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:

978-623-10-9466-7

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

taruhannya. Kepercayaan publik yang rusak seringkali sulit untuk dipulihkan dan berdampak jangka panjang.

Ilustrasi:

Serangan ransomware terhadap perusahaan logistik internasional menyebabkan penghentian operasi selama 5 hari dan kerugian hingga jutaan dolar, disertai turunnya nilai saham secara drastis.

c. Memenuhi regulasi dan kepatuhan hukum (seperti UU PDP, GDPR)
d. Menjaga keberlanjutan layanan digital

4. Studi Kasus Relevan: Tokopedia (2020)

Pada Mei 2020, terjadi kebocoran data dari platform e-commerce Tokopedia, di mana lebih dari 91 juta akun pengguna terekspos, termasuk nama lengkap, email, dan hash password. Meskipun data tidak langsung digunakan untuk serangan, insiden ini mengungkap pentingnya:

a. Perlindungan integritas dan kerahasiaan data pengguna
b. Keamanan database dan sistem autentikasi
c. Kesadaran pengguna terhadap keamanan akun pribadi

5. Ilustrasi Visual (Disarankan Ditambahkan ke Buku)

Untuk memperkuat pemahaman pembaca, visual berikut bisa ditambahkan:

1. Diagram Blok Sistem Informasi: Menunjukkan alur input → proses → output → feedback
2. Gambar CIA Triad dalam bentuk segitiga berwarna
3. Contoh Flowchart Serangan dan Proteksi (misalnya bagaimana enkripsi melindungi email).

6. Tantangan dalam Keamanan Sistem Informasi Modern

Beberapa tantangan yang dihadapi organisasi dalam menjaga keamanan sistem informasi:

a. Kompleksitas sistem yang terus bertambah
b. Ancaman yang semakin canggih (misalnya APT dan *ransomware-as-a-service)*
c. Minimnya kesadaran keamanan pada pengguna akhir
d. Kurangnya anggaran dan tenaga ahli

C. MENGAPA KEMANAN SISTEM INFORMASI PENTING?

Di era digital yang terkoneksi secara masif, keamanan sistem informasi bukan lagi pilihan, melainkan keharusan. Keamanan bukan hanya sekadar memasang antivirus atau firewall, tapi mencakup kebijakan menyeluruh untuk menjaga aset digital dari ancaman yang terus berkembang.

1. Pentingnya Keamanan Informasi bagi Individu, Organisasi, dan Negara

- **Bagi Individu:**
  a. Menjaga privasi data pribadi (alamat, identitas, biometrik)
  b. Mencegah pencurian identitas digital
  c. Melindungi akun media sosial, email, dan finansial dari peretasan
- **Bagi Organisasi:**
  a. Menjaga kerahasiaan informasi bisnis (strategi, data pelanggan, R&D)
  b. Mematuhi regulasi hukum (GDPR, UU Perlindungan Data Pribadi)
  c. Mencegah kerugian finansial akibat serangan siber
- **Bagi Negara:**
  a. Menjaga sistem kritikal seperti pertahanan, energi, dan pemerintahan
  b. Melindungi data kependudukan dan e-government
  c. Mencegah cyberwar dan spionase digital

2. Dampak dari Pelanggaran Keamanan Informasi

Ketika sistem informasi tidak aman, risiko yang muncul bisa sangat luas dan serius, di antaranya:

Tabel 2. Contoh dampak dari Pelanggaran Keamanan Informasi

Jenis Dampak	Contoh Nyata
Finansial	Biaya pemulihan sistem, kehilangan transaksi, denda hukum
Reputasi	Hilangnya kepercayaan publik, pelanggan berhenti menggunakan layanan

Operasional	Gangguan operasional, downtime layanan, kehilangan data
Hukum dan Regulasi	Dikenai sanksi hukum, tuntutan hukum dari pengguna atau mitra bisnis
Psikologis dan Sosial	Ketakutan, ketidakpercayaan publik, penyebaran informasi palsu (hoax)

3. Studi Kasus Aktual: Serangan Siber pada BSSN & Kominfo (Indonesia, 2023)

Pada tahun 2023, Indonesia mengalami peningkatan tajam serangan siber yang menyasar lembaga strategis seperti Badan Siber dan Sandi Negara (BSSN) serta Kementerian Komunikasi dan Informatika (Kominfo). Serangan ini mengungkap beberapa kelemahan, antara lain:

a. Sistem pertahanan digital yang belum merata
b. Kurangnya integrasi dan koordinasi antarlembaga
c. Ketergantungan pada sistem legacy

👉 *Pelajaran: Keamanan sistem informasi harus menjadi agenda strategis nasional, bukan sekadar proyek teknis.*

4. Peran Strategis Keamanan Informasi dalam Keberlangsungan Organisasi

Organisasi modern dituntut untuk:

a. Menyusun kebijakan keamanan informasi *(Information Security Policy)*
b. Menerapkan manajemen risiko informasi
c. Melakukan audit dan evaluasi berkala
d. Melatih SDM melalui kesadaran keamanan siber *(security awareness)*

💪 *Tanpa strategi keamanan yang kuat, transformasi digital justru dapat menjadi bumerang.*

Gambar 1. 3. Siklus Serangan Siber

D. SEJARAH DAN EVOLUSI KEAMANAN INFORMASI

1. Masa Awal: Komunikasi Rahasia dan Kriptografi Klasik

Keamanan informasi bukanlah konsep baru. Jauh sebelum munculnya komputer, orang-orang telah berupaya menjaga kerahasiaan informasi.

Contoh awal:

a. **Kriptografi Caesar Cipher** – digunakan oleh Julius Caesar untuk menyandikan pesan militernya.
b. **Enigma Machine** – digunakan Nazi Jerman dalam Perang Dunia II, dan dipecahkan oleh Alan Turing dan timnya di Bletchley Park.

🔍 *Ciri khas era ini:* Keamanan informasi bersifat manual dan terbatas pada perlindungan komunikasi militer dan diplomatik.

2. Era Komputer (1950–1970): Awal Mula Isu Keamanan Digital

Dengan munculnya komputer mainframe, kebutuhan akan proteksi sistem mulai disadari. Di masa ini, tantangan utamanya adalah:

a. **Fisik**: Melindungi akses ke perangkat keras.
b. **Aksesibilitas**: Sistem komputer belum terkoneksi secara luas, sehingga ancaman masih bersifat lokal.

💡 *Contoh:* Sistem punch card dan terminal terbatas hanya bisa digunakan oleh orang tertentu dengan otorisasi fisik.

3. Era Jaringan (1980–1990): Kemunculan Ancaman Baru

Internet mulai diperkenalkan secara luas, dan sistem informasi menjadi terhubung secara global. Ini memunculkan:

a. Virus komputer pertama (Contoh: *Elk Cloner*, *Brain Virus*)
b. Peretasan jaringan kampus dan militer (misalnya kasus *Morris Worm* tahun 1988)

🔒 Di sinilah kebutuhan terhadap firewall, antivirus, dan metode otentikasi mulai berkembang secara lebih serius.

4. Era Globalisasi Digital (2000–2010): Regulasi dan Standarisasi

Pada masa ini, pelanggaran data mulai marak dan merugikan secara finansial. Muncul berbagai standar dan regulasi seperti:

a. ISO/IEC 27001 – standar sistem manajemen keamanan informasi
b. HIPAA (USA) – untuk perlindungan data kesehatan
c. PCI-DSS – standar keamanan untuk industri pembayaran kartu

📌 *Pergeseran paradigma*: Dari teknis → ke arah kebijakan dan tata kelola.

5. Era Transformasi Digital dan Cloud (2010–Sekarang): Tantangan Kompleks

Saat ini, ancaman keamanan semakin canggih, dan sistem informasi telah menyebar ke berbagai platform: mobile, cloud, IoT, bahkan AI.

⚠️ **Karakteristik ancaman modern:**

a. Serangan zero-day
b. Ransomware-as-a-service (RaaS)
c. Serangan social engineering canggih (spear phishing, deepfake)
d. Eksploitasi kerentanan API dalam sistem cloud

🛡️ **Respons organisasi modern:**

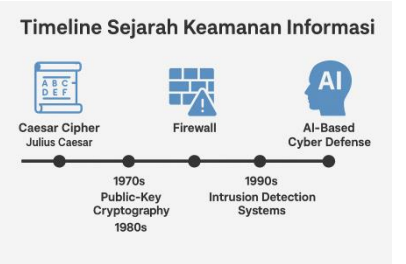
a. Penerapan *Zero Trust Architecture*
b. SIEM (Security Information and Event Management)
c. Tim Red Team dan Blue Team
d. Penggunaan AI dalam deteksi anomali keamanan

6. Studi Kasus Perbandingan: Dulu dan Sekarang

Tabel 3. Studi Kasus Perbandingan: Dulu dan Sekarang

Dulu (2000-an)	Sekarang (2020-an)
Firewall berbasis signature	Firewall berbasis AI dan threat intelligence
Password statis	Autentikasi multifaktor dan biometrik
Data di server internal	Data di cloud publik/hybrid dengan enkripsi kompleks
Serangan via email lampiran	Serangan via phishing berbasis deepfake & spoofing

7. Ilustrasi Visual yang Disarankan



Gambar 1. 6. Timeline sejarah keamanan informasi

E. TUJUAN DAN MANFAAT KEAMANAN SISTEM INFORMASI

1. Tujuan Keamanan Sistem Informasi

Secara umum, keamanan sistem informasi bertujuan untuk:

a. **Menjaga Kerahasiaan *(Confidentiality)***
Memastikan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Ini mencegah kebocoran data sensitif seperti informasi pribadi, rahasia bisnis, dan dokumen negara.

b. Menjaga Integritas *(Integrity)*
Melindungi informasi agar tetap akurat, konsisten, dan tidak dimodifikasi secara tidak sah, baik secara sengaja maupun karena kesalahan sistem.

c. Menjamin Ketersediaan *(Availability)*
Menjaga agar sistem, layanan, dan informasi tetap tersedia dan dapat diakses sesuai kebutuhan, kapan saja dan di mana saja.

📌 Tiga prinsip utama ini disebut **CIA Triad**, dan menjadi fondasi dalam semua praktik keamanan informasi.

d. Akuntabilitas *(Accountability)*
Menjamin bahwa setiap aktivitas dalam sistem dapat ditelusuri kembali ke individu atau proses tertentu. Ini penting dalam audit, investigasi insiden, dan tanggung jawab hukum.

e. **Non-Repudiation *(Non-penyangkalan)***
Memastikan bahwa seseorang tidak dapat menyangkal telah melakukan tindakan tertentu, seperti mengirim pesan atau melakukan transaksi digital. Biasanya melibatkan tanda tangan digital atau log sistem.

f. Keamanan Hukum dan Kepatuhan *(Compliance Security)*
Memenuhi kewajiban hukum dan regulasi, seperti GDPR, UU PDP, atau ISO 27001, agar organisasi tidak mendapat sanksi hukum.

2. Manfaat Keamanan Sistem Informasi
   a. Perlindungan terhadap Ancaman Siber

      Organisasi dapat mendeteksi dan mencegah malware, phishing, ransomware, dan berbagai jenis serangan siber lainnya.

   b. Kepercayaan Pelanggan dan Stakeholder

      Dengan menjaga privasi dan data pelanggan, organisasi membangun reputasi dan loyalitas yang kuat.

   c. Efisiensi Operasional dan Keberlanjutan Bisnis

      Keamanan sistem yang baik mencegah downtime dan mengurangi biaya pemulihan akibat insiden.

   d. Kepatuhan terhadap Regulasi dan Audit

      Menjamin kelayakan organisasi saat diaudit dan menjauhi risiko denda atau tuntutan hukum.

   e. Keunggulan Kompetitif

      Organisasi yang memiliki postur keamanan informasi yang baik sering dipilih oleh mitra bisnis sebagai rekanan terpercaya.

3. Contoh Kasus: Manfaat Nyata dalam Dunia Nyata

   Contoh 1: Perusahaan Fintech
   Sebuah startup fintech menerapkan keamanan berlapis termasuk enkripsi data, autentikasi biometrik, dan audit log. Ketika pesaing mengalami kebocoran data, startup ini justru mendapatkan kepercayaan investor dan mitra strategis.

   Contoh 2: Rumah Sakit Digital

Dengan mengimplementasikan standar HIPAA dan sistem backup otomatis, rumah sakit terhindar dari kerugian besar ketika terjadi serangan ransomware, karena sistem mereka cepat pulih dan pasien tetap dilayani.

F. RUANG LINGKUP KEANANAN SISTEM INFORMASI

1. Komponen-Komponen Utama Keamanan Informasi

Keamanan sistem informasi mencakup banyak elemen yang saling berkaitan. Secara umum, ruang lingkupnya dapat dibagi menjadi lima komponen utama:

a. **Keamanan Fisik (Physical Security)**
   Melindungi perangkat keras (server, router, storage) dari kerusakan, pencurian, atau akses fisik tidak sah.
   📌 *Contoh:* CCTV, kontrol akses ruang server, UPS, dan sistem proteksi kebakaran.

b. **Keamanan Jaringan (Network Security)**
   Melindungi lalu lintas data dari penyadapan, penyusupan, dan serangan siber melalui jaringan.
   📌 *Contoh:* Firewall, IDS/IPS, VPN, segmentasi jaringan.

c. **Keamanan Aplikasi (Application Security)**
   Menjamin bahwa perangkat lunak bebas dari celah keamanan atau kerentanan yang bisa dieksploitasi.
   📌 *Contoh:* Secure coding, pengujian penetrasi, pembaruan perangkat lunak berkala.

d. **Keamanan Data (Data Security)**
   Fokus pada perlindungan terhadap data itu sendiri, baik saat disimpan, diproses, maupun ditransmisikan.
   📌 *Contoh:* Enkripsi, masking data, tokenisasi, backup data.

e. **Keamanan Prosedural dan Kebijakan (Policy and Process Security)**
   Menetapkan aturan dan prosedur internal untuk memastikan praktik keamanan dilakukan secara konsisten.
   📌 *Contoh:* SOP keamanan, pelatihan SDM, kontrol akses berbasis peran.

2. Aspek-Aspek Pendukung dalam Keamanan Informasi

Selain aspek teknis, keamanan sistem informasi juga ditentukan oleh faktor-faktor berikut:

a. Manusia *(People)*

- Faktor manusia sering menjadi titik lemah dalam sistem keamanan (contoh: kesalahan pengguna, social engineering).
- Pelatihan, kesadaran, dan budaya keamanan digital sangat penting.

b. Proses *(Process)*

- Tata kelola keamanan yang sistematis, seperti audit berkala, dokumentasi SOP, dan tanggap darurat insiden siber.

c. Teknologi *(Technology)*

- Teknologi adalah alat bantu, namun tidak akan efektif jika tidak disertai proses dan budaya yang tepat.

3. Area Implementasi Keamanan Sistem Informasi

Untuk implementasi praktis, ruang lingkup keamanan dapat diaplikasikan pada beberapa area berikut:

Tebel 4. Area Implementasi Keamanan Sistem Informasi

Area	Fokus Keamanan
Infrastruktur TI	Jaringan, server, penyimpanan
Sistem Operasi	Patch keamanan, kontrol hak akses
Aplikasi dan Website	Validasi input, autentikasi, enkripsi
Mobile & IoT Devices	Aplikasi ringan, kontrol update, remote wipe
Cloud dan Virtualisasi	IAM cloud, proteksi API, backup multi-zona
Pengguna dan Karyawan	Pelatihan, kebijakan password, social engineering

G. ANCAMAN TERHADAP SISTEM INFORMASI

Beberapa ancaman umum terhadap keamanan sistem informasi antara lain:

Tabel 5. Ancaman terhadap Sistem Informasi

Jenis Ancaman	Penjelasan Singkat	Contoh Nyata
Malware	Perangkat lunak jahat seperti virus, worm	WannaCry, NotPetya

Phishing	Upaya penipuan melalui email/pesan palsu	Email berpura-pura dari bank
Ransomware	Menyandera data korban dengan enkripsi	Serangan pada Colonial Pipeline (2021)
SQL Injection	Serangan melalui celah input database	Kebocoran data Tokopedia
Social Engineering	Manipulasi psikologis pada pengguna	Kasus pencurian akun WhatsApp

H. PRINSIP-PRINSIP DASAR KEAMANAN INFORMASI

Keamanan informasi tidak hanya bergantung pada perangkat keras atau lunak yang digunakan, tetapi juga pada prinsip-prinsip dasar yang membentuk fondasi dari kebijakan dan praktik keamanan yang efektif. Prinsip-prinsip ini membantu organisasi dalam mendesain sistem yang tangguh terhadap ancaman internal maupun eksternal. Berikut adalah lima prinsip dasar yang menjadi landasan utama dalam tata kelola keamanan informasi modern.

1. **Least Privilege**, yaitu memastikan bahwa setiap pengguna, proses, atau sistem hanya diberikan hak akses yang paling minimum yang diperlukan untuk menjalankan tugasnya. Tujuan dari prinsip ini adalah meminimalkan kemungkinan kerusakan yang dapat ditimbulkan baik oleh kesalahan pengguna maupun oleh penyusup yang mengeksploitasi akun tersebut. Sebagai contoh, seorang karyawan keuangan tidak seharusnya memiliki akses ke sistem sumber daya manusia, kecuali memang dibutuhkan secara spesifik.
2. **Defense in Depth,** menganjurkan penerapan beberapa lapisan pengamanan yang saling melengkapi. Jika satu lapisan berhasil ditembus oleh penyerang, masih ada lapisan lain yang akan menghalangi langkah berikutnya. Strategi ini bisa mencakup firewall, antivirus, deteksi intrusi, enkripsi, hingga pelatihan kesadaran keamanan bagi pengguna. Konsep ini bersumber dari pendekatan militer dan sangat efektif untuk mengurangi titik kegagalan tunggal (*single point of failure*).

3. **Separation of Duties,** merupakan prinsip penting dalam pencegahan fraud dan kesalahan operasional. Dalam konteks ini, tanggung jawab atas suatu proses atau sistem dibagi ke dalam beberapa pihak atau individu, agar tidak ada satu pihak yang memiliki kendali penuh. Misalnya, seseorang yang memproses transaksi keuangan tidak boleh sekaligus memiliki wewenang untuk menyetujui transaksi tersebut. Prinsip ini memperkuat kontrol internal dan mengurangi risiko penyalahgunaan kekuasaan.
4. **Fail-Safe Defaults,** menyatakan bahwa sistem harus secara default menolak akses kecuali secara eksplisit diizinkan. Ini dikenal dengan pendekatan "default-deny." Dengan kata lain, akses hanya diberikan jika sudah diperiksa dan dianggap aman. Pendekatan ini sangat penting karena kesalahan konfigurasi yang bersifat terlalu permisif sering kali menjadi celah utama dalam insiden keamanan.
5. **Auditability,** merupakan prinsip yang menekankan pentingnya kemampuan sistem untuk merekam dan melacak aktivitas pengguna serta sistem secara menyeluruh. Audit log atau jejak audit sangat krusial dalam menganalisis insiden, mengidentifikasi pelanggaran, serta memastikan kepatuhan terhadap kebijakan dan regulasi keamanan. Sistem yang baik harus mampu menghasilkan laporan audit yang akurat dan tidak dapat dimanipulasi.

   Dengan memahami dan menerapkan prinsip-prinsip ini secara konsisten, organisasi dapat membangun sistem keamanan informasi yang tidak hanya kokoh secara teknis, tetapi juga memiliki fondasi manajemen yang kuat dan dapat dipertanggungjawabkan.

I. STANDAR DAN KERANGKA KERJA KEAMANAN INFORMASI

Dalam era digital, keamanan informasi tidak cukup hanya mengandalkan teknologi. Diperlukan panduan terstruktur berupa standar dan kerangka kerja untuk memastikan perlindungan data secara menyeluruh dan konsisten. Standar seperti ISO/IEC 27001, NIST, dan COBIT membantu organisasi dalam mengelola risiko, menjaga kepatuhan, dan membangun sistem keamanan yang andal. Bab ini akan

membahas berbagai standar tersebut, serta bagaimana penerapannya dalam dunia nyata.

Tabel 6. Standar Dan Kerangka Kerja Keamanan Informasi

Standar/Kerangka	Keterangan Singkat
ISO/IEC 27001	Standar internasional sistem manajemen keamanan informasi
NIST SP 800-53	Panduan kontrol keamanan informasi dari AS
COBIT	Framework untuk tata kelola TI, termasuk aspek keamanan
OWASP Top 10	Sepuluh ancaman keamanan aplikasi web teratas

J. PERKEMBANGAN TANTANGAN DI ERA DIGITAL

Di tengah arus transformasi digital yang pesat, dunia menghadapi tantangan keamanan informasi yang semakin kompleks. Teknologi-teknologi baru hadir membawa efisiensi, namun bersamaan dengan itu juga membuka celah baru terhadap serangan siber. Berikut ini adalah beberapa tantangan utama yang berkembang di era digital modern:

1. Cloud Computing

   Cloud computing mengubah paradigma penyimpanan dan pengolahan data. Data tidak lagi tersimpan secara lokal di server internal organisasi, tetapi tersebar di pusat data milik penyedia layanan cloud (seperti AWS, Google Cloud, atau Azure).

   Tantangan Keamanan:

   - Kontrol terbatas: Organisasi tidak selalu memiliki kendali penuh atas lokasi fisik data mereka.
   - Shared infrastructure: Satu infrastruktur digunakan banyak pelanggan (multi-tenancy), meningkatkan risiko kebocoran antarakun.
   - Akses jarak jauh: Membuka potensi penyusupan jika autentikasi dan enkripsi tidak memadai.

   Contoh Kasus: Kebocoran data pengguna Capital One pada tahun 2019 yang berasal dari salah satu bucket AWS S3 yang salah dikonfigurasi.

2. Big Data

Big Data memungkinkan analisis masif terhadap berbagai sumber informasi dalam jumlah besar (volume), kecepatan tinggi (velocity), dan beragam format (variety).

Tantangan Keamanan:

- Kesulitan pengawasan: Semakin banyak data, semakin sulit melakukan klasifikasi dan perlindungan secara manual.
- Kelemahan metadata: Metadata dan log analitik bisa dimanfaatkan penyerang untuk melacak pola aktivitas sensitif.
- Kepatuhan hukum: Semakin kompleks data, semakin rumit mengelola privasi (misalnya GDPR atau UU PDP).

Contoh Kasus: Facebook–Cambridge Analytica, di mana data profil pengguna dikumpulkan tanpa izin eksplisit dan digunakan untuk manipulasi politik.

3. IoT *(Internet of Things)*

IoT menghubungkan perangkat fisik (kamera, thermostat, smartwatch, printer, dll.) ke jaringan internet untuk pertukaran data otomatis.

Tantangan Keamanan:

- Firmware lemah: Banyak perangkat tidak dilengkapi sistem keamanan atau update berkala.
- Default credentials: Penggunaan username dan password standar oleh pengguna membuat perangkat rentan.
- Tidak adanya enkripsi: Komunikasi data antar perangkat sering kali tidak dienkripsi.

Contoh Kasus: Botnet Mirai (2016) menggunakan ribuan perangkat IoT yang diretas untuk melakukan serangan DDoS skala besar ke server DNS utama.

4. Remote Work & BYOD

Budaya kerja jarak jauh dan penggunaan perangkat pribadi (BYOD) meningkat drastis, terutama sejak pandemi COVID-19. Pegawai mengakses sistem perusahaan dari lokasi berbeda dan perangkat pribadi seperti smartphone atau laptop non-standar.

Tantangan Keamanan:

- Variasi perangkat dan sistem operasi: Sulit dikontrol dan diamankan secara seragam.

- Akses VPN & WiFi publik: Risiko penyadapan komunikasi atau pencurian kredensial meningkat.
- Shadow IT: Karyawan menggunakan aplikasi atau perangkat tanpa izin formal dari tim TI.

Contoh Kasus: Peretasan akun Zoom dan Microsoft Teams akibat lemahnya autentikasi pada perangkat BYOD karyawan perusahaan.

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.

Langkah-langkah menjaga integritas antara lain:

a. **Hashing:** Menggunakan fungsi hash seperti SHA-256 untuk memverifikasi bahwa data tidak diubah.

b. **Digital Signature:** Menjamin bahwa dokumen atau data berasal dari sumber yang sah dan belum diubah.
c. **Kontrol Versi:** Menyimpan histori perubahan dokumen untuk menghindari kehilangan data asli.
d. **Audit Trail:** Merekam setiap perubahan atau akses terhadap data untuk keperluan verifikasi dan investigasi.

3. Availability (Ketersediaan)

Ketersediaan memastikan bahwa informasi dan sistem selalu dapat diakses oleh pengguna yang berwenang pada saat dibutuhkan. Sistem yang tidak tersedia saat dibutuhkan dapat menyebabkan gangguan layanan, kerugian finansial, hingga krisis reputasi.
Pelanggaran terhadap ketersediaan (Kwon et al., 2022) bisa disebabkan oleh:

a. Serangan DoS (Denial of Service).
b. Gangguan listrik atau bencana alam.
c. Kegagalan perangkat keras atau perangkat lunak.
d. Kesalahan konfigurasi sistem.

Upaya untuk menjaga ketersediaan antara lain:

a. **Backup dan Disaster Recovery:** Menyimpan salinan data secara rutin dan menyusun rencana pemulihan bila terjadi kerusakan.
b. **Redundansi Sistem:** Menggunakan sistem cadangan (failover system) untuk menjaga layanan tetap aktif.
c. **Load Balancing:** Membagi beban kerja antar server agar tidak ada satu pun yang kelebihan beban.
d. **Monitoring Real-Time:** Mengawasi sistem secara terus-menerus untuk mendeteksi dan merespons insiden lebih cepat.
e. **Patching dan Pemeliharaan Berkala:** Memastikan sistem dan aplikasi selalu diperbarui agar tidak rentan terhadap kerusakan atau serangan.

D. ANCAMAN DALAM KEAMANAN INFORMASI

Ancaman terhadap keamanan informasi merupakan segala bentuk potensi bahaya yang dapat mengakibatkan kerusakan, pencurian, gangguan, atau penyalahgunaan informasi yang dimiliki oleh individu, organisasi, maupun sistem. Ancaman ini bisa berasal dari **pihak**

eksternal maupun **internal**, dan dapat bersifat **teknis**, **manusia**, atau **alamiah**.
Secara garis besar, ancaman terhadap keamanan informasi dapat diklasifikasikan ke dalam beberapa kategori utama (Peliukh et al., 2024):

1. Malware (Malicious Software)

Merupakan perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mencuri informasi. Jenis-jenis malware meliputi:

a. **Virus**: Menyisipkan diri ke dalam file atau program, dan menyebar saat file tersebut dijalankan.
b. **Worm**: Menyebar tanpa interaksi pengguna, sering kali mengeksploitasi kerentanan sistem jaringan.
c. **Trojan Horse**: Menyamar sebagai aplikasi yang sah namun berfungsi sebagai pintu belakang bagi penyerang.
d. **Ransomware**: Mengenkripsi data korban dan menuntut tebusan untuk membuka akses.
e. **Spyware**: Memata-matai aktivitas pengguna dan mengirimkan informasi sensitif ke pihak ketiga.

2. Phishing dan Social Engineering

Merupakan upaya manipulatif untuk memperoleh informasi sensitif dengan menyamar sebagai entitas terpercaya. Taktik yang sering digunakan antara lain:

a. Mengirim email palsu dengan tautan berbahaya.
b. Meniru website resmi untuk mencuri kredensial login.
c. Menggunakan pesan teks atau telepon untuk mendapatkan akses ke sistem.

3. Man-in-the-Middle Attack (MitM)

Serangan ini terjadi ketika pihak ketiga secara diam-diam menyusup dan memantau atau memodifikasi komunikasi antara dua pihak tanpa sepengetahuan mereka. Ancaman ini umum terjadi pada komunikasi jaringan yang tidak terenkripsi, seperti Wi-Fi publik yang tidak aman.

4. Denial of Service (DoS) dan Distributed DoS (DDoS)

Serangan yang dimaksud adalah **Denial of Service (DoS)** atau **Distributed Denial of Service (DDoS)**.
Serangan ini dilakukan dengan **membanjiri sistem, server, atau jaringan dengan lalu lintas data berlebihan** hingga sumber daya menjadi tidak mampu merespons permintaan yang sah dari pengguna. Berikut penjelasan dampaknya::

a. Downtime system

Serangan DoS/DDoS dapat membuat sistem tidak dapat diakses atau crash sepenuhnya karena:

1) Konsumsi penuh bandwidth jaringan.
2) Overload pada prosesor/server.
3) Exhaustion (pengurasan) pada memori dan kapasitas sistem.

Akibatnya:

1) Website atau aplikasi tidak bisa diakses pengguna.
2) Operasional digital terganggu sementara waktu atau bahkan berhenti total.

b. Kerugian Operasional

Downtime dan ketidaktersediaan layanan bisa berdampak langsung pada proses bisnis, seperti:

1) Transaksi tertunda atau gagal.
2) Proses produksi yang bergantung pada sistem otomatis menjadi terganggu.
3) Hilangnya kesempatan bisnis, terutama di sektor e-commerce, keuangan, atau layanan berbasis online.

Contoh kerugian:

1) Pendapatan harian menurun.
2) Biaya tambahan untuk mitigasi dan pemulihan sistem.
3) Reputasi perusahaan rusak.
4) Kerugian operasional

c. Gangguan pelayanan publik

Jika serangan DoS/DDoS menyasar layanan publik atau infrastruktur kritis (misalnya pemerintahan, rumah sakit, transportasi, atau layanan darurat), dampaknya bisa sangat serius, seperti:

1) Keterlambatan pelayanan administrasi warga.
2) Sistem antrian atau informasi publik menjadi tidak dapat diakses.
3) Krisis kepercayaan terhadap institusi penyedia layanan.

Contoh nyata:

1) Website layanan pajak down saat masa pelaporan.
2) Sistem rumah sakit terganggu saat darurat medis.

5. Insider Threat

Ancaman ini berasal dari dalam organisasi, baik oleh karyawan, kontraktor, atau mitra bisnis yang memiliki akses sah terhadap informasi. Tipe insider threat:

a. **Malicious Insider**: Karyawan yang berniat mencuri atau merusak informasi.
b. **Negligent Insider**: Pengguna yang ceroboh dan menyebabkan kebocoran data tanpa sengaja.

6. Zero-Day Exploits

Adalah eksploitasi terhadap kerentanan perangkat lunak yang belum diketahui oleh pengembang. Karena belum ada tambalan (patch) yang dirilis, serangan ini sangat berbahaya.

7. Bencana Alam dan Kegagalan Sistem

Walau bukan disebabkan oleh manusia, bencana seperti gempa bumi, banjir, atau kebakaran, serta kegagalan perangkat keras, bisa menghancurkan data penting. Oleh karena itu, mitigasi risiko fisik dan backup data menjadi bagian penting dari keamanan informasi.

