HADLA
MEDIA INFORMASI

KEAMANAN SISTEM INFORMASI :

PERLINDUNGAN DATA DAN PRIVASI DI ERA DIGITAL

Penulis :

Lalu Delsi Samsumar, M.Eng.
Siti Nasiroh, S.Kom, M.Kom.
Miswadi,S.Kom.,M.Kom.
Salman Farizy. S.Kom., M.Kom., MCSE., MVP.
Ir. Chairul Anwar, S.Kom., M.Kom., CITPM.
Imam Halim Mursyidin, S.Kom., M.Kom.
Roynaldy Rosdiyanto, S.Kom., M. Kom.
Wahyu Wijaya Widiyanto, M.Kom.
Rezza Anugrah Mutiarawan, S.Kom., M.Kom.
Prayogo, S.Kom., M.Kom.
Richky Mukin , MCT, MM.
Tri Yusnanto, M.Kom.
Ir. Lukman Medriavin Silalahi, A.Md., ST., MT., IPM., APEC-Eng.
A. Taqwa Martadinata, M.Kom.
Tri Rochmadi, M.Kom., CSCU., CEI., CIISA.
Dede Irawan, S.Kom., M.Kom.
Doni Prastyo, S.Kom., M.Kom.

Editor

NURHADI, S.KOM., M.KOM.

KEAMANAN SISTEM INFORMASI: PERLINDUNGAN DATA DAN PRIVASI DI ERA DIGITAL

Penulis

Lalu Delsi Samsumar
Siti Nasiroh
Miswadi
Salman Farizy
Chairul Anwar
Imam Halim Mursyidin
Roynaldy Rosdiyanto
Wahyu Wijaya Widiyanto
Rezza Anugrah Mutiarawan
Prayogo
Richky Mukin
Tri Yusnanto
Lukman Medriavin Silalahi
A. Taqwa Martadinata
Tri Rochmadi
Dede Irawan
Doni Prastyo

PENERBIT:

HADLA
MEDIA INFORMASI

Website: www.media.hadlacorp.com

UU No 28 tahun 2014 tentang Hak Cipta

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 Rp 100.000.000 (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 Rp. 500.000.000,00 (lima ratus juta rupiah).

3) 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 (l) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

4) Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp. 4.000.000.000,00 (empat miliar rupiah).

KEAMANAN SISTEM INFORMASI: PERLINDUNGAN DATA DAN PRIVASI DI ERA DIGITAL

Tim Penulis:

Lalu Delsi Samsumar
Siti Nasiroh
Miswadi
Salman Farizy
Chairul Anwar
Imam Halim Mursyidin
Roynaldy Rosdiyanto
Wahyu Wijaya Widiyanto
Rezza Anugrah Mutiarawan
Prayogo
Richky Mukin
Tri Yusnanto
Lukman Medriavin Silalahi
A. Taqwa Martadinata
Tri Rochmadi
Dede Irawan
Doni Prastyo

Desain Cover:
Sulaiman
Tata Letak:
Sulaiman
Editor
Nurhadi

ISBN:

-

Cetakan Pertama:
Mei, 2025

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa atas segala rahmat, taufik, dan hidayah-Nya sehingga buku ini yang berjudul "Keamanan Sistem Informasi: Perlindungan Data dan Privasi di Era Digital" dapat disusun dan diselesaikan dengan baik. Buku ini hadir sebagai bentuk kontribusi ilmiah untuk menjawab tantangan nyata di tengah masifnya transformasi digital dan semakin kompleksnya ancaman terhadap sistem informasi.

Kemajuan teknologi informasi telah mendorong dunia ke arah digitalisasi di hampir seluruh sektor kehidupan: mulai dari pendidikan, layanan publik, bisnis, kesehatan, hingga pemerintahan. Namun, di balik kemudahan dan efisiensi tersebut, muncul berbagai kerentanan yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Kasus kebocoran data, peretasan, ransomware, dan pelanggaran privasi telah menjadi isu global yang menuntut perhatian dan kesiapsiagaan tinggi dari semua pihak.

Buku ini disusun secara sistematis dengan cakupan topik yang menyeluruh, dimulai dari konsep dasar keamanan informasi sebagai fondasi penting bagi para pembaca. Dilanjutkan dengan pembahasan tentang ancaman dan kerentanan dalam sistem informasi yang seringkali menjadi titik awal terjadinya insiden keamanan. Untuk itu, pemahaman yang mendalam terhadap keamanan jaringan dan infrastruktur IT menjadi hal yang tidak dapat diabaikan.

Aspek teknis keamanan seperti enkripsi dan kriptografi, autentikasi dan kontrol akses, serta manajemen risiko turut dibahas secara detail agar pembaca dapat memahami bagaimana melindungi sistem secara teknis maupun strategis. Selanjutnya, buku ini juga menyentuh area penting terkait keamanan perangkat keras dan perangkat lunak, serta keamanan aplikasi dan pengujian penetrasi, yang berfungsi sebagai langkah deteksi dan pencegahan dini terhadap potensi celah keamanan.

Sejalan dengan meningkatnya kesadaran akan hak-hak digital, buku ini juga membahas secara khusus mengenai keamanan data dan perlindungan privasi, serta pentingnya penerapan Sistem Manajemen Keamanan Informasi (ISMS) yang berlandaskan pada standar internasional seperti ISO/IEC 27001. Tidak ketinggalan, isu-isu kontemporer juga turut disajikan, termasuk keamanan cloud computing,

keamanan dalam big data dan IoT, hingga keamanan mobile dan BYOD (Bring Your Own Device)—topik-topik yang saat ini sangat relevan di lingkungan kerja modern.

Buku ini juga mengajak pembaca untuk mengenali berbagai serangan siber umum dan teknik pencegahannya, serta memahami langkah-langkah yang tepat dalam menangani insiden melalui forensik digital dan investigasi insiden. Penutup buku ini menghadirkan kajian mengenai tren masa depan dalam keamanan sistem informasi, agar pembaca tidak hanya siap menghadapi tantangan saat ini, tetapi juga mampu mengantisipasi perkembangan yang akan datang.

Kami berharap buku ini dapat menjadi referensi yang berguna, baik bagi mahasiswa, dosen, peneliti, maupun praktisi dan profesional di bidang teknologi informasi. Dengan pendekatan yang bersifat teoritis sekaligus praktis, kami berupaya agar isi buku ini dapat diaplikasikan dalam konteks dunia nyata.

Ucapan terima kasih kami sampaikan kepada seluruh kontributor penulis yang telah menyumbangkan pemikiran dan keahlian terbaiknya dalam penyusunan buku ini. Kami juga menyampaikan apresiasi kepada semua pihak yang telah mendukung, baik secara langsung maupun tidak langsung, sehingga buku ini dapat terbit dan sampai ke tangan para pembaca.

Kami menyadari bahwa penyusunan buku ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang membangun sangat kami harapkan untuk perbaikan pada edisi-edisi selanjutnya. Semoga kehadiran buku ini dapat memberikan manfaat yang sebesar-besarnya bagi pembaca dan menjadi bagian dari upaya kolektif kita dalam menciptakan ekosistem digital yang aman, terpercaya, dan berkelanjutan.

Mei 2025,

Hormat kami,

Tim penulis

PENGANTAR EDITOR

Bismillahirrahmanirrahim,

Alhamdulillah kami panjatkan ke hadirat Allah Subhanahu wa Ta'ala atas segala rahmat, taufik, dan hidayah-Nya sehingga buku ini yang berjudul "Keamanan Sistem Informasi: Perlindungan Data dan Privasi di Era Digital" dapat diterbitkan dan hadir di tengah-tengah pembaca. Buku ini merupakan hasil kolaborasi para penulis dari berbagai bidang keahlian yang memiliki perhatian dan kompetensi dalam dunia keamanan informasi, baik dari sisi teknis maupun manajerial.

Di era digital yang semakin terkoneksi, isu keamanan informasi dan perlindungan privasi menjadi aspek krusial yang tidak lagi dapat dipandang sebelah mata. Serangan siber, penyalahgunaan data pribadi, dan berbagai kerentanan sistem telah menjadi ancaman nyata terhadap integritas, kerahasiaan, dan ketersediaan informasi. Oleh karena itu, pemahaman yang utuh dan mendalam terhadap berbagai aspek keamanan sistem informasi menjadi kebutuhan strategis di berbagai sektor.

Sebagai editor, saya berupaya menghadirkan buku ini dengan struktur yang sistematis, menyajikan alur yang logis dari konsep dasar hingga tantangan kontemporer dalam dunia digital. Pembahasan dimulai dari Konsep Dasar Keamanan Informasi sebagai fondasi pemikiran, kemudian berlanjut ke topik Ancaman dan Kerentanan, Keamanan Jaringan, hingga teknologi penting seperti Enkripsi, Autentikasi, dan Manajemen Risiko. Bab-bab tersebut memberikan pemahaman teknis yang menjadi inti dari perlindungan sistem informasi.

Selanjutnya, buku ini juga membahas area yang sering kali terabaikan namun vital, seperti Keamanan Perangkat Keras dan Lunak, Aplikasi, dan metode Pengujian Penetrasi. Di tengah meningkatnya tuntutan regulasi dan kesadaran publik terhadap privasi, kami juga menyertakan bahasan khusus mengenai Keamanan Data dan Perlindungan Privasi, serta Sistem Manajemen Keamanan Informasi (ISMS) sebagai kerangka kerja yang mendasari pengelolaan keamanan secara berkelanjutan.

Perkembangan teknologi tidak luput dari perhatian, dengan disertakannya pembahasan tentang Keamanan Cloud Computing, Big Data dan IoT, serta Mobile dan BYOD, yang saat ini menjadi tulang

punggung ekosistem kerja dan kehidupan digital. Untuk memperkuat praktik keamanan, bab tentang Serangan Siber, Forensik Digital, dan Investigasi Insiden turut dibahas guna membantu pembaca memahami pola serangan serta strategi respons yang tepat. Buku ini ditutup dengan refleksi atas Tren Masa Depan Keamanan Sistem Informasi, agar pembaca memiliki pandangan ke depan tentang arah perkembangan bidang ini.

Kami berharap buku ini dapat menjadi referensi yang bernilai bagi mahasiswa, dosen, peneliti, serta profesional TI yang berkecimpung dalam pengelolaan dan perlindungan sistem informasi. Buku ini juga dirancang untuk mendorong terciptanya kesadaran kolektif akan pentingnya membangun budaya keamanan digital yang tangguh dan adaptif terhadap perubahan zaman.

Akhir kata, saya mengucapkan terima kasih kepada seluruh penulis atas kontribusi keilmuan dan dedikasi luar biasa yang diberikan dalam penyusunan buku ini. Terima kasih juga kepada semua pihak yang telah membantu dalam proses penerbitan. Kritik dan saran dari pembaca sangat kami nantikan sebagai bekal untuk pengembangan edisi selanjutnya. Semoga buku ini membawa manfaat dan menjadi bagian dari solusi di tengah kompleksitas dunia digital yang terus berkembang.

Mei 2025

Hormat saya

Nurhadi

Editor

DAFTAR ISI

DAFTAR GAMBAR

BAB 1 PENGANTAR KEAMANAN SISTEM INFORMASI

Lalu Delsi Samsumar

A. PENDAHULUAN

Di era digital saat ini, data telah menjadi aset yang sangat penting dan berharga, bahkan sering disebut sebagai "*the new oil*". Hampir seluruh aktivitas individu, bisnis, dan pemerintahan bergantung pada sistem informasi mulai dari penyimpanan catatan medis, transaksi keuangan, hingga layanan publik berbasis daring.

Namun, semakin tinggi ketergantungan terhadap sistem informasi, semakin besar pula risiko terhadap ancaman yang mengintai. Ancaman ini bisa datang dalam berbagai bentuk seperti peretasan (*hacking*), pencurian data pribadi, serangan malware, hingga manipulasi informasi. Seiring dengan meningkatnya kasus kebocoran data dan serangan siber global, keamanan sistem informasi telah menjadi salah satu fokus utama dalam pengelolaan teknologi informasi dan komunikasi.

1. Transformasi Digital dan Kompleksitas Ancaman

Transformasi digital telah membawa efisiensi luar biasa bagi organisasi. Namun, digitalisasi juga membuka celah baru dalam bentuk:

a. Serangan berbasis jaringan
b. Ancaman dari dalam organisasi (*insider threat*)
c. Kelemahan konfigurasi sistem
d. Kebijakan keamanan yang lemah

Bayangkan sebuah rumah sakit yang menyimpan data medis pasien secara digital. Jika sistem tersebut diserang ransomware, maka seluruh data vital bisa disandera dan operasional terganggu secara signifikan. Ini bukan hanya berdampak finansial, tapi juga dapat membahayakan nyawa manusia.

2. Fakta dan Statistik Kekinian

Untuk memahami urgensi keamanan informasi, berikut beberapa data global yang relevan:

a. *IBM Cost of a Data Breach Report 2023* melaporkan bahwa rata-rata kerugian akibat pelanggaran data mencapai USD 4,45 juta per insiden.
b. *Verizon DBIR 2023* mengungkap bahwa lebih dari 83% pelanggaran data melibatkan unsur manusia (human error dan social engineering).
c. *Indonesia* sendiri mencatat lebih dari 40 juta data pengguna bocor dari berbagai platform digital sepanjang tahun 2022–2023, menurut laporan dari CISSReC dan Kominfo.

3. Mengapa Keamanan Sistem Informasi Krusial

Keamanan sistem informasi bukanlah sekadar pilihan tambahan dalam dunia digital modern—melainkan menjadi elemen fundamental dalam menjaga integritas dan keberlangsungan organisasi di berbagai sektor. Dalam lingkungan yang semakin terhubung, serangan siber tidak hanya menjadi lebih sering, tetapi juga lebih kompleks dan merusak. Berikut adalah beberapa alasan utama mengapa keamanan sistem informasi merupakan kebutuhan yang tidak bisa diabaikan:

Gambar 1. 1. Keamanan Sistem Informasi Krusial

1. Melindungi Data Pribadi dan Sensitif

   Data merupakan aset paling berharga dalam dunia digital. Informasi pribadi seperti nomor KTP, riwayat kesehatan, informasi keuangan, dan identitas digital menjadi target utama para peretas (hacker). Jika data ini jatuh ke tangan yang salah, dampaknya bisa sangat luas—mulai dari pencurian identitas, penipuan finansial, hingga pelanggaran hak privasi.

   📌 *Studi Kasus:*
   Pada tahun 2022, sebuah layanan kesehatan digital besar mengalami kebocoran data yang mengekspos lebih dari 50 juta data pasien. Selain merusak reputasi, kasus ini juga memicu tuntutan hukum besar-besaran.

2. Menjaga Kepercayaan Publik dan Reputasi

   Kepercayaan merupakan fondasi utama dalam interaksi digital, baik antara perusahaan dengan pelanggan maupun antar institusi. Sekali terjadi insiden pelanggaran data, kepercayaan publik bisa terkikis dalam hitungan jam, sementara proses pemulihannya bisa memakan waktu bertahun-tahun—dan dalam banyak kasus, tidak pernah benar-benar pulih.

   📌 *Contoh Nyata:*
   Kebocoran data besar yang dialami oleh Facebook (Cambridge Analytica) memicu gelombang protes global dan penurunan signifikan dalam persepsi publik terhadap platform tersebut.

3. Menghindari Kerugian Finansial dan Hukum

   Konsekuensi dari kegagalan melindungi sistem informasi tidak hanya berupa kerugian teknis, tetapi juga kerugian finansial yang sangat besar. Regulasi global seperti GDPR (*General Data Protection Regulation*), CCPA, dan UU Perlindungan Data Pribadi (UU PDP) di Indonesia, menetapkan sanksi berat bagi organisasi yang gagal menjaga data pribadi penggunanya.

   📌 *Fakta Hukum:*
   Denda pelanggaran GDPR dapat mencapai hingga 4% dari total pendapatan tahunan global sebuah perusahaan. Hal ini membuktikan bahwa keamanan informasi adalah investasi, bukan beban.

4. Mendukung Keberlangsungan Operasional

   Serangan terhadap sistem informasi dapat mengakibatkan gangguan operasional yang parah, mulai dari *downtime* aplikasi penting, gangguan layanan pelanggan, hingga kerugian dalam logistik atau produksi. Dalam industri seperti perbankan, layanan kesehatan, dan infrastruktur publik, gangguan semacam ini bisa berdampak langsung pada keselamatan dan kesejahteraan masyarakat.

   📌 *Ilustrasi Kasus:*
   Serangan ransomware pada sistem rumah sakit di Eropa tahun 2021 menyebabkan layanan darurat terganggu selama beberapa hari. Hal ini menunjukkan bahwa ancaman digital juga bisa berdampak pada nyawa manusia.

Keamanan sistem informasi tidak hanya penting untuk melindungi teknologi, tetapi juga untuk menjaga kepercayaan, memenuhi aspek legal, dan memastikan kelangsungan operasional organisasi. Dalam dunia yang semakin tergantung pada digitalisasi, keamanan bukan hanya tentang bertahan dari serangan—tetapi tentang membangun sistem yang *resilient*, adaptif, dan dipercaya oleh seluruh ekosistemnya.

4. Studi Kasus Nyata: Kebocoran Data eHAC Kemenkes

Pada tahun 2021, data pengguna dari aplikasi eHAC (*Electronic Health Alert Card*) milik Kementerian Kesehatan Indonesia bocor dan terekspos di internet. Data yang bocor mencakup informasi pribadi, hasil tes COVID-19, dan data perjalanan. Insiden ini mencoreng kepercayaan publik terhadap layanan pemerintah dan menjadi pelajaran penting tentang pentingnya manajemen keamanan data pada sistem publik.

5. Peran Strategis Keamanan Informasi dalam Dunia Digital

Keamanan sistem informasi bukan hanya urusan divisi IT, tetapi menjadi isu strategis organisasi secara menyeluruh. Dalam dunia yang terkoneksi secara global, semua pihak dari top management hingga pengguna akhir memiliki tanggung jawab terhadap keamanan informasi.

6. Ruang Lingkup Keamanan Sistem Informasi

Keamanan sistem informasi mencakup berbagai aspek teknis, organisasi, dan prosedural yang bertujuan untuk melindungi aset informasi dari berbagai jenis ancaman. Ruang lingkup ini tidak terbatas pada perlindungan sistem komputer semata, tetapi juga mencakup seluruh elemen yang membentuk sistem informasi: manusia, proses, dan teknologi.

Untuk memahami ruang lingkup keamanan secara menyeluruh, pendekatan yang umum digunakan adalah berdasarkan tiga pilar utama: People (Manusia), Process (Proses), dan Technology (Teknologi).

a. Keamanan Manusia *(People Security)*

Manusia sering dianggap sebagai elemen terlemah dalam rantai keamanan informasi. Meskipun teknologi keamanan canggih tersedia, faktor kelalaian, kurangnya kesadaran, atau bahkan niat jahat dari orang dalam (*insider threat*) dapat membuka celah besar dalam sistem.

Fokus perlindungan:

- Edukasi dan pelatihan keamanan informasi (*security awareness training*)
- Pengelolaan hak akses dan prinsip least privilege
- Kebijakan disiplin terhadap pelanggaran protokol keamanan

📌 Contoh: Banyak insiden phishing terjadi karena karyawan tidak mampu mengenali email palsu. Ini menunjukkan pentingnya pelatihan berkelanjutan dalam organisasi.

b. Keamanan Proses *(Process Security)*

Prosedur dan kebijakan memainkan peran penting dalam mengarahkan bagaimana informasi dilindungi. Tanpa adanya proses yang jelas, bahkan sistem keamanan yang paling canggih pun tidak akan efektif.

Fokus perlindungan:

- Pengelolaan risiko dan perencanaan mitigasi
- Dokumentasi dan standar operasional prosedur (SOP)
- Audit internal dan kepatuhan terhadap regulasi seperti ISO/IEC 27001, GDPR, atau UU PDP

📌 Ilustrasi: Prosedur backup dan pemulihan data yang buruk bisa menyebabkan data penting tidak dapat dipulihkan setelah serangan ransomware.

c. Keamanan Teknologi *(Technology Security)*

Teknologi adalah alat yang digunakan untuk menegakkan kontrol keamanan informasi. Ini mencakup perlindungan fisik, jaringan, perangkat keras, perangkat lunak, hingga enkripsi data.

Fokus perlindungan:

- Firewall, antivirus, dan sistem deteksi intrusi (IDS/IPS)
- Enkripsi data dalam penyimpanan dan transmisi
- Autentikasi multifaktor (MFA) dan kontrol akses
- Pemantauan sistem secara real-time (SIEM, log management)

📌 Fakta: Perusahaan yang menggunakan enkripsi end-to-end memiliki risiko kebocoran data yang jauh lebih kecil dibanding yang tidak menggunakannya.

d. Keamanan Fisik *(Physical Security)*

Banyak orang mengabaikan pentingnya keamanan fisik dalam keamanan informasi. Padahal, akses fisik terhadap perangkat keras bisa menyebabkan pencurian data, manipulasi sistem, atau sabotase.

Fokus perlindungan:

- Pengamanan ruang server dan pusat data
- Sistem pengawasan (CCTV), alarm, dan kontrol akses fisik
- Pencegahan terhadap bencana fisik (banjir, kebakaran, dll.)

📌 Contoh: Pencurian laptop yang tidak dienkripsi dari kantor bisa membocorkan informasi penting jika tidak dilindungi secara fisik maupun digital.

e. Keamanan Aplikasi dan Data

Sistem informasi tidak hanya mengandalkan infrastruktur, tetapi juga aplikasi dan data sebagai inti operasionalnya. Kerentanan pada aplikasi bisa menjadi pintu masuk utama bagi serangan siber.

Fokus perlindungan:

- Pengujian penetrasi dan review kode aplikasi
- Manajemen patch dan pembaruan perangkat lunak
- Kebijakan klasifikasi dan retensi data

📌 Ilustrasi: Celah keamanan pada aplikasi e-commerce bisa dimanfaatkan hacker untuk menyisipkan skrip pencurian kartu kredit *(formjacking)*.

f. Keamanan Jaringan dan Infrastruktur

Jaringan adalah jalur utama transfer data antar sistem. Karena sifatnya yang terbuka dan luas, jaringan rentan terhadap berbagai jenis serangan seperti sniffing, spoofing, dan DDoS.

Fokus perlindungan:

- Segmentasi jaringan dan VPN
- Penggunaan firewall dan proxy
- Deteksi anomali trafik dan mitigasi serangan

📌 Studi Kasus: Banyak organisasi mengalami gangguan operasional besar akibat serangan DDoS terhadap server utama mereka.

g. Lingkup Layanan dan Cloud Computing

Transformasi digital dan adopsi cloud menjadikan lingkungan TI lebih dinamis, namun juga lebih kompleks dari sisi keamanan. Lingkungan ini memerlukan model keamanan yang fleksibel dan adaptif.

Fokus perlindungan:

- Manajemen identitas di lingkungan hybrid
- Konfigurasi keamanan cloud (CSPM)
- Pengawasan dan kepatuhan SLA vendor pihak ketiga

📌 Fakta Baru: Lebih dari 90% pelanggaran data di cloud terjadi karena kesalahan konfigurasi, bukan karena kelemahan sistem cloud itu sendiri.

Ruang lingkup keamanan sistem informasi mencakup berbagai dimensi yang saling terkait: manusia, proses, teknologi, fisik, aplikasi, jaringan, dan cloud. Pendekatan yang holistik dan sistemik sangat diperlukan agar organisasi tidak hanya dapat merespons insiden, tetapi juga membangun postur keamanan yang proaktif, berkelanjutan, dan dapat dipercaya.

B. PENGERTIAN SISTEM INFORMASI DAN KEAMANAN

1. Definisi Sistem Informasi

Sistem informasi adalah suatu sistem terorganisasi yang terdiri dari manusia, perangkat keras, perangkat lunak, jaringan, dan data yang bekerja bersama untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi guna mendukung pengambilan keputusan dan pengendalian dalam suatu organisasi.

Komponen Sistem Informasi:

a. Hardware – perangkat fisik (komputer, server, jaringan, IoT)
b. Software – aplikasi yang memproses data (CRM, ERP, database)
c. Data – materi mentah yang diproses menjadi informasi
d. Prosedur – aturan dan proses dalam sistem
e. Manusia – pengguna, admin, dan pengelola sistem

📌 *Contoh:* Sistem Informasi Akademik di universitas yang mencatat data mahasiswa, jadwal kuliah, nilai, dan pembayaran UKT.

2. Keamanan Sistem Informasi

Keamanan sistem informasi (*Information System Security*) adalah praktik dan strategi untuk melindungi seluruh komponen sistem informasi agar terlindungi dari akses tidak sah, gangguan, perubahan, pencurian, atau kerusakan yang dapat mengganggu operasional dan integritas sistem.

Tujuan utama keamanan sistem informasi adalah untuk menjaga tiga aspek utama yang dikenal sebagai **CIA Triad**:

Gambar 1. 2. CIA Triad

Tabel 1. Contoh Implementasi CIA Triad

Aspek	Deskripsi Singkat	Contoh Nyata
Confidentiality **(Kerahasiaan)**	Menjaga agar data hanya dapat diakses oleh pihak yang berwenang	Enkripsi email, proteksi file menggunakan password
Integrity **(Integritas)**	Menjamin bahwa data tidak diubah tanpa otorisasi	Hashing dokumen digital, checksum sistem file
Availability **(Ketersediaan)**	Memastikan sistem dan informasi dapat diakses kapan pun dibutuhkan	Sistem backup, server redundancy, *cloud storage*

3. Mengapa Keamanan Sistem Informasi Penting?

Di era digital yang terhubung secara global, keamanan sistem informasi menjadi landasan penting bagi organisasi, institusi, bahkan individu. Informasi adalah aset strategis, dan perlindungannya bukan sekadar pilihan—melainkan keharusan. Ada empat alasan utama mengapa keamanan sistem informasi harus menjadi prioritas dalam setiap infrastruktur digital. Beberapa alasan utama:

a. Perlindungan privasi pengguna
Privasi bukan hanya hak individu, tetapi juga merupakan salah satu fondasi kepercayaan dalam layanan digital. Data pribadi seperti identitas, lokasi, informasi kesehatan, dan aktivitas online dapat dengan mudah disalahgunakan jika tidak dilindungi. Ancaman seperti pencurian identitas dan pelacakan ilegal menjadi risiko nyata yang merugikan pengguna secara pribadi maupun psikologis.

📌 *Contoh nyata:*
Kebocoran data pengguna aplikasi media sosial dapat dimanfaatkan untuk manipulasi psikologis, kampanye politik, atau pemerasan daring *(cyber extortion).*

b. Menghindari kerugian finansial dan reputasi
Pelanggaran sistem informasi dapat menimbulkan kerugian finansial langsung, seperti denda, kompensasi, atau hilangnya pendapatan karena downtime. Lebih dari itu, reputasi organisasi juga menjadi

BAB 2 KONSEP DASAR KEAMANAN INFORMASI

Siti Nasiroh, M.Kom.

A. PENDAHULUAN

Di era digital saat ini, informasi telah menjadi salah satu aset paling berharga bagi individu, organisasi, maupun negara. Setiap harinya, data dan informasi diproduksi, diproses, dan disimpan dalam jumlah yang sangat besar, baik dalam bentuk teks, gambar, suara, maupun data transaksional. Informasi ini menjadi landasan utama dalam pengambilan keputusan strategis, pelaksanaan operasional, serta sebagai sarana komunikasi dan pertukaran nilai **(Kovba and Moiseenko, 2021).**

Namun, seiring dengan meningkatnya penggunaan teknologi informasi, risiko yang mengancam keamanan informasi juga semakin kompleks. Ancaman ini tidak hanya berasal dari aktor jahat di luar organisasi seperti hacker atau cracker, tetapi juga bisa berasal dari dalam organisasi sendiri, seperti karyawan yang lalai atau memiliki niat buruk. Bahkan, bencana alam dan kesalahan sistem juga dapat menyebabkan kerusakan atau hilangnya data yang vital **(Mustafovski, 2023).**

Keamanan informasi adalah suatu upaya yang dilakukan untuk melindungi informasi dari segala bentuk ancaman, baik yang bersifat internal maupun eksternal, dengan tujuan untuk menjaga kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi tersebut. Tiga aspek ini, yang dikenal dengan istilah CIA Triad, merupakan pilar utama dalam membangun sistem keamanan informasi yang efektif **(Jevtić & Alhudaidi, 2023)**.

Kebutuhan akan keamanan informasi tidak lagi hanya menjadi tanggung jawab departemen teknologi informasi (TI) saja, melainkan menjadi tanggung jawab bersama seluruh lapisan organisasi. Setiap individu yang terlibat dalam pengelolaan dan penggunaan informasi memiliki peran penting dalam menjaga keamanan data. Kesalahan kecil seperti menggunakan kata sandi yang lemah, membuka email

mencurigakan, atau menyebarkan informasi tanpa otorisasi, dapat menjadi celah masuk bagi serangan siber (Choppara, 2022).

Selain itu, banyak organisasi kini terikat dengan regulasi dan standar keamanan informasi yang mewajibkan adanya sistem pengamanan data yang andal, seperti ISO/IEC 27001, NIST, maupun GDPR. Pelanggaran terhadap standar ini tidak hanya berdampak pada kerugian finansial dan reputasi, tetapi juga dapat menimbulkan sanksi hukum (Zebari & Asaad, 2022).

Dengan demikian, memahami konsep dasar keamanan informasi bukan hanya penting bagi profesional IT, tetapi juga bagi manajemen dan seluruh pemangku kepentingan dalam organisasi. Pemahaman ini menjadi dasar untuk membangun kebijakan, prosedur, dan teknologi yang dapat memberikan perlindungan menyeluruh terhadap informasi dalam berbagai bentuknya (Choppara, 2022).

Keamanan informasi yang baik akan menciptakan kepercayaan, menjaga kelangsungan bisnis, serta mendukung upaya digitalisasi yang aman dan berkelanjutan. Dalam bab ini, akan dijelaskan secara menyeluruh mengenai konsep dasar keamanan informasi, ancaman-ancaman yang mungkin terjadi, serta langkah-langkah strategis dalam membangun sistem keamanan informasi yang Tangguh (Somepalli et al., 2020).

B. DEFINISI KEAMANAN INFORMASI

Keamanan informasi adalah praktik perlindungan terhadap informasi agar tetap terlindungi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah. Definisi ini mencakup baik informasi dalam bentuk fisik maupun digital, dan berlaku di seluruh siklus hidup informasi, mulai dari penciptaan, pemrosesan, penyimpanan, hingga penghapusan. (Argaw et al., 2020).

Menurut standar internasional ISO/IEC 27001, keamanan informasi bertujuan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Aspek kerahasiaan menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang; integritas menjaga akurasi dan keutuhan informasi; dan ketersediaan memastikan bahwa informasi tersedia saat dibutuhkan oleh pengguna yang sah.

Selain ketiga aspek utama tersebut, keamanan informasi modern juga memperhatikan aspek-aspek tambahan seperti:

1. dapat menyangkalnya.

Keamanan informasi mencakup dimensi teknis dan non-teknis. Artinya, selain mengandalkan teknologi seperti enkripsi dan firewall, keberhasilan perlindungan informasi juga bergantung pada kebijakan, prosedur operasional, dan perilaku pengguna informasi dalam organisasi.

C. PILAR UTAMA KEAMANAN INFORMASI (CIA TRIAD)

Keamanan informasi dibangun di atas tiga pilar utama yang dikenal dengan sebutan **CIA Triad**, yaitu **Confidentiality (Kerahasiaan)**, **Integrity (Integritas)**, dan **Availability (Ketersediaan)**. Ketiga prinsip ini merupakan kerangka kerja dasar yang menjadi fondasi dari setiap kebijakan, proses, dan teknologi dalam sistem keamanan informasi

Penerapan CIA Triad membantu organisasi dalam merancang dan mengimplementasikan kontrol keamanan yang menyeluruh, memastikan bahwa informasi sensitif tetap terlindungi dari berbagai jenis ancaman, baik yang disengaja maupun tidak disengaja (Miftahul Huda · 2020)

1. **CIA Triad**

Gambar 2. 1. CIA Triad (Confidentiality, Integrity, Availability)

1. Confidentiality (Kerahasiaan)

Kerahasiaan adalah prinsip yang menjamin bahwa informasi hanya dapat diakses oleh individu atau sistem yang memiliki wewenang atau hak akses. Tujuan utama dari aspek ini adalah mencegah pengungkapan informasi kepada pihak yang tidak berwenang.
Pelanggaran terhadap kerahasiaan dapat terjadi melalui berbagai cara **(Argyridou et al., 2022)** , misalnya:

a. Pencurian data oleh peretas.
b. Pengiriman email yang salah alamat.
c. Penggunaan perangkat tanpa otorisasi.

Langkah-langkah untuk menjaga kerahasiaan meliputi:

a. **Enkripsi:** Melindungi data agar tidak dapat dibaca tanpa kunci dekripsi.
b. **Autentikasi:** Memastikan bahwa hanya pengguna yang sah yang dapat mengakses sistem (misalnya login dengan username dan password).
c. **Kontrol Akses Berbasis Peran (RBAC):** Menentukan akses berdasarkan peran pengguna dalam organisasi.
d. **Virtual Private Network (VPN):** Mengamankan koneksi jarak jauh dari lokasi yang tidak terpercaya.
e. **Kebijakan Privasi:** Mengatur bagaimana data pribadi dan sensitif diproses dan disimpan.

2. Integrity (Integritas)

Integritas berkaitan dengan keakuratan, kelengkapan, dan keandalan informasi sepanjang siklus hidupnya. Informasi tidak boleh dimodifikasi, dirusak, atau dihapus secara tidak sah. Integritas menjamin bahwa informasi yang digunakan dalam pengambilan keputusan adalah valid dan tidak dimanipulasi ("Organizational Architecture, Resilience, and Cyberattacks," 2022). Contoh pelanggaran integritas:

a. Data transaksi yang diubah oleh pihak yang tidak sah.
   Ini mengacu pada **modifikasi data secara tidak sah** oleh individu atau entitas yang tidak memiliki otorisasi. Dalam konteks keamanan informasi, ini merupakan bentuk pelanggaran terhadap **integritas data**. Contohnya:
   1) Seseorang yang bukan bagian dari staf keuangan mengakses sistem dan mengubah nominal transaksi.

