SEGURANÇA E PROTEÇÃO DE DADOS

Prof. Priscilla Cunha

pcunha@uni9.pro.br

ENGENHARIA SOCIAL

- Técnica usada por pessoas mal intencionadas para ter acesso a informações confidenciais através da manipulação dos relacionamentos das pessoas, obtendo informações que permitirão o acesso a outras informações mais importantes sem o uso de força bruta.

- Prática pela qual o golpista tem acesso a informações sigilosas explorando a confiança / ingenuidade / falta de treinamento dos colaboradores.

- O invasor faz uso de suas habilidades para obter informações ou acesso indevido a determinado ambiente ou sistema, com a utilização de técnicas de persuasão que acabam na maioria das vezes resultando em informações chaves que poderão ser utilizadas por ele nos seus ataques.

- Foco: obter informações que facilitarão o acesso da pessoa mal intencionada a seu alvo.
- Para cometer esse tipo de ataque não são necessárias a utilização de ferramentas caras, mas sim a realização de ações eficazes, com custo relativamente reduzido e, às vezes, sem custo algum.

- Hoje em dia, a engenharia social é um dos grandes problemas para as empresas. Com as redes sociais, pessoas mal intencionadas conseguem acesso a informações de funcionários desavisados muito facilmente, e essas informações podem levar a acessos indevidos.

- Para piorar, a única medida que as empresas podem tomar para reduzir esses tipo de problema é conscientizar os usuários, pois não há tecnologia que possa impedir esse tipo de situação ou de ataque.
- O golpista explora o lado mais vulnerável da Segurança da Informação, que são pessoas.

- A empresa pode ter o melhor firewall, o melhor antivírus, os melhores controles, mas se não houver preocupação em educar adequadamente o funcionário, que é a parte mais vulnerável do processo, nada disso adianta.
- E qual o alvo de ataque do engenheiro social ?!?!?! Justamente o fator humano!!!

- A ideia principal em um ataque de Engenharia Social é conseguir persuadir as pessoas a fornecerem informações não autorizadas sem o uso de qualquer agressão (e sem que o funcionário se dê conta de que está passando informações importantes).

- Após obter essas informações, a pessoa mal intencionada vai tentar burlar as barreiras física ou lógicas se fazendo valer delas.
- O pior de tudo é que muitas vezes a “falha” do funcionário ocorre por ele não conhecer o valor do ativo informação.

- Com o nível de segurança que se tem nas empresas, ficou mais difícil para pessoas mal intencionadas terem acesso a informações que não deveriam sem usar meios como a engenharia social. Enganar as pessoas, se fazer valer de sua ignorância ou ingenuidade, é simples!

- Formas mais comuns de ataque por engenharia social:
  - Telefonemas;
  - Revirar lixo;
  - Spam / phishing;
  - Páginas da internet falsas;
  - Salas de bate papo e fóruns;
  - Pessoalmente, abusando da boa vontade ou desespero das pessoas, ou mesmo se aproximando delas e desenvolvendo um relacionamento;
  - Redes sociais.

- As informações assim obtidas podem ser o primeiro passo para a pessoa mal intencionada invadir a empresa.
- A internet passou a ser uma ferramenta excelente para a engenharia social. Uma simples pesquisa na internet atrás de informações sobre a empresa alvo de ataque traz uma série de dados que podem ser utilizados para esse fim. O engenheiro social nem precisa sair de casa e se expor.

- Muitos ataques de Engenharia Social são complexos e envolvem diversas etapas e planejamento elaborado, além de combinar o conhecimento da manipulação de pessoas e tecnologia.
- Em geral, o engenheiro social é uma pessoa com boa aparência e facilidade de comunicação.

- O ataque de Engenharia Social exige do atacante uma preparação psicológica grande para o momento do ataque, sendo que às vezes uma interação pessoal é necessária e ele deverá se preparar para enfrentar esse tipo de situação.
- Esse tipo de ação, dependendo da gravidade que possa causar a uma empresa, pode ser enquadrada como “falsidade ideológica”.

COMO EVITAR ATAQUES DE ENGENHARIA SOCIAL

- Implementação e divulgação da PSI, conscientização dos funcionários com relação aos ataques de Engenharia Social e o que eles representam para a empresa;
- Implementação de dispositivos de segurança física e lógica, de forma a diminuir a possibilidade acessos indevidos sem uma autenticação forte, como biometria ou smart cards;

- Monitoramento e acompanhamento constante de pessoas de fora às instalações da empresa;
- Aplicação da política de mesa e impressora limpas;
- Adoção de picotadora de papéis antes do descarte de qualquer informação impressa;

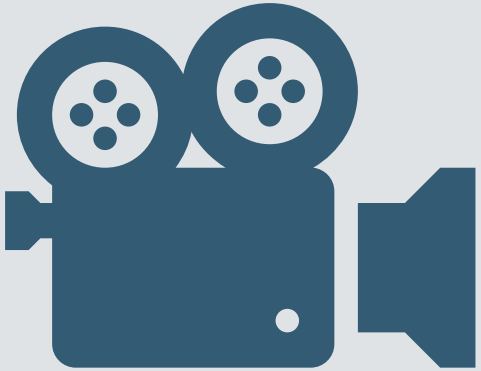
- Treinamento e orientação aos colaboradores da organização para não abrir e-mails estranhos, principalmente os que solicitam a execução de uma ação potencialmente perigosa;
- Monitoramento das atividades dos estagiários e dos aprendizes que, por sua falta de experiência, são frequentes alvos de engenheiros sociais; além disso, pessoas com acesso às informações e locais mais críticos da empresa também devem ser monitorados.

TIPOS DE ATAQUES DE ENGENHARIA SOCIAL

- Diretos
  - Existe contato pessoal entre o atacante e seu alvo, podendo ser realizado por meio de telefonemas, encontros físicos, e o atacante deve se preparar psicologicamente para efetuar esse tipo de ataque, além de ter um “plano de fuga” caso problemas ocorram.

- Indiretos
  - O ataque é realizado utilizando-se ferramentas específicas, que vão desde a utilização do Cavalo de Tróia, ferramentas de monitoração, vírus, keyloggers, screenlogger etc. Ou vasculhando redes sociais.

VÍDEOS



- 9 – Engenharia Social - https://www.youtube.com/watch?v=BbxoegfpcUg
- 9 – engenharia social – animação - https://www.youtube.com/watch?v=mebxuiYb77k

PARA SABER MAIS

- Filme – Caçada Virtual
- https://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm
- http://segurancaiesb.blogspot.com/2011/12/kevin-mitnick-ckacker-que-virou-filme.html


Dúvidas?
Não mais..