ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA

DIVISÃO DE ENSINO

CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2024

OSWALDO SEGUNDO DA COSTA **NETO**, Cap Av

A Implantação da Autenticação por Múltiplos Fatores em Sistemas de Informação da FAB

Rio de Janeiro

2024

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS DA AERONÁUTICA
DIVISÃO DE ENSINO
CURSO DE APERFEIÇOAMENTO DE OFICIAIS 1º/2024

OSWALDO SEGUNDO DA COSTA **NETO**, Cap Av

A Implantação da Autenticação por Múltiplos Fatores em Sistemas de Informação da 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: Márcio Henrique Teixeira de Souza, Ten Cel Av

Rio de Janeiro
2024

OSWALDO SEGUNDO DA COSTA **NETO**, Cap Av

A Implantação da Autenticação por Múltiplos Fatores em Sistemas de Informação da FAB

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

Aprovado por:

Márcio Henrique **Teixeira** de Souza, Ten Cel Av
EAOAR

Alexandra Vidal Pedinotti Zuma, Maj Farm
EAOAR

Rio de Janeiro
2024

RESUMO

A evolução tecnológica na Força Aérea Brasileira (FAB) tem promovido uma digitalização crescente, posicionando o ciberespaço como um domínio crítico na guerra e exigindo atenção significativa para assegurar a segurança e a integridade das operações. Este contexto é agravado pelo fato de o Brasil ser um dos principais alvos globais de ataques cibernéticos, destacando a necessidade de intensificar as medidas de Proteção Cibernética na FAB. Diante dessa realidade, torna-se fundamental considerar o alinhamento da Força com padrões internacionais de melhores práticas de segurança da informação, visando elevar a proteção de sistemas críticos contra ameaças cibernéticas emergentes. A proposta deste ensaio é a implantação de autenticação por múltiplos fatores, ou *Multi-Factor Authentication* (MFA), em todos os sistemas de informação da FAB com acesso à Internet, visando a mitigação dos riscos associados ao comprometimento de credenciais. A MFA introduz camadas adicionais de segurança que dificultam o acesso não autorizado, mesmo frente ao comprometimento de credenciais, pois exige evidências múltiplas e variadas de identificação. Simultaneamente, tal estratégia desencoraja a ação de potenciais invasores ao aumentar a complexidade necessária para a realização de ataques cibernéticos, atuando para desestimular as tentativas de invasão em função do esforço adicional requerido para executar a ação intrusiva. A adoção desta medida é crucial para preservar a eficácia operacional e estratégica da FAB, enfatizando a importância da Proteção Cibernética para a Força e corroborando o objetivo estratégico de proteger o ciberespaço do Comando da Aeronáutica contra ataques cibernéticos.

Palavras-chave: MFA. Proteção Cibernética. Segurança da informação. Ciberespaço. Autenticação por múltiplos fatores.

1 INTRODUÇÃO

A FAB hospeda diversos serviços informacionais que possuem acesso à Internet, desempenhando papéis fundamentais na administração e na segurança de operações. Tais serviços abrangem desde sistemas computacionais até bases de dados sensíveis, que, se comprometidos, podem representar riscos às operações ou à imagem da Força.

Os desafios advindos da intensa digitalização dos meios de informação utilizados pela FAB, juntamente com o reconhecimento de que o Brasil figura entre os principais alvos de ataques cibernéticos no mundo (Sussman; Mok, 2023), reforçam a urgência de identificar oportunidades de aprimoramento nos processos que regem o funcionamento e a utilização desses meios de informação.

Acrescenta-se aos desafios mencionados a existência de práticas criminosas na Internet voltadas à comercialização de credenciais de cidadãos brasileiros obtidas de maneira ilícita, incluindo aquelas utilizadas por militares para acessar os sistemas de informação da Força. Por conseguinte, em uma Força Aérea cada vez mais digital, deve-se considerar os protocolos de autenticação como principal facilitador a fim de manter a segurança na transmissão de dados em sistemas de informação.

