Universitas Indonesia Library >> UI - Tesis Membership

Pengembangan dan Analisis Kerangka Kerja Keamanan Transfer Data Koneksi Host-to-Host pada MPLS, Metro Ethernet, dan SD-WAN Menggunakan Teknik Reduksi Data = Development and Analysis of Host-to-Host Connection Data Transfer Security Framework for MPLS, Metro Ethernet, and SD-WAN Using Data Reduction Techniques

Sianturi, Togu Muara, author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20518467&lokasi=lokal

---

Abstrak

Keamanan data adalah infrastruktur yang dirancang untuk melindungi dan mengamankan data dari akses yang tidak sah, manipulasi data, malfungsi, perusakan, dan pengungkapan data yang tidak sesuai. Saat ini, organisasi banyak menggunakan transfer data untuk memvalidasi dan memverifikasi data menggunakan media yang berbeda terutama dalam koneksi host-to-host. Penelitian ini berfokus pada pertukaran data (end-to-end communication) menggunakan arsitektur jaringan Multi Protocol Label Switching (MPLS), Metro Ethernet, dan Software Defined Wide Area Network (SD-WAN) dengan pihak ketiga. Risiko yang timbul dari serangan siber pada transfer data pada transaksi host-to-host adalah kehilangan data, reputasi institusi, hingga yang paling berisiko adalah distribusi data tersebut. Penelitian ini bertujuan untuk mengembangkan kerangka kerja untuk memverifikasi data yang ditransfer dari satu host ke host lain di PT. ABC dengan standar keamanan yang berlaku yang sesuai dan mengikuti kebutuhan untuk membantu organisasi. Metodologi yang digunakan dalam penelitian ini adalah studi literatur, analisis data dengan metode reduksi data terhadap 4 standar dan aturan keamanan siber dengan tujuan untuk mengembangkan kerangka kerja keamanan transfer data dengan objek penelitian, yaitu ISO/EIC 27001:2013, NIST SP800- 161, ITU-T X.805, dan POJK 4/POJK.05/2021. Pengembangan kerangka kerja menghasilkan 8 dimensi keamanan, 20 kebutuhan keamanan, dan 41 aktivitas, serta memberikan mitigasi yang dapat meningkatkan sistem keamanan pertukaran data pada koneksi host-to-host di PT. ABC. Evaluasi dilakukan dengan dengan pendekatan professional judgement untuk mengetahui deskripsi penilaian ahli pada setiap variabel pembentuk kerangka kerja berdasarkan melengkapi hasil analisis statistik. Melalui konsep kerangka kerja keamanan transfer data host-to-host yang dihasilkan diharapkan dapat menjadi masukan dalam penyusunan instrumen tingkat kematangan keamanan siber dengan pihak ketiga.
.....Data security is an infrastructure designed to protect and secure data from unauthorized access, data manipulation, malfunction, destruction, and inappropriate data disclosure. Currently, organizations widely use data transfer to validate and verify data using different media particularly in host-to-host connections. This research focuses on data exchanged (end-to-end communication) using Multi Protocol Label Switching (MPLS), Metro Ethernet, and Software Defined Wide Area Network (SD-WAN) network architecture with third parties. The risks that arise from cyber attacks on data transfer in host-to-host are data loss, institutional reputation, to the riskiest is the distribution of the data. This research aims to develop a design and analysis framework for verifying data transferred from one host to another in ABC organization by applicable security standards that are appropriate and follow its needs to help the organization. Methodology used in this research is a literature study, data analysis with data reduction method on 4 standards and cyber security policies to develop a data transfer security framework with research objects, namely ISO/EIC 27001:2013, NIST SP800-161, ITU -T X.805, and POJK 4/POJK.05/2021. The framework development resulted in 8

security dimensions, 20 security requirements, and 41 activities, as well as providing mitigations that could improve the security system of data exchange on host-to-host connections at PT. ABC. The evaluation was carried out using a professional judgment approach to determine the description of the expert's judgment on each variable forming the framework based on the complete statistical analysis results. Through the concept of a host-to-host data transfer security framework, it is hoped that it can be used as input in the preparation of cybersecurity maturity level instruments with third parties.