Boas práticas em Cibersegurança

Engenharia Social: por que se importar?

Conheça os números, os males e as contramedidas a esta perigosa estratégia de ataque

Outubro de 2015. Segunda quinzena do mês. O nova-iorquino New York Post foi o primeiro a publicar o acontecido. Diversos outros veículos, como o Guardian, a CNN, a Forbes e a Wired, não tardaram a contar suas próprias versões da história.

Após descobrir que John Brennan, à época diretor da CIA, era cliente da Verizon, um grupo de crackers, alguns ainda no ensino médio, conseguiu ludibriar funcionários da empresa de forma a obter dados pessoais do homem.

Pouco depois, sabendo que o e-mail pessoal de Brennan era da AOL, entraram em contato com a empresa e, usando a informação roubada da Verizon, coagiram os funcionários do provedor de e-mail a reiniciar a senha da conta. Estava feito o estrago.

Ainda que o sucesso da invasão à conta de e-mail pessoal de John Brennan seja discutível, há evidências que levam a crer que os crackers, de fato, conseguiram fazê-lo.

Se o chefe da mais proeminente agência de inteligência do mundo é passível de ataques dessa natureza, o que dizer de nós?

Gente comum

Infelizmente, ataques de engenharia social não atingem apenas ocupantes de cargos estratégicos em países distantes. A mazela é muito democrática.

Se olharmos apenas para phishing (um ataque de engenharia social muito comum, que consiste em coagir pessoas a clicar em links enganosos de maneira a expor informação privilegiada) veremos que, em 2016, segundo o Kaspersky Lab, 27,61% do total global de ataques desse tipo aconteceu no Brasil, sendo que o sistema anti-phishing de clientes da Kaspersky foi acionado, em todo o mundo, quase 155 milhões de vezes no ano.

> Se olharmos apenas para phishing [...] veremos que, em 2016, [...] 27,61% do total global de ataques desse tipo aconteceu no Brasil.

IsYourDataSafe.com atesta que o mercado de informação roubada movimentou, em 2013, mais de 143 bilhões de dólares. Outra fonte, o Ponemon Institute, alega que o custo médio anual, entre empresas com mais de 10 mil funcionários, para conter ataques de phishing que comprometeram credenciais de empregados, é de mais de 380 mil dólares.

Boas práticas em Cibersegurança

Definições

No livro Unmasking the Social Engineer, da Wiley, Christopher Hadnagy define engenharia social assim (adaptado):

> *Any act that influences a person to take an action that may or may not be in their best interest.*

Segundo essa definição, influenciar diretamente uma pessoa a executar uma ação qualquer é o que define engenharia social. O conceito é muito abrangente: por exemplo, um cachorro de porte grande, latindo e correndo obstinadamente em direção a um pobre infeliz, levando-o a correr desesperadamente em sua própria defesa, pode ser classificado como engenheiro social. Nesse caso, o indivíduo atemorizado estaria sendo coagido a executar uma ação em seu próprio interesse.

Até mesmo uma criança recém-nascida, através do choro, influencia os pais a executarem ações e é influenciada por eles de diversas maneiras. A engenharia social, portanto, seria algo nato. É interessante notar que essa definição assume que o engenheiro social é uma entidade ativa no que diz respeito a influenciar as ações de terceiros.

Outra definição possível e menos genérica é a do livro Introdução ao Hacking e aos Testes de Invasão, de Patrick Engebretson, publicado no Brasil pela Novatec, que define engenharia social assim (adaptado):

> *É o processo de explorar as fraquezas "humanas" inerentes a toda organização, com o objetivo de fazer com que um funcionário divulgue informação confidencial.*

Aqui já aparecem os conceitos de recurso humano e de organização. O engenheiro social exploraria a natureza humana de uma organização para conseguir informação privilegiada. No entanto, note que a definição não explicita a necessidade de influência ativa. O engenheiro social apenas se beneficiaria de fraquezas humanas. Que fraquezas são essas? A próxima definição esclarece esse ponto.

Boas práticas em Cibersegurança

Esta é do curso online CompTIA Security+ Certification SYO-401, da Udemy (transcrito):

> *Exploiting the trusting nature of people to gather information or access.*

Essa terceira definição torna claro que a fraqueza explorada pelo engenheiro social é a confiança nata das pessoas. Ademais, vai além de dizer que o engenheiro social deseja obter informação, expandindo o objetivo à obtenção de acesso e, novamente, não cita a necessidade de influência ativa.