E. Aspek Keamanan Informasi

Keamanan informasi yang efektif mencakup kombinasi dari tiga aspek utama (Hidayat et al., 2024):

1. **Teknologi**
   Mencakup perangkat keras dan lunak yang digunakan untuk melindungi informasi. Beberapa contoh teknologi keamanan:
   a. **Firewall dan sistem deteksi/pencegahan intrusi (IDS/IPS)**
   b. **Enkripsi data saat transit dan saat disimpan**
   c. **Sistem autentikasi multifaktor (MFA)**
   d. **Pemantauan jaringan dan sistem secara real-time**
2. **Prosedur dan Kebijakan**
   Berisi pedoman yang dirancang untuk memastikan informasi dikelola dengan aman. Termasuk:
   a. **Kebijakan penggunaan perangkat dan jaringan**
   b. **Panduan klasifikasi informasi**
   c. **Rencana manajemen insiden**
   d. **SOP pengendalian perubahan dan pemulihan bencana**
3. **Sumber Daya Manusia**
   Manusia sering kali menjadi titik lemah dalam keamanan informasi. Oleh karena itu, edukasi dan pelatihan secara berkala sangat penting. Program peningkatan kesadaran keamanan informasi bertujuan:
   a. Menyadarkan pengguna terhadap potensi ancaman
   b. Mengajarkan praktik keamanan dasar seperti mengenali phishing dan membuat kata sandi yang kuat
   c. Membentuk budaya keamanan dalam organisasi

E. STANDAR DAN REGULASI KEAMANAN INFORMASI

Beberapa standar dan regulasi penting dalam keamanan informasi antara lain:

1. **ISO/IEC 27001:** Standar internasional yang memberikan kerangka kerja sistem manajemen keamanan informasi (ISMS), termasuk proses perencanaan, implementasi, pemantauan, dan peningkatan berkelanjutan.
2. **NIST (National Institute of Standards and Technology):** Mengembangkan panduan dan kerangka kerja keamanan siber

untuk membantu organisasi mengelola risiko keamanan informasi.

3. **GDPR (General Data Protection Regulation):** Regulasi Uni Eropa yang mengatur perlindungan data pribadi dan privasi individu.
4. **Undang-Undang ITE (Informasi dan Transaksi Elektronik):** Regulasi di Indonesia yang mengatur penggunaan teknologi informasi dan transaksi elektronik, termasuk aspek keamanan.

Kepatuhan terhadap standar dan regulasi ini tidak hanya membantu organisasi dalam mengelola risiko, tetapi juga meningkatkan kepercayaan publik dan mitra bisnis.

F. STRATEGI IMPLEMENTASI KEAMANAN INFORMASI

Strategi implementasi keamanan informasi melibatkan pendekatan menyeluruh yang menggabungkan aspek teknis dan manajerial. Beberapa langkah strategis utama meliputi:

1. **Identifikasi Aset Informasi:** Menentukan jenis aset informasi yang perlu dilindungi, seperti data pelanggan, informasi keuangan, dan sistem TI penting.
2. **Penilaian Risiko (Risk Assessment):** Menganalisis potensi ancaman dan kerentanan terhadap aset informasi, serta mengevaluasi dampaknya terhadap organisasi.
3. **Pengembangan Kebijakan dan Prosedur:** Merancang aturan dan standar operasional terkait keamanan informasi, termasuk kebijakan kata sandi, kontrol akses, dan penggunaan perangkat pribadi (BYOD).
4. **Penerapan Kontrol Keamanan:** Mengimplementasikan teknologi dan proses seperti firewall, enkripsi, sistem backup, segmentasi jaringan, serta pelatihan keamanan.
5. **Monitoring dan Evaluasi:** Melakukan pemantauan terhadap sistem dan log aktivitas secara berkala, melakukan audit keamanan, serta menguji efektivitas kontrol melalui penetration testing.

6. **Pemulihan dan Peningkatan Berkelanjutan:** Menyusun dan menguji rencana pemulihan bencana (disaster recovery plan) dan business continuity plan untuk menjamin kelangsungan 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:

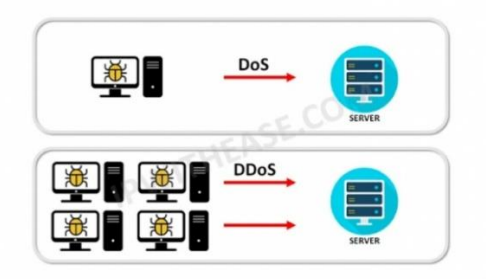
   - Kebakaran yang menghancurkan server
   - Pencurian laptop yang berisi data rahasia

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

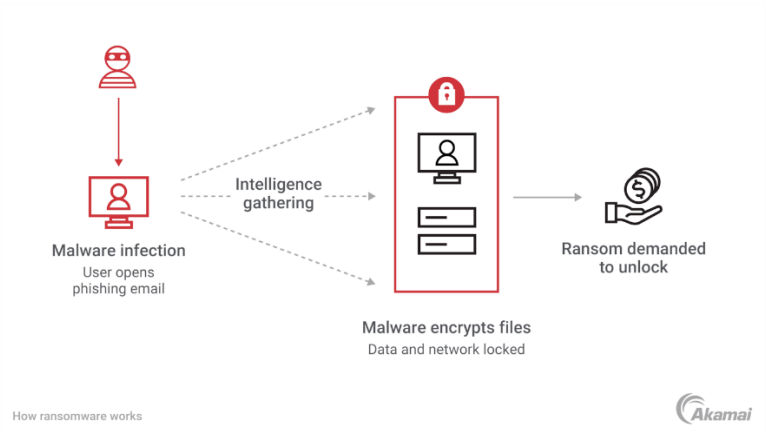
WannaCry menyebar melalui eksploitasi EternalBlue, sebuah kerentanan dalam protokol SMB yang digunakan oleh Windows untuk berbagi file dan printer dalam jaringan. Karena banyak sistem tidak diperbarui dengan patch keamanan yang telah dirilis oleh Microsoft, ransomware ini berhasil masuk dan menyebar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

4. Berdasarkan Metode Serangan.

Ancaman pada metode serangan diklasifikasikan berdasarkan teknik yang digunakan untuk mengeksploitasi sistem :

- Malware Based Attacks.
  Ancaman yang menggunakan software berbahaya seperti virus, worm, trojan, ransomware dan juga spyware.
- Social Engineering.
  Merupakan suatu teknik manipulasi psikologis yang mengecoh pengguna (user) untuk memberikan informasi sensitif, seperti phishing atau pretexting.
- Exploit Based Attacks:
  Serangan yang mengeksploitasi celah keamanan dalam sistem atau software, seperti zero day attacks dan buffer overflow.
- Man in the Middle (MitM) Attacks:
  Adalah suatu serangan yang menyadap komunikasi antara 2 (dua) pihak tanpa sepengetahuan mereka.

5. Berdasarkan Target Serangan.

Ancaman (Threat) dikategorikan berdasarkan suatu target utama yang ingin diserang, seperti misalnya saja :

- Jaringan (Network Threats).
  Serangan yang biasanya menargetkan infrastruktur jaringan, seperti → Firewall, Router atau Server DNS.
  Contohnya :
  - DDoS.
  - Sniffing attacks.
- Aplikasi (Application Threats).
  Serangan yang mengeksploitasi kelemahan dalam software atau web service, seperti :
  - SQL Injection dan
  - Cross Site Scripting (XSS).
- Perangkat Keras (Hardware Threats):
  Ancaman ini menargetkan hardware, seperti :
  - Perusakan server atau penyadapan perangkat IoT.
- Manusia (Human Centric Threats):
  Ancaman ini kebanyakan memanfaatkan kesalahan dari user, seperti :

- Phishing atau insider threats.

6. Berdasarkan Level Risiko

Setiap ancaman memiliki level atau tingkat risiko yang berbeda – beda tergantung pada probabilitas kejadian dan juga dampaknya, seperti:

- Risiko Tinggi (High Risk) :
  Ancaman ini punya dampak yang cukup besar yang dapat menyebabkan kerugian finansial, gangguan operasional, atau kebocoran data besar - besaran. Contohnya :
  - Ransomware atau serangan APT (Advanced Persistent Threats).
- Risiko Menengah (Medium Risk) :
  Ancaman ini berdampak signifikan, tapi masih dapat dikendalikan dengan suatu sistem mitigasi yang baik, seperti :
  - Serangan phishing atau brute force attack.
- Risiko Rendah (Low Risk) :
  Ancaman ini hanya memiliki dampak kecil atau tidak langsung terhadap sistem.
  Seperti :
  - Spam E-Mail atau iklan berbahaya (malvertising).

C. PRINSIP KEAMANAN MELINDUNGI JARINGAN DAN INFRASTRUKTUR IT.

1) Memahami Prinsip Keamanan Jaringan dan Infrastruktur IT.

Di era digital yang kian hari kian berkembang dengan pesat, keamanan jaringan dan infrastruktur IT menjadi salah satu aspek yang cukup krusial dalam menjaga kelangsungan operasional bisnis, pemerintahan, lembaga dan juga organisasi lainnya. Dengan semakin meningkatnya ancaman siber seperti misalnya saja :

- Peretasan.
- Malware.

- Serangan Denia Of Service (DoS).

Gambar 4. 3. Tiga ancaman siber utama

Untuk saat ini pemahaman tentang prinsip keamanan jaringan sudah menjadi kebutuhan yang sangat mendesak bagi para profesional IT dan tentunya juga para pemangku kepentingan lainnya.

Keamanan jaringan dan infrastruktur IT merujuk pada praktik, kebijakan serta teknologi yang didesain untuk melindungi integritas, kerahasiaan dan juga ketersediaan data serta sumber daya (resource) sistem informasi.

Infrastruktur IT mencakup hardware, software, jaringan, dan layanan cloud yang men-support operasional sistem informasi modern. Tanpa sistem keamanan yang kuat, perusahaan/organisasi/lembaga/pemerintahan akan dapat menghadapi risiko kebocoran data (data leak), pencurian informasi sensitif (theft of sensitive information), serta gangguan operasional (operational disruption) yang dapat mengakibatkan dan berdampak yang cukup besar pada keberlangsungan bisnis atau usaha.

Prinsip dasar keamanan jaringan dan infrastruktur IT itu, meliputi konsep Confidentiality, Integrity dan Availability (CIA), yang mempunyai tujuan untuk menjaga informasi agar tetap rahasia, tidak berubah tanpa izin dan juga dapat diakses oleh pihak yang berwenang. Selain daripada itu, pendekatan pertahanan berlapis (defense in depth), manajemen risiko, serta kebijakan keamanan yang sangat ketat juga menjadi komponen utama (main components) dalam strategi keamanan siber yang efektif.
Dengan mengerti serta memahami mengenai prinsip keamanan jaringan dan infrastruktur IT, individu dan juga tentunya perusahaan/organisasi/lembaga/pemerintahan dapat mengambil langkah proaktif dalam mengamankan sistem mereka dari ancaman yang semakin berkembang.

2) 5 (Lima) Prinsip Keamanan Jaringan dan Infrastruktur IT.

Implementasi atau penerapan keamanan jaringan melibatkan berbagai teknik dan teknologi, seperti :
- Firewall,
- Enkripsi,
- Sistem deteksi
- Pencegahan intrusi (IDS/IPS).
- Serta manajemen akses.

Tidak hanya dari aspek teknis saja, keamanan juga mencakup berbagai kebijakan dan prosedur yang mengatur bagaimana sistem tersebut harus dikonfigurasi (configured), diawasi (supervised), dan dipelihara (maintained) untuk dapat mengurangi risiko serangan siber.
Dengan semakin meningkatnya adopsi teknologi cloud (Cloud Technology), Internet of Things (IoT) dan juga kecerdasan buatan (Artificial Intelligence), tantangan dalam menjaga keamanan jaringan menjadi kian kompleks. Oleh sebab itu, pemahaman yang cukup mendalam tantang prinsip keamanan jaringan dan infrastruktur IT begitu menjadi penting bagi profesional IT, manajer keamanan, dan juga organisasi yang ingin menjaga

ketahanan sistem mereka terhadap ancaman digital yang kian berkembang pesat.

Berikut adalah 5 (lima) prinsip utama Keamanan Jaringan dan Infrastruktur IT :

- Kerahasiaan (Confidentiality):
  Memastikan data dan informasi hanya bisa diakses oleh pihak yang berwenang saja, dengan menggunakan enkripsi dan kontrol akses (access control) sebagai langkah utama.

- Integritas (Integrity) :
  Menjaga keutuhan dan juga keakuratan data dengan menerapkan prinsip serta mekanisme seperti hashing, tanda tangan digital dan kontrol perubahan data.

- Ketersediaan (Availability) :
  Memastikan sistem dan juga layanan selalu bisa diakses oleh user yang sah dengan menerapkan redundansi, backup, serta perlindungan terhadap serangan DdoS (Distributed denial of Service).

- Otentikasi dan Otorisasi :
  Menetapkan mekanisme validasi identitas user dan menentukan hak akses (access rights) mereka melalui penggunaan 'password' yang kuat, autentikasi multifaktor (MFA), dan juga manajemen hak akses (access rights).

- Monitoring dan Respons Insiden :
  Menggunakan sistem monitoring atau pemantauan keamanan untuk mendeteksi ancaman secara real time dan menyiapkan rencana respons insiden untuk mengatasi pelanggaran keamanan dengan cepat dan efektif.

D. PENTINGNYA MANAJEMEN RESIKO DALAM KEAMANAN JARINGAN DAN INFRASTRUKTUR IT.

Dengan kemajuan teknologi yang terus menerus dan kian berlangsung, tentunya diperlukan pendekatan yang adaptif dan juga inovatif untuk mengelola risiko serta dapat memaksimalkan manfa'at dari TI tersebut. Teknologi Informasi, dengan segala potensi dan tantangannya, menjadi komponen yang tidak terpisahkan dari kehidupan modern. Penggunaannya yang strategis mampu memberikan nilai tambah yang signifikan, baik untuk individu maupun organisasi.

1. Identifikasi, klasifikasi, analisis dan evaluasi risiko.

   Dengan menerapkan proses identifikasi, klasifikasi, analisis, dan evaluasi risiko yang sistematis, organisasi dapat meningkatkan keamanan jaringan dan infrastruktur IT mereka, serta dapat meminimalkan dampak atau risiko dari potensi ancaman yang ada. Dibawah ini akan dijelaskan 4 (empat) point tersebut diatas :

- Identifikasi Risiko.

  Merupakan langkah awal dalam manajemen risiko keamanan jaringan dan infrastruktur IT. Tujuannya untuk dapat mengenali ancaman potensial yang dapat membahayakan sistem. Contoh beberapa risiko yang umum diidentifikasi dalam keamanan jaringan dan infrastruktur IT meliputi :

  - Serangan Siber → Dapat berupa Malware, Ransomware, phishing, dan juga serangan DDoS.

  - Kelemahan Software dan Hardware → Kerentanan dalam sistem operasi (operating system), aplikasi, dan perangkat jaringan (network device).

  - Kesalahan Manusia (Human Error) → Adalah Kesalahan Konfigurasi (Configuration Error), seperti penggunaan 'password' yang sangat lemah dan juga kelalaian dalam pengelolaan akses.

- Kegagalan Infrastruktur (Infrastructure Failure) → Seperti kegagalan server, pemadaman listrik, atau dapat juga gangguan berupa sistem komunikasi.

- Ancaman orang dalam (Insider Threats) → Ancaman ini biasanya berasal dari orang dalam, baik itu disengaja maupun tidak disengaja.

2. Strategi mitigasi, pengendalian risiko dan respons terhadap risiko.

Dengan menerapkan strategi mitigasi, pengendalian risiko, dan juga respons terhadap risiko secara efektif, tentunya perusahaan/organisasi/lembaga dapat meningkatkan ketahanan terhadap ancaman siber serta bisa melindungi aset digital mereka secara optimal, dibawah ini akan dijelaskan lebih lanjut tentang :

- Strategi Mitigasi Risiko.

Mitigasi risiko dalam keamanan jaringan dan infrastruktur IT bertujuan untuk mengurangi kemungkinan dan dampak dari ancaman yang dapat mengganggu sistem. Strategi mitigasi yang umum diterapkan meliputi :

- Penerapan Keamanan Berlapis (Defense in Depth) → Dapat menggunakan berbagai lapisan keamanan seperti misalnya firewall, IDS/IPS, enkripsi dan juga otentikasi multi faktor.

- Patch Management dan Update Sistem → Untuk menjaga software tetap terbaru (update/upgrade) untuk dapat mengatasi kerentanan keamanan.

- Segmentasi Jaringan → Harus dapat membatasi akses antar segmen jaringan dengan tujuan dapat untuk mengurangi penyebaran serangan.

- Backup dan Disaster Recovery Plan → Mengembangkan bagaimana strategi yang tepat dalam pemulihan data (data recovery), untuk dapat menghadapi kegagalan atau serangan siber.

- Pengendalian Risiko.

  Dapat mencakup pada penerapan kebijakan dan juga prosedur untuk mengelola ancaman yang telah diidentifikasi tentunya. Dibawah ini adalah beberapa langkah pengendalian risiko yang meliputi :

  - Keamanan Akses dan Autentikasi → Dengan menerapkan kebijakan akses berbasis peran (Role Based Access Control) serta autentikasi 2 (dua) faktor (2FA).

  - Enkripsi Data → Menggunakan enkripsi untuk dapat melindungi data sensitif baik itu saat transit maupun saat tersimpan.

  - Monitoring dan Logging → Menggunakan teknik Security Information and Event Management (SIEM) untuk bisa mendeteksi dan juga merespons insiden keamanan secara real time.

  - Pelatihan / Training dan Kesadaran Keamanan → Meningkatkan kesadaran user tentang bahaya dan ancaman siber serta praktik keamanan terbaik.

E. STANDAR DAN BEST PRACTICES DALAM KEAMANAN JARINGAN DAN INFRASTRUKTUR IT.

Untuk memastikan keamanan jaringan dan infrastruktur IT yang optimal, tentunya perusahaan/organisasi/lembaga harus dapat mengikuti standar dan juga praktik terbaik yang telah diakui secara global. Beberapa di antaranya adalah :

1. Standar Keamanan.

   - ISO/IEC 27001 :

Adalah Standar Internasional untuk sistem manajemen keamanan informasi (ISMS).

- NIST Cybersecurity Framework :

  Merupakan pedoman keamanan yang telah dikembangkan oleh National Institute of Standards and Technology.

- CIS Controls :

  Serangkaian atau sederetan kontrol keamanan yang sangat penting yang direkomendasikan oleh Center for Internet Security.

- PCI DSS :

  Standar keamanan untuk perusahaan / organisasi / lembaga yang menangani transaksi pembayaran kartu kredit (credit card).

2. Best Practices dalam keamanan jaringan dan infrastruktur IT.

   - Zero Trust Architecture :

     Mengadopsi prinsip tidak mempercayai user atau device sampai mereka diverifikasi.

   - Least Privilege Access :

     Memberikan hak akses (access rights) minimal yang diperlukan kepada user untuk dapat mengurangi risiko eksploitasi.

   - Security Awareness Training :

     Meningkatkan kesadaran tentang keamanan untuk karyawan melalui pelatihan/training secara berkala.

   - Regular Security Audits and Penetration Testing :

Test dan mengevaluasi keamanan sistem secara rutin atau berkala untuk menemukan celah keamanan (security gap).

- Endpoint Detection and Response (EDR) :

  Menggunakan solusi keamanan yang memantau atau memonitor dan juga merespons ancaman pada perangkat endpoint (endpoint device).

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

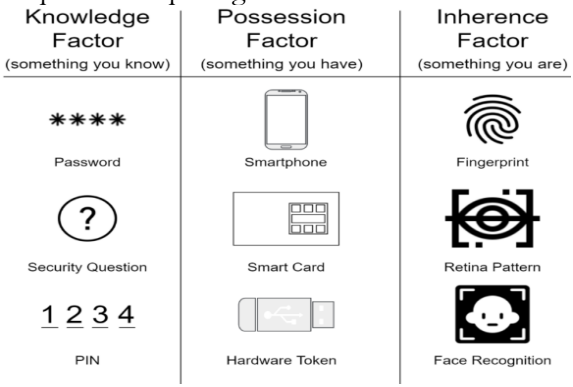
Autentikasi yang aman merupakan salah satu fondasi utama dalam menjaga keamanan sistem informasi. Ancaman keamanan seperti pencurian identitas, akses tidak sah, dan serangan peretas, menjadikan Autentikasi yang kuat diperlukan untuk melindungi sistem informasi. (Windyasari, V. S. et al. 2024) Autentikasi 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 :

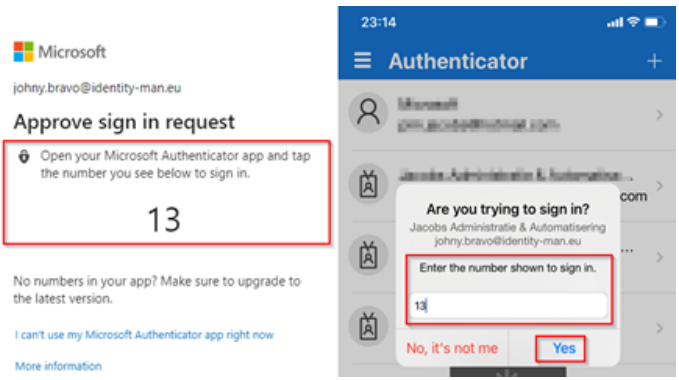


Gambar 6. 1. Jenis-jenis faktor Autentikasi

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.

Metode 2FA memiliki keamanan lebih tinggi dibanding SFA dan mengurangi risiko akses tidak sah akibat pencurian password/PIN. Namun implementasi lebih rumit dibanding SFA dan jika

perangkat kedua hilang (misal HP yang digunakan untuk OTP ke sms atau *authenticator*) maka akses bisa terhambat.

c. *(MFA-Multi Factor Authentication)*
MFA adalah metode autentikasi, jika 2FA hanya menggunakan dua metode untuk memverifikasi dan mengotorisasi upaya masuk pengguna, sedangkan MFA bisa menggunakan dua atau lebih titik pemeriksaan atau faktor dari kategori yang berbeda. Menggunakan dua kategori autentikasi termasuk MFA karena MFA mencangkup 2FA. Namun jika menggunakan tiga atau lebih kategori autentikasi maka termasuk MFA yang lebih kuat. Contoh kombinasi penerapan MFA dapat dilihat pada tabel 6.1

Tabel 6.1 Kombinasi MFA

No	Metode MFA	Kategori	Jumlah faktor
1	Password + OTP dari SMS atau Email atau aplikasi authenticator	*Something you know* + *Something you have*	2FA (termasuk MFA)
2	Password + Sidik jari atau pengenalan wajah	*Something you know* + *Something you are*	2FA (termasuk MFA)
3	• Kartu akses (RFID) + PIN + Sidik jari • RFID + Password + OTP dari aplikasi autentikator • PIN + USB Security Key (YubiKey) + Sidik jari • Password + OTP +Biometrik	*Something you have* + *Something you know* + *Something you are* (Kombinasi lainnya)	MFA dengan 3 faktor
4	• Token fisik + PIN + OTP dari aplikasi authenticator + Pengenalan wajah	*Something you have* + *Something you know* + *Something you have* + *Something you are / the user does*	MFA dengan 4 faktor

	• Smart Card (RFID) + PIN + OTP via email + Geolocation verification	(Kombinasi lainnya)	

MFA biasanya digunakan untuk akses **tingkat tinggi**, seperti akses ke server data center, sistem keuangan. Semakin banyak faktor yang digunakan, semakin sulit bagi penyerang untuk membobol sistem. Tantangan dari MFA adalah pengguna akhir mungkin menganggapnya kurang nyaman dibandingkan kata sandi sederhana dan, oleh karena itu, menolak untuk menggunakannya.

3. Prinsip Keamanan dalam Manajemen Autentikasi

Manajemen Autentikasi sebaiknya memastikan beberapa aspek penting untuk menjaga keamanan sistem informasi diantaranya:

a. Saat pengguna salah memasukkan *username* atau *password*, sistem menampilkan pesan "*Username* atau *password* salah." ATAU Saat menggunakan *Two-Factor Authentication* (2FA), jika kode OTP salah "Kode autentikasi salah."
b. Sistem tidak menampilkan saran nama pengguna, dan hanya membiarkan pengguna mengetik sendiri.
c. Menampilkan pemberitahuan umum bahwa sistem atau layanan hanya boleh diakses oleh pengguna yang berwenang "Harap berhati-hati saat memasukkan informasi *log-in*. Jangan berikan kredensial Anda kepada siapa pun. Akses tanpa izin akan ditindaklanjuti."
d. Sistem tidak memvalidasi satu per satu saat pengguna sedang mengetik "*username* salah" atau "*password* salah". Jika sistem langsung memberi tahu bahwa **password salah** setelah mengetahui username valid, penyerang hanya perlu menebak password, bukan kedua elemen sekaligus. Dengan menyamarkan pesan error, sistem mempersulit upaya serangan *brute force*.
e. Mencatat semua upaya login yang berhasil maupun gagal. Biasanya jika ada banyak percobaan login yang gagal dari satu akun atau IP, itu bisa menjadi tanda ***brute force attack*** (percobaan menebak password secara otomatis). Jika ada banyak login gagal dari akun yang berbeda tetapi dari satu IP, itu bisa menunjukkan ***credential stuffing*** (menggunakan data login curian dari sumber lain).
f. Mengirimkan peringatan keamanan jika ada indikasi percobaan peretasan. Contoh :

1) Terlalu banyak percobaan login yang gagal. Jika seseorang salah memasukkan password lebih dari yang di tetapkan (Mislanya lebih dari 3x), sistem akan mengirimkan email ke Admin
2) Login dari lokasi atau perangkat yang tidak biasa.
3) Perubahan mendadak pada pengaturan akun tanpa otorisasi pengguna.

g. Membuat batas maksimal percobaan *login* (*max login attempts*) untuk mencegah akses tidak sah dan melindungi sistem dari serangan *brute force*. Setelah percobaan gagal *login* akun dapat dikunci sementara (*lockout*) selama jangka waktu tertentu. Batas yang umum digunakan maksimal percobaan *login* adalah 3-5 kali. Sedangkan penguncian akun sementara adalah 30 menit. Dalam penguncian sementara dapat digunakan opsi CAPTCHA atau pengguna menghubungi administrator untuk membuka akun. Menggunakan CAPTCHA untuk membedakan manusia dan bot saat gagal login.
h. Saat pengguna mengetik password, yang muncul di layar adalah tanda bintang (*****) atau titik (●●●●●), bukan teks asli. Namun, ada fitur opsional seperti "Show Password" (misalnya, pengguna dengan gangguan penglihatan).
i. Tidak mengirimkan password dalam bentuk plainteks biasa melalui jaringan. Sistem mengenkripsi password sebelum dikirim melalui sehingga tidak bisa dibaca oleh peretas yang menggunakan "sniffer". Jika pengguna lupa password, sistem mengirimkan tautan untuk mereset password, bukan mengirimkan password asli
j. Validasi input untuk mencegah SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)
k. Informasi Autentikasi sementara dikirim kepada pengguna dengan cara yang aman (misalnya melalui aplikasi pesan yang menyediakan enkripsi *end-to-end*, atau melalui email dengan *link* reset kata sandi). Pengguna akan diminta membuat kata sandi baru daripada menggunakan kata sandi sementara yang lebih rentan.
l. Informasi Autentikasi tidak boleh dibagikan kepada siapa pun.
m. Manajemen kata sandi harus diterapkan, kelemahan penggunaan kata sandi/frasa sandi sebagai satu-satunya faktor autentikasi. Jika kata sandi tersebut dicuri, diretas, atau ditebak, maka sistem atau akun yang dilindungi menjadi sepenuhnya rentan terhadap akses tidak sah. (PCI Security Standards Council, 2022). Hal yang dapat dilakukan :

1) Kata sandi yang sama tidak diperkenankan digunakan diseluruh layanan dan sistem yang berbeda.
2) Sistem informasi memungkinkan pengguna untuk mengubah kata sandinya sendiri (*password reset/ forgot password*) dan menyertakan *username* dan *password* tidak bisa kosong/ *blank*.
3) Mencegah penggunaan ulang kata sandi sebelumnya (*password history 3x*).
4) Menerapkan perubahan kata sandi setelah pemutusan hubungan kerja, untuk user/identitas yang tetap aktif.
5) Password minimal 12 dan Kombinasi Angka, huruf, simbol (seperti !$%#*)
6) Session timeout, idle time : 15 Menit
7) Password diganti otomatis maksimal 90 hari (*password expired*)

B. KONTROL AKSES

Kontrol akses adalah elemen fundamental dalam keamanan sistem informasi yang berhubungan erat dengan identitas pengguna yang telah diverifikasi melalui proses autentikasi dan otorisasi. Autentikasi memastikan bahwa pengguna adalah identitas seseorang atau entitas yang benar, sedangkan otorisasi menentukan apa yang diizinkan untuk dilakukan oleh pengguna setelah proses Autentikasi berhasil. Tujuan dari akses kontrol adalah untuk memastikan akses yang terotorisasi dan untuk mencegah akses yang tak terotorisasi ke informasi dan aset terkait lainnya. (*International Organization for Standardization*, 2022). Sistem yang tidak memiliki mekanisme manajemen hak akses yang baik rentan terhadap ancaman, seperti *privilege escalation*, di mana penyerang dapat meningkatkan hak akses mereka untuk mendapatkan kontrol penuh atas sistem. Berikut adalah beberapa prinsip kunci yang digunakan dalam kontrol akses:

1. ***Prinsip Need-to-use*** **(Kebutuhan untuk menggunakan)**
   Prinsip ini menekankan bahwa hak akses bagi pengguna, aplikasi, atau sistem harus dibatasi hanya pada tingkat yang diperlukan untuk menjalankan tugas atau fungsinya. Dengan memberikan akses seminimal mungkin, potensi penyalahgunaan atau akses yang tidak sah, baik disengaja maupun tidak, dapat dikurangi secara signifikan.
2. ***Prinsip Need-to-Know*** **(Kebutuhan untuk mengetahui)**
   Prinsip ini memastikan bahwa seseorang hanya diberikan akses terhadap informasi atau sumber daya yang relevan dengan tugasnya. Penerapan prinsip ini sangat penting dalam organisasi yang menangani data sensitif, seperti informasi rahasia atau data pelanggan,

di mana akses hanya diberikan kepada individu yang benar-benar membutuhkannya dalam menjalankan pekerjaannya.