Em 2020, um grupo *hacker* divulgou a obtenção de diversas credenciais de funcionários da Administração Pública Federal (APF), incluindo militares da FAB (Souza, 2020). A divulgação dessas credenciais vazadas pode favorecer ações mais intrusivas por parte de atacantes digitais, com o potencial de provocar prejuízos catastróficos para a Força.

Um incidente cibernético ocorrido em 2022 exemplifica as severas consequências estratégicas que podem advir de eventuais vazamentos de dados: uma quantidade massiva de informações vitais de inteligência e detalhes sobre Sistemas de Armas do Exército Polonês foram expostos na Internet. Este comprometimento não apenas colocou em evidência a possibilidade de acesso indevido a informações críticas, mas também aumentou significativamente o risco de espionagem ou sabotagem, levando a potenciais danos irreparáveis à segurança daquele país (Zemla; Wyrwal, 2022).

Inicialmente, a autenticação de fator único, ou *Single-Factor Authentication* (SFA), que utiliza apenas um *login* e senha, era a escolha predominante devido à sua simplicidade e facilidade de uso. No entanto, tal abordagem demonstrou ser vulnerável a uma variedade

de ataques cibernéticos, incluindo *malwares*, ataques de força bruta, entre outros (Kim; Hong, 2011).

A partir da vulnerabilidade supracitada, observou-se uma tendência crescente em direção a métodos de autenticação multifator, ou *Multi-Factor Authentication* (MFA), que reforçam a segurança ao exigir evidências adicionais de identidade, como características humanas únicas, a exemplo do reconhecimento de impressões digitais.

Considerando os desafios apresentados e a importância reconhecida da Defesa Cibernética como uma Ação de Força Aérea (Brasil, 2020), este ensaio propõe a implantação da MFA em todos os sistemas de informação da FAB com acesso à Internet para mitigar os riscos associados ao comprometimento de credenciais de acesso.

Dois argumentos serão desenvolvidos para justificar esta tese. Primeiramente, a utilização de MFA adiciona camadas de segurança que dificultam o acesso não autorizado, mesmo que as credenciais iniciais sejam comprometidas. Em segundo lugar, a adoção de MFA desencoraja a ação de potenciais invasores ao aumentar a complexidade necessária para a realização de ataques cibernéticos.

2 ELEVANDO A PROTEÇÃO CIBERNÉTICA DA FAB COM MFA

Inicialmente adotada, a autenticação de fator único, ou SFA, logo se mostrou insuficiente diante das exigências das instituições que valorizam a segurança da informação como um componente crítico de suas operações (Ometov *et al.*, 2018). A mudança de paradigma foi impulsionada pelo surgimento de novas técnicas de cibercrime e ameaças cibernéticas, evidenciando a necessidade de métodos de autenticação mais robustos (Gunson *et al.*, 2011).

Segundo Ometov *et al.* (2018), há três tipos de fatores utilizados para vincular um indivíduo às suas credenciais de acesso. O primeiro é o Fator de Conhecimento, que se refere a algo que o usuário sabe, como uma senha ou uma palavra-chave. O segundo é o Fator de Posse, que envolve algo que o usuário possui, incluindo cartões, *smartphones* ou outros tipos de *tokens*. O terceiro e último é o Fator Biométrico, que se relaciona com algo inerente ao usuário, seja por meio de dados biométricos ou padrões de comportamento específicos.

Nesse sentido, entende-se como MFA a estratégia de autenticação que alia o Fator

de Conhecimento, como credenciais de *login* e senha, a um outro fator, seja o Fator de Posse ou Fator Biométrico.

Convém ressaltar que a FAB já possui legislação que prevê a utilização de barreiras adicionais para o controle de acesso lógico a sistemas de informação (Brasil, 2022). Entretanto, sua extensão abrange apenas serviços isolados, mediante avaliação prévia de necessidade por parte do Centro de Inteligência da Aeronáutica (CIAER). Propõe-se, portanto, uma mudança de política no sentido de implantar a MFA em todos os sistemas de informação da FAB com acesso à Internet.

2.1 **MFA sob a ótica defensiva**

O objetivo primordial da implantação de MFA é a utilização de ferramentas que tragam uma melhoria no controle de acesso lógico, a fim de proteger acessos indevidos a serviços informacionais e sistemas que necessitam de identificação do usuário.

