ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 2/2022

JOSUÉ FERREIRA DE MELLO AZEREDO, Cap Inf

A implementação de um Programa de Conscientização em Cibersegurança na FAB

Rio de Janeiro

2022

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 2/2022

JOSUÉ FERREIRA DE MELLO AZEREDO, Cap Inf

A implementação de um Programa de Conscientização em Cibersegurança na FAB

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica como requisito parcial para aprovação no Curso de Pós-graduação *Lato Sensu* em Liderança com Ênfase em Gestão no COMAER.
Linha de Pesquisa: Guerra Cibernética
Orientador: Israel Cordeiro dos Santos Rocha, Maj Eng

Rio de Janeiro
2022

JOSUÉ FERREIRA DE MELLO AZEREDO, Cap Inf

A implementação de um Programa de Conscientização em Cibersegurança na FAB

Trabalho de conclusão de curso apresentado no Curso de Aperfeiçoamento de Oficiais da Aeronáutica.

Aprovado por:

_____

Israel Cordeiro dos Santos Rocha, Maj Eng
EAOAR

_____

Alexandra Vidal Pedinotti Zuma, Cap Farm
EAOAR

Rio de Janeiro

2022

RESUMO

As pessoas, enquanto usuários inseridos no ciberespaço, estão sujeitas a ataques de engenharia social que podem causar danos, caso sejam bem sucedidos. O COMAER implementou sua rede interna de protocolos e serviços que, se utilizada por usuários desatentos quanto às ameaças que os cercam, representa um ponto de vulnerabilidade e risco à segurança das informações. Esses usuários podem ser persuadidos a colaborarem com um ataque de engenharia social, sem se darem conta disso. Assim, o presente ensaio defende que um Programa de Conscientização em Cibersegurança direcionado aos militares no âmbito do COMAER, com ênfase em ataques de engenharia social, reduz a vulnerabilidade cibernética causada pelo fator humano. Para embasar essa tese, primeiramente é abordado que o Programa ensinará aos militares as formas de ataques e os riscos a que estão expostos, provendo o conhecimento necessário, tornando-os mais aptos a reconhecer os ataques. Posteriormente, é defendido que o Programa contribuirá para a redução de prejuízos intangíveis, causados por um possível ataque de engenharia social bem sucedido. A implantação de um Programa de Conscientização em Cibersegurança contribuirá para maior segurança dos sistemas de tecnologia da informação que dão suporte à capacidade de emprego e preparo da Força Aérea, contribuindo para a manutenção da confiança da sociedade brasileira nessa instituição. O estudo serve como referência para outras Forças Armadas expandirem e explorarem os aspectos defendidos neste ensaio, visando o aumento de segurança pela mitigação de vulnerabilidades decorrentes de falha humana.

Palavras-chave: Segurança da informação. Engenharia social. Vulnerabilidade. Conscientização em cibersegurança.

1 **INTRODUÇÃO**

Geralmente, quando se pensa em segurança cibernética (ou cibersegurança), considera-se somente a segurança dos meios informatizados e das informações ali contidas, ou seja, pensa-se somente na estrutura física de informática e nos programas que funcionam nessa estrutura. Porém, segundo Bojanc e Jerman-Blažič (2008), o fator humano também é causa de vulnerabilidades, apesar de elas serem normalmente identificadas como um problema técnico.

Logo, apesar da cibersegurança abranger muitas áreas, neste trabalho será considerado somente o escopo das pessoas, inseridas no espaço cibernético (ciberespaço). Ademais, vulnerabilidade será definida neste trabalho como a fraqueza causada pelas pessoas enquanto usuários dos meios de informática, explorada diretamente por ataques de engenharia social.

Bojanc e Jerman-Blažič (2008) explicam um exemplo de exploração dessa vulnerabilidade:

> Esse tipo de vulnerabilidade é causado por usuários que compartilham suas senhas ou usam senhas fracas, não entendem ou ignoram as políticas de segurança, abrem *e-mails* não confiáveis, visitam sites ou baixam *software* que contém código malicioso (BOJANC E JERMAN-BLAŽIČ, 2008, p. 415).

