Era digital yang terus berkembang, kebutuhan akan sistem keamanan informasi yang handal dan efektif semakin mendesak. Semakin kompleksnya ancaman cyber dan semakin tingginya tingkat ketergantungan pada teknologi informasi membuat organisasi, perusahaan, dan individu rentan terhadap serangan peretas, pencurian data, dan pelanggaran privasi. Oleh karena itu, penting bagi kita untuk memahami secara menyeluruh konsep dan praktik sistem keamanan informasi untuk melindungi aset digital yang berharga. Buku ini bertujuan untuk memberikan pandangan menyeluruh tentang sistem keamanan informasi, mulai dari konsep dasar hingga teknologi terkini yang digunakan untuk melindungi data dan infrastruktur komputer. Kami akan membahas mengapa keamanan informasi menjadi begitu penting dalam konteks modern, tantangan utama yang dihadapi dalam menjaga keamanan data, dan langkah-langkah praktis yang dapat diambil untuk mengurangi risiko dan melindungi informasi sensitif.

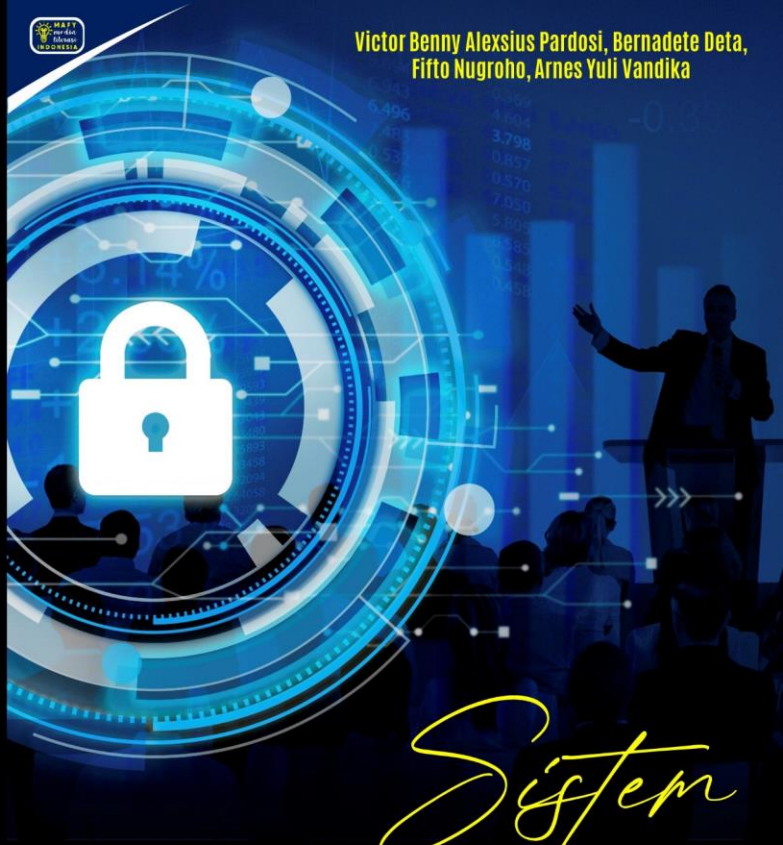
Buku ini membahas tentang Konsep dasar Keamanan Sistem Informasi, Metode Perlindungan dan Legitimasi Informasi, Ancaman Malware dan Teknik Pengamanan, Metode Peretasan dan Pencegahannya, Teknologi Pengamanan Jaringan, Audit dan Keamanan Sistem Informasi, Manajemen Etika dan Tantangan Terkini.

PT MAFY MEDIA LITERASI INDONESIA
ANGGOTA IKAPI 041/SBA/2023
Email : penerbitmafy@gmail.com
Website : penerbitmafy.com
FB : Penerbit Mafy

PENDIDIKAN
ISBN 978-623-8600-34-4
9 786238 606344

SISTEM KEAMANAN INFORMASI

Victor Benny Alexsius Pardosi, Bernadete Deta,
Fifto Nugroho, Arnes Yuli Vandika



Sistem

KEAMANAN INFORMASI

SISTEM KEAMANAN INFORMASI

UU No 28 Tahun 2014 tentang Hak Cipta

Fungsi dan sifat hak cipta Pasal 4

Hak Cipta sebagaimana dimaksud dalam Pasal 3 huruf a merupakan hak eksklusif yang terdiri atas hak moral dan hak ekonomi.

Pembatasan Pelindungan Pasal 26

Ketentuan sebagaimana dimaksud dalam Pasal 23, Pasal 24, dan Pasal 25 tidak berlaku terhadap:

i. penggunaan kutipan singkat ciptaan dan/atau produk hak terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
ii. penggandaan ciptaan dan/atau produk hak terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
iii. penggandaan ciptaan dan/atau produk hak terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan fonogram yang telah dilakukan pengumuman sebagai bahan ajar; dan
iv. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu ciptaan dan/atau produk hak terkait dapat digunakan tanpa izin pelaku pertunjukan, produser fonogram, atau lembaga penyiaran.

Sanksi Pelanggaran Pasal 113

1. Setiap orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap orang yang dengan tanpa hak dan/atau tanpa izin pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).

SISTEM KEAMANAN INFORMASI

Victor Benny Alexsius Pardosi, Bernadete Deta, Fifto Nugroho, Arnes Yuli Vandika

MAFY media literasi INDONESIA

SISTEM KEAMANAN INFORMASI

Penulis:
Victor Benny Alexsius Pardosi, Bernadete Deta,
Fifto Nugroho, dan Arnes Yuli Vandika

Editor:
Andi Asari, SIP., S.Kom., M.A.

Desainer:
Tim Mafy

Sumber Gambar Cover:
www.freepik.com

Ukuran:
x, 130 hlm., 15,5 cm x 23 cm

ISBN:
978-623-8606-34-4

Cetakan Pertama:
April 2024

PT MAFY MEDIA LITERASI INDONESIA
ANGGOTA IKAPI 041/SBA/2023
Kota Solok, Sumatera Barat, Kode Pos 27312
Kontak: 081374311814
Website: www.penerbitmafy.com
E-mail: penerbitmafy@gmail.com

DAFTAR ISI

PRAKATA

Segala puji syukur kami panjatkan kepada Tuhan yang maha Esa, karena atas pertolongan dan limpahan rahmat-Nya sehingga penulis bisa menyelesaikan buku yang berjudul "Sistem Keamanan Informasi". Buku ini di susun secara lengkap dengan tujuan untuk memudahkan para pembaca memahami isi buku ini. Buku ini membahas tentang Konsep Dasar Keamanan Sistem Informasi, Metode Perlindungan dan Legitimasi Informasi, Ancaman Malware dan Teknik Pengamanan, Metode Peretasan dan Pencegahannya, Teknologi Pengamanan Jaringan, Audit dan Keamanan Sistem Informasi, Manajemen Etika dan Tantangan Terkini.

Kami menyadari bahwa buku yang ada di tangan pembaca ini masih banyak kekurangan. Maka dari itu kami sangat mengharapkan saran untuk perbaikan buku ini di masa yang akan datang. Dan tidak lupa kami mengucapkan terimakasih kepada semua pihak yang telah membantu dalam proses penerbitan buku ini. Semoga buku ini dapat membawa manfaat dan dampak positif bagi para pembaca.

Penulis, 4 Maret 2023

Pendahuluan

Era digital yang terus berkembang, kebutuhan akan sistem keamanan informasi yang handal dan efektif semakin mendesak. Semakin kompleksnya ancaman *cyber* dan semakin tingginya tingkat ketergantungan pada teknologi informasi membuat organisasi, perusahaan, dan individu rentan terhadap serangan peretas, pencurian data, dan pelanggaran privasi. Oleh karena itu, penting bagi kita untuk memahami secara menyeluruh konsep dan praktik sistem keamanan informasi untuk melindungi aset digital yang berharga. Buku ini bertujuan untuk memberikan pandangan menyeluruh tentang sistem keamanan informasi, mulai dari konsep dasar hingga teknologi terkini yang digunakan untuk melindungi data dan infrastruktur komputer. Kami akan membahas mengapa keamanan informasi menjadi begitu penting dalam konteks *modern*, tantangan utama yang dihadapi dalam menjaga keamanan data, dan langkah-langkah praktis yang dapat diambil untuk mengurangi risiko dan melindungi informasi sensitif.