Baseado nas três definições aqui expostas, podemos enunciar nossa própria definição de engenharia social:

> Coagir pessoas a executar ações ou aproveitar-se de ações livremente executadas para conseguir acesso a informações ou áreas reservadas, físicas ou virtuais.

Com isso, conseguimos contemplar tanto ataques baseados em influência ativa, como phishing, quanto ataques como dumpster diving (coleta de informação no lixo), de natureza passiva no que diz respeito à influência sobre pessoas e, ainda, tanto informação quanto acesso físicos e digitais.

Fugindo agora da definição, de que maneiras um engenheiro social pode, efetivamente, agir? Infelizmente, as instâncias reais de engenharia social são diversas.

Ataques

Vamos supor a existência de dois personagens: Joãozinho e Mariazinha. Ambos trabalham em uma multinacional. Seus perfis são muito diferentes. Joãozinho vive metido em toda sorte de trambiques. É um vigarista e está insatisfeito com a corporação. Mariazinha, por sua vez, é um doce de pessoa e uma funcionária exemplar.

No ápice de sua insatisfação, Joãozinho resolve atacar a empresa e, apesar de não ter o conhecimento técnico que seria necessário para conduzir um ataque eletrônico, ele é muito "bom de papo" e conhece a instituição razoavelmente bem. Abaixo, quatro "historinhas" possíveis do ataque de Joãozinho são contadas. Todos os ataques descritos são baseados em engenharia social.

Peralis
IT Innovation

Boas práticas em Cibersegurança

Tailgating

Joãozinho sabe que em determinado recinto restrito da empresa há informação que lhe renderia alguns milhares de dólares no mercado negro. O problema é que ele não tem o nível de privilégio necessário para adentrar o recinto: seu crachá "não passa".

Então, ele se posiciona próximo à porta, à espera de uma pessoa com cara de boba. Mariazinha, que trabalha justamente no dito recinto e tinha saído para ir buscar uma xícara de café com leite na copa, aproxima-se de Joãozinho no corredor e, em meio a um simpático sorriso, deseja ao nosso trambiqueiro o mais musical "bom dia". A vítima perfeita.

Joãozinho, depois de retribuir com um "bom dia" mais musical ainda, joga uma conversa mole para o lado da moça sorridente. Em meio a gracejos e sorrisos, diz que esqueceu seu crachá e pergunta se Mariazinha faria a gentileza de deixar ele entrar junto com ela. Esta, muito prestativa, diz que "sim, claro" e assim o faz. Está consumado um ataque de tailgating.

Tailgating é adentrar indevidamente recintos cujo acesso é restrito, explorando a boa vontade de pessoas que têm acesso legítimo. Aliás, o atacante nem precisa explorar a prestatividade de terceiros: pode aproveitar a fração de segundo antes do fechamento de uma porta controlada para passar por ela. Obviamente, isso seria muito mais suspeito, se constatado.

Dumpster diving

Terça-feira. 17:30. Já era hora de Mariazinha ir embora. Precisava passar no banco antes das 18:00 para pagar uma conta. Era o dia do vencimento. Por isso, não perdeu tempo triturando os rascunhos de um documento confidencial que redigira mais cedo. Simplesmente amassou os papéis antes de jogar tudo no lixo e ir embora.

Quarta-feira. Seu Marquinhos, o zelador, por volta das 9 da manhã, como de costume, joga fora um sacolão de papéis usados, depositando-o em uma caçamba que fica ao lado do prédio da empresa. Joãozinho, astucioso, sabe desse hábito do metódico zelador. Por volta das 9:15, desce até a portaria e, aproveitando um momento em que não havia ninguém no estacionamento, recolhe o sacolão e o coloca no espaçoso porta-malas de seu carro.

Mais tarde, já em casa, garimpando o material retirado do saco de lixo, encontra uma porção de cópias amassadas de um documento confidencial, que alguém tinha jogado fora sem triturar. Examinando melhor o conteúdo dos papéis, descobre que eles contêm (bingo!) credenciais de rede temporárias com alto nível de privilégio, a serem disponibilizadas a consultores que prestariam um serviço à corporação dali a alguns dias.

Não poderia ser mais simples: dumpster diving consiste em procurar, no lixo, por informação privilegiada descartada inadequadamente.

Boas práticas em Cibersegurança

Shoulder surfing

Joãozinho sabe que Mariazinha tem acesso a determinado sistema. Por razões hediondas, também deseja ter acesso a ele. A questão é que não há motivos razoáveis para que o pessoal da concessão de acessos aprove isso. Ademais, acessar o sistema com as credenciais de outra pessoa facilitaria muito a tarefa de mascarar as fraudes que porventura quisesse cometer.