Berikut hal yang harus di perhatikan dalam manajemen hak akses :

1. **Manajemen Identititas**
   Manajemen identitas dalam sistem informasi adalah proses yang penting untuk memastikan bahwa hanya individu yang memiliki otoritas. Manajemen identitas mencakup sebagai berikut :
   a. Tidak diperkenankan 1 orang menggunakan duplikat akun. Hal tersebut dikarenakan akan menyulitkan untuk mengontrol akses terhadap data sensitif.
   b. Tidak di perbolehkan menggunakan nama user general atau nama samaran misalnya ("admin", "guest", "user"). Identitas pengguna harus jelas agar setiap tindakan dalam sistem bisa dilacak. Jika terjadi insiden keamanan, nama pengguna unik membantu mengetahui siapa yang bertanggung jawab.
   c. *User Root* atau (*service account*) hanya boleh digunakan dengan alasan yang rasional dan pengguna level tinggi misalnya saat terjadi serangan siber atau kegagalan sistem yang memerlukan intervensi segera. Tidak boleh digunakan untuk tugas sehari-hari yang tidak membutuhkan akses root karena bisa saja seorang user secara tidak sengaja menjalankan perintah hapus.
2. **Hak Akses**
   Salah satu yang menajdi kritikal dalam hak akses adalah proses penyediaan, pencabutan, dan peninjauan hak akses. Berikut poin-poin yang perlu diperhatikan :
   a. Dalam proses pembuatan, perubahan, atau penghapusan akun pengguna, diperlukan dokumentasi sebagai bukti administratif. Beberapa perusahaan besar telah mengadopsi aplikasi atau alat khusus untuk mengelola proses ini, namun jika tidak tersedia, formulir manual yang telah disahkan sesuai dengan tugas dan tanggung jawab masing-masing dapat digunakan. Penting untuk memastikan bahwa pihak yang mengajukan permintaan perubahan bukanlah pihak yang sama dengan yang memberikan persetujuan. Hak akses tidak boleh diberikan sebelum proses otorisasi selesai. Verifikasi terhadap tingkat akses harus dilakukan sesuai dengan kebutuhan, terutama untuk akun dengan hak istimewa seperti administrator, yang harus dibatasi seminimal mungkin. Dengan adanya dokumentasi yang lengkap, potensi manipulasi akun pengguna, seperti pembuatan akun fiktif atau penghapusan jejak aktivitas, dapat dicegah. Dokumentasi juga berfungsi untuk

memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sistem.

b. Memastikan sistem informasi mempunyai *Role-Based Access Control* (RBAC) dan *User Access Matrix* (UAM). Dalam sistem informasi, terdapat beberapa jenis hak akses yang umum diterapkan:
   1) *Read* (Baca): Pengguna diizinkan untuk melihat informasi tetapi tidak dapat mengubahnya.
   2) *Write* (Tulis): Pengguna memiliki hak untuk mengedit atau menambahkan informasi ke sistem.
   3) *Execute* (Eksekusi): Pengguna dapat menjalankan program atau skrip tertentu di dalam sistem.
   4) *Delete* (Hapus): Pengguna memiliki kemampuan untuk menghapus informasi dari sistem.

   RBAC memberikan hak akses untuk roles bukan menerapkan hak akses pelaku atau subjek. Pengguna tidak bisa mengambil hak akses pengguna lain merupakan dasar perbedaan antara RBAC dan DAC. Dalam organisasi, roles dibuat untuk fungsi kerja yang berbeda sesuai dengan peran keanggotaan yang didasarkan pada kompetensi, tugas, dan kewenangan dalam organisasi. (Raharjo Budi, 2021). Hal yang perlu diperhatikan dalam hak akses :
   1) Meninjau hak akses secara berkala, waktu peninajauan dapat dilakukan 1 bulan sekali atau ketika terjadi perubahan signifikan.
   2) Dapat juga pemberian hak akses temporer untuk jangka waktu terbatas dengan memberi tenggang waktu sesuai kebutuhan.
   3) Memelihara rekaman perubahan, pembuatan dan penghapusan terhadap hak akses.

c. Hak akses harus dicabut jika pengguna tidak lagi membutuhkannya/resign 1hari setelah resign. Jika akun tidak segera dicabut, mantan karyawan masih bisa mengakses sistem perusahaan, yang bisa disalahgunakan

d. Akses untuk konsultan, vendor yang melakukan *vulnerability assessment* (penilaian kerentanan) dan *penetration testing* (uji penetrasi), hanya di kasih akses sementara dan terbatas dalam jangka waktu terbatas untuk menyelesaikan tugas mereka.

3. Hak Akses Istimewa (*Privilaged Access Rights*)

Dalam memilih kontrol keamanan sistem informasi, perlu dilakukan pembatasan dan manajemen hak akses istimewa (seperti administrator atau super admin). Tujuannya adalah untuk memastikan hak akses istimewa hanya diberikan pada pengguna, komponen, dan layanan

perangkat lunak yang terotorisasi. (*International Organization for Standardization*, 2022). Hal-hal berikut perlu dipertimbangkan :

a. Mengidentifikasi pengguna yang membutuhkan hak akses istimewa (seperti administrator atau super admin) dengan cara mengalokasikan kepada pengguna yang hanya membutuhkan. Hak akses istimewa harus diberikan hanya ketika diperlukan (masa berlaku berkahirnya gak akses) dan dalam jumlah minimal. Akun dengan hak istimewa adalah **target utama** bagi penyerang siber. Jika akun ini diretas, dampaknya bisa lebih besar dibanding akun biasa.
b. Dalam proses otorisasi juga harus ditentukan siapa yang dapat menyetujui hak akses istimewa termasuk persyaratannya. Personil yang dapat menyetujui akses istimewa adalah Pemilik Sistem (System Owner) dan manajemen tingkat tinggi seperti head, manager atau direktur.
c. Menhindari identitas pengguna admin yang generik seperti "root" dan tidak berbagai hak akses kepada banyak orang.
d. Akses Hak istimewa diharuskan menggunakan 2FA/MFA dan menyimpan log akses Admin/Hak Istimewa.

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.

Proses evaluasi sumber daya dimulai dengan mengelompokkan sumber daya berdasarkan tingkat kepentingannya, berkaitan dengan kemampuan sumber daya dalam mendukung pencapaian tujuan perusahaan. Evaluasi tersebut selanjutnya ditetapkan berdasarkan dua kriteria:

1) Penilaian substitusi sumber daya: biaya untuk membersihkan, memperbaiki, dan mengganti data (jika memungkinkan); dan
2) Dampak yang dihadapi perusahaan akibat kehilangan atau penyalahgunaan sumber daya, seperti potensi kerugian finansial dan/atau konsekuensi hukum atau regulasi dari pengungkapan, pergeseran, ketidaktersediaan, dan/atau kerusakan data, serta informasi dan sumber daya informasi lainnya.

Penilaian ini dapat ditentukan melalui analisis dampak terhadap bisnis. Nilai yang dihasilkan dari dampak pada bisnis umumnya jauh melebihi biaya penggantian yang sederhana, tergantung kepada seberapa penting sumber daya tersebut bagi organisasi dalam mencapai tujuannya.

Evaluasi sumber daya adalah komponen krusial dalam menilai efek dari skenario kejadian, dikarenakan peristiwa tersebut bisa memengaruhi lebih dari satu sumber daya (contohnya sumber daya yang saling terkait), atau sebagian sumber daya tersebut. Beragam risiko dan kelemahan akan memiliki dampak yang beragam pada sumber daya, seperti kehilangan kerahasiaan, integritas, atau ketersediaan.

Penilaian dampak yang dihasilkan berkaitan dengan evaluasi sumber daya yang dikembangkan melalui analisis pengaruh terhadap perusahaan.

Dampak atau hasil dari suatu perusahaan dapat diukur dengan memprediksi hasil dari sebuah peristiwa atau serangkaian peristiwa, atau dengan memanfaatkan informasi dari studi terdahulu atau data yang tersedia. Dampaknya dapat dinyatakan dalam bentuk finansial, teknis, manusia, atau ukuran lain yang relevan bagi organisasi. Kadang-kadang, lebih dari satu nilai diperlukan untuk memahami dampak pada waktu, lokasi, kelompok, atau konteks yang berbeda.

Dampak yang berhubungan dengan waktu dan uang harus dievaluasi dengan metode yang sama seperti yang diterapkan untuk menilai potensi ancaman dan kerentanan. Konsistensi harus dijaga dalam pendekatan baik yang berbasis angka maupun yang bersifat deskriptif.

c. Penilaian Kemungkinan Insiden

Setelah menemukan situasi insiden, penting untuk mengevaluasi kemungkinan dari tiap situasi dan dampak yang mungkin muncul, dengan memakai cara perkiraan kualitatif atau kuantitatif. Hal ini perlu memperhitungkan seberapa sering risiko muncul dan seberapa mudah kelemahan dapat dimanfaatkan, sambil mempertimbangkan:

1) Pengalaman dan informasi yang berkaitan dengan potensi bahaya.
2) Mengenai sumber ancaman yang dilakukan dengan sengaja: alasan dan kemampuan, yang bisa berubah seiring waktu, serta sumber daya yang dapat mendukung penyerang, dan bagaimana persepsi mengenai daya tarik serta kelemahan sumber daya yang berpotensi diserang.
3) Untuk sumber bahaya yang disengaja: variabel geografi seperti keberadaan dekat dengan bahan kimia atau wilayah pengeboran minyak, potensi cuaca ekstrem, serta komponen-komponen yang dapat berkontribusi pada kelalaian manusia dan kerusakan alat.
4) Kerentanan, baik pada tingkat individu maupun secara keseluruhan.
5) Tindakan pengendalian yang diterapkan dan sejauh mana mereka efektif dalam mengurangi kerentanan.

Sebagai ilustrasi, sebuah sistem informasi dapat memiliki kerentanan terhadap risiko pengguna yang menyamarkan identitas mereka serta penggunaan sumber daya yang tidak semestinya. Kerentanan terhadap penyamaran identitas pengguna bisa sangat tinggi disebabkan oleh ketidakadaan verifikasi terhadap pengguna tersebut. Di sisi lain, meski tidak ada verifikasi pengguna, risiko penyalahgunaan sumber daya mungkin tergolong rendah, karena ada sedikit cara untuk melakukan penyalahgunaan tersebut.

Berdasarkan kebutuhan akurasi, sumber daya dapat dikelompokkan, atau mungkin perlu untuk membagi sumber daya menjadi bagian-bagian yang lebih kecil dan mengaitkan

skenario-skenario tertentu dengan setiap bagian. Sebagai contoh, dalam berbagai lokasi, jenis ancaman yang dihadapi oleh sumber daya yang sama dapat bervariasi, atau efektivitas dari kontrol yang tersedia mungkin berbeda.

d. Tingkat Estimasi Risiko

Estimasi risiko memberikan penilaian untuk kemungkinan serta dampak dari suatu risiko. Penilaian ini bisa bersifat deskriptif atau numerik. Estimasi risiko didasarkan pada konsekuensi dan kemungkinan yang telah ditentukan. Selain itu, dapat juga memperhitungkan keuntungan biaya, kepedulian dari pihak-pihak terkait, dan faktor lain yang relevan untuk penilaian risiko.

Estimasi risiko merupakan gabungan dari kemungkinan terjadinya kejadian dan dampaknya.

D. EVALUASI RISIKO

Karakteristik dari keputusan yang berhubungan dengan penilaian risiko serta standar penilaian risiko yang akan digunakan untuk membuat keputusan telah ditentukan saat menetapkan konteks. Keputusan dan konteks ini perlu diperiksa kembali dengan lebih mendalam pada fase ini ketika sudah memahami lebih lanjut mengenai risiko tertentu yang telah diidentifikasi. Untuk menilai risiko, organisasi harus melakukan perbandingan antara perkiraan risiko dengan standar penilaian risiko yang telah ditentukan selama proses penetapan konteks.

Kriteria untuk menilai risiko yang digunakan dalam pengambilan keputusan harus sejalan dengan kondisi manajemen risiko untuk keamanan informasi, baik yang berasal dari luar maupun dalam. Hal ini harus didefinisikan dengan jelas dan juga mempertimbangkan tujuan perusahaan serta perspektif dari pihak-pihak yang terlibat. Keputusan yang dibuat selama proses penilaian risiko terutama didasarkan pada tingkat risiko yang dianggap dapat diterima. Namun, hal-hal seperti dampak, kemungkinan, dan tingkat keyakinan dalam menemukan dan menganalisis risiko juga harus diperhatikan. Penggabungan beberapa risiko yang rendah atau sedang dapat membuat risiko secara keseluruhan menjadi jauh lebih tinggi dan oleh karena itu perlu diatasi.

Pertimbangan harus mencakup :

1) Sifat keamanan informasi: jika salah satu kriteria tidak relevan bagi organisasi (misalnya hilangnya kerahasiaan), maka semua risiko yang berdampak pada kriteria ini mungkin tidak relevan;

2) Kepentingan kegiatan usaha atau aktivitas yang didukung oleh sumber daya tertentu atau kelompok sumber daya: jika suatu kegiatan dianggap tidak terlalu penting, maka risiko yang terkait dengannya akan dianggap lebih rendah dibandingkan risiko yang mempengaruhi kegiatan atau proses yang lebih signifikan.

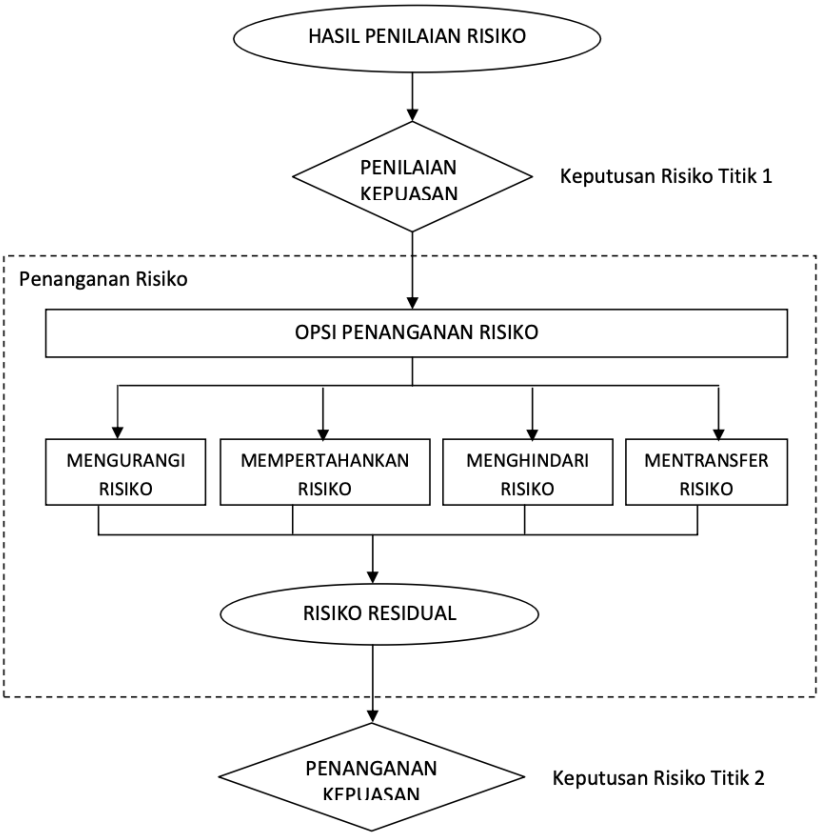
Evaluasi ancaman memanfaatkan pemahaman yang didapat dari penilaian ancaman guna menentukan langkah-langkah yang akan diambil di masa depan. Pilihan yang diambil harus meliputi:

1) Apakah aktivitas perlu dilakukan
2) Pentingnya penanganan risiko dengan mempertimbangkan perkiraan tingkat risiko.

Ketika mengevaluasi risiko, syarat-syarat dari perjanjian, regulasi, dan ketentuan yang berlaku merupakan aspek yang harus diperhatikan selain dari risiko yang telah diantisipasi.

E. PENANGANAN RISIKO

Ada empat opsi yang ada untuk mengelola risiko: menurunkan risiko, menerima risiko, menghindari risiko dan mengalihkan risiko. Tidak sama dengan "mengelola risiko". ISO/IEC 27001 4.2.1. f) 2) memakai definisi "menghadapi risiko". Gambar 2 menggambarkan proses pengelolaan risiko dalam manajemen keamanan informasi .



Gambar 7. 1. Kegiatan Penanganan Risiko

Sumber: Website https://medium.com

Keputusan dalam mengatur risiko seharusnya didasarkan pada analisis risiko, estimasi biaya yang diperlukan untuk menerapkan keputusan itu, serta manfaat yang diinginkan dari keputusan yang diambil.

Jika penurunan yang substansial ketika ancaman dapat dicapai tanpa pengeluaran yang besar, pilihan itu seharusnya dilaksanakan. Alternatif lain untuk peningkatan mungkin tidak begitu menguntungkan dan perlu dipertimbangkan apakah hal itu dapat dibenarkan.

Secara umum, risiko yang dapat memberikan dampak negatif harus dijaga pada tingkat terendah mungkin dan tidak tergantung pada standar yang kaku. Manajer harus memperhatikan risiko yang jarang muncul tetapi

memiliki potensi dampak yang signifikan. Dalam kondisi seperti tersebut, mungkin diperlukan untuk mengambil langkah pengendalian yang tidak sepenuhnya logis hanya demi pertimbangan ekonomi (misalnya, tindakan untuk memastikan kelangsungan operasional dianggap penting untuk menangani risiko yang sangat besar).

Ada empat metode untuk mengelola risiko yang tidak saling menutup satu sama lain. Terkadang, organisasi dapat memperoleh manfaat signifikan saat menggabungkan beberapa pendekatan, misalnya mengurangi potensi risiko terjadi, mereduksi dampaknya, serta memindahkan atau menanggung risiko yang tersisa. Beberapa cara penanganan risiko mungkin efektif dalam menangani lebih dari satu jenis risiko (pelatihan dan pemahaman tentang perlindungan data).

Harus ada strategi untuk menghadapi risiko yang secara jelas menguraikan urutan prioritas untuk setiap penanganan risiko serta waktu pelaksanaannya. Penentuan prioritas dapat dilakukan melalui berbagai metode, termasuk pengklasifikasian ancaman dan penilaian biaya berbanding manfaat. Kewajiban untuk menemukan penyeimbangan antara biaya implementasi kontrol dan pengelolaan pembiayaan terletak pada manajer organisasi.

Memahami pengendalian yang tersedia dapat mengindikasikan yakni jumlah pengendalian tersebut mungkin lebih dari yang dibutuhkan saat ini, terutama jika dilihat dari sisi biaya. Ini juga mencakup pengeluaran untuk pemeliharaan. Jika ada niat untuk menghilangkan pengendalian yang terlalu banyak atau tidak relevan, khususnya yang menghasilkan biaya perawatan yang besar, aspek pengamanan informasi dan biaya wajib diperhatikan. Karena pengendalian dapat saling berinteraksi, menghapus kontrol yang tidak perlu dapat berisiko menurunkan tingkat perlindungan secara umum. Di samping itu, dalam beberapa kasus, sangat bijaksana untuk membiarkan pengendalian yang terlalu banyak tetap ada dibandingkan mengeluarkannya.

Untuk mengatasi ancaman perlu dipikirkan dengan memperhatikan:

1) Bagaimana pihak-pihak yang terlibat merasakan risiko tersebut;
2) Metode paling efektif untuk berinteraksi dengan pihak-pihak itu.

Penentuan konteks menyajikan informasi mengenai regulasi dan ketentuan yang harus dipatuhi oleh sebuah organisasi. Ancaman bagi organisasi muncul jika ketentuan tidak diikuti, sehingga tindakan untuk meminimalkan kemungkinan tersebut perlu diterapkan. Semua kendala -

baik yang bersifat organisasi, teknis, struktural, dan lainnya - yang teridentifikasi selama penentuan konteks harus diperhatikan dalam proses manajemen risiko.

Setelah penyusunan strategi penanganan, penting untuk mengenali risiko yang masih ada. Ini mencakup memperbarui atau mengulangi evaluasi risiko, dengan memperhitungkan dampak yang diinginkan dari tindakan penanganan risiko yang diajukan.

Jika terdapat ancaman yang tersisa yang tidak sesuai dengan standar penerimaan ancaman perusahaan, maka pengelolaan risiko yang lebih mendalam dapat diperlukan sebelum berlanjut ke tahap penerimaan ancaman. Untuk informasi lebih lanjut, silakan lihat ISO/IEC 27002, Klausul 0.3.

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).

D. METODE PERLINDUNGAN PERANGKAT KERAS

Perlindungan perangkat keras menjadi aspek krusial dalam menjaga keamanan sistem komputasi dari ancaman eksternal maupun internal. Dengan meningkatnya serangan berbasis perangkat keras seperti *Firmware attacks*, side-channel *attacks*, dan eksploitasi pada rantai pasokan perangkat keras (*Hardware Supply Chain attacks*), langkah-langkah mitigasi yang efektif sangat diperlukan (Anderson, 2022). Dalam bab ini, akan dibahas beberapa metode utama dalam perlindungan perangkat keras, termasuk enkripsi berbasis perangkat keras, penggunaan Trusted Platform Module (TPM), keamanan dalam desain chip, perlindungan

perangkat mobile dan IoT, serta studi kasus implementasi keamanan perangkat keras di industri manufaktur.

1. Enkripsi dan Autentikasi Berbasis Perangkat Keras

Salah satu metode perlindungan perangkat keras yang paling fundamental adalah penerapan enkripsi dan autentikasi berbasis perangkat keras. Teknik ini memungkinkan data yang tersimpan atau yang sedang diproses dalam perangkat keras tetap terlindungi, bahkan jika perangkat fisik jatuh ke tangan yang tidak berwenang.

a. *Hardware-Based Encryption*: Dibandingkan dengan enkripsi berbasis perangkat lunak, enkripsi berbasis perangkat keras menawarkan performa yang lebih baik dan tingkat keamanan yang lebih tinggi karena tidak bergantung pada sistem operasi yang rentan terhadap serangan (*rootkits*, *Malware*, dan eksploitasi OS-level) (Schneier, 2023). Contoh penerapan enkripsi berbasis perangkat keras meliputi:
   1) *Self-Encrypting Drives* (SEDs) yang menggunakan on-the-fly encryption untuk melindungi data di dalam hard drive atau SSD.
   2) *Secure Enclaves*, seperti *Apple Secure Enclave* dan Intel SGX (*Software Guard Extensions*), yang menyediakan lingkungan eksekusi yang terisolasi untuk pengolahan data sensitif.

b. *Hardware-Based Authentication*: Penggunaan perangkat keras sebagai faktor autentikasi tambahan menjadi semakin populer, terutama dalam lingkungan dengan persyaratan keamanan tinggi. Contoh implementasi autentikasi berbasis perangkat keras meliputi:
   1) *Security Tokens* (contohnya YubiKey) yang memungkinkan autentikasi multi-faktor tanpa memerlukan jaringan eksternal.
   2) *Biometric Authentication Chips*, seperti pemindai sidik jari pada perangkat smartphone dan laptop, yang menggunakan sensor khusus untuk meningkatkan keamanan akses fisik.

2. Penggunaan Trusted Platform Module (TPM)

Trusted Platform Module (TPM) adalah sebuah mikroprosesor kriptografis yang dirancang untuk meningkatkan keamanan perangkat keras dengan menyediakan fungsi enkripsi berbasis perangkat keras, manajemen kunci kriptografi, dan autentikasi platform (NIST, 2022). TPM banyak digunakan dalam sistem operasi modern, seperti Windows 11 yang mewajibkan dukungan TPM 2.0 untuk meningkatkan keamanan perangkat. Keunggulan utama TPM meliputi:

a. *Storage* dan Manajemen Kunci Kriptografi: TPM menyimpan kunci enkripsi dalam modul yang terpisah dari sistem utama, sehingga tidak dapat diakses oleh perangkat lunak berbahaya.
b. *Platform Integrity Measurement*: TPM dapat digunakan untuk mengecek integritas sistem selama proses boot melalui teknologi Secure Boot dan Measured Boot.
c. *Authentication and Secure Identity*: TPM membantu dalam pembuatan dan pengelolaan identitas digital yang aman, yang digunakan dalam implementasi teknologi BitLocker untuk enkripsi disk penuh (full disk encryption).

Studi menunjukkan bahwa penggunaan TPM secara signifikan mengurangi risiko eksploitasi *Firmware* dan serangan berbasis rootkits yang berusaha memanipulasi sistem sebelum sistem operasi dimuat (Goodin, 2021).

3. Keamanan dalam Desain Chip dan Arsitektur Mikroprosesor

Keamanan perangkat keras tidak hanya bergantung pada perangkat tambahan seperti TPM tetapi juga pada desain dasar chip dan mikroprosesor itu sendiri. Beberapa pendekatan utama dalam meningkatkan keamanan pada tingkat arsitektur perangkat keras meliputi:

a. *Secure Boot and Root of Trust*: Teknologi ini memastikan bahwa setiap komponen perangkat lunak yang dimuat saat proses boot berasal dari sumber yang terpercaya dan tidak dimodifikasi oleh pihak ketiga yang tidak sah (Clarke, 2021).
b. *Memory Encryption and Isolation*: Prosesor modern, seperti AMD *Secure Encrypted Virtualization* (SEV) dan *Intel Total Memory Encryption* (TME), menggunakan enkripsi memori untuk mencegah akses tidak sah ke data yang disimpan dalam RAM.
c. *Hardware-Based Access Control*: Menggunakan *Hardware*-assisted *security* untuk membatasi hak akses berdasarkan tingkat keamanan tertentu dalam CPU, seperti fitur ARM *TrustZone* yang memisahkan lingkungan eksekusi aman dan tidak aman dalam arsitektur prosesor mobile.

4. Perlindungan Perangkat Mobile dan IoT

Perangkat mobile dan IoT memiliki risiko keamanan yang unik karena sifatnya yang selalu terhubung ke jaringan dan sering kali tidak memiliki mekanisme perlindungan yang memadai. Beberapa langkah penting dalam perlindungan perangkat mobile dan IoT meliputi:

a. *Secure Boot and Remote Attestation*: Memastikan bahwa *Firmware* yang berjalan pada perangkat mobile dan IoT belum dimodifikasi oleh penyerang.
b. *Network Segmentation*: Memisahkan perangkat IoT dari jaringan utama perusahaan atau organisasi untuk mengurangi risiko eskalasi serangan jika salah satu perangkat dikompromikan.
c. *Regular Firmware Updates and Patch Management*: Pembaruan *Firmware* berkala sangat penting dalam menutup celah keamanan yang ditemukan dalam perangkat IoT dan mobile.

Salah satu tantangan terbesar dalam perlindungan perangkat mobile dan IoT adalah serangan berbasis botnet, seperti Mirai Botnet, yang berhasil menginfeksi ribuan perangkat IoT yang memiliki kredensial default dan mengeksploitasi kelemahan perangkat lunak (Kumar & Lee, 2021).

5. Studi Kasus: Implementasi Keamanan Perangkat Keras di Industri Manufaktur

Industri manufaktur menghadapi tantangan keamanan perangkat keras yang unik karena banyaknya perangkat otomatisasi industri (*Industrial Control Systems* - ICS) dan IoT yang digunakan dalam rantai produksi. Studi kasus berikut menunjukkan bagaimana keamanan perangkat keras diterapkan dalam lingkungan manufaktur. Kasus: Implementasi Secure *Manufacturing* di Intel

Intel telah menerapkan pendekatan keamanan berbasis perangkat keras dalam rantai produksinya untuk mencegah manipulasi pada chip dan perangkat semikonduktor yang mereka produksi. Beberapa langkah yang diambil meliputi:

a. *Chip Anti-Tampering*: Setiap chip dilengkapi dengan teknologi unik untuk mencegah pemalsuan dan pemodifikasian oleh pihak yang tidak berwenang.
b. *Supply Chain Verification*: Penerapan teknologi blockchain untuk memastikan bahwa setiap komponen dalam rantai pasokan berasal dari sumber terpercaya.
c. *Security Testing in Manufacturing Process*: Melibatkan pengujian keamanan ketat pada perangkat sebelum didistribusikan ke pelanggan, termasuk penilaian terhadap serangan fisik dan manipulasi *Firmware* (Intel Security Report, 2022).

Pendekatan ini memungkinkan Intel untuk memastikan bahwa produknya tidak hanya memiliki performa tinggi tetapi juga memenuhi standar keamanan industri yang ketat.

E. METODE PERLINDUNGAN PERANGKAT LUNAK

Perangkat lunak merupakan salah satu elemen paling rentan terhadap serangan siber. Keamanan perangkat lunak menjadi faktor kunci dalam menjaga integritas, kerahasiaan, dan ketersediaan data serta sistem yang digunakan oleh individu dan organisasi. Dengan meningkatnya serangan berbasis perangkat lunak, metode perlindungan yang efektif harus diterapkan secara menyeluruh, mulai dari proses pengembangan hingga saat perangkat lunak digunakan dalam lingkungan operasional (Schneier, 2023).

1. Penggunaan *Sandboxing* dan Virtualisasi

Sandboxing dan virtualisasi adalah teknik utama dalam isolasi eksekusi perangkat lunak untuk mencegah *Malware* atau aplikasi yang tidak terpercaya dari mengakses sumber daya sistem utama.

Sandboxing adalah metode keamanan yang menjalankan aplikasi dalam lingkungan yang terisolasi sehingga program yang mencurigakan tidak dapat mengakses data atau sistem di luar batasan yang ditentukan. Contoh penerapannya:

a. *Google Chrome* dan *Microsoft Edge* menggunakan *Sandboxing* untuk membatasi akses browser terhadap sistem operasi, sehingga jika terjadi eksploitasi di dalam browser, dampaknya dapat diminimalisir (Google Security Blog, 2021).
b. Android dan iOS menerapkan *Sandboxing* untuk membatasi aplikasi pihak ketiga agar tidak dapat mengakses data aplikasi lain.
c. Virtualisasi, di sisi lain, memungkinkan sistem operasi atau aplikasi berjalan di lingkungan yang terpisah dari perangkat keras utama. Teknologi ini memungkinkan implementasi *Virtual Machines* (VMs) atau containers seperti Docker dan Kubernetes untuk meningkatkan keamanan dan fleksibilitas sistem perangkat lunak (Anderson, 2022).

Manfaat utama *Sandboxing* dan virtualisasi termasuk:

a. Mengurangi risiko serangan *Malware* dengan membatasi akses ke sumber daya sistem.
b. Mencegah eksploitasi berbasis aplikasi dari berdampak pada sistem utama.

c. Memungkinkan uji coba perangkat lunak dalam lingkungan yang aman tanpa membahayakan sistem produksi.