2) Hacker berhasil masuk ke sistem dan memodifikasi riwayat pembayaran pelanggan.

Dampak dari kejadian ini bisa sangat serius, seperti:

1) Kerugian finansial.
2) Hilangnya kepercayaan pelanggan.
3) Masalah hukum atau kepatuhan regulasi.

b. Perubahan tidak sengaja karena kesalahan perangkat lunak.
Ini adalah perubahan data atau konfigurasi sistem yang terjadi akibat **bug atau kesalahan logika dalam perangkat lunak**, bukan karena tindakan manusia secara langsung. Misalnya:

1) Sistem akuntansi yang salah menghitung total karena kesalahan dalam kode program.
2) Aplikasi yang menyimpan data dengan format salah, sehingga menyebabkan kerusakan atau kehilangan informasi.

Dampaknya bisa mencakup:

1) Kesalahan laporan.
2) Kegagalan sistem.
3) Ketidakakuratan data operasional.

c. File konfigurasi sistem yang diubah oleh malware.
Dalam kasus ini, **malware (perangkat lunak berbahaya)** yang menyusup ke sistem mengubah file konfigurasi sistem untuk keuntungan penyerang. Tujuannya bisa beragam:

1) Memberi akses tak terbatas ke sistem (backdoor).
2) Melemahkan sistem keamanan.
3) Mengarahkan data atau lalu lintas ke server penyerang (misalnya melalui perubahan file hosts atau pengaturan DNS).

Contoh:

- Malware mengubah pengaturan firewall agar koneksi dari luar dapat masuk.
- Trojan memodifikasi konfigurasi sistem agar dapat bertahan dan aktif setelah sistem di-restart.

Dampaknya bisa sangat merusak, termasuk:

1) Kehilangan kendali atas sistem.
2) Kebocoran data sensitif.
3) Gangguan operasional.

BAB 3 ANCAMAN DAN KERENTANAN DALAM

Miswadi, S.Kom., M.Kom.

A. PENDAHULUAN

Sistem informasi merupakan bagian penting dalam organisasi modern. Namun, sistem ini rentan terhadap berbagai ancaman yang dapat mengganggu operasional, mencuri data, atau merusak sistem. Memahami ancaman dan kerentanan dalam sistem informasi sangat penting agar dapat mengambil langkah-langkah perlindungan yang tepat.

Seiring dengan berkembangnya teknologi, ancaman terhadap sistem informasi juga semakin kompleks. Serangan siber, baik yang berasal dari individu maupun kelompok terorganisir, dapat menyebabkan kebocoran data yang merugikan perusahaan dan individu. Oleh karena itu, diperlukan pemahaman mendalam tentang bentuk ancaman serta cara mitigasinya agar sistem informasi tetap aman dan dapat berfungsi secara optimal.

Selain faktor eksternal seperti peretasan dan malware, faktor internal seperti kesalahan manusia dan kebijakan keamanan yang lemah juga dapat menjadi celah keamanan yang signifikan. Keamanan sistem informasi harus mencakup pendekatan yang holistik, melibatkan teknologi, kebijakan, serta pelatihan sumber daya manusia agar dapat menghadapi ancaman yang terus berkembang.

Pada bab ini, akan dibahas lebih lanjut mengenai pengertian ancaman dan kerentanan, jenis ancaman dan kerentanan dalam sistem informasi, contoh kasus ancaman dan kerentanan serta metode perlindungan dari ancaman dan kerentanan

B. PENGERTIAN ANCAMAN DAN KERENTANAN DALAM SISTEM INFORMASI

Ancaman adalah segala sesuatu yang berpotensi merusak atau mengganggu sistem informasi, baik yang berasal dari dalam maupun luar organisasi. Ancaman bisa bersifat fisik, logis, maupun sosial, dan sering kali berkembang seiring dengan kemajuan teknologi.

Kerentanan adalah kelemahan dalam sistem informasi yang dapat dieksploitasi oleh ancaman untuk menyebabkan dampak negatif.

Kerentanan bisa muncul akibat kelemahan teknologi, kesalahan manusia, atau kebijakan yang tidak memadai dalam suatu organisasi.
Jenis Ancaman

1. Ancaman Fisik: Kerusakan perangkat keras akibat bencana alam, pencurian, atau sabotase.
2. Ancaman Siber: Serangan siber seperti virus, malware, phishing, dan peretasan.
3. Ancaman Sosial: Teknik rekayasa sosial yang memanipulasi individu untuk mengungkapkan informasi sensitif.

Jenis Kerentanan

1. Kerentanan Teknologi: Software dengan bug, sistem yang tidak diperbarui, dan protokol keamanan yang lemah.
2. Kerentanan Manusia: Kurangnya kesadaran akan keamanan informasi, penggunaan password yang lemah, dan mudahnya pengguna tertipu oleh serangan phishing.
3. Kerentanan Proses: Kebijakan keamanan yang tidak jelas, kurangnya backup data, serta pengelolaan akses yang buruk.

Contoh:

- Ancaman: Serangan siber oleh hacker
- Kerentanan: Penggunaan password yang lemah memungkinkan hacker mencuri kredensial pengguna.

Ilustrasi Kasus
Sebagai contoh, serangan malware WannaCry tahun 2017 memanfaatkan kerentanan pada protokol SMB di sistem operasi Windows yang tidak diperbarui. Ribuan komputer di berbagai organisasi menjadi korban karena tidak memiliki perlindungan yang memadai.

Tindakan Pencegahan:

- Memastikan sistem selalu diperbarui dengan patch terbaru.
- Menggunakan firewall dan antivirus untuk mencegah eksploitasi kerentanan.
- Melakukan pelatihan keamanan kepada pengguna agar tidak mudah tertipu oleh serangan phishing.

Dengan memahami berbagai jenis ancaman dan kerentanan dalam sistem informasi, organisasi dapat mengembangkan strategi keamanan yang lebih efektif untuk melindungi aset digital mereka

Gambar 3. 1. Siklus keamanan informasi – Identifikasi, Proteksi, Deteksi, Respon, Pemulihan (Sumber: NIST)

C. JENIS ANCAMAN DALAM SISTEM INFORMASI

1. Ancaman Fisik

   Ancaman yang berkaitan dengan kerusakan perangkat keras akibat bencana alam, pencurian, atau sabotase.

   Contoh:

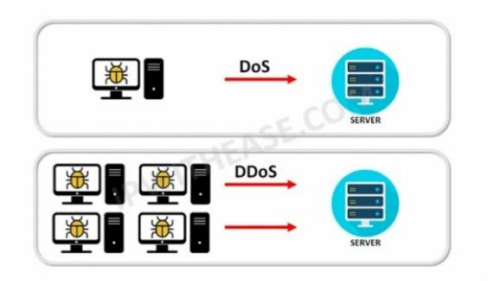
   - Kebakaran yang menghancurkan server
   - Pencurian laptop yang berisi data rahasia

2. Ancaman Logis

Ancaman yang menyerang perangkat lunak, jaringan, atau data dalam sistem informasi.

Contoh:

- Virus dan malware
- Serangan Denial of Service (DoS)



Gambar 3. 2. Ilustrasi serangan DoS terhadap server (sumber : https://cyberthreat.id)

D. JENIS KERENTANAN DALAM SISTEM INFORMASI

Keamanan sistem informasi merupakan aspek krusial dalam operasional bisnis dan pemerintahan. Namun, berbagai kerentanan sering kali dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses, mencuri, atau merusak data. Kerentanan dalam sistem informasi dapat dikategorikan ke dalam kerentanan teknologi, kerentanan manusia, dan kerentanan proses.

1. Kerentanan Teknologi

Kerentanan yang bersumber dari aspek teknologi biasanya terjadi karena adanya kelemahan dalam perangkat lunak, sistem operasi, atau metode komunikasi yang digunakan. Beberapa jenisnya meliputi:

- Software dengan Bug atau Celah Keamanan Perangkat lunak yang dikembangkan tanpa pengujian keamanan yang memadai sering kali memiliki celah yang dapat dieksploitasi oleh peretas. Contoh kasus terkenal adalah eksploitasi kerentanan pada sistem operasi Windows oleh malware WannaCry, yang menyebabkan gangguan global pada tahun 2017. Oleh karena itu, pengujian berkala dan pembaruan sistem merupakan langkah penting dalam mitigasi risiko.
- Penggunaan Protokol Komunikasi yang Tidak Terenkripsi Data yang dikirim melalui jaringan tanpa enkripsi berisiko disadap oleh pihak yang tidak berwenang. Penggunaan protokol seperti HTTP tanpa SSL/TLS dapat membuka peluang bagi serangan Man-in-the-Middle (MitM) di mana penyerang dapat membaca dan mengubah data secara diam-diam. Mengadopsi VPN, HTTPS, dan

enkripsi end-to-end dapat meningkatkan perlindungan data dalam komunikasi digital.

2. Kerentanan Manusia

Serangan siber sering kali menargetkan kelemahan manusia, karena faktor psikologis dan kurangnya kesadaran keamanan sering kali menyebabkan pelanggaran data. Beberapa kerentanan yang umum meliputi:

- Kurangnya Pelatihan Keamanan bagi Karyawan
  Karyawan yang tidak memahami pentingnya pengamanan data dan privasi sering kali menjadi target empuk bagi serangan sosial rekayasa (social engineering). Tanpa edukasi yang tepat, karyawan dapat secara tidak sengaja membagikan kredensial akses atau mengabaikan prosedur keamanan yang telah ditetapkan.
- **Phishing melalui Email**
  Serangan phishing adalah metode manipulasi di mana peretas mengirimkan email atau pesan palsu yang tampak resmi dengan tujuan mencuri data sensitif. Banyak pengguna tertipu oleh tampilan email yang menyerupai institusi terpercaya, sehingga mereka secara sukarela memasukkan informasi login atau melakukan transaksi tanpa sadar bahwa mereka sedang menjadi target serangan.

3. Kerentanan Proses

Selain teknologi dan manusia, prosedur dan kebijakan keamanan yang tidak memadai juga dapat menjadi celah yang memungkinkan serangan siber. Beberapa bentuk kerentanan proses meliputi:

- **Kebijakan Keamanan yang Lemah**
  Banyak organisasi yang tidak memiliki standar keamanan yang jelas, sehingga menciptakan inkonsistensi dalam perlindungan data. Tanpa kebijakan seperti penggunaan kata sandi yang kuat, pembatasan akses berdasarkan peran, serta audit keamanan berkala, sistem informasi menjadi lebih rentan terhadap pelanggaran data.
- **Kurangnya Backup Data Secara Rutin**
  Salah satu kesalahan umum dalam manajemen keamanan adalah tidak memiliki cadangan data (backup) yang cukup untuk mengantisipasi kehilangan akibat serangan atau kegagalan

sistem. Tanpa sistem backup yang memadai, organisasi berisiko kehilangan informasi penting yang dapat berdampak serius pada operasional bisnis.

Mengidentifikasi dan memahami berbagai jenis kerentanan dalam sistem informasi sangat penting untuk meningkatkan perlindungan data serta mencegah risiko serangan siber. Kombinasi antara teknologi yang aman, kesadaran manusia, dan kebijakan yang efektif akan memberikan fondasi yang lebih kuat dalam menjaga keamanan sistem informasi.

E. CONTOH KASUS ANCAMAN DAN KERENTANAN

Ancaman terhadap sistem informasi dapat terjadi dalam berbagai bentuk, mulai dari serangan siber hingga eksploitasi kelemahan dalam infrastruktur teknologi. Salah satu kasus yang menjadi perhatian global adalah serangan ransomware WannaCry pada tahun 2017, yang berdampak luas pada berbagai organisasi dan perusahaan di seluruh dunia.

Studi Kasus: Serangan Ransomware WannaCry (2017)

Pada 12 Mei 2017, dunia dikejutkan oleh serangan ransomware WannaCry, sebuah perangkat lunak berbahaya yang mengenkripsi data pengguna dan meminta tebusan untuk mendapatkan akses kembali. WannaCry menyebar dengan sangat cepat karena memanfaatkan kerentanan dalam protokol SMB (Server Message Block) pada sistem operasi Windows, terutama pada versi yang belum diperbarui.

Dampak Serangan

Serangan ini menginfeksi lebih dari 200.000 komputer di 150 negara, termasuk instansi pemerintah, rumah sakit, perusahaan multinasional, dan organisasi lainnya. Beberapa dampak besar yang ditimbulkan meliputi:

- Rumah sakit di Inggris (NHS) mengalami gangguan operasional, menyebabkan ribuan janji medis dibatalkan.
- Perusahaan seperti FedEx dan Renault harus menghentikan operasi sementara karena sistem mereka terinfeksi ransomware.
- Kerugian finansial mencapai miliaran dolar akibat gangguan bisnis dan upaya pemulihan data yang terkena ransomware.

Cara Penyebaran

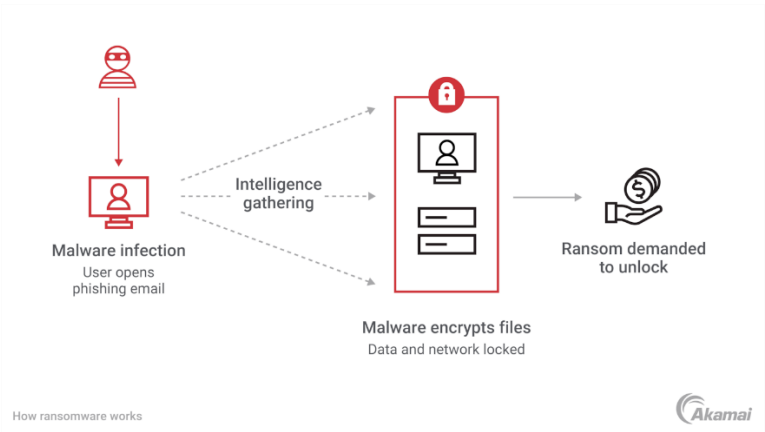
WannaCry menyebar melalui eksploitasi EternalBlue, sebuah kerentanan dalam protokol SMB yang digunakan oleh Windows untuk berbagi file dan printer dalam jaringan. Karena banyak sistem tidak diperbarui dengan patch keamanan yang telah dirilis oleh Microsoft, ransomware ini berhasil masuk dan menyebar ke banyak perangkat dalam waktu singkat.

Pelajaran yang Bisa Dipetik

Serangan ini memberikan banyak pelajaran berharga bagi individu maupun organisasi dalam meningkatkan keamanan sistem mereka. Beberapa langkah preventif yang perlu diterapkan antara lain:

- Selalu Update Sistem Operasi dan Aplikasi
  Memastikan sistem selalu diperbarui dengan patch keamanan terbaru adalah langkah paling efektif dalam mencegah eksploitasi kerentanan. Microsoft sebenarnya telah merilis pembaruan keamanan sebelum serangan terjadi, tetapi banyak sistem belum menerapkannya.
- Gunakan Firewall dan Anti-Malware
  Firewall membantu menyaring lalu lintas jaringan yang mencurigakan, sementara anti-malware berfungsi mendeteksi dan menghapus perangkat lunak berbahaya sebelum dapat menyebabkan kerusakan lebih lanjut.
- Edukasi dan Kesadaran Keamanan Siber
  Banyak serangan ransomware terjadi karena kurangnya kesadaran pengguna terhadap ancaman siber. Pelatihan keamanan dan simulasi serangan dapat membantu meningkatkan kewaspadaan dan mengurangi risiko terinfeksi malware.

Dengan memahami contoh kasus seperti WannaCry, kita dapat mengambil langkah-langkah pencegahan yang lebih baik untuk melindungi sistem dan data dari ancaman yang serupa di masa mendatang. Kesadaran dan tindakan proaktif dalam keamanan informasi sangatlah penting untuk menghindari dampak yang merugikan.



Gambar 3. 3. Diagram penyebaran ransomware WannaCry

F. METODE PERLINDUNGAN DARI ANCAMAN DAN KERENTANAN

Dalam era digital yang berkembang pesat, ancaman terhadap keamanan informasi dan data semakin kompleks dan beragam. Oleh karena itu, diperlukan metode perlindungan yang komprehensif untuk memastikan sistem dan informasi tetap aman dari serangan serta kerentanan. Metode perlindungan dapat dibagi menjadi tiga kategori utama: keamanan fisik, keamanan logis, dan keamanan prosedural.

1. Keamanan Fisik

Keamanan fisik berfokus pada perlindungan infrastruktur teknologi dari akses yang tidak sah atau kerusakan akibat faktor eksternal. Beberapa langkah utama dalam keamanan fisik meliputi:

- Penyimpanan Server di Ruang yang Terkunci
  Server merupakan komponen penting dalam sistem informasi, sehingga perlu disimpan di lokasi yang aman. Ruang server harus memiliki akses terbatas hanya untuk personel yang berwenang dan dilengkapi dengan sistem penguncian yang kuat, seperti kunci elektronik atau biometrik.
- Penggunaan CCTV dan Akses Kontrol
  Pemantauan secara real-time menggunakan CCTV sangat efektif untuk mengidentifikasi aktivitas mencurigakan yang dapat

membahayakan sistem. Selain itu, akses kontrol seperti kartu identitas berbasis RFID atau pengenalan wajah dapat memastikan hanya individu yang berwenang yang dapat memasuki area penting.

2. Keamanan Logis

Keamanan logis bertujuan melindungi data dan sistem dari akses yang tidak sah melalui teknologi informasi. Beberapa metode utama yang digunakan adalah:

- Firewall dan Intrusion Detection System (IDS)
  Firewall berfungsi sebagai benteng pertama yang menyaring lalu lintas jaringan dan mencegah akses yang mencurigakan. Sementara itu, Intrusion Detection System (IDS) mendeteksi serta memperingatkan administrator jika ada aktivitas yang tidak biasa, memungkinkan respons cepat terhadap ancaman.
- Enkripsi Data dan VPN
  Enkripsi digunakan untuk mengubah data menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang, sehingga menjamin keamanan informasi dalam proses penyimpanan maupun transmisi. Selain itu, Virtual Private Network (VPN) memungkinkan koneksi aman antara pengguna dan jaringan internal, melindungi data dari kemungkinan intersepsi oleh pihak eksternal.

3. Keamanan Prosedural

Keamanan prosedural melibatkan penerapan kebijakan dan pelatihan guna meningkatkan kesadaran serta kepatuhan terhadap standar keamanan. Langkah-langkah yang dapat diterapkan meliputi:

- Kebijakan Password yang Kuat
  Penggunaan password yang kompleks dan sulit ditebak merupakan aspek penting dalam menjaga keamanan akun pengguna. Kebijakan ini mencakup penerapan kombinasi huruf besar, huruf kecil, angka, dan simbol, serta penggantian password secara berkala untuk mengurangi risiko pembobolan.
- Pelatihan Keamanan bagi Karyawan
  Kesadaran karyawan terhadap ancaman siber sangat krusial dalam membangun ekosistem kerja yang aman. Pelatihan mengenai phishing, malware, dan praktik keamanan digital dapat meningkatkan kewaspadaan serta mengurangi risiko serangan yang disebabkan oleh kelalaian individu.

Dengan menerapkan keamanan fisik, logis, dan prosedural secara menyeluruh, organisasi dapat meminimalkan ancaman serta kerentanan yang dapat merugikan sistem dan data mereka. Keamanan yang terintegrasi dan berkelanjutan merupakan kunci dalam menjaga stabilitas dan keandalan sistem teknologi informasi.

BAB 4 Keamanan Jaringan dan Infrastruktur IT

Salman Farizy, S.Kom., M.Kom.

A. PENDAHULUAN

Keamanan jaringan dan infrastruktur IT merupakan suatu elemen yang fundamental untuk perlindungan sistem informasi modern, apalagi dengan maraknya era digital saat ini yang kian terhubung atau terkoneksi, jaringan komputer (computer network) menjadi tulang punggung (backbone) komunikasi dan juga operasional organisasi/perusahaan/lembaga, dimulai dari sektor bisnis, pemerintahan, transportasi, market place, kesehatan hingga pendidikan.

Dengan semakin maraknya kejadian akhir – akhir ini dan juga dengan meningkatnya ancaman siber seperti misalnya malware, serangan ransomware, hingga ancaman Distributed Denial of Service (DDoS), sehingga penting dirasa untuk memastikan bahwa jaringan dan infrastruktur IT dirancang, dikelola, dan diawasi dengan baik.

1. Konsep Dasar Keamanan Jaringan dan Infrastruktur IT.

   Teknologi Informasi (TI) merupakan bidang yang mengintegrasikan hardware, software, jaringan, cloud, data center dan juga data dalam proses untuk mendukung pengumpulan, penyimpanan, pemerosesan, serta distribusi informasi. Dalam era digital dan dunia modern, TI menjadi elemen yang cukup penting atau vital yang kita ketahui bersama menunjang hampir di semua aspek kehidupan manusia.

Gambar 4. 1. Komponen Jaringan Komputer dan Infrastruktur IT

Pada intinya, TI berfungsi sebagai suatu solusi untuk meningkatkan efisiensi, efektivitas, dan juga tentunya produktivitas dengan cara otomatisasi proses dan untuk mempercepat komunikasi. Teknologi informasi tersebut dibangun atas dasar "CIA Triad," yang mencakup :

- Kerahasiaan (Confidentiality), → Memastikan bahwa informasi hanya bisa diakses oleh pengguna (user) atau entitas yang tentunya memiliki otorisasi, misalnya dengan teknik enkripsi dan autentikasi.
- Integritas (Integrity), → Menjaga supaya informasi tetap lengkap atau utuh dan tentunya tidak dilakukan modifikasi secara illegal, melalui penggunaan tanda tangan digital atau hash functions.
- Ketersediaan (Availability), → Memastikan bahwa informasi dan juga sistem bisa diakses kapan pun diperlukan oleh pengguna (user) yang legal, dengan menggunakan redundansi sistem atau mekanisme pemulihan (recovery) secara otomatis.

Berikut adalah Gambar 4.2 yang menggambarkan CIA Triad dalam bentuk diagram segitiga.

Gambar 4. 2. Infografis CIA Triad

Teknologi Informasi kian berkembang seiring dengan kemajuan teknologi, komputer pribadi (Personnal Computer), internet, hingga cloud computing muncul dan berkembang yang

memungkinkan akses informasi secara menyeluruh dengan biaya yang tentunya lebih terjangkau. Untuk saat ini, teknologi seperti kecerdasan buatan (AI), blockchain, dan Internet of Things (IoT) menjadi suatu tren baru yang dapat mengubah cara manusia dapat berinteraksi dengan teknologi.

Komponen utama TI mencakup diantaranya perangkat keras (Hardware), perangkat lunak (Software), jaringan, dan pengelolaan data. Hardware seperti komputer, server, dan perangkat IoT, merupakan dasar pondasi fisik yang memungkinkan dalam pengoperasian sistem TI. Software yang terdiri dari sistem operasi (Operating System), aplikasi bisnis, dan program supporting lainnya yang memberikan instruksi kepada hardware untuk menjalankan tugas tertentu. Jaringan, seperti internet atau intranet, memungkinkan komunikasi dan berbagi resource antar perangkat (device). Sementara itu, pengelolaan data menjadi elemen yang cukup krusial dalam mendukung pengambilan keputusan (Decision Making) yang berbasis informasi.

TI telah diaplikasikan dan diimplementasikan diberbagai macam sektor untuk berbagai tujuan dan juga keperluan :
Di dunia bisnis misalnya, TI digunakan untuk otomasi proses, analisis data, dan juga manajemen rantai pasokan (supply chain management).
Dalam dunia pendidikan, TI membantu dalam pembelajaran daring (terhubung melalui jejaring komputer, internet, dan lain sebagainya) dengan platform e-learning.
Di bidang kesehatan, teknologi mendukung pengelolaan rekam medis (medical record) elektronik dan sistem telemedicine.
Pemerintah (Government) menggunakan & memanfaatkan layanan TI untuk membangun layanan publik (Public Service) berbasis e-Government untuk meningkatkan efisiensi dan tentunya yang lebih penting adalah transparansi. Tapi, penerapan TI saat ini juga menghadapi berbagai kendala juga tantangan, seperti misalnya ancaman keamanan siber, kepatuhan terhadap regulasi privasi data (data privacy), dan ketersediaan infrastruktur yang cukup andal.

2. Komponen Keamanan Jaringan Komputer.

Keamanan jaringan dan infrastruktur IT bisa mencakup sejumlah Langkah-langkah dan juga teknologi untuk dapat mencegah, mengidentifikasi serta dapat merespon ancaman keamanan jaringan komputer. Ini meliputi:

- Firewall, →Merupakan teknologi yang digunakan untuk dapat memonitor dan juga memfilter aktivitas atau lalu lintas jaringan. Selain itu firewall juga bisa berfungsi untuk memblokir akses yang tidak sah atau illegal ke jaringan, mencegah serangan spam, spyware, malware dan juga virus, serta berfungsi pula dalam mengidentifikasi aktivitas lalu lintas jaringan yang mencurigakan.
- Enkripsi data, → Suatu proses merubah data menjadi suatu bentuk yang tidak dapat dibaca atau diakses tanpa izin, Ini sangat membantu sekali untuk melindungi data sensitif dari akses yang tidak sah (unauthorized access) atau kebocoran.
- Keamanan Fisik, → Meliputi suatu tindakan untuk mencegah akses fisik (physical access) yang tidak sah ke perangkat jaringan (network device), seperti misalnya saja adalah dengan mengunci ruang atau area server, memasang sensor gerak (motion sensor) dan yang cukup penting dengan melengkapi kamera pengawas.
- Penyaringan dan deteksi malware atau sejenisnya, → Perangkat lunak antivirus (Software Antivirus) dan antispyware biasanya digunakan untuk memeriksa serta mencegah infeksi malware pada 'network device', sementara software untuk mendeteksi malware digunakan juga untuk mendeteksi malware yang sudah terinfeksi pada jaringan.
- Keamanan Akses, → Melibatkan penerapan tindakan keamanan seperti penggunaan 'password' yang kuat, autentikasi 2 (dua) faktor, dan pemeriksaan identitas user untuk bisa memastikan bahwa hanya user yang sah saja yang punya akses ke jaringan.
- Manajemen Patch, → Melakukan pembaharuan (update) software dan sistem operasi (Operating System) untuk memperbaiki kerentanan keamanan dan juga memastikan bahwa perangkat jaringan (Network Device) selalu diperbaharui dengan versi yang terbaru.

B. MENGIDENTIFIKASI JENIS ANCAMAN TERHADAP JARINGAN DAN INFRASTRUKTUR.

1. Kriteria Ancaman (Threat Criteria).

Memasuki Era digital saat ini, keamanan siber menjadi suatu ancaman terhadap jaringan dan juga infrastruktur IT, yang dapat dikategorikan berdasarkan dan bermacam kriteria untuk bisa memahami dampak dan tentunya adalah tingkat risikonya.

Dengan memahami dan juga mengenali ciri khas atau karakteristik dari tiap - tiap ancaman (treat), perusahaan/organisasi/lembaga dapat menentukan strategi mitigasi yang cukup efektif.

Dibawah ini beberapa kriteria utama dalam mengklasifikasikan ancaman (threat) terhadap jaringan dan juga infrastruktur IT:

- Berdasarkan Sumber Ancaman (Threat Source).

  Bisa berasal dari faktor internal maupun eksternal, antara lain :

  Ancaman Internal (Internal Threats) → Berasal dari dalam perusahaan/organisasi/lembaga, seperti misalnya saja adalah karyawan, mitra bisnis atau sistem yang rentan akibat terjadi kesalahan konfigurasi atau kebocoran data.

  Ancaman Eksternal (External Threats) → Berasal dari luar perusahaan/organisasi/lembaga, seperti misalnya saja adalah peretas (hackers), group kriminal siber atau bahkan aktor negara (State Sponsored Attackers).

2. Berdasarkan Tujuan dan Motivasi Serangan.

Ancaman ternyata dapat diklasifikasikan berdasarkan suatu motif dibalik suatu serangan, seperti dibawah ini :

- Finansial.
  Serangan ini punya tujuan untuk mendapatkan benefit atau keuntungan finansial, seperti ransomware atau juga pencurian data kartu kredit (Credit Card).
- Espionase.

Serangan ini punya tujuan untuk mencuri data sensitif demi kepentingan dunia industri ataupun politik.

- Sabotase.
  Sabotase adalah suatu upaya merusak sistem atau layanan yang punya tujuan untuk mengganggu operasional suatu perusahaan/organisasi/lembaga atau bahkan negara.
- Hacktivism.
  Serangan yang dilakukan oleh biasanya oleh kelompok aktivis digital dengan tujuan untuk memprotes suatu kebijakan atau ideologi tertentu.

3. Berdasarkan Dampak terhadap Suatu Sistem.

Tiap - tiap ancaman biasanya punya dampak yang cukup berbeda pada sistem, diantaranya adalah:

- Gangguan Ketersediaan (Availability Attacks) :
  Serangan ini punya tujuan untuk membuat layanan tidak tersedia, seperti serangan DDoS (Distributed Denial of Service).
- Pelanggaran Kerahasiaan (Confidentiality Breaches) :
  Serangan ini dapat menyebabkan kebocoran informasi sensitif, seperti misalnya saja adalah phishing ataupun data breach.

- Pelanggaran Integritas (Integrity Attacks) :
  Merupakan serangan yang punya tujuan untuk memanipulasi atau mengubah data tanpa izin, seperti → SQL injection atau serangan terhadap sistem log (log system).

- Penyalahgunaan Akses (Privilege Escalation) :
  Jenis serangan ini kebanyakan mengeksploitasi kelemahan sistem untuk mendapatkan hak akses (access rights) yang lebih tinggi dari yang seharusnya.

BAB 05 ENKRIPSI DAN KRIPTOGRAFI

Ir. Chairul Anwar, S.Kom., M.Kom., CITPM

A. PENGERTIAN ENKRIPSI DAN KRIPTOGRAFI

Kriptografi adalah seni dan ilmu untuk mengubah data menjadi bentuk yang tidak dapat dibaca oleh orang tanpa pengetahuan khusus. Salah satu metode kriptografi yang dikenal sebagai enkripsi menggunakan algoritma tertentu untuk mengubah pesan asli (*plaintext*) menjadi pesan yang tidak dapat dibaca (*ciphertext*). Komunikasi, transaksi perbankan, keamanan siber, dan penyimpanan data adalah beberapa bidang di mana teknologi ini sangat penting.

Kriptografi, menurut Stallings (2020), adalah metode yang digunakan untuk melindungi data dengan mengubahnya menjadi bentuk yang tidak dapat dipahami oleh orang lain tanpa menggunakan kunci yang tepat. Kurose dan Ross (2020) menyatakan bahwa enkripsi adalah teknik utama untuk keamanan informasi yang digunakan untuk melindungi privasi komunikasi digital. Di sisi lain, Schneeier (2020) menggambarkan enkripsi sebagai proses mengubah data menjadi format yang tidak dapat dipahami tanpa informasi tambahan. Kriptografi menjaga kerahasiaan dan otentikasi data dalam komunikasi, menurut Diffie dan Hellman (2020).

B. KONSEP DASAR KRIPTOGRAFI

Ciphertext adalah data yang telah dienkripsi dan tidak dapat dibaca tanpa proses dekripsi, sedangkan plaintext adalah data asli sebelum dienkripsi. Enkripsi mengubah plaintext menjadi ciphertext, dan dekripsi mengubah ciphertext kembali menjadi plaintext. Kunci, atau kunci, adalah informasi rahasia yang digunakan dalam proses enkripsi dan dekripsi dalam kriptografi.

William Stallings (2020) menekankan bahwa kriptografi kontemporer tidak hanya berfokus pada enkripsi tetapi juga pada elemen keamanan lainnya, seperti autentikasi dan integritas data. Menurut Stallings, konsep dasar kriptografi terdiri dari penggunaan algoritma matematis untuk

mengamankan data dan komunikasi, dan algoritma ini dimaksudkan untuk memastikan bahwa hanya pihak yang memiliki otorisasi yang dapat mengakses informasi yang telah dienkripsi.

Menurut Schneier (2020), kriptografi memainkan peran penting dalam menjamin keamanan data di jaringan yang tidak aman. Ia mengatakan bahwa komunikasi digital akan sangat rentan terhadap serangan seperti penyadapan dan manipulasi data jika tidak ada mekanisme enkripsi yang kuat. Schneier menekankan bahwa setiap metode enkripsi harus diuji keamanannya agar dapat menangkal ancaman baru.

Kurose dan Ross (2020) menyoroti ide dasar kriptografi yang mencakup selain enkripsi dan dekripsi metode seperti hashing dan tanda tangan digital. Tanda tangan digital digunakan untuk memastikan identitas pengirim dalam transaksi digital, sedangkan hashing memastikan integritas data dengan membuat nilai unik dari informasi. Keamanan data dapat diperkuat dengan menggabungkan metode ini.

Diffie dan Hellman (2020) mengatakan bahwa konsep kriptografi berkembang dari pendekatan klasik seperti sandi substitusi hingga pendekatan modern seperti enkripsi berbasis kunci publik. Mereka menekankan bahwa kemajuan dalam kriptografi memungkinkan pengamanan komunikasi digital dalam berbagai aplikasi, seperti transaksi finansial dan percakapan rahasia.

Kriptografi berbasis kunci publik menjadi kemajuan penting dalam keamanan digital, menurut Rivest, Shamir, dan Adleman (2020). Mereka menciptakan algoritma RSA, yang saat ini menjadi salah satu metode enkripsi paling aman. Mereka menegaskan bahwa kriptografi kontemporer harus terus berkembang seiring dengan meningkatnya kemampuan komputasi yang dapat digunakan untuk membobol sistem enkripsi yang ada.

Secara umum, tujuan kriptografi adalah untuk memenuhi empat elemen keamanan, yaitu:

1. Kerahasiaan (Kerahasiaan): memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang.
2. Integritas (Integritas): Menjamin bahwa pihak yang tidak berwenang tidak mengubah data.
3. Otentikasi, juga disebut autentikasi, adalah proses untuk memastikan bahwa orang yang mengirimkan dan menerima informasi adalah orang yang sebenarnya.