No contexto da Força Aérea Brasileira (FAB), Jesus (2020) percebeu em simulações de ataques *hackers* contra os sistemas de informática da Academia da Força Aérea, a possibilidade de atacar um usuário, induzindo-o a clicar em um endereço eletrônico malicioso. Este é um exemplo de ataque de engenharia social chamado *phishing,* que significa “pescar” em inglês, fazendo uma alusão ao *hacker* tentando “fisgar” um usuário por meio do *e-mail.*

Pelo exemplo acima, podemos concluir que um atacante que usa a engenharia social é um *hacker* que explora fraquezas do usuário. Engenharia social é a arte de persuadir os usuários a comprometer os sistemas de informação, manipulando-os para divulgar informações confidenciais, conforme define Krombholz (2014).

Baseado nesse cenário, este ensaio propõe que um Programa de Conscientização em Cibersegurança implantado em todas as Organizações Militares (OM) do Comando da Aeronáutica (COMAER), focado em ataques de engenharia social, proporciona maior segurança para as informações.

Dois argumentos serão desenvolvidos para justificar esta tese. Primeiramente, o Programa reduzirá o risco de usuários do COMAER serem persuadidos a viabilizar ataques dessa natureza. O segundo argumento defende que o Programa reduzirá os prejuízos institucionais intangíveis causados por um ataque de engenharia social, caso seja bem sucedido.

2 **CONSCIENTIZAÇÃO E CIBERSEGURANÇA**

O COMAER, visando aprimorar a comunicação, armazenamento e acesso às informações, implantou uma rede interna de protocolos e serviços semelhantes à internet, a qual de o nome de INTRAER. Os usuários, ao utilizarem essa rede de forma despreparada quanto às ameaças que os rondam, possibilitaram condições favoráveis para exploração de ataques de engenharia social.

Nesse sentido, saber como um engenheiro social age e quais políticas de segurança adotar, reduz esse despreparo dos usuários. Parsons *et al.* (2014) complementam dizendo que uma cultura de segurança da informação é possível de ser atingida quando os usuários conhecem os conceitos e políticas de segurança da informação.

Na FAB, essa cultura se traduz na postura de segurança atingida pelo militar a qual se refletirá na predisposição em atuar com proatividade (engajamento) e trará maior segurança aos sistemas informatizados que ele utiliza, pois diminui a sua exposição involuntária ao ataque de um *hacker.*

2.1 **Do conhecimento à segurança**

O caminho mais vulnerável que os *hackers* procuram é o fator humano, pois é o componente mais frágil conforme descrevem He e Zhang (2019). Dessa maneira, a atuação de um funcionário de forma inconsciente ou despreparada o torna um alvo para o ataque cibernético, conforme nos explica Glaspie e Karwowski (2017).

Por outro lado, segundo Zwilling *et al.* (2020), quanto mais conhecimento as pessoas têm sobre segurança cibernética maior é a sua consciência situacional, e usuários com mais conhecimento desse tipo tomam mais medidas para prevenir ataques, principalmente quando as ferramentas de defesa são simples e familiares.

Corroboram com essa ideia Kweon *et al.* (2019), quando declararam que a implementação de um treinamento em segurança cibernética é um método eficaz para aprimorar a capacidade de segurança dos funcionários de uma empresa. Assim como em uma empresa, podemos considerar que será alcançado um aperfeiçoamento da capacidade de segurança individual dos militares do COMAER, devido à maior consciência dos perigos que os cercam.

Nesse sentido, o Programa que este ensaio propõe, ocorrerá de forma semelhante ao Programa de Fortalecimento de Valores da FAB, abordando diferentes ângulos sobre o tema e utilizando questionários interativos e metodologias ativas de transmissão do conhecimento. Propõe-se ainda que, uma vez por ano ocorra uma "Semana de Cibersegurança", aos moldes da Semana de Prevenção de Acidentes, para promover de forma concentrada a consciência situacional cibernética no âmbito do COMAER.

Dessa forma, haverá continuidade na educação dos usuários, o que contribuirá para a diminuição da vulnerabilidade dos dados a serem protegidos. Esse pensamento é sustentado por Kweon *et al.* (2019), quando dizem que uma educação e treinamento em segurança da informação por um prazo mais longo, pode reduzir a probabilidade de incidentes de segurança da informação.