Dalam perjalanan ini, kita akan menjelajahi berbagai jenis ancaman *cyber*, seperti serangan *phishing*, *malware*, dan serangan DDoS, serta teknik dan alat yang digunakan oleh peretas untuk mengeksploitasi kelemahan dalam sistem. Kami juga akan membahas pentingnya kebijakan keamanan yang efektif, pelatihan karyawan, dan teknologi keamanan yang canggih dalam membangun pertahanan yang kokoh terhadap ancaman *cyber* yang terus berkembang. Dengan pemahaman yang kuat tentang sistem keamanan informasi, diharapkan pembaca akan dapat mengidentifikasi risiko yang ada, mengambil langkah-langkah proaktif untuk melindungi diri, dan berkontribusi pada pembentukan lingkungan digital yang lebih aman dan andal bagi semua orang. Teruslah bergabung dengan kami saat kami memperdalam pengetahuan kita tentang keamanan informasi, menjaga kesadaran terhadap ancaman, dan memperkuat pertahanan kami terhadap peretasan dan serangan *cyber*.

BAB I

KONSEP DASAR KEAMANAN SISTEM INFORMASI

A. Pengantar Keamanan Sistem Informasi

Keamanan sistem informasi merujuk pada perlindungan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, inspeksi, pencatatan atau penghancuran yang tidak sah. Tujuannya ialah untuk menjaga kerahasiaan, integritas, dan ketersediaan data dan sistem informasi mencakup langkah-langkah yang dirancang untuk mencegah pelanggaran keamanan yang melibatkan informasi yang disimpan secara elektronik dan fisik. Menjaga agar informasi sensitif tetap bersembunyi dari orang yang tidak berhak, memastikan bahwa hanya individu yang berhak saja yang dapat mengakses informasi tersebut. Memastikan bahwa informasi akurat dan lengkap, dan bahwa tidak ada modifikasi yang tidak sah terhadap data, baik sengaja maupun tidak sengaja (Stallings, 2017).

Menjamin bahwa informasi dan sumber daya terkait dapat diakses oleh individu yang berhak ketika dibutuhkan. Penerapan keamanan sistem informasi

melibatkan penggunaan teknologi keamanan fisik dan elektronik, prosedur administratif, serta kebijakan manajemen yang komprehensif termasuk penggunaan *firewall*, enkripsi, *software antivirus*, serta praktik seperti autentikasi pengguna dan manajemen akses. Keamanan sistem informasi menjadi semakin penting seiring dengan meningkatnya ancaman *cyber* seperti *malware*, *phising*, dan serangan *ransomware*, serta kebutuhan untuk mematuhi peraturan perlindungan data seperti *General Data Protection Regulation* (GDPR) di Uni Eropa dan berbagai Undang-Undang perlindungan data lainnya di seluruh dunia. Keamanan informasi merupakan salah satu aspek kritis dalam pengelolaan teknologi informasi dan komunikasi, terutama di era digital saat ini, di mana data dan informasi menjadi aset berharga bagi individu, bisnis, dan pemerintah. Pentingnya keamanan informasi dapat dilihat dari beberapa perspektif utama, diantaranya:

1. Perlindungan Data Pribadi

   Dengan meningkatnya pengumpulan data pribadi oleh perusahaan dan organisasi, keamanan informasi membantu melindungi privasi individu dan mencegah pencurian identitas. Peraturan seperti *General Data Protection Regulation* (GDPR) di Uni Eropa dan berbagai Undang-Undang perlindungan data di seluruh dunia menekankan pentingnya keamanan informasi untuk mematuhi hukum.

2. Integritas dan Kepercayaan Bisnis

   Keamanan informasi yang efektif membangun kepercayaan pelanggan, yang krusial untuk keberlangsungan bisnis online dan *e-commerce*.

Pelanggaran keamanan dapat merusak reputasi perusahaan secara signifikan, mempengaruhi kepercayaan dan loyalitas pelanggan dalam jangka panjang.

3. Operasional dan Kontinuitas Bisnis

   Serangan siber seperti ransomware dapat mengganggu operasional bisnis dengan menahan data sebagai tebusan, sehingga keamanan informasi penting untuk memastikan ketersediaan layanan. Strategi keamanan informasi yang efektif termasuk rencana pemulihan bencana untuk memastikan bisnis dapat terus beroperasi bahkan setelah insiden keamanan.

4. Kepatuhan Terhadap Regulasi

   Bisnis dan organisasi sering diwajibkan oleh Undang-Undang untuk melindungi data pelanggan dan informasi sensitif lainnya. Pelanggaran keamanan informasi dapat mengakibatkan denda yang besar dan sanksi lainnya dari regulator.

5. Perlindungan Terhadap Ancaman Siber

   Lanskap ancaman siber terus berkembang, dengan serangan menjadi lebih canggih sehingga keamanan informasi yang kuat diperlukan untuk melindungi terhadap risiko ini. Biaya untuk menerapkan keamanan informasi seringkali jauh lebih rendah dibandingkan dengan kerugian finansial dan non-finansial akibat pelanggaran keamanan.

6. Perlindungan Properti Intelektual

   Keamanan informasi juga penting untuk melindungi properti intelektual dan informasi rahasia bisnis yang jika bocor dapat menguntungkan pesaing.

Dalam konteks global saat ini, di mana serangan siber menjadi semakin sering terjadi dan data menjadi semakin terintegrasi dalam kehidupan sehari-hari, pentingnya keamanan informasi tidak bisa diremehkan. Hal ini membutuhkan komitmen berkelanjutan dari semua pihak, mulai dari individu hingga pemerintah, untuk melindungi infrastruktur informasi dan memastikan bahwa data dan sistem tetap aman dari ancaman.

B. Prinsip Dasar Keamanan Informasi

1. Kerahasiaan *(Confidentiality)*

Prinsip dasar kerahasiaan *(confidentiality)* dalam keamanan informasi merujuk pada perlindungan informasi dari akses tidak sah atau pengungkapan kepada pihak yang tidak berhak. Tujuan dari prinsip kerahasiaan adalah untuk memastikan bahwa informasi sensitif, seperti data pribadi, rahasia bisnis, atau informasi keuangan hanya dapat diakses oleh individu atau entitas yang memiliki izin untuk melihat atau menggunakan informasi tersebut. Kerahasiaan merupakan salah satu pilar utama dalam triad keamanan informasi, bersama dengan integritas dan ketersediaan.

Implementasi Kerahasiaan

Untuk menjaga kerahasiaan informasi, organisasi menerapkan berbagai strategi dan teknologi, termasuk: (Florackis et al., 2023).

a. Enkripsi

   Menggunakan algoritma matematika untuk mengubah informasi menjadi format yang tidak dapat dibaca tanpa kunci deskripsi. Enkripsi digunakan baik untuk data yang disimpan *(data at rest)* maupun data yang dikirimkan *(data in transit)*.

b. Kontrol Akses

   Menerapkan kebijakan yang membatasi akses ke informasi hanya kepada pengguna yang berhak. Dapat meliputi autentikasi pengguna, manajemen hak akses, dan pembagian peran *(role based access control).*

c. Pelatihan Kesadaran Keamanan

   Mengedukasi karyawan tentang pentingnya menjaga kerahasiaan informasi dan cara-cara untuk melindungi data dari kebocoran atau akses tidak sah.

d. Penggunaan *Virtual Private Networks* (VPN)

   Memungkinkan transmisi data yang aman melalui jaringan publik seperti *internet* dengan membuat terowongan enkripsi antara perangkat pengguna dan jaringan.

e. *Non-Disclosure Agreements* (NDA)

   Perjanjian hukum antara pihak-pihak yang terlibat dalam pertukaran informasi yang

menetapkan batasan tentang bagaimana informasi dapat digunakan dan diungkapkan.