4. Non-repudiasi: menahan seseorang dari menyangkal bahwa mereka telah mengirim atau menerima suatu pesan.

C. JENIS-JENIS KRIPTOGRAFI

1. Kriptografi yang berbentuk simetris

   Untuk enkripsi dan dekripsi, kriptografi simetris menggunakan satu kunci. AES (Advanced Encryption Standard), DES (Data Encryption Standard), dan RC4 adalah beberapa algoritma yang paling umum digunakan. Metode ini menguntungkan karena cepat dan efektif, tetapi memiliki kelemahan dalam penyebaran kunci yang sulit dan risiko kompromi jika kunci diketahui.

   Percontohan serta Perhitungan

   Sebagai contoh, jika kita menggunakan algoritma Caesar Cipher untuk mengenkripsi kata "HELLO", kita akan melakukan pergeseran 3 pada kata tersebut.

   H → K

   H → E

   L → O

   L → O

   O → R

   Cipher teks adalah "KHOOR".

Meskipun teknik ini sederhana, Kurose dan Ross (2020) menyatakan bahwa algoritma simetris kontemporer seperti AES jauh lebih kompleks dan aman karena menggunakan transformasi matematis yang lebih kuat.

2. Kriptografi yang tidak simetris

Metode ini menggunakan dua kunci: kunci publik (public key) dan kunci privat (private key). Ini membedakannya dari kriptografi simetris. Salah satu contoh algoritma yang digunakan adalah RSA, ECC (Elliptic Curve Cryptography), dan DSA. Kelebihan kriptografi asimetris adalah meskipun lebih lambat daripada metode simetris, itu membuat komunikasi terbuka lebih aman.

Percontohan serta Perhitungan

Kita memilih dua bilangan prima besar dalam RSA:

q = 53, p = 61

n=p×q=61×50=3233

f(n) = (p-1)(q-1) = (61-1)(53-1) = 3120

Pilih e = 17 (bilangan prima yang relatif dengan 3120).

Hitung d, dan dapatkan bahwa d ≡ e−1 mod ϕ (n) = 2753.

Karena itu, pasangan penting adalah:

Publik key: (e=17, n=3233)

Konfirmasi pribadi: (d=2753, n=3233)

Jika M = 65 (misalnya, huruf "A") dikodekan:

C = Me, n = 6517, dan 3233 = 2790.

Menurut Rivest, Shamir, dan Adleman (2020), masalah faktorisasi bilangan prima besar adalah kunci keamanan RSA.

3. Kriptografi Multifungsi

Kriptografi hibrida menggabungkan fitur kriptografi simetris dan asimetris. Kriptografi asimetris biasanya digunakan untuk mendistribusikan kunci enkripsi simetris, yang kemudian digunakan untuk mengenkripsi banyak data. Protokol SSL/TLS, yang digunakan dalam komunikasi web, adalah contoh penggunaan kriptografi hibrida.

Contoh Penggunaan

Ketika pengguna mengakses situs web melalui protokol HTTPS, mereka melakukan hal berikut:

a. Klien menerima kunci publik RSA dari server.
b. Kunci publik ini digunakan oleh klien untuk mengenkripsi kunci sesi AES.
c. Kunci privat RSA digunakan untuk mendekripsi kunci sesi oleh server.
d. AES yang lebih cepat digunakan untuk semua komunikasi berikutnya.

e. Metode ini memungkinkan komunikasi yang aman dan efektif tanpa menguras sumber daya komputer, menurut Schneier (2020).

D. ALGORITMA

Beberapa algoritma enkripsi yang paling umum digunakan adalah: Algoritma enkripsi mengamankan informasi dengan mengubahnya menjadi format yang tidak dapat dipahami tanpa kunci dekripsi.

A. Standar Enkripsi Tinggi (AES)

AES adalah algoritma enkripsi simetris yang menggunakan ukuran kunci 128, 192, atau 256 bit. Menurut Daemen dan Rijmen (2020), karena lebih aman dan efisien, AES menggantikan DES. Proses enkripsi AES terdiri dari beberapa putaran transformasi, seperti penambahan kunci, substitusi byte, pergantian baris, dan pencampuran kolom.

Perhitungan AES contoh 128-bit

Sebagai contoh, anggaplah string berikut: 0x3243F6A8885A308D313198A2E0370734

a. S-box digunakan untuk substitusi byte.
b. Baris yang bergerak dalam matriks 4×4.
c. Kombinasi kolom dan matriks transformasi.
d. Tambahan kunci melalui operasi XOR

Setelah beberapa putaran, ciphertext yang sulit ditebak tanpa kunci dihasilkan.

B. Protokol Enkripsi Data Standar (DES)

Menurut Kurose dan Ross (2020), DES adalah algoritma enkripsi simetris yang menggunakan kunci 56-bit dan membagi data menjadi blok 64-bit. Ini menggunakan 16 putaran enkripsi dengan fungsi substitusi dan permutasi.

Sebuah contoh perhitungan DES

Misalkan teks biasa: "HELLO123" diubah menjadi biner dan kemudian diproses dengan:

a. Perubahan awal
b. Blok dibagi menjadi dua bagian.

c. Enkripsi menggunakan kunci round dan fungsi Feistel.
d. Ciphertext dibuat setelah permutasi.

C. RSA (Rivest-Shamir-Adleman)

RSA adalah algoritma enkripsi asimetris dengan dua kunci: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Menurut Rivest, Shamir, dan Adleman (2020), masalah faktorisasi bilangan prima besar adalah kunci keamanan RSA.

Beberapa contoh perhitungan RSA

Misalkan kita memutuskan untuk menggunakan bilangan prima:

q = 53, p = 61

n=p×q=61×50=3233

f(n) = (p-1)(q-1) = (61-1)(53-1) = 3120

Pilih e = 17 (bilangan prima relatif dengan 3120).

Hitung d, dan dapatkan bahwa d ≡ e−1 mod ϕ (n) = 2753.

Jika M = 65 dikodekan:

C = Me, n = 6517, dan 3233 = 2790.

Dekripsi data:

M = C d mod n = 2790 2753 mod 3233 = 65

Protokol keamanan seperti SSL/TLS menggunakan RSA untuk komunikasi yang aman.

E. HASHING DAN DIGITAL SIGNATURE

1. Hashing

Menurut Krawczyk et al. (2020), hashing digunakan untuk memastikan integritas data dalam sistem keamanan digital dengan mengubah data menjadi nilai tetap (hash value) yang unik yang tidak dapat dikembalikan ke bentuk aslinya.

Contoh perhitungan hash SHA-256

a. Misalkan teks bertuliskan "Hello World":
b. Transformasi teks ke dalam format biner atau ASCII.
c. Tambah ke algoritma SHA-256.
d. Hasil yang diperoleh adalah sebagai berikut: **a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b53b5d49f4494e36e**

Setiap perubahan kecil pada input akan mengubah hash secara signifikan, menjamin keamanan data.

2. Tanda tangan digital

Tanda tangan digital, juga dikenal sebagai tanda tangan digital, adalah metode otentikasi yang menggunakan kriptografi asimetris untuk menjamin keaslian dan integritas data. Menurut Rivest, Shamir, dan Adleman (2020), algoritma hashing dan kunci privat digunakan untuk membuat tanda tangan digital, yang kemudian divalidasi dengan kunci publik.

Contoh Digital Signature menggunakan RSA untuk Perhitungan

Misalkan kita menerima pesan yang disebut "Dokumen Penting":

a. Menghash pesan dengan SHA-256:
   - Hasil hash adalah:

     e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855, dan hasilnya adalah

b. hash enkripsi menggunakan kunci privat RSA:
   - Penanda = Hash^d mod n
   - Sebuah tanda tangan disertakan dalam pesan.
c. Penerima mendekripsi tanda tangan dengan menggunakan kunci publik:
   - Signature^e mod n = Hash
d. Jika hash dan hash asli sama, pesan itu valid.

E-banking, kontrak digital, dan blockchain menggunakan tanda digital untuk mencegah pemalsuan data.

F. IMPLEMENTASI KRIP

Teknik enkripsi, hashing, dan tanda tangan digital digunakan dalam berbagai sistem keamanan informasi sebagai bagian dari implementasi kriptografi. Menurut Schneier (2020), untuk mencegah kebocoran data, serangan siber, dan pelanggaran privasi, sangat penting untuk menerapkan kriptografi yang efektif. Berikut adalah beberapa contoh bagaimana kriptografi digunakan dalam berbagai industri:

1. Keamanan Komunikasi dan Jaringan

Protokol keamanan seperti SSL/TLS menggunakan kriptografi untuk melindungi komunikasi antara klien dan server. Protokol ini mengenkripsi data yang dikirim melalui internet agar orang yang tidak berwenang tidak dapat melihatnya.

Beberapa contoh perhitungan SSL/TLS

Misalkan sebuah browser berusaha mengakses situs web yang menggunakan protokol HTTPS:

a. Browser mengirimkan permintaan ke server untuk berkoneksi.
b. Sertifikat SSL yang mengandung kunci publik RSA dikirimkan oleh server.
c. Setelah menggunakan kunci publik RSA untuk mengenkripsi "kunci sesi", browser mengirimkannya ke server.
d. Kunci privat server digunakan untuk mendekripsi "kunci sesi".

Ini adalah "kunci sesi" yang digunakan untuk mengenkripsi data yang dikirim melalui enkripsi AES.

2. Keamanan Data Database

Ketika data sensitif disimpan dalam basis data, kriptografi digunakan sehingga hanya orang yang berwenang yang dapat mengaksesnya. Salah satu contoh enkripsi yang sering digunakan dalam sistem basis data kontemporer adalah AES.

Perhitungan Contoh Enkripsi AES pada Basis Data

Misalkan kami memiliki informasi pengguna:

a. Nama pengguna adalah "user123".
b. Passwordnya adalah "mypassword".

Metode enkripsi AES-128:

a. Transformasi teks menjadi bentuk biner.
b. Dengan menggunakan S-box AES, lakukan substitusi byte.
c. Pergeseran baris dan campuran kolom.
d. Menggabungkan kunci enkripsi menggunakan operasi XOR.

Data disimpan dalam basis data dengan hash password SHA-256 untuk keamanan tambahan: **f1d2d2f924e986ac86fdf7b36c94bcdf32beec15.**

3. Kriptografi Blockchain dan Cryptocurrency

Hashing dan kriptografi asimetris digunakan dalam blockchain untuk menjamin transaksi. Untuk menjamin integritas data, setiap blok rantai memiliki hash khusus.

Perhitungan Hash pada Blockchain: Contoh

Misalkan data berikut ada dalam sebuah transaksi:

a. Penyebar: Alice
b. Pemberi: Bob
c. Total: 5 BTC

Dengan SHA-256:

a. Data transaksi diubah menjadi format biner.
b. Hashing menggunakan SHA-256.
c. Identitas transaksi didasarkan pada hash hasil: 6fe2a5df..cbf5c4a1a8e7c6d4

Disebabkan fakta bahwa setiap blok memiliki hash yang bergantung pada blok sebelumnya, manipulasi data menjadi lebih sulit.

4. Kriptografi untuk Tanda Tangan Digital dan Sistem e-Government

Dokumen elektronik seperti kontrak digital, e-KTP, dan sertifikat elektronik dilindungi dengan tanda tangan digital.

Perhitungan Tanda Tangan Digital menggunakan RSA

Misalkan dokumen elektronik bertuliskan "Surat Keputusan".

a. Hashing file dengan SHA-256:

- Hash hasilnya adalah d2d2c3f...9a1f4b.

b. Enkripsi hash menggunakan kunci pengirim privat:
   - Penanda = Hash^d mod n

c. Penerima mendekripsi tanda tangan dengan kunci yang tersedia untuk umum:
   - Signature^e mod n = Hash

d. Dokumen valid jika hash asli dan hasil dekripsi cocok.

Sistem tanda tangan digital untuk dokumen resmi menggunakan implementasi ini.

Kurose dan Ross (2020) menyatakan bahwa untuk melindungi privasi pengguna dan memastikan keamanan komunikasi di dunia maya, penerapan kriptografi yang kuat dalam sistem digital sangat penting.

G. RANGKUMAN

Di era digital, kriptografi adalah teknologi yang sangat penting untuk menjaga keamanan dan kerahasiaan informasi. Algoritma enkripsi seperti AES dan RSA sangat penting untuk melindungi komunikasi dan penyimpanan data, dan hashing dan tanda tangan digital digunakan untuk memastikan integritas dan autentikasi informasi.

Dengan perkembangan teknologi dan ancaman keamanan yang terus meningkat, kriptografi yang kuat menjadi semakin penting untuk menjaga keamanan informasi di berbagai sektor. Oleh karena itu, sangat penting bagi individu dan organisasi untuk memahami konsep dan penerapan kriptografi untuk menjaga keamanan informasi mereka.

BAB 6 AUTENTIKASI DAN KONTROL AKSES

Imam Halim Mursyidin, S.Kom., M.Kom.

A. AUTENTIKASI

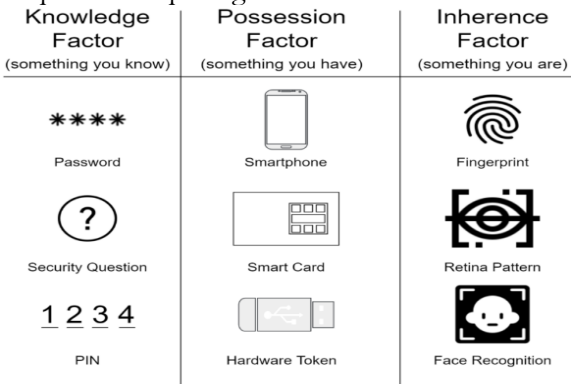
Autentikasi yang aman merupakan salah satu fondasi utama dalam menjaga keamanan sistem informasi. Ancaman keamanan seperti pencurian identitas, akses tidak sah, dan serangan peretas, menjadikan Autentikasi yang kuat diperlukan untuk melindungi sistem informasi. (Windyasari, V. S. et al. 2024) Autentikasi sendiri merupakan proses verifikasi identitas seseorang atau entitas yang mencoba mengakses sistem. Tujuan utama dari Autentikasi adalah memastikan bahwa hanya individu atau perangkat yang sah yang diizinkan untuk mengakses sistem. Autentikasi yang lemah dapat membuka celah bagi pelaku kejahatan siber untuk mengakses informasi penting, baik itu data pribadi maupun rahasia perusahaan.

1. Jenis Autentikasi

Untuk mengakses sistem dan data sensitif seperti aplikasi perbankan, basis data rahasia, atau bahkan gedung perkantoran yang dibatasi—pengguna sering kali harus melewati beberapa bentuk proses autentikasi. Artinya, mereka harus membuktikan bahwa mereka adalah pengguna yang sah. Dalam sistem autentikasi paling dasar, yang dibutuhkan hanyalah kata sandi atau yang disebut *Single Factor Authentication* (SFA). Namun Penggunaan juga dapat menggunaaan 2 faktor autentikasi (2FA) dan *Multi Factor Authentication* (MFA). Misalnya, pengguna masuk ke jaringan perusahaan tempat mereka bekerja, yang dilindungi oleh solusi MFA. Sistem akan meminta faktor autentikasi pertama, biasanya berupa kombinasi nama pengguna dan kata sandi.Jika faktor pertama valid, sistem akan meminta faktor kedua. Terdapat lebih banyak variasi pada faktor kedua, yang dapat berkisar dari kode akses sekali pakai hingga biometrik dan lainnya. Jika pengguna ingin mengakses bagian jaringan yang sangat sensitif, mereka bahkan mungkin perlu menyediakan faktor ketiga.

Berbagai jenis faktor dianggap lebih aman daripada penggunaan beberapa faktor dengan jenis yang sama karena penjahat dunia maya perlu menggunakan metode terpisah di beberapa saluran untuk memecahkan setiap faktor. Misalnya, peretas dapat mencuri kata sandi

pengguna dengan menanamkan Akira di komputer mereka. Namun, Akira tersebut tidak akan mengambil kode sandi yang dikirim ke ponsel pengguna, dan tidak akan menyalin sidik jari pengguna. Penyerang perlu menyadap pesan SMS yang berisi kode sandi dan meretas pemindai sidik jari untuk mengumpulkan semua informasi yang mereka butuhkan guna membajak akun pengguna. Berikut jenis-jenis faktor dapat dilihat pada gambar 6.1 :



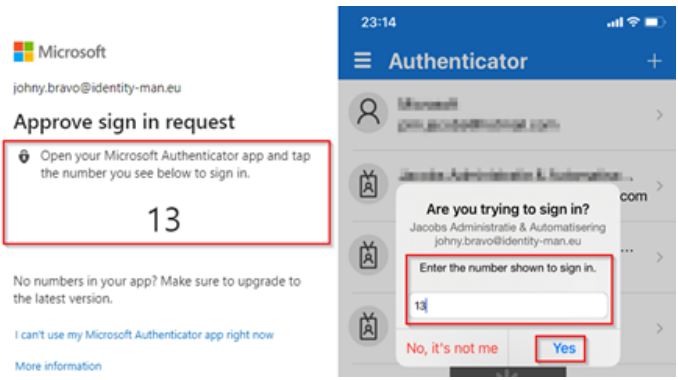
Gambar 6. 1. Jenis-jenis faktor Autentikasi

Sumber: Website https://rublon.com

a. ***Something you know/knowledge*** **(faktor pengetahuan)**
Faktor pengetahuan adalah faktor yang hanya diketahui oelh pengguna misalnya password, PIN, jawaban atas pertanyaan keamanan. Faktor ini dianggap apling rentan Peretas dapat memperoleh kata sandi dan faktor pengetahuan lainnya melalui serangan *phising*, memasang *malware* pada perangkat pengguna, atau melakukan serangan *brute-force* dengan menggunakan bot untuk membuat dan menguji kata sandi potensial pada akun hingga berhasil. Komponen yang dapat melemahkan lainnya adalah pertanyaan keamanan yang di anggap klasik seperti siapa nama gadis ibu Anda? atau berapa tanggal lahir anda ?, ini merupakan pertanyaan kalsik yang mudah ditebak melalui riset media sosial dan mengelabui pengguna agar membocorkan informasi pribadi. Oleh karenanya dengan menggunakan verifikasi dua langkah (2FA) memberikan beberapa keamanan tambahan karena memerlukan lebih dari satu faktor, tetapi tidak seaman MFA yang sebenarnya.

b. **S*omething you have/posession*** **(faktor kepemilikan)**, faktor kepemilikan adalah hal-hal yang dimiliki seseorang yang dapat

digunakan untuk membuktikan identitasnya. Faktor kepemilikan contohnya token digital dan token yang berbentuk fisik. token digital adalah kunci keamanan yang disimpan atau dibuat oleh perangkat yang dimiliki pengguna biasanya *smartphone* dan laptop, misalnya kode *one-time password* (OTP) yang berubah setiap kali pengguna masuk. OTP adalah kode unik yang dikirimkan ke *smartphone* atau laptop pengguna melalui SMS, email, atau aplikasi autentikator. Di dalam OTP *terdapat time-based one-time password* (TOTP) dimana setiap OTP dikirimkan dalam waktu 30-60, apabila dalam waktu tersebut habis maka kata sandi akan menjadi usang dan pengguna harus melakukan permintaan OTP kembali. Sedangkan penggunaan OTP menggunakan aplikasi autentikator seperti *Google Authenticator* dan *Microsoft Authenticator* pada gambar 6,2.



Gambar 6. 2. Microsoft Authenticator

Sumber: Website https://identity-man.eu

Bentuk autentikasi l;ainnya adalah menggunakan perangkat keras khusus yang berfungsi sebagai token fisik. Beberapa token fisik dicolokkan ke port USB komputer dan mengirimkan informasi autentikasi secara otomatis seperti contoh pada gambar 6.3

Gambar 6. 3. Token

Sumber: Website https://www.yubico.com

Keuntungan utama dari faktor kepemilikan adalah bahwa pelaku kejahatan harus memiliki faktor tersebut, namun, faktor kepemilikan bukanlah hal yang sepenuhnya aman, *smartphone* atau token milik pengguna dapat dicuri, hilang, atau salah tempat. Selain itu terdapat juga serangan SIM Swap (SIM *Hijacking*) Penyerang menipu operator seluler untuk mentransfer nomor korban ke SIM baru yang mereka kendalikan. Setelah berhasil, penyerang bisa menerima semua SMS, termasuk OTP, yang memungkinkan mereka mengambil alih akun korban.

c. ***Something you are*** **(faktor bawaan)**, seperti biometrik, disebut biometrik akrena faktor bawaan yakni ciri fisik yang unik bagi pengguna, seperti sidik jari, pengenalan wajah, suara atau retina. Banyak *smartphone* dan laptop dilengkapi dengan pemindai wajah dan pembaca sidik jari sebagai faktor autentikasi. Meskipun faktor bawaan merupakan salah satu yang paling sulit dipecahkan, hal itu dapat dilakukan sidik jari bisa dipalsukan menggunakan cetak 3D dari jejak sidik jari yang tertinggal di permukaan seperti kaca atau layar atau foto berkualitas tinggi. Kemajuan teknologi seperti *artificial intelligence* (AI) juga dapat disalahgunakan untuk mengelabui perangkat lunak pengenalan wajah. Faktor lainnya yaitu seperti cahaya yang buruk, luka di jari, atau sensor kotor bisa menyebabkan kegagalan autentikasi. Jika data biometrik terganggu, data tersebut tidak dapat diubah dengan cepat atau mudah, sehingga sulit menghentikan serangan yang sedang berlangsung dan mendapatkan kembali kendali atas akun.

d. ***Something the user does/ Behavior*** **(faktor prilaku)**, faktor perilaku yang memverifikasi identitas pengguna berdasarkan pola perilaku, seperti rentang alamat IP umum pengguna, sistem

membandingkan alamat IP login dengan alamat IP yang biasa digunakan contoh: Jika pengguna biasanya login dari Indonesia tetapi tiba-tiba mencoba login dari Rusia, sistem bisa menolak akses, lokasi (*Geolocation*) Sistem memverifikasi apakah login berasal dari lokasi yang biasa digunakan oleh pengguna. Penyerang juga dapat memalsukan alamat IP mereka agar tampak terhubung ke VPN perusahaan, sehingga mengelabui sistem autentikasi. Namun penggunaan faktor prilaku perlu hati-hati karena dapat false positive, misalnya jika pengguna bepergian dan login dari lokasi berbeda.

2. Kategori Metode Autentikasi

Metode autentikasi berdasarkan jumlah faktor yang digunakan untuk memverifikasi identitas pengguna dapat diklasifikasikan menjadi tiga kategori utama: *Single-Factor Authentication* (SFA), *Two-Factor Authentication* (2FA), dan *Multi-Factor Authentication* (MFA).

a. Autentikasi Faktor Tunggal *(SFA-Single Factor Authentication)*
SFA adalah metode autentikasi yang hanya menggunakan satu faktor verifikasi untuk mengakses suatu sistem. Faktor yang digunakan biasanya berupa password atau PIN. Secara kelebihan mudah digunakan dan diimplementasikan dan tidak memerlukan perangkat tambahan. Namun karena hanya menggunakan satu faktor verifikasi dalam hal keamanan menjadi rendah dan rentan terhadap serangan *brute force*, *phishing*, atau *credential stuffing*. Berikut beberapa contoh penggunaan SFA :
1) Login ke akun sistem hanya dengan **username dan password**.
2) Membuka kunci ponsel hanya dengan **PIN.**

b. Autentikasi Dua Faktor *(2FA-Two Factor Authentication)*
2FA adalah metode autentikasi yang menggunakan dua faktor berbeda untuk memverifikasi identitas pengguna. Faktor ini harus berasal dari dua kategori yang berbeda Kombinasi 2FA yang dapat dilakukan adalah :
1) **Kata Sandi + (*One-Time Password*) OTP via aplikasi *authenticator* atau token atau SMS atau email**. OTP berubah setiap detik sehingga meskipun kata sandi dicuri, penyerang masih memerlukan akses fisik ke perangkat untuk mendapatkan OTP.
Kata Sandi + Biometrik (Sidik Jari/Pengenalan Wajah). Biometrik sulit dipalsukan karena setiap orang memiliki

karakteristik fisik yang unik, selain itu pengguna tidak perlu perangkat tambahan, cukup menggunakan sensor di perangkat (*smartphone* atau laptop). Namun informasi Autentikasi biometrik sebaiknya dibatalkan jika pernah di bobol. Autentikasi biometrik juga mungkin tak tersedia pada kondisi tertentu (misalnya penuaan, kerusakan), untuk mengantisipasinya, Autentikasi biometrik sebaiknya disertai dengan teknik Autentikasi lainnya.

2) **Kata Sandi + Token.** Token adalah perangkat fisik atau aplikasi perangkat lunak yang menghasilkan kode Autentikasi satu kali (*One-Time Password*/OTP). Token ini membuktikan bahwa pengguna memiliki perangkat fisik yang sah. Penyerang tidak bisa mendapatkan akses ke sistem hanya dengan mengetahui kata sandi; mereka juga harus memiliki token fisik atau perangkat yang menghasilkan OTP.

Contoh penggunaannya dapat dilakukan untuk :

1) Layanan keuangan dan perbankan seperti login ke internet banking, aplikasi dompet digital, layanan pembayaran online.
2) Akses ke layanan cloud seperti gmail, google drive, microsoft, one drive, Aple ID app store dan iCloude, dropbox dan penyimpanan cloud lainnya.
3) Sistem perusahaan dan akses ke jaringan seperti VPN, sistem ERP, email perusahaan, dan aplikasi kerja lainnya.
4) Akun media sosial dan komunikasi seperti facebook, instagram, twitter/x, whatsapp, telegram dan lainnya
5) Aplikasi e-commerce dan marketplace seperti Tokopedia, shopee, amazon, alibaba dan lainnya
6) Layanan pemerintah dan pendidikan seperti portal pajak DJP onlinem BPJS, Dukcapil maupun portal akademik seperti e-learning, LMS dan lainnya.

Akses biometrik biasanya dibutuhkan untuk layanan yang disebutkan di atas namun berbasis *mobile* seperti smartphone & tablet. Selain itu biometrik dapat digunakan untuk akses keamanan fisik seperti kunci pintu pintar (*smart lock*) yang memerlukan sidik jari atau wajah + PIN cadangan, brankas digital dengan sensor biometrik dan lainnya.

BAB 7 MANAJEMEN RISIKO DALAM SISTEM INFORMASI

Roynaldy Rosdiyanto, M.Kom.

A. PENGERTIAN MANAJEMEN RISIKO

Manajemen risiko merupakan langkah terencana untuk mengenali, menganalisis, menilai, dan mengatur risiko di dalam suatu organisasi atau proyek. Sasaran utama dari manajemen risiko adalah untuk mengurangi atau memperkecil efek buruk dari risiko serta memaksimalkan potensi yang ada.

B. PENILAIAN RISIKO KEAMANAN INFORMASI

Risiko dapat dijelaskan sebagai kombinasi dari dampak yang muncul setelah terjadinya suatu insiden yang tidak diharapkan dan kemungkinan terjadinya insiden tersebut. Evaluasi risiko bertujuan untuk menilai atau menggambarkan secara kualitatif suatu risiko dan memberikan kesempatan kepada pengelola untuk mengurutkan risiko berdasarkan tingkat keparahan yang mereka anggap atau kriteria lain yang telah ditetapkan.

Penilaian risiko memuat kegiatan-kegiatan sebagai berikut :

1. Analisa Risiko
   - Identifikasi risiko
   - Estimasi Risiko
2. Evaluasi Risiko

Penilaian risiko menilai nilai sumber daya informasi, menemukan ancaman yang ada dan kelemahan yang mungkin ada, mengidentifikasi kontrol yang sudah ada dan dampaknya terhadap risiko yang ditemukan, Melaksanakan penilaian terhadap potensi dampak dari setiap risiko, menentukan tingkat prioritas berdasarkan tingkat keparahan dan kemungkinan terjadinya, serta mengelompokkan risiko-risiko tersebut sesuai dengan kriteria evaluasi yang telah ditetapkan dalam konteks manajemen proyek yang relevan.

Penilaian risiko sering kali dijalankan dalam beberapa langkah. Di langkah pertama, evaluasi umum dilakukan untuk mengidentifikasi bahaya yang mungkin berdampak besar dan membutuhkan penyelidikan lebih lanjut. Langkah selanjutnya mungkin mencakup pemeriksaan lebih rinci mengenai risiko besar yang telah ditemukan sebelumnya. Jika data yang didapatkan tidak memadai untuk mengevaluasi risiko, maka dilakukan analisis yang lebih mendalam, mungkin pada aspek tertentu dari keseluruhan cakupan, dan bisa jadi dengan menerapkan metode yang berbeda. Keputusan tentang bagaimana mengevaluasi risiko sepenuhnya menjadi hak organisasi, yang dapat memilih berdasarkan tujuan dan target evaluasi risiko.

C. ANALISIS RISIKO

1. Identifikasi Risiko

a. Pengenalan Terhadap Identifikasi Risiko
   Tujuan dari mengenali risiko adalah untuk mengetahui kemungkinan hal-hal yang dapat menyebabkan kerugian, serta agar dapat mengerti bagaimana, di tempat, dan alasan kerugian itu bisa terjadi. Langkah-langkah yang diuraikan harus mengumpulkan data yang diperlukan untuk menghitung risiko.

b. Identifikasi sumber daya-sumber daya
   Sumber daya adalah hal-hal yang memiliki nilai untuk suatu organisasi dan perlu dilindungi. Saat melakukan identifikasi sumber daya, Penting untuk diingat bahwa sistem informasi melibatkan lebih dari sekadar komputer dan program. Identifikasi sumber daya harus dilakukan dengan detail yang akurat agar informasi yang cukup dapat dikumpulkan untuk mengevaluasi risiko. Seberapa rinci informasi yang dikumpulkan saat identifikasi sumber daya akan berdampak pada jumlah keseluruhan informasi yang didapat selama penilaian risiko. Detail ini dapat ditingkatkan dalam proses penilaian risiko selanjutnya.

   Setiap sumber daya harus memiliki seseorang yang ditunjuk sebagai pemilik untuk memastikan adanya rasa tanggung jawab dan akuntabilitas atas sumber daya yang dimaksud. Pemilik sumber daya mungkin tidak memiliki sumber daya itu secara langsung, tetapi mereka berkewajiban dalam hal penciptaan, pengembangan, perawatan, penggunaan, serta menjaga tingkat keamanan yang tepat. Umumnya, pemilik properti adalah orang

yang paling ahli dalam menilai nilai sumber daya untuk organisasi tersebut. Pemeriksaan batas adalah zona di mana sumber daya milik organisasi diidentifikasi untuk dikelola melalui prosedur manajemen risiko terkait keamanan informasi.

c. Identifikasi Ancaman

Ancaman memiliki potensi untuk merusak kekayaan seperti informasi, proses, dan sistem, yang mengakibatkan bahaya bagi lembaga. Ancaman dapat muncul baik dari lingkungan alami maupun dari tindakan manusia, dengan sifat yang bisa terjadi secara sengaja atau tidak. Mengenali asal-usul ancaman yang terjadi secara tidak sengaja dan yang disengaja sangatlah penting. Sumber ancaman bisa berasal dari internal atau eksternal organisasi. Ancaman harus diidentifikasi secara luas dan berdasarkan kategori tertentu (misalnya perbuatan ilegal, kerusakan fisik, atau masalah teknis), serta mengelompokkan ancaman tertentu ke dalam kategori yang sesuai.

Ini mengindikasikan bahwa setiap risiko perlu diperhitungkan, termasuk yang tidak terduga, walaupun jumlah usaha yang diperlukan tetap terbatas. Beberapa risiko bisa berpengaruh pada lebih dari satu sumber daya, dan dalam situasi seperti itu, dampaknya dapat berbeda-beda tergantung pada sumber daya yang terpengaruh.

Informasi untuk mengenali ancaman dan memprediksi kemungkinan terjadinya bisa diperoleh dari pemilik sumber daya atau pengguna, staf sumber daya manusia, manajemen fasilitas, serta ahli keamanan informasi, keamanan fisik, departemen hukum, dan organisasi lain seperti lembaga hukum, institusi meteorologi, perusahaan asuransi, dan pemerintah nasional. Aspek lingkungan dan budaya juga perlu dipertimbangkan saat mengatasi ancaman.

Pengalaman sebelumnya dari kejadian-kejadian serta evaluasi terhadap ancaman yang telah terjadi sebelumnya harus dipertimbangkan dalam analisis yang sedang dilakukan saat ini. Selain itu, akan sangat bermanfaat untuk memeriksa daftar ancaman lain yang mungkin terkait secara khusus dengan suatu organisasi atau bidang usaha guna memperluas daftar ancaman yang umum, jika itu relevan. Kumpulan ancaman dan informasi

statistik dapat diakses melalui berbagai lembaga seperti industri, pemerintah, badan hukum, perusahaan asuransi, dan sebagainya.

Saat menggunakan katalog ancaman atau hasil penilaian ancaman sebelumnya, kita harus ingat bahwa ancaman yang relevan dapat terus berubah, terutama jika lingkungan bisnis atau sistem informasi mengalami perubahan.

d. Identifikasi Kontrol yang ada

Menemukan kontrol yang ada adalah langkah penting untuk menghindari pekerjaan atau pengeluaran yang tidak diperlukan, seperti pada kasus pengulangan kontrol. Selain itu, saat mengidentifikasi kontrol yang sedang berlangsung, perlu dilakukan evaluasi untuk memastikan bahwa kontrol tersebut berfungsi sebagaimana mestinya - Referensi untuk audit SMKI yang sudah ada perlu membatasi waktu yang dihabiskan dalam proses ini. Apabila pengedalian tidak beroperasi dengan baik berdasarkan harapan, situasi ini dapat menimbulkan berbagai permasalahan. Penting untuk memperhatikan keadaan di mana kontrol yang telah dipilih (atau strategi) tidak berfungsi dengan efektif dalam praktik sehingga perlunya kontrol tambahan untuk mengatasi risiko yang sudah diketahui. Dalam konteks SMKI, sesuai dengan standar ISO/IEC 27001, hal ini diperkuat dengan pengukuran tentang seberapa efektif kontrol tersebut. Salah satu metode untuk menilai pengaruh dari kontrol adalah dengan menganalisis seberapa signifikan kontrol tersebut dapat mengurangi kemungkinan ancaman dan kemudahan dalam memanfaatkan celah, atau akibat dari insiden tersebut. Tinjauan oleh manajemen dan laporan audit juga menyajikan wawasan mengenai seberapa efektif kontrol yang ada.

