Investigação da ferramenta Keycloak na Mitigação de Incidentes Cibernéticos: Uma Abordagem Integrada com o Programa de Privacidade e Segurança da Informação (PPSI)

Lídia Bononi P. Tomaz[1,3], Patrícia Araújo de Oliveira[2,3], Éder Souza Gualberto[3]

[1]Instituto Federal do Triângulo Mineiro
Uberaba-MG, Brasil (IFTM)

[2]Universidade Federal do Amapá
Macapá-AP, Brasil (UNIFAP)

[3]Universidade de Brasília
Brasília-DF, Brasil (UnB)

lidia@iftm.edu.br, araoli@unifap.br, eder.gualberto@redes.unb.br

Abstract. *This paper aims to explore the Keycloak tool for mitigating cyber incidents considering the controls of the Federal Government's Privacy and Information Security Program (PPSI). Keycloak is an open source Identity Access Management (IAM) that centralizes user authentication and authorization operations, offers access control, logs capabilities for audits and monitoring. Thus, the objective of this paper is to investigate Keycloak's capabilities to strengthen information security, improve data protection and increase responsiveness to cybersecurity incidents.*

Resumo. *Este artigo visa explorar a ferramenta Keycloak para a mitigação de incidentes cibernéticos considerando os controles do Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal. O Keycloak é uma solução open source de gerenciamento de identidade e acesso (IAM – Identity Access Management) que centraliza as operações de autenticação e autorização de usuários, oferece controle de acesso, recursos de logs para auditorias e monitoramento. Assim, o objetivo deste artigo é investigar os recursos do Keycloak para fortalecer a segurança da informação, melhorar a proteção de dados e aumentar a capacidade de resposta a incidentes de segurança cibernética.*

1. Introdução

Normas internacionais como a ISO/IEC 27002:2022, que trata da segurança da informação, segurança cibernética e proteção à privacidade [International Organization for Standardization 2022] e controles de segurança da informação como o *Critical Security Controls* versão 8 do *Center for Internet Security* (CIS) - CIS v8 [Center for Internet Security 2021] - e o NIST CSF (*National Institute of Standards and Technology Cybersecurity Framework*) [National Institute of Standards and Technology 2024] abordam, dentre as diversas medidas propostas, um conjunto específico para tratar sobre gestão de contas e controle de acesso dentro das organizações.

No Brasil, em 2023, foi proposto o Programa de Privacidade e Segurança da Informação (PPSI) pela Secretaria do Governo Digital por meio do Ministério de Gestão e

Inovação. O intuito do PPSI é orientar os órgãos e entidades do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) quanto à implantação de práticas de privacidade e segurança visando aumentar sua maturidade e resiliência [Ministério de Gestão e Inovação 2024]. O programa é acompanhado de um *framework* que, nas questões de segurança cibernética, se baseia nos controles do CIS v8 e NIST CSF.

Este artigo realiza um estudo sobre a ferramenta de IAM denominada Keycloak [Red Hat 2024]. Entre suas principais características destacam-se a centralização de autenticação e autorização, controle de acesso, e logs para auditorias e monitoramento. O objetivo é investigar os recursos desta ferramenta para verificar as medidas de controles de gestão de contas e controle de acesso do PPSI que ela pode auxiliar os órgãos do Governo a cumprir, visando aumentar sua capacidade de resposta a incidentes de segurança cibernética. Além disso, é feita uma relação com outros frameworks de controle como o CIS v8, o NIST CSF e a ISO/IEC 27002:2022. Os resultados mostraram que, com a configuração adequada, das 14 medidas contempladas nos controles de gestão de contas e controle de acesso no PPSI, 11 podem ser totalmente implementadas. Os três controles restantes dependem de ações de governança dentro da instituição.

Este trabalho está organizado da seguinte forma: a Seção 2 apresenta a relação de gestão de contas, controle de acesso e o PPSI, a Seção 3 aborda o estudo realizado sobre a ferramenta Keycloak, a Seção 4 apresenta a conclusão e trabalhos futuros.