Tantangan dalam Menjaga Kerahasiaan

a. Serangan *Cyber*

Ancaman seperti *phising*, *malware*, dan serangan *man in the middle* dapat mengkompromikan kerahasiaan informasi.

b. Insider Threats

Risiko dari dalam organisasi, baik disengaja maupun tidak disengaja, yang dapat mengakibatkan kebocoran informasi.

c. Kompleksitas Data

Volume data yang besar dan kompleksitas sistem informasi dapat membuat sulit untuk mengidentifikasi dan melindungi semua informasi sensitif.

Pentingnya Kerahasiaan

a. Pemenuhan Regulasi

Banyak Undang-Undang dan regulasi, seperti *General Data Protection Regulation* (GDPR), menuntut perlindungan kerahasiaan data pribadi.

b. Kepercayaan dan Reputasi

Mampu menjaga kerahasiaan informasi membangun kepercayaan dari pelanggan dan mitra bisnis serta melindungi reputasi organisasi.

c. Keunggulan Kompetitif

Rahasia bisnis dan informasi proprietari yang terjaga kerahasiaannya dapat memberikan keunggulan kompetitif bagi organisasi.

Menjaga kerahasiaan informasi memerlukan pendekatan holistik yang mencakup teknologi, proses, dan kebijakan serta keterlibatan aktif dari semua pihak dalam organisasi.

2. Integritas *(Integrity)*

Integritas dalam konteks keamanan informasi merujuk pada perlindungan informasi dari modifikasi yang tidak sah, baik disengaja maupun tidak disengaja. Hal ini menjamin bahwa data tetap akurat dan lengkap sepanjang siklus hidupnya (Wijoyo, Rosadi, et al., 2023). Integritas adalah salah satu dari tiga pilar utama dalam model keamanan informasi, bersama dengan kerahasiaan *(confidentiality)* dan ketersediaan *(availability),* yang sering disingkat menjadi triad CIA.

Implementasi Integritas

Untuk memastikan integritas data, organisasi mengimplementasikan berbagai kontrol dan teknik, termasuk:

a. Kontrol Akses

Memastikan bahwa hanya pengguna yang berhak dapat mengakses dan memodifikasi data. Kontrol akses yang ketat membantu mencegah akses atau perubahan tidak sah terhadap informasi.

b. Penggunaan Fungsi Hash

Fungsi hash digunakan untuk memverifikasi integritas data dengan menghasilkan ringkasan data (hash *value*) yang

unik. Perubahan apapun pada data akan menghasilkan nilai hash yang berbeda, sehingga mudah mendeteksi modifikasi.

c. Tanda Tangan Digital

Menggunakan kriptografi untuk memverifikasi pengirim dan memastikan bahwa pesan tidak diubah selama transmisi. Tanda tangan digital menyediakan otentikasi dan integritas untuk komunikasi digital.

d. *Audit* dan *Logging*

Mencatat aktivitas pengguna dan sistem secara detail untuk menyediakan bukti historis dari transaksi dan dapat digunakan untuk mendeteksi, menyelidiki, dan mencegah perubahan tidak sah.

e. Manajemen Patch dan Pembaruan

Memastikan bahwa semua sistem operasi dan aplikasi terus diperbarui dengan patch keamanan terkini untuk melindungi terhadap kerentanan yang dapat dimanfaatkan untuk merusak data.

Tantangan dalam Menjaga Integritas

a. Serangan Siber

Serangan seperti *malware* dan *ransomware* dapat merusak atau mengubah data.

b. Kesalahan Manusia

Kesalahan tidak disengaja oleh pengguna atau administrator sistem dapat mengakibatkan perubahan atau penghapusan data.

c. *Insider Threats*

Ancaman dari dalam organisasi, di mana karyawan dengan akses dapat secara sengaja mengubah informasi untuk tujuan jahat.

Pentingnya Integritas

a. Kepercayaan

Integritas data yang terjaga membangun kepercayaan dari pengguna, pelanggan, dan mitra bisnis.

b. Pemenuhan Regulasi

Banyak regulasi dan standar industri mengharuskan organisasi untuk menjaga integritas data, seperti *Health Insurance Portability and Accountability* (HIPAA) untuk data kesehatan dan PCI DSS untuk data kartu pembayaran.

c. Pengambilan Keputusan

Keputusan bisnis yang akurat dan tepat waktu bergantung pada data yang akurat dan lengkap. Kerusakan pada integritas data dapat mengakibatkan kerugian finansial dan reputasi.

Memastikan integritas data memerlukan kombinasi dari kontrol teknis, prosedur operasional, dan kebijakan keamanan yang efektif. Pendekatan berlapis ini membantu melindungi data dari modifikasi tidak sah, memastikan keakuratan dan keandalan informasi yang digunakan oleh organisasi.

3. Ketersediaan *(Availability)*

Ketersediaan *(availability)* dalam konteks keamanan informasi merujuk pada prinsip yang menjamin informasi dan sistem terkait dapat diakses dan digunakan oleh pihak yang berhak kapan pun dibutuhkan. Prinsip ini menekankan pentingnya memastikan bahwa data, aplikasi, dan sumber daya informasi teknologi lainnya tersedia untuk operasi bisnis yang berkelanjutan, tanpa gangguan yang signifikan. Ketersediaan menjadi salah satu dari tiga pilar utama dalam model keamanan informasi CIA *Triad*, bersama dengan Kerahasiaan *(Confidentiality)* dan Integritas *(Integrity).*

Implementasi Ketersediaan

Untuk memastikan ketersediaan, organisasi menerapkan berbagai teknik dan strategi, termasuk:

a. *Redundansi* dan *Failover*

Menduplikasi sistem kritis dan komponen jaringan untuk memastikan bahwa jika satu sistem gagal, sistem lain dapat mengambil alih tanpa gangguan yang signifikan terhadap layanan.

b. Backup Data

Melakukan backup data secara teratur ke lokasi yang aman dan terpisah untuk memastikan bahwa data dapat dipulihkan setelah insiden kehilangan data, seperti serangan ransomware atau kerusakan fisik.

c. Pemulihan Bencana *(Disaster Recovery)*

Mengembangkan dan mengimplementasi-kan rencana pemulihan bencana yang mencakup prosedur dan langkah-langkah untuk memulihkan operasi informasi teknologi setelah bencana atau kegagalan sistem.

d. Pemeliharaan dan Pembaruan

Menjaga perangkat keras dan perangkat lunak agar tetap diperbarui dan dalam kondisi baik, termasuk penerapan patch keamanan untuk mengurangi risiko *downtime* karena kerentanan.

e. Pengukuran Kinerja dan *Monitoring*

Memantau kinerja sistem dan jaringan secara berkelanjutan untuk mendeteksi dan mengatasi masalah ketersediaan sebelum berdampak pada pengguna akhir.

Tantangan dalam Menjaga Ketersediaan

a. Serangan DoS/DdoS

Serangan *Denial of Service* (DoS) dan *Dsitributed Denial of Service* (DDoS) dirancang untuk membanjiri jaringan atau sumber daya dengan lalu lintas yang berlebihan mengakibatkan layanan tidak tersedia bagi pengguna yang sah.

b. Kegagalan Infrastruktur

Kerusakan pada infrastruktur fisik, seperti kerusakan perangkat keras atau gangguan listrik, dapat menyebabkan *downtime* yang signifikan.

c. Kesalahan Manusia

Kesalahan operasional oleh staf informasi teknologi atau pengguna dapat tidak sengaja mengganggu ketersediaan sistem dan layanan.

Pentingnya Ketersediaan

a. Kontinuitas Bisnis

Menjaga ketersediaan sistem informasi penting untuk memastikan operasi bisnis yang berkelanjutan dan menghindari kerugian finansial akibat downtime.

b. Kepatuhan Regulasi

Beberapa regulasi dan standar industri mensyaratkan organisasi untuk memastikan ketersediaan data dan layanan, menjadikannya komponen penting dari kepatuhan.

c. Kepuasan Pengguna

Ketersediaan layanan yang konsisten mempengaruhi pengalaman dan kepuasan pengguna, yang dapat mempengaruhi reputasi dan kesetiaan pelanggan.

