TAG de: Engenharia social
Tema da TAG: Relatório de teste de invasão utilizando engenharia social
Palestrante: Franklin Martins
Candidata: Fernanda S. Freire

Introdução da TAG

Empresa: Licusa
O que fazem: Empresa de seguros

Relatório

Primeiro passo: preparação – conhecendo a linguagem usada

Para preparar-me para um ataque de engenharia social, comecei estudando o jargão de seguradores, como funcionários de empresas de seguro se comunicam normalmente. Encontrei online um dicionário de "segurês" que são "gírias" desta área. Segue abaixo palavras comuns (e seus significados) utilizadas entre os funcionários e que foram utlizadas no teste.

Jargão:
APÓLICE – É o documento que discrimina o bem segurado, suas coberturas e garantias contratadas pelo segurado, bem como os direitos e deveres das partes contratantes.
BENEFICIÁRIO – Pessoa física ou jurídica a favor da qual o pagamento da indenização deve ser efetuado.
CONDIÇÕES GERAIS – Conjunto de cláusulas contratuais que estabelecem obrigações e direitos, do segurado e da seguradora, de um mesmo contrato de seguro.
CORRETOR DE SEGUROS – Intermediário autônomo, pessoa física ou jurídica, legalmente autorizado a representar o segurado, angariar e promover contratos de seguro entre as seguradoras e as pessoas físicas ou jurídicas, de direito público ou privado.
SUSEP – Superintendência de Seguros Privados. Autarquia federal responsável pela regulação e fiscalização do mercado de seguros.

Por que o jargão é importante? Pois um dos principais passos para uma boa engenharia social é o conhecimento e uso dos jargões, visto que aumenta sua credibilidade e prova que está situado naquilo também.

Segundo passo: preparação – conhecendo a empresa

Após conhecer e estudar o vocabulário utilizado, começa o estudo da empresa e seus funcionários. Utilizando redes como Glassdoor, Linkdlin, Facebook, Instagram, Twitter, etc. Bem como google hacking.
Objetivos mirados e atingidos nesse passo:

- Descobrir a opinião dos funcionários a respeito da empresa;
- Descobrir a empresa terciária que trabalha no local;
- Encontrar funcionários da empresa insatisfeitos;
- Descobrir quais são os funcionários do RH da empresa;
- Descobrir corretores da empresa;
- Ver fotos de funcionários na empresa;
- Descobrir bares frequentes que funcionários frequentam;

Pelo Linkdlin, descobri alguns os funcionários da empresa e segui para suas contas no Facebook. Encontrei entre os perfis analisados, três pessoas muito interessante, um funcionário insatisfeito com

a empresa, uma funcionária de RH carismática que posta tudo em suas redes como público (inclusive, fotos na empresa e com “tias” da limpeza, como ela dissera em uma das fotos onde tirou uma foto com a funcionária tercerizada, que, pelo uniforme, é da empresa **LimpBem**) e uma corretora externa (que disponibiliza número para contato pelo Linkdln).
Seguindo mais a fundo, descobri que o funcionário insatisfeito parecia ter um costume de beber as sextas a noite após o trabalho em um bar próximo a empresa, bem como descobri que alguns colegas da empresa (incluindo a funcionária carismática) costumam se reunir em alguns fins de semana em um barzinho chamado Adão.
Pelo lindkln da empresa, notei que estão contratando e pedem o envio do currículo em formato PDF pelo e-mail.

Terceiro passo: Informações “inofensivas” nocivas

Ligação feita: A corretora externa da empresa, Silvania.
Nome usado: Juliana Lacerda Santos
Conversa:
– Boa tarde! Corretora de seguros da Licuso, Silvania, com quem falo? – Disse a corretora assim que atendeu.
– Boa tarde! Juliana Lacerda. Gostaria de saber mais dos seguros oferecidos e o por que vocês seriam a melhor opção. – Pergunto.
– Bom, oferecemos seguros de todos os tipos, desde vida a carro, casas, aparelhos eletrônicos entre outros. Qual seria o que está interessada? Somos sua melhor opção visto que em nossa empresa valorisamos o segurado acima de tudo. – Ela responde contente por ver avanço em uma possível futura assegurada.
– Entendo, estou interessada no seguro de vida. Podemos fazer um orcamento? Como funcionam os metodos de segurança que utilizaram para proteger meus dados? Qual é a minha garantia que estaram protegidos? – Pergunto com falsa preocupação. No entanto, sei que tais dúvidas devem ser frequentes.
– Claro! Eu poderia pedir o seu e-mail? Para lhe encaminhar alguns dados que precisaria para fazer seu orçamento. Infelizmente não posso lhe garantir que são mantidos em sigilo, todavia asseguro sempre não informar seus dados. Para garantir, você pode acessar a SUSEP e fazer uma pesquisa consultando a empresa pelo órgão.-- Explicou prontamente.
– Claro! Meu email é lacerdajulianaJLS@gmail.com. Obrigada por todas as informações, mas apenas mais uma pergunta. Quem tem acesso as minhas informações? – Respondo.
– A pessoa que tem acesso a eles sou eu e, caso algo aconteça, a empresa para poder efetuar todos os procedimentos.
– Entendo, obrigada mais uma vez! Devo esperar seu e-mail agora?
– Sim, irei enviá-los prontamente assim que encerramos a ligação.
– Obrigada, estou no aguardo.