Pengendalian yang telah diatur akan dilaksanakan sesuai dengan strategi manajemen risiko harus dievaluasi dengan pendekatan yang mirip dengan yang telah diterapkan.

Kontrol yang sedang diterapkan sekarang atau yang sedang disusun mungkin terlihat tidak efisien, kurang mencukupi, atau bahkan tidak warranted. Jika terdeteksi bahwa kontrol itu tidak diperlukan atau kurang efektif, maka diperlukan suatu analisis untuk memutuskan apakah kontrol tersebut sebaiknya dihilangkan, diganti dengan alternatif kontrol yang lebih sesuai, atau dipertahankan, contohnya, karena faktor biaya.

Untuk memahami pengendalian yang telah diterapkan atau yang sedang disusun, kegiatan berikut ini dapat sangat bermanfaat :

1) Melakukan analisis terhadap dokumen yang berisi informasi tentang pengendalian, termasuk strategi untuk mengatasi potensi risiko. Ketika prosedur pengelolaan keamanan informasi harus didokumentasikan dengan cermat, dan semua kontrol yang telah diterapkan atau masih dalam tahap perencanaan, beserta status implementasinya, harus dapat diakses;
2) Konfirmasikan dengan orang-orang yang bertanggung jawab atas perlindungan informasi, seperti petugas keamanan data, petugas keamanan sistem informasi, manajer pengembangan, atau manajer operasional, serta para pengguna untuk memastikan bahwa kontrol yang sesuai benar-benar diterapkan pada proses informasi atau sistem informasi yang sedang dinilai.
3) 3) Melakukan evaluasi langsung terhadap kontrol fisik, menilai apa yang telah diterapkan berdasarkan daftar kontrol yang seharusnya ada, serta menilai pelaksanaannya, apakah mereka berfungsi dengan baik dan efektif; atau
4) Melakukan evaluasi terhadap temuan audit internal.

e. Identifikasi Kerentanan

Kerentanan yang bisa dimanfaatkan oleh bahaya untuk merugikan properti atau lembaga perlu dikenali dalam bidang-bidang berikut :

1) Struktur Organisasi
2) Mekanisme dan aturan
3) Praktik manajerial
4) Sumber daya manuasia
5) Lingkungan fisik
6) Pengaturan sistem informasi
7) Perangkat keras, perangkat lunak, atau alat komunikasi
8) Keberlanjutan dari pihak ekternal

Adanya kerentanan itu tidak secara otomatis menunjukkan adanya risiko, karena harus terdapat hal yang muncul ketika mengeksploitasinya.

Kelemahan yang belum teridentifikasi terancam Mungkin tidak memerlukan pemantauan terus-menerus, namun tetap perlu diidentifikasi dan diperhatikan terhadap kemungkinan

perubahan yang dapat terjadi. Penting untuk diingat bahwa jika pengendalian tidak diterapkan secara tepat atau tidak berfungsi sebagaimana mestinya, maka itu dapat menjadi kerentanan. Keberhasilan kontrol bergantung pada konteks di mana ia diterapkan. Sebaliknya, jika terdapat ancaman tanpa adanya kerentanan yang relevan, maka itu mungkin tidak menyampaikan risiko.

Kerentanan dapat terkait dengan sifat-sifat dari sumber daya yang dapat digunakan dengan cara atau untuk maksud yang tidak sesuai dengan tujuan saat sumber daya tersebut dibeli atau diciptakan. Kita perlu memikirkan kerentanan yang timbul dari berbagai faktor, seperti kerentanan yang berasal dari aspek internal atau eksternal sumber daya.

f. Identifikasi Konsekuens

Dampak bisa berupa berkurangnya efektivitas, keadaan operasi yang merugikan, kerugian dalam bisnis, reputasi yang buruk, kerusakan, dan lainnya.

Aktivitas ini mencari kerusakan atau dampak pada organisasi yang bisa muncul dari situasi insiden. Sebuah insiden yang terjadi adalah penjelasan mengenai bahaya yang memanfaatkan kelemahan tertentu atau sekumpulan kelemahan dalam konteks keamanan informasi (merujuk pada ISO/IEC 27002, Klausul 13). Dampak dari insiden akan dinilai berdasarkan standar pengaruh yang telah ditetapkan pada tahap penetapan konteks. Hal ini dapat berpengaruh pada satu atau lebih sumber daya atau elemen dari sumber daya tersebut.

Oleh karena itu, sumber daya mungkin sudah memiliki nilai yang ditentukan, baik dari sudut pandang biaya keuangan maupun dampak yang dapat terjadi pada bisnis jika sumber daya tersebut rusak atau dalam ancaman. Dampak yang terjadi bisa bersifat sementara atau mungkin juga bersifat permanen, seperti yang terjadi pada kasus kerusakan sumber daya.

Pelaksanaan potensi insiden dalam aspek-aspek (namun tidak terbatas pada):

1) Analisa & Durasi Perbaikan.
2) Jam kerja yang terbuang.
3) Kesempatan yang terlewat.
4) Keamanan dan kesehatan.

5) Pengeluaran finansial untuk keahlian tertentu guna memperbaiki kerusakan.
6) Citra reputasi dan itikad baik.

2. Estimasi Risiko

a. Pendekatan untuk Estimasi Risiko

Penilaian risiko bisa dilaksanakan dengan bermacam tipe kedalaman, berdasarkan seberapa signifikan sumber daya itu, seberapa banyak kerentanan yang teridentifikasi, dan apakah ada kejadian sebelumnya yang melibatkan entitas tersebut. Cara untuk menilai risiko dapat bersifat kualitatif, kuantitatif, atau kombinasi dari keduanya, sesuai dengan konteks yang ada. Dalam praktik, sering kali pendekatan kualitatif diambil lebih dulu untuk memperoleh pemahaman umum mengenai tingkat risiko dan untuk mengidentifikasi risiko-risiko utama.

Setelah itu, mungkin perlu dilakukan kajian yang lebih rinci atau analisis angka untuk risiko-risiko yang signifikan, karena umumnya analisis kualitatif lebih sederhana dan lebih hemat biaya daripada analisis kuantitatif. Tipe analisis yang dilakukan harus sejalan dengan standar penilaian risiko yang telah ditetapkan sebagai komponen penentuan konteks.

Penjelasan lebih mendalam mengenai metodologi estimasi akan disampaikan.:

1) Penilaian Kualitaf

Suatu skala untuk menilai seberapa besar kemungkinan suatu dampak yang dapat terjadi, seperti tingkat Rendah, Sedang, dan Tinggi. Salah satu keuntungan dari estimasi kualitatif adalah kemudahan pemahaman bagi semua individu yang terlibat, tetapi kekurangan utamanya adalah bergantung pada preferensi pribadi terkait skala yang diterapkan.

Ukuran ini dimodifikasi agar sesuai dengan konteks tertentu serta penjelasan yang berbeda dapat diterapkan pada variasi berbagai jenis risiko. Penilaian kualitatif dapat diterapkan :

a. Sebagai langkah pertama dalam mengidentifikasi risiko yang memerlukan pengawasan lebih lanjut;
b. Di mana jenis analisis ini tepat untuk pengambilan keputusan;

c. Di mana jika data numerik atau sumber daya yang ada tidak cukup untuk melakukan evaluasi secara kuantitatif.

Analisis kualitatif harus didasarkan pada informasi yang relevan dan data yang ada.

2) Penilaian Kuantitatif
Menggunakan skala berbasis angka, berbeda menggunakan skala deskriptif yang diterapkan dalam penilaian kualitatif, guna menilai dampak serta peluang, dengan memanfaatkan dari beragam sumber. Mutu analisis sangat dipengaruhi oleh sejauh mana angka-angka tersebut akurat dan lengkap serta validitas model yang digunakan. Dalam banyak kasus, estimasi kuantitatif memanfaatkan data dari kejadian yang telah berlalu, memberikan manfaat yang bisa langsung dihubungkan dengan sasaran keamanan informasi dan fokus organisasi. Namun, sebuah kelemahan dari pendekatan ini Adalah terbatasnya data terkait risiko-risiko baru atau kekurangan dalam perlindungan keamanan informasi. Kelemahan dari metode kuantitatif bisa muncul saat data faktual yang telah diverifikasi tidak tersedia, yang dapat menyebabkan persepsi yang salah mengenai nilai dan akurasi penilaian risiko.

Cara efek dan peluang ditunjukkan serta metode untuk menggabungkannya dalam menunjukkan tingkat bahaya dapat bervariasi tergantung pada tipe ancaman dan sasaran dari evaluasi terhadap risiko yang ingin diraih. Keraguan dan perbedaan dalam efek dan peluang perlu diperhatikan dalam analisis dan dijelaskan dengan tegas.

b. Penilaian Konsekuensi
Setelah mengidentifikasi semua sumber daya dalam studi tersebut, penting untuk memperhatikan nilai-nilai yang diberikan kepada sumber daya saat mengevaluasi pengaruhnya.

Pengaruh terhadap usaha dapat dikatakan baik dalam bentuk kualitatif maupun kuantitatif, tetapi memberikan nilai berupa uang secara umum bisa memberikan data tambahan untuk mendukung proses pengambilan keputusan sehingga meningkatkan efektivitasnya.

BAB 8 KEAMANAN PERANGKAT KERAS DAN PERANGKAT

Wahyu Wijaya Widiyanto, M.Kom.

A. PENDAHULUAN

Di era digital, keamanan sistem informasi sangat penting karena kelangsungan operasi bisnis dan organisasi. Keamanan sistem informasi mencakup berbagai isu yang harus meliputi sistem perangkat keras dan perangkat lunak yang dianggap sebagai fondasi dari seluruh ekosistem teknologi informasi (Stallings & Brown, 2018). Keamanan ini melindungi integritas organisasi, ketersediaan, dan kerahasiaan informasi dari berbagai ancaman internal dan eksternal (Whitman & Mattord, 2021).

Dengan meningkatnya adopsi *Cloud Computing*, *Internet of Things* (IoT), dan kecerdasan buatan (AI), ancaman terhadap keamanan sistem perangkat keras dan perangkat lunak semakin menantang. Gangguan operasional, pencurian data, atau bahkan sabotase dapat terkait langsung dengan kerentanan dalam perangkat keras dan dapat mengakibatkan kerugian finansial yang signifikan (Schneier, 2020). Perangkat lunak yang tidak aman, di sisi lain, dapat dengan mudah menjadi target peretas yang menggunakan teknik seperti menyisipkan *Malware*, *Ransomware*, atau mengeksploitasi kerentanan yang diketahui dalam program kode (Anderson, 2021).

Fokus bab ini akan membahas pemahaman komprehensif tentang strategi, teknik, dan praktik terbaik yang paling efektif untuk mengamankan sistem perangkat keras dan perangkat lunak komputer. Diskusi akan mencakup ancaman umum dan cara untuk menguranginya.

B. DEFINISI DAN RUANG LINGKUP KEAMANAN PERANGKAT KERAS DAN PERANGKAT LUNAK

Dalam era digital yang semakin berkembang, keamanan perangkat keras dan perangkat lunak menjadi aspek yang krusial dalam melindungi sistem informasi dari berbagai ancaman siber. Keamanan perangkat keras (*Hardware security*) mengacu pada serangkaian strategi, teknik, dan perangkat yang digunakan untuk melindungi komponen fisik komputer, server, jaringan, dan perangkat lainnya dari akses yang tidak sah,

sabotase, atau manipulasi berbahaya (Stallings, 2020). Perlindungan ini mencakup aspek desain, manufaktur, hingga implementasi perangkat keras di lingkungan operasional.

Sementara itu, keamanan perangkat lunak (*software security*) berfokus pada langkah-langkah yang diterapkan dalam pengembangan, penggunaan, dan pemeliharaan perangkat lunak untuk mencegah eksploitasi kerentanan yang dapat membahayakan sistem (Schneider, 2021). Keamanan ini mencakup praktik pengkodean yang aman (*secure coding*), pembaruan perangkat lunak secara berkala, serta penerapan enkripsi dan autentikasi untuk melindungi data sensitif.

Dalam praktiknya, keamanan perangkat keras dan perangkat lunak saling berkaitan karena keduanya membentuk sistem komputasi yang kompleks. Sebagai contoh, serangan berbasis *Firmware* dapat mengeksploitasi kelemahan perangkat keras, sementara eksploitasi perangkat lunak sering kali berujung pada pengambilalihan kendali atas perangkat keras tertentu (Anderson, 2022).

1. Pentingnya Keamanan dalam Era Digital

Di era digital saat ini, hampir semua aspek kehidupan manusia bergantung pada teknologi informasi, mulai dari komunikasi, perbankan, industri, hingga pemerintahan. Transformasi digital ini membawa manfaat yang luar biasa, tetapi juga meningkatkan risiko serangan siber yang lebih kompleks dan canggih.

Salah satu alasan utama mengapa keamanan perangkat keras dan perangkat lunak sangat penting adalah meningkatnya jumlah dan skala serangan siber. Laporan tahunan *Verizon Data Breach Investigations Report* (2023) menunjukkan bahwa lebih dari 60% serangan siber yang terjadi pada tahun lalu melibatkan eksploitasi perangkat lunak yang rentan, sementara 25% di antaranya menargetkan perangkat keras melalui manipulasi *Firmware* dan serangan berbasis *chip*.

Selain itu, keberadaan *Internet of Things* (IoT) dan perangkat pintar juga memperluas vektor serangan, di mana banyak perangkat tidak memiliki mekanisme keamanan yang memadai (Kumar & Lee, 2021). Tanpa pengamanan yang kuat, peretas dapat mengeksploitasi perangkat ini untuk mengakses jaringan yang lebih luas, mencuri data, atau bahkan mengganggu infrastruktur penting seperti rumah sakit dan sistem transportasi publik.

Keamanan juga penting dalam perspektif hukum dan regulasi. Banyak negara telah mengadopsi kebijakan ketat terkait keamanan siber, seperti GDPR (*General Data Protection Regulation*) di Uni Eropa dan NIST *Cybersecurity Framework* di Amerika Serikat. Regulasi ini mengharuskan perusahaan untuk mengadopsi langkah-langkah keamanan yang ketat dalam melindungi data pengguna dan infrastruktur digital mereka (NIST, 2022).

2. Tren Ancaman dan Perkembangan Teknologi Keamanan Terbaru

Tren ancaman dalam dunia keamanan siber terus berkembang seiring dengan kemajuan teknologi dan strategi yang digunakan oleh penyerang. Beberapa ancaman terbaru yang sering muncul dalam ekosistem perangkat keras dan perangkat lunak meliputi:

a. Serangan *Ransomware* yang Lebih Canggih

Ransomware telah menjadi salah satu bentuk serangan yang paling merugikan dalam beberapa tahun terakhir. Teknik baru seperti *double extortion* memungkinkan peretas tidak hanya mengenkripsi data korban, tetapi juga mengancam untuk membocorkannya ke publik jika tebusan tidak dibayar (Palmer, 2022).

b. Eksploitasi *Zero-Day*

Kerentanan *Zero-Day* merupakan celah keamanan yang belum diketahui oleh vendor perangkat lunak, sehingga tidak memiliki perbaikan resmi pada saat serangan terjadi. Para penyerang dapat menjual atau mengeksploitasi kerentanan ini untuk mendapatkan akses tidak sah ke sistem penting (Schneier, 2023).

c. Serangan *Supply Chain* terhadap Perangkat Keras dan Perangkat Lunak

Salah satu ancaman yang semakin meningkat adalah serangan terhadap rantai pasokan (*Supply Chain attacks*), di mana penyerang menyusup ke dalam perangkat lunak atau perangkat keras selama tahap produksi atau distribusi. Insiden seperti serangan *SolarWinds* pada 2020 menunjukkan betapa besarnya dampak dari eksploitasi jenis ini (Clarke, 2021).

d. Penggunaan Kecerdasan Buatan (AI) dalam Serangan Siber

AI telah digunakan untuk meningkatkan efektivitas serangan siber, seperti dengan mengotomatisasi eksploitasi kerentanan atau memanfaatkan algoritma pembelajaran mesin untuk menghindari deteksi oleh sistem keamanan (Goodfellow et al., 2020).

Sebagai respons terhadap ancaman ini, perkembangan teknologi keamanan juga mengalami peningkatan pesat. Beberapa inovasi terbaru yang berkontribusi dalam memperkuat keamanan perangkat keras dan perangkat lunak antara lain:

a. *Zero Trust Architecture* (ZTA): Model keamanan yang mengasumsikan bahwa tidak ada entitas dalam atau luar jaringan yang dapat dipercaya secara default, sehingga setiap akses harus diautentikasi dan diverifikasi secara ketat (NIST, 2022).
b. *Hardware Security Module* (HSM): Perangkat khusus yang dirancang untuk melindungi dan mengelola kunci kriptografi dengan keamanan tingkat tinggi (Anderson, 2022).
c. Penggunaan AI dalam Keamanan Siber: Implementasi AI untuk mendeteksi pola anomali dalam lalu lintas jaringan dan menganalisis ancaman secara real-time (Goodfellow et al., 2020).
d. Teknik *Homomorphic Encryption*: Sebuah metode enkripsi yang memungkinkan perhitungan dilakukan pada data terenkripsi tanpa harus mendekripsinya terlebih dahulu, meningkatkan keamanan dalam pemrosesan data di lingkungan cloud (Schneider, 2021).

Dengan memahami pentingnya keamanan perangkat keras dan perangkat lunak, serta mengikuti perkembangan teknologi keamanan terbaru, individu dan organisasi dapat meningkatkan kesiapan mereka dalam menghadapi ancaman siber yang semakin kompleks. Ke depan, integrasi strategi keamanan berbasis AI, penggunaan enkripsi yang lebih canggih, serta implementasi kebijakan keamanan yang ketat akan menjadi elemen kunci dalam memastikan ketahanan dunia digital.

C. ANCAMAN TERHADAP PERANGKAT KERAS DAN PERANGKAT LUNAK

Keamanan perangkat keras dan perangkat lunak merupakan fondasi utama dalam menjaga sistem informasi tetap terlindungi dari berbagai ancaman siber. Seiring dengan berkembangnya teknologi, teknik serangan yang digunakan oleh aktor jahat juga semakin canggih dan beragam. Ancaman terhadap perangkat keras dan perangkat lunak dapat datang dari berbagai sumber, baik melalui eksploitasi kelemahan sistem maupun manipulasi langsung terhadap komponen fisik perangkat (Anderson, 2022).

1. Jenis-jenis Ancaman Keamanan Perangkat Keras

Keamanan perangkat keras sering kali diabaikan dibandingkan dengan keamanan perangkat lunak, padahal ancaman terhadap komponen fisik

suatu sistem dapat berdampak luas terhadap keamanan data dan operasional organisasi. Berikut adalah beberapa jenis ancaman utama terhadap perangkat keras:

a. Serangan Fisik (*Physical Tampering*, *Side-Channel Attacks*)

Serangan fisik pada perangkat keras terjadi ketika penyerang mendapatkan akses langsung ke perangkat dan melakukan manipulasi terhadap komponen internalnya. Dua metode serangan yang umum digunakan adalah:

1) *Physical Tampering* (Manipulasi Fisik): Penyerang dapat membuka casing perangkat untuk memodifikasi komponen atau menyisipkan perangkat tambahan yang memungkinkan pencurian data atau pengendalian jarak jauh (Wright, 2021). Salah satu contohnya adalah pemasangan *Hardware* keylogger pada *keyboard* komputer untuk mencatat setiap penekanan tombol pengguna tanpa diketahui.
2) *Side-Channel Attacks*: Teknik ini mengeksploitasi informasi kebocoran dari perangkat keras, seperti konsumsi daya, emisi elektromagnetik, atau waktu eksekusi operasi kriptografi untuk mengekstrak data sensitif (Kocher et al., 2019). Serangan seperti *Power Analysis Attack* dapat digunakan untuk membongkar kunci enkripsi dalam perangkat *smart card* dan *chip* kartu kredit.

b. Serangan Berbasis *Firmware* dan BIOS

Firmware dan BIOS merupakan perangkat lunak tingkat rendah yang mengontrol interaksi perangkat keras dengan sistem operasi. Jika *Firmware* atau BIOS mengalami eksploitasi, penyerang dapat memperoleh akses tingkat tinggi ke sistem yang sulit dideteksi dan diperbaiki (Rutkowska, 2020).

1) *BIOS Rootkit*: *Malware* yang menyerang BIOS untuk menyusupkan kode berbahaya yang bertahan meskipun sistem diinstal ulang. Salah satu kasus terkenal adalah Lojax, *Malware* pertama yang berhasil menanamkan *rootkit* di *Unified Extensible Firmware Interface* (UEFI) untuk mengontrol sistem secara permanen (Kaspersky, 2021).
2) *Firmware Hijacking*: Penyerang dapat mengunggah *Firmware* berbahaya ke perangkat jaringan seperti *router* dan kamera pengawas untuk mengalihkan lalu lintas data atau menciptakan *backdoor* yang memungkinkan akses jarak jauh.

c. *Penetrasi Chip* dan *Backdoor* Perangkat Keras

Penyerang tingkat lanjut dapat menyusupkan *backdoor* dalam perangkat keras selama tahap manufaktur atau distribusi, sehingga menciptakan celah keamanan yang sulit dideteksi. Beberapa contoh ancaman ini meliputi:

1) Implant *Hardware Backdoor*: Perubahan desain pada chip yang memberikan akses tersembunyi kepada pihak tertentu. Penelitian oleh Bloomberg (2018) mengungkap dugaan infiltrasi chip dalam server perusahaan teknologi besar yang memungkinkan mata-mata mendapatkan akses ilegal ke data.
2) *Chip Penetration Attack*: Menggunakan teknik reverse *engineering* untuk membongkar arsitektur mikroprosesor dan mengekstrak kunci kriptografi atau *Firmware* yang digunakan dalam perangkat (Anderson, 2022).

2. Jenis-jenis Ancaman Keamanan Perangkat Lunak

Keamanan perangkat lunak menghadapi berbagai ancaman yang terus berkembang, mulai dari serangan berbasis *Malware* hingga eksploitasi kelemahan dalam kode program. Berikut adalah beberapa jenis ancaman utama terhadap perangkat lunak:

a. *Malware* (Virus, Trojan, *Ransomware*)

Malware adalah perangkat lunak berbahaya yang dirancang untuk merusak, mencuri data, atau mengambil kendali atas sistem. Beberapa jenis *Malware* yang sering digunakan oleh penyerang antara lain:

1) *Virus*: Program yang menyebar dengan menempel pada file atau program lain dan aktif ketika file tersebut dijalankan. *Virus* dapat merusak atau menghapus data serta menginfeksi file lain dalam sistem (Schneier, 2023).
2) *Trojan*: *Malware* yang menyamar sebagai perangkat lunak yang tampak sah, tetapi sebenarnya memiliki fungsi berbahaya, seperti mencuri informasi login atau membuka *backdoor* untuk akses jarak jauh.
3) *Ransomware*: Jenis *Malware* yang mengenkripsi data korban dan meminta tebusan agar data tersebut dapat dipulihkan. Contoh serangan *Ransomware* terkenal adalah WannaCry

yang menginfeksi lebih dari 200.000 komputer di seluruh dunia pada 2017 (Palmer, 2022).

b. Serangan *Zero-Day* dan Eksploitasi Kerentanan

Serangan *Zero-Day* terjadi ketika penyerang mengeksploitasi kerentanan yang belum diketahui oleh vendor perangkat lunak, sehingga belum ada perbaikan resmi. Serangan ini sangat berbahaya karena sering kali digunakan dalam operasi spionase siber atau sabotase sistem kritis.

1) *Stuxnet*: Salah satu serangan *Zero-Day* paling terkenal yang menargetkan fasilitas nuklir Iran dengan mengeksploitasi kerentanan dalam sistem kontrol industri (Zetter, 2019).
2) *Log4Shell* (2021): Kerentanan dalam pustaka Log4j yang memungkinkan penyerang mengeksekusi kode dari jarak jauh dan mengambil kendali atas server yang terdampak (Apache Foundation, 2021).

c. Serangan Berbasis Jaringan (*DDoS, Man-in-the-Middle*)

Serangan terhadap perangkat lunak sering kali melibatkan eksploitasi jaringan untuk mengganggu layanan atau mencuri informasi yang dikirim melalui komunikasi digital. Dua bentuk serangan utama adalah:

1) *Distributed Denial-of-Service* (DDoS): Serangan yang membanjiri server dengan lalu lintas berlebihan sehingga menyebabkan layanan tidak dapat diakses. Serangan ini sering digunakan dalam sabotase bisnis atau sebagai alat pemerasan terhadap perusahaan besar (Mirkovic & Reiher, 2020).
2) *Man-in-the-Middle* (MitM): Penyerang menyusup ke komunikasi antara dua pihak untuk mencuri atau memodifikasi data yang dikirimkan. Serangan ini sering terjadi di jaringan Wi-Fi publik yang tidak terenkripsi (Goodfellow et al., 2020).

BAB 9 KEAMANAN APLIKASI DAN PENGUJIAN PENETRASI

Rezza Anugrah Mutiarawan, M.Kom.

A. PENGANTAR KEAMANAN APLIKASI

1. Pentingnya Keamanan Aplikasi dalam Sistem Informasi

Dalam era digital saat ini, hampir seluruh aktivitas organisasi maupun individu sangat bergantung pada aplikasi. Aplikasi menjadi komponen kunci yang memudahkan berbagai proses bisnis dan interaksi antar pengguna dalam sistem informasi. Dengan semakin meningkatnya ketergantungan tersebut, aspek keamanan aplikasi menjadi faktor yang sangat vital. Keamanan aplikasi tidak hanya melindungi data pribadi pengguna, tetapi juga menjamin kelangsungan operasional bisnis agar tidak terganggu oleh serangan atau gangguan keamanan.

Pentingnya keamanan aplikasi dapat dilihat dari konsekuensi yang mungkin timbul jika terjadi pelanggaran keamanan. Sebuah aplikasi yang rentan dapat menyebabkan kebocoran data sensitif, seperti informasi pribadi, data keuangan, dan rahasia perusahaan. Dampak dari kebocoran data ini sangat signifikan, termasuk kerugian finansial, kerusakan reputasi, hingga risiko hukum yang serius. Oleh karena itu, mengamankan aplikasi merupakan langkah preventif yang harus selalu diutamakan dalam manajemen risiko sistem informasi.

Tidak hanya terbatas pada melindungi data, keamanan aplikasi juga penting untuk mempertahankan kepercayaan pengguna. Sebuah organisasi yang memiliki aplikasi dengan tingkat keamanan rendah akan kehilangan kepercayaan pengguna dan mitra bisnisnya. Kepercayaan adalah aset yang sangat mahal dalam dunia digital, karena sekali hilang maka sangat sulit dan mahal untuk dipulihkan. Oleh sebab itu, implementasi keamanan aplikasi secara tepat dan efektif menjadi sebuah kebutuhan mutlak dalam menjaga kredibilitas dan keberlanjutan organisasi di mata publik.

2. Ancaman Umum Terhadap Aplikasi

Dalam ranah keamanan aplikasi, berbagai jenis ancaman terus berkembang seiring kemajuan teknologi. Salah satu kategori yang sering dijumpai adalah serangan berbasis injeksi, seperti **SQL *Injection*** dan ***Cross-Site Scripting*** **(XSS)**. Kedua jenis serangan ini mengeksploitasi celah dalam sistem aplikasi untuk mendapatkan akses tidak sah, memanipulasi data, atau merusak integritas informasi di dalam basis data. Oleh karena itu, penting bagi para pengembang untuk memahami pola dan karakteristik dari jenis ancaman ini, serta mengambil tindakan pencegahan dan mitigasi yang tepat guna menjaga keamanan serta kestabilan sistem yang digunakan.

Selain injeksi, ancaman lainnya yang sering terjadi adalah serangan terhadap autentikasi, seperti *brute force* dan credential stuffing. Jenis serangan ini mencoba membobol akun pengguna dengan cara menebak kombinasi *username* dan *password* secara sistematis. Apabila berhasil, penyerang dapat mengakses data sensitif pengguna bahkan hingga mengambil alih kendali penuh atas akun-akun penting dalam aplikasi tersebut.

Salah satu bentuk ancaman yang cukup umum terhadap aplikasi adalah serangan ***Denial of Service*** **(DoS)** dan ***Distributed Denial of Service*** **(DDoS)**. Tujuan dari serangan ini adalah untuk membuat sistem tidak mampu merespons permintaan yang sah dari pengguna dengan cara membanjiri server menggunakan lalu lintas data dalam jumlah besar. Akibatnya, layanan dapat terganggu, tidak tersedia, atau bahkan berhenti total. Dampak dari serangan semacam ini dapat sangat merugikan operasional organisasi karena menurunnya ketersediaan sistem dan layanan yang bergantung pada aplikasi tersebut.

Lebih lanjut, ancaman juga datang dari eksploitasi celah keamanan yang diakibatkan oleh kurangnya proses *patching* atau *update* pada aplikasi. Kondisi ini menyebabkan aplikasi tetap memiliki kerentanan yang sudah diketahui oleh penyerang. Banyak serangan siber berhasil karena organisasi mengabaikan pentingnya update keamanan aplikasi, sehingga celah-celah keamanan tetap terbuka dan mudah dieksploitasi.

3. Tujuan dan Prinsip Keamanan Aplikasi

Salah satu tujuan utama dari keamanan aplikasi adalah memastikan terpenuhinya tiga pilar utama dalam perlindungan informasi, yaitu **kerahasiaan** (*confidentiality*), **integritas** (*integrity*), dan **ketersediaan** (*availability*). Kerahasiaan berkaitan dengan pembatasan akses terhadap informasi sensitif, sehingga hanya pihak yang memiliki hak dan otorisasi yang dapat mengaksesnya. Sementara itu, integritas menekankan bahwa data yang tersimpan dalam sistem tidak boleh mengalami perubahan tanpa izin, guna menjaga keakuratan dan keandalannya. Ketersediaan merujuk pada kemampuan sistem atau layanan untuk tetap dapat digunakan oleh pengguna yang berwenang kapan pun dibutuhkan.

Selain tiga tujuan utama tersebut, prinsip dasar keamanan aplikasi juga mencakup autentikasi dan otorisasi. Autentikasi memastikan bahwa setiap pengguna atau sistem yang mengakses aplikasi benar-benar merupakan pihak yang sah. Sedangkan otorisasi menjamin bahwa setiap pengguna atau sistem hanya dapat mengakses informasi atau layanan yang telah sesuai dengan hak akses yang ditetapkan.

Prinsip keamanan aplikasi juga menekankan pada konsep pengelolaan keamanan secara berkelanjutan, yang dikenal dengan istilah security by design. Artinya, keamanan harus diintegrasikan sejak awal proses pengembangan aplikasi, bukan sebagai tambahan setelah aplikasi selesai dikembangkan. Pendekatan ini membantu organisasi untuk mengantisipasi berbagai ancaman lebih dini, sehingga meminimalisir celah keamanan sejak tahap desain aplikasi.

Prinsip penting lainnya adalah *defense-in-depth* atau pertahanan berlapis. Prinsip ini menekankan perlunya berbagai lapisan kontrol keamanan di setiap tingkat aplikasi maupun infrastruktur yang mendukungnya. Dengan pendekatan ini, jika salah satu lapisan keamanan gagal ditembus, maka masih ada lapisan keamanan lainnya yang mampu mencegah atau memperlambat serangan sehingga risiko kerusakan bisa ditekan seminimal mungkin.

Dengan memahami tujuan dan prinsip tersebut, pengelola sistem informasi diharapkan dapat menerapkan strategi yang efektif untuk melindungi aplikasi mereka. Keamanan aplikasi bukan hanya tanggung jawab tim teknis semata, tetapi juga memerlukan kolaborasi seluruh

elemen organisasi untuk menciptakan ekosistem yang aman dan terpercaya bagi pengguna aplikasi maupun pemilik sistem informasi.

B. KERENTANAN UMUM PADA APLIKASI

Seiring bertambahnya kebutuhan pengguna dan meningkatnya kompleksitas fitur dalam aplikasi modern, risiko keamanan juga turut berkembang. Di balik berbagai kemudahan yang ditawarkan, sering kali tersembunyi celah-celah yang berpotensi dieksploitasi oleh aktor jahat. Oleh karena itu, penting bagi organisasi untuk mengenali jenis-jenis kerentanan yang umum terjadi dalam aplikasi, sebagai bagian dari strategi untuk memperkuat sistem keamanan dan mengurangi kemungkinan terjadinya insiden siber yang merugikan.

1. *Injection* (*SQL Injection*, *Command Injection*)

Salah satu kerentanan yang paling umum dan serius adalah serangan ***Injection***, terutama *SQL Injection*. *SQL Injection* terjadi ketika penyerang memanfaatkan celah pada input pengguna yang tidak tervalidasi dengan baik untuk mengeksekusi perintah SQL berbahaya pada basis data. Dampaknya bisa sangat fatal, termasuk bocornya data sensitif, penghapusan atau modifikasi data secara tidak sah, hingga pengambilalihan kontrol penuh atas database dan server.

Selain *SQL Injection*, jenis serangan *Injection* lainnya adalah ***Command Injection***, yang memungkinkan penyerang menjalankan perintah sistem operasi secara langsung melalui input aplikasi yang tidak aman. Dalam serangan ini, penyerang bisa mendapatkan akses ke sistem operasi secara penuh, menghapus file penting, atau bahkan menguasai sistem secara keseluruhan. Oleh karena itu, setiap aplikasi perlu memiliki validasi dan sanitasi input yang kuat untuk mencegah terjadinya jenis serangan ini.