2. Penerapan Prinsip Keamanan dalam Pengembangan Perangkat Lunak (Secure Coding Practices)

Salah satu langkah paling penting dalam perlindungan perangkat lunak adalah menerapkan prinsip keamanan sejak tahap pengembangan perangkat lunak. Pendekatan ini dikenal sebagai *Secure Coding Practices*, yang mencakup teknik berikut:

a. *Principle of Least Privilege* (PoLP): Perangkat lunak hanya boleh diberikan akses minimal yang diperlukan untuk menjalankan tugasnya, sehingga jika terjadi kompromi, dampaknya tetap terbatas (Howard & LeBlanc, 2020).
b. *Input Validation and Sanitization*: Semua data yang dimasukkan oleh pengguna harus divalidasi dan dibersihkan untuk mencegah serangan seperti SQL Injection atau Cross-Site Scripting (XSS).
c. *Use of Secure APIs*: Menghindari penggunaan fungsi yang tidak aman dalam pengembangan perangkat lunak dan menggantinya dengan API yang telah diuji keamanannya.
d. *Code Reviews and Static Analysis*: Meninjau kode secara berkala menggunakan alat analisis statis seperti SonarQube atau Checkmarx untuk mendeteksi potensi kelemahan keamanan sebelum perangkat lunak diproduksi.

Dengan menerapkan prinsip-prinsip ini, pengembang dapat mengurangi risiko eksploitasi kerentanan perangkat lunak yang dapat membahayakan sistem dan data pengguna.

3. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS)

Intrusion Detection Systems (IDS) dan *Intrusion Prevention Systems* (IPS) adalah solusi keamanan yang dirancang untuk mendeteksi dan mencegah serangan terhadap perangkat lunak dan jaringan.

IDS bertugas untuk memantau aktivitas sistem atau jaringan dan mendeteksi perilaku mencurigakan yang dapat mengindikasikan serangan siber, seperti anomali lalu lintas jaringan atau upaya akses ilegal. IDS dapat bersifat *Host-Based* IDS (HIDS) atau *Network-Based* IDS (NIDS) (Mirkovic & Reiher, 2020).

IPS, di sisi lain, tidak hanya mendeteksi ancaman tetapi juga bertindak secara otomatis untuk memblokir serangan sebelum mencapai targetnya. Contohnya adalah perangkat *firewall* canggih seperti *Cisco Firepower* IPS

yang mampu mengidentifikasi dan memblokir lalu lintas mencurigakan secara *real-time*.

Keuntungan utama IDS/IPS dalam perlindungan perangkat lunak meliputi:

a. Mendeteksi serangan berbasis eksploitasi perangkat lunak seperti buffer overflow dan brute force attack.
b. Menganalisis lalu lintas jaringan untuk mengidentifikasi pola serangan yang mencurigakan.
c. Memblokir akses yang mencurigakan sebelum mencapai sistem target.

4. Keamanan Sistem Operasi dan Mitigasi Eksploitasi

Sistem operasi (OS) adalah komponen inti yang mengelola perangkat lunak dan perangkat keras. Oleh karena itu, menjaga keamanan sistem operasi adalah langkah utama dalam melindungi perangkat lunak dari ancaman. Beberapa teknik utama dalam meningkatkan keamanan OS meliputi:

a. *Regular Security Patching*: Pembaruan sistem operasi secara berkala untuk memperbaiki kerentanan keamanan yang ditemukan (Schneier, 2023).
b. *Address Space Layout Randomization* (ASLR): Teknik yang mengacak lokasi memori tempat program dan pustaka sistem disimpan untuk mencegah eksploitasi berbasis *buffer overflow*.
c. *Data Execution Prevention* (DEP): Mencegah eksekusi kode berbahaya di area memori yang seharusnya tidak dapat dieksekusi.
d. *Use of Secure Boot*: Memastikan hanya perangkat lunak yang telah diverifikasi dapat dijalankan saat startup, sehingga mencegah serangan *rootkit* dan *bootkit*.

Penerapan teknik ini secara konsisten dapat mengurangi kemungkinan eksploitasi sistem operasi oleh *Malware* atau penyerang siber.

5. Studi Kasus: Penerapan DevSecOps dalam Pengembangan Perangkat Lunak Modern

DevSecOps adalah pendekatan modern dalam pengembangan perangkat lunak yang mengintegrasikan keamanan sebagai bagian dari siklus hidup perangkat lunak (Software Development Lifecycle - SDLC).

Kasus: Implementasi DevSecOps di Netflix

Netflix adalah salah satu perusahaan yang mengadopsi DevSecOps secara luas dalam siklus pengembangan perangkat lunak mereka. Beberapa langkah yang mereka ambil untuk memastikan keamanan perangkat lunak meliputi:

a. Automated Security Testing: Netflix menggunakan alat otomatis seperti Gauntlt dan OWASP ZAP untuk menguji keamanan aplikasi mereka dalam lingkungan produksi secara real-time.
b. Security-as-Code: Tim pengembang memasukkan kebijakan keamanan langsung ke dalam kode sumber dan mengotomatiskan kepatuhan terhadap standar keamanan menggunakan alat seperti HashiCorp Vault.
c. Real-time Threat Detection: Sistem Netflix dilengkapi dengan machine learning-based anomaly detection, yang dapat mendeteksi perilaku mencurigakan dan mengaktifkan mitigasi otomatis dalam hitungan detik.

Keberhasilan Netflix dalam mengimplementasikan DevSecOps menunjukkan bahwa integrasi keamanan dalam proses pengembangan perangkat lunak tidak hanya meningkatkan keamanan tetapi juga mempercepat siklus rilis aplikasi tanpa mengorbankan perlindungan terhadap ancaman siber.

F. TEKNIK KRIPTOGRAFI UNTUK KEAMANAN SISTEM

Kriptografi merupakan salah satu teknik fundamental dalam keamanan informasi yang digunakan untuk melindungi data dari akses tidak sah. Dalam dunia digital modern, kriptografi berperan dalam berbagai aspek keamanan, mulai dari enkripsi komunikasi hingga perlindungan data dalam sistem penyimpanan dan transaksi finansial. Dengan meningkatnya ancaman terhadap keamanan siber, teknik kriptografi terus berkembang untuk menghadapi berbagai metode serangan yang semakin canggih (Schneier, 2023).

1. Prinsip Dasar Kriptografi dan Penerapannya

Kriptografi berasal dari bahasa Yunani, kryptos yang berarti "tersembunyi" dan graphein yang berarti "menulis". Prinsip utama dalam kriptografi adalah menjaga kerahasiaan (confidentiality), integritas (integrity), otentikasi (authentication), dan non-repudiasi (non-repudiation) dalam komunikasi digital (Stallings, 2020).

Beberapa konsep utama dalam kriptografi adalah:

a. Enkripsi dan Dekripsi: Proses mengubah data asli (plaintext) menjadi bentuk yang tidak dapat dibaca (ciphertext) menggunakan algoritma enkripsi, dan sebaliknya.
b. Kunci Kriptografi: Elemen penting dalam enkripsi yang menentukan bagaimana data dienkripsi dan didekripsi. Terdapat dua jenis utama kunci:
c. Kriptografi Simetris: Menggunakan satu kunci untuk enkripsi dan dekripsi, seperti dalam algoritma AES.
d. Kriptografi Asimetris: Menggunakan dua kunci (publik dan privat) untuk proses enkripsi dan dekripsi, seperti dalam algoritma RSA dan ECC.
e. Fungsi Hash: Digunakan untuk memastikan integritas data tanpa memerlukan kunci enkripsi, seperti dalam algoritma SHA-256.

2. Algoritma Kriptografi Modern (AES, RSA, ECC)

Teknologi kriptografi terus berkembang dengan munculnya berbagai algoritma yang menawarkan kombinasi keamanan dan efisiensi yang lebih baik. Beberapa algoritma utama yang digunakan dalam sistem modern meliputi:

a. *Advanced Encryption Standard* (AES)

AES adalah algoritma enkripsi simetris yang dikembangkan oleh *National Institute of Standards and Technology* (NIST) dan menjadi standar global dalam keamanan data (Daemen & Rijmen, 2021). AES menggunakan ukuran kunci 128-bit, 192-bit, atau 256-bit dan telah diadopsi secara luas dalam aplikasi seperti:

1) Enkripsi data pada perangkat penyimpanan (misalnya, BitLocker pada Windows).
2) Komunikasi aman dalam jaringan Wi-Fi (WPA2 dan WPA3).
3) Proteksi data dalam sistem cloud dan layanan online.

b. Rivest-Shamir-Adleman (RSA)

RSA adalah algoritma kriptografi asimetris yang digunakan dalam banyak sistem keamanan, terutama untuk:

1) Enkripsi dan dekripsi data yang memerlukan kunci publik dan privat.
2) Pembuatan tanda tangan digital untuk memastikan autentikasi pengguna.
3) Sistem keamanan berbasis PKI (Public Key Infrastructure).

RSA menawarkan keamanan yang tinggi tetapi kurang efisien dibandingkan AES dalam menangani volume data yang besar. Oleh karena itu, RSA sering dikombinasikan dengan AES dalam berbagai sistem keamanan (Stallings, 2020).

c. *Elliptic Curve Cryptography* (ECC)

ECC adalah algoritma kriptografi asimetris yang lebih efisien dibandingkan RSA karena dapat mencapai tingkat keamanan yang setara dengan ukuran kunci yang lebih kecil. ECC banyak digunakan dalam:

1) Keamanan komunikasi dalam perangkat IoT yang memiliki keterbatasan sumber daya.
2) Tanda tangan digital dalam transaksi *blockchain* dan *cryptocurrency*.
3) Sertifikat SSL/TLS dalam komunikasi web yang aman.

Dengan ukuran kunci yang lebih kecil, ECC menawarkan kecepatan eksekusi yang lebih tinggi dan penggunaan daya yang lebih rendah, menjadikannya pilihan utama dalam sistem kriptografi modern (Koblitz & Menezes, 2021).

3. Manajemen Kunci Kriptografi dan Protokol Enkripsi

Manajemen kunci adalah aspek kritis dalam sistem kriptografi. Bahkan algoritma yang paling kuat sekalipun dapat menjadi tidak aman jika kunci kriptografi tidak dikelola dengan baik. Beberapa prinsip utama dalam manajemen kunci meliputi:

a. *Secure Key Storage*: Kunci harus disimpan di lokasi yang aman, seperti dalam *Hardware* Security Module (HSM) atau Trusted Platform Module (TPM) untuk mencegah pencurian atau manipulasi.
b. *Key Rotation*: Kunci harus diperbarui secara berkala untuk mengurangi risiko kompromi.
c. *Access Control*: Hanya entitas yang berwenang yang boleh mengakses atau menggunakan kunci.

Sementara itu, beberapa protokol enkripsi yang banyak digunakan dalam pengamanan data meliputi:

a. IPsec: Digunakan untuk mengamankan komunikasi dalam jaringan menggunakan enkripsi berbasis AES atau RSA.
b. PGP (*Pretty Good Privacy*): Digunakan dalam enkripsi email untuk melindungi komunikasi antar pengguna.

c. SSH (*Secure Shell*): Digunakan untuk koneksi jarak jauh yang aman pada server dan perangkat jaringan.

4. Implementasi SSL/TLS untuk Komunikasi Aman

Secure Sockets Layer (SSL) dan Transport Layer Security (TLS) adalah protokol keamanan yang digunakan dalam komunikasi internet untuk melindungi data yang dikirim antara server dan klien. TLS menggantikan SSL dan menjadi standar utama dalam keamanan komunikasi web.

Manfaat SSL/TLS dalam Keamanan Sistem

a. Enkripsi Data: Memastikan bahwa semua data yang dikirim melalui internet tidak dapat dibaca oleh pihak ketiga.
b. Autentikasi: Memverifikasi identitas server untuk mencegah serangan *Man-in-the-Middle* (MitM).
c. Integritas Data: Menggunakan kode autentikasi pesan (*Message Authentication Code* - MAC) untuk memastikan bahwa data tidak diubah selama proses transmisi.

SSL/TLS diterapkan dalam berbagai layanan, termasuk:

a. Protokol HTTPS untuk keamanan situs web.
b. Keamanan transaksi keuangan dan pembayaran online.
c. Keamanan email dan layanan komunikasi terenkripsi.

5. Studi Kasus: Serangan terhadap Enkripsi dan Mitigasinya

a. Kasus: Serangan terhadap Enkripsi dalam TLS (*BEAST Attack*)

Pada tahun 2011, serangan BEAST (Browser Exploit Against SSL/TLS) ditemukan oleh peneliti keamanan yang mengeksploitasi kelemahan dalam enkripsi TLS 1.0. Penyerang dapat mengakses komunikasi yang dienkripsi dengan mendekripsi paket data yang dikirim antara klien dan server (Rizzo & Duong, 2011).

b. Mitigasi Serangan
    1) Mengupgrade sistem ke TLS 1.2 atau TLS 1.3, yang memiliki perlindungan lebih kuat terhadap serangan BEAST.
    2) Menggunakan mode enkripsi yang lebih aman, seperti GCM (Galois/Counter Mode), dibandingkan CBC (*Cipher Block Chaining*).
    3) Menerapkan HTTP *Strict Transport Security* (HSTS) untuk memastikan koneksi hanya menggunakan protokol aman.

G. MANAJEMEN KEAMANAN PERANGKAT KERAS DAN PERANGKAT LUNAK

Manajemen keamanan perangkat keras dan perangkat lunak merupakan komponen kunci dalam strategi perlindungan sistem informasi. Dengan ancaman yang semakin berkembang, pendekatan sistematis diperlukan untuk memastikan bahwa perangkat keras dan perangkat lunak tetap terlindungi dari eksploitasi. Dalam bab ini, akan dibahas berbagai aspek penting, termasuk kebijakan keamanan informasi dan standar internasional, manajemen patch dan pembaruan sistem, keamanan dalam rantai pasokan, implementasi keamanan berbasis AI dan *machine learning*, serta studi kasus serangan *Supply Chain* dan dampaknya pada perusahaan teknologi.

1. Kebijakan Keamanan Informasi dan Standar Internasional (ISO 27001, NIST)

Keamanan informasi tidak hanya bergantung pada teknologi tetapi juga pada kebijakan dan regulasi yang mengatur bagaimana informasi dikelola dan dilindungi. Dua standar utama yang digunakan secara global dalam manajemen keamanan informasi adalah:

a. ISO 27001: Standar internasional untuk sistem manajemen keamanan informasi (ISMS) yang menyediakan kerangka kerja untuk menetapkan, menerapkan, dan memelihara praktik terbaik dalam keamanan informasi. Standar ini mencakup aspek kebijakan keamanan, manajemen risiko, dan audit keamanan.
b. NIST *Cybersecurity Framework*: Dikembangkan oleh National Institute of Standards and Technology (NIST), *framework* ini berfokus pada identifikasi, perlindungan, deteksi, respons, dan pemulihan dari serangan siber.

Kepatuhan terhadap standar ini memungkinkan organisasi untuk membangun ekosistem keamanan yang lebih kuat dan mampu menghadapi ancaman siber dengan lebih baik.

2. Manajemen Patch dan Pembaruan Sistem

Pembaruan sistem perangkat lunak dan *Firmware* sangat penting dalam menjaga keamanan. Banyak serangan siber terjadi karena eksploitasi kerentanan yang belum diperbaiki. Oleh karena itu, manajemen patch yang efektif mencakup:

a. Pembaruan rutin: Menyediakan dan menerapkan patch keamanan secara berkala untuk menutup celah keamanan yang ditemukan.
b. Patch Management Automation: Menggunakan alat otomatis seperti WSUS (*Windows Server Update Services*) atau Red Hat Satellite untuk mengelola pembaruan dalam skala besar.
c. Testing sebelum deployment: Menguji patch di lingkungan uji sebelum diterapkan ke sistem produksi untuk menghindari dampak negatif yang tidak diinginkan.

3. Keamanan dalam Rantai Pasokan Perangkat Keras dan Perangkat Lunak

Serangan *Supply Chain* telah meningkat dalam beberapa tahun terakhir, di mana penyerang menargetkan vendor perangkat keras dan perangkat lunak untuk menyusup ke sistem pelanggan mereka. Tindakan mitigasi yang dapat diterapkan meliputi:

a. Verifikasi Keaslian Komponen Perangkat Keras: Menggunakan teknologi seperti chip anti-tampering dan blockchain-based *Supply Chain* tracking.
b. Kode Sumber yang Transparan: Menerapkan kebijakan code review dan memverifikasi integritas perangkat lunak yang berasal dari pihak ketiga.
c. *Security Audits* terhadap Vendor: Menetapkan persyaratan keamanan yang ketat untuk semua vendor dalam rantai pasokan perangkat keras dan perangkat lunak.

4. Implementasi Keamanan Berbasis AI dan Machine Learning

Kecerdasan buatan (AI) dan *machine learning* (ML) semakin digunakan untuk meningkatkan keamanan siber. Beberapa aplikasi utama dari teknologi ini meliputi:

a. Deteksi ancaman secara real-time: AI digunakan dalam sistem SIEM (*Security Information and Event Management*) untuk mengidentifikasi pola anomali dalam lalu lintas jaringan.
b. Prediksi Serangan Siber: ML digunakan untuk mempelajari pola serangan sebelumnya dan memperkirakan potensi serangan di masa mendatang.
c. Otomatisasi respons keamanan: Sistem berbasis AI dapat mengambil tindakan otomatis dalam menghadapi ancaman, seperti memblokir alamat IP berbahaya atau mengkarantina file yang mencurigakan.

5. Studi Kasus: Serangan *Supply Chain* dan Dampaknya pada Perusahaan Teknologi

Kasus: Serangan *SolarWinds* (2020)

SolarWinds mengalami serangan *Supply Chain* ketika pembaruan perangkat lunak mereka disusupi oleh penyerang, yang kemudian digunakan untuk menyusup ke berbagai instansi pemerintah dan perusahaan teknologi besar.

Dampak:

a. Ribuan organisasi terkena dampaknya, termasuk pemerintah AS dan perusahaan besar seperti Microsoft.
b. Menyebabkan kebocoran data berskala besar dan ancaman terhadap keamanan nasional.

Pelajaran yang dapat dipetik:

a. Perlunya audit keamanan yang lebih ketat terhadap kode sumber dan rantai pasokan perangkat lunak.
b. Pentingnya deteksi ancaman berbasis AI untuk mengidentifikasi perilaku mencurigakan lebih awal.

H. BEST PRACTICES DALAM KEAMANAN SIBER

Keamanan siber memerlukan pendekatan yang berlapis dan berkelanjutan. Dalam bab ini, akan dibahas konsep *Zero Trust Architecture* (ZTA), penerapan *Multi-Factor Authentication* (MFA), strategi pemulihan dari serangan siber, manajemen risiko TI, serta studi kasus insiden keamanan besar dalam sejarah industri teknologi.

1. Konsep *Zero Trust Architecture* (ZTA)

Zero Trust Architecture (ZTA) adalah paradigma keamanan yang mengasumsikan bahwa tidak ada entitas yang dapat dipercaya secara default, baik di dalam maupun di luar jaringan. Prinsip utama ZTA meliputi:

a. Verifikasi terus-menerus: Tidak ada pengguna atau perangkat yang otomatis dipercaya; setiap akses harus diautentikasi dan diverifikasi.
b. Segmentasi Jaringan: Memisahkan jaringan untuk menghindari akses tidak sah ke seluruh sistem jika terjadi kompromi.
c. Prinsip *Least Privilege*: Pengguna hanya diberikan akses ke sumber daya yang benar-benar mereka butuhkan.

2. Penerapan *Multi-Factor Authentication* (MFA)

MFA merupakan metode autentikasi yang mewajibkan pengguna untuk memberikan lebih dari satu faktor validasi untuk mengakses suatu sistem, seperti:

a. Kombinasi kata sandi dan OTP (One-Time Password).
b. Biometrik seperti sidik jari atau pengenalan wajah.
c. Autentikasi perangkat (*Hardware* tokens seperti YubiKey).

MFA telah terbukti secara signifikan mengurangi risiko serangan brute force dan phishing.

3. Strategi Pemulihan dari Serangan Siber

Ketika terjadi serangan siber, organisasi harus memiliki strategi pemulihan yang efektif, seperti:

a. *Disaster Recovery Plan* (DRP): Rencana untuk mengembalikan sistem yang terdampak serangan *Ransomware* atau DDoS.
b. *Regular Data Backup*: Penyimpanan cadangan data secara berkala untuk menghindari kehilangan data permanen.
c. *Incident Response Team*: Tim yang bertugas menangani insiden keamanan dan menyiapkan langkah pemulihan.

4. Manajemen Risiko dalam Pengembangan dan Operasional TI

Manajemen risiko dalam keamanan siber mencakup:

a. Identifikasi ancaman potensial: Memahami jenis serangan yang dapat terjadi.
b. Penilaian risiko: Mengukur dampak dari berbagai jenis serangan terhadap operasional bisnis.
c. Mitigasi dan monitoring: Mengembangkan strategi pencegahan dan pemantauan ancaman secara real-time.

5. Studi Kasus: Pembelajaran dari Insiden Keamanan Besar

Kasus: Serangan *WannaCry* (2017)

WannaCry adalah *Ransomware* global yang mengeksploitasi kelemahan dalam protokol SMB di sistem *Windows*.

Dampak:

a. Ratusan ribu komputer di lebih dari 150 negara terinfeksi.
b. Rumah sakit, institusi keuangan, dan bisnis besar mengalami kerugian miliaran dolar.

Pelajaran yang dapat diambil:

a. Pentingnya pembaruan perangkat lunak secara rutin.
b. Backup data secara berkala untuk menghindari kehilangan data akibat *Ransomware*.

I. RANGKUMAN

Keamanan perangkat keras dan perangkat lunak merupakan aspek krusial dalam melindungi sistem informasi dari ancaman siber yang semakin berkembang. Keamanan perangkat keras mencakup perlindungan terhadap komponen fisik komputer, server, dan jaringan dari manipulasi, sabotase, dan akses tidak sah. Sementara itu, keamanan perangkat lunak berfokus pada pengembangan, pemeliharaan, dan pengamanan sistem dari eksploitasi kerentanan yang dapat membahayakan data dan infrastruktur. Dalam era digital ini, eksploitasi perangkat lunak dan serangan berbasis *Firmware* telah meningkat secara signifikan, memperlihatkan pentingnya strategi keamanan yang komprehensif dan berlapis.

Berbagai ancaman siber yang semakin berkembang meliputi *Ransomware* yang lebih canggih dengan metode double extortion, serangan *Zero-Day* yang mengeksploitasi celah keamanan yang belum diperbaiki, serta serangan *Supply Chain* yang menargetkan vendor perangkat keras dan perangkat lunak. Selain itu, penggunaan kecerdasan buatan (AI) oleh penyerang untuk mengotomatisasi eksploitasi dan menghindari deteksi sistem keamanan menjadi tantangan baru dalam keamanan siber. Sebagai respons terhadap ancaman ini, teknologi keamanan berkembang dengan cepat, termasuk penerapan *Zero Trust Architecture* (ZTA) yang memastikan setiap akses ke sistem harus melalui autentikasi ketat, *Hardware Security Module* (HSM) untuk perlindungan kunci kriptografi, serta implementasi enkripsi canggih seperti *homomorphic encryption* yang memungkinkan perhitungan dilakukan pada data terenkripsi tanpa mendekripsinya terlebih dahulu.

Dalam menghadapi serangan terhadap perangkat keras, beberapa metode perlindungan yang diterapkan antara lain adalah enkripsi berbasis perangkat keras seperti *Self-Encrypting Drives* (SEDs) dan Secure Enclaves, penggunaan *Trusted Platform Module* (TPM) untuk menyimpan

kunci enkripsi dengan aman, serta penerapan *Secure Boot dan Root of Trust* untuk memastikan sistem operasi hanya memuat perangkat lunak yang sah. Perlindungan perangkat *mobile* dan *Internet of Things* (IoT) juga menjadi tantangan tersendiri karena sifatnya yang selalu terhubung ke jaringan. Langkah-langkah mitigasi seperti network segmentation, pembaruan *Firmware* berkala, dan *remote attestation* diterapkan untuk mengurangi risiko eksploitasi pada perangkat ini.

Keamanan perangkat lunak juga membutuhkan berbagai metode perlindungan yang sistematis. Salah satu pendekatan utama adalah penggunaan *Sandboxing* dan virtualisasi untuk membatasi akses aplikasi terhadap sumber daya sistem utama. Selain itu, praktik Secure Coding sangat penting untuk menghindari eksploitasi kode melalui validasi input, penggunaan API yang aman, serta prinsip *Least Privilege* yang membatasi akses perangkat lunak hanya pada fungsi yang diperlukan. Untuk mendeteksi ancaman yang sedang berlangsung, organisasi menerapkan *Intrusion Detection Systems* (IDS) dan Intrusion *Prevention Systems* (IPS) guna memantau dan memblokir aktivitas mencurigakan secara real-time. Keamanan sistem operasi juga diperkuat dengan patching berkala, *Address Space Layout Randomization* (ASLR), dan *Data Execution Prevention* (DEP) guna mencegah eksekusi kode berbahaya. Sebagai contoh, perusahaan seperti Netflix telah mengadopsi pendekatan DevSecOps, di mana keamanan diintegrasikan ke dalam siklus pengembangan perangkat lunak melalui pengujian otomatis dan monitoring ancaman berbasis AI.

Teknik kriptografi juga memainkan peran penting dalam keamanan sistem, dengan berbagai algoritma yang digunakan untuk melindungi data dan komunikasi. *Advanced Encryption Standard* (AES) menjadi standar global dalam enkripsi data berkecepatan tinggi, sementara *Rivest-Shamir-Adleman* (RSA) dan *Elliptic Curve Cryptography* (ECC) digunakan dalam autentikasi dan tanda tangan digital. Manajemen kunci kriptografi yang baik sangat penting, dengan pendekatan seperti *Hardware Security Module* (HSM) dan *Trusted Platform Module* (TPM) untuk menyimpan kunci secara aman serta menerapkan rotasi kunci berkala guna mengurangi risiko kebocoran. Dalam komunikasi digital, *Secure Sockets Layer* (SSL) dan *Transport Layer Security* (TLS) menjadi standar utama dalam melindungi data yang dikirim melalui internet. Studi kasus seperti serangan BEAST Attack (2011) yang mengeksploitasi kelemahan TLS 1.0 menunjukkan pentingnya penggunaan protokol keamanan terbaru seperti TLS 1.2 dan TLS 1.3 untuk memastikan komunikasi yang aman.

Manajemen keamanan perangkat keras dan perangkat lunak membutuhkan pendekatan berbasis kebijakan dan standar internasional, seperti ISO 27001 dan NIST *Cybersecurity Framework*, yang memberikan pedoman bagi organisasi dalam mengelola risiko keamanan informasi. Selain itu, manajemen patch dan pembaruan sistem menjadi krusial dalam menutup celah keamanan yang sering dieksploitasi oleh penyerang. Serangan terhadap rantai pasokan perangkat keras dan perangkat lunak semakin meningkat, seperti yang terlihat dalam kasus *SolarWinds* Attack (2020) yang menyebabkan kebocoran data besar-besaran dan kompromi terhadap berbagai instansi pemerintah serta perusahaan teknologi. Untuk mengatasi ancaman ini, perusahaan mulai menerapkan *Supply Chain verification* berbasis blockchain dan audit keamanan vendor yang lebih ketat. Selain itu, penggunaan AI dan machine learning dalam deteksi ancaman real-time semakin diperkuat untuk mengidentifikasi pola serangan dan melakukan mitigasi otomatis sebelum terjadi eskalasi.

Dalam menerapkan best practices dalam keamanan siber, konsep *Zero Trust Architecture* (ZTA) menjadi landasan utama, di mana setiap permintaan akses harus melalui autentikasi dan verifikasi yang ketat tanpa asumsi kepercayaan terhadap jaringan internal. Selain itu, *Multi-Factor Authentication* (MFA) diterapkan untuk memperkuat perlindungan akses dengan kombinasi kata sandi, OTP (*One-Time Password*), biometrik, atau autentikasi perangkat keras. Organisasi juga perlu menyiapkan strategi pemulihan dari serangan siber, seperti *Disaster Recovery Plan* (DRP), backup data berkala, dan tim respons insiden guna memastikan sistem dapat segera dipulihkan jika terjadi serangan. Dalam konteks manajemen risiko TI, pendekatan yang digunakan mencakup identifikasi ancaman potensial, analisis dampak serangan, serta mitigasi dan pemantauan ancaman secara berkelanjutan. Studi kasus serangan *WannaCry* (2017) menjadi pelajaran berharga dalam pentingnya *patching* rutin dan backup data sebagai langkah mitigasi terhadap *Ransomware.*

Kesimpulannya, keamanan perangkat keras dan perangkat lunak merupakan aspek yang tidak dapat dipisahkan dalam melindungi sistem informasi di era digital. Dengan meningkatnya ancaman siber yang semakin kompleks, diperlukan pendekatan perlindungan yang mencakup kombinasi teknologi, kebijakan, dan strategi manajemen risiko. Penerapan standar keamanan global seperti ISO 27001 dan NIST, pendekatan berbasis Zero Trust, serta adopsi teknologi keamanan mutakhir seperti AI, enkripsi tingkat lanjut, dan DevSecOps menjadi langkah krusial dalam menghadapi tantangan keamanan siber di masa depan. Dengan strategi yang tepat, individu dan organisasi dapat

meningkatkan ketahanan terhadap serangan siber serta memastikan perlindungan optimal terhadap data dan infrastruktur digital mereka.

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

tepat, aplikasi sangat rentan terhadap eksploitasi yang dapat berakibat fatal seperti kebocoran data sensitif atau bahkan kehilangan kontrol atas aplikasi tersebut. Oleh sebab itu, metode pengamanan aplikasi menjadi bagian integral dalam proses pengembangan perangkat lunak modern.

1. *Secure Coding Practices*

Salah satu metode utama dalam pengamanan aplikasi adalah ***Secure Coding Practices*** atau praktik pengkodean yang aman. *Secure coding* merupakan pendekatan yang memastikan setiap baris kode yang ditulis oleh *developer* bebas dari celah keamanan yang umum terjadi. Praktik ini menekankan pentingnya edukasi dan kesadaran *developer* mengenai kerentanan umum seperti *injection*, *buffer overflow*, XSS, dan berbagai ancaman keamanan lainnya. Dengan menerapkan standar pengkodean yang aman seperti OWASP *Secure Coding Guidelines* atau CERT *Secure Coding* Standards, developer mampu menghasilkan aplikasi yang tahan terhadap berbagai serangan siber.