2. Gestão de Contas, Controle de Acesso e o PPSI

A Gestão de Identidade e Acesso (IAM - *Identity Access Management*) é um conceito fundamental para a área de Segurança da Informação, pois envolve a criação, o gerenciamento e o monitoramento das identidades dos usuários, considerando o controle de acesso estabelecido pela organização. Este processo inclui a autenticação de usuários, a autorização para acessar recursos específicos e a auditoria contínua desses acessos para assegurar conformidade e segurança.

No contexto das medidas voltadas para gestão de contas e controle de acesso, observa-se no PPSI a indicação do uso de ferramentas de IAM, visando prover uma estratégia centralizada para gestão de contas de usuários e permissionamento aos recursos das aplicações [Singh et al. 2023]. Salienta-se que os controles de segurança do PPSI correspondem aos controles do CIS v8 e relaciona cada um dos controles com as funções do NIST. Nesta perspectiva, as medidas que o Keycloak pode ajudar a cumprir no PPSI são: *Controle 5 - Gestão de contas* e *Controle 6 - Gestão do Controle de Acesso* que estão relacionadas às funções NIST de identificar e proteger.

O controle 5 do PPSI traz orientações em relação a Gestão de Contas e recomenda o uso de processos e ferramentas para atribuir e gerenciar autorização de credenciais para contas de usuários, o que o faz um importante guia para o desenvolvimento de um programa de IAM nas organizações.

O controle 6 do PSSI, que estabelece medidas para o gerenciamento de acesso em contas corporativas, visa estabelecer orientações para que os usuários tenham acesso apenas aos dados ou ativos corporativos apropriados para suas funções e garantir que haja autenticação forte para dados ou funções corporativas críticas ou sensíveis. O controle traz a recomendação de que as contas devem ter apenas a autorização mínima necessária para as funções estabelecidas.

ID no PPSI	ID no CIS V8	Função no NIST CSF	Título da medida	Keycloak
5.1	5.1	IDENTIFICAR	Estabelecer e manter um inventário de contas	✓
5.2	5.5	IDENTIFICAR	Restringir e manter um inventário de contas de serviço	✓
5.3	5.2	PROTEGER	Usar senhas exclusivas	✗
5.4	5.4	PROTEGER	Restringir privilégios de administrador a contas de Administrador dedicadas	✓
5.5	5.6	PROTEGER	Centralizar a gestão de contas	✓
5.6	5.3	RESPONDER	Desabilitar contas inativas	✓
6.1	6.6	IDENTIFICAR	Estabelecer e manter um inventário de sistemas de conta de autenticação e autorização	✓
6.2	6.1	PROTEGER	Estabelecer um processo de concessão de acesso	✗
6.3	6.2	PROTEGER	Estabelecer um processo de revogação de acesso	✗
6.4	6.3	PROTEGER	Exigir MFA para aplicações expostas externamente	✓
6.5	6.4	PROTEGER	Exigir MFA para acesso remoto à rede	✓
6.6	6.5	PROTEGER	Exigir MFA para acesso administrativo	✓
6.7	6.7	PROTEGER	Centralizar o controle de acesso	✓
6.8	6.8	PROTEGER	Definir e manter o controle de acesso baseado em funções	✓

Tabela 1. Relação entre Keycloak e os Controles baseados no PPSI, CIS v8 e NIST CSF.

Além disso, o controle 6 recomenda empregar uma abordagem de gerenciamento de acesso privilegiado (PAM - *Privileged Access Management*), que tem por objetivo focar no gerenciamento de contas de usuários que representam um maior risco para a organização, seja de usuários com funções de administradores que têm o papel de adicionar, alterar e remover outras contas, ou fazer alterações de configuração em sistemas operacionais e aplicações, ou mesmo usuários que acessam o ambiente corporativo a partir de redes não confiáveis. O PPSI/CIS v8 reforça também a importância do uso de ferramentas que possibilitem Autenticação Multifator (MFA - *Multi-factor Authentication*).

3. A ferramenta Keycloak

O Keycloak é uma ferramenta de código aberto desenvolvida para IAM pela Red Hat [Hat 2024]. Se corretamente configurada, ela pode ser um mecanismo eficaz para o atendimento das medidas relacionadas a gestão de contas e controle de acesso presentes nos frameworks do PPSI, CIS v8 e NIST CSF.