2. *Cross-Site Scription* (XSS)

Kerentanan selanjutnya yang sering ditemukan adalah ***Cross-Site Scripting*** **(XSS)**. XSS terjadi ketika penyerang berhasil menyisipkan skrip jahat (biasanya JavaScript) ke dalam halaman web yang dikunjungi oleh pengguna lain. Akibatnya, skrip tersebut dieksekusi oleh browser korban, yang dapat menyebabkan pencurian data pribadi seperti cookie

sesi, data login, hingga tindakan manipulasi halaman web yang mengarahkan korban ke situs palsu (*phishing*).

Cross-Site Scripting (XSS) terdiri dari tiga kategori utama, yaitu ***Stored* XSS**, ***Reflected* XSS**, dan ***DOM-based* XSS**. Di antara ketiganya, *Stored* XSS dianggap paling berbahaya karena skrip jahat disimpan secara permanen di dalam basis data aplikasi dan akan dieksekusi setiap kali pengguna mengakses halaman yang terinfeksi. Untuk mencegah serangan semacam ini, aplikasi perlu melakukan validasi ketat terhadap setiap *input* pengguna dan menerapkan teknik *encoding output* yang tepat guna menghindari penyisipan skrip berbahaya.

3. *Broken Authentication* dan *Session Management*

Broken Authentication dan *Session Management* termasuk dalam jenis kerentanan serius yang sering ditemukan dalam aplikasi modern. Masalah ini biasanya timbul karena kesalahan dalam implementasi sistem autentikasi dan pengelolaan sesi pengguna. Jika kedua mekanisme tersebut tidak dirancang dengan benar, penyerang dapat mengeksploitasi celah yang ada untuk mencuri identitas, mengambil alih sesi pengguna, atau mengakses akun tanpa melalui proses otorisasi yang sah. Kondisi seperti ini berpotensi mengancam keamanan data dan operasional aplikasi secara keseluruhan.

Contoh kelemahan yang sering ditemukan dalam kategori ini meliputi penggunaan *password default* yang tidak diganti, sesi yang tidak kadaluwarsa setelah *logout*, hingga transmisi informasi autentikasi yang tidak terenkripsi. Oleh karena itu, penting bagi developer untuk memastikan proses autentikasi dan pengelolaan sesi dilakukan secara aman, misalnya dengan menerapkan *Multi-Factor Authentication* (MFA), password hashing yang kuat, pengaturan sesi yang aman, dan mengelola token autentikasi dengan baik.

4. *Security Misconfiguration*

Selanjutnya, ***Security Misconfiguration*** merupakan jenis kerentanan yang terjadi akibat kesalahan konfigurasi dalam aplikasi atau infrastruktur pendukungnya. Misalnya, pengaturan server web yang tidak aman, konfigurasi *default* yang tidak diubah setelah instalasi, atau pengaturan izin akses yang terlalu permisif. *Security misconfiguration* sering kali menjadi pintu masuk utama bagi penyerang untuk

mengeksploitasi sistem karena celah tersebut sangat mudah ditemukan melalui teknik-teknik sederhana seperti scanning otomatis.

Untuk menghindari *security misconfiguration*, pengelola sistem harus memastikan semua konfigurasi aplikasi diperiksa secara rutin, dilakukan hardening terhadap konfigurasi *default*, memperbarui patch keamanan secara reguler, dan memastikan bahwa tidak ada informasi sensitif yang terbuka secara tidak sengaja kepada publik.

5. *Insecure Direct Object References* (IDOR)

Salah satu celah keamanan yang perlu diwaspadai dalam aplikasi modern adalah **IDOR**. Masalah ini muncul ketika sistem secara langsung memberikan akses terhadap data internal seperti file rahasia atau informasi pengguna tanpa melakukan pemeriksaan otorisasi yang cukup. Dalam kondisi seperti ini, penyerang bisa menyalahgunakan parameter URL atau permintaan lainnya untuk mengakses sumber daya yang seharusnya hanya bisa diakses oleh pengguna tertentu.

Misalnya, jika sebuah aplikasi memiliki URL seperti example.com/profile?id=123, penyerang bisa mengganti ID tersebut dengan angka lain, misalnya 124, untuk melihat profil pengguna lain secara ilegal. Solusi untuk mencegah IDOR adalah dengan selalu memvalidasi hak akses pengguna sebelum memberikan akses ke data, menggunakan referensi objek tidak langsung, seperti UUID atau referensi terenkripsi, serta menerapkan pengelolaan hak akses yang ketat.

Mengetahui berbagai jenis kerentanan tersebut, jelas bahwa pengelolaan keamanan aplikasi bukan lagi menjadi tugas yang boleh diabaikan. *Developer*, *administrator*, serta pengelola sistem informasi perlu memahami dan menerapkan prinsip-prinsip *secure coding*, validasi input yang ketat, pengelolaan sesi dan autentikasi yang kuat, konfigurasi yang aman, serta mekanisme otorisasi yang memadai. Upaya ini menjadi kunci penting dalam membangun aplikasi yang aman, handal, dan terlindungi dari berbagai ancaman keamanan yang terus berkembang di dunia digital.

C. METODE PENGAMANAN APLIKASI

Keamanan aplikasi merupakan aspek penting dalam pengelolaan sistem informasi yang harus diintegrasikan sejak tahap awal pengembangan hingga implementasi. Tanpa metode pengamanan yang

BAB 10 KEAMANAN DATA DAN PERLINDUNGAN PRIVASI

Peayogo, S.Kom., M.Kom.

A. PENGERTIAN KONSEP KEAMANAN DATA

Sebagian orang mungkin berpikir CIA adalah badan intelijen Amerika Serikat. Namun, jelas ada sumber lain untuk pernyataan CIA pada sistem keamanan umumnya. Salah satu aturan utama dalam menentukan keamanan jaringan atau informasi adalah kerahasiaan, integritas, dan ketersediaan (CIA, juga dikenal sebagai CIA Triad). Aturan lainnya adalah kerahasiaan, keaslian, ketersediaan, dan manfaat. informasi.

Aturan lainnya (Confidentiality, dikenal *Posession* dengan or *control*, *integrity Authenticity*, *Availability*, dan *Utility*).

Gambar 10. 1. Sigitiga CIA

Sumber : https://www.readynez.com/

Confidentiality, atau rahasia, berarti menjaga kerahasiaan informasi dengan membatasi hak seseorang untuk mengaksesnya, yang biasanya dilakukan dengan menggunakan enkripsi. Data pribadi seperti nama, tanggal lahir, penyakit yang pernah diderita, nomor kartu kredit, nama ibu kandung, dan sebagainya harus aman, serta data milik organisasi atau perusahaan. Ada saat-saat ketika kerahasiaan sejalan dengan *privacy*. Aspek ini dimaksudkan untuk:

a. Membatasi pengaksesan terhadap informasi sesuai tingkat kerahasiaannya
b. Melindungi data / informasi agar tidak diketahui oleh pihak yang tidak berwenangan

Integrity atau Integritas, atau keaslian, berarti menunjukkan bahwa data atau informasi yang dimiliki tetap asli dan tidak berubah tanpa izin pemiliknya. Integritas mengacu pada seberapa dapat dipercaya suatu informasi. Dua mekanisme pengamanan integritas adalah mekanisme priventif dan detektif. Mekanisme priventif mengontrol akses untuk mencegah data diubah, dan mekanisme detektif mengidentifikasi perubahan yang dilakukan oleh orang lain. Aspek ini dimaksudkan untuk:

a. Menjaga agar data dan program tidak diubah tanpa izin oleh pihak yang tidak berwenang
b. Memberikan jaminan bahwa informasi dan data yang ada pada sumber daya dapat dipercaya.

Availability (ketersediaan) berhubungan dengan ketersediaan informasi ketika dibutuhkan. Artinya, informasi harus selalu tersedia saat dibutuhkan oleh user, dan dapat dengan cepat diakses. Serangan yang paling lazim untuk jenis keamanan ini adalah *Distributed Denial of Service* (DDoS). Serangan ini memenuhi resource atau sumber informasi (*server*) dengan permintaan yang banyak atau permintaan diluar perkiraan sehingga server tidak dapat melayani permintaan lain atau bahkan *down*.

B. ANCAMAN KEAMANAN

Ancaman yang sering dihadapi oleh masalah keamanan dapat dikategorikan dalam salah satu kategori berikut:

1) Ancaman dari manusia dapat berupa:

a. *Hacking*, *cracking*, atau sesiapa saja yang berusaha atau telah mengakses sistem tanpa izin pihak yang berwenang. Tujuannya dapat berupa pencurian perusakan.
b. Memasukkan program ilegal seperti *virus*, *worm*, atau *malicious software*
c. Kemampuan user yang terbatas untuk menggunakan dan memelihara sistem, serta kurangnya pengetahuan tentang keamanan sistem.

2) Kesalahan perangkat keras dapat berupa ancaman berikut:

a. Tidak stabilnya pasokan listrik yang dapat menyebabkan kerusakan pada perangkat
b. Korsleting listrik, yang dapat menghentikan proses sistem atau bahkan menyebabkan kerusakan sistem.
c. Segala jenis gangguan fisik yang memengaruhi perangkat baik secara langsung maupun tak langsung

3) Kegagalan perangkat lunak dapat berupa:

a. Kesalahan sistem operasi;
b. kesalahan saat meng-update program;
c. atau uji coba program yang tidak memadai, yang menyebabkan *error* perangkat lunak.

4) Ancaman alam,

Ancaman alam itu seperti banjir, adalah tidak dapat dicegah. Tanah runtuh atau longsor,kebakaran, dan sebagainya

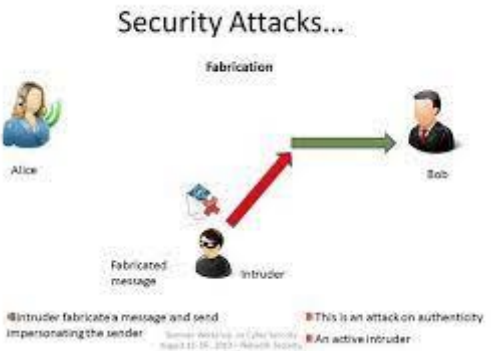
C. MODEL SERANGAN KEAMANAN

Ada beberapa model serangan terhadap keamanan (Stalling, 1995) diantaranya adalah:

1. **Interruption.**
   Yang dimaksud dengan serangan ini ditujukan untuk aspek ketersediaan (*availability*), sehingga ini yang menjadikan

sistem tidak tersedia atau rusak. Adapun contoh serangan ini yaitu *denial of service attack*

2. **Interception.**
   Yaitu serangan berupa pihak yang tidak memiliki wewenang berhasil mengakses data / informasi. Misalnya dengan melakukan penyadapan (*wiretapping*).
3. **Modification**.
   Yaitu berupa Serangan pihak yang tidak memiliki wewenang berhasil memodifikasi aset atau data/informasi yang dimiliki organisasi/perusahaan.
4. **Fabrication**.
   Apa yang dimaksud dengan serangan fabrication? Adapun Serangan ini berupa pihak yang tidak berwenang menjadi seolah-olah pengguna sah dan mengirimkan pesan palsu kedalam sistem. Menyerang aspek autentikasi. Contoh dengan memasukkan pesan-pesan palsu seperti e-mail palsu ke jaringan komputer.



Gambar 10. 2. Security Attack

Sumber : https://eng.libretexts.org/

D. MEMAHAMI REKAYASA SOSIAL

Salah satu perusahaan antivirus terbesar, yaitu Norton menyatakan bahwa rekayasa sosial, juga dikenal sebagai social engineering, adalah tindakan menipu seseorang untuk

mengungkapkan informasi atau mengambil tindakan melalui teknologi.
Mengambil keuntungan dari kecenderungan alami dan perasaan korban adalah tujuan utamanya. Serangan rakayasa sosial terdiri dari enam kategori berikut:

1. **Baiting**: Jenis rekayasa sosial ini bergantung pada korban untuk menerima atau menolak "umpan". *Concord*: Seorang penipu mungkin meninggalkan stik USB yang penuh dengan malware untuk target melihatnya, yang dilabeli dengan kata-kata menarik seperti "rahasia" atau "bonus". Target yang mengambil umpan akan mengambil stik USB dan menghubungkannya ke komputer untuk melihat apa yang ada di dalamnya. *Malware* akan secara otomatis menginjeksi dirinya ke komputer setelah itu.
2. **Phising**: Ini adalah metode terkenal untuk mendapatkan informasi dari korban. Pelaku biasanya mengirimkan email atau teks ke orang yang dimaksud untuk mendapatkan informasi. yang dapat membantu tindakan kriminal yang lebih besar.
3. **Hacking** email dan spam kontak Beberapa pelaku mencoba memerintahkan akun email dan daftar kontak akun spam, contohnya. Kita mungkin tidak akan berpikir dua kali untuk membuka email dengan subjek "Lihat situs ini" jika teman kita mengirimkannya. Pelaku dapat membuat orang-orang di daftar kontak percaya bahwa mereka menerima email dari seseorang yang mereka kenal dengan mengambil akun email mereka. Tujuannya adalah menyebarkan *malware* dan menipu orang dari data mereka.
4. **Preposisi** Pelaku menipu korban dengan alasan yang menarik. Katakanlah Anda menerima email, menyebut Anda sebagai penerima wasiat. Email meminta informasi pribadi Anda untuk membuktikan bahwa Anda adalah penerima sebenarnya dan untuk mempercepat transfer warisan Anda. Sebaliknya, Anda berisiko memberi penipu kemampuan untuk tidak menambahkan ke rekening

bank Anda, tetapi untuk mengakses dan menarik dana Anda.

5. **Quid pro quo**: jenis penipuan ini memerlukan perjanjian tertentu. Pelaku mencoba mengorbankan 26 orang. yakin bahwa transaksi itu adil. Contoh *Scammer* dapat memanggil target, berpura-pura menjadi teknisi dukungan TI. Korban mungkin menyerahkan kredensial masuk ke komputer mereka, mengira mereka menerima dukungan teknis sebagai imbalan. Sebagai gantinya, *scammer* sekarang dapat mengendalikan komputer korban, memuatnya dengan *malware* atau, mungkin, mencuri informasi pribadi dari komputer untuk melakukan pencurian identitas.
6. **Vishing**. *Vishing* adalah versi suara phishing. "V" adalah singkatan dari *voice*, tetapi sebaliknya, upaya penipuannya sama. Penjahat menggunakan telepon untuk menipu korban agar menyerahkan informasi yang berharga. Contoh Seorang penjahat mungkin memanggil seorang karyawan, menyamar sebagai rekan kerja. Penjahat mungkin menang atas korban untuk memberikan kredensial masuk atau informasi lain yang dapat digunakan untuk menargetkan perusahaan atau karyawannya.

E. PRINSIP-PRINSIP KEAMANAN

Ada 7 prinsip dasar pada keamanan sistem, menurut (Stoneburner, dkk., 2004) adalah sebagai berikut:

1. **Prinsip 1. Menetapkan kebijakan (*policy*) keamanan yang baik sebagai dasar untuk desain sistem**.
   Pada Saat membangun sistem informasi, kebijakan keamanan sangat penting. Dimulai dengan komitmen organisasi terhadap keamanan Informasi disajikan dalam bentuk pernyataan kebijakan umum. Selanjutnya, kebijakan ini diterapkan pada setiap aspek desain sistem atau solusi keamanan saat terjadi insiden. Dokumen ini harus menjelaskan sasaran keamanan dan mencakup prosedur, standar, dan protokol arsitektur keamanan.

2. **Prinsip 2. Pertimbangkan keamanan sebagai bagian penting dari keseluruhan sistem**. sistem informasi. Setelah sistem dikembangkan, keamanan akan sulit dan mahal untuk diterapkan, sehingga perlu diintegrasikan sepenuhnya ke dalam proses siklus sistem.
3. **Prinsip 3. Jelaskan batas keamanan fisik dan logis yang ditetapkan dalam dokumen kebijakan keamanan**.
   Teknologi informasi terdiri dari bagian fisik dan bagian non-fisik. logika Ada batasan yang jelas di kedua bidang ini. Jika Anda tahu apa yang harus dilindungi dari faktor eksternal, Anda dapat merencanakan tindakan perlindungan yang dibutuhkan. Oleh karena itu, batas keamanan harus dipikirkan dan disertakan dalam kebijakan keamanan dan dokumentasi sistem.
4. **Prinsip 4 Pastikan pengembang dilatih tentang pengembangan keamanan perangkat lunak**. pengembangan perangkat lunak yang aman mencakup perancangan, pengembangan, kontrol konfigurasi, integrasi, dan pengujian.
5. **Prinsip 5. Kurangi resiko**. Resiko adalah gabungan dari kemungkinan bahaya tertentu (baik secara sengaja atau tidak). membuat kerentanan sistem secara tidak sengaja) dan konsekuensi negatif untuk operasi organisasi, aset, atau individu yang terlibat jika hal ini terjadi. Harus diakui bahwa, dari segi biaya, analisis resiko efektif. Untuk setiap kontrol yang diusulkan, analisis biaya kemungkinan insiden keamanan harus dilakukan. Tujuannya adalah untuk meningkatkan kemampuan perusahaan dengan mengurangi resiko bisnis ke tingkat yang wajar.
6. **Prinsip 6. Asumsikan bahwa sistem eksternal tidak aman**. Sistem eksternal umumnya seharusnya dianggap tidak aman. Akibatnya, pengembang harus merancang fitur keamanan dengan cara ini untuk mengatasi masalah ini.

7. **Prinsip 7. Menemukan potensi hubungan antara pengurakan resiko dan peningkatan atau penurunan biaya dalam aspek lain efektivitas operasional**. Prinsip nomor 4 terkait dengan prinsip ini. Perancang sistem harus menemukan dan menangani semua kebutuhan operasional untuk memenuhi persyaratan keamanan. Mengubah tujuan keamanan dapat meningkatkan biaya, tetapi menemukan dan memperbaiki masalah keamanan secepat mungkin akan menghasilkan sistem yang lebih efisien.

BAB 11 SISTEM MANAJEMEN KEAMANAN INFORMASI

Richky Mukin , MCT, MM

A. PENDAHULUAN

Di era digital, perlindungan data pribadi telah muncul sebagai perhatian penting bagi individu, organisasi, dan pemerintah di seluruh dunia. Karena Indonesia mengalami digitalisasi yang cepat di berbagai sektor, kerahasiaan data pribadi menghadapi tantangan yang belum pernah terjadi sebelumnya.

Integrasi Sistem Manajemen Keamanan Informasi (SMKI) telah menjadi penting dalam membangun kerangka kerja yang kuat untuk melindungi informasi sensitif. Makalah ini mengkaji penerapan Sistem Manajemen Keamanan Informasi di Indonesia yang secara khusus berfokus pada perlindungan kerahasiaan data pribadi. Pembahasan akan menganalisis dampak SMKI terhadap perlindungan data pribadi di Indonesia, mengidentifikasi potensi risiko dan ancaman terhadap kerahasiaan data dalam konteks Indonesia, dan mengeksplorasi tantangan unik yang dihadapi saat menerapkan SMKI di negara ini.

Dengan Undang-Undang Perlindungan Data Pribadi Indonesia yang baru-baru ini disahkan pada tahun 2022, memahami persimpangan antara kerangka kerja regulasi dan implementasi teknis menjadi semakin relevan. Analisis ini bertujuan untuk berkontribusi pada wacana yang berkembang tentang praktik keamanan informasi di negara berkembang, dengan perhatian khusus pada lanskap teknologi dan pertimbangan budaya Indonesia yang memengaruhi pendekatan perlindungan data.

B. DAMPAK PENERAPAN SMKI TERHADAP PERLINDUNGAN DATA PRIBADI

Penerapan Sistem Manajemen Keamanan Informasi telah menunjukkan dampak yang mendalam terhadap perlindungan data pribadi di Indonesia, mengubah cara organisasi mendekati perlindungan data di berbagai dimensi. Untuk memahami dampak ini secara

komprehensif, penting untuk mengkaji evolusi adopsi SMKI di Indonesia dan hubungannya dengan hasil perlindungan data.

Secara historis, pendekatan Indonesia terhadap keamanan informasi telah terfragmentasi, dengan praktik yang tidak konsisten di berbagai sektor. Pengenalan kerangka SMKI yang terstandarisasi, khususnya ISO/IEC 27001, telah menyediakan metodologi terstruktur bagi organisasi untuk mengidentifikasi, menilai, dan mengurangi risiko terhadap aset informasi, termasuk data pribadi. Penelitian oleh Nasution dan Bahsoan (2019) menunjukkan bahwa organisasi yang telah menerapkan SMKI yang sesuai dengan ISO 27001 telah mengalami penurunan insiden pelanggaran data sebesar 43% dibandingkan dengan organisasi yang tidak memiliki sistem formal.

Salah satu dampak signifikan dari penerapan SMKI adalah pengembangan skema klasifikasi data yang komprehensif dalam organisasi-organisasi di Indonesia. Kerangka klasifikasi ini memungkinkan identifikasi data pribadi sensitif yang memerlukan langkah-langkah perlindungan yang lebih baik. Misalnya, PT Telekomunikasi Indonesia (Telkom), perusahaan telekomunikasi terbesar di negara ini, menerapkan SMKI yang mengkategorikan data pelanggan berdasarkan tingkat sensitivitas, dan menerapkan kontrol keamanan yang bertahap. Pendekatan ini menghasilkan alokasi sumber daya yang lebih baik dan perlindungan yang lebih efektif untuk informasi pribadi berisiko tinggi.

SMKI juga telah menumbuhkan budaya kesadaran keamanan dalam organisasi-organisasi di Indonesia. Sebuah studi oleh Tim Respons Insiden Keamanan Indonesia untuk Infrastruktur Internet (ID-SIRTII) menemukan bahwa perusahaan-perusahaan dengan SMKI yang mapan melakukan pelatihan kesadaran keamanan 2,7 kali lebih sering daripada yang tidak memiliki sistem tersebut. Pergeseran budaya ini berdampak khususnya di negara yang tingkat literasi teknologinya sangat bervariasi di berbagai segmen demografi. Peningkatan kesadaran di antara staf yang menangani data pribadi telah mengurangi insiden rekayasa sosial dan pelanggaran terkait kesalahan manusia sekitar 31% dalam organisasi-organisasi yang mematuhi SMKI.

Infrastruktur teknis untuk melindungi data pribadi juga telah diperkuat melalui penerapan SMKI. Organisasi semakin mengadopsi enkripsi, kontrol akses, dan saluran komunikasi aman sebagai praktik standar. Menurut Forum Keamanan Siber Indonesia (ICSF), tingkat penerapan enkripsi untuk data pribadi yang tersimpan meningkat dari

27% menjadi 64% antara tahun 2018 dan 2022 di antara organisasi yang mengadopsi kerangka kerja SMKI. Peningkatan teknis ini secara langsung meningkatkan perlindungan kerahasiaan untuk data pribadi.

Dampak penting lainnya adalah terbentuknya kemampuan respons insiden. Kerangka kerja SMKI mengamanatkan pengembangan prosedur untuk mendeteksi, melaporkan, dan menanggapi insiden keamanan. Otoritas Jasa Keuangan (OJK) melaporkan bahwa lembaga keuangan dengan SMKI yang matang merespons pelanggaran data 76% lebih cepat daripada lembaga yang tidak memiliki sistem tersebut, sehingga secara signifikan mengurangi waktu paparan dan potensi kerusakan pada kerahasiaan data pribadi.

Hubungan antara penerapan SMKI dan kepatuhan regulasi juga semakin erat. Dengan disahkannya Undang-Undang Perlindungan Data Pribadi Indonesia pada tahun 2022, organisasi dengan kerangka SMKI yang mapan telah menemukan posisi yang lebih baik untuk memenuhi persyaratan kepatuhan. Sebuah survei yang dilakukan oleh Deloitte Indonesia menemukan bahwa perusahaan dengan SMKI yang sudah ada sebelumnya membutuhkan waktu dan sumber daya 47% lebih sedikit untuk mencapai kepatuhan terhadap undang-undang baru dibandingkan dengan mereka yang memulai dari awal.

Dampak ekonomi penerapan SMKI terhadap perlindungan data tidak boleh diabaikan. Meskipun biaya penerapan awal cukup besar, berbagai organisasi telah melaporkan manfaat ekonomi jangka panjang. Bank Central Asia (BCA), bank swasta terbesar di Indonesia, mendokumentasikan penurunan biaya sebesar 28% yang terkait dengan insiden keamanan setelah penerapan SMKI yang komprehensif, yang menunjukkan kelayakan ekonomi dari investasi dalam kerangka kerja perlindungan data.

Namun, dampak SMKI belum merata di semua sektor di Indonesia. Instansi pemerintah dan perusahaan besar telah menunjukkan peningkatan yang lebih signifikan dalam perlindungan data pribadi dibandingkan usaha kecil dan menengah (UKM), yang sering kali kekurangan sumber daya untuk penerapan SMKI secara komprehensif. Kesenjangan ini menimbulkan kerentanan yang mengkhawatirkan dalam lanskap perlindungan data nasional, karena UKM secara kolektif memproses sejumlah besar data pribadi.

Selain itu, dampak SMKI pada arus data lintas batas perlu mendapat perhatian. Seiring dengan meningkatnya partisipasi Indonesia dalam

ekonomi digital global, SMKI telah memfasilitasi peningkatan kepatuhan terhadap standar perlindungan data internasional. Hal ini memungkinkan bisnis Indonesia untuk terlibat lebih percaya diri dalam transfer data internasional sambil mempertahankan perlindungan yang tepat untuk informasi pribadi, sehingga meningkatkan posisi negara di pasar digital global.

Lanskap digital Indonesia menghadirkan serangkaian risiko dan ancaman yang kompleks terhadap kerahasiaan data pribadi, yang dibentuk oleh faktor teknologi, sosial politik, dan budaya yang unik bagi negara tersebut. Memahami ancaman ini sangat penting untuk mengembangkan Sistem Manajemen Keamanan Informasi yang efektif yang mengatasi tantangan khusus Indonesia.

Serangan siber merupakan salah satu ancaman paling menonjol terhadap kerahasiaan data pribadi di Indonesia. Negara ini telah mengalami peningkatan dramatis dalam ancaman siber yang canggih, dengan Badan Siber dan Sandi Negara (BSSN) melaporkan lebih dari 1,4 miliar serangan siber pada tahun 2021 saja, meningkat 1.000% dari tahun 2018. Serangan ini semakin menargetkan repositori data pribadi, dengan lembaga keuangan dan platform e-commerce sebagai target utama. Pada tahun 2022, beberapa pelanggaran data besar memengaruhi jutaan orang Indonesia, termasuk terungkapnya 279 juta catatan warga negara dari basis data pemerintah, yang menyoroti skala lanskap ancaman.

Ancaman internal merupakan faktor risiko signifikan lainnya. Norma budaya di Indonesia, yang menekankan hubungan komunal dan keharmonisan sosial, terkadang dapat bertentangan dengan prinsip kerahasiaan data. Penelitian oleh Indonesia Institute for Corporate Governance menemukan bahwa karyawan di organisasi Indonesia 23% lebih mungkin untuk berbagi informasi sensitif dengan kolega di luar protokol akses formal dibandingkan dengan rata-rata global. Dinamika budaya ini menciptakan tantangan unik untuk implementasi SMKI, yang memerlukan adaptasi kerangka kerja standar untuk mengatasi pola perilaku ini.

Kerentanan infrastruktur digital Indonesia memperparah ancaman ini. Meskipun ada peningkatan signifikan dalam beberapa tahun terakhir, perkembangan teknologi yang tidak konsisten di seluruh nusantara menyebabkan banyak sistem yang memproses data pribadi beroperasi pada perangkat lunak dan perangkat keras yang sudah ketinggalan zaman. Survei tahun 2021 oleh Asosiasi Penyedia Layanan Internet Indonesia mengungkapkan bahwa 41% organisasi yang menangani data

pribadi menggunakan sistem operasi yang tidak lagi menerima pembaruan keamanan. Kerentanan teknis ini menyediakan vektor serangan bagi pelaku ancaman yang mencari akses tidak sah ke informasi pribadi.

Kesenjangan regulasi, meskipun ada kemajuan legislatif baru-baru ini, terus menimbulkan risiko terhadap kerahasiaan data pribadi. Meskipun Undang-Undang Perlindungan Data Pribadi 2022 merupakan langkah maju yang signifikan, mekanisme implementasi dan kemampuan penegakan hukum masih dalam tahap pengembangan. Selama masa transisi ini, ketidakpastian regulasi menciptakan lingkungan di mana standar perlindungan data dapat diterapkan secara tidak konsisten. Selain itu, fragmentasi pengawasan regulasi di berbagai lembaga pemerintah menciptakan tantangan koordinasi yang dapat dimanfaatkan oleh pelaku kejahatan.

Bencana alam menimbulkan risiko unik terhadap kerahasiaan data di Indonesia yang sering kali diabaikan dalam kerangka kerja SMKI standar. Sebagai negara yang terletak di Cincin Api Pasifik, Indonesia sering mengalami gempa bumi, letusan gunung berapi, dan tsunami yang dapat membahayakan kontrol keamanan fisik yang melindungi fasilitas penyimpanan data. Selama operasi pemulihan bencana, prosedur darurat dapat melewati protokol keamanan normal, yang berpotensi mengekspos data pribadi. Sebuah studi oleh Badan Nasional Penanggulangan Bencana (BNPB) menemukan bahwa 37% organisasi tidak memiliki protokol khusus untuk menjaga kerahasiaan data selama bencana alam.

Serangan rekayasa sosial sangat efektif di Indonesia karena faktor budaya dan tingkat literasi digital yang berbeda-beda. Kampanye phishing sering kali mengeksploitasi tingkat kepercayaan yang tinggi terhadap otoritas dan pemimpin masyarakat yang menjadi ciri khas masyarakat Indonesia. Kementerian Komunikasi dan Teknologi Informasi melaporkan peningkatan serangan rekayasa sosial sebesar 78% antara tahun 2020 dan 2022, dengan banyak yang menargetkan data pribadi melalui peniruan identitas pejabat pemerintah atau pemimpin agama.

Kerentanan aplikasi seluler merupakan vektor ancaman signifikan lainnya. Indonesia memiliki salah satu tingkat penggunaan internet seluler tertinggi di dunia, dengan lebih dari 73% akses internet terjadi melalui telepon pintar. Banyak aplikasi yang dikembangkan secara lokal tidak memiliki pengujian keamanan yang kuat dan mengandung kerentanan yang dapat mengekspos data pribadi. Penelitian oleh Tim

Tanggap Darurat Komputer Indonesia mengidentifikasi kelemahan keamanan di 67% dari 100 aplikasi seluler teratas di Indonesia, dengan 43% memiliki kerentanan yang dapat menyebabkan akses tidak sah ke data pribadi.

Risiko pihak ketiga semakin signifikan seiring dengan semakin banyaknya organisasi di Indonesia yang mengadopsi transformasi digital melalui kemitraan dengan penyedia teknologi. Rantai pasokan yang diperluas sering kali mencakup entitas dengan berbagai tingkat kematangan keamanan. Sebuah studi tahun 2021 oleh PwC Indonesia menemukan bahwa hanya 24% organisasi yang menilai praktik keamanan informasi vendor dan mitra mereka secara menyeluruh, sehingga menciptakan potensi titik buta dalam kerangka perlindungan data mereka.

Komersialisasi data yang tidak sah merupakan ancaman yang terus meningkat seiring dengan meningkatnya nilai ekonomi data pribadi. Telah terjadi banyak kasus penjualan basis data yang berisi informasi pribadi warga Indonesia di pasar gelap. Dalam beberapa kasus, hal ini melibatkan karyawan organisasi yang sah yang mengekstraksi dan menjual data untuk keuntungan pribadi. Unit Kejahatan Siber Kepolisian Indonesia melaporkan peningkatan 132% dalam kasus yang melibatkan perdagangan data pribadi ilegal antara tahun 2019 dan 2022.

Terakhir, kesadaran keamanan yang terbatas di antara masyarakat umum menciptakan kerentanan yang signifikan. Meskipun tingkat adopsi media sosial di Indonesia tinggi, pemahaman tentang konsep privasi digital masih terbatas di antara banyak pengguna. Sebuah survei nasional yang dilakukan oleh Yayasan Konsumen Indonesia menemukan bahwa 76% pengguna internet jarang membaca kebijakan privasi sebelum membagikan informasi pribadi, dan 82% menggunakan kata sandi yang sama di beberapa layanan. Kurangnya kesadaran ini secara signifikan melemahkan upaya kerahasiaan data pribadi terlepas dari langkah-langkah keamanan organisasi.

C. POTENSI RISIKO DAN ANCAMAN TERHADAP KERAHASIAAN DATA PRIBADI DI INDONESIA

Lanskap digital Indonesia menghadirkan serangkaian risiko dan ancaman yang kompleks terhadap kerahasiaan data pribadi, yang dibentuk oleh faktor teknologi, sosial politik, dan budaya yang unik bagi negara tersebut. Memahami ancaman ini sangat penting untuk mengembangkan Sistem Manajemen Keamanan Informasi yang efektif yang mengatasi tantangan khusus Indonesia.

Serangan siber merupakan salah satu ancaman paling menonjol terhadap kerahasiaan data pribadi di Indonesia. Negara ini telah mengalami peningkatan dramatis dalam ancaman siber yang canggih, dengan Badan Siber dan Sandi Negara (BSSN) melaporkan lebih dari 1,4 miliar serangan siber pada tahun 2021 saja, meningkat 1.000% dari tahun 2018. Serangan ini semakin menargetkan repositori data pribadi, dengan lembaga keuangan dan platform e-commerce sebagai target utama. Pada tahun 2022, beberapa pelanggaran data besar memengaruhi jutaan orang Indonesia, termasuk terungkapnya 279 juta catatan warga negara dari basis data pemerintah, yang menyoroti skala lanskap ancaman.

