ENGENHARIA SOCIAL, A AÇÃO HUMANA NA PRÁTICA ILEGAL DE ACESSO À INFORMAÇÃO

Marcelo Ferreira, Olavo Alexandrino, Renata Pelin, Walter Jardim

Pós Graduação Engenharia de Software
Faculdade Boa Viagem (FBV) – Recife – PE

marcelongb@yahoo.com.br, oalexandrino@gmail.com,
renata_pelin@hotmail.com, walter_jardim@hotmail.com

Abstract. *The advent of Internet brought a new way of how the society deals with information. The concept of connectivity provided by the Internet has created many different ways of human socialization. At the same time, the need for new techniques of security for Internet took place, and has been used through millions of Internet accesses. Great techniques of informations' security have originated every year. But, many times they are not as effective as the collection of techniques used to manipulate people. These are known as Social Engineering. Even fabulous machines, softwares, and other means of technical protection might not stand a chance against social engineering techniques, because they are based on specific humans actions which software and hardware cannot predict or prevent.*

Resumo. *Com o advento da internet há alguns anos, ocorreu uma reviravolta no formato com que a sociedade em geral lida com a informação. Por outro lado, paralelamente, veio a necessidade de segurança para a informação transitada pelas milhões de conexões, transações, e acessos na rede. O surgimento, desenvolvimento e melhoria dos métodos tecnológicos de segurança da informação são notáveis, mas não tão eficazes quando lidam com um aspecto humano, a Engenharia Social. Mesmo com todo um cenário eletrônico-computacional que uma grande empresa possa ter, ela não estará livre da ação humana interpessoal pré-existente antes mesmo do nascimento dos computadores.*

Introdução

A questão de segurança nos Sistemas de Informação, amplamente discutida pelos meios de comunicação atuais, vem se tornando num grande problema quando o assunto é a escolha das ferramentas, metodologias, tecnologias e/ou aparato tecnológico para a sua prevenção e combate. Não obstante, métodos estejam sendo usados com sucesso em diversas empresas e corporações, torna-se mais complicado quando a questão envolve aspectos humanos e/ou culturais. Estes, indubitavelmente, não têm recebido uma merecida atenção quando da adoção de uma solução.

A princípio, o primeiro desafio quando se fala de segurança é a delineação do escopo do que será auditado, gerenciado ou controlado. Uma vez terminada essa fase, parte-se para o processo técnico já descrito acima, ou seja, escolha do aparato físico-tecnológico. Entretanto, o elemento humano introduz uma imprevisível variação no processo de segurança que não apenas pode ser combatido tecnicamente. Ataques de Engenharia Social são eficazes em uma larga variedade de formatos, que vão desde a uma simples procura de restos de informações jogadas nas lixeiras, a métodos persuasivos, onde a iteração do atacante é mais visível, tais como conversas telefônicas, onde a captura de informações privilegiada é transparentemente usada.

O fator humano deixado em segundo plano, e muitas vezes sumariamente não considerado, é o ponto central de ataques de Engenharia Social que tem como objetivo a exploração dessa fragilidade.

1. Coleta de informações

Vivemos em um mundo globalizado, a informação está dispersa nos mais variados meios de comunicação seja ele, impresso, na televisão ou na internet. Este último, pela sua natureza, consegue abranger todos os setores, todas as classes e culturas. Vivemos em um momento onde a popularização de blogs, fóruns e principalmente comunidades sociais é evidente. Nos grandes sites de buscas é possível encontrar respostas para a grande maioria, senão todas as perguntas do mundo contemporâneo. Dados, a priori, sigilosos estão completamente expostos na grande rede. Com um simples resultado de vestibular ou concurso público, é possível descobrir dados pessoais dos participantes, tais como CPF, RG, e etc. Os dados estão na rede, e mesmo que os próprios sites não existam mais, eles podem ser arquivados pelos mecanismos de busca, tais como o Google. Nessa mesma linha vemos que os próprios usuários não medem esforços em disseminar seus dados pessoais, como nome completo, dos seus familiares, endereço, gostos musicais, livros e filmes prediletos como em sites de relacionamento como é o Orkut, do mesmo Google.

A coleta de informações pode ser considerada como o primeiro passo para um efetivo sucesso de ataque. Já que, conhecendo bem a vítima (sendo ela uma pessoa ou um sistema) será mais fácil se utilizar de outros meios como a descoberta de senhas respondendo às perguntas, supostamente secretas. Os usuários mal treinados costumam cadastrar senhas óbvias como fatos ou dados da sua vida pessoal. Os mais famosos, amplamente usados, são datas de nascimento, o próprio nome, iniciais, etc. Aliando-se à fraqueza de segurança no qual os sistemas são implementados, como por exemplo, permitir que o usuário utilize o seu próprio nome como parte da senha, os que usam da Engenharia Social, podem facilmente descobrir, redefinir uma senha antes, protegida.

