Materi Seminar Nasional Karsa Nusantara I Tahun 2024 (Karsa Nusantara 2024)

Menjaga Integritas dan Keamanan Informasi

Nonot Wisnu Karyanto*[1]

[1,] Program Studi Informatika, Fakultas Teknik, Universitas Wijaya Kusuma Surabaya, Indonesia
Email:[1]nonotwk@uwks.ac.id
*Penulis Korespondensi

Abstrak

Keamanan informasi merupakan upaya perlindungan terhadap sumber daya informasi dari penyalahgunaan oleh pihak yang tidak berwenang. Konsep dasar keamanan informasi mencakup aspek kerahasiaan, integritas, ketersediaan, autentikasi, otorisasi, audit, manajemen risiko, kesadaran pengguna, kepatuhan regulasi, serta tanggap insiden. Untuk membangun sistem keamanan informasi yang kuat, diperlukan dukungan dari struktur organisasi, kebijakan keamanan, prosedur pengamanan, dan sumber daya manusia yang kompeten. Ancaman terhadap keamanan informasi dapat berasal dari faktor internal maupun eksternal, baik yang disengaja maupun tidak disengaja, sehingga menimbulkan risiko seperti pengungkapan, perubahan, atau penghancuran data. Pengelolaan keamanan informasi terbagi menjadi manajemen keamanan informasi harian dan manajemen keberlanjutan bisnis. Selain itu, integritas dan keandalan data menjadi faktor penting dalam menjaga validitas informasi. Penerapan standar keamanan informasi menjadi pedoman dalam melindungi data dari berbagai ancaman, dengan tujuan utama menjaga kerahasiaan, integritas, dan ketersediaan informasi. Kesimpulan dari keamanan informasi menegaskan pentingnya proteksi data, kepatuhan regulasi, pendidikan dan pelatihan, investasi dalam teknologi, serta kesiapan menghadapi insiden keamanan.

Kata kunci: Keamanan Informasi, Integritas, Manajemen Risiko, Perlindungan Data, Standar Keamanan

Abstract

Information security is an effort to protect information resources from misuse by unauthorized parties. The fundamental concepts of information security include confidentiality, integrity, availability, authentication, authorization, auditing, risk management, user awareness, regulatory compliance, and incident response. To build a strong information security system, support is needed from organizational structures, security policies, security procedures, and competent human resources. Threats to information security can come from both internal and external factors, whether intentional or unintentional, leading to risks such as data disclosure, modification, or destruction. Information security management is divided into daily information security management and business continuity management. Additionally, data integrity and reliability are crucial in maintaining the validity of information. The implementation of information security standards serves as a guideline for protecting data from various threats, with the primary goal of ensuring confidentiality, integrity, and availability. The conclusion of information security emphasizes the importance of data protection, regulatory compliance, education and training, investment in technology, and preparedness for security incidents.

***Keywords**: Data Protection, Information Security, Integrity, Risk Management, Security Standards*

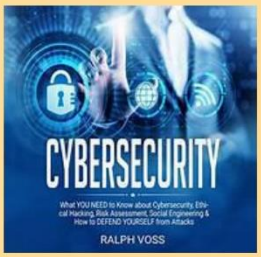
Fakultas Teknik,
Universitas Wijaya Kusuma Surabaya
ISSN: XXXX-XXXX, Eissn: XXXX-XXXX
2024

Konsep dan Praktek Dasar Keamanan Informasi

1. Kerahasiaan (Confidentiality)
2. Integritas (Integrity)
3. Ketersediaan (Availability)
4. Autentikasi (Authentication)
5. Otorisasi (Authorization)
6. Audit dan Pemantauan (Auditing and Monitoring)
7. Manajemen Risiko (Risk Management)
8. Pelatihan dan Kesadaran Pengguna (User Training and Awareness)
9. Kepatuhan dan Regulasi (Compliance and Regulation)
10. Tanggap Insiden (Incident Response)

