Segurança da Informação: Engenharia Social nas Organizações

FREITAS, Caio Guimarães de [1]

FREITAS, Caio Guimarães de. **Segurança da Informação: Engenharia Social nas Organizações.** Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 03, Ed. 04, Vol. 04, pp. 116-124, Abril de 2018. ISSN:2448-0959

Resumo

A engenharia social utiliza técnicas para explorar a vulnerabilidade ocasionada pelo o fator humano no intuito de driblar as barreiras de segurança tecnológicas cada vez mais avançadas. O presente artigo tem o objetivo geral de apresentar o aspecto da engenharia social na segurança da informação. Analisando as técnicas utilizadas por atacantes que utilizam de engenharia social obter informações sensíveis, bem como as contramedidas que podem ser implementadas no intuito de mitigar tais ameaças à segurança da informação. Dentre os autores pesquisados para a constituição conceitual deste trabalho, destacaram-se Silva (2015), Casaca (2014), Weidman (2014), Reynolds (2016) e Kratikal (2017). A metodologia utilizada foi a pesquisa descritiva, tendo como coleta de dados o levantamento bibliográfico. As conclusões mais relevantes são que é fundamental ter em mente que a segurança da informação depende totalmente do fator humano de modo que se este for negligenciado pode trazer prejuízos as organizações tornando inúteis os investimentos feitos em tecnologia para segurança da informação.

Palavras-chave: Engenharia Social, Segurança da Informação, Organizações.

Introdução

A Informação pode ser considerada um dos ativos de maior valor para empresas e demais organizações, isso faz com que as informações possam ser alvo de pessoas mal-intencionadas.

Muitas organizações as organizações costumam relegar a responsabilidade pela segurança da informação apenas aos seus setores de informática fazendo investimentos em produtos como antivírus, firewalls, entre outros produtos tecnológicos de última geração, acreditando que isso protegerá a segurança de suas informações de ataques hackers.

Acontece que pessoas mal-intencionadas podem obter informações sensíveis das organizações de diversas maneiras, incluindo métodos que não se utilizem de meios informáticos para tal.

Nesse contexto as organizações costumam negligenciar a importância do fator humano na segurança da informação, ignorando que o comportamento dos empregados e demais colaboradores tem um grande impacto na segurança.

Faz-se necessário, portanto, a tomada ações no sentido de garantir a segurança dessas informações levando em consideração não apenas os aspectos tecnológicos, mas também o aspecto humano.

Nesse cenário se insere a engenharia social como uma tentativa explorar a vulnerabilidade ocasionada pelo o fator humano no intuito de driblar as barreiras de segurança tecnológicas cada vez mais avançadas.

O presente artigo tem o objetivo geral de apresentar o aspecto da engenharia social na segurança da informação. Delimitando-se a analisar as técnicas utilizadas por atacantes que utilizam de engenharia social obter informações sensíveis, bem como as contramedidas que podem ser implementadas no intuito de mitigar tais ameaças à segurança da informação.

Este trabalho justifica-se pela importância de se conhecer os métodos utilizados pela engenharia social para explorar a vulnerabilidade humana no intuito de obter informações sensíveis às organizações, bem como conhecer os meios que podem ser utilizados para prevenção contra tais tipos de ataque.

A metodologia deste trabalho é a pesquisa descritiva, tendo como coleta de dados o levantamento bibliográfico.

Segurança da informação: Engenharia Social

O ser humano é um dos elementos mais importantes ao se tratar sobre a segurança da informação. As

pessoas se relacionam diretamente com a informação visto que estão envolvidas com os processos de negócio, de modo que cada indivíduo é peça chave para manter a segurança da informação (SILVA, 2015).

Nesse contexto a engenharia social concerne a situações em que uma pessoa tem acesso a uma informação sensível ou obtém privilégios não autorizados de acesso a sistemas ou a locais por meio do estabelecimento de relações de confiança com elementos internos da organização. Ou seja, trata-se de manipular as pessoas para atingir um objetivo. A engenharia social relaciona-se mais à psicologia e à sociologia do que com a tecnologia (CASACA, 2014).