A Tabela 1 apresenta a relação das medidas dos controles do PPSI que o Keycloak pode ser eficaz, as referenciando com o CIS v8 e função NIST CSF. A primeira coluna da Tabela 1 apresenta os identificadores (ID) do framework PPSI, a segunda coluna relaciona os identificadores (ID) do CIS v8, a terceira coluna apresenta a função deste controle dentro do NIST CSF, a coluna "Título da Medida" corresponde ao título do controle extraído do CIS v8, visto que no PPSI, apesar do texto da medida ter o mesmo significado, está no formato interrogativo. Por esta razão, optou-se por usar o formato do CIS por estar no infinitivo impessoal. A última coluna apresenta um símbolo verde em formato de *check* para os itens em que há possibilidade de implementação do controle a partir da ferramenta Keycloak. Os itens que não podem ser configurados no Keycloak foram expostos pelo símbolo em vermelho em formato de *x*.

Conforme pode ser observado na Tabela 1, a ferramenta Keycloak permite cobrir 11 de 14 das medidas relacionados à gestão de contas e controle de acesso do PPSI. É importante destacar que os itens que não podem ser implementados diretamente na ferramenta Keycloak envolvem ações que requerem a intervenção de agentes externos, como a criação de senhas exclusivas ou o estabelecimento de processos. Todavia, mesmo nesses casos, a ferramenta Keycloak estará envolvida.

Adicionalmente, destaca-se a ISO/IEC 27002:2022 [International Organization for Standardization 2022], que apresenta um conjunto de orientações sobre segurança da informação, segurança cibernética e proteção à privacidade. Nesta norma, observa-se que o Keycloak é uma ferramenta que auxilia na implementação das orientações dos controle de acesso, gestão de identidade, informações de autenticação e direitos de acesso, cujos identificadores nesta norma são, respectivamente, 5.15, 5.16, 5.17 e 5.18.

4. Conclusão e trabalhos futuros

Este trabalho apresentou um estudo sobre uma ferramenta de gerenciamento de identidade de acesso, do inglês *Identity Access Management - IAM*, denominada Keycloak. Foram apresentadas as características gerais da ferramenta, cenários de aplicação e a sua relação com controles de segurança. Neste último caso, foram enfatizados os controles de gestão de contas e controle de acesso do PPSI que o Keycloak pode auxiliar a cumprir. Além disso, também foi feita a relação com os controles do CIS v8, funções do NIST CSF e a possibilidade de atender à algumas orientações da ISO/IEC 27002:2022. Assim, foi possível concluir que o Keycloak é uma ferramenta versátil e poderosa que pode auxiliar as organizações, em especial, as do SISP que estão trabalhando na implantação do PPSI, a cumprir os controles voltados para gestão de contas e controles de acesso, bem como apoiar outros controles como o de registros de auditorias. Desta forma, a ferramenta pode ser um subsídio de segurança cibernética.

Como trabalho futuro pretende-se realizar uma PoC (*Proof of Concept*) da ferramenta Keycloak em um ambiente organizacional real.

Referências

Center for Internet Security (2021). Cis controls version 8. `https://www.cisecurity.org/controls/v8/`. Accessed: 2024-06-30.

Hat, R. (2024). Red hat official website. `https://www.redhat.com/en`. Accessed: 2024-06-30.

International Organization for Standardization (2022). Iso/iec 27002:2022 information security, cybersecurity and privacy protection – information security controls. Standard. Accessed: 2024-06-30.

Ministério de Gestão e Inovação (2024). Guia Framework do Programa de Privacidade e Segurança da Informação (PPSI). `https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos`. Accessed: 2024-06-30.

National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. Technical report, National Institute of Standards and Technology. Accessed: 2024-06-30.

Red Hat (2024). Keycloak: Open source identity and access management. `https://www.keycloak.org/`. Accessed: 2024-06-30.

Singh, C., Thakkar, R., and Warraich, J. (2023). Am identity access management—importance in maintaining security systems within organizations. *European Journal of Engineering and Technology Research*, 8(4):30–38.