Para exemplificar a necessidade da implantação de MFA como uma barreira adicional na segurança cibernética, considera-se que o *phishing* é uma ameaça significativa neste contexto. O *phishing* é uma técnica de engenharia social que envolve o envio de comunicações fraudulentas, geralmente por e-mail, que se passam por entidades confiáveis com o objetivo de enganar os indivíduos para que forneçam dados pessoais, como senhas ou informações de cartão de crédito (Aleroud; Zhou, 2017).

Em um cenário onde o militar da FAB não consiga identificar de imediato a ameaça em sua caixa de e-mail, ele pode inadvertidamente interagir com ela e fornecer ao criminoso suas informações de nome de usuário e senha.

Contudo, a implantação de uma política de MFA no sistema informacional exige que, além do nome de usuário e senha, seja fornecida uma segunda etapa de verificação, podendo ser através de algo que o usuário tenha consigo (Fator de Posse) ou algo que o identifique fisicamente (Fator Biométrico). A falta de acesso do criminoso a este segundo fator de autenticação cria um obstáculo que neutraliza a tentativa de ataque.

Adicionalmente, a problemática da segurança das informações é amplificada pela prática comum de reutilização de credenciais por parte dos usuários em diversos sistemas. Esta tendência não apenas facilita o trabalho dos criminosos em potencial, ao aumentar a probabilidade de que uma única credencial comprometida possa ser usada para acessar

múltiplos serviços, mas também sublinha a importância de implementar medidas de segurança mais robustas, como a MFA.

O *National Institute of Standards and Technology* (NIST) dos Estados Unidos da América (EUA) fornece diretrizes que reforçam a importância da adoção da MFA como mecanismo de proteção de sistemas digitais. Especificamente, a Publicação Especial 800-63B descreve os padrões para serviços de identidade digital, que incluem recomendações para o uso da MFA (NIST, 2017).

Segundo NIST (2017), no contexto da MFA, há três diferentes níveis de garantia de autenticação, ou *Authentication Assurance Levels* (AALs), que os sistemas de informação devem observar, a fim de proverem a segurança adequada de seus dados.

O AAL1 oferece uma garantia básica sobre a identidade do usuário, exigindo, no mínimo, a autenticação baseada em um único fator. Por sua vez, o AAL2 busca proporcionar uma alta confiança na assertividade da identidade do usuário, requerendo a prova de posse e controle sobre dois fatores distintos de autenticação. Por fim, o AAL3 destina-se a oferecer um nível de confiança muito alto na autenticação, exigindo também dois fatores distintos, com a particularidade de um deles ser um autenticador criptográfico baseado em hardware.

Tais níveis são projetados para orientar organizações na seleção da força apropriada dos mecanismos de autenticação com base na sensibilidade das informações protegidas. Quanto mais alto o nível, mais forte deve ser a autenticação para resistir a ataques e acessos não autorizados (NIST, 2017).

As diretrizes do NIST, reconhecidas internacionalmente por estabelecerem padrões de excelência em segurança cibernética, incluem o uso estratégico de MFA para destacar a importância de robustecer as barreiras contra cibercriminosos.

A adoção de MFA, em níveis AAL2 ou AAL3, não apenas alinha a FAB às melhores práticas internacionais em segurança cibernética, mas também reforça sua capacidade de proteger informações sensíveis contra as ameaças cada vez mais sofisticadas no ciberespaço.

Portanto, propõe-se a implantação da MFA em todos os sistemas de informação da FAB com acesso à Internet, a fim de adicionar camadas de segurança que dificultam o acesso não autorizado e, consequentemente, elevar a Proteção Cibernética da Força.

2.2 **MFA sob a ótica ofensiva**

Além da compreensão da importância dos mecanismos de fortalecimento da Proteção Cibernética sob o ponto de vista defensivo, torna-se imprescindível expandir a visão a fim de incluir a perspectiva do atacante. Essa mudança de foco é crucial, pois permite a compreensão dos métodos de ataque e promove um entendimento bidirecional da Proteção Cibernética.