Dukungan yang diberikan untuk membentuk keamanan informasi

1. Penyediaan struktur organisasi
2. Kebijakan keamanan
3. Prosedur Proses Pengamanan
4. Sumber Daya manusia



Seminar Nasional

Penerapan Keamanan Informasi

- Perusahaan
- Organisasi
- Lembaga Pemerintahan
- Perguruan Tinggi atau
- Individu

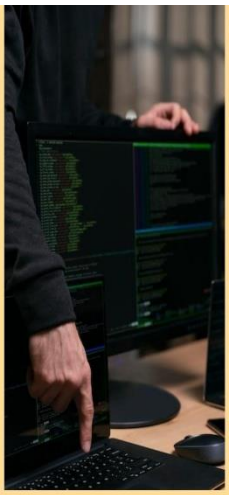
Fakultas Teknik,
Universitas Wijaya Kusuma Surabaya
ISSN: XXXX-XXXX, Eissn: XXXX-XXXX
2024

Tujuan Keamanan Informasi

adalah untuk melindungi informasi dari berbagai ancaman guna memastikan kelangsungan bisnis, meminimalisir risiko, dan memaksimalkan keuntungan serta peluang bisnis.

Kedudukan

Tingkat keamanan informasi memiliki kedudukan yang berlawanan dengan tingkat akses informasi. Semakin mudah suatu informasi untuk diakses, maka tingkat keamanan informasi menjadi semakin rumit. Kondisi ini dikarenakan informasi tidak lagi hanya dapat diakses secara fisik. Informasi kini dapat diakses secara non fisik melalui internet dengan media komputer. Kemudahan akses ini menambah peluang kebocoran atau pembobolan informasi.



Fakultas Teknik,
Universitas Wijaya Kusuma Surabaya
ISSN: XXXX-XXXX, Eissn: XXXX-XXXX
2024

Aspek Keamanan

Keamanan informasi adalah praktik melindungi informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis, meminimalisir risiko, dan memaksimalkan ROI serta peluang bisnis.

- Kerahasiaan (Confidentiality)
- Integritas (Integrity)
- Ketersediaan (Availability)
- Keaslian (Authenticity)
- Akuntabilitas (Accountability)
- Kontrol Akses (Access Control)
- Manajemen Risiko (Risk Management)
- Kepatuhan (Compliance)
- Kesadaran dan Pelatihan (Awareness and Training)
- Kebijakan dan Prosedur (Policies and Procedures)

Ancaman

Setiap hal yang dapat memberikan kondisi berbahaya terhadap sumber daya informasi disebut sebagai ancaman keamanan informasi. Bentuk ancaman ini dapat berupa orang, organisasi, mekanisme atau suatu peristiwa. Ancaman keamanan informasi dapat ada secara disengaja maupun tidak disengaja. Penyebab timbulnya ancaman keamanan informasi dapat berasal dari sisi internal maupun eksternal

Fakultas Teknik,
Universitas Wijaya Kusuma Surabaya
ISSN: XXXX-XXXX, Eissn: XXXX-XXXX
2024

Resiko

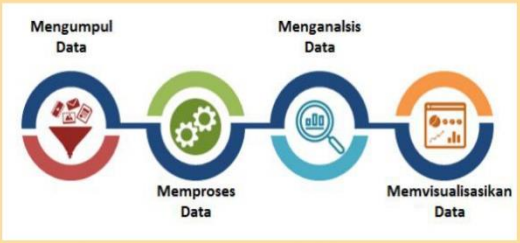
Risiko merupakan berbagai kemungkinan yang dapat disebabkan oleh ancaman informasi selama melakukan pelanggaran keamanan informasi. Timbulnya risiko keamanan informasi merupakan akibat dari tindakan yang dilakukan tanpa pemberian hak pengelolaan. Terdapat beberapa jenis risiko keamanan informasi yaitu pengungkapan, penggunaan, penghancuran, penolakan layanan dan pengubahan informasi tanpa pemberian hak pengelolaan.

