INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO – Campus Paracatu

CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

NATAN LIMA FERREIRA FERNANDES DE SOUSA

ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO

PARACATU, MG

2016

NATAN LIMA FERREIRA FERNANDES DE SOUSA

ENGENHARIA SOCIAL NA SEGURANÇA DA INFORMAÇÃO

Trabalho requisito parcial para conclusão da disciplina de Segurança de Redes do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas no Instituto Federal do Triângulo Mineiro, Campus Paracatu.

Orientador: Prof. Roitier Campos Gonçalves

PARACATU, MG

2016

SUMÁRIO

1 INTRODUÇÃO

A informação é o elemento básico para que a evolução aconteça e o desenvolvimento humano se realize de forma completa (COURY, 2001). Conforme Campos, (2007, p. 21) "A informação é elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor". Portanto pode-se afirmar que a informação é elemento mais valioso de uma corporação, sendo alvo constante de ameaças. Deste modo, é fundamental a implantação de políticas de segurança da informação com o objetivo de reduzir ou evitar vulnerabilidades e prejuízos, chances de fraude ou perda de informações.

A Engenharia Social entende a inaptidão dos usuários nas áreas pertinentes a tecnologia da segurança da informação como o elemento mais vulnerável de qualquer sistema de segurança da informação. Pelo fato de não estarem cientes do valor da informática, não lhes dão devida preocupação.

2. ENGENHARIA SOCIAL

A Engenharia Social, não sendo particular da área da informática, é uma ferramenta na qual são exploradas falhas humanas em organizações, tanto físicas quanto jurídicas.

Um engenheiro social não é um profissional da engenharia social, mas sim uma pessoa que possui conhecimento em diversas áreas, visto que não é uma faculdade, e sim um agrupamento de técnicas. Os ataques da engenharia social podem ser divididos em dois grupos:

2.1 ATAQUES DIRETOS

Os ataques diretos, como propriamente nomeados, são definidos pelo contato direto entre o engenheiro social e a vítima. Este contato se dá por meio de telefonemas, e-mails, mensagens de texto e até mesmo pessoalmente. O que exige do engenheiro, meticulosidade;

um planejamento prévio detalhado, articulação e criatividade para o sucesso do plano. Além de sempre haver de possuir um plano reserva para o caso de falha na operação do primeiro.

2.2 ATAQUES INDIRETOS

Estes ataques são caracterizados pela utilização de meios indiretos entre o engenheiro e a vítima, como o uso de ferramentas e técnicas de invasão ou softwares prejudiciais como vírus ou sites e emails falsos no intuito de obter as informações desejadas.

A figura abaixo exemplifica o ciclo de ataque da engenharia social, compreendido em quatro etapas: reunir informações, desenvolver o relacionamento com a vítima, exploração e execução. (ALLEN, 2006, p.5)

Figura 1 - O ciclo
Fonte: (ALLEN, 2006)

3. INFORMAÇÃO E SUA SEGURANÇA

3.1 A INFORMAÇÃO

"A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos,

apresentada em filmes ou falada em conversas" (ISO/IEC 27002:2005, 2005). Seja qual for a forma em que ela é armazenada, a informação é um conjunto de dados, que processados geram uma informação. Conforme a ISO/IEC 27002:2005(2005), um dado não tem valor antes de ser processado, mas a partir do seu processamento, ele passa a ser considerado uma informação, esta que gera conhecimento. A informação é um ativo que como qualquer outro, é crucial para uma corporação, e deve ser propriamente protegida. A informação é tida como um dos, senão o recurso mais importante de uma organização.

3.2 SEGURANÇA DA INFORMAÇÃO

Ao se falar em segurança da informação, deve ser levado em consideração três conceitos básicos (confidencialidade, integridade e disponibilidade), pois toda ação que venha a comprometer um destes, estará atentando contra a segurança.

3.2.1 CONFIDENCIALIDADE

A partir de um momento em que a informação esteja disponível, de certa forma, para uma pessoa não autorizada, intencionalmente ou não, acontece a quebra de confidencialidade.

3.2.2 INTEGRIDADE

Ocorre a quebra de integridade quando a informação é alterada, falsificada ou furtada. A integridade é garantida quando a informação é sempre mantida em seu formato original.

3.2.3 DISPONIBILIDADE

É a garantia de que a informação estará sempre disponível quando necessária. Quando acontece de a informação não estar disponível, seja tanto por causa de um ataque ou invasão, quanto por motivo de servidores inoperantes, é considerada uma quebra de disponibilidade, mesmo interrupções involuntárias, não intencionais.