Ketersediaan membutuhkan perencanaan dan investasi dalam infrastruktur, prosedur, dan kebijakan yang memadai untuk memastikan bahwa sistem dan data dapat diandalkan dan tersedia bagi pengguna yang membutuhkan, bahkan di hadapan gangguan atau serangan (Lestari & Nasution, 2023).

C. Ancaman dan Serangan terhadap Sistem Informasi

Tabel 1. Jenis Ancaman dan Serangan terhadap Sistem Informasi

Jenis Ancaman/ Serangan	Deskripsi	Contoh
Malware	Perangkat lunak jahat yang dirancang untuk merusak atau mendapatkan akses tidak sah ke sistem termasuk *virus*, *worm*, *trojan*, dan *ransomware*.	*WannaCry Ransomware*: Serangan *ransomware* global pada tahun 2017 yang mengenkripsi *file* pada sistem yang terinfeksi dan meminta tebusan untuk deskripsi.
Phising	Teknik penipuan yang bertujuan untuk mendapatkan data sensitif seperti *username* dan *password* dengan menyamar sebagai entitas terpercaya dalam komunikasi elektronik.	*Email Phising Bank*: Email yang menyamar sebagai bank meminta korban untuk memperbarui informasi akun melalui link palsu yang mengarah ke situs phising.
Serangan *Man in the Middle* (MitM)	Serangan dimana penyerang secara diam-diam meneruskan atau mengubah komunikasi antara dua pihak yang berkomunikasi tanpa pengetahuan.	Intersepsi WiFi: Penyerang yang menggunakan teknik *sniffing* pada jaringan WiFi publik untuk mencuri informasi yang ditransmisikan antara pengguna dan situs *web*.

Menghadapi ancaman dan serangan ini membutuhkan strategi keamanan informasi yang komprehensif termasuk penerapan kebijakan keamanan yang ketat, penggunaan teknologi keamanan terkini, dan pelatihan kesadaran keamanan bagi semua pengguna sistem (Saputra et al., 2023).

BAB II

METODE PERLINDUNGAN DAN LEGITIMASI INFORMASI

A. Enkripsi Data

Dalam konteks perkembangan teknologi informasi, data memegang peran sentral sebagai sarana utama untuk menyimpan, mengelola, dan menyampaikan informasi yang diperlukan oleh masyarakat. Namun, seiring dengan pertumbuhan penggunaan data, perhatian terhadap aspek keamanan menjadi semakin penting, terutama dalam konteks pertukaran *file* yang mencakup informasi yang bersifat rahasia. Suatu solusi efektif untuk menangani tantangan ini adalah melalui penerapan suatu proses kriptografis yang dikenal sebagai enkripsi data, di mana data yang diinginkan untuk disampaikan atau disimpan diacak menjadi suatu bentuk kode rahasia (Suryawan & Hamdani, 2013).

Enkripsi merupakan langkah transformasi data ke dalam bentuk yang tidak dapat dibaca, kecuali oleh entitas yang memiliki kunci dekripsi yang sesuai. Tindakan ini bertujuan untuk menjaga kerahasiaan informasi yang bersifat sensitif dan melindunginya dari

upaya akses yang tidak diotorisasi. Dalam konteks era digital, pentingnya keamanan data menjadi semakin signifikan mengingat adanya ancaman serius terhadap privasi dan potensi serangan siber (Wijoyo, Rahmawati, et al., 2023). Proses enkripsi tersebut bukan hanya memberikan perlindungan terhadap potensi akses yang tidak sah, tetapi juga berkontribusi pada pengamanan integritas dan kerahasiaan informasi yang terkandung dalam berkas-berkas tersebut, memberikan tingkat keamanan yang lebih tinggi dalam berbagai konteks pertukaran informasi dan pengelolaan data rahasia.

Dalam konteks keamanan informasi, prinsip utama adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi. Fungsi utama pengamanan informasi adalah untuk memberikan perlindungan terhadap akses yang tidak sah, pengubahan, atau penghapusan informasi, sehingga hanya pihak yang memiliki hak akses yang sah yang dapat membaca dan memanipulasi data tersebut (Wulandari & Nurhayati, 2023). Dengan penerapan prinsip-prinsip ini, sistem informasi diharapkan dapat memberikan jaminan terhadap kerahasiaan informasi, mencegah perubahan data yang tidak sah, dan memastikan ketersediaan informasi dengan tingkat keamanan yang optimal (Primartha Rifkie, 2011).

Manfaat penggunaan enkripsi data dapat diuraikan sebagai berikut. Pertama, fungsi enkripsi bertindak sebagai benteng pertahanan yang efektif, mencegah penyusup atau entitas lain yang tidak memiliki izin untuk mengakses dan mengetahui isi informasi yang tersimpan. Sehingga, hanya pihak yang telah diberi izin yang memiliki kemampuan untuk membaca dan

memahami informasi tersebut. Kedua, manfaat enkripsi melibatkan perlindungan data dari risiko penyadapan, sehingga memastikan bahwa keamanan informasi terjaga dengan efisien.

Proses enkripsi data melibatkan transformasi data informasi asli menjadi suatu format yang teracak dan tidak dapat dibaca oleh pihak yang tidak memiliki akses yang sah. Dalam pelaksanaannya, enkripsi dapat dilakukan melalui penggunaan kunci publik atau kunci privat, di mana kedua jenis kunci ini memiliki kebijakan distribusi yang terbatas hanya kepada pihak-pihak yang terlibat dalam komunikasi atau pertukaran data.

Enkripsi yang menggunakan kunci publik dan kunci privat sering kali disebut sebagai kriptografi kunci publik. Salah satu contoh yang paling umum adalah algoritma RSA (Rivest-Shamir-Adleman). Dalam RSA, pesan dienkripsi menggunakan kunci publik dan hanya bisa didekripsi oleh penerima menggunakan kunci privat yang sesuai.

Berikut adalah alur umum dari proses enkripsi menggunakan algoritma RSA yang telah disebutkan sebelumnya:

1. Membuat kunci privat
    a. Alex menghasilkan sepasang kunci RSA: kunci publik dan kunci privat.
    b. Kunci publik terdiri dari dua bagian: modulus (n) dan eksponen enkripsi (e).
    c. Kunci privat juga terdiri dari dua bagian: modulus (n) dan eksponen dekripsi (d).

2. Pesan:
   Santy memiliki pesan yang ingin dikirimkan ke Alex. Pesan ini akan diubah menjadi format numerik untuk enkripsi RSA (contohnya, dengan mengonversi teks ke bilangan bulat menggunakan kode ASCII).

3. Enkripsi:
   a. Santy menggunakan kunci publik Alex (n dan e) untuk mengenkripsi pesan.
   b. Pesan diubah menjadi format numerik dan dienkripsi menggunakan rumus khusus.
   c. Hasilnya adalah ciphertext, yang kemudian akan dikirimkan ke Alex.

4. Dekripsi:
   a. Alex menerima ciphertext dari Santy.
   b. Alex menggunakan kunci privatnya (n dan d) untuk mendekripsi ciphertext.
   c. Ciphertext diubah kembali menjadi pesan asli menggunakan rumus yang sesuai.
   d. Alex sekarang memiliki pesan asli yang telah berhasil didekripsi.

Dengan demikian, alur proses enkripsi RSA melibatkan pembuatan kunci, enkripsi pesan dengan kunci publik penerima, pengiriman ciphertext ke penerima, dan akhirnya dekripsi pesan menggunakan kunci privat penerima.

B. Penggunaan Sandi dan Kunci Rahasia

Proteksi kata sandi merujuk pada langkah-langkah keamanan yang melibatkan penggunaan kode atau kata kunci rahasia sebagai mekanisme penghalang guna mencegah akses yang tidak sah terhadap perangkat atau akun tertentu. Aspek yang tidak terpisahkan dari keamanan siber adalah perlindungan terhadap kata sandi, yang secara efektif menyediakan lapisan pertahanan dalam melindungi informasi yang bersifat sensitif melalui pengamanan kredensial *login*.