Ancaman internal merupakan faktor risiko signifikan lainnya. Norma budaya di Indonesia, yang menekankan hubungan komunal dan keharmonisan sosial, terkadang dapat bertentangan dengan prinsip kerahasiaan data. Penelitian oleh Indonesia Institute for Corporate Governance menemukan bahwa karyawan di organisasi Indonesia 23% lebih mungkin untuk berbagi informasi sensitif dengan kolega di luar protokol akses formal dibandingkan dengan rata-rata global. Dinamika budaya ini menciptakan tantangan unik untuk implementasi SMKI, yang memerlukan adaptasi kerangka kerja standar untuk mengatasi pola perilaku ini.

Kerentanan infrastruktur digital Indonesia memperparah ancaman ini. Meskipun ada peningkatan signifikan dalam beberapa tahun terakhir, perkembangan teknologi yang tidak konsisten di seluruh nusantara menyebabkan banyak sistem yang memproses data pribadi beroperasi pada perangkat lunak dan perangkat keras yang sudah ketinggalan zaman. Survei tahun 2021 oleh Asosiasi Penyedia Layanan Internet Indonesia mengungkapkan bahwa 41% organisasi yang menangani data pribadi menggunakan sistem operasi yang tidak lagi menerima pembaruan keamanan. Kerentanan teknis ini menyediakan vektor serangan bagi pelaku ancaman yang mencari akses tidak sah ke informasi pribadi.

BAB 12 KEAMANAN CLOUD COMPUTING

Tri Yusnanto, M.Kom.

A. PENGERTIAN KEAMANAN CLOUD COMPUTING

Cloud computing telah menjadi salah satu inovasi teknologi paling revolusioner dalam beberapa dekade terakhir. Dengan kemampuan untuk menyediakan sumber daya komputasi melalui internet tanpa memerlukan infrastruktur fisik langsung, cloud computing menawarkan fleksibilitas, efisiensi biaya, dan skalabilitas yang luar biasa. Internet adalah jaringan elektronik global yang menggunakan teknologi satelit untuk menghubungkan komputer di seluruh dunia(Yusnanto et al., 2025). Saat ini, Internet telah menjadi sarana penting bagi masyarakat umum di banyak negara.

Namun, popularitasnya juga membawa tantangan besar terkait keamanan. Keamanan cloud computing adalah upaya sistematis untuk melindungi data, aplikasi, dan infrastruktur yang dihosting di cloud dari ancaman siber, pelanggaran privasi, dan kerugian lainnya.

Keamanan ini bukan hanya tanggung jawab penyedia layanan cloud (seperti Amazon Web Services, Microsoft Azure, atau Google Cloud), tetapi juga tanggung jawab bersama antara penyedia dan pengguna akhir. Model ini dikenal sebagai Shared Responsibility Model , di mana penyedia bertanggung jawab atas keamanan infrastruktur fisik dan jaringan, sementara pengguna bertanggung jawab atas keamanan data dan aplikasi mereka sendiri.

Keamanan cloud computing merujuk pada serangkaian praktik, teknologi, dan kebijakan yang dirancang untuk melindungi data, aplikasi, infrastruktur, dan layanan yang dihosting di lingkungan cloud. Cloud computing sendiri adalah model pengiriman layanan komputasi berbasis internet, yang memungkinkan pengguna mengakses sumber daya seperti server, penyimpanan, database, jaringan, hingga perangkat lunak tanpa harus memiliki infrastruktur fisik secara langsung. Dalam konteks ini, keamanan cloud menjadi aspek krusial karena mencakup perlindungan

terhadap ancaman siber, akses tidak sah, kehilangan data, dan pelanggaran privasi.

Data yang disimpan di cloud sering mengandung informasi sensitif dan berharga, termasuk data pribadi, data bisnis, dan data pelanggan. Konsumen yang menggunakan layanan cloud harus mempercayai penyedia layanan untuk menjaga kerahasiaan, integritas, dan ketersediaan data mereka. Resiko yang terkait dengan penggunaan cloud computing ini termasuk kemungkinan pencurian data dan tindakan cybercrime atau lainnya yang dapat merugikan pengguna. Hacker akan melakukan serangan ke sistem yang paling mungkin menyimpan data senistif pengguna cloud computing. Oleh karena itu, memahami risiko keamanan data saat menggunakan cloud computing sangat penting untuk memahami keamanan cloud computing. Pengguna dapat meningkatkan keamanan data mereka dalam cloud computing dan melindunginya dari ancaman keamanan dengan menggunakan praktik keamanan yang tepat.

Gambar 12. 1. Ilustrasi keamann Cloud computing(www.freepik.com)

Cloud computing menawarkan banyak manfaat, termasuk fleksibilitas, skalabilitas, efisiensi biaya, dan kemudahan akses. Namun, karakteristiknya yang bersifat terdistribusi dan didasarkan pada internet juga membawa risiko tersendiri. Oleh karena itu, keamanan cloud bertujuan untuk memastikan bahwa data dan aplikasi yang disimpan di cloud tetap aman dari berbagai ancaman, baik yang berasal dari luar maupun dalam organisasi.

B. FUNGSI KEAMANAN CLOUD COMPUTING

Fungsi keamanan cloud computing adalah untuk melindungi data, aplikasi, dan infrastruktur yang dihosting di cloud dari berbagai ancaman dan risiko. Keamanan cloud bertujuan untuk memastikan bahwa data yang disimpan dan diproses di cloud tetap aman dari akses yang tidak sah, kebocoran, kerusakan, atau kehilangan. Ini mencakup perlindungan terhadap **data pribadi**, **informasi sensitif**, serta **keselamatan aplikasi dan layanan cloud**. Keamanan cloud juga berfokus pada **penegakan kebijakan akses**, yang memastikan hanya pengguna yang berwenang yang dapat mengakses data atau aplikasi tertentu. **Enkripsi data** adalah salah satu fitur utama, yang menjamin data tetap aman baik saat disimpan (data at rest) maupun saat dikirimkan (data in transit). Dengan enkripsi, meskipun data jatuh ke tangan yang salah, data tersebut tidak dapat dibaca tanpa kunci enkripsi yang sesuai.

Selain itu, **monitoring dan auditing** adalah bagian penting dari keamanan cloud. Aktivitas pengguna dan administrator dipantau untuk mendeteksi perilaku mencurigakan atau pelanggaran. **Audit log** yang jelas memungkinkan organisasi untuk melacak siapa yang mengakses data, kapan, dan apa yang dilakukan, yang membantu dalam investigasi jika terjadi insiden keamanan. Fungsi lainnya adalah memastikan **keamanan fisik data center** tempat penyimpanan data cloud, di mana kontrol akses fisik, pengawasan, dan redundansi diperlukan untuk menjaga data tetap aman dari ancaman fisik seperti pencurian atau kerusakan. Peningkatan kemanan dilakukan untuk melindungi data sebuah organisasi atupun data penting lainya terhadap ancaman seperti penghancuran atau penyalahgunaan yang dikarenakan oleh virus yang meyebabkan kerugian yang disengaja maupun tidak disengaja(Yusnanto et al., 2019). Secara keseluruhan, fungsi utama keamanan cloud computing adalah untuk **melindungi data, menjaga kerahasiaan dan integritasnya,** serta memastikan bahwa aplikasi dan layanan yang berjalan di cloud dapat diakses secara aman tanpa risiko terhadap kerahasiaan atau ketersediaan data.

C. JENIS-JENIS KEAMANAN CLOUD COMPUTING

1. Keamanan Data (Data Security)

Keamanan Data merupakan salah satu aspek paling krusial dalam Keamanan Cloud Computing yang berfokus pada perlindungan data dari akses tidak sah, modifikasi, pencurian, atau kehilangan saat data disimpan di cloud maupun saat ditransmisikan melalui jaringan.

Tujuan: Melindungi data dari kehilangan, kebocoran, atau akses ilegal.
Implementasi:

a. Enkripsi data saat disimpan (at-rest) dan saat ditransmisikan (in-transit) **cara untuk mengamankan informasi sensitif** dari akses tidak sah dengan cara mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak memiliki kunci dekripsi yang sah. IAM (Identity and Access Management) amerupakan salah satu contoh sebuah kerangka kerja kebijakan dan teknologi yang memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sumber daya di lingkungan cloud, pada waktu dan hak akses yang sesuai.
   IAM merupakan salah satu elemen terpenting dalam cloud security karena hampir semua insiden keamanan disebabkan oleh akses yang salah konfigurasi atau penyalahgunaan kredensial.

b. Penggunaan Data Loss Prevention (DLP) merupakan serangkaian kebijakan, alat, dan proses yang digunakan untuk mendeteksi, mencegah, dan memantau pengiriman data sensitif agar tidak keluar dari lingkungan yang aman — baik secara tidak disengaja maupun karena aktivitas berbahaya. Tiga are pengguanaan Data Loss Prevention ada didalam tabael dibawah ini

***Tabel.1** Data Loss Prevention*

AREA	PENJELASAN
Data in Use	Saat data sedang diakses atau digunakan (misal: mengetik, copy-paste, upload).
Data in Motion	Saat data sedang dikirim melalui jaringan (misal: email, FTP, web).
Data in Rest	Saat data tersimpan di media penyimpanan (hard disk, database, cloud).

c. Penghapusan data secara aman (secure deletion) merupakanmerupakan proses menghapus data dari media penyimpanan (baik fisik maupun digital) dengan cara yang memastikan data tersebut tidak dapat dipulihkan kembali oleh pihak mana pun, termasuk menggunakan software recovery.

Langkah ini penting dalam keamanan cloud computing karena data yang sudah tidak digunakan tetap bisa menjadi target kebocoran jika tidak dihapus dengan benar.

2. Keamanan Jaringan (Network Security)

Keamanan jaringan merupakan sebuah cara atau upaya sistematis untuk menjaga integritas, kerahasiaan, dan ketersediaan jaringan komputer serta data yang mengalir di dalamnya dari berbagai macam ancaman, baik dari dalam maupun luar organisasi.

Tujuan: Mencegah akses tidak sah dan serangan jaringan ke infrastruktur cloud. Implementasi:

a. Firewall berbasis cloud (Cloud Firewall) merupakan sistem keamanan jaringan yang dihosting di lingkungan cloud dan digunakan untuk memfilter lalu lintas jaringan masuk dan keluar berdasarkan aturan keamanan yang ditentukan. Tidak seperti firewall tradisional yang berada secara fisik di perangkat keras lokal, cloud firewall bekerja secara virtual dan terdistribusi, serta dapat diintegrasikan langsung dengan layanan cloud seperti AWS, Azure, atau GCP

b. VPN dan tunneling adalah sebuah proses membungkus dan mengenkripsi data yang dikirimkan melalui internet publik ke dalam sebuah "terowongan" virtual, sehingga data tersebut tidak bisa dilihat atau dimodifikasi oleh pihak ketiga yang tidak berwenang.

c. IDS/IPS (Intrusion Detection & Prevention Systems) adalah teknologi yang digunakan untuk mendeteksi dan mencegah akses yang tidak sah atau berbahaya ke dalam jaringan komputer atau sistem. IDPS bertujuan untuk melindungi data dan infrastruktur dari ancaman yang berpotensi merusak atau mengekspos kerentanannya. Intrusion Detection System IDS bertugas mendeteksi potensi ancaman dan memberikan peringatan kepada administrator jaringan atau sistem. IDS tidak menghentikan atau mencegah ancaman secara langsung, tetapi mengidentifikasi aktivitas mencurigakan berdasarkan pola atau anomali. Intrusion Prevention System) IPS berfungsi untuk tidak hanya mendeteksi ancaman tetapi juga secara aktif mencegah serangan dengan mengambil tindakan seperti memblokir atau menghentikan komunikasi yang mencurigakan.

IPS sering kali terintegrasi dengan IDS untuk memberikan perlindungan yang lebih menyeluruh.

3. Keamanan Aplikasi (Application Security)

Merupakan serangkaian tindakan, kebijakan, dan alat yang diterapkan untuk melindungi aplikasi perangkat lunak dari ancaman dan kerentanannya yang dapat disalahgunakan oleh pihak yang tidak sah. Keamanan aplikasi bertujuan untuk mencegah eksploitasi kerentanannya selama seluruh siklus hidup pengembangan perangkat lunak, mulai dari perancangan hingga pemeliharaan.

Tujuan: Melindungi aplikasi cloud dari eksploitasi dan serangan (misalnya XSS, SQL Injection). Implementasi:

a. Pengetesan keamanan aplikasi (security testing) adalah melakukan pengujian keamanan secara menyeluruh pada aplikasi untuk mendeteksi kerentanannya antara lain:
Penetration testing (Pen testing): Menguji kerentanannya dengan cara mensimulasikan serangan untuk menemukan potensi titik lemah.
Static Application Security Testing (SAST): Menganalisis kode sumber aplikasi secara statis untuk menemukan kerentanannya sebelum aplikasi dijalankan. Dynamic Application Security Testing (DAST): Menguji aplikasi saat sedang berjalan (runtime) untuk mengidentifikasi kerentanan yang hanya muncul saat aplikasi dioperasikan.

b. Web Application Firewall (WAF) adalah sebuah cara dalam sistem keamanan yang dirancang untuk melindungi aplikasi web dari ancaman dan serangan yang mencoba mengeksploitasi kerentanannya. WAF berfungsi sebagai perisai antara pengguna dan aplikasi web, menyaring dan memantau lalu lintas HTTP/HTTPS yang masuk dan keluar dari aplikasi web untuk mendeteksi dan mencegah potensi serangan.

c. Secure API Gateway merupakan komponen keamanan yang bertindak sebagai perantara antara klien (misalnya aplikasi atau pengguna) dan backend (misalnya layanan mikro atau aplikasi web). API Gateway bertanggung jawab untuk mengelola dan mengamankan komunikasi antara pengguna dan API yang digunakan dalam aplikasi.

d. CI/CD pipeline dengan keamanan tertanam (DevSecOps) sebuah pendekatan yang mengintegrasikan keamanan langsung ke dalam proses Continuous Integration (CI) dan Continuous Deployment (CD) dalam pengembangan perangkat lunak. Tujuan utamanya adalah

untuk memastikan bahwa setiap bagian dari proses pengembangan, pengujian, dan penerapan perangkat lunak secara otomatis memeriksa

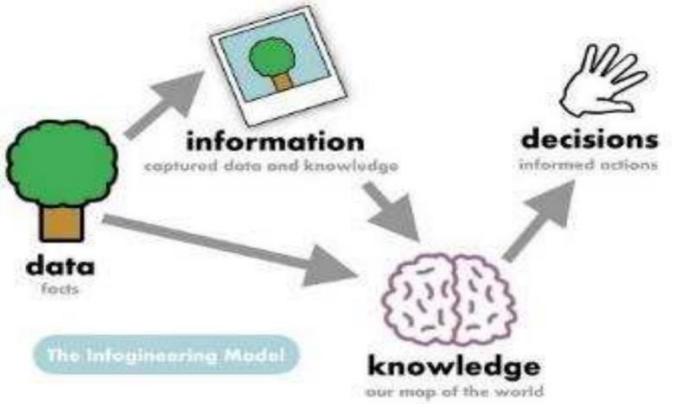
BAB 13 KEAMANAN DALAM BIG DATA DAN IOT

Ir. Lukman Medriavin Silalahi, A.Md., ST., MT., IPM., APEC-Eng
Andhika Kurniawan, Yudi Putra Wiratama, Suntoro, Zaldi Bima Aditya, Supriyadi Sofyan.

A. PENGERTIAN BIG DATA DAN IOT

Pada bab ini akan dijelaskan keamanan dalam Big Data dan IoT (*Internet of Things*) (El Hamdi, Abouabdellah and Oudani, 2020) berdasarkan keamanan, karakteristik, kategori, teknologi dasar dan tantangan masa depan.

Pentingnya (Xu, 2020) mengolah data-data kecil hingga membentuk Big Data seakan mengumpulkan serpihan puzzle kecil yang, ketika digabungkan, membentuk gambaran yang jauh lebih besar dan kaya. Dengan membayangkan sebagai kurator data, mengumpulkan setiap potongan informasi seperti yang ditunjukkan pada Gambar 1.



Gambar 13. 1. Gambaran umum big data

Dari ilustrasi gambar 13.1 terlihat beberapa komponen penting dalam konteks Big Data, antara lain:

1. Data (Fakta, deskripsi Dunia)
2. Informasi mentah yang menggambarkan realitas.Informasi (Data Tertangkap dan Pengetahuan): Proses mencatat atau mengambil Data dan Pengetahuan pada suatu titik waktu tertentu. Penting

untuk disadari bahwa Data dan Pengetahuan bersifat dinamis dan dapat berkembang seiring berjalannya waktu.

3. Pengetahuan (Peta/Model) merupakan representasi tentang dunia, bukan dunia sebenarnya itu sendiri. Saat ini, satu-satunya hal yang mampu menyimpan dan membangun pengetahuan adalah otak, dan untuk membangun pengetahuan, memerlukan Informasi dan Data sebagai bahan baku.

Selain itu, IoT (*Intenet of Things*) merupakan dimensi baru pada layanan internet (Budiyanto and Silalahi, 2023a, 2023b; Lukman Medriavin Silalahi, Simanjuntak and Rochendi, 2023). Dengan IoT memungkinkan segala sesuatu dapat berkomunikasi dengan kapanpun dan dimanapun. Definisi IoT adalah konsep yang menggambarkan jaringan perangkat fisik yang dilengkapi dengan sensor, perangkat lunak, dan teknologi lain untuk tujuan menghubungkan dan bertukar data dengan perangkat dan sistem lain melalui internet (Silalahi, Ikhsan, *et al.*, 2022; Silalahi *et al.*, 2024; Budiyanto *et al.*, 2024). Perangkat bisa brupa dari perangkat rumah tangga, perangkat di kantor hingga perangkat diindustri.

Secara sederhana IoT terdiri dari dua kata Internet dan Things:

1. Internet:Koneksi yang menghubungkan perangkat.
2. Things: Perangkat fisik atau peralatan sehari-hari.

Dalam IoT akan melibatkan beberapa hal meliputi perangkat fisik, konektivitas, platform IoT (Website dan Aplikasi) dan sensor dan aktuator. Dalam konsep IoT, segala sesuatu bisa diotomatisasi dan menghasilkan analisa data (Silalahi, Ikhsan, *et al.*, 2022; Silalahi, Jatikusumo, *et al.*, 2022; Silalahi *et al.*, 2024; Silalahi, Rochendi and Simanjuntak, 2024).

Dengan mengaktifkan IoT, masyarakat dapat mengontrol peralatan kehidupan sehari-hari dengan cara yang cerdas dan mudah. Ada banyak alasan yang membuat IoT layak untuk dilakukan, misalnya infrastruktur Internet telah tersedia hampir di semua. Selain itu, ukuran perangkat keras memungkinkan yang semakin kecil dapat digabungkan ke dalam perangkat sehari-hari. Karena berbasis internet maka setiap perangkat harus mempunyai alamat yang mana ini sudah ditunjang dengan hadirnya protokol IPv6 yang memiliki ruang alamat yang besar, sehingga kita dapat menetapkan IP untuk setiap perangkat (Wulandari *et al.*, 2021; Budiyanto *et al.*, 2022, 2024).

B. KARAKTERISTIK DAN TANTANG BIG DATA DAN IOT

IoT dan Big Data berdasarkan karakteristiknya antara lain:

1. Dinamis dan Beradaptasi Sendiri
   Perangkat dan sistem dapat menyesuaikan diri secara dinamis dengan perubahan konteks dan mengambil tindakan berdasarkan kondisi, konteks pengguna, atau lingkungan yang terdeteksi.
2. Protokol Komunikasi yang Interoperable
   Dukungan beberapa protokol komunikasi yang dapat dioperasikan bersama, memungkinkan perangkat untuk berkomunikasi tidak hanya satu sama lain tetapi juga dengan infrastruktur jaringan yang lebih besar.
3. Identitas Unik
   Setiap perangkat Big Data dan IoT memiliki identitas unik berupa alamat IP.
4. Konfigurasi Mandiri
   Memungkinkan banyak perangkat untuk bekerja sama secara otomatis guna menyediakan fungsi tertentu tanpa intervensi.
5. Terintegrasi ke dalam Jaringan Informasi
   Perangkat dapat terhubung ke jaringan informasi yang lebih besar, yang memungkinkan untuk berkomunikasi dan bertukar data dengan perangkat dan sistem lain.

Teknologi dasar yang berkaitan dengan Big Data dan IoT antara lain:

1. M2M (*Machine to Machine*)
   M2M merujuk pada jaringan antar mesin untuk pemantauan dan pengendalian jarak jauh serta pertukaran data. Jaringan area M2M terdiri dari mesin yang memiliki modul jaringan bawaan untuk penginderaan, aktuasi, dan komunikasi. Berbagai protokol komunikasi seperti Zigbee, Bluetooth, M-bus nirkabel, dll.
2. CPS (*Cyber-Physical Systems*)
   Integrasi antara komputasi, jaringan, dan proses fisik. Komputer dan jaringan yang tertanam memantau dan mengendalikan proses fisik, dengan loop umpan balik di mana proses fisik mempengaruhi komputasi dan sebaliknya.
3. WoT (*Web of Things*)
   Istilah yang digunakan untuk menggambarkan pendekatan, gaya arsitektur perangkat lunak, dan pola pemrograman yang memungkinkan objek dunia nyata menjadi bagian dari *website*. Deskripsi benda mencakup metadata dan antarmuka benda dengan cara yang terstandarisasi, dengan tujuan agar benda dapat berkomunikasi dengan benda lain di dunia yang heterogen.

Tantangan teknologi Big Data dan IoT antara lain:

1. Keamanan
   Keamanan adalah tantangan terbesar dalam Big Data dan IoT. Semakin banyak perangkat yang terhubung, semakin besar kemungkinan adanya eksploitasi kerentanan keamanan. Perangkat yang dirancang dengan buruk dapat mengekspos data pengguna terhadap pencurian dengan membiarkan data tidak terlindungi dengan baik, dan dalam beberapa kasus, dapat mengancam kesehatan dan keselamatan orang.
2. Skalabilitas
   Miliaran perangkat yang terhubung ke internet membentuk jaringan besar yang memerlukan pemrosesan volume data yang sangat besar sehingga dibutuhkan suatu sistem yang menyimpan dan menganalisis data dari perangkat yang mampu diskalakan.
3. Interoperabilitas
   Standar teknologi masih terfragmentasi di banyak area, dan teknologi ini perlu disatukan. Ini akan membantu dalam membangun *framework* dan standar umum untuk perangkat. Karena proses standarisasi masih kurang, interoperabilitas Big Data dan IoT dengan perangkat lama harus dianggap penting. Kurangnya interoperabilitas ini menghambat pencapaian visi benda-benda pintar yang benar-benar terhubung dan dapat dioperasikan sehari-hari.
4. Bandwidth
   Konektivitas merupakan tantangan besar bagi Big Data dan IoT. Berdasarkan pertumbuhan eksponensial pasar, beberapa ahli khawatir bahwa aplikasi Big Data dan IoT yang membutuhkan bandwidth besar seperti streaming video akan bersaing untuk mendapatkan ruang pada model server-klien saat ini.

C. SERANGAN DAN PENANGANAN *BRUTEFORCE*

Bruteforce attack merupakan salah satu teknik serangan siber yang paling umum digunakan untuk menembus sistem keamanan dengan mencoba semua kombinasi kata sandi. Berdasarkan penelitian Amijoyo, (Amijoyo, Umar and Yudhana, 2020) bahwa perangkat seperti Hydra dan Medusa sering digunakan untuk menyerang sistem berbasis Telnet dan SSH. Selain itu, Akbar (Akbar, Hariyadi and Hanani, 2023) menunjukkan bahwa serangan pada protokol IoT seperti MQTT dapat dideteksi secara efisien menggunakan algoritma Random Forest. Cara untuk menganalisis pola serangan bruteforce, mengevaluasi metode deteksi, dan mengusulkan strategi mitigasi yang efektif.

BAB 14 SERANGAN SIBER UMUM DAN TEKNIK

A. Taqwa Martadinata, M.Kom.

Dalam era digitalisasi yang pesat, serangan siber menjadi ancaman nyata yang semakin kompleks dan canggih. Dengan infrastruktur digital yang saling terhubung, risiko keamanan siber meningkat secara dramatis, mempengaruhi individu, organisasi, dan negara. Berdasarkan data terkini, serangan siber di Indonesia dan Dunia diperkirakan akan meningkat secara signifikan menjelang tahun 2025, dengan pola serangan yang semakin beragam dan tingkat kecanggihan yang lebih tinggi(Badan Siber dan Sandi Negara 2023)(Cisco 2024). Buku ini menyajikan analisis komprehensif tentang jenis-jenis serangan siber kontemporer, tren terbaru, teknik pencegahan efektif, dan studi kasus yang relevan dari Indonesia dan Dunia, untuk memberikan landasan pengetahuan bagi pengembangan strategi keamanan siber yang tangguh.

A. LANSKAP ANCAMAN SIBER *2025*

Berdasarkan laporan terbaru dari Global Cybersecurity Outlook 2025, lanskap keamanan siber global semakin kompleks akibat perkembangan teknologi, perubahan geopolitik, dan evolusi kejahatan siber(Detik 2022). Menurut data dari Badan Siber dan Sandi Negara (BSSN), terdapat lebih dari 1,2 miliar ancaman siber yang terdeteksi di Indonesia pada tahun 2023, mencakup berbagai jenis serangan dari malware hingga phishing(Badan Siber dan Sandi Negara 2023)

B. JENIS SERANGAN SIBER PALING UMUM

1. Malware

Gambar 14. 1. Gambar Malware (Source:(Freepik 2025a))

Lebih dari 1,2 miliar varian malware tercatat(CM-Alliance 2025).
Contoh:
Trojan menyamar sebagai aplikasi sah untuk mencuri data(Embroker 2025a).

2. Ransomware: Ancaman yang Terus Berevolusi

Gambar 14. 2. Gambar Ransomware (Source: (Freepik 2025c))

Ransomware tetap menjadi salah satu ancaman paling serius, meningkat 67% pada 2023(CM-Alliance 2025), menarget sektor kesehatan, energi, dan keuangan. Kemudian proyeksi peningkatan sebesar 30% pada tahun 2025(Edavos 2025). Serangan ini menyandera sistem atau data dengan mengenkripsinya, kemudian meminta tebusan untuk dekripsi.

Contoh serius terjadi pada Juni 2024, ketika Pusat Data Nasional (PDN) Indonesia dilumpuhkan oleh ransomware "Brain Cipher". Serangan dimulai dengan mematikan Windows Defender,

memungkinkan malware beroperasi tanpa hambatan. Dampaknya sangat besar, termasuk gangguan pada layanan imigrasi di bandara dan berbagai layanan publik lainnya(IDN 2025).

3. *Phishing* dan Rekayasa Sosial

Gambar 14. 3. Gambar Phishing (Source: (Freepik 2025b))

Phishing telah berkembang dari sekadar email penipuan sederhana menjadi serangan yang sangat canggih dan tertarget. Pada tahun 2025, teknik *phishing* diprediksi akan memanfaatkan kecerdasan buatan (AI) untuk menghasilkan konten yang lebih meyakinkan dan personalisasi yang lebih tinggi(Integrasolusi 2024).

Bentuk-bentuk baru seperti "*pig butchering*" (penipuan finansial jangka panjang yang melibatkan manipulasi psikologis) dan "*vishing*" (*phishing* suara) semakin sulit dideteksi karena melibatkan *deepfake* dan suara sintetis yang sangat realistis(Integrasolusi 2024)(J. T. University 2025).

4. Supply Chain Attacks (Serangan Rantai Pasokan)

Serangan rantai pasokan semakin meningkat karena penyerang menyadari bahwa vendor dan mitra bisnis sering menjadi titik lemah dalam ekosistem keamanan. Penyerang menargetkan organisasi pihak ketiga untuk mendapatkan akses ke target utama yang lebih besar dan lebih terlindungi(Edavos 2025).

Di tahun 2025, serangan ini diprediksi semakin menargetkan ekosistem sumber terbuka dan infrastruktur cloud yang kompleks. Hal ini menjadikan audit keamanan terhadap seluruh rantai pasokan sebagai komponen kritis dalam strategi keamanan siber(Integrasolusi 2024)

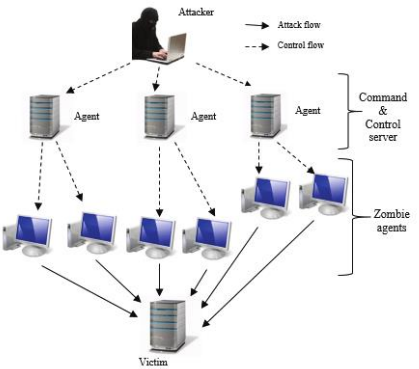
5. AI Agentik dan Serangan Berbasis Kecerdasan Buatan

Lembaga Riset Keamanan Siber *Communication and Information System Security Research Center* (CISSReC) mengidentifikasi AI Agentik sebagai ancaman utama yang harus diwaspadai pada 2025(Integrasolusi 2024)(J. T. University 2025). AI Agentik dapat:

- Mengotomatiskan serangan siber secara masif
- Melakukan pengintaian dan eksploitasi dengan presisi tinggi
- Beradaptasi secara real-time untuk mengatasi mekanisme pertahanan
- Meningkatkan kompleksitas dan tingkat keberhasilan serangan(Integrasolusi 2024)

Teknologi ini memungkinkan peretas untuk menjalankan operasi yang lebih efisien dengan sumber daya minimal, sementara dampaknya bisa sangat signifikan.

6. Distributed Denial of Service (DDoS)



Gambar 14. 4. Gambar DDoS

(Source:(Iddris, Abdulai, and Boateng 2019))

Serangan DDoS bertujuan melumpuhkan sistem dengan membanjirinya dengan trafik yang berlebihan. Meski tergolong teknik serangan klasik, DDoS tetap efektif dan sering digunakan untuk melumpuhkan layanan online atau sebagai pengalih perhatian dari serangan lain yang lebih canggih(Cisco 2024). Meningkat 13% pada awal 2024(CM-Alliance 2025), membanjiri server dengan lalu lintas palsu.

BAB 15 FORENSIK DIGITAL DAN INVESTIGASI INSIDEN

Tri Rochmadi, M.Kom., CSCU., CEI., CIISA.

A. PENDAHULUAN

1. Ancaman dan Serangan Siber

Dalam era digital saat ini, ancaman dan serangan siber telah menjadi isu krusial yang memengaruhi berbagai sektor, mulai dari pemerintahan hingga perusahaan swasta, Tabel 1.

Tabel 1. Sektor Terdampak Serangan siber

Sektor Terdampak	Jumlah
Pemerintahan	186
Lainnya	60
Keuangan	38
Transportasi	24
ESDM	18
TIK	5
Kesehatan	5
Pangan	5
Pertahanan	2

Sumber: (Id-SIRTII/CC – BSSN, 2024)

Serangan seperti malware, ransomware, phishing, dan Distributed Denial of Service (DDoS) dapat menyebabkan kerugian finansial yang signifikan serta merusak reputasi organisasi (Singh et al., 2022). Perkembangan teknologi yang pesat juga memberikan celah bagi pelaku kejahatan siber untuk mengeksploitasi sistem yang rentan (Rochmadi & Pasa, 2021). Oleh karena itu, pemahaman mendalam tentang berbagai jenis ancaman siber menjadi langkah awal dalam membangun strategi pertahanan yang efektif (S. A. Nugroho & Rochmadi, 2024).

Selain itu, serangan siber tidak hanya berdampak pada aspek teknis, tetapi juga dapat memengaruhi stabilitas sosial dan politik suatu negara. Contohnya, serangan terhadap infrastruktur kritis seperti jaringan listrik atau sistem komunikasi dapat mengganggu kehidupan masyarakat secara luas. Oleh karena itu, penting bagi setiap entitas untuk tidak hanya fokus pada pencegahan, tetapi juga pada kesiapan dalam merespons insiden siber yang mungkin terjadi (Rochmadi et al., 2024).

2. Peran Forensik Digital dalam Keamanan Informasi
   Forensik digital memainkan peran vital dalam menjaga keamanan informasi dengan cara mengidentifikasi, mengumpulkan, dan menganalisis bukti digital dari insiden siber (Rochmadi, 2019). Melalui pendekatan ini, penyelidik dapat memahami bagaimana serangan terjadi, siapa pelakunya, dan sejauh mana dampaknya terhadap sistem yang diserang. Informasi yang diperoleh dari forensik digital sangat penting untuk memperbaiki kerentanan sistem dan mencegah serangan serupa di masa depan.
   Selain itu, hasil dari investigasi forensik digital dapat digunakan sebagai alat bukti dalam proses hukum. Dengan demikian, forensik digital tidak hanya berkontribusi pada aspek teknis keamanan informasi, tetapi juga pada penegakan hukum terhadap pelaku kejahatan siber. Integrasi antara forensik digital dan kebijakan keamanan informasi yang komprehensif akan memperkuat pertahanan organisasi terhadap ancaman siber.
3. Tujuan Investigasi Insiden
   Investigasi insiden bertujuan untuk memahami secara menyeluruh tentang insiden keamanan yang terjadi, termasuk metode yang digunakan oleh penyerang dan titik kelemahan yang dimanfaatkan. Dengan informasi ini, organisasi dapat mengambil langkah-langkah yang tepat untuk menanggulangi insiden dan mencegah terulangnya kejadian serupa. Proses investigasi juga membantu dalam mengidentifikasi data atau sistem yang terpengaruh, sehingga memungkinkan pemulihan yang lebih cepat dan efisien.
   Selain itu, investigasi insiden berperan penting dalam meningkatkan kesadaran dan kesiapan organisasi terhadap ancaman siber. Melalui analisis insiden yang telah terjadi, organisasi dapat memperbarui kebijakan keamanan, meningkatkan pelatihan bagi karyawan, dan memperkuat infrastruktur TI agar sejalan dengan keamanan informasi (S. Nugroho & Rochmadi, 2024). Dengan demikian, investigasi insiden tidak hanya berfungsi sebagai respons terhadap

serangan, tetapi juga sebagai alat untuk memperkuat pertahanan siber secara keseluruhan.