O Programa proporcionará ao militar uma maior clareza de como ele está vulnerável, ensinando as formas de atuação do *hacker* e as múltiplas possibilidades de ataques, inclusive o *phishing*, além de conhecer as ferramentas que estão à sua disposição para se proteger.

Adicionalmente, segundo Zwilling *et al.* (2020) um programa conscientização em Cibersegurança tem um papel importante para motivar os usuários a adotarem comportamentos proativos. Isto se refletirá na iniciativa dos usuários em praticar os conhecimentos adquiridos durante o programa.

Assim, o Programa de Conscientização em Cibersegurança proposto neste ensaio, salientando os possíveis ataques de engenharia social, trará aos militares o conhecimento necessário para atuar na sua proteção individual, ensinando aos usuários as ferramentas de proteção e as táticas utilizadas pelos atacantes, aumentando sua consciência situacional sobre os perigos do espaço cibernético e diminuindo as falhas decorrentes de erro humano. Consequentemente, o programa trará maior segurança para as informações e sistemas de tecnologia da informação da FAB.

2.2 **Os prejuízos causados por ataques bem sucedidos**

A Força Aérea como membro integrante das Forças Armadas goza da maior confiança entre as instituições brasileiras, como mostra o estudo publicado no jornal Folha de São Paulo (2019). Porém, essa confiança pode ser reduzida caso a sociedade perceba uma incapacidade da FAB de manter sua segurança cibernética.

Nesse contexto, a FAB possui sistemas de gerenciamento informatizados que são utilizados diariamente e muitas decisões são tomadas baseadas nas informações que lá existem. Portanto, uma perda ou alteração dessas informações causaria um grande prejuízo na reputação da Força como um todo. Bojanc e Jerman-Blažič (2008) complementam esse raciocínio pontuando que ataques aos sistemas de informação são um potencial causador de grandes perdas de dados, serviços e operação do negócio.

Adicionalmente, ataques *hackers* ocorrem diariamente e, quando bem sucedidos, causam prejuízos intangíveis como visto nesta notícia:

> O Twitter pediu desculpas neste sábado, após a divulgação de que *hackers* que tiveram acesso a contas de personalidades e políticos o que conseguiram após "manipularem um pequeno número de funcionários", o que representa um golpe na confiança dos usuários, reconheceu a rede social.[...] O Twitter reconheceu o dano que o ataque pode causar à reputação da empresa: "Estamos envergonhados, decepcionados e, principalmente, sentimos muito. Sabemos que precisamos reconquistar sua confiança e apoiaremos todos os esforços realizados para que os responsáveis respondam na Justiça." (YAHOO! NOTICIAS, 2020).

Nesse caso, o ataque foi realizado contra funcionários de uma empresa, porém de forma análoga, poderia ter sido direcionada a um militar para tentar ludibriá-lo, obtendo acesso não autorizado aos sistemas da FAB e podendo destruir ou alterar informações. Isso poderia causar danos à reputação da instituição.

Nesse sentido, o conhecimento e as informações de posse do COMAER possuem um valor imensurável. Segundo Silva e Nogueira (2019), os prejuízos causados por possíveis danos a sistemas computacionais, vindos de ataques cibernéticos, são facilmente perceptíveis, no entanto, sua quantificação não é banal e apresenta elevados níveis de complexidade.

Além disso, as vulnerabilidades causadas pelos usuários permitem a ocorrência de incidentes que podem afetar negativamente o negócio de uma empresa, causando danos, prejuízos ou repercussões, no mínimo indesejáveis, para os

produtos e para a imagem da empresa, conforme alerta Silva (2011). Essa condição favorável ao ataque pode ser mitigada pela conscientização dos usuários.

Logo, a implantação do Programa de Conscientização em Cibersegurança proposto neste ensaio, focado em ataques que visam persuadir os usuários a comprometerem os sistemas de informação, reduzirá os riscos de ocorrerem prejuízos à imagem da instituição causados por um ataque de engenharia social.