Neste sentido, compreender a MFA do ponto de vista ofensivo põe luz às motivações e táticas dos atacantes. Portanto, entende-se que a adoção de MFA desencoraja suas potenciais ações ofensivas, pois há expressivo aumento de complexidade necessária para a realização de ataques cibernéticos.

A teoria da oportunidade na criminologia sugere que infratores, quando optam pelo cometimento de crimes, procuram uma oportunidade ou um alvo prático (Fennelly; Perry, 2018). Além disso, Felson e Clarke (1998) argumentam que a prevenção de crimes é possível através da redução de oportunidades para os criminosos.

Similarmente, Fennelly e Perry (2018) sustentam que um efetivo controle de acesso é fator determinante para a redução de crimes:

> O Controle Natural de Acesso é um conceito de *design* direcionado principalmente para diminuir as oportunidades de crime, desencorajando o acesso a alvos de crime e criando uma percepção de risco para os infratores. Isso é uma extensão lógica da ideia de reforço territorial. É alcançado projetando ruas, calçadas, entradas de edifícios e portais de bairros para indicar claramente as rotas públicas, e desencorajando o acesso a áreas privadas com elementos estruturais (Fennelly; Perry, 2018, p. 8).

Paralelamente, é possível correlacionar o conceito citado, originário da criminologia, com estratégias de Proteção Cibernética. Enquanto Fennelly e Perry (2018) se referem às barreiras físicas que desencorajam a entrada não autorizada por meio de um *design* estratégico, a MFA serve como uma barreira digital equivalente, reduzindo as oportunidades de acesso indevido no ciberespaço.

A MFA incorpora digitalmente os princípios de dissuasão e percepção de risco, elevando o esforço necessário para realização de ataques cibernéticos de maneira similar ao Controle Natural de Acesso. Ao implementar controles de acesso mais rigorosos nos sistemas, reduz a atratividade dos alvos para atacantes, alterando sua análise de risco e recompensa, o que proporciona uma segurança cibernética mais eficaz.

Van der Putten, Meijnders e Rood (2015) exemplificam e analisam o uso da dissuasão contra ameaças não convencionais, dentre elas as ameaças cibernéticas, destacando sua relevância para a segurança nacional holandesa. Ressaltam a necessidade de aprimorar mecanismos de defesa a fim de obter maior resiliência cibernética e elevar os custos aos cibercriminosos, diminuindo a atratividade dos ataques cibernéticos.

Portanto, propõe-se a implantação da MFA em todos os sistemas de informação da FAB com acesso à Internet, visando desencorajar a ação de potenciais invasores cibernéticos.

3 **CONCLUSÃO**

A crescente evolução tecnológica e digitalização da FAB, juntamente com as constantes ameaças de ataques cibernéticos reforçam a necessidade de fortalecer o seu ciberespaço. Problemas como vazamentos de credenciais de militares podem ocasionar impactos a nível estratégico, particularmente quando comprometem sistemas críticos ou que contenham informações sensíveis.

Dessa forma, este ensaio defendeu a implantação da MFA em todos os sistemas de informação da FAB com acesso à Internet como medida essencial para mitigar os riscos associados ao comprometimento de credenciais de acesso.

A introdução de camadas adicionais de segurança, viabilizada pela utilização do MFA, proporciona o alinhamento da Força com as melhores práticas de segurança da informação, buscando a conformidade com os padrões do NIST. Tal estratégia representa um avanço significativo na proteção dos ativos computacionais, elevando o nível de segurança no ciberespaço.

Adicionalmente, a adoção de MFA desencoraja a ação de potenciais invasores ao aumentar a complexidade necessária para a realização de ataques cibernéticos, atuando para desestimular as tentativas de invasão em função do esforço adicional requerido para executar a ação intrusiva.

Reforça-se que tal medida, ao ser aplicada, atuará como uma barreira adicional de segurança, ampliando as capacidades de Proteção Cibernética da Força e corroborando o objetivo estratégico de proteger o ciberespaço do Comando da Aeronáutica de ataques cibernéticos, contido no Plano Estratégico Militar da Aeronáutica (Brasil, 2018).