Praktik ini melibatkan penetapan dan verifikasi identitas pengguna, serta pembatasan akses ke perangkat, berkas, dan akun tertentu. Perlindungan kata sandi memastikan bahwa hanya entitas pengguna yang sah yang diberi wewenang untuk memberikan kata sandi yang tepat, sehingga memberikan akses yang terkendali terhadap aset digital. Dalam menghadapi ancaman keamanan *cyber* yang semakin kompleks, diperlukan upaya yang komprehensif. Pentingnya pemahaman mengenai keamanan *cyber*, terutama dalam konteks proteksi data, menunjukkan perlunya strategi yang efektif (Arfan Dwi Madya et al., 2023).

Keamanan kata sandi memiliki signifikansi yang sangat tinggi dalam era digital saat ini, di mana pelaku kejahatan dunia maya menggunakan beragam strategi seperti *phishing*, *malware*, dan serangan *brute force* untuk memperoleh akses yang tidak sah ke akun-akun pengguna. Oleh karena itu, mendukung dan mengimplementasikan praktik terbaik menjadi suatu keharusan, seperti penggunaan kata sandi yang kompleks dengan kombinasi karakter huruf (baik huruf besar maupun huruf kecil), angka, dan simbol khusus.

Selain itu, dianjurkan untuk secara rutin mengubah kata sandi dan menghindari penggunaan kata sandi yang sama pada beberapa platform dan aplikasi (Slamet et al., 2022). Melalui penerapan langkah-langkah perlindungan kata sandi ini, pengguna dapat secara substansial mengurangi risiko terhadap ancaman dunia maya serta melindungi dengan efektif aset digital yang dimilikinya.

Selain kunci rahasia menjadi elemen kunci dalam menyusun strategi keamanan informasi. Pengelolaan dan distribusi kunci rahasia ini memegang peranan penting untuk memastikan bahwa hanya pihak yang berwenang yang dapat mengakses dan memahami informasi yang telah dienkripsi. Keberhasilan dalam menjaga kerahasiaan dan keutuhan informasi seringkali sangat tergantung pada keamanan dan manajemen kunci rahasia ini (Syahputri et al., 2023).

Dalam penggunaan umumnya, sandi dan kunci rahasia bekerja secara sinergis untuk memastikan tingkat keamanan yang optimal terhadap akses terhadap informasi dan data. Sandi berfungsi sebagai mekanisme perlindungan terhadap akses yang tidak sah ke akun individu, sementara kunci rahasia mengatasi proses enkripsi dan dekripsi data untuk melindungi informasi yang sedang dikirim atau disimpan. Melalui integrasi sandi dan kunci rahasia, sistem keamanan informasi dapat memberikan tingkat perlindungan yang kuat terhadap potensi ancaman keamanan.

C. Sertifikat Digital

Sertifikat digital atau sertifikat elektronik, dalam konteks perlindungan informasi, merupakan alat kunci yang digunakan untuk memvalidasi keaslian dan integritas data dalam lingkungan digital. Sertifikat ini berfungsi sebagai instrumen untuk memastikan bahwa proses pertukaran atau penyimpanan informasi dilakukan dengan aman dan berasal dari sumber yang sah. Penggunaan sertifikat elektronik melibatkan penerapan teknologi kriptografi, di mana pasangan kunci publik dan kunci privat digunakan untuk menandatangani dan memverifikasi tanda tangan digital. Selain itu, sertifikat elektronik dapat terlibat dalam proses enkripsi data, memberikan lapisan tambahan keamanan terhadap potensi akses yang tidak sah.

Dalam hal ini, sertifikat elektronik menjadi suatu komponen integral dalam strategi perlindungan informasi, membantu mencegah manipulasi data, memastikan keabsahan pengirim atau penerima informasi, dan menyediakan saluran yang aman untuk pertukaran data sensitif. Dengan demikian, peran sertifikat elektronik sangat penting dalam mencapai tingkat keamanan yang tinggi dalam konteks perlindungan informasi di dunia digital. Secara singkat, sertifikat elektronik yang sering disebut sebagai sertifikat digital, digunakan untuk mengesahkan keautentikan perangkat. Selain itu, dokumen tersebut dapat difungsikan untuk menegaskan keabsahan pengguna yang memiliki hak akses dalam suatu layanan.

Terdapat beberapa kategori sertifikat digital yang lazim digunakan, bergantung pada tujuan dan kebutuhan yang diinginkan dalam kerangka keamanan digital. Berikut merupakan beberapa ragam sertifikat digital yang umumnya diaplikasikan:

1. **Sertifikat SSL/TLS (*Secure Sockets Layer/Transport Layer Security*)**

   Berperan dalam menjamin keamanan komunikasi antara pengguna dan server web, serta memverifikasi bahwa data yang dikirimkan melalui HTTPS (*Hypertext Transfer Protocol Secure*) telah dienkripsi.

2. **Sertifikat Kode (*Code Signing Certificate*)**

   Digunakan untuk mengesahkan otentikasi dan keutuhan kode perangkat lunak atau aplikasi, membuktikan bahwa kode tersebut tidak mengalami modifikasi oleh entitas yang tidak berhak setelah ditandatangani.

3. **Sertifikat Email (*Email Certificate*)**

   Diterapkan untuk melindungi dan mengamankan komunikasi melalui email, serta menambahkan tanda tangan digital pada pesan guna menegaskan keabsahan pengirim.

4. **Sertifikat Identitas (*Identity Certificate*)**

   Menyediakan identitas digital untuk pengguna atau perangkat, sering digunakan dalam pengaturan akses ke sistem atau layanan yang berkaitan dengan identitas.

5. **Sertifikat Kunci Publik (*Public Key Certificate*)**

   Bertugas dalam infrastruktur kunci publik (PKI) untuk mengesahkan dan mengaitkan kunci publik dengan subjek tertentu, seperti individu atau perusahaan.

6. **Sertifikat Kunci Pribadi (*Private Key Certificate*)**

   Melibatkan penyertaan kunci pribadi yang terkait dengan kunci publik tertentu, sering dipakai dalam proses otentikasi dan enkripsi.

7. **Sertifikat Server (*Server Certificate*)**

   Serupa dengan sertifikat SSL/TLS, digunakan untuk memverifikasi identitas dan melindungi komunikasi antara server dan klien.

8. **Sertifikat Perangkat (*Device Certificate*)**

   Menetapkan identitas digital untuk perangkat, sering digunakan dalam konteks jaringan perangkat *Internet of Things* (IoT) atau perangkat terkait.

Tiap kategori sertifikat digital memiliki peran dan fungsi masing-masing dalam kerangka keamanan digital, berkontribusi pada upaya memastikan keaslian, integritas, dan kerahasiaan informasi dalam berbagai aplikasi dan layanan. Selain itu, terdapat beberapa manfaat signifikan dari sertifikat digital, sebagai berikut:

1. **Keamanan**

   Sertifikat digital digunakan untuk mengamankan komunikasi baik secara internal maupun eksternal dengan mengenkripsi data, mencegah potensi serangan yang bertujuan mencuri atau mengakses informasi sensitif.

2. **Skalabilitas**

   Sertifikat ini memberikan kemudahan bagi berbagai jenis dan ukuran bisnis dengan memberikan tingkat enkripsi yang seragam. Kemampuannya yang dapat diperluas memungkinkan pencabutan, penerbitan, dan pembaruan dengan cepat, dikelola melalui platform pusat, serta digunakan untuk melindungi perangkat pengguna.

3. **Keaslian**

   Sertifikat digital memainkan peran sentral dalam menjamin keaslian komunikasi online, terutama dalam menghadapi ancaman siber yang semakin meluas. Ini memastikan bahwa pesan pengguna selalu dapat diidentifikasi sebagai asli dan sampai ke tujuannya tanpa ancaman manipulasi.

4. **Keandalan**

   Sertifikat digital hanya dikeluarkan oleh pihak yang dipercayai dan diotorisasi. Di Indonesia, kewenangan untuk mengeluarkan sertifikat digital terbatas pada Penyelenggara Sertifikasi Elektronik (PSrE), menjamin bahwa proses penerbitannya dapat diandalkan dan dapat dipertanggungjawabkan.