Pela sua essência, a Coleta de Informações vem antes de qualquer tipo de segurança, uma vez que o local que o indivíduo guarda suas informações pessoais, se diz respeito exclusivamente a ele. Guardando em local inseguro, como no celular, agenda ou como em um caderno, afastará a possibilidade de gerência de segurança oferecida por um sistema tecnológico.

2. Falsa autoridade

A Falsa Autoridade é uma das mais clássicas e simples formas de ataque. Consistindo na ação em que um indivíduo usa o poder do seu cargo e/ou autoridade para conseguir informações privilegiadas. Porém, o uso do poder não é executado pelo detentor da posição, e sim por aquele que se faz passar por ele, um impostor. Usualmente executada de maneira não pessoal, como telefonemas ou, até por emails, onde o atacante se faz passar por um gerente, administrador de redes, e que vai até o subordinado á procura da informação desejada.

Usada em conjunto com a Coleta de Informações, a Falsa Autoridade é muito forte quando utilizada com usuários despreparados. Pois o atacante já sabe onde agir, sabe de antemão os pontos fracos, as formas de persuasão que deverão ou não ser utilizadas a fim de intimidar ou convencer a vítima na execução de tarefas ou na busca de informações.

3. Falsa autoridade por telefone

Um dos ataques mais comuns hoje em dia é feito por telefone. Pessoas mal intencionadas se fazem passar por empresas conhecidas e confiáveis, e se aproveitam da ingenuidade de outras para conseguirem informações importantes. É comum vermos reportagens onde, por exemplo, uma pessoa liga dizendo que é da operadora de cartão de crédito, informado à pessoa responsável pelo cartão que ela foi sorteada e para receber o premio é necessário informar alguns dados, dentre eles, a senha. Algumas pessoas realmente estão participando de alguma promoção e na euforia nem percebem que acabam por informar sua senha. Vemos aqui mais uma forma em que a Coleta de Informações é fundamental para um ataque bem executado.

Outro alvo são os *call centers*, onde os atendentes são treinados para sempre falar bem e esclarecer quaisquer dúvidas. É nesse contexto que entra o “hacker”, que através destas ligações pode conseguir valiosas informações de algum atendente despreparado pra um ataque desse tipo.

A partir da Coleta de Informações o número de telefone de uma empresa pode ser facilmente conseguido e conseqüentemente os ramais também. Como algumas empresas aceitam ligações diretas para os ramais, os “hackers” ligam dizendo ser da sua empresa, da área de suporte, por exemplo, e acabam conseguindo informações importantes, tanto sobre as pessoas, quanto sobre a própria empresa.

4. Lixo

Outra forma popular de engenharia social é a coleta de informações através do lixo das empresas. Isso porque ele pode conter agendas telefônicas, organogramas, calendários de reuniões, manuais de sistemas, memorandos, relatórios, papéis com login e senha escritos, dentre outros. Esses materiais provêem diversos tipos de informações importantes para os “hackers”.

Os organogramas, por exemplo, podem indicar pessoas em posições mais altas na empresa, facilitando o ataque por Falsa Autoridade, citada no item 2. As agendas telefônicas indicam os ramais dos funcionários, facilitando o ataque por telefone, citado no item 3. Os manuais de sistema podem até indicar como acessar informações importantes da empresa. Por isso, o lixo das empresas constitui uma fonte valiosa de informação para pessoas má intencionadas.

5. Engenharia social on-line e senhas

Não se pode deixar de falar sobre a engenharia social on-line e senhas. Como dito anteriormente, no item 1, as informações estão dispersas em diversos meios, principalmente na internet. Saber escolher uma boa senha, usar a pergunta secreta corretamente e utilizar diferentes senhas ajuda a reduzir o risco de ataque da engenharia social on-line.

Um dos principais fatores que contribuem para este tipo de ataque é que os usuários normalmente usam a mesma senha para quase, senão todos, seus serviços, sites, entre outros. Portanto, basta o “hacker” descobrir uma senha pra ter acesso a diversas contas do usuário. E não é difícil conseguir essa senha. O “hacker” pode se utilizar da resposta de uma pergunta secreta ou até enviando emails falsos para o usuário, pedindo que o mesmo informe sua senha no email.

Outras formas de realizar este tipo de ataque são as salas de bate papo, onde o “hacker” se passa por uma pessoa bem intencionada e se aproveita do sentimento alheio. Também podemos citar o envio de email com vírus que quando instalados no computador podem captar todo tipo de informação digitada.

