DA CONCEPÇÃO À IMPLEMENTAÇÃO DE SSE EM PROVEDORES DE SERVIÇOS DE INTERNET

FROM CONCEPTION TO IMPLEMENTATION OF SSE IN INTERNET SERVICE PROVIDERS

EMERSON EIKITI MATSUKAWA
UNINOVE – UNIVERSIDADE NOVE DE JULHO

BENNY KRAMER COSTA
UNINOVE – UNIVERSIDADE NOVE DE JULHO

ALEXANDRE RODRIGUES PINTO
UNINOVE – UNIVERSIDADE NOVE DE JULHO

THIAGO YOKOYAMA MATSUMOTO
UNINOVE – UNIVERSIDADE NOVE DE JULHO

Comunicação:
O XIII SINGEP foi realizado em conjunto com a 13th Conferência Internacional do CIK (CYRUS Institute of Knowledge), em formato híbrido, com sede presencial na UNINOVE - Universidade Nove de Julho, no Brasil.

Agradecimento à orgão de fomento:
Agradecimentos ao Fundo de Apoio à Pesquisa - FAP UNINOVE e à CAPES.

DA CONCEPÇÃO À IMPLEMENTAÇÃO DE SSE EM PROVEDORES DE SERVIÇOS DE INTERNET

Objetivo do estudo
Analisar os desafios técnicos e estratégicos enfrentados por um provedor de serviços de internet (ISP) na migração de uma arquitetura de segurança legada para um modelo baseado em Zero Trust Architecture, com uso de solução Security Service Edge (SSE).

Relevância/originalidade
O estudo contribui ao explorar empiricamente a integração de soluções SSE com infraestruturas legadas em ambientes brownfield, respondendo a lacunas entre a teoria da Zero Trust Architecture (ZTA) e sua implementação prática em contextos operacionais complexos e tecnicamente restritivos.

Metodologia/abordagem
Trata-se de um relato técnico qualitativo, fundamentado em um estudo de caso único. Os dados foram coletados por observação não participante e análise de artefatos de projeto, acompanhando todo o ciclo de vida da intervenção em um ISP de médio porte.

Principais resultados
A migração promoveu melhorias significativas na segurança, produtividade e experiência do usuário, substituindo VPN por acesso ZTA e centralizando políticas em plataforma unificada, sem comprometer sistemas legados críticos como VoIP, sensíveis à latência e à disponibilidade.

Contribuições teóricas/metodológicas
Oferecer evidências empíricas inéditas sobre a aplicação do framework ZTA (NIST SP 800-207) em ambientes híbridos, propondo um modelo prático e replicável que contribui para o avanço da literatura em segurança da informação aplicada e gestão de infraestrutura.

Contribuições sociais/para a gestão
Apoiar gestores na modernização segura de ambientes operacionais legados, detalhando fatores críticos de sucesso na adoção de SSE em organizações complexas, e demonstrando como elevar o nível de segurança sem prejudicar a performance e usabilidade dos serviços.

Palavras-chave: Arquitetura de Confiança Zero (ZTA), Security Service Edge (SSE), Cibersegurança, Provedor de Serviços de Internet (ISP), Relato Técnico

FROM CONCEPTION TO IMPLEMENTATION OF SSE IN INTERNET SERVICE PROVIDERS

Study purpose
To analyze the technical and strategic challenges faced by an Internet Service Provider (ISP) during the migration from a legacy security architecture to a model based on Zero Trust Architecture (ZTA), through the implementation of a Security Service Edge (SSE) solution.

Relevance / originality
This study contributes by empirically exploring the integration of SSE solutions with legacy infrastructures in brownfield environments, addressing existing gaps between the theoretical foundations of Zero Trust Architecture and its practical implementation in complex and technically constrained operational contexts.

Methodology / approach
This is a qualitative technical report based on a single-case study. Data were collected through non-participant observation and analysis of project artifacts, covering the entire lifecycle of the intervention within a medium-sized ISP.

Main results
The migration led to significant improvements in security, productivity, and user experience by replacing VPN access with ZTA-based access and centralizing policy management in a unified platform, without compromising latency-sensitive and critical legacy systems such as VoIP services.

Theoretical / methodological contributions
The study provides novel empirical evidence on the application of the ZTA framework (NIST SP 800-207) in hybrid environments, proposing a practical and replicable model that advances the literature on applied information security and infrastructure management.

Social / management contributions
It supports managers in the secure modernization of legacy operational environments by detailing critical success factors for the adoption of SSE in complex organizations and demonstrating how to enhance security levels without compromising service performance and usability.

Keywords: Zero Trust Architecture (ZTA), Security Service Edge (SSE), Cybersecurity, Internet Service Provider (ISP), Technical Report