forma de um bem, para em troca infectar computadores ou passar por um controle de segurança físico;

Quid Pro Quo
Promete um presente a vítima, na forma de um serviço, para em troca a vítima passar informações relevantes;

Tailgating
Se passar por alguém legítimo ou usar algúem legítimo para entrar uma área física restrita;

Referências:

- Franklin Martins (@Frankitin);
- https://klickpages.com.br/blog/pesquisa-avancada-google/;
- https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/;
- Experiência anedótica, a.k.a. vozes da minha cabeça;