D. Teknik Otentikasi Pengguna

Otentikasi merupakan suatu mekanisme yang dapat melakukan verifikasi terhadap identitas asli seorang pengguna. Dengan merinci kutipan tersebut, otentikasi dapat diartikan sebagai metode untuk menegaskan identitas seseorang melalui sejumlah prosedur tertentu yang menjadi persyaratan verifikasi identitas pengguna (Islam Al Makassari et al., 2022).

Proses autentikasi pengguna merujuk pada langkah-langkah yang diambil untuk mengenali individu yang meminta izin akses ke suatu sistem, jaringan, atau perangkat. Pengaturan kontrol akses ini umumnya bergantung pada identitas pengguna yang diidentifikasi melalui informasi kredensial seperti nama pengguna dan kata sandi. Di samping itu, teknologi autentikasi lainnya, termasuk metode biometrik dan aplikasi autentikasi, juga diterapkan untuk memverifikasi identitas pengguna.

Signifikansi autentikasi pengguna terletak pada kemampuannya untuk mencegah akses yang tidak sah terhadap informasi yang bersifat sensitif. Sebagai contoh, melalui *user authentication*, seorang pengguna (A) hanya memiliki hak akses terhadap informasi yang relevan, sementara tidak dapat mengakses informasi yang bersifat rahasia dari pengguna lain (B). Penggunaan metode autentikasi yang tidak aman dapat memberikan celah bagi penjahat dunia maya untuk masuk ke dalam sistem dan mencuri informasi yang mungkin merugikan. Metode keamanan digital yang menjanjikan tingkat keamanan tinggi dalam lingkungan digital adalah Autentikasi Dua Faktor (2FA). Mekanisme ini beroperasi dengan mengharuskan pemilik akun membuktikan keasliannya melalui penggunaan kata sandi sekali pakai

yang dikirimkan oleh server setelah mendeteksi percobaan penggunaan akun oleh pemilik atau pihak lain (Musu et al., 2022).

Berikut ini adalah beberapa contoh implementasi umum dari *user authentication* yang digunakan untuk meningkatkan keamanan sistem modern.

1. **Otentikasi Kata Sandi**

   Metode otentikasi yang umum yang mana mengharuskan pengguna memasukkan kombinasi huruf, angka, atau karakter khusus. Untuk meningkatkan keamanan, disarankan untuk membuat kata sandi yang kuat dengan menggabungkan berbagai opsi yang tersedia.

2. **Otentikasi Multi-Faktor (MFA)**

   Metode otentikasi yang melibatkan dua atau lebih cara independen untuk mengidentifikasi pengguna. Contohnya mencakup penggunaan kode yang dihasilkan dari ponsel cerdas, tes *captcha*, sidik jari, biometrik suara, hingga pengenalan wajah.

3. **Otentikasi Berbasis Sertifikat**

   Teknologi otentikasi yang mengidentifikasi pengguna, mesin, atau perangkat melalui penggunaan sertifikat digital. Sertifikat ini, mirip dengan SIM atau paspor elektronik, berisi identitas digital pengguna, termasuk kunci publik dan tanda tangan digital dari otoritas sertifikasi. Sertifikat digital membuktikan kepemilikan kunci publik dan hanya diterbitkan oleh otoritas sertifikasi.

4. Otentikasi Biometrik

Merupakan proses keamanan yang memanfaatkan karakteristik biologis unik individu. Metode otentikasi biometrik mengeliminasi kebutuhan untuk mengingat kata sandi yang kompleks. Dengan peningkatan dalam teknologi dan metode otentikasi, serangan terhadap kata sandi dapat dicegah, serta risiko pelanggaran data dapat diminimalkan.

E. Pengaturan Akses

Pengaturan akses dalam keamanan informasi merujuk pada proses mengontrol dan mengelola hak akses terhadap data, sistem, atau sumber daya informasi tertentu agar tidak terjadi penyalahgunaan hak akses serta adanya prosedur pengendalian hak akses guna melindungi kerahasiaan, integritas, dan ketersediaan data, serta mencegah akses yang tidak sah atau penyalahgunaan sumber daya (Wahyudi et al., 2020). Tujuan utama dari pengaturan akses adalah memastikan bahwa hanya pengguna yang memiliki hak dan wewenang yang sesuai yang dapat mengakses informasi atau melakukan tindakan tertentu dalam suatu lingkungan informasi.

Access control memiliki beberapa komponen utama yang dirancang dengan tujuan menjaga akses yang sah, antara lain:

1. **Kredensial dan Metode Identifikasi**

   Digunakan untuk mengidentifikasi dan memverifikasi identitas individu sebelum memberikan akses ke area terbatas. Jenis kredensial melibatkan kartu akses, kunci elektronik, kode PIN, sidik jari, dan pemindaian wajah.

2. ***Access Reader***

   Perangkat untuk membaca dan memvalidasi kredensial atau metode identifikasi, seperti pembaca kartu, pemindai sidik jari, sesuai dengan metode yang digunakan.

3. ***Controller***

   Unit pemrosesan yang mengelola dan mengontrol aliran informasi antara pembaca akses, sistem pengunci pintu, dan sistem manajemen akses. *Controller* membuat keputusan akses berdasarkan informasi dari pembaca akses.

4. **Sistem *Door Lock***

   Komponen yang mengendalikan kunci atau mekanisme pengunci pintu, berinteraksi dengan *controller* untuk membuka atau mengunci pintu sesuai dengan otorisasi.

5. **Sistem Manajemen Akses**

   Perangkat lunak untuk mengelola pengguna, otorisasi, dan kebijakan akses dalam sistem kontrol akses. Memungkinkan administrator mengatur hak akses, mengelola pengguna, dan melacak aktivitas akses secara efisien.

Pada dasarnya, tujuan utama dari sistem kontrol akses adalah untuk mengurangi risiko keamanan yang dapat timbul dalam bentuk akses tidak sah, baik pada sistem fisik maupun sistem logika. Manfaat penerapan kontrol akses melibatkan aspek-aspek berikut:

1. **Keamanan Fisik**

   Sistem kontrol akses berperan dalam melindungi keamanan fisik fasilitas dengan mencegah akses yang tidak diizinkan ke area terbatas. Tujuannya adalah untuk mencegah potensi pencurian, kerusakan, atau tindakan kriminal terhadap aset berharga.

2. **Keamanan Data dan Informasi**

   Dengan membatasi akses hanya kepada personel yang memiliki otorisasi, risiko kebocoran atau penyalahgunaan informasi dapat diminimalkan secara signifikan.

3. **Pengawasan dan Pencatatan**

   Administrator keamanan dapat melacak individu yang memasuki area terbatas, mencatat waktu masuk, dan durasi tinggal. Hal ini memiliki peran penting dalam investigasi keamanan dan audit internal.

4. **Penyederhanaan Proses**

   Melalui otomatisasi otorisasi, staf yang diizinkan dapat memasuki area tanpa harus menunggu validasi dari petugas keamanan. Ini memberikan efisiensi waktu dan pengelolaan akses yang lebih efektif.

5. Keandalan dan Fleksibilitas

Administrator keamanan dapat dengan mudah memperbarui dan mengelola otorisasi akses secara *real-time*. Mereka juga dapat memberikan otorisasi yang berbeda berdasarkan tingkat keamanan atau waktu tertentu, sesuai dengan kebutuhan organisasi.

KESIMPULAN

Sistem keamanan informasi adalah aspek yang sangat vital dalam era digital saat ini, di mana data menjadi aset yang sangat berharga bagi organisasi dan individu. Buku ini telah menyoroti pentingnya sistem keamanan informasi dalam melindungi data sensitif dari berbagai ancaman peretasan yang semakin kompleks dan canggih. Dari serangan phishing hingga serangan DDoS, ancaman terhadap keamanan informasi dapat mengakibatkan kerugian finansial, pencurian identitas, dan bahkan merusak reputasi organisasi. Langkah-langkah pencegahan seperti menerapkan kebijakan keamanan yang ketat, pelatihan karyawan, penggunaan teknologi keamanan canggih, dan pemantauan yang terus-menerus sangat penting untuk mengurangi risiko peretasan. Selain itu, penting untuk memahami tujuan di balik serangan peretasan, yang dapat bervariasi dari pencurian data hingga *sabotase*.