Dalam *Secure Coding Practices*, terdapat beberapa prinsip dasar seperti memvalidasi semua input pengguna, menerapkan prinsip *least privilege* (memberikan hak akses minimal yang dibutuhkan), serta menghindari penggunaan fungsi yang sudah diketahui rentan. Penggunaan otomatisasi seperti *static code analyzer*, *vulnerability scanner*, dan *peer review* secara rutin juga menjadi praktik terbaik yang dapat membantu mengidentifikasi potensi masalah sejak dini, sehingga aplikasi bisa lebih aman saat diluncurkan.

2. Manajemen *Session* dan Autentikasi

Selain *secure coding*, **Manajemen *Session* dan Autentikasi** juga merupakan bagian penting dari metode pengamanan aplikasi. Manajemen sesi yang baik memastikan bahwa sesi pengguna dilindungi dengan ketat dari ancaman seperti session *hijacking* atau session *fixation*. Sesi pengguna harus diatur sedemikian rupa agar bersifat unik, memiliki waktu kedaluwarsa yang singkat, dan dienkripsi saat disimpan maupun dikirimkan melalui jaringan. Implementasi token sesi yang aman serta penerapan cookie dengan atribut *secure* dan *HttpOnly* dapat mencegah pencurian sesi oleh penyerang.

Dalam sistem autentikasi, penerapan metode **multi-faktor (*Multi-Factor Authentication*/MFA)** sangat direkomendasikan untuk meningkatkan keamanan akses pengguna terhadap aplikasi. Pendekatan ini menggabungkan beberapa lapisan verifikasi, seperti informasi yang hanya diketahui oleh pengguna (contohnya kata sandi), perangkat yang dimiliki pengguna (seperti token fisik atau aplikasi autentikasi), serta ciri khas yang bersifat biologis, seperti sidik jari atau fitur biometrik lainnya. Penggunaan MFA terbukti efektif dalam menekan risiko pencurian akun melalui teknik seperti *brute force*, *phishing*, maupun eksploitasi lain yang menyasar proses login.

3. Implementasi *Input* Validasi dan *Output Encoding*

Salah satu pendekatan krusial dalam memperkuat keamanan aplikasi adalah dengan memastikan bahwa setiap data yang diterima telah divalidasi dengan benar dan dienkode sebelum diproses lebih lanjut. Proses validasi input dan *encoding output* berfungsi untuk memastikan bahwa data sesuai dengan format yang diizinkan serta tidak membawa risiko ke sistem. Tanpa mekanisme ini, aplikasi menjadi rentan terhadap serangan seperti penyisipan perintah SQL, manipulasi perintah sistem, atau penyalahgunaan skrip di sisi klien (*Cross-Site Scripting/XSS*). Untuk mencegahnya, pengembang disarankan menggunakan strategi penyaringan berbasis *whitelist* yang hanya memperbolehkan data yang telah ditentukan sebelumnya.

Di sisi lain, *output encoding* adalah proses mengubah *output* aplikasi agar aman ketika ditampilkan di browser pengguna. Metode ini terutama efektif dalam mencegah serangan XSS, yang terjadi ketika penyerang menyisipkan skrip jahat melalui data pengguna yang kemudian dieksekusi oleh *browser* korban. Dengan menerapkan *encoding output* yang tepat, seperti HTML *entity encoding* atau JavaScript *encoding*, risiko eksploitasi XSS dapat diminimalisasi secara signifikan.

4. Pengamanana API dan Layanan Web

Terakhir, namun tidak kalah penting, adalah metode pengamanan aplikasi melalui **Pengamanan API dan Layanan Web**. Di era digital saat ini, sebagian besar aplikasi terhubung melalui layanan web atau *Application Programming Interface* (API). API yang tidak diamankan dengan baik dapat menjadi celah yang mudah dimanfaatkan oleh

penyerang untuk mengakses data atau melakukan serangan. Oleh karena itu, pengamanan API harus mencakup autentikasi API yang kuat, manajemen hak akses yang ketat, dan proteksi terhadap serangan spesifik seperti rate limiting dan *throttling* untuk mencegah serangan *denial of service* (DoS).

Selain itu, penerapan standar keamanan API seperti *OAuth* untuk autentikasi dan OpenAPI (sebelumnya dikenal dengan *Swagger*) untuk dokumentasi yang jelas dan aman, menjadi praktik umum yang dianjurkan. Setiap permintaan (*request*) dan tanggapan (*response*) API harus diverifikasi dan divalidasi, sehingga tidak ada celah manipulasi parameter yang dapat mengekspos data sensitif atau fungsi aplikasi yang tidak diinginkan. Penggunaan HTTPS untuk enkripsi lalu lintas data antara klien dan server API juga menjadi langkah wajib dalam mengamankan komunikasi API.

Dengan menerapkan berbagai metode pengamanan secara konsisten dan terintegrasi, tingkat keamanan aplikasi dapat meningkat secara signifikan. Untuk mencapainya, kolaborasi erat antara *developer* dan tim keamanan sangat dibutuhkan, khususnya dalam penerapan praktik pengkodean yang aman (*Secure Coding Practices*), manajemen sesi dan autentikasi yang andal, validasi input yang ketat, serta encoding output yang tepat. Selain itu, perlindungan menyeluruh terhadap API dan layanan web juga harus menjadi prioritas utama.

Sinergi ini menjadi kunci dalam menciptakan ekosistem aplikasi yang **aman**, **terlindungi**, dan **dapat dipercaya** oleh seluruh pihak yang mengakses maupun mengelolanya.

D. PENGANTAR PENGUJIAN PENETRASI (*PENETRATION TESTING*)

1. Definisi dan Tujuan Penetrasi *Testing*

Dalam era digital yang penuh tantangan ini, sistem informasi dituntut untuk memiliki tingkat keamanan yang sangat tinggi. Salah satu pendekatan untuk memastikan keamanan sistem informasi adalah dengan melakukan pengujian penetrasi atau lebih dikenal dengan istilah

penetration *testing*. Secara sederhana, *penetration testing* adalah simulasi serangan siber yang dilakukan oleh tenaga ahli keamanan untuk mengevaluasi tingkat keamanan suatu sistem atau aplikasi. Metode ini bertujuan untuk menemukan celah keamanan sebelum celah tersebut dimanfaatkan oleh penyerang yang sebenarnya.

Tujuan utama dari penetration testing adalah mengidentifikasi kerentanan yang terdapat dalam sebuah sistem, jaringan, atau aplikasi. Melalui metode ini, tim keamanan dapat memahami sejauh mana sistem tersebut mampu bertahan dari berbagai jenis serangan siber. *Penetration testing* juga membantu organisasi dalam mengukur efektivitas dari kebijakan keamanan yang diterapkan, serta memberikan gambaran jelas mengenai dampak yang bisa terjadi jika sistem tersebut berhasil diretas oleh pihak yang tidak berwenang.

Selain itu, *penetration testing* juga bertujuan untuk meningkatkan kesadaran keamanan di lingkungan organisasi. Hasil dari pengujian ini biasanya digunakan untuk memberikan rekomendasi atau langkah-langkah korektif dalam mengatasi kerentanan yang ditemukan. Dengan begitu, *penetration testing* bukan sekadar alat pengujian, tetapi juga menjadi bagian dari proses penguatan sistem keamanan secara menyeluruh dan berkelanjutan.

2. Jenis Pengujian Pentetrasi (*black-box, white-box, gray-box*)

Dalam praktiknya, pengujian penetrasi dapat dilakukan melalui berbagai strategi pendekatan. Salah satu pendekatan yang banyak diterapkan adalah **pengujian tipe *black-box***, yaitu ketika penguji melakukan penilaian terhadap sistem tanpa diberikan informasi sebelumnya mengenai struktur internal. Dalam skenario ini, penguji bertindak layaknya peretas eksternal yang tidak memiliki hak akses apa pun. Tujuan dari metode ini adalah untuk mensimulasikan serangan dari luar secara realistis dan menilai ketahanan sistem dalam menghadapi ancaman tanpa dukungan pengetahuan internal.

Pendekatan kedua dalam pengujian penetrasi dikenal sebagai ***white-box testing***, yang merupakan kebalikan dari metode *black-box*. Dalam skenario ini, penguji diberikan **akses penuh terhadap informasi internal sistem**, termasuk arsitektur, kode sumber aplikasi, dokumentasi teknis, serta kredensial pengguna. Dengan informasi yang komprehensif

tersebut, penguji dapat melakukan analisis mendalam untuk mengidentifikasi celah keamanan yang mungkin sulit ditemukan melalui pendekatan tanpa informasi. *White-box testing* sangat efektif dalam mengungkap kerentanan yang disebabkan oleh kesalahan pemrograman atau konfigurasi sistem *internal*.

Selain pendekatan *black-box* dan *white-box*, terdapat juga metode pengujian yang dikenal sebagai ***gray-box testing***. Teknik ini berada di antara kedua pendekatan tersebut, di mana penguji diberikan akses terbatas terhadap informasi sistem, seperti struktur dasar arsitektur atau akun pengguna dengan hak akses yang terbatas. Pendekatan ini merepresentasikan skenario serangan dari pihak yang memiliki sebagian informasi, baik melalui kebocoran data internal maupun melalui rekayasa sosial. *Gray-box* testing sangat efektif untuk menguji sistem dalam kondisi yang lebih realistis, karena banyak serangan siber modern dilakukan dengan tingkat pengetahuan parsial terhadap target.

3. Tahapan Umum Dalam Penetrasi Testing

Dalam praktik pengujian penetrasi, terdapat beberapa tahapan utama yang umumnya harus dilalui. Tahap pertama adalah **perencanaan dan persiapan**. Pada fase ini, penguji bekerja sama dengan tim internal organisasi untuk menetapkan ruang lingkup pengujian, memilih pendekatan yang akan digunakan (seperti *black-box*, *white-box*, atau *gray-box*), serta menyusun kesepakatan yang jelas terkait batasan dan aturan teknis, termasuk hal-hal yang diizinkan dan yang harus dihindari selama proses pengujian berlangsung.

Tahap berikutnya adalah **pengumpulan informasi (information gathering)**. Di tahap ini, penguji akan mengumpulkan berbagai informasi mengenai target pengujian. Aktivitas ini meliputi pemetaan jaringan, scanning port, identifikasi layanan aktif, hingga pencarian data publik yang tersedia secara daring. Informasi tersebut sangat penting untuk mengidentifikasi titik-titik potensial yang rentan terhadap serangan.

Setelah informasi terkumpul, tahap selanjutnya adalah **eksploitasi kerentanan**. Pada tahap ini, penguji akan mencoba memanfaatkan celah keamanan yang telah teridentifikasi. Aktivitas eksploitasi dilakukan dengan teknik-teknik tertentu, seperti mencoba mengeksekusi perintah ilegal, mengakses data secara tidak sah, atau mencoba mengambil alih

kontrol penuh terhadap sistem yang diuji. Tujuan utama dari tahap ini adalah membuktikan apakah kerentanan yang ditemukan benar-benar bisa dimanfaatkan untuk meretas sistem.

Tahapan berikutnya disebut sebagai tahap **analisis dan dokumentasi**. Setelah tahap eksploitasi selesai, semua hasil pengujian akan didokumentasikan secara detail. Dokumentasi ini mencakup deskripsi kerentanan, dampak yang mungkin timbul, bukti eksploitasi, serta rekomendasi untuk memperbaiki celah keamanan tersebut. Laporan yang dihasilkan pada tahap ini merupakan aset penting bagi organisasi dalam upaya perbaikan keamanan.

Tahapan terakhir adalah **pelaporan dan tindak lanjut**. Dalam tahap ini, laporan penetration testing diserahkan kepada tim manajemen atau pihak yang bertanggung jawab terhadap keamanan sistem. Organisasi kemudian akan menggunakan laporan ini sebagai dasar untuk mengambil langkah-langkah mitigasi, melakukan perbaikan konfigurasi, dan memperbarui kebijakan keamanan agar celah keamanan yang ditemukan tidak lagi dapat dieksploitasi di masa depan.

Melalui penerapan penetration *testing* yang terstruktur dan sistematis, organisasi dapat secara efektif mengidentifikasi, mengevaluasi, serta memperkuat sistem keamanan informasi yang dimilikinya. Pendekatan ini tidak hanya bermanfaat untuk melindungi data penting dari ancaman eksternal, tetapi juga berkontribusi dalam membangun budaya keamanan yang kuat di lingkungan organisasi. Oleh karena itu, pengujian penetrasi menjadi salah satu langkah strategis dalam menciptakan ekosistem digital yang **aman**, **terlindungi**, dan **dapat dipercaya** oleh seluruh pemangku kepentingan.

E. TEKNIK DAN ALAT PENGUJIAN PENETRASI

1. Teknik *reconnaissance* dan *scanning*

Pengujian penetrasi merupakan proses yang kompleks dan sistematis. Untuk memastikan efektivitas pengujian, diperlukan berbagai teknik dan alat bantu yang dirancang khusus untuk mengeksplorasi celah-celah keamanan dalam sistem. Dalam pelaksanaannya, *penetration tester* atau *ethical hacker* menggunakan tahapan dan teknik tertentu yang dimulai dari

pengumpulan informasi hingga eksploitasi, dan berakhir pada pelaporan temuan.

Tahapan awal dalam pengujian penetrasi dikenal dengan **teknik *reconnaissance* dan *scanning***. *Reconnaissance* adalah proses pengumpulan informasi sebanyak mungkin mengenai target, baik secara pasif maupun aktif. Dalam tahap pasif, informasi dikumpulkan tanpa berinteraksi langsung dengan sistem target, misalnya dengan mencari data publik di mesin pencari, WHOIS, DNS *lookup*, dan media sosial. Sedangkan pada tahap aktif, penguji mulai melakukan interaksi langsung dengan sistem seperti melakukan *port* scanning atau *service enumeration.*

Scanning merupakan kelanjutan dari *reconnaissance* aktif. Dalam tahap ini, penetration *tester* melakukan pemindaian terhadap port terbuka, layanan yang berjalan, sistem operasi, dan versi perangkat lunak yang digunakan. Tools seperti **Nmap**, **Netcat**, atau **Masscan** sering digunakan dalam fase ini untuk memperoleh pemahaman menyeluruh tentang permukaan serangan (*attack surface*). Informasi ini penting untuk mengidentifikasi titik-titik lemah yang dapat dieksploitasi pada tahap berikutnya.

2. Exploitation dan privilege escalation

Setelah data awal diperoleh, tahap selanjutnya adalah ***exploitation***, yaitu tahap di mana penguji mencoba memanfaatkan kerentanan yang telah ditemukan untuk mendapatkan akses ke sistem target. Eksploitasi dilakukan dengan menggunakan *payload* khusus untuk menjalankan perintah ilegal, membuka shell jarak jauh (*remote shell*), atau memperoleh akses terhadap data sensitif. Eksploitasi juga bisa mencakup injeksi kode, pengambilalihan sesi, serta manipulasi parameter aplikasi.

Dalam banyak kasus, setelah berhasil mengeksploitasi sebuah sistem, akses awal yang didapat hanya bersifat terbatas. Oleh karena itu, penguji akan melanjutkan ke tahap ***privilege escalation***, yaitu teknik untuk meningkatkan hak akses dari pengguna biasa menjadi *administrator* atau *root.* Teknik ini memungkinkan penguji untuk mengontrol penuh sistem target, mengakses file kritikal, menginstal malware, atau melakukan pivoting ke sistem lain dalam jaringan. Privilege escalation dapat dilakukan melalui eksploitasi konfigurasi sistem yang salah, service yang berjalan dengan hak akses tinggi, atau kelemahan dalam sistem operasi.

3. Alat populer: OWASP ZAP, *Burp Suite*, *Metasploit*

Dalam menunjang aktivitas uji keamanan aplikasi, terdapat berbagai tools yang kerap digunakan oleh praktisi keamanan siber. Salah satu alat sumber terbuka yang cukup populer di kalangan penetration tester adalah **OWASP ZAP (Zed Attack Proxy)**. Tool ini dirancang untuk melakukan evaluasi terhadap celah keamanan pada aplikasi berbasis web. Dengan fitur seperti pemindaian otomatis dan fungsi proxy yang bersifat interaktif, ZAP memungkinkan pengguna untuk memantau, menganalisis, dan memodifikasi lalu lintas HTTP secara langsung selama proses pengujian berlangsung.

Selain ZAP, ada juga ***Burp Suite***, sebuah *toolkit* yang sangat populer dalam pengujian penetrasi aplikasi web. *Burp Suite* menyediakan fitur yang sangat lengkap, mulai dari spidering (pemindaian struktur web), *vulnerability scanning*, hingga *repeater* dan *intruder* yang memungkinkan pengujian secara manual terhadap *input-input* berbahaya. *Burp Suite* banyak digunakan untuk menemukan celah seperti XSS, SQL *Injection*, dan kelemahan autentikasi.

Untuk pengujian eksploitasi yang lebih mendalam, terutama terhadap sistem dan jaringan, ***Metasploit Framework*** menjadi pilihan utama. *Metasploit* adalah platform *open-source* yang menyediakan berbagai modul eksploitasi yang dapat digunakan untuk menyerang dan menguji sistem target secara otomatis. *Metasploit* juga mendukung pengujian *privilege escalation* dan *post-exploitation*, serta memungkinkan penelusuran lanjutan ke jaringan internal.

4. Dokumentasi dan pelaporan hasil pengujian

Setelah semua tahap pengujian dilakukan, proses yang tak kalah penting adalah **dokumentasi dan pelaporan hasil pengujian**. Penguji harus mencatat setiap langkah yang dilakukan, termasuk metode yang digunakan, kerentanan yang ditemukan, bukti eksploitasi, serta dampak potensial dari celah tersebut. Dokumentasi yang baik tidak hanya berguna untuk proses internal, tetapi juga menjadi bukti kepada pihak manajemen bahwa pengujian dilakukan secara profesional dan bertanggung jawab.

Pelaporan hasil pengujian biasanya mencakup ringkasan eksekutif untuk pembaca non-teknis, serta bagian teknis yang memuat deskripsi

rinci dari setiap temuan. Setiap kerentanan biasanya disertai dengan tingkat risiko (tinggi, sedang, rendah), bukti eksploitasi (*screenshot*, *log*, *payload*), dan rekomendasi mitigasi. Laporan ini menjadi dasar bagi tim keamanan atau pengembang untuk segera menutup celah yang ada dan meningkatkan postur keamanan sistem.

Kesimpulannya, pengujian penetrasi yang efektif tidak hanya bergantung pada keahlian teknis penguji, tetapi juga pada penggunaan teknik yang tepat dan alat bantu yang andal. Mulai dari tahap *reconnaissance* hingga pelaporan, setiap langkah harus dilakukan secara sistematis dan terstruktur. Dengan demikian, organisasi dapat mengidentifikasi dan mengatasi kerentanan yang ada sebelum dimanfaatkan oleh penyerang sesungguhnya, sekaligus meningkatkan kesadaran akan pentingnya keamanan informasi.

F. STUDI KASUS: PENGUJIAN PENETRASI APLIKASI WEB

Untuk memberikan pemahaman yang lebih konkret mengenai praktik pengujian penetrasi, berikut disajikan studi kasus yang menggambarkan proses lengkap pengujian terhadap sebuah aplikasi web nyata. Aplikasi yang diuji adalah sistem manajemen pelanggan berbasis web yang digunakan oleh sebuah perusahaan retail nasional. Tujuan utama dari pengujian ini adalah mengidentifikasi potensi kerentanan yang dapat membahayakan data pelanggan serta mengevaluasi ketahanan sistem terhadap berbagai serangan umum.

1. Proses pengujian penetrasi pada aplikasi web nyata

Tahap awal dimulai dengan proses **perencanaan dan kesepakatan ruang lingkup pengujian**. Tim pengujian bersama dengan pemilik sistem menyepakati bahwa metode yang digunakan adalah *gray-box testing*, di mana penguji memiliki akses terbatas seperti pengguna biasa. Lingkup pengujian dibatasi hanya pada modul *login*, *dashboard* pengguna, dan fitur pencarian pelanggan. Akses ke *database* dan infrastruktur jaringan dikecualikan demi alasan kepatuhan.

2. Identifikasi kerentanan, eksploitasi, dan rekomendasi perbaikan

Selanjutnya, penguji melakukan **reconnaissance dan scanning**. Dengan menggunakan alat seperti OWASP ZAP dan Nmap, penguji

berhasil mengidentifikasi bahwa aplikasi berjalan di atas *framework* PHP lama yang belum diperbarui, serta memiliki beberapa endpoint API yang tidak dilindungi autentikasi. Informasi ini menjadi titik awal untuk eksplorasi lebih lanjut terhadap potensi celah keamanan.

Dalam proses **pengujian input dan eksploitasi**, ditemukan bahwa formulir login aplikasi tidak menerapkan mekanisme *rate-limiting*, sehingga rentan terhadap serangan *brute force*. Selain itu, pada fitur pencarian pelanggan, ditemukan celah **SQL Injection** yang memungkinkan penguji memanipulasi *query* untuk mengakses informasi seluruh pelanggan yang tersimpan di database, meskipun pengguna hanya memiliki hak akses terbatas.

3. Analisis dampak risiko dari hasil pengujian penetras

Penguji juga berhasil melakukan ***Cross-Site Scripting*** **(XSS)** pada halaman pengumuman internal, di mana pengguna dapat menginput HTML yang akan ditampilkan ke seluruh pengguna lain. Dengan memanfaatkan skrip XSS, penguji mencuri *cookie* sesi *administrator* dan berhasil *login* sebagai admin tanpa kredensial. Hal ini menandakan bahwa sesi tidak diamankan dengan baik, dan aplikasi tidak menerapkan HttpOnly pada *cookie*.

Berdasarkan temuan tersebut, penguji menyusun laporan yang memuat **rekomendasi perbaikan**. Beberapa saran yang diberikan antara lain: menerapkan *parameterized* query untuk mencegah SQL *Injection*, menambahkan *rate-limiting* dan CAPTCHA pada formulir login, serta melakukan *output encoding* pada semua data yang ditampilkan kembali ke *browser*. Selain itu, direkomendasikan juga untuk mengaktifkan pengaturan *cookie secure* dan HttpOnly, serta memperbarui *framework* ke versi yang lebih aman.

Setelah eksploitasi dilakukan, tim penguji juga menyusun **analisis dampak risiko**. Dalam skenario terburuk, penyerang dapat mencuri seluruh data pelanggan termasuk informasi pribadi seperti nama, alamat, dan riwayat pembelian. Hal ini dapat mengakibatkan pelanggaran terhadap regulasi perlindungan data seperti UU PDP atau GDPR, serta merusak reputasi perusahaan di mata publik. Potensi kerugian finansial juga sangat besar, terutama jika data yang bocor dijual atau digunakan untuk tindakan kriminal.

Dampak teknis lainnya adalah kemungkinan serangan lateral (lateral *movement*), di mana penyerang dapat menggunakan akses yang diperoleh untuk menyusup lebih dalam ke sistem *internal* perusahaan, termasuk sistem pembayaran atau manajemen inventaris. Jika eksploitasi ini tidak segera ditangani, organisasi dapat menghadapi serangan yang lebih kompleks dan berbahaya di masa mendatang.

Setelah laporan diserahkan, tim pengembang melakukan patching terhadap semua kerentanan yang ditemukan. Aplikasi kemudian diuji ulang (*retest*) untuk memastikan bahwa perbaikan telah berhasil diterapkan. Dari hasil *retesting*, semua kerentanan telah ditutup dengan baik dan tidak ditemukan celah tambahan. Proses ini menunjukkan bagaimana pengujian penetrasi dapat menjadi alat evaluasi sekaligus langkah preventif yang sangat efektif dalam siklus keamanan aplikasi.

Studi kasus ini menegaskan bahwa pengujian penetrasi bukan hanya sekadar kegiatan teknis, tetapi merupakan komponen penting dalam manajemen risiko organisasi. Dengan pendekatan yang sistematis dan profesional, perusahaan dapat mengantisipasi ancaman keamanan lebih dini dan melindungi aset digitalnya dari ancaman nyata di dunia siber yang terus berkembang.

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

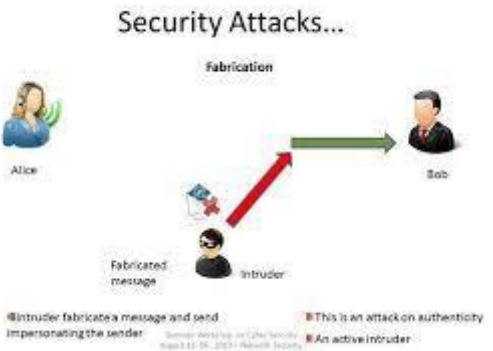
C. MODEL SERANGAN KEAMANAN

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.

F. KEAMANAN DATA DAN PRIVASI DATA

Pengembangan ekonomi digital sebuah negara sangat dipengaruhi oleh perlindungan privasi dan data pribadi, tanpa terkecuali Indonesia. Adanya kepercayaan dipengaruhi oleh perlindungan daring, atau kepercayaan online, yang merupakan komponen penting dalam transaksi digital.

Karena pengguna jaringan tidak akan melakukan transaksi digital jika mereka merasa privasi dan data pribadinya terancam, privasi dan data pribadi sangat penting. Salah satu cara data pribadi dan privasi dilindungi adalah bagaimana data diproses, termasuk data pengguna sensitif.

Menyebarkannya ke pihak yang tidak bertanggung jawab dapat menyebabkan kerugian finansial atau bahkan mengancam keselamatan dan keamanan pemilik. Pertumbuhan ekonomi dihasilkan dari pelanggaran privasi dan data pribadi.

Di tanah air, banyak berita tentang penipuan yang dilakukan melalui situs e-commerce, atau perdagangan elektronik.

Dengan demikian, kepercayaan masyarakat terhadap situs transaksi perdagangan online menurun. Masyarakat yang menyadari ini tidak ingin menggunakan kartu kredit yang melibatkan data pribadi dan privasi. Seiring dengan banyaknya situs e-commerce di Indonesia, perlindungan data pribadi dan privasi sangat diperlukan. Dengan memanfaatkan media sosial seperti Facebook dan Instagram, penipuan kini tumbuh subur.

Dengan hilangnya kepercayaan masyarakat terhadap situs web perdagangan online dan perdagangan online yang memanfaatkan media dalam jaringan lainnya, pertumbuhan ekonomi digital Indonesia akan stagnan dan bahkan cenderung menurun seiring dengan hilangnya kepercayaan pengguna.

Tidak sedikit orang Indonesia yang mengeluhkan iklan melalui telepon, yang termasuk dalam kategori pemasaran langsung, karena menawarkan produk keuangan seperti asuransi dan pinjaman secara langsung tanpa manfaat. Salah satu masalah dengan praktik semacam ini adalah penyebaran data pribadi konsumen atau masyarakat yang tidak sesuai dengan prinsip etika. Bisnis yang menggunakan direct marketing melalui telepon menyebarkan data pelanggan secara luas. Otoritas Jasa Keuangan dapat digunakan sebagai lembaga pengaduan apabila masalah semacam ini muncul. Namun demikian, telemarketing yang tidak mendapatkan persetujuan masyarakat terlebih dahulu masih banyak dilakukan di Indonesia.

Selain kasus direct marketing, permintaan data kartu keluarga untuk pendaftaran kartu prabayar juga menjadi kontroversi. Masalah besar muncul karena privasi dan perlindungan data pribadi pelanggan. Dalam situasi ini, operator telepon seluler bertanggung jawab atas pengumpulan, pengolahan, dan pemrosesan data pribadi yang banyak diberikan oleh masyarakat karena kebijakan pemerintah. Kedua hal di atas menunjukkan bahwa kesadaran hukum masyarakat dan ketidakefektifan sistem hukum.

Karena tidak ada keamanan masyarakat di tengah era ekonomi digital, hukum diperlukan untuk menjaga perkembangan ekonomi digital agar berjalan dengan lancar. Sebaliknya, perlindungan Tidak cukup untuk mendorong pertumbuhan ekonomi digital Indonesia karena instrumen hukum yang khusus untuk perlindungan privasi dan data pribadi belum ada dan masih bersifat sektoral. Untuk mencapai hal ini, peraturan Indonesia mengenai privasi dan data pribadi harus dievaluasi terlebih dahulu. Peraturan ini dapat membantu pertumbuhan ekonomi digital. Hal ini dapat dicapai melalui penggunaan teknik penelusuran hukum. Dalam hal moralitas, Anda juga harus tahu bagaimana seharusnya. Pergeseran dari era ekonomi tradisional ke era ekonomi digital dapat berdampak pada perlindungan privasi dan data pribadi di Indonesia.

Sangat penting untuk menyelidiki topik ini karena Indonesia sedang mengalami peralihan dari era ekonomi tradisional ke era ekonomi digital. Era ekonomi tradisional terjadi sebelum kemajuan teknologi informasi. berat. Perdagangan dana dan transaksi lainnya antara masyarakat dilakukan secara langsung selama era ekonomi konvensional. Transaksi jenis ini membutuhkan kedua pihak untuk hadir secara fisik di waktu dan tempat yang sama. Dalam era ekonomi digital, transaksi seperti yang disebutkan sebelumnya dapat dilakukan dengan bantuan teknologi informasi dan komunikasi. Akibatnya, muncul era baru yang dikenal sebagai ekonomi digital atau "ekonomi digital". Berikut ini adalah gambaran yang tepat dari era ekonomi digital yang diberikan oleh Atkinson dan McKay2:

"The digital economy represents the pervasive use of IT (hardware, software, applications and telecommunications) in all aspects of the economy, including internal operations of organizations (business, government and non-profit)…"

Saat ini Cara orang berbisnis dan bertransaksi telah diubah oleh perkembangan pesat teknologi informasi dan komunikasi. Akibatnya, transaksi yang disebut sebagai "transaksi elektronik", "komersial elektronik", dan "bisnis elektronik". Ekonomi digital sekarang melanda Indonesia. Klaim ini didukung oleh keadaan masyarakat Indonesia yang menganggap internet dan telepon seluler sebagai barang, dan keduanya digunakan oleh pedagang dan penjual untuk menunjukkan transaksi elektronik melalui jaringan internet. Hal ini berarti bahwa undang-undang yang mengatur bisnis harus mengikuti atau bahkan mengantisipasi perkembangan ke Era Ekonomi Digital.

G. PERLINDUNGAN PRIVASI DAN DATA PRIBADI

Jika data memiliki hubungan dengan seseorang, itu dianggap data pribadi dan dapat digunakan untuk mengidentifikasi pemiliknya. Sebagai contoh, tempatkan nomor telepon di dalam secarik kertas kosong. adalah kumpulan data. Berbeda halnya jika secarik kertas berisi nomor telepon dan nama pemiliknya; nomor telepon di secarik kertas kosong bukan data pribadi karena tidak

dapat digunakan untuk mengidentifikasi pemiliknya, tetapi nomor telepon dan nama pemiliknya adalah data yang dapat digunakan. untuk mengidentifikasi pemilik data tersebut, oleh karena itu dapat disebut sebagai data pribadi.