Todos os dias funcionários e colaboradores de organizações precisam lidar com informações, além disso, os meios que armazenam ou trafegam dados também são manipulados por pessoas. Com isso, para que a segurança da informação se torne possível, é necessário que as pessoas façam a sua parte com responsabilidade (SILVA, 2015).

As organizações devem procurar garantir que os colaboradores envolvidos compreendem suas responsabilidades no que concerne à segurança da informação, de modo a garantir a confidencialidade, integridade e disponibilidade da informação, visto que, de modo geral, as pessoas não apresentam um bom entendimento do funcionamento das normas de segurança da informação ou das ameaças a que estão vulneráveis (CASACA, 2014).

Pessoas mal-intencionadas podem estar vinculadas ou não a uma organização. Há também, o caso particular de funcionários que já foram desligados da organização, porém ainda podem representar uma forte ameaça à segurança da informação, uma vez que estes conhecem processos e sistemas da empresa. ?Pessoas que ainda estão vinculadas à organização, podem levar informações sensíveis ao público por vários motivos, seja para ganho financeiro, insatisfação, entre outras motivações?. Nas organizações pode-se encontrar pessoas de todos os perfis, por isso é importante que a segurança da informação de uma atenção especial àqueles que possuem acesso a processos organizacionais da instituição (SILVA, 2015).

Conforme Casaca (2014), é comum dizer que as pessoas são o elo mais fraco da segurança da informação, porém elas podem ser tanto o elo mais fraco quanto o elo mais forte da cadeia da segurança, também podem ser o único obstáculo ou a ferramenta menos segura para prevenção de incidentes indesejados.

Com a evolução tecnológica constante, o desafio de se garantir segurança da informação passa a ser ainda maior, especialmente quando envolve o ser humano, visto que abrange uma mudança cultural. Esta mudança cultural compreende tanto o convívio social quanto o profissional (SILVA, 2015).

Os ataques que utilizam engenharia social podem não requerer nenhuma tecnologia ou envolver requisitos

técnicos complexos. Um engenheiro social, procura explorar as vulnerabilidades humanas como a falta de conscientização a respeito de políticas de segurança ou até mesmo o desejo de ser prestativo com outras pessoas entre outros pontos (WEIDMAN, 2014).

Existem vários elementos responsáveis pela segurança da informação, o que inclui desde sistemas tecnológicos avançados até o ser humano. Silva (2015), afirma que o ser humano é o principal responsável pela garantia da segurança da informação, bem como o maior produtor de dados, os quais se tornam informações por meio dos sistemas. Por isso, a segurança não deve ser realizada somente por sistemas de informação.

O principal objetivo de um engenheiro social é conseguir informações pessoais de seu alvo. Essas informações podem servir para preparar um ataque mais intenso ou a execução de um roubo financeiro. Comumente, os engenheiros sociais encontram meios para instalar algum malware no sistema de empresas para obter acesso a dados pessoais, contas de computador e outras informações confidenciais (REYNOLDS, 2016).

Segundo Silva (2015), reportagens revelam diariamente a falta de interesse ao tema da segurança da informação por parte das organizações. Há ainda as ações de usuários negligentes que divulgam informações sigilosas em redes sociais, compartilham senha, acessam páginas não confiáveis, passam dados sigilosos via telefone, entre outras.

Os engenheiros sociais, por vezes, procuram algo que possam se traduzir em vantagem competitiva. Os itens mais comuns buscados pelos engenheiros sociais incluem informações pessoais, crachás de identidade, cartões de acesso, senhas, números de contas, detalhes de sistemas de computadores, listas telefônicas, informações sobre URLs não públicos, servidores e nomes de alvos com privilégios de acesso, entre outros (REYNOLDS, 2016). ?