Meningkatkan kesadaran tentang ancaman keamanan informasi dan menerapkan praktik keamanan yang baik, organisasi dan individu dapat meningkatkan ketahanan mereka terhadap serangan peretasan. Namun, upaya pencegahan harus bersifat proaktif dan terus-menerus, mengingat ancaman keamanan informasi terus berkembang seiring dengan kemajuan teknologi. Dengan demikian, investasi dalam sistem keamanan informasi bukanlah pilihan,

tetapi suatu keharusan bagi organisasi yang ingin melindungi data sensitif mereka dan menjaga kepercayaan pengguna. Melalui kerjasama antara pemerintah, industri, dan lembaga keamanan *cyber*, kita dapat membangun lingkungan digital yang lebih aman dan terpercaya untuk masa depan.

Daftar pustaka

Anshori, S. (2018). Pemanfaatan Teknologi Informasi Dan Komunikasi Sebagai Media Pembelajaran. *Civic-Culture: Jurnal Ilmu Pendidikan PKn Dan Sosial Budaya*, *9924*, 88–100.

Arfan Dwi Madya, Bagas Djoko Haryanto, & Devi Putri Ningsih. (2023). Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity. *Indonesian Journal of Education And Computer Science*, *1*(3), 127–135. https://doi.org/10.60076/indotech.v1i3.236

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Baran, M. V. (2021). Principles of legal regulation of the institute of information security. *Uzhhorod National University Herald. Series: Law*, *66*, 129–134. https://doi.org/10.24144/2307-3322.2021.66.22

Bisri, M. H., & Asmoro, B. T. (2019). Etika Pelayanan Publik di Indonesia. *Journal of Governance Innovation*, *1*(1), 59–76. https://doi.org/10.36636/jogiv.v1i1.298

Boja, C., Adrian, & VISOIU. (2007). Optimization of Antivirus Software. *Informatica Economica Journal*.

Boyle, R., & Panko, R. R. (2015). *Corporate Computer Security* (Fourth edition). Pearson.

Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley.

Ciampa, M. D. (2010). *Security Awareness: Applying Practical Security in Your World* (Third Edition). Course Technology, Cengage Learning.

Di Pietro, R., & Mancini, L. V. (2008). *Intrusion Detection Systems*. Springer US.

Dronov, V. Y., & Dronova, G. A. (2022). Principles of information security management system. *Journal of Physics: Conference Series*, *2182*(1), 012092. https://doi.org/10.1088/1742-6596/2182/1/012092

Ermana, F., Tanuwijaya, H., & Mastan, I. (2010). Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 pada PT. BPR JATIM. *Sistem Informasi STMKTK Surabaya*.

Fadlil, A., Riadi, I., & Aji, S. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmu Teknik Elektro Komputer Dan Informatika (JITEKI)*, *3*(1), 11–19.

Fahrezi, A., Apriliani, N., Ajijah, N., & Juardi, D. (2022). Keamanan Data dan Transaksi dalam Pemanfaatan Cloud sebagai Service. *Jurnal Pendidikan Dan Konseling*, *4*(4), 5530–5536.

Faidlatul Habibah, A., Shabira, F., & Irwansyah, I. (2021). Pengaplikasian Teori Penetrasi Sosial pada Aplikasi Online Dating. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *3*(1), 44–53. https://doi.org/10.47233/jteksis.v3i1.183

Fajriyani, D., Fauzi, A., Devi Kurniawati, M., Yudo Prakoso Dewo, A., Fahri Baihaqi, A., & Nasution, Z. (2023). Tantangan Kompetensi SDM dalam Menghadapi Era Digital (Literatur Review). *Jurnal Ekonomi Manajemen Sistem Informasi*, *4*(6), 1004–1013. https://doi.org/10.31933/jemsi.v4i6.1631

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351–407.

Gunawan, I. (2021). Analisis Keamanan Data Pada Website Dengan Wireshark. *JES (Jurnal Elektro Smart)*, *1*(1), 16–19.

Hogue, J. (2006). *Intrusion Prevention Fundamentals*. Cisco Press.

Islam Al Makassari, S. M. J., Budiman, T., & Yulianto, A. B. (2022). Rancangan Program Otomatisasi Otentikasi Pengguna Untuk Otorisasi Pada Website Dengan Python Dan Selenium Web Driver. *Jurnal Manajamen Informatika Jayakarta*, *2*(4), 326. https://doi.org/10.52362/jmijayakarta.v2i4.917

Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography, Second Edition*. Taylor \& Francis.

Lella, I., Tsekmezoglou, E., Naydenov, R., Malatras, A., García, S., Valeros, V., & Gomaa, A. (2022). *ENISA Threat Landscape for Ransomware Attacks*. ENISA.

Lestari, D., & Nasution, M. I. P. (2023). Peranan Sistem dan Teknologi Informasi Pada Proses Bisnis Informasi:(Keamanan Informasi Dalam Era Digital, Tantangan Dan Solusi Untuk Bisnis Organisasi). *Kohesi: Jurnal Sains Dan Teknologi*, *1*(12), 101–110.

Ligh, M., Adair, S., Hartstein, B., & Richard, M. (2010). *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*. Wiley.

Li, Q. xiang, Ji, H. min, & Huang, Y. min. (2022). The information leakage strategies of the supply chain under the block chain technology introduction. *Omega*, *110*, 102616. https://doi.org/10.1016/J.OMEGA.2022.102616

Malin, C. H., Casey, E., & Aquilina, J. M. (2012). *Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides*. Syngress.

Musu, W., Muhtamar, S., Palullu, A., Patendean, W., Dipa Makassar Mks, U., & Perintis Kemerdekaan Km, J. (2022). Analisis Pola Penggunaan Fitur Autentikasi Dua Faktor oleh para Remaja di Media Sosial. *JURNAL SISTEM INFORMASI DAN TEKNOLOGI INFORMASI*, *212*(2), 212–213. https://doi.org/https://doi.org/10.36774/jusiti.v11i2

Natsir, F. (2021). Analisis Forensik Konten dan Timestamp pada Aplikasi Tiktok. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, *6*(2), 203–209.

Noonan, W., & Dubrawsky, I. (2006). *Firewall Fundamentals*. Pearson Education.

Primartha Rifkie. (2011). Penerapan Enkripsi dan Dekripsi File Menggunakan Data Encryption Standard (DES). *ISNN : 2355-4614 / Universitas Sriwijaya*, *3*(2), 371–387.

P, S., & K, K. (2023). Computer Security and Privacy: Principles and Practice. In *Cutting-Edge Technologies in Innovations in Computer Science and Engineering*.

San International Scientific Publications. https://doi.org/10.59646/csebookc4/004

Purwaningrum, O., Nadhiroh, B., & Mukaromah, S. (2021). Literature Review Audit Sistem Informasi Menggunakan Kerangka Kerja Cobit 5. *Jurnal Informatika Dan Sistem Informasi*, *2*(3).

Putra, I. A., Fahimah, M., Umam, K., & Jannah, K. (2022). Sosialisasi Inovasi Dan Strategi Pemasaran Produk Industri Kecil Di Era New Normal. *Dedication : Jurnal Pengabdian Masyarakat*, *6*(1), 13–20. https://doi.org/10.31537/dedication.v6i1.652

Rahayu, Y. D. P., & Trianto, N. (2021). Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1. *Info Kripto*, *15*(3), 105–111.

Rasaputhra, S., Peiris, V., Magallagoda, R., Panditasekara, C., Wisenthige, K., & Jayasuriya, N. (2024). Do technological, environmental and entrepreneurial factors affect social commerce adoption? *Journal of Small Business and Enterprise Development*. https://doi.org/10.1108/JSBED-09-2023-0420

Rehman, R. U. (2003). *Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID*. Prentice Hall PTR.