Seseorang yang dapat diidentifikasi adalah seseorang yang dapat dikenali atau diidentifikasi secara langsung atau tidak langsung berdasarkan nomor tanda pengenal atau salah satu atau lebih faktor khusus yang berkaitan dengan identifikasi seseorang secara fisik, mental, psikologis, budaya, atau sosial. Dalam mekanisme perlindungan data pribadi, entitas yang dilindungi adalah "orang perorangan", bukan "badan hukum", karena hak untuk menghormati kehidupan pribadi, yang juga dikenal sebagai hak perlindungan kehidupan pribadi, berasal dari hak untuk menghormati kehidupan pribadi manusia.

Karena konsep kehidupan pribadi terkait dengan manusia sebagai makhluk hidup, orang perorangan adalah pemilik utama hak perlindungan data pribadi. Ada sejumlah kategori subyek hukum yang harus diatur untuk melindungi data pribadi. "Pengelola Data Pribadi", yang dapat berupa individu, badan hukum swasta atau publik, dan organisasi, adalah subjek hukum yang pertama.

Komunitas lain yang mengelola data pribadi secara individual atau kolektif. Pengelola Data Pribadi melakukan "pengelolaan data pribadi", yang mencakup semua tindakan atau kumpulan tindakan yang dilakukan terhadap data pribadi, baik dengan menggunakan alat olah data secara otomatis maupun manual, secara terorganisir dan menggunakan sistem penyimpanan data. Kegiatan ini termasuk, tetapi tidak terbatas pada, pemrosesan, penggunaan, pengungkapan, penyebaran, dan pengamanan data pribadi.

"Pemroses Data Pribadi" adalah subjek hukum tambahan. Pemroses Data Pribadi adalah entitas publik atau swasta serta organisasi masyarakat lainnya yang melakukan tugas pemrosesan data pribadi atas nama pengelola data. Kegiatan pemrosesan data pribadi termasuk pengumpulan, data pribadi disimpan, dicatat, atau disimpan; atau melakukan penyusunan, penyesuaian, perubahan data pribadi; pemulihan kembali data yang telah dihapus; pengungkapan data pribadi; penggabungan, pembetulan, penghapusan, atau penghancuran data pribadi.

Pada Era Ekonomi digital dimana Infrastruktur dan aktivitas telekomunikasi memainkan peran penting dalam menjalankan transaksi elektronik dan pertukaran informasi di era ekonomi digital. Untuk tujuan ini, Indonesia memiliki Undang-Undang Nomor 36/1999, Telekomunikasi Undang-undang tersebut juga mengatur data pribadi.

Larangan penyadapan diatur dalam Pasal 40 Undang Undang Nomor 36 Tahun 1999 tentang Telekomunikasi. Setiap orang dilarang menyadap informasi yang dikirim melalui jaringan telekomunikasi. Larangan ini membantu menjaga privasi dan data pribadi. Selain itu, Pasal 42 ayat (1) menyatakan bahwa penyelenggara jasa telekomunikasi bertanggung jawab untuk menjaga kerahasiaan informasi yang dikomunikasikan.

H. PRINSIP HAK PRIVASI TERHADAP DATA PRIBADI

Dalam era digital yang semakin maju ini, konsep hak privasi terhadap data pribadi sangat penting. Kita menggunakan teknologi dan memberikan data pribadi secara online setiap hari. Data pribadi berarti apa pun yang dapat secara langsung atau tidak langsung mengidentifikasi seseorang Data seperti nama, alamat, nomor telepon, alamat email, tanggal lahir, nomor identifikasi, data keuangan, dan informasi medis adalah salah satu contohnya. Namun, dengan memberikan informasi ini, kita juga meningkatkan kemungkinan penyalahgunaan data dan pelanggaran privasi.Hak privasi terhadap data pribadi mencakup hak setiap orang untuk mengetahui apa yang terjadi dengan data pribadi mereka, siapa yang dapat mengaksesnya, tujuan penggunaan data, dan bagaimana datadigunakan.

Hak privasi terhadap data pribadi mencakup hak setiap orang untuk mengetahui apa yang terjadi dengan data pribadi mereka, siapa yang dapat mengaksesnya, tujuan penggunaan data, dan bagaimana data digunakan. tertentu diproses dan disimpan. Lebih dari itu, prinsip ini juga melibatkan hak untuk memberikan izin atau persetujuan atas penggunaan data pribadi tersebut. Selain itu, mereka juga memiliki hak untuk meminta penghapusan data (hak untuk lupa) atau koreksi jika data tersebut salah.

Tujuan dari hak privasi terhadap data pribadi adalah untuk melindungi hak asasi manusia dan martabat individu serta memastikan bahwa data digunakan dengan cara yang etis dan jujur. Hal ini tidak hanya berkaitan dengan bukan hanya perusahaan yang mengumpulkan data, tetapi juga pemerintah dan lembaga lain yang mengumpulkan, memproses, dan menggunakan data pribadi. Beberapa kasus hak privasi yang dilanggar atau dianggap melanggar di Indonesia termasuk bocornya data pribadi pada layanan BPJS kesehatan pada tahun 2021 dan pelanggaran data di toko online Tokopedia pada tahun 2020. Data pribadi yang dikumpulkan oleh puluhan juta pengguna, yang mencakup informasi seperti nama, alamat email, nomor telepon, dan lainnya, masih belum jelas kebenarannya. Salah satu contoh data pribadi yang dikumpulkan oleh pengguna aplikasi transportasi online seperti Gojek dan Grab masih belum jelas kebenarannya.

Warren dan Brandheis menciptakan hak atas privasi—terkadang disebut hak untuk tidak diganggu—dalam sebuah manuskrip di Harvard University Law School berjudul "Hak atas Privasi."

Menurut Warren dan Brandheis dalam jurnal tersebut, peningkatan dan kemajuan teknologi telah meningkatkan kesadaran masyarakat tentang hak setiap orang untuk menikmati hidup.

Warren dan Brandeis mengatakan, "Privasi adalah hak untuk menikmati hidup dan hak untuk dibiarkan sendiri, dan perkembangan hukum ini tidak dapat dihindari dan menuntut pengakuan hukum." Setiap individu berhak untuk menikmati privasinya, yang harus dilindungi.

I. RANGKUMAN

Keamanan data merupakan komponen vital dalam pengelolaan informasi di era digital saat ini. Dalam konteks yang semakin bergantung pada teknologi informasi dan komunikasi, data telah menjadi aset berharga bagi individu, organisasi, maupun negara. Oleh karena itu, menjaga keamanan data berarti melindungi informasi dari berbagai ancaman, baik itu dari serangan siber, akses tidak sah, pencurian, maupun kerusakan akibat kesalahan sistem atau bencana alam.

Tujuan utama dari keamanan data adalah untuk memastikan tiga aspek penting: kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data. Kerahasiaan menjamin bahwa hanya pihak yang berwenang yang dapat mengakses informasi, integritas menjaga agar data tetap akurat dan tidak berubah tanpa izin, sedangkan ketersediaan memastikan bahwa data dapat diakses kapan pun diperlukan.

Penerapan keamanan data mencakup berbagai langkah teknis dan non-teknis. Langkah teknis meliputi penggunaan sistem enkripsi, firewall, autentikasi ganda (multi-factor authentication), serta pembaruan sistem secara berkala. Sementara itu, langkah non-teknis mencakup edukasi kepada pengguna, penyusunan kebijakan keamanan informasi, dan pengawasan terhadap akses data secara ketat.

Tantangan dalam menjaga keamanan data semakin kompleks seiring meningkatnya jumlah perangkat yang terhubung ke internet, munculnya teknologi baru seperti Internet of Things (IoT) dan kecerdasan buatan (AI), serta semakin canggihnya metode serangan siber. Oleh sebab itu, strategi keamanan harus terus berkembang dan beradaptasi dengan perubahan teknologi serta pola serangan yang dinamis.

Kesadaran akan pentingnya keamanan data harus dimiliki oleh semua pihak, bukan hanya oleh tim IT atau penyedia layanan digital. Keterlibatan aktif dari seluruh elemen organisasi dan masyarakat dalam menjaga data akan menciptakan ekosistem digital yang lebih aman dan terpercaya. Dengan keamanan data yang kuat, kepercayaan publik terhadap teknologi dan layanan digital dapat ditingkatkan, sekaligus mendukung pertumbuhan digital yang berkelanjutan dan bertanggung jawab.

Berdasarkan uraian diatas Perlindungan privasi dan data pribadi merupakan aspek yang sangat krusial dalam kehidupan modern, terutama di era digital yang serba terhubung ini. Informasi pribadi seperti nama, alamat, nomor identitas, riwayat kesehatan, hingga data keuangan kini banyak tersimpan dan diproses secara digital oleh berbagai pihak, baik oleh pemerintah, perusahaan, maupun platform daring. Hal ini menimbulkan tantangan baru terkait keamanan dan integritas data, serta risiko penyalahgunaan oleh pihak yang tidak bertanggung jawab. Dengan demikian Perlu

kehati-hatian yang ekstra dalam hal data pribadi dalam hal dan bidang apapun.

Kemudian pentingnya perlindungan data pribadi tidak hanya berkaitan dengan keamanan teknis, tetapi juga menyangkut hak asasi manusia, yaitu hak atas privasi. Setiap individu berhak mengontrol siapa saja yang dapat mengakses dan menggunakan informasi pribadinya, serta untuk tujuan apa data tersebut digunakan. Tanpa adanya perlindungan yang memadai, data pribadi bisa dimanfaatkan untuk berbagai tujuan negatif, seperti penipuan, pencurian identitas, atau manipulasi perilaku konsumen.

Sudah banyak kasus kejadian yang menyangkut dengan penyalahgunaan data pribadi yang seharusnya dilindungi dan terlindungi.

Oleh karena itu, banyak negara termasuk Indonesia telah mengadopsi regulasi khusus, seperti Undang-Undang Perlindungan Data Pribadi (UU PDP), yang bertujuan untuk memberikan jaminan hukum atas pemrosesan data pribadi. Regulasi ini menuntut agar pengumpulan dan pemrosesan data dilakukan secara transparan, adil, dan hanya untuk tujuan yang sah. Selain itu, terdapat kewajiban bagi pengelola data untuk menjaga kerahasiaan, integritas, dan ketersediaan data pribadi dari akses tidak sah dan kebocoran informasi.

Namun, perlindungan data pribadi tidak bisa hanya bergantung pada regulasi semata. Kesadaran dan literasi digital masyarakat juga memegang peranan penting. Setiap individu perlu memahami risiko yang ada serta menerapkan langkah-langkah pencegahan, seperti menggunakan kata sandi yang kuat, tidak sembarangan membagikan informasi pribadi di internet, dan membaca kebijakan privasi sebelum menggunakan layanan digital.Ini hal yang terpenting karena masih banyak masyarakat yang masih ceroboh, dan memang jarang membaca kebijakan privasi yang biasanya sudah ada pada salah satu platform tertentu.

Dengan kombinasi antara perlindungan hukum yang kuat, tanggung jawab dari pengelola data, dan kesadaran individu, maka keamanan dan privasi data pribadi dapat lebih terjamin. Ini bukan hanya soal melindungi informasi, tetapi juga menjaga kepercayaan masyarakat dalam berinteraksi di dunia digital.

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.

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.

D. TANTANGAN SISTEM MANAJEMEN KEMANANAN INFORMASI

Penerapan Sistem Manajemen Keamanan Informasi di Indonesia menghadirkan tantangan tersendiri yang berasal dari kondisi ekonomi, konteks budaya, lanskap teknologi, dan struktur tata kelola negara. Tantangan-tantangan ini harus ditangani secara efektif untuk mewujudkan potensi SMKI dalam melindungi kerahasiaan data pribadi.

Keterbatasan sumber daya merupakan tantangan mendasar, terutama bagi organisasi di luar pusat kota besar. Perekonomian Indonesia dicirikan oleh kesenjangan yang signifikan antara wilayah dan sektor, yang mengakibatkan beragamnya kapasitas untuk investasi SMKI. Sementara lembaga keuangan besar dan perusahaan telekomunikasi di Jakarta dapat menerapkan sistem keamanan yang canggih, perusahaan menengah di kota-kota sekunder sering kali kesulitan dengan penerapan dasar. Penelitian oleh Asosiasi Keamanan Informasi Indonesia menunjukkan bahwa organisasi di luar Jawa menghabiskan rata-rata 62% lebih sedikit untuk keamanan informasi daripada rekan-rekan mereka di wilayah ibu kota. Kesenjangan ini menciptakan tingkat perlindungan yang tidak konsisten di seluruh ekosistem pemrosesan data.

Kekurangan tenaga profesional keamanan informasi yang berkualifikasi memperparah keterbatasan sumber daya. Indonesia menghadapi kesenjangan keterampilan yang signifikan, dengan Kementerian Komunikasi dan Teknologi Informasi memperkirakan kekurangan sekitar 600.000 spesialis keamanan siber. Kekurangan ini khususnya sangat parah bagi para profesional yang memiliki keahlian dalam kerangka SMKI internasional dan persyaratan peraturan Indonesia. Organisasi yang menerapkan SMKI sering kali mengalami kesulitan dalam merekrut dan mempertahankan staf dengan kualifikasi yang diperlukan, yang menyebabkan keterlambatan implementasi dan hasil yang kurang optimal. Terbatasnya jumlah konsultan dengan keahlian khusus dalam mengadaptasi kerangka global ke konteks Indonesia semakin memperburuk tantangan ini.

Heterogenitas teknologi di seluruh lanskap bisnis Indonesia menimbulkan tantangan integrasi yang signifikan bagi penerapan SMKI. Banyak organisasi mengoperasikan lingkungan hibrida yang menggabungkan sistem lama dengan teknologi yang lebih baru, sehingga menciptakan arsitektur keamanan yang kompleks. Sebuah studi oleh IDC Indonesia menemukan bahwa 68% perusahaan besar secara bersamaan mengelola sedikitnya tiga generasi infrastruktur teknologi, yang masing-masing memerlukan pendekatan keamanan yang berbeda. Heterogenitas ini meningkatkan kompleksitas penerapan kontrol keamanan yang konsisten dan mempersulit proses penilaian risiko.

Faktor budaya secara signifikan memengaruhi penerapan SMKI di Indonesia. Sifat hierarkis banyak organisasi Indonesia dapat memengaruhi struktur tata kelola keamanan dan pelaporan insiden. Staf

junior mungkin ragu untuk melaporkan masalah keamanan kepada atasan, sehingga menciptakan celah deteksi. Selain itu, penekanan budaya pada pemeliharaan keharmonisan (dikenal sebagai "rukun") dapat menghambat pelaporan pelanggaran kebijakan oleh rekan kerja. Penelitian yang dipublikasikan dalam Jurnal Ilmu Sosial Indonesia menunjukkan bahwa karyawan di organisasi Indonesia 34% lebih kecil kemungkinannya untuk melaporkan ketidakpatuhan oleh rekan kerja dibandingkan dengan rekan kerja di Barat. Kerangka kerja SMKI yang dikembangkan dalam konteks Barat sering kali gagal memperhitungkan dinamika budaya ini.

Kompleksitas regulasi menghadirkan tantangan signifikan lainnya. Meskipun telah diperkenalkannya Undang-Undang Perlindungan Data Pribadi, lanskap regulasi Indonesia untuk perlindungan data masih terfragmentasi di berbagai regulasi sektoral. Lembaga keuangan harus mematuhi regulasi OJK, penyedia layanan kesehatan dengan arahan Kementerian Kesehatan, dan perusahaan telekomunikasi dengan persyaratan KOMINFO, masing-masing dengan ekspektasi keamanan yang sedikit berbeda. Tambal sulam regulasi ini menciptakan tantangan kepatuhan bagi organisasi yang beroperasi di berbagai sektor. Survei tahun 2021 oleh KPMG Indonesia menemukan bahwa 73% organisasi melaporkan kesulitan dalam merekonsiliasi berbagai persyaratan regulasi dalam satu kerangka SMKI.

Kendala bahasa memengaruhi efektivitas implementasi SMKI. Sebagian besar kerangka kerja, standar, dan praktik terbaik internasional didokumentasikan terutama dalam bahasa Inggris, sementara staf operasional di banyak organisasi Indonesia mungkin memiliki kemampuan bahasa Inggris yang terbatas. Hal ini menciptakan potensi salah tafsir terhadap persyaratan selama implementasi. Organisasi sering kali perlu menginvestasikan sumber daya yang signifikan dalam menerjemahkan dan mengontekstualisasikan dokumentasi SMKI, yang dapat menimbulkan ketidakkonsistenan dan keterlambatan. Adaptasi terminologi keamanan teknis ke Bahasa Indonesia menghadirkan tantangan khusus di mana terjemahan langsung mungkin tidak ada atau memiliki konotasi yang berbeda.

Penyebaran geografis menambah kompleksitas implementasi SMKI bagi organisasi yang beroperasi di seluruh kepulauan Indonesia yang luas. Memastikan kontrol keamanan yang konsisten di seluruh fasilitas di berbagai pulau, yang sering kali memiliki tingkat konektivitas dan keandalan infrastruktur yang berbeda-beda, menghadirkan tantangan

logistik. Organisasi dengan operasi nasional melaporkan biaya implementasi SMKI 2,3 kali lebih tinggi dibandingkan dengan organisasi yang beroperasi di satu lokasi, menurut penelitian oleh Forum Keamanan Informasi Indonesia. Kemampuan audit dan pemantauan jarak jauh menjadi penting tetapi sulit untuk diterapkan di wilayah dengan konektivitas terbatas.

Sifat informal dari banyak proses bisnis di berbagai segmen ekonomi Indonesia menciptakan tantangan dokumentasi untuk penerapan SMKI. ISO 27001 dan kerangka kerja serupa menekankan prosedur terdokumentasi dan bukti efektivitas pengendalian, yang bertentangan dengan gaya operasional yang lebih informal yang umum di banyak organisasi Indonesia. Perusahaan kecil dan menengah sering kali beroperasi dengan dokumentasi formal yang minim, sehingga transisi ke persyaratan SMKI menjadi sangat menantang. Sebuah studi oleh Kamar Dagang Indonesia menemukan bahwa 64% UKM mengidentifikasi persyaratan dokumentasi sebagai hambatan paling signifikan terhadap adopsi SMKI.

Menyeimbangkan keamanan dengan kegunaan menimbulkan tantangan dalam konteks Indonesia, di mana literasi digital sangat bervariasi. Menerapkan kontrol keamanan yang ketat dapat menimbulkan gesekan yang menghambat penerapan, khususnya di lingkungan tempat pengguna memiliki keterbatasan kemampuan teknis. Organisasi melaporkan bahwa langkah-langkah keamanan yang berlebihan sering kali mengarah pada solusi sementara yang pada akhirnya merusak tujuan perlindungan. Menemukan keseimbangan yang tepat memerlukan pertimbangan cermat terhadap kemampuan pengguna dan persyaratan operasional yang khusus untuk konteks Indonesia.

Terakhir, komitmen kepemimpinan sangat bervariasi di berbagai organisasi. Meskipun manajemen senior mungkin menyetujui penerapan SMKI, keterlibatan berkelanjutan selama proses penerapan sering kali kurang. Keamanan sering kali dipandang sebagai masalah teknis daripada masalah strategis, yang mengakibatkan kurangnya kewenangan dan sumber daya bagi tim penerapan. Sebuah survei oleh Deloitte Indonesia menemukan bahwa hanya 28% organisasi yang memiliki perwakilan di tingkat dewan untuk masalah keamanan informasi, jauh lebih rendah dari rata-rata global sebesar 53%. Kesenjangan tata kelola ini melemahkan efektivitas upaya penerapan SMKI dan membatasi potensinya untuk meningkatkan kerahasiaan data pribadi.

E. KESIMPULAN

Penerapan Sistem Manajemen Keamanan Informasi di Indonesia merupakan upaya penting dalam menjaga kerahasiaan data pribadi di tengah percepatan transformasi digital negara ini. Pemeriksaan ini telah mengungkap dampak SMKI yang beragam pada praktik perlindungan data di seluruh lanskap Indonesia, yang menyoroti peningkatan signifikan dalam postur keamanan organisasi, kemampuan respons insiden, dan perlindungan teknis untuk informasi pribadi. Standarisasi praktik keamanan melalui kerangka kerja seperti ISO 27001 telah berkontribusi pada pendekatan yang lebih sistematis terhadap perlindungan data, meskipun penerapannya tidak merata di berbagai sektor dan wilayah.

Bersamaan dengan itu, analisis tersebut telah mengidentifikasi lanskap ancaman kompleks yang menimbulkan risiko substansial terhadap kerahasiaan data pribadi di Indonesia. Kombinasi serangan siber yang canggih, faktor budaya unik yang memengaruhi ancaman internal, kerentanan infrastruktur, dan kesenjangan regulasi menciptakan lingkungan yang menantang untuk melindungi informasi sensitif. Ancaman-ancaman ini semakin diperparah oleh risiko bencana alam yang khusus untuk posisi geografis Indonesia dan meluasnya penggunaan teknologi seluler dengan kontrol keamanan yang tidak konsisten.

Tantangan implementasi yang diidentifikasi—termasuk kendala sumber daya, kekurangan keterampilan, faktor budaya, kompleksitas regulasi, dan penyebaran geografis—menyoroti perlunya pendekatan yang disesuaikan secara kontekstual terhadap implementasi SMKI di Indonesia. Kerangka kerja standar yang dikembangkan dalam konteks Barat memerlukan modifikasi signifikan untuk mengatasi keadaan unik Indonesia dan berfungsi secara efektif dalam budaya organisasinya yang beragam.

Ke depannya, beberapa prioritas strategis muncul untuk memperkuat perlindungan data pribadi melalui SMKI di Indonesia. Pertama, ada kebutuhan yang jelas untuk inisiatif peningkatan kapasitas yang mengatasi kesenjangan keterampilan keamanan, khususnya di wilayah di luar Jawa. Kedua, upaya harmonisasi regulasi harus bertujuan untuk menciptakan koherensi yang lebih besar antara persyaratan sektoral dan Undang-Undang Perlindungan Data Pribadi yang menyeluruh. Ketiga, pedoman implementasi khusus Indonesia untuk SMKI yang memperhitungkan konteks budaya lokal dan realitas operasional akan secara signifikan meningkatkan tingkat adopsi dan efektivitas.

Seiring dengan perjalanan digital Indonesia, perlindungan data pribadi melalui penerapan SMKI yang efektif akan tetap menjadi perhatian penting bagi organisasi di semua sektor. Keberhasilan upaya ini tidak hanya bergantung pada solusi teknis, tetapi juga pada penanganan faktor sosial-budaya, ekonomi, dan geografis yang unik yang membentuk lanskap keamanan informasi Indonesia. Dengan mengembangkan pendekatan yang menanggapi faktor kontekstual ini sambil tetap menjaga keselarasan dengan standar internasional, Indonesia dapat membangun kerangka kerja yang kuat untuk perlindungan data pribadi yang mendukung hak privasi individu dan inovasi digital yang berkelanjutan.

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

dan melindungi terhadap ancaman keamanan, tanpa mengorbankan kecepatan dan efisiensi.

4. Keamanan Infrastruktur (Infrastructure Security)

Merujuk pada langkah-langkah dan tindakan yang diambil untuk melindungi perangkat keras, perangkat lunak, jaringan, serta semua elemen lain yang membentuk infrastruktur IT dari ancaman atau serangan yang dapat merusak integritas, kerahasiaan, dan ketersediaannya. Infrastruktur IT yang aman memastikan bahwa data, aplikasi, dan sistem berjalan dengan lancar, bebas dari gangguan yang disebabkan oleh ancaman eksternal maupun internal.

Tujuannya adalah untukMelindungi hardware dan virtual machine (VM) dari kerusakan fisik dan manipulasi. Implementasi:

a. Keamanan fisik di data center merupakan langkah-langkah dan kontrol yang diterapkan untuk melindungi perangkat keras, perangkat lunak, dan data yang ada di dalam data center dari ancaman fisik seperti pencurian, kebakaran, bencana alam, atau akses yang tidak sah. Keamanan fisik sangat penting karena data center menyimpan data sensitif dan mendukung operasi kritis bagi banyak organisasi, sehingga setiap gangguan dapat menyebabkan kerugian yang besar baik dari segi finansial maupun reputasi.
b. Pengelolaan patch & update system yaitu sebuah proses penting dalam menjaga keamanan dan kinerja sistem IT dengan cara memastikan bahwa perangkat keras, perangkat lunak, dan aplikasi selalu diperbarui dengan patch atau pembaruan terbaru. Patch dan update dirancang untuk memperbaiki kerentanannya, meningkatkan fungsionalitas, dan menambah fitur baru yang diperlukan untuk menjaga agar sistem tetap aman, stabil, dan efisien
c. Isolasi VM dan kontainer pada teknik yang digunakan untuk memisahkan lingkungan atau aplikasi yang berjalan pada sistem yang sama, dengan tujuan meningkatkan keamanan, kinerja, dan stabilitas. Meskipun keduanya, **Virtual Machine (VM)** dan **kontainer**, memiliki konsep isolasi yang sama—yaitu memisahkan aplikasi dan layanan agar tidak saling memengaruhi—keduanya berbeda dalam cara implementasinya dan tingkat isolasi yang diberikan.**Virtual Machine (VM)** merupakan sebuah mesin virtual yang berjalan di atas perangkat keras fisik melalui **hypervisor**, sebuah perangkat lunak yang mengelola dan mengontrol VM. Setiap VM berisi seluruh sistem operasi (OS) lengkap, termasuk kernel, aplikasi, dan pustaka sistem

lainnya. Isolasi antara VM dilakukan pada tingkat **hardware virtualisasi**, dengan setiap VM memiliki salinan lengkap dari OS-nya sendiri.

5. Keamanan Cloud Provider (Cloud Provider Security)

Langkah-langkah yang diambil oleh penyedia layanan cloud (cloud service provider atau CSP) untuk melindungi infrastruktur dan layanan yang mereka tawarkan kepada pengguna mereka. Keamanan cloud menjadi semakin penting karena semakin banyak organisasi yang memindahkan data dan aplikasi mereka ke cloud. Cloud computing menawarkan berbagai keuntungan, tetapi juga memperkenalkan berbagai tantangan dalam hal kontrol, kebijakan, dan potensi risiko keamanan.

Keamanan yang ditawarkan oleh penyedia cloud umumnya mencakup berbagai aspek, mulai dari keamanan fisik pusat data, kontrol akses, enkripsi data, hingga perlindungan terhadap serangan siber(Romindo, R., et al., 2024). Namun, meskipun penyedia cloud memiliki banyak fitur keamanan, penting untuk diingat bahwa keamanan cloud adalah tanggung jawab bersama (shared responsibility model), yang berarti bahwa selain perlindungan yang disediakan oleh penyedia cloud, pelanggan juga memiliki tanggung jawab untuk melindungi data mereka dan aplikasi yang mereka jalankan di cloud. Tujuan: Kepercayaan bahwa penyedia cloud mematuhi standar keamanan. Implementasi:

a. Sertifikasi: ISO 27001, SOC 2, PCI DSS merupakan standar internasional yang digunakan untuk mengevaluasi dan mengelola keamanan informasi dan data sensitif. Sertifikasi ini memberikan jaminan bahwa organisasi yang memilikinya telah memenuhi standar yang ketat dalam hal pengelolaan risiko dan perlindungan data. Masing-masing sertifikasi ini berfokus pada aspek tertentu dari keamanan informasi dan sangat penting untuk membangun kepercayaan pelanggan dan mitra bisnis.
   i. **ISO/IEC 27001** adalah standar internasional untuk **sistem manajemen keamanan informasi (ISMS)** yang dirancang untuk membantu organisasi melindungi informasi sensitif. Sertifikasi ISO 27001 menetapkan persyaratan untuk merancang, mengimplementasikan, mengelola, dan memelihara ISMS yang efektif untuk melindungi data dari ancaman yang dapat merusak kerahasiaan, integritas, dan ketersediaan informasi.

Dengan melekukan Manajemen Risiko: Menekankan pentingnya pendekatan berbasis risiko untuk mengidentifikasi, mengevaluasi, dan mengelola ancaman terhadap informasi sensitif. **Kontrol Keamanan**: Mencakup kontrol yang terkait dengan kebijakan, prosedur, kontrol fisik, dan teknologi untuk menjaga keamanan informasi. **Audit dan Pemantauan**: Organisasi yang memiliki sertifikasi ISO 27001 harus melakukan audit dan pemantauan berkelanjutan untuk memastikan bahwa sistem manajemen keamanan informasi mereka tetap efektif dan sesuai dengan standar. **Perbaikan Berkelanjutan**: Proses untuk mengevaluasi dan memperbaiki kebijakan dan prosedur ISMS agar tetap relevan dengan ancaman dan teknologi yang terus berkembang.

ii. **SOC 2 (System and Organization Controls 2)** adalah standar yang dikeluarkan oleh **American Institute of Certified Public Accountants (AICPA)** yang mengatur kontrol yang diterapkan oleh penyedia layanan cloud atau pihak ketiga untuk melindungi data pelanggan. Sertifikasi SOC 2 berfokus pada lima prinsip utama: **Keamanan, Ketersediaan, Integritas Pemrosesan, Kerahasiaan, dan Privasi**.

Keamanan: Melibatkan perlindungan terhadap sistem dari akses yang tidak sah atau serangan. **Ketersediaan**: Menjamin bahwa layanan tersedia sesuai dengan komitmen dan harapan. **Integritas Pemrosesan**: Memastikan bahwa pemrosesan data dilakukan secara akurat, lengkap, dan tepat waktu. **Kerahasiaan**: Menjaga data yang sensitif agar tetap aman dan hanya dapat diakses oleh pihak yang berwenang. **Privasi**: Memastikan bahwa informasi pribadi yang dikumpulkan oleh organisasi digunakan dan dikelola dengan cara yang sesuai dengan kebijakan privasi.

SOC 2 dikategorikan dalam dua tipe laporan: **Tipe I**: Menilai apakah kontrol yang diterapkan sesuai dengan standar pada titik waktu tertentu dan**Tipe II**: Menilai efektivitas kontrol tersebut selama periode waktu tertentu (misalnya, enam bulan atau setahun).

iii. **PCI DSS (Payment Card Industry Data Security Standard)PCI DSS (Payment Card Industry Data Security Standard)** adalah

serangkaian persyaratan yang diterbitkan oleh **Payment Card Industry Security Standards Council (PCI SSC)** untuk melindungi data kartu pembayaran, seperti kartu kredit dan debit. PCI DSS digunakan oleh organisasi yang menangani, menyimpan, atau memproses informasi kartu pembayaran dan bertujuan untuk mengurangi risiko kebocoran data kartu pembayaran(B. Surya & T. David, 2022). Dengan cara melakukan **Keamanan Jaringan**: Mengharuskan perusahaan untuk mengamankan jaringan mereka dengan firewall, kontrol akses, dan perlindungan lainnya(Setiawan, D., et al., 2025).