Se não tiverem a formação adequada e sem ações de sensibilização em segurança as pessoas podem tornar-se o elo mais fraco da segurança da informação. Com isso as organizações acabam não conseguindo atingir os seus objetivos em matéria de conformidade com as normas. De outro modo colaboradores bem treinado podem tornar-se o elo mais forte da infraestrutura de segurança de uma organização (CASACA, 2014).

Vale destacar que o ser humano só pode atuar como parte fundamental na segurança da informação quando o mesmo ciente do valor dos dados e os riscos aos quais eles estão expostos. Isto é, para que os funcionários e demais colaboradores contribuam com a segurança da informação, eles precisam entender a importância da informação, quais seriam as possíveis consequências de uma informação sigilosa vir a público, ou de uma má utilização de uma informação sigilosa por alguém (SILVA, 2015).

Conforme Casaca (2014), a segurança é um problema das pessoas e não da tecnologia, visto que são as pessoas que controlam a tecnologia, além disso a tecnologia é desenhada para ser utilizada pelas pessoas e a maior parte das tecnologias de segurança são desenhadas para funcionarem em conformidade com um comportamento responsável por parte dos utilizadores, o que nem sempre acontece.

Há várias etapas na engenharia social, sendo que na maioria das vezes o ataque de engenharia social é composto de quatro passos que são: coleta de informações, desenvolvimento de uma relação, exploração e execução. Geralmente a conversa é uma cobertura concisa de todas as etapas que um atacante segue para realizar um ataque. O primeiro passo é a coleta de informações. O atacante primeiro coleta dados sobre o indivíduo ou sobre uma organização em particular como o nome de um empregado, costumes, número de telefone entre outros detalhes pessoais de alguma fonte aberta como organogramas da empresa (KRATIKAL, 2017).

Comumente os setores mais visados a serem alvo de engenharia social são as áreas onde os empregados têm acesso a informação confidencial, interagem com o público e não estão sensibilizados para as ameaças da engenharia social. Os funcionários mais expostos a esses ataques são secretários ou assessores, e administradores de redes ou de bases de dados. Os riscos relacionados com a engenharia social são bastante altos, considerando as suas peculiaridades e possíveis consequências. As medidas de segurança contra estes tipos de ataques devem ser tomadas, principalmente, com treinamentos e ações de sensibilização para conformidade do comportamento dos colaboradores com o estabelecido nas políticas e procedimentos (CASACA, 2014).

Depois de coletar as informações, o atacante começa a desenvolver uma relação com o alvo. Essa fase abrange ligações telefônicas, solicitações de amizade em redes sociais, encontros pessoais, etc. Ao desenvolver o relacionamento com a vítima, o atacante pode forjar uma identidade se utilizando de perfis falsos, por exemplo. O princípio dessa fase é reforçar a conexão e manter o diálogo aberto para fazer uso do relacionamento e conseguir a informação para a qual o contato foi iniciado (KRATIKAL, 2017).

Um dos aspectos humanos de que a engenharia social se utiliza é a reciprocidade. Em muitos casos, quando as pessoas recebem mimos, elas sentem a necessidade de retribuir. O tempo entre oferecer um presente e pedir um favor é crucial. Isso ocorre porque caso o atacante peça o favor imediatamente após dar um presente a vítima pode perceber que na verdade trata-se de um suborno. É possível que vítima aja desconfortavelmente quando se tornar ciente da situação. Deste modo, é comum que um engenheiro social de um presente, por exemplo, a um guarda ou recepcionista de um edifício pela manhã e a volte para pedir um favor pela tarde (REYNOLDS, 2016).

Depois que o atacante consegue conquistar a confiança do alvo, ele tira vantagem dessa confiança para convencer a vítima a executar as suas solicitações e então conseguir a informação confidencial que

geralmente as pessoas vão divulgar espontaneamente por educação. Dependendo do golpe em questão, isso pode levar alguns minutos ou alguns meses (KRATIKAL, 2017).