6. Eavesdropping

Como diz um ditado popular, “as paredes têm ouvido”. O termo em Inglês pode ser definido como: ouvir alguém, um grupo, uma reunião secretamente. O atacante que usa essa técnica, não faz nada mais do que escutar e observar as ações que acontecem em seu ambiente. Eles observam as discussões que estão ocorrendo, vai tomando nota de tudo que possa ser útil. Ele tem a vantagem de estar obtendo dados fundamentalmente reais, uma vez que está capturando direto da fonte. Evidentemente, nem toda escuta pode ser útil, mas pode facilmente ser utilizada com sucesso juntamente com outras técnicas de Engenharia Social.

7. Medo

Em se tratando de Engenharia Social jamais podemos esperar que o atacante tenha uma boa índole. Da mesma forma, não devemos achar que ele se encontra distante da nossa empresa, do nosso time ou do projeto em que trabalhamos. O ser humano é passível de erro, todos nós erramos e nem sempre a repercussão de um erro é bem assimilada por todos. Também, não muito raro, erramos e julgamos que tal problema não merece ser difundido. Preferimos guardá-lo ao invés de deixá-lo transparente a todos. Porém, muitas vezes esquecemos que alguém pode perceber esse erro e usá-lo num futuro próximo para obtenção de informações.

Em um cenário real poderíamos executar alguma ação verdadeiramente proibida como acessar o setor financeiro do sistema da empresa, ou mesmo bater o ponto de casa todos os dias através do uso de alguma ferramenta remota. Alguém, descobrindo fatos

como esses, pode muito facilmente lhe enviar um email anônimo, requerendo-lhe informações privilegiadas como a senha de acesso a alguma área de um sistema gerenciado. Caso você não o responda, ele lhe entregará. Você não pensa duas vezes, e fornece a informação requerida. Desse modo, o atacante pode conseguir o que precisa sem sequer ser reconhecido, de maneira totalmente transparente.

8. Falsa autoridade pessoalmente

Embora mais rara, a falsa autoridade onde uma pessoa se passa por outra fisicamente é perfeitamente possível. Como simplesmente algum executivo bem trajado indaga sua secretária alegando que tem uma reunião com seu chefe. A empresa não tem nenhum dispositivo de cadastro físico, como registro de pessoal de quem acessa o escritório ou registro via fotos, já muito comum em fábricas. Pela persuasão, o atacante consegue coletar informações, ou mesmo ter acesso aos interiores do escritório.

Esse tipo de abordagem também pode burlar um verdadeiro aparato tecnológico instalado em prédios ou empresas. Muitas vezes os atacantes, nesse caso é mais comum uma ação em grupo, também se utiliza da figura feminina, que a partir das suas características fenotípicas consegue entrar sem nenhum transtorno. Nesse caso, vemos claramente que a questão de treinamento é fundamental para o sucesso do sistema implantado. Uma vez que não adianta investir milhares em equipamentos quando se esquece do treinamento para usá-lo.

9. Como diminuir o risco?

9.1 Criptografia

O avanço da tecnologia e, por conseguinte, dos sistemas mudaram a forma de troca de informação entre os setores corporativos. Em empresas maiores é permitido o uso de programas mensageiros até mesmo em formato corporativo. Quando se usa uma ferramenta como essa, pouca gente toma nota do que está ocorrendo. A grande maioria dos softwares mais utilizados não oferece uma forma de criptografar as mensagens. Desse modo, toda a conversa está trafegando livremente pela rede interna da empresa. A simples instalação de um analisador de pacotes, conhecido como *sniffer*, pode interceptar as conversas em formato de texto. Percebe-se que não é necessário ser um perito em informática para conseguir informações privilegiadas. O uso de criptografia pode facilmente impedir esse acesso oculto. Por outro lado podem surgir outros problemas dependendo da forma que os são encriptados.

Uma solução aceitável é o desenvolvimento de criptografia baseada em chaves público-privadas. Cada participante, ou seja, cada usuário do programa mensageiro teria uma chave pública que seria distribuída para todos os demais, enquanto a chave privada deve ser conhecida apenas pelo seu dono.

Usando um algoritmo de criptografia, uma mensagem que é criptografada com a chave pública pode somente ser decifrada pela sua chave privada correspondente. Do mesmo modo, uma mensagem cifrada com a chave privada pode somente ser decifrada pela sua chave pública correspondente.

Isso garantiria você ter certeza que está falando com o seu amigo de trabalho e ainda saber que sua conversa está oculta. Pois mesmo que o atacante capture os dados via rede, não teria como decifrá-los uma vez que não possui a chave privada.