3 **CONCLUSÃO**

No desenvolvimento deste ensaio, verificou-se que o ciberespaço é composto, dentre outras coisas, pelas pessoas que ali realizam suas atividades. Caso as pessoas utilizem a rede INTRAER de forma desatenta quanto às ameaças que os rondam, estas representam um ponto de vulnerabilidade e risco à segurança das informações, uma vez que poderão ser persuadidos a colaborar com um ataque de engenharia social, sem se darem conta disso.

Assim, um Programa de Conscientização em Cibersegurança direcionado aos militares no âmbito do COMAER, com ênfase em ataques de engenharia social, reduz a vulnerabilidade cibernética causada pelo fator humano, pois ensinará aos militares as formas de ataques e os riscos ao qual estão expostos, provendo o conhecimento necessário, tornando-os mais aptos a reconhecer os ataques.

Adicionalmente, o Programa contribuirá para a redução dos riscos de ocorrerem prejuízos intangíveis causados por um ataque efetivo de engenharia social. A quebra de segurança de uma instituição tão respeitada quanto a FAB pode representar danos à imagem da instituição e descrédito perante a sociedade.

Este Programa de Conscientização contribuirá para maior segurança dos sistemas de tecnologia da informação que dão suporte à capacidade de emprego e preparo da Força Aérea, contribuindo para a manutenção da confiança da sociedade brasileira nessa instituição. Além disso, este ensaio serve como referência para outras Forças Armadas expandirem e explorarem os aspectos defendidos neste ensaio visando o aumento de segurança pela mitigação de vulnerabilidades decorrentes de falha humana.

REFERÊNCIAS

BOJANC, B.; JERMAN-BLAŽIČ, B. An economic modelling approach to information security risk management. **International Journal of Information Management**, v. 28, n. 5, p. 413-422, 2008.

FORÇAS Armadas têm maior grau de confiança entre instituições. **Folha de São Paulo**, São Paulo, 10 jul. 2019. Disponível em: https://datafolha.folha.uol.com.br/opiniaopublica/2019/07/1988221-forcas-armadas-tem-maior-grau-de-confianca-entre-instituicoes.shtml. Acesso em: 21 jul. 2022.

GLASPIE, H. W.; KARWOWSKI, W. Human factors in information security culture: A literature review. In: **International Conference on Applied Human Factors and Ergonomics**. Springer, Cham, 2017. p. 269-280.

HE, W.; ZHANG, Z. Enterprise cybersecurity training and awareness programs: Recommendations for success. **Journal of Organizational Computing and Electronic Commerce**, v. 29, n. 4, p. 249-257, 2019.

JESUS, L. F.; BISPO, C. A. F. Análise dos benefícios de pentests regulares nas redes do Comando da Aeronáutica. In: Seminário de Cibernética, 2. 2020, Rio de Janeiro. **Anais.** II Seminário de Segurança e Defesa Cibernética: desafios da defesa cibernética na projeção espacial brasileira. Rio de Janeiro: Universidade da Força Aérea, 2020.

KROMBHOLZ, K. *et al.* Advanced social engineering attacks. **Journal of Information Security and applications**, v. 22, p. 113-122, 2015.

KWEON, E. *et al*. The utility of information security training and education on cybersecurity incidents: an empirical evidence. **Information Systems Frontiers**, v. 23, n. 2, p. 361-373, 2021.

PARSONS, K. *et al.* A study of information security awareness in Australian government organisations. **Information Management & Computer Security**, 2014.

SILVA, A. O. Engenharia social: o fator humano na segurança da informação. **Coleção Meira Mattos: revista das ciências militares**, n. 23, 8 nov. 2011.

SILVA, W. R.; NOGUEIRA, J. M. Ataques cibernéticos e medidas governamentais para combatê-los. **O Comunicante**, v. 9, n. 1, p. 42-57, 2019.

TWITTER pede desculpas por colaboração de funcionários em ataque de hackers. **Yahoo! Notícias**, São Paulo, 18 jul. 2020. Disponível em: https://br.noticias.yahoo.com/twitter-afirma-hackers-manipularam-funcionários-terem-acesso-contas-120354042--finance.html. Acesso em: 21 jul. 2022.

ZWILLING, M. *et al*. Cyber security awareness, knowledge and behavior: a comparative study. **Journal of Computer Information Systems**, v. 62, n. 1, p. 82-97, 2022.