Existem diversas técnicas que podem ser utilizadas por um engenheiro social para atingir seus objetivos, essas técnicas podem utilizar tecnologia ou não. Por exemplo, uma técnica típica utilizada pela engenharia social é a chamada *Friending*. Essa técnica consiste em um engenheiro social ganhar a confiança da sua vítima e pedir para ela abrir anexos de e-mails ou links, que contêm malware. Assim que o atacante consiga acesso ao sistema corporativo e encontre sua vulnerabilidade por meio do malware, ele poderá começar a explorar. Como exemplo de um ataque sem utilização de tecnologia, uma pessoa poderia tentar se apresentar como um empregado de uma empresa terceirizada ou até mesmo forjar um crachá apenas para obter acesso em um prédio seguro. Essas ações podem ser quase imperceptíveis, um engenheiro social poderia, por exemplo, se oferecer para reparar a porta para um indivíduo que pertence a uma empresa ou fazer elogios a uma recepcionista para obter acesso ao prédio (REYNOLDS, 2016).

Outro exemplo comum de ataque acontece quando o help desk de TI recebe um telefonema desesperado de um suposto assistente de algum chefe na organização, que argumenta não estar conseguindo acessar seu email. Em situações como estas os funcionários tendem a ser solícitos. Deste modo, a não ser que haja uma política de segurança, o funcionário do help desk acabará passando a informação pelo telefone, mesmo que a pessoa que ligou não seja quem diz ser (WEIDMAN, 2014).

No último estágio de um ataque o engenheiro social utiliza a informação confidencial. Depois de conseguir a informação desejada o atacante sai de cena ou encerra a comunicação com a vítima sem deixa-la apreensiva (KRATIKAL, 2017).

A ação maliciosa dos ataques abrange, geralmente, de três tipos de atividades: fraude, roubo de informação ou sabotagem. Outras ações perpetradas por atacantes internos podem incluir espionagem, terrorismo, extorsão, suborno e corrupção. Estas ações maliciosas tornam os impactos dos ataques internos devastadores, tanto em termos financeiros, como no caso de fraude e roubo de informação, como em danos provocados aos sistemas e infraestrutura tecnológicas em sabotagens (CASACA, 2014).

Existem várias maneiras pelas quais evitar ameaças internas à uma organização, como políticas de acesso do usuário. Todos os funcionários da organização devem saber que existem políticas e ações de segurança que devem ser impostas e podem haver penalidades severas por infrações. Deve haver um procedimento específico para determinar como o acesso é concedido tanto a sistemas quanto a instalações. O procedimento deve indicar quem está autorizado a aprovar o acesso e quem pode aprovar quaisquer exceções. Nenhum indivíduo deve ter excesso de privilégio do que o necessário para realizar suas tarefas. As informações da empresa devem ser protegidas. Uma política deve ser implantada declarando que ninguém está autorizado a fornecer qualquer informação que seja mais do que necessária (KRATIKAL,

2017).

O engenheiro social pode tentar confundir as pessoas, como fingir que esqueceu alguma coisa em uma das salas do prédio após uma reunião. É provável que o guarda ou a recepcionista deixem o engenheiro social entrar no local. Para evitar que algo assim aconteça, os funcionários devem ficar céticos. Na maioria dos casos, os engenheiros sociais passam semanas para estabelecer as bases para estabelecer um relacionamento recíproco com seus alvos, levando-os a ter acesso a áreas seguras ou sensíveis (REYNOLDS, 2016).

Outra maneira de proteger as informações sensíveis da organização contra engenharia social, como exemplo, a empresa deve estabelecer políticas em que o papel de qualquer função importante seja fornecido a um grupo de pessoas, de modo que nenhuma delas possa saber exatamente o processo de negócio completo da organização. Esse método é conhecido como compartimentação de dados, pois ninguém realmente tem acesso ao conjunto completo de dados. Todo funcionário tem acesso apenas a informações limitadas (KRATIKAL, 2017).

A engenharia social utiliza táticas psicológicas básicas que os atacantes empregam para obter a confiança de seus alvos e então conseguir o que desejam. É necessário que conhecer os princípios subjacentes da engenharia social para que seja mais fácil reconhecer e prevenir ameaças desse tipo (REYNOLDS, 2016).

