Engenharia social (segurança da informação)

Em Segurança da informação, chama-se **Engenharia Social** as práticas utilizadas para obter acesso a informações importantes ou sigilosas em organizações ou sistemas por meio da enganação ou exploração da confiança das pessoas. Para isso, o golpista pode se passar por outra pessoa, assumir outra personalidade, fingir que é um profissional de determinada área, etc. É uma forma de entrar em organizações que não necessita da força bruta ou de erros em máquinas. Explora as falhas de segurança das próprias pessoas que, quando não treinadas para esses ataques, podem ser facilmente manipuladas.

Entendendo a Engenharia Social

Engenharia social compreende a inaptidão dos indivíduos manterem-se atualizados com diversas questões pertinentes a tecnologia da informatica, além de não estarem conscientes do valor da informatica que eles possuem e, portanto, não terem preocupação em proteger essa informação conscientemente. É importante salientar que, a engenharia social é aplicada em diversos setores da segurança da informação independente de sistemas computacionais, software e ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o **ser humano**, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social. Dentre essas características, pode-se destacar:

- **Vaidade pessoal e/ou profissional:** O ser humano costuma ser mais receptivo a avaliação positiva e favorável aos seus objetivos, aceitando basicamente argumentos favoráveis a sua avaliação pessoal ou profissional ligada diretamente ao benefício próprio ou coletivo de forma demonstrativa.
- **Autoconfiança:** O ser humano busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou individuo.
- **Formação profissional:** O ser humano busca valorizar sua formação e suas habilidades adquiridas nesta faculdade, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal buscando o reconhecimento pessoal inconscientemente em primeiro plano.
- **Vontade de ser útil :** O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário.
- **Busca por novas amizades :** O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.
- **Propagação de responsabilidade :** Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.
- **Persuasão :** Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

A engenharia social não é exclusivamente utilizada em informática, a engenharia social é uma ferramenta onde exploram-se falhas humanas em organizações físicas ou jurídicas onde operadores do sistema de segurança da informação possuem poder de decisão parcial ou total ao sistema de segurança da informação seja ele físico ou virtual, porém devemos considerar que as informações pessoais, não documentadas, conhecimentos, saber, não são informações físicas ou virtuais, elas fazem parte de um sistema em que possuem características comportamentais e psicológicas na qual a engenharia social passa a ser auxiliada por outras técnicas como: leitura fria, linguagem corporal, leitura quente, termos usados no auxílio da engenharia social para obter informações que não são físicas ou virtuais mas sim comportamentais e psicológicas.

A engenharia social é praticada em diversas profissões beneficamente ou não, visando proteger um sistema da segurança da informação ou atacar um sistema da segurança da informação.

Um engenheiro social não é um profissional na engenharia social (a engenharia social não é uma faculdade e sim técnicas), mas trata-se de uma pessoa que possui conhecimentos em diversas áreas profundamente ou não, 99% das pessoas que praticam a engenharia social, de forma benéfica ou não, trabalham em grandes empresas ou em empresas de médio porte, visando buscar falhas em um sistema de segurança da informação para aperfeiçoar ou explorar falhas.

Exemplos de empresas:

- **Agencias caça talentos:** Estas empresas buscam pessoas com habilidades na engenharia social para usar de forma benéfica dentro da empresa, visando aperfeiçoar a abordagem de pessoas com talentos por parte de seus funcionários que sofrem ataques constantes de engenharia social para revelarem talentos descobertos pela empresa.
- **Seguradoras, Planos de Saúde:** Estas empresas buscam constantemente na internet e outros meios de busca de pessoas com talentos em engenharia social, visando reduzir ataques individuais ou coletivos visando proteger o quadro de clientes, visando evitar a migração de clientes para outras empresas da mesma atividade.

A engenharia social muito confundida com a arte da enganação em termos técnicos por estar relacionada em casos de violação da segurança da informação virtualmente e físicamente, porém devemos lembrar que a engenharia social é utilizada para a proteção da informação também, estes casos são freqüentes e não são divulgados por motivos de segurança da informação de uma pessoa juridica ou pessoa física, uma falha descoberta por uma pessoa com habilidades na engenharia social ela pode ser explorada de duas formas, beneficamente ou maleficamente, sua atuação como pessoa com habilidades na engenharia social contratado para solucionar falhas e não amplia-las, está é a forma benéfica de usar a engenharia social, a forma maléfica de utilizar a engenharia social está ligada a 99% dos casos por pessoas que buscam violar, obter a informação de forma desonesta, buscando lucros pessoas ou empresariais, lembramos que a engenharia social não é uma faculdade e sim uma habilidade pessoal de um profissional ou não em uma determinada área, profissão, dedicação, hobby, entre outros.

A engenharia social é utilizada no dia-a-dia de pessoas comuns ou não de forma involuntária, o que difere o uso involuntário da engenharia social do prejulgamento ou dedução é a vaidade pessoal ligada ao objetivo pessoal que induz a engelharia social involuntária, freqüentes em lugares comuns como:

Exemplos de locais:

- **Feiras livres:** A engenharia social involuntária é freqüente nas feiras livres em desconfiamos da qualidade, da validade, do preço, usamos a engelharia social involuntária para obtermos informações que nos favoreça diretamente, esta forma de praticar a engenharia social involuntária é avaliada como traço comportamental.
- **Bares:** A engenharia social involuntária é freqüente em bares, buscando informações que possam nos favorecer, em sua grande maioria esta pratica está ligada à conquista, romantismo, de uma forma geral visando a conquista afetiva ou amorosa de uma segunda pessoa seja organizadamente ou não.