Riadi, I., Yudhana, A., & Yunanri, W. (2020). Analisis Keamanan Website Open Journal System Menggunakan Metode Vulnerability Assessment. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(4), 853–860.

Riskiyadi, M. (2020). (2020). Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime. *Cyber Security Dan Forensik Digital*, *3*(2), 12–21.

Rumetna, M. S., Lina, T. N., Santoso, A. B., Karay, J., Komansilan, R., & Kaitelapatay, B. G. (2022). Pengetahuan Serta Peran Auditor Secara Komprehensif Dalam Menghadapi Dampak Perkembangan Teknologi Informasi. *Jurnal Komtika (Komputasi Dan Informatika)*, *6*(1), 26–38.

Saputra, L. A., Akbar, F. M., Cahyaningtias, F., Ningrum, M. P., & Fauzi, A. (2023). Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan. *Jurnal Pendidikan Siber Nusantara*, *1*(2), 58–66.

Slamet, M. R., Ikhlash, M., & Wulandari, F. (2022). Analisis Penilaian Keamanan Informasi Dengan Menggunakan Penilaian Mandiri Keamanan Informasi (Paman Kami). *Journal of Applied Business Administration*, *6*(1), 41–50. https://doi.org/10.30871/jaba.v6i2.3604

Solechan, A. (2021). Audit Sistem Informasi Audit Sistem Informasi. *Yayasan Prima Agus Teknik*.

Stallings, W. (2006). *Cryptography and Network Security: Principles and Practice*. Pearson/Prentice Hall.

Stallings, W. (2007). *Network Security Essentials: Applications and Standards*. Prentice Hall.

Stallings, W. (2011). *Network Security Essentials: Applications and Standards* (Fourth edition). Prentice Hall.

Stallings, W. (2017). *Cryptography and Network Secuirty*.

Suryawan, S. H., & Hamdani. (2013). Pengamanan Data File dengan Menggunakan Algortitma Enkripsi Rivest Code 5. *Jurnal Informatika Mulawarman Edisi Juli*, *8*(2), 44–49. https://doi.org/http://dx.doi.org/10.30872/jim.v8i2.106

Syahputri, N. I., Harahap, H., Siregar, R., & Tommy, T. (2023). Penyuluhan Pentingnya Two Factor Authentication

dan Aplikasinya Di Era Keamanan Digital. *Jurnal Pengabdian Masyarakat Bangsa*, *1*(6), 768–773. https://doi.org/10.59837/jpmba.v1i6.256

Tanenbaum, A. S., & Wetherall, D. (2011). *Computer Networks* (Fifth Edition). Pearson Prentice Hall.

Wahyudi, H., Zulianto, A., Maulana, A., Mardira Indonesia, S., & Langlangbuana, U. (2020). Audit Keamanan Sistem Informasi Manajemen Akademik dan Kemahasiswaan Menggunakan SNI ISO/IEC 27001:2013 (Studi Kasus STMIK Mardira Indonesia) Heri. *Jurnal Computech & Bisnis*, *Vol. 14 No*(1), 40–46. https://doi.org/10.5281/zenodo.3929072

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security* (Fourth Edition). Course Technology.

Wijoyo, A., Rahmawati, T., Agustin, W., & Muhammad Saputra, B. (2023). Perlindungan Data Sensitif : Enkripsi Sebagai Pilar Utama Keamanan Komputer. *CHIPSET : Jurnal Ilmu Komputer, Teknik, Dan Multimedia*, *1*(2), 84–91. https://doi.org/https://doi.org/10.9999/9yrtfr34

Wijoyo, A., Rosadi, A., Hakim, F. I., Hanafi, M., & Sidik, R. (2023). Keamanan Jaringan Melindungi Sistem dari Serangan Luar. *JRIIN: Jurnal Riset Informatika Dan Inovasi*, *1*(3).

Wulandari, I., & Nurhayati, C. (2023). Pengamanan Data Pribadi Mahasiswa Prodi Akuntansi Universitas Trunojoyo Madura. *Jurnal Ilmiah Dan Manajemen Sistem Informasi*, *9*(2), 89–96. https://doi.org/http://dx.doi.org/10.24014/rmsi.v9i2.23715

TENTANG PENULIS

Victor Benny Alexsius Pardosi, S.Kom., M.Sc.

Dosen Fakultas Ilmu Komputer
Universitas Dharma AUB Surakarta
PT Transformasi Data Digital
(HostData.id)

Penulis lahir di Aceh Tengah pada tanggal 31 Januari 1991. Merupakan seorang praktisi IT yang memiliki lebih dari sepuluh tahun pengalaman sebagai Web Developer dan System Administrator. Selain itu, Penulis juga menjabat sebagai dosen di Program Studi Sistem Informasi di Fakultas Ilmu Komputer, Universitas Dharma AUB Surakarta. Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi di STMIK Dharmapala Riau lalu melanjutkan S2 jurusan Computer Science di NRTPU, Russia. Tertarik dalam penelitian bidang Network & Cloud Security, Information Security, Internet of Things, Usable Security & Privacy, Data Protection, dan Artificial Intelligence. Saat ini, terlibat aktif dalam membangun Hosting dan VPS yang terjangkau, khususnya untuk kalangan pelajar, sehingga mempermudah implementasi dan praktek dengan tujuan mengembangkan komunitas open source serta mulai mengadopsi IPv6 melalui Dual Stack NAT VPS.

Bernadete Deta, M.Kom.
Dosen Teknik Informatika
Fakultas Teknik Informatika
Larantuka

Penulis lahir di Larantuka-Flores Timur tanggal 31 Juli. Penulis adalah dosen pada Program Studi Teknik Informatika Fakultas Teknik, Institut Keguruan dan Teknologi Larantuka (IKTL). Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi Universitas Dinamika Surabaya tahun 2018 dan Magister management sistem Informasi dari Binus University tahun 2022.

Bidang pengajaran dan penelitian penulis adalah Struktur Data, Sistem Basis Data, Management Basis Data, Komputasi Nomerik, Jaringan komputer dan Pemrograman Jaringan Komputer.

Fifto Nugroho
Dosen Program Studi Sistem Komputer
Fakultas Ilmu Komputer, Universitas
Bung Karno

Fifto Nugroho, S.T., M.Kom. Lahir di Kota Jakarta, bulan Oktober 1982. Alumnus dari Universitas Persada Indonesia, Fakultas Teknologi Industri, Program Studi Teknik Informatika, dengan capaian kelulusan sebagai Sarjana Teknik pada Bulan November 2006. Melanjutkan studi strata dua pada Program Magister Ilmu Komputer di Universitas Bunda Mulia dan lulus pada Bulan Agustus 2013 mencapai gelar Magister Komputer. Pada tahun 2014 diangkat menjadi Dosen Tetap Yayasan Pendidikan Soekarno di Universitas Bung Karno dan ditempatkan di Fakultas Ilmu Komputer pada Program Studi Sistem Komputer. Sampai dengan buku ini diterbitkan, aktif ikut serta dalam keanggotaan di lima organisasi nasional profesi di Indonesia, yaitu, Persatuan Insinyur Indonesia (PII), Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM), Ikatan Ahli Informatika Indonesia (IAII), Asosiasi Internet of Things Indonesia (ASIOTI), dan Asosiasi Big Data dan AI (ABDI).

Arnes Yuli Vandika

Seorang Dosen, Peneliti dan Pekerja ICT Teknis part-time, sehari-hari mengampu mata kuliah Jaringan Komputer, Sistem Operasi, Sistem Terdistribusi, Cloud Computing dan E-Bisnis pada salah satu universitas swasta di Lampung. Tertarik dengan bidang Cloud System, ICT CyberSecurity, juga Artificial Intelligence dan Machine Learning. Member IEEE, penikmat musik Jazz, hobby Jogging dan penggemar film fiksi ilmiah seperti Star Trek dan Star Wars dsb. “Mudah-mudahan buku ini mampu memberikan nuansa referensi ilmiah kepada para pembaca , terutama teman-teman dosen, mahasiswa serta pembaca lain nya, Salam ”.

Dapat di hubungi : *arnes@ieee.org*