Requisitos de segurança para arquitetura de um sistema de controle de acesso com cadeia de aprovação

RESUMO ESTENDIDO - Disciplina de TCC029009

Sarom Torres Gaier
Estudante do Curso de Engenharia de Telecomunicações

Prof. Ederson Torresini, M. Sc
Professor orientador

Semestre 2024.1

Resumo- *O acesso a infraestruturas físicas em empresas é restrito e controlado por credenciais obtidas após rigorosos processos de aprovação. Em empresas com múltiplos Centros de Processamento de Dados (CPDs), cada unidade adota sistemas de autenticação próprios, o que torna complexa a concessão e revogação de acessos, especialmente quando há necessidade de acessos cruzados ou de terceiros. A descentralização desses processos pode levar a erros e aumentar os riscos de segurança, como vazamento de credenciais. Esse trabalho propõe estabelecer os requisitos mínimos de segurança para uma arquitetura centralizada para gestão de acessos, visando maior eficiência e segurança no controle e rastreamento de operações.*

Palavras-chave: Controle de Acesso. Cadeia de aprovação. Centro de Processamento de Dados (CPDs).

1 Introdução

O acesso às infraestruturas físicas de empresas e instituições é geralmente restrito a indivíduos específicos e controlado por credenciais obtidas após um rigoroso processo de aprovação. Frequentemente, colaboradores de outras localidades da mesma empresa necessitam acessar áreas diferentes das suas origens, o que demanda concessões temporárias e pontuais de acesso. Além disso, fornecedores e prestadores de serviços também precisam ter seus acessos aprovados e receber as devidas credenciais de maneira segura.

No cenário em que há múltiplos Centros de Processamento de Dados (CPDs) dentro de uma mesma empresa, cada CPD possui seu próprio sistema de autenticação, conectado a suas bases individuais de credenciais para colaboradores autorizados. Esse processo de aprovação geralmente segue regras de segurança rigorosas, envolvendo várias pessoas responsáveis em cada localidade, o que pode resultar em cadeias de aprovação complexas. Sem um mecanismo unificado, cada localidade pode adotar seus próprios processos e ferramentas de aprovação, aumentando a complexidade na solicitação e autorização de acessos para colaboradores e terceiros. A segurança nos processos de revisão e revogação de acesso também é crucial, e em um cenário descentralizado, cada unidade opera isoladamente, sem uma visão completa dos acessos, o que pode levar a erros na revogação ou até mesmo à falta dela (CHUNG; FERRAIOLO; KUHN, 2006).

A necessidade de acesso cruzado entre diferentes CPDs dentro de uma empresa, bem como os acessos de fornecedores ou parceiros externos, requer um rigoroso processo de autorização, envolvendo várias etapas e diferentes políticas de segurança para cada credencial. Isso resulta na emissão de múltiplas credenciais de acesso, o que pode aumentar os riscos de segurança, como vazamento de credenciais e falha na revogação de acesso após o período necessário (FERRAIOLO et al., 2001).

Dada a complexidade e sensibilidade dessas operações, é necessário que os sistemas de gerenciamento de acesso sejam não apenas seguros, mas também eficientes e fáceis de administrar. Este trabalho propõe estabelecer critérios mínimos de segurança para uma arquitetura centralizadora de gestão de acessos a infraestruturas físicas, como CPDs, permitindo a geração de solicitações de acesso, a submissão a cadeias de aprovação e a rastreabilidade das operações realizadas no sistema.

1.1 Objetivo geral

O objetivo desse trabalho é estabelecer os critérios mínimos de segurança para uma arquitetura de um sistema centralizador de gestão de acessos a estruturas físicas tais como Centro de Processamento de Dados (CPDs).

1.2 Objetivos específicos

Os principais objetivos desse trabalho são:

- Elaborar os casos de usos mínimos necessários a serem atendidos para um sistema centralizador de gestão de acessos;
- Definir os requisitos mínimos de controles de acesso necessários para garantir a implantação de cadeias de autorização no sistema.
- Definir os requisitos mínimos de segurança para gerar rastros de auditoria que garantam a rastreabilidade das ações realizadas nos sistema.

2 Metodologia

A seguir estão detalhadas as etapas essenciais para atingir os objetivos definidos:

2.1 Casos de Uso

Serão criados casos de uso relativos às principais funcionalidades específicas do sistema autorização. Isso permitirá identificar as operações críticas em que são necessárias ações de aprovação hierárquica e etapas extras de segurança. Nesse caso, poderão ser utilizados diagramas UML ou descrições dos elementos estruturais a fim de representar cada cenário.

2.2 Modelo de controle de acesso

Será definido um modelo de controle de acesso que permita a separação de responsabilidades e que evidencie quais atributos são necessários para a execução das operação no sistema.

2.3 Fluxo de Cadeia de Aprovação

Será definido um fluxo de cadeia de aprovação estabelecendo quais atores são responsáveis por delegar e autorizar determinada concessão de acesso. Além disso serão definidas ações de solicitação de acesso e definições de novas cadeias de aprovação. Serão utilizados fluxogramas e/ou matrizes de cadeia de aprovação a qual permitam identificar quem são os donos dos recursos e quem são as partes interessadas.

2.4 Persistência de dados e mensageirias

Serão definidos os requisitos de segurança para persistência das identidades, credenciais e informações de acesso, tais como serviços de diretórios e/ou base de dados. Além disso, serão estabelecidos os canais de comunicação e notificação dos eventos a serem disparados pelo sistema.

2.5 Rastreabilidade e auditoria

Serão definidos critérios e padrões de atributos e ações a fim de gerar rastros de auditoria de maneira que todas as ações críticas possam ser auditadas inequivocamente.

3 Resultados Esperados

Os resultados esperados deste trabalho incluem a elaboração dos requisitos mínimos de segurança de uma arquitetura centralizada para a gestão de

acessos físicos, que aumentará a eficiência e segurança no controle de credenciais em empresas com múltiplos Centros de Processamento de Dados (CPDs). Espera-se reduzir a complexidade das cadeias de aprovação e minimizar os riscos de segurança associados à emissão e revogação de credenciais. Além disso, a centralização deve permitir uma visão integrada dos acessos concedidos, facilitando a rastreabilidade e a auditoria das operações realizadas, garantindo maior conformidade com as políticas de segurança e melhorando a administração de acessos tanto para colaboradores internos quanto para fornecedores externos.

4 Considerações Parciais/Finais

A centralização da gestão de acessos a infraestruturas físicas, como CPDs, é essencial para aumentar a segurança e eficiência operacional. A proposta reduz a complexidade dos processos descentralizados, minimizando riscos como vazamento de credenciais e falhas na revogação de acessos. Além disso, facilita a administração e rastreabilidade, garantindo maior conformidade com políticas de segurança e um controle mais rigoroso e auditável dos acessos.

Referências

CHUNG; FERRAIOLO, D.; KUHN, D. *Assessment of Access Control Systems*. [S.l.]: NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, 2006.

FERRAIOLO, D. F. et al. Proposed nist standard for role-based access control. *ACM Trans. Inf. Syst. Secur.*, Association for Computing Machinery, New York, NY, USA, v. 4, n. 3, p. 224–274, aug 2001. ISSN 1094-9224. Disponível em: <https://doi.org/10.1145/501978.501980>.