4. TIPOS DE VULNERABILIDADES

Segundo Peixoto (2006), os tipos de vulnerabilidades existentes podem ser do tipo físicas, naturais, por hardware, por software, mídias, comunicação e humanas.

- **Físicas**: Compreendem as vulnerabilidades físicas salas de centro de processamento de dados mal planejadas, estrutura de segurança fora dos padrões exigidos.
- **Naturais**: Máquinas são sempre propícias à sofrer danos de causas naturais como umidade, fogo, sujeira, além de cortes de energia e temperatura.
- **Hardware**: Deterioração, obsolescência ou mau uso.
- **Software**: Erros de configuração, vazamento de informações, perda de dados ou indisponibilidade de recursos.
- **Mídias**: Mídias físicas como CDs podem ser facilmente perdido ou danificados, muitas vezes de forma irreparável.
- **Comunicação**: Acessos não autorizados ou perda de comunicação.
- **Humanas**: Como por exemplo, por meio das técnicas de engenharia social, as vulnerabilidades são encontradas na falta de treinamento, conscientização ou o não seguimento das políticas de segurança pelos operadores.

Ainda segundo Peixoto (2006, p. 39), "Infelizmente ainda não é da cultura de nosso país as empresas adotarem potencial investimento em segurança digital mais especificamente na segurança das informações."

5. O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO

O "fator humano", em qualquer organização sempre será o elemento mais vulnerável na segurança. Os maiores engenheiros sociais tiram proveito das fraquezas ou gostos pessoais de suas vítimas para se aproximarem e alcançarem seus objetivos. (MARCELO; PEREIRA, 2005)

Um assunto grandemente discutido atualmente é a questão da necessidade do elemento humano como base da segurança da informação. O fator humano é uma das maiores

causas de invasões e ataques, como por exemplo, devido a um descuido básico com a segurança.

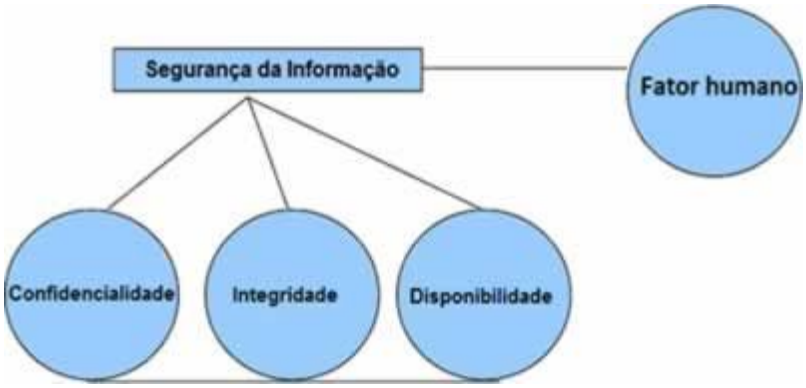

Figura 2 - Atual modelo da segurança da informação
Fonte: (SILVA, M; COSTA, 2009)

Figura 3 - Proposta de novo modelo para a segurança da informação.

Fonte: (SILVA, M; COSTA, 2009)

Existem propostas de modelos para a segurança da informação que incluem o primordial fator humano como um dos pilares fundamentais da informação, visto que o modelo atual o considera à um nível não base. (ALVES, 2010, p. 23)

5.1 VULNERABILIDADES

Pode-se destacar as seguintes características do ser humano que o torna vulnerável a ataques de engenharia social: (JUNIOR, 2006).

- O ser humano procura parecer prestativo e querer ajudar os outros quando necessário.
- Os humanos gostam de serem elogiados, o que muitas vezes os deixam à vontade para fornecer informações.
- Muitas vezes o ser humano se julga não ser o único responsável pelo conjunto de responsabilidades, assim, postergando de si a culpa a outrem.
- O ser humano possui características que o tornam facilmente vulneráveis a manipulação. É caracterizada pela capacidade de convencer, buscando assim respostas desejadas para alcançar o objetivo.

O funcionário insatisfeito, desmotivado ou desvalorizado é uma outra grande vulnerabilidade dentro da organização. (PRESCOTT, 2007)

6. O ENGENHEIRO SOCIAL

As técnicas utilizadas pelo engenheiro social se baseia na exploração da ingenuidade dos usuários e da persuasão, trabalhando psicologicamente a vítima utilizando de identificações falsas, carisma e outras formas de ganhar a confiança. O engenheiro social é dotado de um enorme poder de criatividade (ALVES, 2010).

E conforme Araújo (2005), o engenheiro social geralmente é uma pessoa agradável. Educado, simpático, carismático, mas sobretudo criativo, flexível e dinâmico.