A engenharia social lida com varias formas e técnicas em situações diversas, pessoas com habilidades na engenharia social que atuam nesta área por muitos anos definem a engenharia social como umas das ferramentas mais utilizadas no mundo em comunicação humana, visando proteger a informação ou não, divulgar a informação ou não, uma arma ou uma flor em suas mãos com uma imagem desfocada ou focada, porém muito perigosa ao coração.

Técnicas

A maioria das técnicas de engenharia social consiste em obter informações privilegiadas enganando os usuários de um determinado sistema através de identificações falsas, aquisição de carisma e confiança da vítima. Um ataque de engenharia social pode se dar através de qualquer meio de comunicação. Tendo-se destaque para telefonemas, conversas diretas com a vítima, e-mail e WWW. Algumas dessas técnicas são:

- **Vírus que se espalham por e-mail**

Criadores de vírus geralmente usam e-mail para a propagar de suas criações. Na maioria dos casos, é necessário que o usuário ao receber o e-mail execute o arquivo em anexo para que seu computador seja contaminado. O criador do vírus pensa então em uma maneira de fazer com que o usuário clique no anexo. Um dos métodos mais usados é colocar um texto que desperte a curiosidade do usuário. O texto pode tratar de sexo, de amor, de notícias atuais ou até mesmo de um assunto particular do internauta. Um dos exemplos mais clássicos é o vírus I Love You, que chegava ao e-mail das pessoas usando este mesmo nome. Ao receber a mensagem, muitos pensavam que tinham um(a) admirador(a) secreto(a) e na expectativa de descobrir quem era, clicavam no anexo e contaminam o computador. Repare que neste caso, o autor explorou um assunto que mexe com qualquer pessoa. Alguns vírus possuem a característica de se espalhar muito facilmente e por isso recebem o nome de worms (vermes). Aqui, a engenharia social também pode ser aplicada. Imagine, por exemplo, que um worm se espalha por e-mail usando como tema cartões virtuais de amizade. O internauta que acreditar na mensagem vai contaminar seu computador e o worm, para se propagar, envia cópias da mesma mensagem para a lista de contatos da vítima e coloca o endereço de e-mail dela como remetente. Quando alguém da lista receber a mensagem, vai pensar que foi um conhecido que enviou aquele e-mail e como o assunto é amizade, pode acreditar que está mesmo recebendo um cartão virtual de seu amigo. A tática de engenharia social para este caso, explora um assunto cabível a qualquer pessoa: a amizade.

- **E-mails falsos (spam)**

Este é um dos tipos de ataque de engenharia social mais comuns e é usado principalmente para obter informações financeiras da pessoa, como número de conta-corrente e senha. Neste caso, o aspecto explorado é a confiança. Boa parte dos criadores desses e-mails são criminosos que desejam roubar o dinheiro presente em contas bancárias. Porém, os sistemas dos bancos são muito bem protegidos e quase que invioláveis! Como é inviável tentar burlar a seguranças dos sistemas bancários, é mais fácil ao criminoso tentar enganar as pessoas para que elas forneçam suas informações bancárias. A tática usada é a seguinte: o criminoso adquire uma lista de e-mails usados para SPAM que contém milhões de endereços, depois vai a um site de um banco muito conhecido, copia o layout da página e o salva em um site provisório, que tem a url semelhante ao site do banco. Por exemplo, imagine que o nome do banco seja 'Banco Dinheiro' e o site seja www.bancodinheiro.com. O criminoso cria um site semelhante: 'www.bancodinhero.com' ou 'www.bancodinheiro.com.br' ou 'www.bancodinheiro.org', enfim. Neste site, ele faz uma cópia **idêntica** a do banco e disponibiliza campos específicos para o usuário digitar seus dados confidenciais. O passo seguinte é enviar um e-mail à lista adquirida usando um layout semelhante ao do site. Esse e-mail é acompanhado por um link que leva ao site falso. Para fazer com que o internauta clique no link, o texto da mensagem pode, por exemplo, sugerir uma premiação: "Você acaba de ser premiado com 10 mil reais. Clique no link para atualizar seu cadastro e receber o prêmio". Como a instituição bancária escolhida geralmente é muito conhecida, as chances de que o internauta que recebeu o e-mail seja cliente do banco são grandes. Assim, ele pode pensar que de fato foi o banco que enviou aquela mensagem, afinal, o e-mail e o site do link tem o layout da instituição. Como conseqüência, a vítima ingenuamente digita seus dados e dias depois percebe que todo o dinheiro da sua conta sumiu! Repare que em casos assim, o golpista usa a imagem de confiabilidade que o banco tem para enganar as pessoas. Mensagens falsas que dizem que o internauta recebeu um cartão virtual ou ganhou um prêmio de uma empresa grande são comuns. Independente do assunto tratado em e-mails desse tipo, todos tentam convencer o internauta a clicar em um link ou no anexo. A forma utilizada para convencer o usuário a fazer isso é uma tática de engenharia social.

Ver também

- Phishing

Fontes e Editores da Página

Engenharia social (segurança da informação) *Fonte*: http://pt.wikipedia.org/w/index.php?oldid=19800887 *Contribuidores*: Adailton, Alancarv, Diotti, Dtavares, Filipedumont, GOE, GabrielOPadoan, Hermógenes Teixeira Pinto Filho, Joaodp, Lechatjaune, Marcio Benvenuto de Lima, Mfigbr, Nuno Tavares, Pedropaulovc, Radaway, Rei-artur, Rodrigo Bragança, TXiKi, Villarinho, Webcruiser, 44 edições anónimas

Licença