Pengelolaan

Pengelolaan keamanan informasi terbagi menjadi keamanan harian yang disebut manajemen keamanan informasi, dan persiapan pemecahan masalah operasional yang disebut manajemen keberlanjutan bisnis.Pengelolaan keamanan informasi dapat diberikan kepada petugas keamanan sistem informasi.

Integritas Data

Integritas data adalah konsep dalam pengelolaan data yang menjamin keakuratan, kelengkapan, dan konsistensi data sepanjang *life cycle*, memastikan data tidak *corrupted* atau diubah secara tidak sah.



Alasan Pentingnya Menjaga Integritas Data

- **Efisiensi operasional**
- **Kepatuhan regulasi**
- **Kepercayaan pelanggan**
- **Keamanan data**
- **Analitik dan wawasan bisnis**
- **Optimasi sumber daya**
- **Meningkatkan kualitas produk atau layanan**
- **Mengurangi risiko**

Fakultas Teknik,
Universitas Wijaya Kusuma Surabaya
ISSN: XXXX-XXXX, Eissn: XXXX-XXXX
2024

Metode Menjaga Integritas Data

- Validasi Data
- Enkripsi Data
- Kontrol Akses
- Audit dan Pematauan
- Redundansi dan Backup
- Kontrol Kualitas Data
- Pendidikan dan Pelatihan
- Pemulihan Bencana

Keandalan Data

adalah sejauh mana data atau hasil yang diperoleh dari suatu penelitian atau pengukuran konsisten dan dapat dipercaya. Keandalan ini penting dalam berbagai bidang, seperti penelitian ilmiah, analisis bisnis, pengembangan produk, dan pengambilan keputusan.

Fakultas Teknik,
Universitas Wijaya Kusuma Surabaya
ISSN: XXXX-XXXX, Eissn: XXXX-XXXX
2024

Aspek Keandalan Data

1. Reproduksibilitas (Reproducibility)
2. Konsistensi Internal (Internal Consistency)
3. Stabilitas (Stability)
4. Kesetaraan Antar-pengamat (Inter-rater Reliability)

Standar Keamanan

Standar keamanan informasi adalah seperangkat praktik, kebijakan, prosedur, dan teknologi yang dirancang untuk melindungi informasi dari berbagai ancaman, seperti akses tidak sah, pengungkapan tidak sah, modifikasi, atau penghancuran. Tujuan utama dari standar keamanan informasi adalah untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi yang sensitif atau penting bagi suatu organisasi atau individu.

Kesimpulan yang dapat diperoleh dari keamanan informasi :

1. **Pentingnya Proteksi Data**
2. **Ancaman Keamanan**
3. **Kepatuhan dan Regulasi**
4. **Pendidikan dan Pelatihan**
5. **Manajemen Risiko**
6. **Investasi dalam Teknologi**
7. **Pentingnya Pengawasan dan Audit**
8. **Kesiapan terhadap Insiden**

Referensi :

1. "Information Security Management Principles" oleh Andy Taylor, David Alexander, Amanda Finch, dan David Sutton.
2. "Security Engineering: A Guide to Building Dependable Distributed Systems" oleh Ross Anderson.
3. "Computer Security: Principles and Practice" oleh William Stallings dan Lawrie Brown.
4. **"Database System Concepts" oleh Silberschatz, Korth, dan Sudarshan** - Buku ini membahas berbagai konsep dan teknik dalam manajemen database, termasuk integritas data.
5. **Websites and Online Resources**: Situs web seperti SANS Institute, InfoSec Institute, dan CSO Online yang menyediakan artikel, panduan, dan sumber daya tentang keamanan informasi.
6. https://rootofscience.com/blog/wp-content/uploads/2020/10/image-52-580x241.png
7. https://r17.co.id/assets/img/article/20221109080446221109-R17G-Artikel-Waspada.jpg
8. https://glints.com/id/lowongan/wp-content/uploads/2020/08/integritas-dalam-bekerja.png
9. https://png.pngtree.com/png-vector/20220621/ourmid/pngtree-vector-illustration-of-decorative-elements-depicting-database-cloud-network-servers-and-compute