O engenheiro social, muitas das vezes, sequer precisa encontrar a vítima pessoalmente para conseguir o que deseja. Boa parte dos ataques pode ser feita por meio de um simples telefonema, sem nem mesmo ter ideia de como a vítima se parece.

Grandes prejuízos já foram causados a empresas por causa do senso de confiança de pessoas e empresas. Uma dessas ações foi parar até mesmo no “Guinness, o Livro dos Recordes”. Stanley Mark Rifkin, o responsável pelo ataque, consultor de banco, conseguiu

roubar US$ 10,2 milhões por meio de uma transferência bancária feita com telefonemas, em 1978.

6.1 COMO AGE O ENGENHEIRO SOCIAL

O ambiente de trabalho pode ser uma fonte de informações importantes ou confidenciais apenas bastando um olhar atento. A maior parte das empresas reaproveita folhas para novas impressões. Apesar de ser uma prática de economia e preocupação ambiental, não é raro encontrar na pilha de papeis reaproveitados que possam ter informações confidenciais. Pode ser ainda que se encontre até folhas com a palavra "CONFIDENCIAL" no cabeçalho.

O telefone é a principal e preferida ferramenta dos engenheiros sociais. É possível conseguir informações confidenciais e acesso a pessoas importantes da organização com uma simples ligação.

Conforme Felipe Arruda, em sua matéria sobre Engenharia Social no TecMundo, É comum os engenheiros sociais também usarem e-mails ou chats para arrancarem dados ou manipularem alguém. "Um truque comum é o engenheiro social tentar se passar por administrador da rede ou técnico de um serviço que possa estar apresentando "problemas". Com essa abordagem, pode ser que ele consiga o usuário e a senha da vítima. E já que muitas pessoas costumam usar a mesma senha para diversos perfis online, o agressor acaba tendo acesso a uma grande quantidade de informações pessoais da vítima".

Todos os métodos mencionados só funcionam perfeitamente se o engenheiro social explorar as fraquezas psicológicas do ser humano. Truques são utilizados para isso, um destes, por exemplo, é colocar a vítima numa situação em que ela se veja subordinado a um procedimento, como exemplo, abordar um funcionário da empresa pedindo para que ele responda um formulário que todos no setor já responderam, e que só falta ele. O que dificilmente seria recusado.

REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, Malcon. **Social Engineering:** A Means to Violate a Computer System. SANS Institute InfoSec Reading Room, 2006. Disponível em <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529>. Acesso em: 5 nov. 2016.

ALVES, Cássio Bastos. **Segurança da Informação vs. Engenharia Social**: Como se proteger para não ser mais uma vítima. Centro Universitário do Distrito Federal, 2010.

ARAUJO, Eduardo E. **A Vulnerabilidade Humana na Segurança da Informação.** Faculdade de Ciências Aplicadas de Minas, 2005.

CAMPOS, André. **Sistema de Segurança da Informação:** Controlando os Riscos. 2. ed. Florianópolis: Visual Books, 2007.

CARDOSO, Fabio Eder; DE OLIVEIRA, Paulo Cesar. **Política de Segurança da Informação nas Empresas.** Faculdade de Tecnologia de Ourinhos, 2013.

COURY, Wilson Biancardi. **Poder e Informação.** Disponível em <http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=424> Acesso em: 6 de nov. 2012.

JUNIOR, Guilherme. **Entendendo o que é Engenharia Social.** 2006. Disponível em: <http://www.vivaolinux.com.br/artigo/Entendendo-o-que-e-Engenharia-Social>. Acesso em: 6 nov. 2016.

MARCELO, Antonio; PEREIRA, Marcos. **A Arte de Hackear Pessoas.** Brasport**,** Rio de Janeiro, 2005.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Brasport, Rio de Janeiro, 2006.

PRESCOTT, Roberta. **Fator Humano:** Um dos Pilares da Segurança da Informação. 2007. Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=41990>. Acesso em: 8 nov. 2016.

SILVA, Maicon H. L. F. da; COSTA, V. A. de S. F. **O Fator Humano Como Pilar da Segurança da Informação:** Uma proposta alternativa. 2009. Disponível em: <http://www.eventosufrpe.com.br/jepex2009/cd/resumos/R0052-3.pdf>. Acesso em: 6 nov. 2016.

ARRUDA, Felipe. Matéria do Tecmundo: **Engenharia Social:** o malware mais antigo do mundo. 2011. Disponível em: <http://www.tecmundo.com.br/seguranca/8445-engenharia-social-o-malware-mais-antigo-do-mundo.htm>. Acesso em: 8 nov. 2016.