Pengelolaan Akses: Mengelola dan membatasi akses ke data kartu pembayaran hanya kepada individu yang berwenang. **Enkripsi**: Memastikan bahwa data kartu pembayaran dilindungi dengan enkripsi baik saat disimpan (data at rest) maupun saat dikirimkan (data in transit)(Stallings, 2013). **Pemantauan dan Pengujian**: Menuntut adanya pemantauan dan pengujian sistem untuk mendeteksi aktivitas yang mencurigakan serta memastikan kontrol keamanan berfungsi dengan baik. **Pengelolaan Kerentanannya**: Mengidentifikasi dan menangani kerentanannya dalam sistem yang berhubungan dengan pemrosesan data kartu pembayaran.

b. Layanan keamanan terintegrasi dari penyedia (misalnya AWS GuardDuty, Azure Security Center) Fitur keamanan yang disediakan langsung oleh platform cloud seperti **Amazon Web Services (AWS)**, **Microsoft Azure**, atau **Google Cloud Platform (GCP)** untuk membantu pengguna memantau, mendeteksi, merespons, dan melindungi infrastruktur cloud mereka dari ancaman keamanan. Layanan ini memungkinkan pengguna untuk **mengintegrasikan keamanan ke dalam seluruh arsitektur cloud** mereka secara native, tanpa perlu solusi pihak ketiga, sehingga meningkatkan efisiensi dan visibilitas keamanan

6. Keamanan Backup dan Recovery

Merupakan aspek kritikal dalam strategi keamanan cloud computing. Ini bertujuan untuk memastikan bahwa data tetap **tersedia, utuh, dan dapat dipulihkan** jika terjadi insiden seperti serangan siber, kerusakan sistem, atau bencana alam. Backup tanpa pengamanan dapat

menjadi titik lemah yang dapat dimanfaatkan oleh penyerang, sementara recovery yang tidak efektif dapat mengakibatkan kehilangan data permanen atau downtime berkepanjangan.

Tujuan: Menjamin data dapat dipulihkan saat terjadi insiden atau bencana. Implementasi:

a. Backup berkala (snapshot, offsite) adalah salah satu praktik penting dalam menjaga **keberlangsungan data dan keamanan sistem informasi** di lingkungan cloud computing. Dengan melakukan backup secara berkala, organisasi dapat meminimalisir kehilangan data akibat kesalahan manusia, serangan siber, atau kegagalan sistem.
b. Disaster Recovery Plan (DRP) merupakan serangkaian prosedur yang dirancang untuk **memulihkan sistem, data, dan infrastruktur TI** yang terkena dampak **bencana** baik bencana alam, kegagalan perangkat keras, serangan siber, maupun kesalahan manusia sehingga organisasi dapat **melanjutkan operasional bisnis secepat mungkin**. DRP merupakan bagian penting dari **Business Continuity Planning (BCP)** dan sangat krusial dalam konteks **cloud computing,** di mana ketergantungan terhadap layanan digital sangat tinggi.
c. High Availability & Redundancy adalah dua konsep penting dalam arsitektur sistem cloud yang bertujuan untuk **menjamin ketersediaan layanan secara terus-menerus,** bahkan ketika terjadi kegagalan pada komponen tertentu. Dalam konteks keamanan cloud computing, HA & Redundancy sangat penting untuk memastikan **layanan tetap berjalan tanpa gangguan yang merusak data, performa, atau kepercayaan pengguna. High Availability (HA)** mengacu pada desain sistem yang **minim gangguan (downtime)** dan tetap berfungsi dengan baik bahkan saat terjadi kerusakan atau lonjakan beban. **Redundancy** berarti menyiapkan **komponen cadangan (backup)** untuk menggantikan komponen utama jika terjadi kegagalan.

7. Keamanan Privasi dan Kepatuhan (Privacy & Compliance)

Keamanan privasi dan kepatuhan merupakan aspek penting dalam penggunaan layanan cloud, terutama ketika data yang disimpan atau diproses mencakup **informasi sensitif** seperti data pribadi, data keuangan, atau data kesehatan. Cloud computing harus

diimplementasikan dengan memperhatikan **perlindungan data pribadi** serta **kepatuhan terhadap peraturan dan standar industri** yang berlaku secara lokal maupun internasional.

Tujuannya adalah Memastikan data pribadi diproses sesuai regulasi antara lain.

a. Kepatuhan terhadap GDPR, HIPAA, dsb. Cloud computing memungkinkan organisasi menyimpan dan memproses data di berbagai wilayah geografis. Hal ini membawa tantangan dalam **memastikan bahwa pengelolaan data mematuhi berbagai regulasi perlindungan data** di masing-masing negara atau industri. Oleh karena itu, organisasi harus memahami dan menerapkan **kepatuhan (compliance)** terhadap regulasi seperti **GDPR, HIPAA, PCI DSS**, dan lainnya agar tidak terkena sanksi hukum serta menjaga kepercayaan pengguna. GDPR adalah regulasi perlindungan data pribadi yang berlaku di seluruh negara Uni Eropa dan berdampak global bagi organisasi yang menangani data warga EU. HIPAA melindungi data kesehatan pribadi (PHI Protected Health Information) dan berlaku untuk rumah sakit, laboratorium, serta penyedia teknologi kesehatan. PCI DSS mengatur standar keamanan untuk organisasi yang memproses, menyimpan, atau mentransmisikan data kartu kredit/debit.
b. Kebijakan privasi dan data anonymization Dalam ekosistem cloud computing, **kebijakan privasi** dan **data anonymization** menjadi bagian penting untuk melindungi informasi sensitif pengguna serta memastikan kepatuhan terhadap peraturan perlindungan data seperti **GDPR, UU PDP,** dan lainnya. Keduanya membantu organisasi menjaga kepercayaan pengguna serta meminimalkan risiko penyalahgunaan atau kebocoran data. **Kebijakan privasi** adalah dokumen atau aturan yang menjelaskan **bagaimana data pribadi dikumpulkan, digunakan, disimpan, dan dibagikan** oleh organisasi, terutama saat menggunakan layanan cloud. sedangkan **Data anonymization** adalah proses **menghilangkan atau menyamarkan identitas individu** dari kumpulan data agar tidak bisa dikaitkan kembali dengan individu tersebut, meskipun data dibocorkan atau dibagikan.
C. Audit & monitoring akses data merupakan langkah krusial untuk mendeteksi, menganalisis, dan mencegah aktivitas yang mencurigakan atau tidak sah terhadap data. Ini merupakan bagian

dari **strategi keamanan proaktif** untuk menjaga integritas, kerahasiaan, dan ketersediaan data yang tersimpan dan diproses di cloud.

D. RANGKUMAN

Keamanan cloud computing melibatkan langkah-langkah terintegrasi untuk melindungi data, aplikasi, dan infrastruktur cloud. Dimulai dengan memastikan **keamanan aplikasi dan API** melalui pengujian kerentanannya dan menggunakan alat seperti **Web Application Firewalls (WAF)** dan **API Gateway yang aman**. Dalam pengembangan aplikasi, penting juga untuk menerapkan **DevSecOps** (keamanan tertanam dalam CI/CD) untuk meminimalkan potensi celah keamanan.

Selanjutnya, **keamanan infrastruktur** memastikan perlindungan fisik data center, pengelolaan patch dan update sistem secara rutin, serta penerapan **isolasi VM dan kontainer** untuk memisahkan aplikasi dan mengurangi risiko. Penerapan **High Availability & Redundancy** juga penting untuk menjaga ketersediaan sistem, bahkan jika terjadi gangguan. Penting juga untuk memilih **cloud provider dengan sertifikasi keamanan** seperti **ISO 27001, SOC 2, dan PCI DSS**, serta menggunakan **layanan keamanan terintegrasi** yang disediakan oleh penyedia cloud, seperti **AWS GuardDuty atau Azure Security Center**, untuk memantau dan melindungi layanan cloud secara otomatis.

Keamanan backup dan recovery memastikan data penting terlindungi dengan melakukan **backup berkala** dan merencanakan **Disaster Recovery Plan (DRP)** untuk pemulihan data setelah insiden. Dengan memastikan **redundansi** dan **high availability**, data tetap tersedia meskipun terjadi gangguan besar. Selain itu, **kepatuhan terhadap regulasi** seperti **GDPR, HIPAA, PCI DSS, dan UU PDP** penting untuk melindungi data pribadi dan memastikan organisasi mematuhi standar hukum yang berlaku. **Kebijakan privasi** yang jelas menjelaskan bagaimana data dikumpulkan, disimpan, dan digunakan, sementara **data anonymization** digunakan untuk mengurangi risiko penyalahgunaan data dengan menyamarkan atau menghapus identitas pribadi dalam data.

Terakhir, **audit dan monitoring akses data** sangat penting untuk melacak siapa yang mengakses data dan aplikasi cloud. **Log aktivitas** dan **pemantauan real-time** membantu mendeteksi anomali atau aktivitas mencurigakan, dan sistem **alerting otomatis** memberi notifikasi jika

terjadi pelanggaran atau ketidaknormalan. Integrasi dengan **sistem SIEM** memungkinkan pengumpulan dan analisis log secara terpusat untuk keamanan yang lebih efektif.

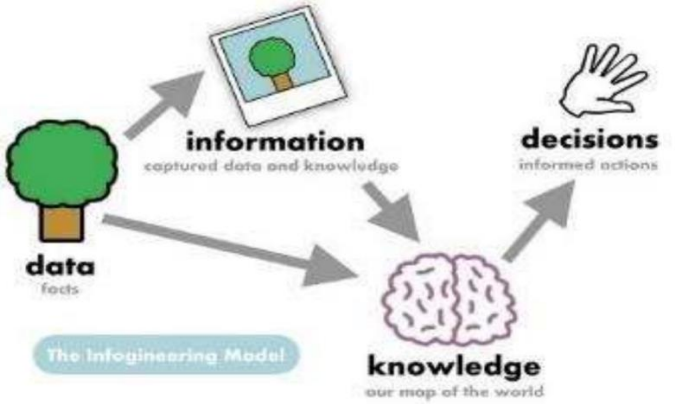
BAB 13 KEAMANAN DALAM BIG DATA DAN IOT

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:

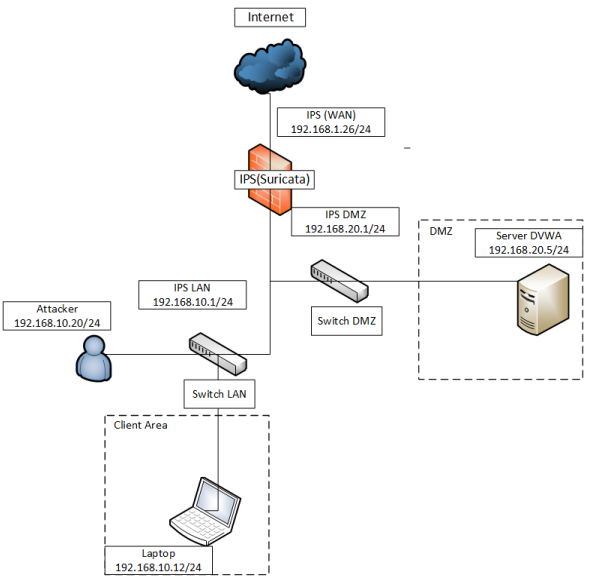
1. Keamanan
   Keamanan adalah tantangan terbesar dalam Big Data dan IoT. Semakin banyak perangkat yang terhubung, semakin besar kemungkinan adanya eksploitasi kerentanan keamanan. Perangkat yang dirancang dengan buruk dapat mengekspos data pengguna terhadap pencurian dengan membiarkan data tidak terlindungi 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.

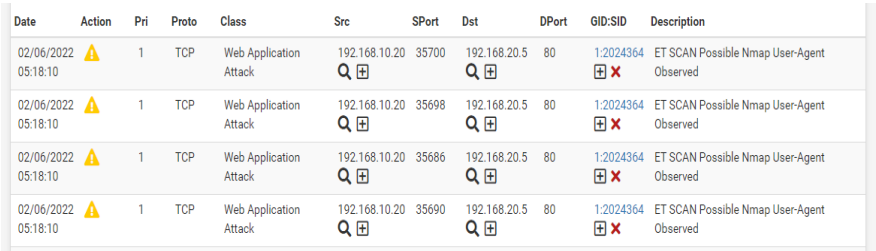
Hasil pengamatan juga mengungkapkan bahwa penggunaan algoritma Bcrypt (Batubara, Efendi and Nababan, 2021) dan implementasi IDS berbasis Snort (Hidayat and Ramli, 2023) mampu memberikan perlindungan signifikan terhadap serangan. Dengan meningkatnya jumlah insiden serangan bruteforce pada server dan perangkat IoT, diperlukan pendekatan yang komprehensif untuk menganalisis pola serangan, mendeteksi kelemahan, dan menerapkan teknologi mitigasi yang lebih efektif. Oleh karena itu melakukan identifikasi ancaman dari serangan bruteforce, mengevaluasi metode deteksi seperti Intrusion Detection System (IDS) berbasis Snort, dan memberikan rekomendasi untuk meningkatkan keamanan jaringan juga memberikan rekomendasi praktis untuk mengadopsi teknologi mitigasi seperti CAPTCHA, autentikasi dua faktor, dan IDS sebagai langkah strategis dalam meningkatkan keamanan jaringan.

Berdasarkan hasil riset analisis keamanan jaringan menggunakan IPS (*Intrusion Prevention System*) yang dilakukan oleh Lukman Silalahi (Silalahi and Kurniawan, 2023) mengangkat masalah tentang celah keamanan jaringan untuk disusupi oleh peretas jaringan internet, diantaranya yakni *Port Scanning*, DDoS (Distribute Denial of Service), *Bruteforce* yang ditunjukkan pada gambar 13.2.



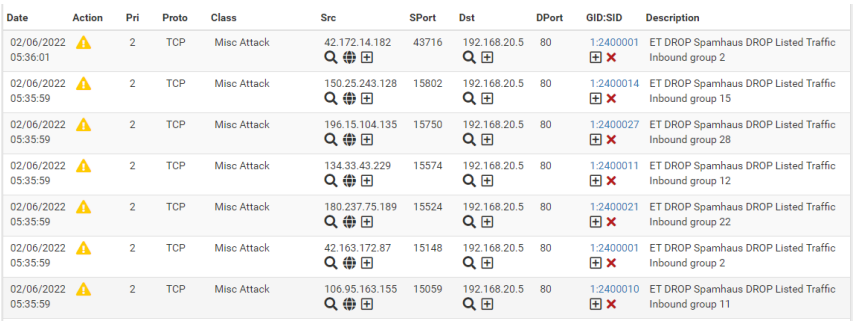
Gambar 13. 2. Topologi IPS (Silalahi and Kurniawan, 2023)

Hasil riset menunjukkan keberhasilan pendeteksian setiap serangan yang terjadi dan melakukan blokir akses masuk ke server yang ditunjukkan pada gambar 13.3 hingga gambar 13.5. Metode riset adalah riset eksperimental yang bersifat kuantitatif menggunakan IPS serta dikombinasikan antara fitur blocking dari Firewall dan fitur detection capabilities dari IDS (*Intrusion Detection System*).



Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/06/2022 05:18:10	⚠	1	TCP	Web Application Attack	192.168.10.20	35700	192.168.20.5	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed
02/06/2022 05:18:10	⚠	1	TCP	Web Application Attack	192.168.10.20	35698	192.168.20.5	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed
02/06/2022 05:18:10	⚠	1	TCP	Web Application Attack	192.168.10.20	35686	192.168.20.5	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed
02/06/2022 05:18:10	⚠	1	TCP	Web Application Attack	192.168.10.20	35690	192.168.20.5	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed

Gambar 13. 3. Hasil deteksi Port Scanning (Silalahi and Kurniawan, 2023)



Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/06/2022 05:36:01	⚠	2	TCP	Misc Attack	42.172.14.182	43716	192.168.20.5	80	1:2400001	ET DROP Spamhaus DROP Listed Traffic Inbound group 2
02/06/2022 05:35:59	⚠	2	TCP	Misc Attack	150.25.243.128	15802	192.168.20.5	80	1:2400014	ET DROP Spamhaus DROP Listed Traffic Inbound group 15
02/06/2022 05:35:59	⚠	2	TCP	Misc Attack	196.15.104.135	15750	192.168.20.5	80	1:2400027	ET DROP Spamhaus DROP Listed Traffic Inbound group 28
02/06/2022 05:35:59	⚠	2	TCP	Misc Attack	134.33.43.229	15574	192.168.20.5	80	1:2400011	ET DROP Spamhaus DROP Listed Traffic Inbound group 12
02/06/2022 05:35:59	⚠	2	TCP	Misc Attack	180.237.75.189	15524	192.168.20.5	80	1:2400021	ET DROP Spamhaus DROP Listed Traffic Inbound group 22
02/06/2022 05:35:59	⚠	2	TCP	Misc Attack	42.163.172.87	15148	192.168.20.5	80	1:2400001	ET DROP Spamhaus DROP Listed Traffic Inbound group 2
02/06/2022 05:35:59	⚠	2	TCP	Misc Attack	106.95.163.155	15059	192.168.20.5	80	1:2400010	ET DROP Spamhaus DROP Listed Traffic Inbound group 11

Gambar 13. 4. Hasil deteksi DDoS (Silalahi and Kurniawan, 2023)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35898	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35896	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35888	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35892	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35894	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35886	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35884	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35882	192.168.20.5	80	1:1001	Bruteforce Detection
02/06/2022 06:33:54	⚠	1	TCP	Potential Corporate Privacy Violation	192.168.10.20	35880	192.168.20.5	80	1:1001	Bruteforce Detection

Gambar 13. 5. Hasil deteksi Bruteforce (Silalahi and Kurniawan, 2023)

D. RANGKUMAN

Dokumen ini menjelaskan konsep dasar, karakteristik, serta tantangan dari Big Data dan Internet of Things (IoT). Big Data dipahami sebagai akumulasi data kecil yang, ketika diolah, membentuk gambaran besar yang informatif. IoT merujuk pada jaringan perangkat fisik yang terkoneksi internet, dilengkapi sensor dan teknologi yang memungkinkan pertukaran data antar perangkat. IoT memungkinkan otomatisasi berbagai aspek kehidupan dengan dukungan infrastruktur internet dan teknologi seperti IPv6.

Karakteristik utama Big Data dan IoT meliputi kemampuan adaptif, interoperabilitas protokol komunikasi, identitas unik tiap perangkat, konfigurasi mandiri, dan keterhubungan dalam jaringan informasi. Teknologi dasar pendukungnya antara lain M2M (Machine to Machine), CPS (Cyber-Physical Systems), dan WoT (Web of Things).

Tantangan utama mencakup isu keamanan, skalabilitas, interoperabilitas antar perangkat dan sistem, serta kebutuhan bandwidth tinggi. Salah satu fokus keamanan adalah serangan bruteforce yang dapat dideteksi dengan IDS seperti Snort dan dicegah dengan autentikasi dua faktor dan CAPTCHA.

Penelitian oleh Silalahi dan Kurniawan menunjukkan bahwa IPS mampu mendeteksi serangan seperti port scanning, DDoS, dan bruteforce, serta memblokir akses secara efisien. Strategi mitigasi keamanan jaringan sangat penting untuk mendukung adopsi Big Data dan IoT secara luas.

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)

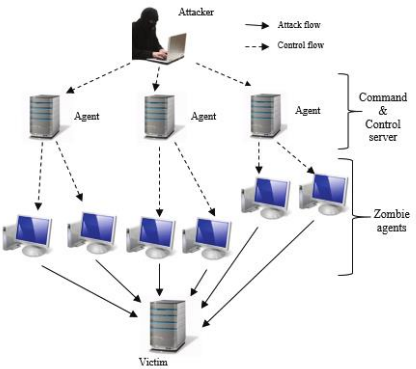
5. AI Agentik dan Serangan Berbasis Kecerdasan Buatan

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.

7. Kerentanan Pihak Ketiga

Peretas menyusup melalui vendor atau mitra dengan keamanan lemah(Embroker 2025a)

C. STRATEGI DAN TEKNIK PENCEGAHAN

1. Implementasi Firewall dan Sistem Deteksi Intrusi

Firewall berfungsi sebagai penghalang antara jaringan internal dan eksternal, memblokir akses tidak sah dan menyaring trafik mencurigakan. Keuntungan utama implementasi firewall meliputi:

- Memblokir akses ilegal ke jaringan
- Menyaring lalu lintas data berbahaya
- Meningkatkan keamanan jaringan secara keseluruhan(Kompas 2025)

Untuk efektivitas optimal, disarankan untuk:

- Memastikan firewall selalu aktif dan diperbarui
- Menyesuaikan konfigurasi firewall dengan kebutuhan jaringan
- Menggunakan firewall baik di tingkat jaringan maupun perangkat(Kompas 2025)

2. Enkripsi Data

Enkripsi mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang tepat, menjadikannya garis pertahanan penting dalam melindungi informasi sensitif. Manfaat utama enkripsi data meliputi:

- Melindungi informasi sensitif meskipun jatuh ke tangan yang salah
- Memenuhi kepatuhan terhadap regulasi keamanan data
- Meningkatkan kepercayaan pelanggan dan pemangku kepentingan(Kompas 2025)

3. Autentikasi Multi-Faktor

Implementasi two-factor authentication (2FA) atau multi-factor authentication (MFA) sangat direkomendasikan untuk meningkatkan keamanan akses. Metode ini memerlukan verifikasi melalui dua atau lebih mekanisme independen, sehingga mencegah akses tidak sah meskipun password diketahui oleh pihak lain(Sibermate 2024).

4. Pembaruan dan Patching Reguler

Memperbarui software dan sistem secara teratur merupakan langkah fundamental dalam keamanan siber. Banyak serangan siber memanfaatkan kerentanan yang sudah diketahui namun belum diperbaiki pada sistem yang tidak diperbarui(Sibermate 2024). Disarankan untuk:

- Mengaktifkan pembaruan otomatis bila memungkinkan
- Menyiapkan jadwal pembaruan reguler untuk sistem kritis
- Menerapkan proses pengujian patch sebelum implementasi pada lingkungan produksi

5. Edukasi dan Kesadaran Keamanan

Faktor manusia tetap menjadi komponen penting dalam keamanan siber. Program edukasi dan peningkatan kesadaran harus mencakup:

- Pelatihan untuk mengenali upaya phishing dan social engineering
- Praktik pengelolaan password yang aman
- Prosedur pelaporan insiden keamanan
- Simulasi serangan untuk mengevaluasi kesiapan(Sibermate 2024)(Edavos 2025)

6. Backup Data Reguler

Strategi backup yang efektif merupakan pertahanan terakhir yang krusial terhadap ransomware dan bencana data lainnya. Praktik terbaik meliputi:

- Menerapkan aturan backup 3-2-1 (3 salinan data, pada 2 media berbeda, dengan 1 salinan off-site)
- Melakukan backup secara reguler dan terencana
- Menguji prosedur pemulihan data secara berkala(Edavos 2025)

D. STUDI KASUS SERANGAN SIBER DI INDONESIA DAN DUNIA

1. Serangan Ransomware LockBit pada Bank Syariah Indonesia (2023)

Kelompok peretas Rusia bernama LockBit melumpuhkan server Bank Syariah Indonesia pada Mei 2023, menyebabkan

aplikasi mobile banking tidak dapat diakses. Serangan ini mengakibatkan hilangnya 1,5 TB data, termasuk informasi pribadi nasabah dan karyawan. Peretas meminta tebusan untuk mengembalikan data, jika tidak data tersebut akan dijual di dark web(IDN 2025)(Tempo 2024).

BSI fokus pada pemulihan sistem dan normalisasi layanan perbankan, yang berangsur pulih sejak 11 Mei 2023. Kasus ini menjadi pembelajaran penting tentang pentingnya keamanan siber di sektor finansial dan perlunya sistem backup serta rencana pemulihan bencana yang efektif(IDN 2025).

2. Kebocoran Data Pelanggan Biznet (2024)

Kasus kebocoran data 380.000 pelanggan Biznet Networks, diikuti oleh 150.000 data jaringan Biznet lainnya, menunjukkan kompleksitas dalam menangani threat insider dan ancaman eksternal. Awalnya, pelaku mengklaim sebagai karyawan Biznet, namun investigasi mengungkapkan bahwa serangan dilakukan oleh pihak eksternal(IDN 2025).

Biznet berkolaborasi dengan kepolisian untuk menyelidiki kasus tersebut, mendemonstrasikan pentingnya kerjasama antara sektor privat dan penegak hukum dalam menangani insiden keamanan siber(IDN 2025).

3. Peretasan Situs BKN dan Penjualan Data ASN (2024)

Seorang guru honorer berhasil membobol sistem Badan Kepegawaian Negara menggunakan metode SQL injection. Pelaku mendapatkan akses kredensial dari forum dark web, kemudian mengunduh 6,3 GB data kepegawaian ASN untuk dijual, menghasilkan keuntungan sekitar 8.000 dolar AS(IDN 2025).

Kasus ini menyoroti pentingnya:

- Keamanan aplikasi dan pengujian kerentanan reguler
- Pemantauan aktivitas pengguna yang mencurigakan
- Praktik pengkodean aman untuk mencegah serangan injeksi SQL

4. Serangan pada Platform Kripto Indodax (2024)

Serangan terhadap Indodax menyebabkan kerugian mencapai Rp280 miliar. Insiden bermula ketika seorang karyawan mengambil pekerjaan freelance menggunakan laptop kantor yang memiliki akses ke server. Tanpa disadari, ini merupakan penipuan yang berujung pada masuknya malware, memungkinkan peretas mengakses server dan mencuri aset kripto(IDN 2025).

Indodax bergerak cepat dengan membekukan seluruh aktivitas, dan berhasil menyelesaikan masalah dalam 80 jam, dengan saldo anggota tetap aman. Kasus ini menekankan pentingnya:

- Kebijakan keamanan yang ketat untuk perangkat kerja
- Kesadaran karyawan terhadap social engineering
- Kemampuan respons insiden yang efektif(IDN 2025)

5. Serangan Siber pada Tokopedia (2020)

Peretas bernama ShinyHunters membocorkan sekitar 91 juta data pengguna dan 7 juta data penjual Tokopedia pada 2020. Serangan memanfaatkan celah keamanan di sistem Cloud dengan teknik SQL injection kompleks(CSIRT 2025).

Tokopedia merespons dengan mengonfirmasi bahwa data telah terenkripsi dan sulit diakses oleh peretas. Untuk mencegah serangan phishing pasca-insiden, mereka menyarankan pengguna untuk rutin mengganti kata sandi. Selanjutnya, Tokopedia meningkatkan keamanannya melalui adopsi teknologi automasi, deteksi, dan respons sesuai standar keamanan global, serta melakukan evaluasi tahunan bersama pihak ketiga(CSIRT 2025).

6. Pelanggaran Data Equifax (2017)

Deskripsi:
Serangan ini memanfaatkan kerentanan CVE-2017-5638 pada Apache Struts yang tidak ditambal. Peretas mengakses portal pengaduan online Equifax selama 76 hari (Mei-Juli 2017), mengekstrak data 147 juta konsumen termasuk nama, SSN, alamat, dan nomor SIM(B. University 2025).

Dampak:

- Kerugian finansial mencapai $1.7 miliar (termasuk denda FTC $700 juta).
- Penurunan 35% nilai saham Equifax dalam seminggu.
- 209.000 nomor kartu kredit bocor

Pelajaran:
Pembaruan rutin sistem dan manajemen kerentanan wajib(B. University 2025).

7. Ransomware WannaCry (2017)

Deskripsi:
Menyebar via exploit EternalBlue (CVE-2017-0144) yang dikembangkan NSA, menginfeksi 230.000 komputer di 150 negara dalam 4 hari. NHS Inggris menjadi korban terparah dengan 70.000 perangkat medis terenkripsi(B. University 2025).

Dampak:
- Rumah sakit dan lembaga pemerintah lumpuh.
- Kerugian global diperkirakan $4 miliar

Pelajaran:
Pembaruan patch sistem kritis(B. University 2025).

8. Spyware WhatsApp Meta (2025)

Deskripsi:
Peretas menyusup ke akun jurnalis dan aktivis via spyware(C. S. C. C. Library 2023).

Dampak:
Ancaman terhadap privasi komunikasi global.

Pencegahan:
Otentikasi dua faktor (MFA) dan pemantauan ancaman real-time(C. S. C. C. Library 2023).

9. Serangan Ransomware Colonial Pipeline (2021)

Deskripsi:
Serangan DarkSide menghentikan operasi pipa bahan bakar AS(ProserveIT 2025).

Dampak:
Kelangkaan BBM dan tebusan $4,4 juta.

Pelajaran:
- Penerapan *network microsegmentation* untuk sistem SCADA.
- Isolasi jaringan dan rencana respons insiden(ProserveIT 2025).

10. Kebocoran Data DISA Global (2025)

Deskripsi:
3.3 juta data tes narkoba dan latar belakang pekerja bocor akibat konfigurasi IAM yang lemah. Peretas mengakses sistem selama 72 hari sebelum terdeteksi(U. Library n.d.)(C. S. C. C. Library 2023).

Penyebab:
- Enkripsi data-at-rest tidak diimplementasikan
- *Privileged access management* tidak terpusat
- Kelemahan kontrol akses dan enkripsi.

11. Peretasan Cisco Routers oleh Salt Typhoon (2025)

Deskripsi:
Peretas Cina mengeksploitasi CVE-2023-20198 di IOS XE untuk instalasi backdoor di 1.000 router ISP. Serangan menyasar lawful intercept systems untuk penyadapan(U. Library n.d.).

Dampak:
- 1.000 perangkat di AS, India, dan Amerika Latin disusupi.
- Kebocoran metadata 5 juta pengguna

12. Pencurian Dana Bybit ETH (2025)

Deskripsi:
Lazarus Group (Korea Utara) mencuri 401.347 ETH ($1,46) miliar dicuri dari cold wallet Bybit. Serangan menggunakan teknik address poisoning dan chain-hopping di Tornado Cash(U. Library n.d.).

Pencegahan:
Multi-signature wallets dan audit keamanan rutin.

13. Phishing Microsoft 365 (2025)

Deskripsi:
Ancaman Storm-237 mencuri email melalui device code phishing(U. Library n.d.).

Sasaran:
Sektor pemerintah, energi, dan telekomunikasi.

14. Serangan Ransomware HCRG Care Group (2025)

Deskripsi:
Gangguan layanan kesehatan Inggris akibat enkripsi data(C. S. C. C. Library 2023). Serangan LockBit 3.0 menginfeksi sistem EHR di 40 rumah sakit Inggris via phishing COVID-19 vaksin. Data pasien dienkripsi dengan ChaCha20-Poly1305.