REFERÊNCIAS

ALEROUD, Ahmed; ZHOU, Lina. Phishing Environments, Techniques, and Countermeasures: A Survey. **Computers & Security**, v. 68, p. 160–196, jul. 2017. ISSN 01674048. DOI: 10.1016/j.cose.2017.04.006.

BRASIL. Comando da Aeronáutica. Comando-Geral de Apoio. Portaria COMGAP Nº 42/ADLG, de 2 de maio de 2022. Aprova a reedição da Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 81, f. 5930, maio 2022.

BRASIL. Comando da Aeronáutica. Portaria Nº 1.224/GC3, de 10 de novembro de 2020. Aprova a reedição da Doutrina Básica da Força Aérea Brasileira (DCA 1-1). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 205, f. 14971, nov. 2020.

BRASIL. Comando da Aeronáutica. Portaria Nº 2.102/GC3, de 18 de dezembro de 2018. Aprova a reedição do Plano Estratégico Militar da Aeronáutica (PEMAER). **Boletim do Comando da Aeronáutica**, Rio de Janeiro, n. 222, f. 14766, dez. 2018.

FELSON, Marcus; CLARKE, Ronald. **Opportunity Makes the Thief**: Practical Theory for Crime Prevention. 1st. edition. London: Home office, Policing and Reducing Crime Unit, 1998. (Police Research Series, 98). ISBN 978-1-84082-159-8.

FENNELLY, Lawrence; PERRY, Marianna. **CPTED and Traditional Security Countermeasures**: 150 Things You Should Know. Boca Raton: CRC Press, Taylor & Francis Group, 2018. ISBN 978-1-138-48974-5.

GUNSON, Nancie *et al.* User Perceptions of Security and Usability of Single-Factor and Two-Factor Authentication in Automated Telephone Banking. **Computers & Security**, v. 30, n. 4, p. 208–220, jun. 2011. ISSN 01674048. DOI: 10.1016/j.cose.2010.12.001. Acesso em: 25 fev. 2024.

KIM, Jae-Jung; HONG, Seng-Phil. A method of risk assessment for multi-factor authentication. **Journal of Information Processing Systems**, Korea Information Processing Society, v. 7, n. 1, p. 187–198, 2011.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Digital Identity Guidelines**: Authentication and Lifecycle Management. Special Publication. [*S. l.*], 2017. Disponível em: https://doi.org/10.6028/NIST.SP.800-63b. Acesso em: 3 out. 2023.

OMETOV, Aleksandr *et al.* Multi-Factor Authentication: A Survey. **Cryptography**, v. 2, n. 1, p. 1, jan. 2018. ISSN 2410-387X. DOI: 10.3390/cryptography2010001. Acesso em: 24 fev. 2024.

SOUZA, Ramon. **USP, Marinha e Força Aérea**: Grupo vaza dados de três instituições ao mesmo tempo. Mar. 2020. Disponível em: https://thehack.com.br/usp-marinha-e-forca-aerea-grupo-vaza-dados-de-tres-instituicoes-ao-mesmo-tempo. Acesso em: 24 fev. 2024.

SUSSMAN, Bruce; MOK, Christine. **The Top 10 Countries Most Targeted by Cyberattacks**. Set. 2023. Disponível em: https://blogs.blackberry.com/en/2023/02/top-10-countries-most-targeted-by-cyberattacks-2023-report. Acesso em: 8 mar. 2024.

VAN DER PUTTEN, Frans-Paul; MEIJNDERS, Minke; ROOD, Jan. Deterrence as a Security Concept against Non-Traditional Threats. **Clingendael**, jun. 2015. Disponível em: https://www.clingendael.org/sites/default/files/2017-09/deterrence_as_a_security_concept_against_non_traditional_threats.pdf. Acesso em: 14 mar. 2024.

ZEMLA, Edyta; WYRWAL, Marcin. **Gigantyczny wyciek danych z wojska. Ponad 1,7 mln pozycji w internecie**. Jan. 2022. Disponível em: https://wiadomosci.onet.pl/kraj/gigantyczny-wyciek-danych-z-wojska-ponad-17-mln-pozycji-w-internecie/1mknjtf. Acesso em: 29 fev. 2024.