B. KONSEP DASAR FORENSIK DIGITAL

1. Definisi dan Sejarah Forensik Digital

   Forensik digital adalah proses pengumpulan, pelestarian, analisis, dan presentasi bukti digital yang sah secara hukum. Proses ini digunakan untuk menyelidiki dan mengungkap tindak kejahatan yang melibatkan teknologi informasi (Nurindahsari & Zen, 2021), seperti peretasan, pencurian data, atau penyebaran malware. Seiring dengan berkembangnya teknologi, kejahatan digital pun ikut berkembang, sehingga diperlukan pendekatan ilmiah untuk menangani bukti digital. Inilah yang menjadi dasar berkembangnya ilmu forensik digital sebagai cabang dari forensik komputer.

   Sejarah forensik digital dimulai pada akhir 1980-an, ketika komputer mulai digunakan dalam kegiatan kriminal dan penegak hukum menyadari perlunya pendekatan khusus untuk menangani bukti digital. Salah satu kasus penting adalah kasus kriminal yang melibatkan penggunaan komputer oleh pelaku, yang mendorong pembentukan unit forensik digital pertama di lembaga penegak hukum. Sejak itu, berbagai organisasi internasional seperti FBI, INTERPOL, dan NIST mulai mengembangkan metodologi dan standar dalam praktik forensik digital. Kini, forensik digital telah menjadi bagian penting dalam sistem peradilan (Effendy, 2021) di banyak negara.

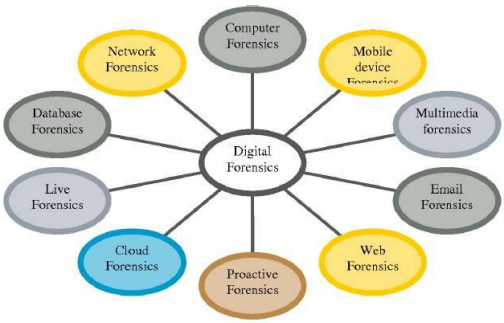
2. Prinsip-Prinsip Forensik Digital

   Prinsip utama dalam forensik digital adalah menjaga integritas bukti digital. Artinya, data yang dikumpulkan harus tetap utuh dan tidak boleh dimodifikasi selama proses investigasi berlangsung. Untuk memastikan hal ini, digunakan metode seperti hashing (MD5/SHA-1) guna memverifikasi keaslian data (Yudhana et al., 2022). Selain itu, proses dokumentasi harus dilakukan secara menyeluruh agar semua langkah dapat dipertanggungjawabkan di pengadilan.

   Prinsip penting lainnya adalah chain of custody, yaitu pencatatan yang jelas dan rinci tentang siapa saja yang menangani bukti digital, kapan, dan untuk tujuan apa. Catatan ini sangat penting untuk menjaga kredibilitas bukti dan menghindari penolakan di pengadilan (Friedl & Pernul, 2024). Forensik digital juga harus mengikuti prosedur yang dapat diuji ulang, sehingga hasil

analisisnya dapat diterima sebagai bukti ilmiah. Prinsip-prinsip ini menjadi fondasi dari setiap proses investigasi forensik yang profesional dan sah secara hukum.

3. Etika dan Hukum dalam Forensik Digital
   Etika merupakan aspek penting dalam praktik forensik digital karena penyelidik sering kali menangani data yang bersifat pribadi dan sensitif (Dinarti et al., 2024). Profesional forensik digital wajib menjaga kerahasiaan data dan menghormati privasi individu yang terkait dalam kasus. Pelanggaran etika dapat merusak integritas penyelidik dan bahkan menyebabkan bukti dianggap tidak sah di pengadilan. Oleh karena itu, pelatihan dan sertifikasi etika sering kali menjadi syarat bagi praktisi forensik digital.
   Di sisi lain, aspek hukum dari forensik digital sangat bergantung pada peraturan perundang-undangan yang berlaku di suatu negara. Di Indonesia, Undang-Undang ITE menjadi dasar hukum utama dalam menangani kejahatan digital dan penggunaan bukti elektronik. Selain itu, ada juga regulasi internasional seperti GDPR di Eropa yang mengatur perlindungan data pribadi. Praktisi forensik digital harus memahami kerangka hukum yang berlaku agar setiap tindakan yang dilakukan tetap berada dalam jalur legal dan dapat diterima di ranah peradilan.
4. Jenis Forensik Digital dan Sumber Bukti Digital
   Forensik digital mencakup berbagai jenis, tergantung pada perangkat dan sistem yang dianalisis. Di antaranya adalah forensik komputer, forensik jaringan, forensik perangkat mobile, dan forensik cloud, dan lainnya, Gambar 1. Forensik komputer fokus pada penyelidikan perangkat seperti hard disk, sedangkan forensik jaringan berfokus pada lalu lintas data dan aktivitas jaringan. Sementara itu, forensik perangkat mobile melibatkan ponsel pintar dan tablet, yang kini menjadi target utama karena menyimpan banyak data personal.



Gambar 15. 1. Jenis Forensik Digital (Pericherla, 2025)

Sumber bukti digital sangat beragam, mulai dari file sistem, log aktivitas, email, pesan instan, metadata, hingga artefak memori (Rochmadi, 2018), (Aji et al., 2020). Bukti digital ini bisa diperoleh dari bukti elektronik seperti, berbagai media penyimpanan seperti hard drive, SSD, flashdisk, printer, tablet, bahkan RAM, (Pooe, 2018)seperti Gambar 2. Selain itu, sumber dari cloud computing dan media sosial juga mulai sering dijadikan bukti karena meningkatnya adopsi teknologi ini. Pemahaman tentang berbagai jenis bukti digital sangat penting agar penyelidik dapat melakukan pendekatan yang tepat dalam setiap kasus.

Gambar 15. 2. Barang Bukti Elektronik

C. PROSES INVESTIGASI FORENSIK DIGITAL

Proses investigasi forensik digital memerlukan pendekatan sistematis dan metodologi yang terstruktur agar bukti yang dikumpulkan sah secara hukum dan hasil investigasinya dapat dipercaya. Beberapa framework yang umum digunakan adalah model dari NIST (National Institute of Standards and Technology) (Riadi & Ruslan, 2023), ACPO Guidelines dari Inggris (Sheunesu et al., 2020), dan Digital Forensics Process Model. Masing-masing model memiliki tahapan yang relatif mirip, yaitu identifikasi, akuisisi, analisis, dokumentasi, dan pelaporan. Tujuannya adalah memastikan setiap langkah memiliki dasar yang kuat dan dapat dipertanggungjawabkan.

Dalam praktiknya, pendekatan ini juga harus fleksibel, menyesuaikan jenis kasus dan kompleksitas bukti digital yang ditangani. Misalnya, dalam kasus forensik cloud atau mobile, metode akuisisi dan analisis sangat berbeda dengan forensik komputer tradisional. Oleh karena itu, penyelidik forensik digital harus memahami berbagai model dan memiliki keterampilan teknis yang memadai untuk menyesuaikan metodologi yang digunakan. Evaluasi berkelanjutan terhadap proses dan hasil juga menjadi bagian penting dalam meningkatkan efektivitas investigasi.

1. Identifikasi Insiden
   Identifikasi merupakan tahap pertama dalam proses investigasi, di mana penyelidik harus menentukan bahwa sebuah insiden benar-benar terjadi. Tanda-tanda insiden bisa berupa aktivitas jaringan yang tidak biasa, sistem yang tidak responsif, atau laporan dari pengguna mengenai anomali tertentu. Pada tahap ini, penting untuk segera mengklasifikasikan jenis insiden agar pendekatan investigasi bisa diarahkan secara tepat. Deteksi dini sangat krusial untuk meminimalkan kerusakan lebih lanjut, dan bisa menerapkan digital forensic readiness agar investigasi lebih efektif dan efisien (Rochmadi et al., 2024).
   Alat bantu seperti sistem IDS (Intrusion Detection System), log server, dan perangkat monitoring lainnya sangat membantu dalam proses identifikasi ini. Tim keamanan informasi juga harus menetapkan kriteria khusus mengenai apa yang dikategorikan sebagai insiden keamanan. Kejelasan dalam proses ini akan mempercepat pengambilan keputusan dan mempermudah langkah-langkah selanjutnya seperti akuisisi data. Dokumentasi awal dari gejala insiden juga harus dilakukan secara sistematis.

2. Akuisisi dan Pelestarian Bukti Digital
   Akuisisi merupakan proses pengambilan data dari sistem yang terdampak, dengan cara yang menjamin keutuhan dan keasliannya. Pada tahap ini, dilakukan proses imaging atau bit-by-bit copy dari perangkat penyimpanan, baik itu hard disk, SSD, maupun perangkat mobile. Setiap data yang diambil harus disertai dengan verifikasi melalui hashing (misalnya menggunakan algoritma MD5 atau SHA-256) agar tidak ada perubahan sedikit pun dari aslinya (Michael & Herbert, 2021). Hal ini penting untuk memastikan bahwa bukti tersebut valid dan dapat diterima.
   Pelestarian bukti berarti menjaga agar bukti yang telah diambil tidak terkontaminasi atau rusak, baik secara teknis maupun prosedural. Ini termasuk menjaga lingkungan penyimpanan data yang aman, serta memastikan chain of custody, catatan yang menunjukkan siapa saja yang menangani bukti selalu lengkap dan terjaga. Penyimpanan dilakukan pada media forensik khusus, dan biasanya ada salinan cadangan yang disimpan secara terpisah. Langkah ini menjadi kunci dalam mempertahankan kredibilitas atau mengamankan bukti untuk keperluan investigasi forensik (Jimenez & Fernandez, 2022).
3. Analisis Bukti Digital
   Analisis merupakan tahap paling intensif dalam proses forensik digital, karena melibatkan penafsiran dari data mentah yang dikumpulkan. Proses ini mencakup pencarian artefak digital seperti file yang dihapus, aktivitas pengguna, log sistem, dan metadata (Al-Dhaqm et al., 2020) yang dapat mengungkap pola serangan atau aktivitas mencurigakan, contoh metadata dapat dilihat pada Tabel 2.

Tabel 2. Contoh Metadata File

Attribut	Nilai
Name	Outlook
Logical Size	4,096
Category	Unknown
Signature Analysis	Unknown
Last Accessed	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
File Created	06/23/19 06:08:44 AM (-4:00 Eastern Daylight Time)

Last Written	04/23/20 12:46:21 AM (-4:00 Eastern Daylight Time)
Is Indexed	Yes
MD5	e6936d8fc6d134b0f9499e9ddcc2d21eef
SHA1	ef073eea71bae5b3f85f9787e1c7a6ce7827fb21
Item Path	E01Capture/C/Users/Dropbox/Outlook
True Path	C:/Users/Dropbox/Outlook
Description	Folder, Archive

Sumber: (Gilmore, 2020)

Tools seperti Autopsy, FTK, atau Volatility sering digunakan untuk mengekstraksi dan memvisualisasikan bukti digital dari berbagai jenis media. Tujuan utama analisis adalah mengungkap "apa yang terjadi", "kapan", dan "oleh siapa".

Selama analisis, penyelidik harus tetap objektif dan mengikuti prosedur yang terdokumentasi. Bukti yang ditemukan harus dikaitkan dengan hipotesis atau dugaan awal dan kemudian diuji keabsahannya. Analisis juga bisa mencakup teknik seperti timeline analysis untuk menyusun kronologi kejadian, serta koroborasi data antar sumber. Keakuratan dan dokumentasi yang teliti sangat penting agar hasil analisis dapat dibuktikan di forum hukum.

4. Dokumentasi dan Pelaporan

   Dokumentasi harus dilakukan di setiap tahap proses forensik untuk memastikan bahwa semua kegiatan dapat diaudit dan dipertanggungjawabkan. Ini mencakup deskripsi alat yang digunakan, pengaturan konfigurasi, waktu pengambilan bukti, hasil hashing, hingga langkah-langkah dalam analisis. Semua ini harus dituangkan dalam format yang baku agar dapat digunakan sebagai bagian dari laporan resmi.

   Pelaporan adalah keluaran akhir dari proses forensik digital yang biasanya diserahkan kepada manajemen, tim hukum, atau bahkan pengadilan. Laporan harus disusun secara sistematis dan menggunakan bahasa yang bisa dipahami oleh non-teknis, tanpa menghilangkan aspek teknis yang penting. Di dalam laporan, biasanya disertakan ringkasan eksekutif, metodologi, temuan utama, serta rekomendasi tindak lanjut (Riadi & Bashor, 2022). Kualitas laporan sangat memengaruhi dampak dari proses investigasi secara keseluruhan.

5. Penyajian Bukti

BAB 16 KEAMANAN MOBILE DAN BYOD

Dede Irawan, M.Kom.

A. KEAMANAN MOBILE

Aplikasi mobile telah menjadi bagian penting dari kehidupan sehari-hari. Namun, dengan meningkatnya penggunaan aplikasi mobile, risiko keamanan juga meningkat. Oleh karena itu, keamanan aplikasi mobile menjadi faktor krusial dalam melindungi data pengguna dan sistem dari ancaman siber.

1. Ancaman dan Pencegahan Keamanan Aplikasi Mobile

a) Malware dan Virus

Malware adalah perangkat lunak berbahaya yang dirancang untuk menyusup, merusak, atau mencuri data dari perangkat pengguna tanpa izin. Seiring berkembangnya teknologi, malware semakin canggih dan mampu mengeksploitasi celah keamanan pada sistem operasi Android maupun IOS. Dalam konteks keamanan aplikasi seluler, malware menjadi ancaman serius yang dapat merusak privasi pengguna, mencuri informasi sensitif, dan bahkan mengambil alih kendali penuh perangkat. Malware pada perangkat mobile telah berkembang pesat dalam beberapa tahun terakhir, dari sekadar iklan berbahaya hingga serangan yang sangat canggih yang bisa mengontrol perangkat dari jarak jauh. Beberapa varian malware yang berbahaya meliputi:

1) **Trojan Horse**
   Menyamar sebagai aplikasi sah tetapi diam-diam mencuri data pengguna.
2) **Spyware**
   Mengumpulkan informasi pribadi tanpa sepengetahuan pengguna.
3) **Ransomware**

Mengenkripsi data pengguna dan meminta tebusan agar data dapat diakses kembali.

4) **Adware**
   Menampilkan iklan berlebihan yang mengganggu dan sering kali mengunduh perangkat lunak tambahan secara diam-diam.

Malware modern bahkan mampu memanipulasi sistem keamanan perangkat, seperti melewati sistem autentikasi dua faktor (2FA), mengelabui pengguna agar mengunduh aplikasi palsu, dan mengakses data pribadi tanpa izin. Saat ini Malware dapat masuk ke perangkat mobile melalui berbagai metode, termasuk:

1) **Aplikasi Berbahaya**
   Aplikasi yang diunduh dari sumber tidak resmi sering kali mengandung malware tersembunyi.
2) **Serangan Jaringan**
   Penggunaan WiFi publik yang tidak aman dapat memungkinkan peretas menginjeksi malware ke dalam perangkat.
3) **Eksploitasi Kerentanan**
   Celah keamanan dalam sistem operasi atau aplikasi dapat dimanfaatkan oleh malware untuk masuk ke perangkat.

Setelah menginfeksi perangkat, malware dapat melakukan berbagai tindakan berbahaya seperti mencuri informasi login, mengontrol perangkat, mengunduh aplikasi tambahan tanpa izin, dan bahkan merekam aktivitas pengguna.

Untuk melindungi perangkat mobile dan aplikasi dari malware, beberapa langkah pencegahan dapat diterapkan:

1) **Menginstal Aplikasi dari Sumber Resmi** – Selalu unduh aplikasi dari Google Play Store atau Apple App Store untuk menghindari aplikasi berbahaya.

2) **Menggunakan Keamanan Tambahan** – Gunakan solusi keamanan seperti antivirus, firewall, dan VPN untuk melindungi data dari serangan malware.

3) **Memperbarui Perangkat dan Aplikasi Secara Rutin** – Pembaruan perangkat lunak sering kali mengandung perbaikan keamanan untuk mengatasi celah yang bisa

dimanfaatkan oleh malware. Pembaruan perangkat lunak, baik untuk sistem operasi, aplikasi, maupun firmware, sering kali mencakup perbaikan keamanan untuk mengatasi kerentanan yang dapat dieksploitasi oleh malware. Pengembang perangkat lunak secara berkala mengidentifikasi dan menambal celah ini melalui patch keamanan.

4) **Hati-hati dengan Izin Aplikasi** – Jangan sembarangan memberikan izin akses yang tidak relevan saat menginstal aplikasi.

5) **Menghindari Koneksi WiFi Publik Tanpa Perlindungan** – Gunakan VPN saat mengakses WiFi publik untuk menghindari serangan man-in-the-middle.

6) **Menggunakan Autentikasi yang Kuat** – Gunakan autentikasi multifaktor (MFA) dan kata sandi yang kuat untuk mencegah pencurian kredensial.

7) **Waspada terhadap Phishing dan Social Engineering** – Jangan mengklik tautan mencurigakan dalam email atau pesan yang tidak dikenal.

b) **Man-in-the-Middle (MitM) Attack:**
Man-in-the-Middle (MitM) Attack adalah serangan siber di mana penyerang menyusup ke dalam komunikasi antara dua pihak, misalnya antara aplikasi mobile dan server, tanpa diketahui oleh pihak yang terlibat. Serangan ini memungkinkan peretas untuk mencegat, mengubah, atau bahkan menyisipkan data berbahaya ke dalam komunikasi yang terjadi. Serangan MitM dapat menyebabkan Informasi pribadi, kata sandi, dan detail perbankan dapat dicuri oleh penyerang atau Penyerang dapat menggunakan kredensial yang dicuri untuk mengakses akun korban di berbagai layanan.

Pada aplikasi mobile, serangan MitM sering terjadi saat perangkat terhubung ke jaringan yang tidak aman, seperti WiFi publik atau koneksi yang dienkripsi dengan buruk. Dengan mengelabui perangkat korban agar percaya bahwa mereka berkomunikasi dengan server yang sah, peretas dapat mencuri data sensitif seperti kredensial login, informasi kartu

BAB 17 TREN MASA DEPAN DALAM KEAMANAN SISTEM INFORMASI

Doni Prastyo, S.Kom., M.Kom.

A. PENDAHULUAN

Dalam era digital yang terus berkembang, keamanan sistem informasi telah menjadi salah satu aspek paling krusial dalam manajemen teknologi informasi. Serangan siber tidak hanya meningkat dalam jumlah, tetapi juga dalam kompleksitas, skala, dan dampaknya terhadap organisasi. Oleh karena itu, memahami tren masa depan dalam keamanan sistem informasi menjadi penting untuk membangun strategi pertahanan yang adaptif dan proaktif. Bab ini membahas beberapa tren utama yang diperkirakan akan mendominasi lanskap keamanan sistem informasi dalam beberapa tahun ke depan, dengan dukungan dari literatur dan kajian ilmiah terkini.

B. INTEGRASI KECERDASAN BUATAN (AI) DAN *MACHINE LEARNING* (ML) DALAM KEAMANAN SIBER

Ancaman keamanan siber semakin berkembang dari waktu ke waktu, baik dari segi volume, variasi, maupun kompleksitas. Serangan tidak lagi bersifat generik, melainkan cenderung bertarget, terotomatisasi, dan adaptif. Di tengah tantangan ini, pendekatan keamanan tradisional berbasis aturan (rule-based systems) dan daftar tanda tangan (signature-based detection) menjadi kurang memadai.

Oleh karena itu, muncul kebutuhan akan pendekatan yang lebih dinamis, adaptif, dan cerdas. Kecerdasan Buatan (Artificial Intelligence/AI) dan Pembelajaran Mesin (Machine Learning/ML) menawarkan potensi tersebut, dengan kemampuan untuk belajar dari data, mengenali pola, dan membuat prediksi terhadap ancaman baru secara otomatis.

1. Peran Strategis AI/ML dalam Keamanan Siber

Peran strategis AI/ML dalam keamanan siber terletak pada kemampuannya untuk secara proaktif mendeteksi ancaman, menganalisis

pola serangan secara real-time, serta mengotomatisasi respons terhadap insiden guna meningkatkan kecepatan dan akurasi pertahanan siber. Berikut beberapa peran strategis AI/ML dalam keamanan siber :

a. Anomaly Detection
   Dengan supervised atau unsupervised learning, sistem dapat mengidentifikasi aktivitas yang tidak biasa misalnya login dari lokasi geografis baru atau pola akses data yang menyimpang dari kebiasaan pengguna.
b. Automated Malware Detection
   AI dapat digunakan untuk menganalisis ribuan sampel malware baru per hari dan mengklasifikasikannya berdasarkan ciri-ciri perilaku, bukan hanya hash file. Hal ini memungkinkan deteksi varian baru dari malware yang tidak dikenal sebelumnya.
c. Phishing Detection
   NLP (Natural Language Processing) digunakan untuk menganalisis isi pesan email atau URL dan mengenali indikasi phishing secara otomatis, jauh sebelum kampanye phishing menyebar luas.
d. Threat Intelligence Correlation
   AI dapat membantu mengintegrasikan dan mengkorelasikan data dari berbagai sumber intelijen ancaman (threat feeds), baik dari internal maupun eksternal organisasi, untuk membangun konteks yang lebih utuh terhadap potensi serangan.

2. Teknik Mechine Learning yang Digunakan

Beberapa pendekatan ML yang umum digunakan dalam keamanan siber meliputi:

a. Supervised Learning: digunakan saat terdapat dataset berlabel, seperti klasifikasi email spam vs. non-spam.
b. Unsupervised Learning: digunakan untuk deteksi anomali ketika tidak ada label data, seperti clustering trafik mencurigakan.
c. Reinforcement Learning: cocok untuk sistem yang harus mengambil keputusan berkelanjutan dan belajar dari feedback, seperti dalam dynamic access control.

3. Keunggulan

Berikut adalah Keunggulan dalam Penerapan AI/ML di Keamanan Sistem Informasi :

a. Skalabilitas dalam Mengelola Data Besar (Big Data)
   AI dan ML mampu memproses serta menganalisis volume data yang sangat besar secara real-time, yang sangat penting dalam

lingkungan siber modern di mana jumlah log, event, dan aktivitas jaringan sangat masif dan terus bertambah.

b. Deteksi Zero-Day Attack Tanpa Ketergantungan pada Signature
Berbeda dengan sistem tradisional yang bergantung pada signature atau pola serangan yang telah diketahui, AI/ML dapat mengenali anomali dan mendeteksi serangan baru (zero-day) melalui pembelajaran pola yang tidak lazim dalam sistem.

c. Otomatisasi dan Efisiensi Kerja Tim SOC (Security Operation Center)
AI/ML dapat mengotomatisasi tugas-tugas rutin seperti penyaringan alert, korelasi log, dan prioritisasi insiden, sehingga memungkinkan tim SOC fokus pada ancaman kritis dan analisis yang membutuhkan penilaian manusia.

4. Tantangan

Berikut adalah Tantangan dalam Penerapan AI/ML di Keamanan Sistem Informasi :

a. Kebutuhan Data Besar dan Berkualitas
Akurasi model ML sangat bergantung pada ketersediaan dataset yang besar, bersih, dan representatif. Kurangnya data atau data yang bias dapat menyebabkan performa sistem menurun dan deteksi ancaman menjadi tidak andal.

b. Bias dan Overfitting
Model yang tidak dilatih secara seimbang dapat mengalami bias terhadap jenis data tertentu atau overfitting, yakni terlalu menyesuaikan dengan data pelatihan sehingga tidak mampu melakukan generalisasi terhadap data baru

c. Adversarial Attacks
Penyerang dapat menggunakan teknik adversarial machine learning untuk menyisipkan input yang dimodifikasi secara halus agar dapat mengelabui model AI, membuatnya gagal dalam mengidentifikasi serangan dengan benar

d. Keterbatasan Explainability (Black Box)
Model seperti deep learning sering kali sulit untuk dijelaskan cara kerjanya (black box model), yang menyulitkan analis keamanan dalam memahami dasar pengambilan keputusan sistem, dan dapat mengurangi kepercayaan serta menghambat proses forensik atau audit.

DAFTAR PUSTAKA

Ananda, L. R., Hafiza, L., Jannah, M., Samsumar, L. D., Anisa, D., Nurdin, A. M., ... & Wijanarko, S. (2024). Jaringan Komputer.

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

Aji, M. P., Rochmadi, T., & Hariyadi, D. (2020). Logical Acquisition in the Forensic Investigation Process of Android Smartphones based on Agent using Open Source Software. 2nd International Conference on Engineering and Applied Sciences (2nd InCEAS), 1–6. https://doi.org/10.1088/1757-899X/771/1/012024

Akbar, G.M.I., Hariyadi, M.A. and Hanani, A. (2023) 'Detection of Bruteforce Attacks on the MQTT Protocol Using Random Forest Algorithm', Internet of Things and Artificial Intelligence Journal, 3(3), pp. 250–272. Available at: https://doi.org/10.31763/iota.v3i3.630.

Al-Dhaqm, A., Razak, S. A., Siddique, K., Ikuesan, R. A., & Kebande, V. R. (2020). Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field. IEEE Access, 8, 145018–145032. https://doi.org/10.1109/ACCESS.2020.3008696

Amijoyo, T., Umar, R. and Yudhana, A. (2020) 'Bruteforce In The Hydra Process And Telnet Service Using The Naïve Bayes Method: Bruteforce In The Hydra Process And Telnet Service Using The Naïve Bayes Method', Jurnal Mantik, 4(1), pp. 319–326. Available at: https://iocscience.org/ejournal/index.php/mantik/article/view/752 (Accessed: 20 April 2025).

Anderson, R. (2020) Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley.

Anderson, R. (2022). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

Andress, J. (2014). The basics of information security: Understanding the fundamentals of InfoSec. Syngress Publishing.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 1–10. https://doi.org/10.1186/S12911-020-01161-7

Argyridou, E., Nifakos, S., Laoudias, C., Panta, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2022). Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Healthcare Organisations (Preprint). Journal of Medical Internet Research. https://doi.org/10.2196/41294

Arvandi, M., 2005, Analysis of Neural Network Based Ciphers, Thesis, University, Toronto

B. Surya, & T. David. (2022). Keamanan Data Pribadi Dalam Sistem Pembayaran E-Wallet Terhadap Ancaman Penipuan Dan Pengelabuan (Cyber Crime),. Jurnal Fakultas Hukum, Hal. 298-306.

Baltzan, P. (2021). Business Driven Information Systems (7th ed.). McGraw-Hill.

Batubara, T.P., Efendi, S. and Nababan, E.B. (2021) 'Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force', Journal of Physics: Conference Series, 1811(1), p. 012129. Available at: https://doi.org/10.1088/1742-6596/1811/1/012129.

Bloomberg. (2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. Bloomberg Businessweek.

Bocij, P., Greasley, A., & Hickie, S. (2021). Business Information Systems: Technology, Development and Management for the Modern Business (6th ed.). Pearson.

Brooks, D., & Chen, H. (2014) "Mobile Security for BYOD in the Enterprise," Mobile Computing and Security, Springer.Budhi Gustiandi (2023) Langkah Awal Menguasai Bahasa Pemrograman Python, Langkah Awal Menguasai Bahasa Pemrograman Python. Available at: https://doi.org/10.55981/brin.656.

Budiyanto, S. and Silalahi, L.M. (2023a) 'Internet of Things for 4.0 Industry Revolution', Journal of Innovation and Community Engagement, 4(3 SE-Articles), pp. 164–173. Available at: https://doi.org/10.28932/ice.v4i3.7316.

Budiyanto, S. and Silalahi, L.M. (2023b) 'Internet of Things for 4.0 Industry Revolution', Journal of Innovation and Community Engagement, 4(3), pp. 164–173. Available at: https://doi.org/10.28932/ice.v4i3.7316.

Budiyanto, S. et al. (2022) 'Smart Door Lock Prototype Design at Internet of Things-Based Airport', in 2022 5th International Conference of Computer and Informatics Engineering (IC2IE). IEEE, pp. 331–334. Available at: https://doi.org/10.1109/IC2IE56416.2022.9970074.

Budiyanto, S. et al. (2024) 'Peran Kesehatan dan Keselamatan Kerja Pekerja Rumah Tangga: Fokus pada Kelistrikan Rumah Tangga Berbasis Internet of Things di Penang Malaysia', MINDA BAHARU, 8(2), pp. 358–365. Available at: https://doi.org/https://doi.org/10.33373/jmb.v8i2.6300.

Burgett, A. (2024, May 8). Practical Incident Response Guidance from NIST SP 800-61. ArmorPoint. https://armorpoint.com/2024/05/08/a-step-by-step-guide-to-incident-response-practical-guidance-from-nist-sp-800-61/

Cheng, L., Liu, F., Yao, D., & Zhang, Q. (2017). Security and Privacy in Smart Home Environments: A Systematic Literature Review. Computer Networks, 148, 295–306. https://doi.org/10.1016/j.comnet.2018.11.001

Choppara, M. (2022). Digitalised Information Security in Data Communication in Organizational Flow. International Journal For

Science Technology And Engineering, 10(6), 2825–2829. https://doi.org/10.22214/ijraset.2022.44485

Choppara, M. (2022). Digitalised Information Security in Data Communication in Organizational Flow. International Journal For Science Technology And Engineering, 10(6), 2825–2829. https://doi.org/10.22214/ijraset.2022.44485

Clarke, R. (2021). Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060

Daemen, J., & Rijmen, V. (2021). The Design of Rijndael: AES – The Advanced Encryption Standard. Springer.

Davenport, T. H., & Short, J. E. (2020). The New Industrial Engineering: Information Technology and Business Process Redesign. Sloan Management Review, 31(4), 11-27.

Denning, D.E., 1982, Cryptography and Data Security, Addison-Wesley Publishing, Canada.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. The Journal of Strategic Information Systems, 30(4), 101693.

Dinarti, N. S., Rizkya Salsabila, S., & Herlambang, Y. T. (2024). Dilema Etika dan Moral dalam Era Digital: Pendekatan Aksiologi Teknologi terhadap Privasi Keamanan, dan Kejahatan Siber. Jurnal Pendidikan Ilmu-Ilmu Sosial Dan Humaniora, 1. https://doi.org/10.26418/jdn.v2i1.74931

Effendy, T. W. (2021). Digital Forensic Readines Index (DiFRI) untuk Mengukur Kesiapan Penanggulangan Cybercrime pada Kantor Wilayah Kementerian Hukum dan HAM DIY. Cyber Security Dan

Forensik Digital, 4(1), 18–23. https://doi.org/10.14421/csecurity.2021.4.1.2235

El Hamdi, S., Abouabdellah, A. and Oudani, M. (2020) 'Efficient simulated annealing algorithm for wireless sensors location in logistics 4.0', in B. Y. and M. F.-Z. (eds) 5th International Conference on Logistics Operations Management, GOL 2020. MOSIL, TICLab, University of Ibn Tofail, International University of Rabat Kenitra, Rabat, Morocco: Institute of Electrical and Electronics Engineers Inc. Available at: https://doi.org/10.1109/GOL49479.2020.9314747.

ENISA (European Union Agency for Cybersecurity). (2021). Threat Landscape for Supply Chain Attacks. https://www.enisa.europa.eu

Friedl, S., & Pernul, G. (2024). IoT Forensics Readiness - influencing factors. In Forensic Science International: Digital Investigation (Vol. 49). Elsevier Ltd. https://doi.org/10.1016/j.fsidi.2024.301768

Friedle, C. (2021). Information Systems Security in Organisations: A Critical Literature Review. iSCHANNEL, 16(1).

Gartner. (2022). Top Security and Risk Management Trends. Gartner Research Report. https://www.gartner.com

Gilmore, R. W. , C. C. E. (2020, May 22). Computer Forensics: What is metadata? PROTUS3. https://protus3.com/computer-forensics-metadata/

Goodfellow, I., Bengio, Y., & Courville, A. (2020). Deep Learning and Cybersecurity. MIT Press.

Goodin, D. (2021). TPM and Security: A Deep Dive. Cybersecurity Journal, 12(4), 88-102.

Hammer, M., & Champy, J. (2021). Reengineering the Corporation: A Manifesto for Business Revolution (3rd ed.). HarperBusiness.

Harmon, P. (2020). Business Process Change: A Business Process Management Guide for Managers and Process Professionals (4th ed.). Morgan Kaufmann.

Hidayat, D. and Ramli, R. (2023) 'Mengoptimalkan Pencegahan Serangan Brute Force pada Linux melalui Penerapan Metode Aplikasi IDS Snort', JiTEKH, 11(2), pp. 57–61. Available at: https://doi.org/10.35447/jitekh.v11i2.764.

Hidayat, R. A. F., Lingga, M. R., Hardi, R., Veriyadna, A. H., & Arsyadona, A. (2024). Efektivitas Manajemen Risiko Sumber Daya Manusia dalam Menghadapi Risiko Keamanan Data Karyawan di Sektor Teknologi. Manajemen Kreatif Jurnal, 3(1), 01–09. https://doi.org/10.55606/makreju.v3i1.3557

Homoliak, I., Venugopalan, S., Reijsbergen, D., Schumi, R., & Szalachowski, P. (2020). A Security Reference Architecture for Blockchain-Based Systems. IEEE Transactions on Secure and Dependable Computing, 19(1), 90–106. https://doi.org/10.1109/TDSC.2020.3024014

Howard, M., & LeBlanc, D. (2020). Writing Secure Code. Microsoft Press.

Howarth, F., 2013, 5 Key Steps to Ensuring Database Security, Faulkner Information Services.

https://www.google.co.id/books/edition/Keamanan_Data_dan_Informasi/NSsbEQAAQBAJ?hl=id&gbpv=1&dq=definisi+keamanan+informasi&pg=PA24&printsec=frontcover

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation. https://www.ibm.com/security/data-breach

Id-SIRTII/CC – BSSN. (2024). Lanskap Keamanan Siber Indonesia. https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

Intel Security Report. (2022). Securing the Semiconductor Supply Chain. Intel Corporation.

ISO/IEC 27001:2013. Information Security Management Systems.

ISO/IEC 27002 (2022). Information security, cybersecurity and privacy protection — Information security controls. International Organization for Standardization. pp. A.5.15, A.5.17, A.5.18, A.8.5.