As organizações devem desenvolver em seu colaborador a consciência a importância da proteção da informação para os negócios. Deste modo, faz-se necessário oferecer treinamentos constantes a respeito do uso correto dos sistemas de informação adotados pela empresa. É necessário que sempre que possível a organização promova eventos que apresentem aos funcionários a importância da segurança da informação, os riscos a que tais dados estão expostos podem representar e qual a melhor forma de manipular as informações organizacionais. ?Vazamentos de informações corporativas geralmente vêm a público através de funcionários descuidados (SILVA, 2015).

Organizações devem investir tempo e esforço no treinamento de seus colaboradores no que concerne aos ataques de engenharia social. Independentemente do tipo de tecnologia de segurança implantado, eles terão acesso a informações sensíveis ou a controles de segurança que, em mãos erradas podem prejudicar a organização. Algumas orientações dadas em treinamentos de segurança podem ser óbvias como “não compartilhe sua senha com ninguém”. Outras orientações quanto à segurança podem ser novidade para muitos funcionários (WEIDMAN, 2014).

A intenção dos cursos é fornecer conhecimento às partes interessadas para proteger os sistemas de informação e dados sensíveis de ameaças internas e externas. A Engenharia Social é considerada a forma mais difícil de ataque para se defender porque não pode ser defendida com qualquer hardware ou

software sozinho. Uma defesa bem-sucedida depende da implementação de boas políticas e da educação dos funcionários para seguir essas medidas (KRATIKAL, 2017).

Conclusão

Este estudo tem o objetivo geral de apresentar o aspecto da engenharia social na segurança da informação. Ao realizar a análise das técnicas utilizadas por atacantes que utilizam de engenharia social para obter informações das organizações, pode-se observar que existem diversas técnicas sistemáticas de ataques para manipular potenciais vítimas através de engenharia social, com ou sem a utilização de ferramentas tecnológicas. Além disso pode-se observar que o fator humano pode representar uma vulnerabilidade que pode ser explorada com facilidade através da engenharia social, se não houver medidas de prevenção adequadas.

Ao analisar as contramedidas que podem ser implementadas no intuito de mitigar tais ameaças à segurança da informação observa-se que dever haver ciência por parte da alta direção de que a segurança da informação não se restringe a ataques tecnológicos, bem como deve haver conscientização por parte dos empregados de que eles têm um papel fundamental na garantia de segurança da informação.

Portanto é importante ter em mente que a segurança da informação depende totalmente do fator humano, de modo que se este for negligenciado, pode trazer prejuízos as organizações tornando inúteis os investimentos feitos em tecnologia para proteger a informação de ataques através dos meios informáticos. Os avanços nas técnicas de ataque à segurança da informação são frequentes, de modo que as medidas de segurança atuais podem vir a tornar-se obsoletas posteriormente. Com isso, novos trabalhos podem ser realizados no sentido de apresentar os avanços e inovações nas contra medidas para garantir a segurança da informação.

Referências

SILVA, C. A. **O Elo Mais Fraco da Segurança da Informação:** Pessoas Representam o Maior Desafio. Edição do Kindle, 2015.

KRATIKAL, A. **Social Engineering**: The Art Of Exploitation (V Book 1). Edição do Kindle, 2017.

WEIDMAN, G. **Testes de Invasão**: uma introdução prática ao hacking. São Paulo, Novatec Editora Ltda, 2014, ISBN: 978-85-7522-407-6.

CASACA, J. A. **Gestão do Risco na Segurança da Informação:** Conceitos e Metodologias. Createspace Independent Pub, 2014, ISBN: 978-1497450110.

REYNOLDS, V. **Social Engineering**: The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception. 2 ed. Vince Reynolds, 2016.

[1] Graduado na Área de Computação, atua como servidor público na Suframa no cargo de Analista Técnico Administrativo – TI.