Depois de descobrir que Mariazinha é um doce de pessoa, aproxima-se dela em um momento em que ela não aparenta estar muito ocupada e, entre sorrisos e mentiras, pede que ela faça a gentileza de verificar qualquer coisa para ele no sistema. Não querendo desapontar o simpático interlocutor, Mariazinha, imediatamente, faz que sim e começa a digitar suas credenciais para fazer login no tal sistema.

Joãozinho, incrivelmente discreto e astuto, memoriza as credenciais que a moça digita. Depois que ela lhe apresenta o que pedira, agradece educadamente e se vai. Sucesso. Mais tarde, utilizaria as credenciais roubadas para se autenticar como se fosse Mariazinha.

Conforme o exemplo descreve, ataques de shoulder surfing consistem em obter informação confidencial "espiando" o que a vítima está fazendo no computador.

Impersonation

"Bom dia, você que é a Mariazinha?", pergunta o homem de terno, levemente inclinado para a frente, braços apoiados um sobre o outro, como que cruzados, na mureta da baia. Mariazinha diz que "sim, sou eu". O homem se identifica: era Zezinho, o supervisor de compras. Viera falar diretamente com Mariazinha porque precisava de uma informação urgente. Estava fechando a documentação necessária à auditoria que ia acontecer na segunda e alguns valores, justo os que Mariazinha declarara, não estavam batendo.

Ele pergunta se Mariazinha poderia abrir o SAP para ver, junto com ele, o que de fato deveria ser declarado. De certo a moça cometera algum erro. Mariazinha, não querendo pôr a auditoria a perder, prontamente concorda com o circunspecto supervisor e pede que ele se sente ao lado dela, para conferirem os valores. Juntos fazem os cálculos, o homem anota as informações de que precisa, agradece, toma o cafezinho que Mariazinha oferece, apressado, e depois vai embora. Sucesso.

Joãozinho, nosso talentoso engenheiro social, se fizera passar por Zezinho, supervisor de compras, para obter informação privilegiada. Impersonation consiste em se passar por terceiros para obter vantagens, muitas vezes recorrendo à forja de situações urgentes ou colocando alguma pressão sobre a vítima.

Diversos outros tipos de ataque compõem o arsenal do engenheiro social, como phishing, hoaxing, whaling, water holing, etc. Ataques dessa natureza estão, comumente, ligados à prestatividade e à confiança nata das vítimas e, ainda, a algum conhecimento de processos internos. A interação social, quase sempre, é um elemento-chave na condução de um ataque de engenharia social bem sucedido.

> Ataques dessa natureza estão, comumente, ligados à prestatividade e à confiança nata das vítimas e [...] A interação social [...] é um elemento-chave [...]

Boas práticas em Cibersegurança

Contramedidas

Apesar de contramedidas de segurança física serem as mais evidentes no combate à engenharia social, a educação do usuário, sem dúvida, é o caminho ao sucesso corporativo no que diz respeito à segurança da informação. Aliás, atualmente, é imprescindível que usuários domésticos também tenham conhecimento em Cibersegurança. O cibercrime está em todo lugar e a sua principal "vantagem competitiva" atualmente é a desinformação do público geral.

Apesar de contramedidas de segurança física serem as mais evidentes no combate à engenharia social, a educação do usuário, sem dúvida, é o caminho ao sucesso corporativo no que diz respeito à segurança da informação. Aliás, atualmente, é imprescindível que usuários domésticos também tenham conhecimento em Cibersegurança. O cibercrime está em todo lugar e a sua principal "vantagem competitiva" atualmente é a desinformação do público geral.

> [...] a educação do usuário, sem dúvida, é o caminho ao sucesso corporativo no que diz respeito à segurança da informação.

Quando se fala de segurança, mais do que educar o usuário, uma corporação bem-sucedida no quesito é uma organização onde impera uma sólida cultura de segurança da informação. Isso é algo extremamente difícil de atingir, simplesmente porque vai de encontro à confiança intrínseca que temos uns nos outros. A insistência no tema, sem dúvida, é uma das armas mais importantes das pessoas cuja responsabilidade é zelar pela segurança corporativa.

Este artigo foi publicado originalmente por seu autor no LinkedIn e utilizado neste material com a devida autorização.

A publicação original pode ser lida aqui.