Porém, esse método nos remete a uma questão: como, e onde guardar a chave privada? Esses programas muitas vezes utilizam de uma senha pessoal para acesso. Um atacante pode primeiramente coletar informações sobre a vítima. Uma vez coletada, ele parte para um ataque no sentindo de adivinhar a senha da vítima. A vítima, mal treinada, define sua senha, dica de senha, resposta da pergunta de redefinição de senha como sendo uma informação óbvia. Muitas vezes não é culpa dela, pois os próprios sistemas, algumas vezes não permitem que os usuários definam suas próprios perguntas/respostas secretas. O atacante consegue redefinir a senha, efetua o acesso no programa mensageiro em qualquer máquina.

Depois disso, utilizando de Falsa Autoridade, conversa com a vítima e a envia outra chave pública (pois a anterior estava na estação de trabalho do usuário com a senha roubada). A vítima não percebe aceita e conversa naturalmente com o atacante. Agora, além de ver com os próprios olhos a conversa, pode o atacante interceptar os dados via rede e decifrar-los. Desse modo, o esquema de criptografia adotado foi vencido.

Isso não significa que o formato utilizado não seja eficaz. Para melhorar a segurança, uma boa idéia já em uso, é a utilização de um *token* junto com a senha. Esse mecanismo consiste em um dispositivo físico que fica com o detentor das chaves e muda periodicamente. Quando o usuário partir para sua autenticação do sistema ele teria que informa sua senha e também um número randômico gerado pelo *token.* Agora nesse caso só com um roubo permitiria um atacante um sucesso, pois sequer ele poderia logar no sistema.

9.2 Segurança

Apesar de todos os ataques vistos, onde os mesmos não dependem de toda segurança lógica e física adotadas pelas empresas, é possível diminuir o risco com educação, treinamentos pessoais. O primeiro passo é fazer com que segurança seja um assunto onde todos os funcionários se preocupem e procurem ficar atentos no desenvolvimento de qualquer sistema.

Através da educação, os funcionários podem perceber a importância da segurança da informação e que existem pessoas preparadas para se beneficiar de qualquer fragilidade apresentada pelos sistemas. É importante apresentar os dois lados da história, a respeito de segurança computacional. Dessa maneira, as pessoas são menos suscetíveis a serem dissuadidas de sua posição, e estando elas envolvidas com segurança, essa posição é estar do lado da segurança dos seus dados.

Existem outros tipos de cuidado, mas que são mais desprezíveis pelas pessoas. A capacidade de lidar com estresse e autoconfiança são alguns exemplos. Pessoas menos submissas tendem a lidar melhor com estresse e possuem razoável autoconfiança. Lidar com estresse e autoconfiança, são habilidades que podem ser ensinadas, ou pelo menos, melhoradas. Treinamentos desse tipo são usados para melhorar a conduta, auto estima, dentre outras qualidades, das pessoas.

Também é importante para as empresas manter seus funcionários atualizados e principalmente estimulados. Funcionários desestimulados são um grande perigo para a segurança dos dados. Isso porque eles passam a não se preocupar mais com a empresa e num momento de raiva podem acabar divulgando senhas, brechas ou até mesmo excluindo dados importantes.

Conclusão

A segurança da informação deve estar sempre em primeiro plano, tanto segurança física quanto lógica. Porém, a engenharia social se concentra no lado mais fraco dos sistemas computacionais, os seres humanos. Somos suscetíveis a erros.

Talvez por não vermos os bits e bytes sendo transferidos e não percebermos que pessoas podem estar de olho em nossas informações, acabamos não dando valor a pequenas atitudes. Estas atitudes podem ser desde a definição de uma senha forte à omissão de certos dados em redes sociais, por exemplo.

Existem vários tipos de ataques. Para cada um deles, existe uma forma de se prevenir. Mas todas as pessoas, sem exceção, são alvos potenciais desse tipo de ataque, ou seja, não existe um grupo específico que seja alvo. Por isso, não há como afirmar que nossos dados estarão sempre seguros. As empresas podem diminuir o risco treinando seus funcionários. Já para outras pessoas, é necessário cuidado, conscientização e informação. O uso bem feito da informação é o que faz a diferença.

Referências

BRENNER, Susan “The Psychology of Social Engineering”

POPPER, Marcos Antônio e BRIGNOLI, Juliano Tonizetti “Engenharia Social, um perigo eminente” – Instituto Catarinense de Pós Graduação - ICPG

GRANGER, Sarah “Social Engineering Fundamentals, Part I: Hacker tatics” – http://online.securityfocus.com/infocus/1527.

GRANGER, Sarah “Social Engineering Fundamentals, Part II: Combat strategies” – http://online.securityfocus.com/infocus/1533.