Uso do envio de currículo: Backdoor pelo curriculo.pdf

Uso do funcionário insatifeito:

Em uma noite de sexta fui no bar que o funcionário insatisfeito mais frequentava, não surpresa, o encontrei bebendo no balcão. E, após sentar-me próxima e falar um pouco com o mesmo, ele começa.
— Não aguento, entende? Eu trabalho em uma empresa de merda que não sabe valorizar ninguém. Não dá. Depois reclamam dos erros, eles pagam mal e cobram muito. Não é assim que funciona. – Ele fala.
— Respira, conta aí o que houve. Falar sempre ajuda, não é o que dizem? – Digo com preocupação, o incentivando e oferecendo mais bebida, que ele prontamente aceita.

— Eu trabalho como programador, só que meu chefe me dá prazos absurdos para fazer coisas que precisam de tempo e atenção. Atualmente está reclamando do programa crashando lá. Claro que iria crashar! Me deu 2 semanas para fazer algo que necessita de dois meses! Está cheio de gambiarra. – Ele confessa, alegrando-me internamente.
— Odeio te dizer isso, mas concordo que seu chefe é um babaca. Típico caso que acha que "nove mulheres podem ter um filho em um mês." – Exalto o quanto estou do lado dele e bebo um pouco.
— Não é?! E ainda é pior porque estou praticamente sozinho. Essa empresa quase não dá atenção para o TI. Mais vale investir em uma festa para os donos do que no setor de TI, para eles. – Ele continua.
– Nunca pensou em conseguir outro emprego? Provavelmente qualquer empresa vai ser melhor. – Pergunto.
– Não é falta de vontade, é falta de oportunidade. Tudo que eu queria era deixar aquela maldita empresa. – Ele lamenta enquanto bebe novamente.
– Bom, eu tenho uns amigos no RH da minha empresa, por que não me dá seu número e e-mail? – Pergunto descontraidamente mexendo no canudo – Eu não garanto nada, mas sei que tem uma área de TI e nenhum deles reclama, não custa tentar. Me dê seus contatos e me envia seu currículo para eu encaminhar, que tal? – Falo quando ele olha.
– Não sei… – ele vacila.
– Vamos, somos praticamente amigos de bar. Não custa tentar, melhor do que ficar infeliz na empresa.
Ele concorda e passa o pedido.

Quarto passo: infiltração

Sabendo a roupa dos funcionários da empresa de limpeza, visto-me como uma após mandar fazer uma blusa com sua logo.
Levo comigo para empresa um saco plastico preto, um pano flanela, um pendrive infectado por mim.
Ao chegar a empresa, espero algum funcionário entrar e sigo o modelo de como ele fez, subindo direto pela a escada para o andar que a funcionária parou.
Chegando lá, procuro a área de limpeza e vejo onde estão os outros da limpeza, entrando na área e pegando uma das lixeiras moveis, cobrindo-a com o saco que trouxe, quando saio e começo a fazer meu trabalho de limpeza, entrando em suas salas, passando um pano pelos móvies e, então, pegando os lixos das centrifogas e lixeiras, jogando no meu saco. Faço isso em todas as salas e saio com a lixeira móvel até a área das escadas, onde pego o saco de papeis e desco pela escada, saindo apenas quando noto o corredor vazio.

Já em casa, remonto os papeis triturados e vejo os somente amaçados. Não me supreendo quando encontro dados confidenciais do cliente e contas da empresa.
Me supreendo menos ainda quando descubro que meu curriculo foi aberto bem como o pendrive plugado.

Quinto passo: Relatório.