Jevtić, N., & Alhudaidi, I. (2023). The importance of information security for organizations. Serbian Journal of Engineering Management, 8(2), 48–53. https://doi.org/10.5937/sjem2302048j

Jimenez, M. B., & Fernandez, D. (2022). A Framework for SDN Forensic Readiness and Cybersecurity Incident Response. 2022 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN 2022 - Proceedings, 112–116. https://doi.org/10.1109/NFV-SDN56302.2022.9974648

Juledi, A. P., Huda, M. K., Putra, M. T. D., Samsumar, L. D., Adi, P. D. P., & Nurdiansyah, Y. (2024, November). Performance Evaluation of LoRa 923 MHz for the Internet of Things. In 2024 IEEE 10th Information Technology International Seminar (ITIS) (pp. 30-34). IEEE.

Juliharta, I. G. P. K., Adrian, A., & Erawan, A. P. D. (2024). Buku Keamanan Siber: Esensi Keamanan Sistem Informasi.

Kadek Rima Anggen Suari, I Made Sarjana, Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia, 2023, Vol. 6 No. 1 April 2023, 132-146

Kamariotou, M., & Kitsios, F. (2023). Information systems strategy and security policy: A conceptual framework. Electronics, 12(2), 382.

Kaspersky. (2021). Lojax: The First UEFI Rootkit Detected in the Wild. Kaspersky Lab.

Kaur, J., & Arora, A. (2016). Security testing of web applications: Issues and challenges. International Journal of Computer Applications, 144(6), 28–33.

Kementerian Komunikasi dan Informatika Republik Indonesia, 2014, Panduan Penangan Insiden Keamanan Database, BPPT CSIRT.

Komalasari, R., Widians, J. A., Meilani, B. D., Arifin, N. Y., Sepriano, S., Syam, S., ... & Darwin, D. (2023). Pengantar Ilmu Komputer: Teori Komprehensif Perkembangan Ilmu Komputer Terkini. PT. Sonpedia Publishing Indonesia.

Kumar, S., & Lee, J. (2021). Security Challenges in IoT Devices: A Review and Future Directions. Journal of Cybersecurity Research, 18(2), 120-135.

Kwon, H., Shin, Y.-J., Jeong, J., Kim, K., & Shin, D. (2022). Measures to Ensure the Sustainability of Information Systems in the COVID-19 Environment. Sustainability, 15(1), 35. https://doi.org/10.3390/su15010035

Laudon, K. C., & Laudon, J. P. (2021). Management Information Systems: Managing the Digital Firm (16th ed.). Pearson.

Lukman Medriavin Silalahi, Simanjuntak, I.U.V. and Rochendi, A.D. (2023) 'Internet of Things Education Teaching and Learning Centre Harapan Bunda School Jakarta', ABDIMAS: Jurnal Pengabdian Masyarakat, 6(4 SE-Articles), pp. 4439–4448. Available at: https://doi.org/10.35568/abdimas.v6i4.3862.

McClure, S., Scambray, J., & Kurtz, G. (2009). Hacking exposed web applications: Web application security secrets & solutions (3rd ed.). McGraw-Hill.

McKinsey & Company. (2021). The Future of Cybersecurity in the Cloud Era. https://www.mckinsey.com

Menezes, A. J., Orschot, P.C. dan Vanstone, S.A., 1996, Handbook of Applied Cryptography, Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

Michael, E. W., & Herbert, J. M. (2021). Principles of Information Security, Seventh Edition (7th ed.). Cengage Learning, Inc.

Milan, R. M. S., & Rochmadi, T. (2024). Analisis dan Monitor Sniffing Paket Data Jaringan Lokal dengan Network Analyzer Wireshark.

CyberSecurity Dan Forensik Digital, 6(2), 62–68. https://doi.org/10.14421/csecurity.2023.6.2.4279

Mirkovic, J., & Reiher, P. (2020). Intrusion Detection and Prevention Systems: The Evolution of Cybersecurity Defense. MIT Press.

Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. Wiley.

MKovba, D.M. and Moiseenko, Y.Y. (2021) 'The Digital Society in the 21st Century: Security Issue', KnE Social Sciences [Preprint]. Available at: https://doi.org/10.18502/kss.v5i2.8387.

Mpungu, C., George, C., & Mapp, G. (2024). Digital Forensics Readiness in Big Data Wireless Networks: A Novel Framework and Incident Response Script for Linux-Hadoop Environments. https://doi.org/10.20944/preprints202407.1803.v1

Mustafovski, R. (2023). Ensuring information security in the digital age. https://doi.org/10.46763/etima2321119m

National Institute of Standards and Technology (NIST). (2022). Zero Trust Architecture Guidelines. Retrieved from https://www.nist.gov/cyberframework.

NIST. (2020). Zero Trust Architecture (Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Nugroho, M. A. (2019). Keamanan Aplikasi Mobile: Perlindungan Data dan Privasi dalam Dunia Digital. Andi.

Nugroho, S. A., & Rochmadi, T. (2024). Analisis Keamanan Sistem Informasi Pusaka Magelang Menggunakan Open Web Application Security Project (OWASP) dan Information Systems Security Assessment Framework (ISSAF). CyberSecurity Dan Forensik Digital, 7(1), 56–61. https://doi.org/10.14421/csecurity.2024.7.1.4555

Nugroho, S., & Rochmadi, T. (2024). Analysis of Information Security Readiness Using the Index KAMI. DECODE: Jurnal Pendidikan Teknologi Informasi, 4(3), 881–886. https://doi.org/10.51454/decode.v4i3.602

Nurindahsari, F., & Zen, B. P. (2021). Analisis Statik Keamanan Aplikasi Video Streaming Berbasis Android Menggunakan Mobile Security Framework (MobSF) Security Static Analysis Of Android-Based Video Streaming Application Using Mobile Security Framework (MobSF). CyberSecurity Dan Forensik Digital, 4(2), 2615–8442. https://databoks.katadata.co.id

O'Brien, J. A., & Marakas, G. M. (2020). Introduction to Information Systems (17th ed.). McGraw-Hill.

Oktarino, A., Iqbal, M., Apriyanti, L., Fahnun, B. U., Rakhmawati, S., Nurhayati, S., ... & Alam, S. N. (2024). Konsep Manajemen Proyek Sistem Informasi. CV. Gita Lentera.

OpenAI. (2025). ChatGPT (GPT-4), versi 2025.04.20 [Model bahasa besar]. Diakses pada 20 April 2025, dari https://chat.openai.com

Organizational Architecture, Resilience, and Cyberattacks. (2022). IEEE Transactions on Engineering Management, 69(5), 2218–2233. https://doi.org/10.1109/tem.2020.3004610

OWASP Foundation. (2021). OWASP Top Ten Web Application Security Risks. https://owasp.org/www-project-top-ten/

Palmer, D. (2022). The Evolution of Ransomware Attacks and Countermeasures. Cybersecurity Journal, 29(3), 45-67.

PCI Security Standards Council. (2022). Payment Card Industry Data Security Standard (PCI DSS) v4.0 (pp. 169-189). PCI SSC.

Pearlson, K. E., Saunders, C. S., & Galletta, D. F. (2020). Managing and Using Information Systems: A Strategic Approach (7th ed.). Wiley.

Pericherla, S. (2025, January 30). Introduction to Digital Forensics. Startertutorials.

https://www.startertutorials.com/blog/introduction-to-digital-forensics.html

Pooe, E. A. (2018). Developing a Multidisciplinary Digital Forensic Readiness Model for Evidentiary Data Handling.

Pratama, A. D. (2018). Bring Your Own Device (BYOD): Tantangan dan Solusi dalam Keamanan Perangkat Perusahaan. Gramedia.

Raharjo, Budi. (2021). Keamanan Sistem Informasi. Jakarta: Yayasan Prima Agus Teknik.

Rainer, R. K., & Cegielski, C. G. (2022). Introduction to Information Systems: Supporting and Transforming Business (8th ed.). Wiley.

Riadi, I., & Bashor, F. M. (2022). Digital Forensik (Forensik Email). Penerbit Diandra.

Riadi, I., & Ruslan, T. (2023). Analisis Forensik Digital pada Whatsapp dan Facebook Menggunakan Metode NIST. Jurnal Fasilkom, 13.

Rochmadi, T. (2018). Live Forensik untuk Analisa Anti Forensik pada Web Browser Studi Kasus Browzar. Indonesian Journal of Business Intelligence, 1(1), 32–38. https://doi.org/10.21927/ijubi.v1i1.878

Rochmadi, T. (2019). Deteksi Bukti Digital pada Adrive Cloud Storage Menggunakan Live Forensik. Cyber Security Dan Forensik Digital , 2(2), 65–68. https://doi.org/10.14421/csecurity.2019.2.2.1455

Rochmadi, T., & Pasa, I. Y. (2021). Pengukuran Risiko dan Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi di BKD XYZ Berdasarkan ISO 27001 / SNI. CyberSecurity Dan Forensik Digital, 4(1), 38–43. https://doi.org/10.14421/csecurity.2021.4.1.2439

Rochmadi, T., Fadlil, A., & Riadi, I. (2024). Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital. CyberSecurity Dan Forensik Digital, 7(2), 81–89. https://doi.org/10.14421/csecurity.2024.7.2.4861

Rochmadi, T., Wicaksono, Y., & Nisa, N. D. (2020). Digital Evidence Identification of Android Device using Live Forensics Acquisition on Cloud Storage (iDrive). International Journal of Computer Applications, 175(26), 40–43. https://doi.org/10.5120/ijca2020920815

Romindo, R., Suradi, A., Yusnanto, T., Altin, D., Boari, Y., ., Barlian, A., & Judijanto, L. (2024). E-COMMERCE DAN E-BUSINESS: Konsep dan Implementasi. Yayasan Literasi Sains Indonesia.

Ross, R., et al. (2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53.

Rouse, M. (2020). Privilege escalation. TechTarget – SearchSecurity. https://www.techtarget.com/searchsecurity/definition/privilege-escalation

Sadikin, R., 2012, Kriptografi untuk Keamanan Jaringan, Penerbit ANDI, Yogyakarta.

Samsumar, L. D., & Gunawan, K. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi Kasus Di Kampus Stmik Mataram. Jurnal Ilmiah Teknologi Infomasi Terapan, 4(1).

Santoso, E. (2021). Keamanan Jaringan dan Mobile: Mengelola Risiko dalam Sistem dan Perangkat Mobile. Salemba Empat.

Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (IDPS) (Special Publication 800-94). National Institute of Standards and Technology (NIST).

Schneier, B. (2015). Secrets and Lies: Digital Security in a Networked World. Wiley.

Schneier, B. (2023). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

Schneier, B. (2023). Secrets and Lies: Digital Security in a Networked World. Wiley.

Setiawan, D., Maulani, G., Abdillah, Sukoco, B., Yusnanto,T., Monita, V., & Sintong, P., S. ,. D. ,. (2025). BLOCKCHAIN (1st ed.). CV.

Sharma, S., & Kalra, S. (2020). Blockchain-based security architecture for the Internet of Things: A comprehensive review. Computer Communications, 154, 361-380. https://doi.org/10.1016/j.comcom.2020.03.004

Sheunesu, M. M. H. S. V., Victor, R. K., Richard, A. I., & Nickson, M. K. (2020). Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes. IEEE Xplore, 200–205. https://doi.org/10.1109/ICIoT48696.2020.9089494

Shukla, A., Katt, B., Nweke, L. O., Yeng, P. K., & Weldehawaryat, G. K. (2022). System security assurance: A systematic literature review. Computer Science Review, 45, 100496.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Silalahi, L.M. and Kurniawan, A. (2023) 'Analisis Keamanan Jaringan Menggunakan Intrusion Prevention System (Ips) Dengan Metode Traffic Behavior', Electrician: Jurnal Rekayasa dan Teknologi Elektro, 17(1), pp. 71–76.

Silalahi, L.M. et al. (2024) 'Smart Home Control System Design using Internet of Things Based Energy Harvesting Technology', in 2024 IEEE 6th Symposium on Computers & Informatics (ISCI). IEEE, pp. 43–48. Available at: https://doi.org/10.1109/ISCI62787.2024.10667797.

Silalahi, L.M., Ikhsan, M., et al. (2022) 'Designing a Thief Detection Prototype using Banana Pi M2+ Based Image Visual Capture Method and Email Notifications', in 2022 5th International Conference of Computer and Informatics Engineering (IC2IE), pp.

293–296. Available at: https://doi.org/10.1109/IC2IE56416.2022.9970065.

Silalahi, L.M., Jatikusumo, D., et al. (2022) 'Internet of things implementation and analysis of fuzzy Tsukamoto in prototype irrigation of rice', International Journal of Electrical and Computer Engineering (IJECE), 12(6), p. 6022. Available at: https://doi.org/10.11591/ijece.v12i6.pp6022-6033.

Silalahi, L.M., Rochendi, A.D. and Simanjuntak, I.U.V. (2024) 'Perancangan Kendali Filter Air Tanah Berbasis Logika Fuzzy dan Pemantauan Kondisinya Menggunakan Platform IoT', JTERA (Jurnal Teknologi Rekayasa), 8(2), pp. 199–208. Available at: https://doi.org/10.31544/jtera.v8.i2.2023.199-208.

Simao, J., et al. (2018). Penetration testing in web applications: A systematic mapping study. Journal of Information Security and Applications, 43, 78–95. https://doi.org/10.1016/j.jisa.2018.09.003 (tambahkan DOI jika tersedia)

Singh, A., Ikuesan, R. A., & Venter, H. (2022). Secure Storage Model for Digital Forensic Readiness. IEEE Access, 10, 19469–19480. https://doi.org/10.1109/ACCESS.2022.3151403

Somepalli, S. H., Tangella, S. K. R., & Yalamanchili, S. (2020). Information Security Management. 11(2), 1–16. https://doi.org/10.2478/HJBPA-2020-0015

Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, 305–316. https://doi.org/10.1109/SP.2010.25

Stair, R. M., & Reynolds, G. W. (2021). Principles of Information Systems (14th ed.). Cengage Learning.

Stallings, W. (2013). Cryptography and Network Security: Principles and Practice. (1st ed.). Prentice Hall Press.

Stallings, W. (2018). Computer Security: Principles and Practice. Pearson.

Stallings, W. (2020). Cryptography and Network Security: Principles and Practice. Pearson.

Symantec. (2021). Internet Security Threat Report. Broadcom Inc. https://symantec-enterprise-blogs.security.com

Thron, R., Dirnberger, H., Tjoa, S., & Quirchmayr, G. (2022). Requirements and Challenges for Digital Forensic Readiness in Industrial Automation and Control Systems. ACM International Conference Proceeding Series, 232–238. https://doi.org/10.1145/3524338.3524374

Turban, E., Pollard, C., & Wood, G. (2022). Information Technology for Management: On-Demand Strategies for Performance, Growth and Sustainability (12th ed.). Wiley.

Valacich, J., & Schneider, C. (2022). Information Systems Today: Managing the Digital World (9th ed.). Pearson.

Weske, M. (2020). Business Process Management: Concepts, Languages, Architectures (3rd ed.). Springer.

West, J., & Zeng, X. (2016) "Bring Your Own Device (BYOD): A Survey of Security Issues and Solutions," International Journal of Computer Science and Information Security, 14(8), 312-320.

Windyasari, V. S. et al. (2024) Pengenalan Sistem Informasi Secara Umum. Jakarta: PT. Hadla Media Informasi, pp. 54-57.

Wulandari, I. et al. (2021) 'Studi Literatur Review : Integrasi Kurikulum Pembelajaran Cerdas Biosensor Menggunakan Teknologi Internet of Things', Jurnal Tiarsie, 18(3), pp. 97–102. Available at: https://doi.org/10.32816/tiarsie.v18i3.109.

Xu, L.D. (2020) 'The contribution of systems science to Industry 4.0', Systems Research and Behavioral Science, 37(4), pp. 618–631. Available at: https://doi.org/10.1002/sres.2705.

Yudhana, A., Riadi, I., & Yudhi Prasongko, R. (2022). Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS). Jurnal Informatika: Jurnal Pengembangan IT (JPIT), 7(1).

Yusnanto, T., Machmudi, M. A., & Mustofa, K. (2019). PENGARUH KERUSAKAN PERANGKAT PENYIMPANAN HARDISK DAN FLASHDISK TERHADAP VIRUS KASPERSKY INTERNET SECURITY. 15(2).

Yusnanto, T., Muin, M. A., & Mustofa, K. (2025). Data Security Analysis on the Use of E-Commerce to Prevent Online Fraud. 4.

Zebari, D. A., & Asaad, R. R. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. Applied Computing Journal, 227–244. https://doi.org/10.52098/acj.202260

Zetter, K. (2019). Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown.

TENTANG PENULIS

Lalu Delsi Samsumar, M.Eng.

Seorang penulis dan dosen tetap Prodi Teknologi Informasi pada Universitas Teknologi Mataram. Lahir di Lombok Tengah, 43 tahun lalu. Penulis merupakan anak Keempat dari empat bersaudara. Pendidikan yang telah ditempuh program Sarjana (S1) Universitas Mataram dan Program Pasca Sarjana (S2) di Universitas Gadjah Mada pada Program Magister Teknologi Informasi (MTI). Penulis telah menulis dan menerbitkan beberapa buku semenjak tahun 2023. Berikut judul buku yang telah ditulis dan terbitkan: Pengantar Ilmu Komputer : Teori Komprehensif Perkembangan Ilmu Komputer Terkini (2023), Konsep Manajemen Proyek Sistem Informasi (2024), Jaringan Komputer (2024), dan Keamanan Informasi : Strategi dan Teknik Perlindungan (2025.

Siti Nasiroh, M.Kom..

Adalah dosen tetap Prodi Informatika pada Fakultas Sains dan Teknik Universitas Perwira Purbalingga. Lahir di Banyumas, 14 Desember 1971. Pendidikan telah ditempuh program Sarjana (S1) manajemen informatika pada STIMIK Tasikmalaya dan Program Pasca Sarjana (S2) di Universitas Islam Indonesia Teknik Informatika. Berikut judul buku yang telah ditulis dan terbitkan: Interaksi Manusia dan Komputer dan Metodologi Penelitian Teknologi Informasi.

Miswadi, S.Kom., M.Kom.

Miswadi *"Mas Raden"* Lahir di Kota Gombong - Kebumen pada bulan Mei 1975. Tamat dari sekolah STM Wongsorejo Gombong – Kebumen Jurusan Listrik Instalasi tahun 1994 dan menyelesaikan program Studi Diploma III (D3) Teknik Komputer Di STMIK Bani Saleh Bekasi tahun 2000. Dan tahun 2006 melanjutkan Program Studi S1 Jurusan Teknik Informatika (S.Kom) selesai Tahun 2008 di STMIK Bani Saleh Bekasi. Pada tahun 2012 melanjutkan studi Magister Ilmu Komputer (S2) di Universitas Budi Luhur Jakarta dan selesai pada tahun 2015.

Tahun 1994 ~ 2000 bekerja di perusahaan Indomobil Group sebagai Quality Assurance dan terakhir sebagai staf personalia. Saat ini sedang bekerja pada salah satu perusahaan Manufacture di Cikarang, Bekasi tepatnya pada PT Kiyokuni Indonesia sebagai IT Departement Head yang bertanggung jawab menangani Sistem Jaringan, Hardware, Software, Aplikasi Database dan Server (Email, Proxy, VPN, Firewall & Proxy). Tahun 2011 mengaplikasikan pengalaman di dunia industri dengan menjadi tenaga pengajar SMK jurusan TKJ dan Dosen di STMIK, Politeknik di Bekasi.

Konsentrasi Inti pada bidang jaringan komputer, infrastruktur dan Network/Database, serta menagani Server dengan Platform Microsoft dan Unix (GNU – Linux), dan pengembangan teknologi dan aplikasi untuk perusahaan manufaktur. Juga aktif dalam, komunitas IT, organisasi keagamaan dan kegiatan sosial lainnya. Mempunyai Hobby "Jalan-jalan", membaca, jogging. Senang membantu dan berdiskusi tentang Agama Islam, bidang komputer dan perkembangan teknologi informasi. Informasi lebih lanjut mengenai penulis dapat dilihat pada: E-Mail: miswadi@kiyokuni.co.id, miswadi@gmail.com

Salman Farizy. S.Kom, M.Kom, MCSE, MVP

Menyelesaikan pendidikan dasar dan menengah di SDN 01 Cipinang Besar, SMPN 25 Cipinang Muara Jakarta Timur dan SMAN 91 Pondok Kelapa Jakarta Timur, sedangkan untuk perguruan tinggi Strata satu (S1) di Universitas Gunadarma dan Pasca Sarjana di STMIK Eresha yang saat ini sudah merger atau bergabung dengan Universitas Pamulang, penulis sempat bekerja dibeberapa perusahaan asing dan juga lokal seperti Mattel Indonesia, Frigorex Indonesia, Kaltimex Energy, Microsoft Gold Partner, IT Consultant (partime) dan akhirnya memutuskan untuk menjadi Dosen tetap Universitas Pamulang. Mudah-mudahan dengan adanya buku ini akan menambah pengetahuan dan dapat bermanfaat tertutama buat adik-adik mahasiswa yang hobi mengexplore dan mencoba hal–hal yang baru.

Ir. Chairul Anwar, S.Kom., M.Kom., CITPM

Ir. Chairul Anwar, S.Kom., M.Kom., CITPM adalah seorang akademisi, praktisi, dan penulis di bidang Teknologi Informasi. Saat ini, beliau menjabat sebagai Presiden Direktur PT Teknologi Informatika Solusindo serta merupakan dosen tetap di Universitas Pamulang. Dengan pengalaman luas sebagai konsultan IT dan pengembang produk teknologi, beliau memiliki keahlian dalam manajemen proyek perangkat lunak, arsitektur IT, serta inovasi teknologi di era digital. Lahir di Jakarta, beliau menempuh pendidikan Sarjana (S1) di Universitas Pamulang, Program Studi Teknik Informatika, kemudian melanjutkan pendidikan Magister (S2) di universitas yang sama dalam

bidang Teknik Informatika. Selain itu, beliau juga menyandang gelar Insinyur (Ir.) dari Institut Teknologi Indonesia, yang semakin memperkuat kompetensinya dalam bidang rekayasa dan teknologi. Sebagai seorang profesional bersertifikasi Certified IT Project Manager (CITPM), beliau aktif dalam berbagai penelitian, seminar, serta pengembangan teknologi yang mendukung transformasi digital di industri dan akademik. Selain mengajar dan berkarier di dunia industri, beliau juga aktif menulis buku dan karya ilmiah. Beberapa buku yang telah diterbitkan antara lain "Manajemen Proyek Perangkat Lunak dengan Studi Kasus Microsoft Project" dan "Inovasi Teknologi dan Sistem Informasi dalam Transformasi Digital". Dengan pengalaman dan dedikasinya di bidang teknologi informasi, Ir. Chairul Anwar terus berkontribusi dalam dunia pendidikan serta industri teknologi dengan visi menciptakan solusi inovatif yang berdampak luas bagi masyarakat..

Imam Halim Mursyidin, S.Kom., M.Kom.

Seorang penulis dan dosen Prodi Sistem Informasi pada Universitas Islam Syekh Yusuf Tangerang. Pendidikan telah ditempuh program Sarjana (S1) Universitas Budi Luhur Prodi Sistem Informasi dan Program Pasca Sarjana (S2) di Universitas Budi Luhur prodi Ilmu Komputer. Selain itu penulis bekerja sebagai praktisi IT Auditor, *Compliance* dan *Risk* management di perusahaan swasta bidang *financial technology*. Dengan pengalaman lebih dari 7 tahun di bidang ini, penulis telah menggabungkan pengetahuan akademis dan praktisi untuk memberikan wawasan yang mendalam tentang pentingnya keamanan informasi dalam era digital. Sebagai IT Auditor penulis memiliki pengalaman langsung dalam menerapkan dan mengaudit sistem manajemen keamanan informasi yang dihadapi organisasi.

Roynaldy Rosdiyanto, M.Kom

Seorang penulis dan dosen tetap Prodi Sistem Informasi pada Universitas Bina Sarana Informatika. Pendidikan yang telah ditempuh Program Sarjana (S1) di Universitas Budi Luhur Prodi Sistem Informasi dan Program Pasca Sarjana (S2) di Universitas Budi Luhur Prodi Ilmu Komputer. Selain itu penulis juga bekerja sebagai praktisi di sebuah perusahaan swasta bidang Software Developer dan IT Consultant. Dengan pengalaman lebih dari 7 tahun dibidang pengembangan software developer, penulis telah menggabungkan pengetahuan akademis dan praktisi untuk memberikan wawasan yang mendalam tentang pentingnya keamanan informasi dalam era digital.

Wahyu Wijaya Widiyanto, M.Kom.

adalah seorang dosen tetap pada Program Studi Manajemen Informasi Kesehatan di Politeknik Indonusa Surakarta. Beliau menyelesaikan pendidikan Sarjana (S1) di STMIK Duta Bangsa pada tahun 2016 dan meraih gelar Magister Komputer (S2) dari Universitas Amikom Yogyakarta pada tahun 2019. Sebagai akademisi, beliau memiliki minat penelitian dalam bidang sistem informasi, big data, dan data mining. Beliau telah menerbitkan lebih dari 30 publikasi ilmiah yang telah dibaca sebanyak 17.917 kali dan mendapatkan 192 sitasi. Selain itu, beliau juga aktif dalam kegiatan pengabdian masyarakat, seperti pelatihan pembuatan media pembelajaran video asinkron untuk peningkatan pembelajaran daring.

Prayogo, S.Kom., M.Kom

Penulis lahir di Purworejo, Jawa Tengah bulan Juli 1972. Penulis menamatkan pendidikan dasar dan menengah di Purworejo , setelah lulus dari SMK , hijrah ke Tangerang bekerja sebagai Riset Development dan kemudian sambil melanjutkan kuliah S1 di STMIK Masa Depan Cimone Tangerang Jurusan Teknik Informatika, kemudian melanjutkan S2 di STMIK Eresha Jakarta, yang kemudian merger dengan Universitas Pamulang Jakarta Program studi Magister Teknik Informatika. Memulai mengajar Tahun 2013 menjadi pengajar Tidak tetap di Amik MAPAN dan STMIK Masa Depan yang hingga saat ini menjadi Dosen Tetap di AMIK MAPAN Kota Tangerang . Penulis juga mempunyai pengalaman mengajar di beberapa kampus yaitu, Institute Global Tangerang, UTPAS di kota Tangerang, Mengajar di Kampus LP3i Cimone Tangerang, selain itu juga mengajar di STBA Teknocrat Cikupa Kabupaten Tangerang. Selain itu Penulis pernah mengajar di Program Prakerja Pemerintah di LPK Geti Serpong sebagai LPK yang ditunjuk Pemerintah.Penulis juga menulis di blog : https://e-prayogo.blogspot.com/ . Dan juga mempunyai channel youtube : https://youtu.be/E7FOhPkbFqw?si=Jajc5gGwO5ZnTmd_Dan instagram:https://www.instagram.com/surya_prayogo.official?igsh=aW40MGY4MWRobDk3

Richky Mukin , MCT , MM

Richky Mukin adalah seorang profesional IT Security dan Project Manager dengan pengalaman lebih dari 20 tahun di bidang manajemen keamanan informasi, tata kelola TI, dan implementasi standar internasional. Beliau memiliki sertifikasi internasional yang diakui di bidangnya, termasuk:

- ISO/IEC 27001 Lead Auditor/Implementer (Spesialis Sistem Manajemen Keamanan Informasi).
- ISO/IEC 20000 Lead Auditor (Spesialis Manajemen Layanan TI).
- Microsoft Certified Trainer (MCT) untuk solusi keamanan dan infrastruktur TI.

Pengalaman Profesional:

1. Konsultan IT Security & ISO Standards
    - Memimpin implementasi ISO 27001 dan ISO 20000 di berbagai organisasi, termasuk sektor perbankan, telekomunikasi, dan pemerintahan di Indonesia.
    - Membantu klien dalam penyusunan kebijakan keamanan informasi, manajemen risiko, dan compliance dengan regulasi seperti UU PDP Indonesia.
    - Melakukan audit dan gap analysis untuk memastikan kesesuaian dengan standar internasional.
1. Project Manager
    - Mengelola proyek transformasi digital dengan fokus pada keamanan siber, migrasi cloud, dan tata kelola TI.
    - Berpengalaman dalam mengintegrasikan kerangka kerja ITIL, COBIT, dan NIST CSF dengan standar ISO.
2. Edukator & Pembicara
    - Dosen tamu dan pelatih untuk topik keamanan informasi di universitas dan lembaga sertifikasi.

Tri Yusnanto, M.Kom.

Penulis lahir di Magelang tanggal 02 Agustus 1983. Penulis merupakan dosen tetap pada Yayasan pada Program Studi Manajemen Informatika, STMIK Bina Patria. Penulis menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika sekitar tahun 2009 lulus pada tahun 2013 kemudian melanjutkan studi S2 Teknik Informatika di Universitas Amikom Yogyakarta Lulus pada tahun 2017. Penulis menekuni bidang informatika selain itu penulis juga aktif diberbagai keanggotaan pendidikan dalam karirnya sebagai pengajar penulis juga menerbitkan berbagai jurnal tentang teknologi dan juga informatika, selain itu penulis juga beberapakali ikut dalam kolaborasi penulisan buku baik dibidang pendidikan atau pun dibidang informatika.

Ir. Lukman Medriavin Silalahi, A.Md., ST., MT., IPM., APEC-Eng

Lukman Medriavin Silalahi memperoleh gelar Magister Teknik Elektro dari Universitas Mercu Buana pada tahun 2019 dan melanjutkan pendidikan sekolah Doktor (S3) di Departemen Teknik Elektro Universitas Indonesia pada tahun 2024 hingga buku ini diterbitkan. Beliau juga telah memperoleh sertifikasi IPM (Insinyur Profesional Madya) yang diperoleh dari PII (Persatuan Insinyur Indonesia) dan juga memperoleh pengakuan sebagai APEC-Engineer pada *International Engineering Alliance*. Saat ini, kepangkatan Dosen berada pada tingkat Lektor dengan KUM (300) dan ditempatkan sebagai Dosen Tetap di Program Studi Informatika, Universitas Siber Asia. Beliau juga telah berhasil mempublikasikan sebanyak 42 artikel ilmiah

sebagai penulis pertama atau co-author pada jurnal maupun konferen internasional bereputasi terindeks Scopus. Selain itu, kegiatan beliau sebagai anggota dari IEEE Communications Society Indonesia Chapter. Penelitian beliau antara lain: Keamanan Jaringan (Network Security), Teknik Telekomunikasi (Telecommunication Engineering), Rekayasa Lalu Lintas Telekomunikasi (Telecommunication Traffic Engineering), Teknik Sistem Kendali (Control System Engineering), dan Wireless-IoT (Internet of Things).

A.Taqwa Martadinata, M.Kom.

Seorang penulis dan dosen tetap Prodi Informatika pada Universitas Bina Insan. Lahir di Lubuklinggau, 14 Oktober 1995. Penulis merupakan anak Keempat dari empat bersaudara dari pasangan Bapak Muchtar Bastari dan Ibu Hindun Nurbaya. Pendidikan telah ditempuh program Sarjana (S1) STMIK Musirawas Prodi Tekni Informatika dan Program Pasca Sarjana (S2) di Universitas Bina Darma prodi Teknik Informatika. Penulis memiliki dua (1) buah hati Mush'ab Abdullah Taqwa dari pasangan Khoirun Nisa (Ummah Nisa). Berikut judul buku yang telah ditulis dan terbitkan: Sistem informasi geografis berbasis android : studi kasus aplikasi SIG pariwisata, Perancangan Enterprise Architecture Teknologi Informasi Adaptif dan Sistem Informasi Geografis dengan PHP Native & Leafleat.JS Berbasis Web Mobile (Studi Kasus : Sebaran Data Program Keluarga Harapan).

Tri Rochmadi, M.Kom., CSCU., CEI., CIISA

Seorang penulis dan dosen tetap Prodi Sistem Informasi di Universitas Alma Ata. Pendidikan telah ditempuh program Sarjana (S1) STMIK El Rahma Yogyakarta jurusan Teknik Informatika, (S2) di Universitas Islam Indonesia prodi Informatika, dengan konsentrasi adalah forensik digital. Penulis saat buku ini ditulis sedang menjalani proses doktoral (S3) di Universitas Ahmad Dahlan prodi Informatika dengan peminatan Digital Forensics. Berikut judul buku yang telah ditulis dan terbitkan: Menulis dan Mempublikasikan Artikel di Jurnal Nasional: Panduan untuk Guru dan Dosen Pemula, Internet Marketing for Your Business, Penerapan Teknologi Informasi Di Berbagai Sektor, Mengenal Jogja: Spirit Edukasi Seni & Budaya. Selain aktif menulis buku, penulis juga memiliki portal berita untuk dunia kampus dengan website campusqu.com.

Dede Irawan, M.Kom.

Seorang software engineer dan dosen tetap Prodi Bisnis Digital pada Universitas Islam Syekh Yusuf Tangerang. Lahir di Jakarta, 28 Juni 1993. Pendidikan yang telah ditempuh program Sarjana (S1) Universitas Budi Luhur Prodi Teknik Informatika dan Program Pasca Sarjana (S2) di Universitas Budi Luhur prodi Teknologi Sistem Informasi. Penulis juga merupakan pemilik dari Digital Agency yang bernama nanproject.my.id.

Doni Prastyo, S.Kom., M.Kom.

Seorang penulis dan dosen tetap Prodi Teknik Informatika pada Universitas Islam Syekh Yusuf Tangerang. Lahir di Blora, 22 Oktober 1993. Penulis menyelesaikan pendidikan Sarjana (S1) di Universitas Islam Syekh Yusuf Tangerang, Program Studi Teknik Informatika, dan kemudian meraih gelar Magister (S2) di program Ilmu Komputer di Universitas Budiluhur Jakarta. Selain mengajar, penulis memiliki pengalaman praktis dalam dunia pengembangan perangkat lunak, khususnya dalam penguasaan bahasa pemrograman web (PHP, Javascript), mobile (flutter) dan juga IOT.