Respons:
Pemulihan data dari cadangan terisolasi.

15. Eksploitasi Firewall Palo Alto (2025)

Deskripsi:
Eksploitasi CVE-2025-XXXX di PAN-OS memungkinkan RCE via SAML. 1.200 organisasi pemerintah terpapar.

Peretas mengeksploitasi kerentanan firewall untuk akses jaringan(C. S. C. C. Library 2023).

Solusi:

Pemindaian kerentanan otomatis dengan AI[7].

16. Kebocoran Data GrubHub (2025)

Deskripsi:

Data pengguna, kurir, dan merchant dicuri via pihak ketiga(C. S. C. C. Library 2023)(U. Library n.d.). API pihak ketiga yang tidak diamankan mengakibatkan kebocoran 18 juta data pengguna. Penyerang menggunakan teknik credential stuffing dengan 2.1 juta permintaan/jam.

Pencegahan:

- Audit keamanan vendor dan segmentasi jaringan(Embroker 2025a).
- API security gateway dengan rate limiting dan schema validation

17. Serangan Lazarus Group via LinkedIn (2025)

Deskripsi:

Malware disebar melalui job offer palsu di LinkedIn(C. S. C. C. Library 2023). 750 karyawan tech company mengunduh RAT tersembunyi dalam dokumen "tawaran kerja". Malware menggunakan DNS-over-HTTPS untuk C2.

Modus:

- Deepfake video dalam proses wawancara
- Pencurian kredensial dan instalasi remote access trojan (RAT).

18. NotPetya Ransomware (2017)

Deskripsi:

Menyebar via pembaruan software palsu, rugi $10 miliar(ProserveIT 2025). Serangan berkedok update

software MeDoc di Ukraina, menyebar ke 65 negara. Menggunakan algoritma Salsa20 untuk enkripsi.

Pelajaran:
- Verifikasi integritas pembaruan sistem.
- *Cryptographic signing* untuk verifikasi *update* otomatis.

19. Insider Threat di Insight Partners (2025)

Deskripsi:
Social engineering mengakibatkan akses ilegal ke sistem VC(U. Library n.d.). Karyawan terpancing phising memberikan akses ke repositori GitHub berisi kode VC. 12 startup kehilangan IP senilai $450 juta.

Strategi:
- Pelatihan kesadaran keamanan dan least privilege access(Embroker 2025b).
- User behavior analytics (UBA) untuk aktivitas git abnormal
- Implementasi confidential computing untuk data sensitive

20. Kerentanan IoT di Sektor Kesehatan (2025)

Deskripsi:
2,7 miliar catatan pasien terbuka akibat konfigurasi salah(C. S. C. C. Library 2023). 2.7 miliar catatan pasien terekspos akibat default password pada IoT MRI. Perangkat terhubung ke Shodan tanpa autentikasi.

Solusi:
- Enkripsi data dan segmentasi jaringan IoT(Embroker 2025b).
- IoT security posture management dengan integrasi NAC.
- Enkripsi end-to-end menggunakan algoritma Kyber-1024.

E. RANGKUMAN

Serangan siber akan terus berkembang dalam kompleksitas dan frekuensi seiring kemajuan teknologi. Tahun 2025 diprediksi menjadi titik kritis dengan intensifikasi serangan yang didukung AI, meningkatnya serangan rantai pasokan, dan evolusi ransomware. Dalam menghadapi tantangan ini, diperlukan pendekatan holistik yang mengintegrasikan solusi teknis, kebijakan organisasi, dan pengembangan kapasitas manusia.

Perusahaan dan lembaga di Indonesia dan Dunia perlu memprioritaskan investasi pada keamanan siber, melakukan evaluasi risiko secara berkelanjutan, mengimplementasikan strategi pertahanan berlapis, dan membangun budaya keamanan siber yang kuat. Kolaborasi antara sektor publik dan swasta juga menjadi kunci dalam menghadapi ancaman siber yang semakin canggih dan berimplikasi luas.

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.

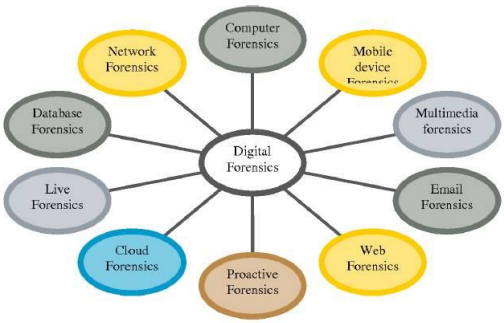
2. Prinsip-Prinsip Forensik Digital

   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

Penyajian bukti merupakan tahap akhir di mana hasil investigasi disampaikan kepada pihak terkait, termasuk aparat penegak hukum atau pengadilan. Di sini, penyelidik harus mampu menjelaskan proses dan temuan forensik secara jelas, meyakinkan, dan berdasarkan prosedur ilmiah. Kesiapan untuk memberikan kesaksian sebagai expert witness juga menjadi bagian dari tugas forensik digital dalam kasus hukum.

Bukti yang disajikan harus disertai dengan dokumentasi pendukung yang lengkap serta dapat diverifikasi oleh pihak lain. Untuk itu, penting bagi penyelidik memiliki keterampilan komunikasi, selain keahlian teknis, agar bukti dapat dipahami dan dipercaya. Dalam beberapa kasus, penyajian juga mencakup simulasi atau visualisasi temuan agar lebih mudah dicerna oleh hakim atau juri. Akurasi dan kredibilitas menjadi faktor utama dalam menentukan keberhasilan penyajian bukti.

D. TEKNIK DAN ALAT FORENSIK DIGITAL

1. Imaging atau Akuisisi

   Teknik imaging adalah fondasi dari proses forensik digital karena memungkinkan penyelidik membuat salinan persis (bit-by-bit) dari media penyimpanan yang sedang dianalisis. Dengan cara ini, data asli tidak akan diubah atau rusak selama proses investigasi berlangsung. Salinan ini biasa disebut sebagai forensic image dan disimpan dalam format seperti E01 (EnCase), AFF (Advanced Forensic Format), atau RAW (dd). Teknik ini penting untuk menjaga integritas bukti digital dan memastikan bisa digunakan di pengadilan.

   Proses imaging dilakukan menggunakan perangkat atau software khusus seperti FTK Imager, Guymager, atau write blocker (Thron et al., 2022) hardware untuk mencegah penulisan ulang data ke media sumber. Sebelum dan sesudah proses imaging, nilai hash (misalnya SHA-256) dari disk diperiksa untuk memastikan salinan benar-benar identik dengan aslinya. Imaging tidak hanya dilakukan pada hard disk, tapi juga bisa mencakup SSD, USB drive, kartu memori, dan bahkan perangkat mobile. Dengan memiliki salinan, penyelidik dapat melakukan analisis berulang tanpa risiko merusak bukti asli.
2. File Carving dan Metadata Analysis

   File carving adalah teknik untuk mengekstrak file dari media digital tanpa bergantung pada struktur sistem file, sering kali digunakan untuk mencari file yang sudah dihapus atau rusak.

Metode ini mencari pola header dan footer file tertentu, seperti JPEG, PDF, atau DOCX, untuk menemukan dan menyusun ulang file. Teknik ini sangat berguna saat sistem file telah dihapus atau dikorupsi, tapi data mentah masih tersedia di disk. Tools seperti Scalpel, PhotoRec, dan Autopsy mendukung file carving secara efisien.

Di sisi lain, analisis metadata memberikan informasi penting mengenai file digital, seperti waktu pembuatan, modifikasi, pengguna terakhir, dan bahkan lokasi GPS untuk gambar. Metadata bisa menjadi petunjuk penting dalam menentukan kronologi kejadian atau mengidentifikasi aktivitas pengguna (Mpungu et al., 2024). Misalnya, metadata dari dokumen Microsoft Word bisa mengungkap siapa pembuatnya dan kapan dokumen terakhir dibuka. Analisis metadata ini juga sangat berguna untuk menilai keaslian file atau mengidentifikasi adanya manipulasi data.

3. Tools Forensik Populer berdasarkan Kegunaannya

Dalam praktik forensik digital, berbagai alat digunakan tergantung pada jenis analisis yang dilakukan. Untuk imaging dan akuisisi data, tools seperti FTK Imager, Guymager, dan dd sangat populer. Sedangkan untuk analisis data, Autopsy (Rochmadi et al., 2020), Sleuth Kit, EnCase, dan X-Ways Forensics digunakan secara luas di lingkungan profesional. Untuk analisis memori dan aktivitas runtime, Volatility dan Rekall menjadi pilihan utama karena mendukung ekstraksi informasi dari dump RAM.

Dalam konteks forensik jaringan, tools seperti Wireshark (Milan & Rochmadi, 2024), tcpdump, dan NetworkMiner membantu menyusun kronologi komunikasi data dan mendeteksi anomali jaringan. Untuk pelacakan aktivitas internet dan artefak browser, Browser History Examiner atau NirSoft Tools sering digunakan. Selain itu, Magnet AXIOM adalah alat all-in-one yang banyak digunakan untuk kasus kompleks, terutama yang melibatkan perangkat mobile, cloud, dan sosial media. Memilih alat yang tepat sangat menentukan keberhasilan investigasi, karena setiap tool memiliki kekuatan dan keterbatasan masing-masing.

E. INVESTIGASI INSIDEN KEAMANAN INFORMASI

1. Definisi dan Klasifikasi Insiden

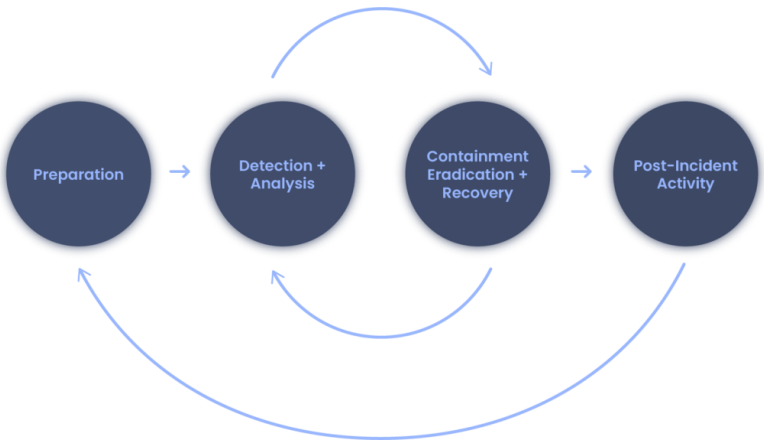
Insiden keamanan informasi didefinisikan sebagai kejadian yang mengganggu atau mengancam integritas, kerahasiaan, dan ketersediaan sistem informasi. Insiden ini dapat berupa serangan

dari pihak luar seperti peretasan dan DDoS, atau dari pihak dalam seperti penyalahgunaan akses oleh karyawan. Tidak semua anomali dikategorikan sebagai insiden, diperlukan evaluasi apakah kejadian tersebut berdampak pada sistem secara signifikan. Deteksi dini terhadap insiden sangat penting untuk menghindari kerusakan yang meluas.

Klasifikasi insiden dilakukan berdasarkan jenis, tingkat keparahan, dan sumber serangan. Misalnya, insiden bisa dikelompokkan sebagai malware infection, unauthorized access, data leakage, atau denial of service. Beberapa organisasi juga menerapkan sistem level (seperti Level 1, 2, dan 3) untuk membedakan insiden kecil hingga kritis. Klasifikasi ini membantu tim tanggap insiden dalam memprioritaskan respon dan mengalokasikan sumber daya secara efektif.

2. Tahapan Investigasi Insiden

   Proses investigasi insiden mengikuti tahapan yang sistematis untuk memastikan tanggapan yang tepat dan terkoordinasi. Model yang paling umum digunakan adalah NIST SP 800-61, yang mencakup enam tahap: preparation, identification, containment, eradication, recovery, dan lessons learned.



Gambar 15. 3. Tahap NIST SP 800-61 (Burgett, 2024)

Tahap preparation meliputi pembuatan kebijakan, pelatihan tim, dan pengadaan alat deteksi. Sementara tahap identification fokus pada mendeteksi adanya insiden dan menentukan dampaknya.

Setelah insiden diidentifikasi, tim akan masuk ke tahap containment, yaitu membatasi penyebaran insiden agar tidak berdampak lebih luas. Lalu dilakukan eradication untuk menghapus penyebab insiden dan recovery untuk memulihkan sistem ke kondisi normal. Tahap terakhir adalah lessons learned, yang bertujuan mengevaluasi proses investigasi agar organisasi lebih siap di masa depan. Pendokumentasian seluruh proses sangat penting agar dapat digunakan sebagai referensi dalam insiden selanjutnya.

3. Integrasi Forensik Digital dalam Proses Respon Insiden

   Forensik digital memainkan peran strategis dalam proses investigasi insiden karena memungkinkan penyelidik memahami secara detail bagaimana serangan terjadi. Melalui analisis log, artefak sistem, dan bukti digital lainnya, forensik membantu mengungkap titik masuk penyerang, metode yang digunakan, serta kerusakan yang ditimbulkan. Proses ini tidak hanya mendukung langkah-langkah teknis, tetapi juga memberi dasar bagi tindakan hukum terhadap pelaku. Integrasi antara tim tanggap insiden dan tim forensik sangat penting untuk efisiensi dan akurasi investigasi.

   Dalam praktiknya, integrasi ini berarti setiap proses respon insiden dari deteksi hingga pemulihan diiringi dengan pelestarian bukti digital. Forensik juga menyediakan informasi penting untuk pembuatan kebijakan keamanan baru dan peningkatan sistem monitoring. Kolaborasi antara tim IT, keamanan siber, dan forensik memperkuat keseluruhan ketahanan organisasi terhadap ancaman digital. Dengan demikian, forensik digital bukan hanya alat reaktif, tapi juga bagian dari strategi proaktif dalam manajemen risiko siber.

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

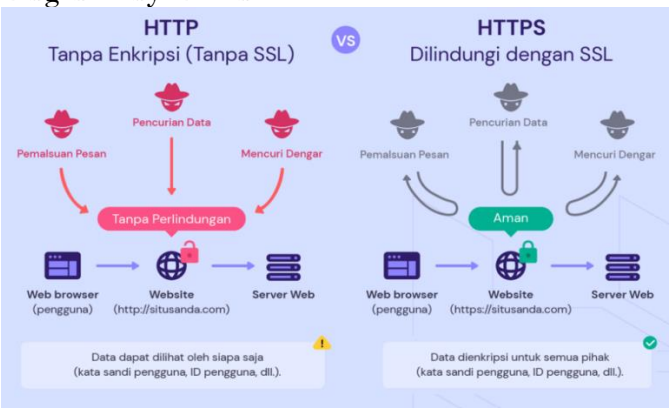
kredit, atau data pribadi lainnya. Serangan MitM biasanya dilakukan dalam beberapa tahap berikut:

1) **WiFi Spoofing (Evil Twin Attack)**
   Penyerang membuat jaringan WiFi palsu yang menyerupai jaringan asli, misalnya "Free Airport WiFi" atau "Coffee Shop WiFi". Ketika pengguna terhubung ke WiFi palsu ini, semua data yang mereka kirimkan melalui jaringan dapat disadap oleh penyerang. Teknik ini sering digunakan di tempat umum seperti bandara, hotel, atau kafe.
2) **ARP Spoofing (Address Resolution Protocol Spoofing)**
   Penyerang mengelabui jaringan dengan berpura-pura menjadi gateway atau router yang sah. Ini memungkinkan mereka untuk mencegat lalu lintas data antara perangkat pengguna dan server. Teknik ini dapat digunakan untuk menguping atau memodifikasi komunikasi tanpa diketahui korban.
3) **DNS Spoofing (Domain Name System Spoofing)**
   Penyerang memanipulasi sistem DNS sehingga pengguna yang mencoba mengakses situs atau aplikasi tertentu akan diarahkan ke situs palsu yang dikendalikan oleh penyerang. Contohnya, pengguna yang ingin login ke aplikasi mobile banking dapat diarahkan ke situs palsu yang menyerupai bank aslinya. Setelah korban memasukkan kredensial login, data tersebut langsung dicuri oleh penyerang.

Untuk melindungi aplikasi mobile dari serangan MitM, langkah-langkah berikut dapat diterapkan:

1) **Gunakan Enkripsi yang Kuat (TLS/SSL)**
   Pastikan semua komunikasi antara aplikasi dan server menggunakan HTTPS dengan protokol TLS 1.2 atau 1.3. TLS (Transport Layer Security) adalah protokol keamanan yang mengenkripsi data sebelum dikirimkan melalui jaringan, sehingga hanya pihak yang memiliki kunci dekripsi yang benar yang dapat membacanya. Tujuan utama TLS Menyembunyikan data yang ditransfer. Caranya yaitu dengan menerapkan proses encoding informasi agar tidak bisa terbaca oleh pihak

ketiga. Serta memastikan keaslian identitas kedua pihak dengan menyediakan sertifikat.



Gambar 16. 1. Perbedaan menggunakan TLS dengan tidak

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

Jika aplikasi masih menggunakan protokol lama seperti TLS 1.0 atau TLS 1.1, maka dapat dianggap tidak aman dan tidak sesuai standar keamanan modern. Dengan TLS 1.2 atau 1.3, data menjadi lebih sulit diubah atau disadap karena terenkripsi dengan algoritma yang lebih aman.

2) **Gunakan VPN saat Menggunakan Jaringan Publik**
VPN (Virtual Private Network) berfungsi dengan mengenkripsi lalu lintas internet dan mengarahkannya melalui server aman sebelum mencapai tujuan akhirnya. Proses ini menyembunyikan alamat IP pengguna dan melindungi data dari penyadapan

Gambar 16. 2. VPN Process

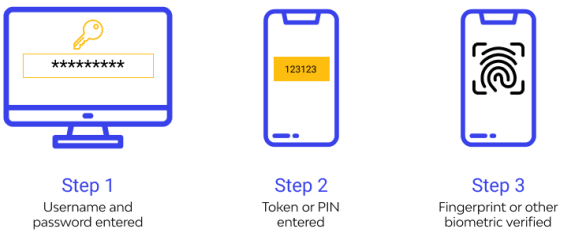
Sumber: Website https://wasiswa.com

Proses kerja VPN secara sederhana:

- Perangkat pengguna mengenkripsi data sebelum dikirim melalui jaringan.
- Data dikirim melalui "terowongan aman" VPN ke server VPN.
- Server VPN meneruskan data ke situs web atau layanan online yang diakses.
- Data yang dikirim kembali ke pengguna juga dienkripsi sebelum diterima.

3) **Gunakan Autentikasi Multifaktor (MFA)**

MFA menambah lapisan keamanan ekstra dengan meminta kode verifikasi tambahan selain kata sandi. Ini membantu mengurangi risiko pencurian akun meskipun kredensial telah dicuri.



Gambar 16. 3. MFA Process

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

Autentikasi multifaktor menggunakan pendekatan terstruktur untuk memverifikasi identitas pengguna. Pendekatan ini mencakup permintaan kredensial verifikasi tambahan, satu demi satu. Untuk kategori yang berbeda, faktor verifikasi beragam. Salah satu proses verifikasi yang paling luas adalah OTP atau kata sandi sekali pakai. OTP biasanya berupa kode 4-8 digit, yang dibagikan kepada pengguna melalui SMS, email, dan panggilan telepon bahkan tambahan *biometric* seperti *fingerprint.*

c) **Injection Attacks**

Serangan *Injection attack* adalah jenis serangan keamanan di mana penyerang menyisipkan kode berbahaya ke dalam aplikasi, dengan tujuan memanipulasi, mencuri, atau merusak data serta mengendalikan sistem target. Serangan ini sering terjadi ketika sebuah aplikasi tidak memvalidasi atau membersihkan input pengguna dengan benar, sehingga penyerang dapat memasukkan skrip atau perintah berbahaya ke dalam aplikasi.

Injection attack dapat mempengaruhi berbagai jenis sistem, termasuk database, server, API, hingga browser web, dan dapat menyebabkan kebocoran informasi sensitif, pengambilalihan akun, atau eksekusi kode berbahaya di perangkat korban.

Berikut adalah beberapa jenis serangan injection yang sering terjadi pada aplikasi mobile dan web:

1) **SQL Injection (SQLi) dan Command Injection**
   Penyerang menyisipkan perintah SQL berbahaya ke dalam input aplikasi untuk memanipulasi database. Dampaknya penyerang dapat mengambil atau mencuri informasi sensitif dari database, menghapus atau mengubah data dalam sistem atau mengakses akun pengguna tanpa otorisasi.
2) **Cross-Site Scripting (XSS)**
   Penyerang menyisipkan skrip berbahaya (biasanya JavaScript) ke dalam halaman web yang dijalankan di browser pengguna lain. Meskipun aplikasi seluler mungkin tidak menampilkan HTML secara langsung seperti peramban web, aplikasi tersebut sering kali mengandalkan tampilan web atau peramban tertanam untuk menampilkan konten dari sumber eksternal. Hal ini membuka peluang terjadinya serangan XSS, karena skrip berbahaya yang dimasukkan ke dalam konten web dapat dijalankan dalam konteks aplikasi seluler, yang berpotensi membahayakan data dan keamanan pengguna.

Serangan seperti SQL Injection (SQLi), Cross-Site Scripting (XSS), dan Command Injection, sering terjadi karena aplikasi tidak melakukan validasi input dengan baik, tidak mengamankan output yang dikirim ke pengguna, atau menyusun kueri database tanpa perlindungan.

1) **Validasi Input**
   Validasi input adalah proses memeriksa, memfilter, dan memastikan bahwa data yang dimasukkan oleh pengguna

aman dan sesuai dengan format yang diharapkan. Dengan melakukan validasi yang ketat, aplikasi dapat mencegah penyerang menyisipkan kode berbahaya ke dalam sistem.

- Hanya mengizinkan karakter atau format yang diperbolehkan. Contoh: Jika hanya angka yang diperbolehkan untuk ID pengguna, maka hanya karakter 0-9 yang diterima.
- Batasi panjang maksimum input untuk mencegah buffer overflow atau injeksi kode panjang.
- Memblokir karakter berbahaya, tetapi sering kali tidak cukup karena metode bypass dapat digunakan oleh penyerang.

```python
from flask import request
import re

def validate_username(username):
    if not re.match("^[a-zA-Z0-9_]{3,20}$", username):
        return False  # Input tidak valid
    return True

user_input = request.form['username']
if validate_username(user_input):
    print("Input Valid")
else:
    print("Input Tidak Valid")
```

Gambar 16. 4. Validasi Inputan

2) Output Encoding

Output encoding adalah teknik untuk mengubah karakter berbahaya menjadi format aman sebelum dikirim ke pengguna, sehingga kode berbahaya tidak akan dieksekusi oleh browser atau sistem.

```
function encodeHTML(str) {
    return str.replace(/&/g, "&amp;")
              .replace(/</g, "&lt;")
              .replace(/>/g, "&gt;")
              .replace(/"/g, "&quot;")
              .replace(/'/g, "&#039;");
}

let user_input = "<script>alert('Hacked!')</script>";
let safe_output = encodeHTML(user_input);
console.log(safe_output);  // Output: &lt;script&gt;alert('Hacked!')&lt;/script&gt;
```

Gambar 16. 5. Output Encoding

3) Parameterized Query

Kueri berparameter adalah teknik di mana input pengguna dipisahkan dari perintah SQL, sehingga data tidak dapat dieksekusi sebagai kode SQL. Mencegah SQL Injection (SQLi), di mana penyerang bisa menyisipkan kode SQL berbahaya ke dalam input.

```
username = input("Masukkan username: ")
password = input("Masukkan password: ")

query = "SELECT * FROM users WHERE username = '" + username + "' AND password = '" + password
cursor.execute(query)  # Rentan terhadap SQL Injection!
```

Gambar 16. 6. Parameterized Query

Praktek keamanan mobile Kebijakan keamanan perangkat seluler harus mencakup aspek berikut:

a) Pendaftaran Perangkat Seluler

- Setiap perangkat seluler yang digunakan untuk mengakses sistem organisasi harus didaftarkan terlebih dahulu.
- Mencatat informasi perangkat seperti IMEI, sistem operasi, dan pengguna yang berwenang.
- Menggunakan sistem Mobile Device Management (MDM) untuk memantau dan

b) Persyaratan untuk Perlindungan Fisik

- Perangkat harus disimpan di tempat yang aman dan tidak boleh ditinggalkan di area publik tanpa pengawasan.

- Gunakan kunci atau loker untuk menyimpan perangkat yang tidak digunakan.
- Saat bepergian, perangkat harus diamankan menggunakan tas atau dompet khusus dengan perlindungan tambahan.

c) Pembatasan Instalasi Perangkat Lunak

- Hanya perangkat lunak yang disetujui oleh organisasi yang boleh diinstal.
- Mencegah pemasangan aplikasi dari sumber tidak resmi yang dapat membawa malware.
- Gunakan daftar aplikasi yang diperbolehkan (whitelisting) untuk mengontrol aplikasi yang bisa diinstal.

d) Persyaratan untuk Versi Perangkat Lunak dan Tambalan Keamanan

- Sistem operasi dan aplikasi harus selalu diperbarui ke versi terbaru.
- Patch keamanan harus diterapkan segera setelah dirilis oleh vendor.
- Mencegah penggunaan perangkat dengan sistem operasi yang sudah tidak didukung.

e) Pembatasan Koneksi ke Layanan Informasi

- Hanya jaringan yang aman (misalnya VPN atau jaringan internal organisasi) yang boleh digunakan untuk mengakses sistem perusahaan.
- Hindari penggunaan Wi-Fi publik tanpa perlindungan enkripsi yang kuat.
- Batasi akses ke layanan cloud yang tidak terverifikasi untuk mencegah kebocoran data.

f) Kontrol Akses

- Gunakan autentikasi multifaktor (MFA) untuk mengakses sistem perusahaan dari perangkat seluler.
- Terapkan kebijakan kata sandi yang kuat dengan enkripsi data.
- Pastikan perangkat terkunci secara otomatis setelah periode tidak aktif tertentu.

g) Teknik Kriptografi

- Enkripsi data yang tersimpan dan yang dikirim melalui perangkat seluler.
- Gunakan enkripsi end-to-end untuk komunikasi sensitif.
- Terapkan sertifikat digital untuk mengamankan koneksi perangkat ke server organisasi.

h) Perlindungan Malware

- Instal perangkat lunak anti-malware yang diperbarui secara berkala.
- Gunakan firewall pada perangkat untuk mencegah akses tidak sah.
- Blokir akses ke situs web atau aplikasi berbahaya.

i) Penonaktifan, Penghapusan, atau Penguncian Jarak Jauh

- Perangkat yang hilang atau dicuri harus dapat dikunci atau dihapus datanya dari jarak jauh.
- Gunakan fitur "Find My Device" atau solusi MDM untuk melacak dan menghapus data pada perangkat yang tidak lagi digunakan.
- Pastikan data bisnis tidak dapat diakses setelah perangkat dinonaktifkan.

j) Cadangan Data (Backup)

- Data penting harus dicadangkan secara berkala ke lokasi yang aman.
- Gunakan layanan cloud yang terenkripsi untuk menyimpan data cadangan.
- Pastikan perangkat tetap dapat mencadangkan data meskipun tidak selalu terhubung ke jaringan perusahaan.

k) Penggunaan Layanan Web dan Aplikasi Web

- Batasi akses aplikasi web hanya melalui koneksi yang aman.
- Gunakan autentikasi berbasis token atau sertifikat digital untuk mengakses layanan web.

- Pastikan browser yang digunakan telah diperbarui dan memiliki proteksi keamanan aktif.

l) Perlindungan Perangkat Seluler di Lingkungan Tidak Terlindungi

- Saat menggunakan perangkat di tempat umum atau ruang rapat, hindari mengakses informasi sensitif tanpa perlindungan layar.
- Gunakan VPN saat mengakses jaringan perusahaan dari lokasi eksternal.
- Terapkan mode privasi untuk mencegah rekaman audio atau video tanpa izin.

m) Perlindungan Fisik terhadap Pencurian

- Jangan meninggalkan perangkat di dalam kendaraan atau tempat umum tanpa pengawasan.
- Gunakan pengamanan tambahan seperti pelacak GPS atau alarm keamanan pada perangkat seluler.
- Terapkan kebijakan pelaporan kehilangan perangkat segera setelah terjadi insiden.

n) Pelatihan dan Kesadaran Keamanan bagi Pengguna Perangkat Seluler

- Lakukan pelatihan reguler bagi pengguna tentang cara mengamankan perangkat seluler mereka.
- Sosialisasikan risiko keamanan dan teknik mitigasi kepada karyawan.
- Pastikan pengguna memahami kebijakan dan prosedur terkait keamanan perangkat seluler.

B. BRING YOUR OWN DEVICE (BYOD)

Kebijakan yang mengatur penggunaan perangkat pribadi oleh karyawan, seperti laptop, smartphone, atau tablet, dalam lingkungan kerja semakin banyak diterapkan seiring dengan pesatnya perkembangan teknologi. Pendekatan ini memungkinkan karyawan bekerja dengan lebih fleksibel dan meningkatkan produktivitas karena mereka dapat mengakses data serta sistem perusahaan dari mana saja. Namun, untuk memastikan keamanan informasi perusahaan, diperlukan penerapan

kebijakan serta teknologi perlindungan yang ketat. Hal ini mencakup penggunaan enkripsi data, pengelolaan akses yang ketat, serta penerapan langkah-langkah keamanan tambahan untuk menjaga integritas informasi yang diakses melalui perangkat pribadi.

Daya tarik BYOD tidak dapat disangkal. Karyawan menikmati kebebasan untuk menggunakan perangkat yang familiar dan mudah digunakan, yang tentunya dapat meningkatkan kenyamanan dan efisiensi mereka. Sementara itu, perusahaan dapat menghemat biaya yang signifikan dalam pengadaan dan pemeliharaan perangkat keras, sekaligus mengembangkan tenaga kerja yang lebih terlibat dan fleksibel.

Namun, seiring dengan meningkatnya adopsi BYOD**,** masalah keamanan juga meningkat. Misalnya, terkait kebocoran data, akses tidak sah, dan infeksi malware. Sebuah Laporan dari Bitglass mengungkapkan bahwa 82% responden dari berbagai perusahaan mengizinkan karyawan menggunakan perangkat pribadi untuk bekerja.

Sayangnya, banyak organisasi masih kekurangan langkah-langkah yang memadai untuk melindungi data perusahaan dalam ekosistem BYOD**.** Artikel ini akan membantu Anda menjawab tantangan dan menawarkan solusi untuk fenomena ini.

Selain itu, kebijakan BYOD (Bring Your Own Device) juga perlu menetapkan batasan terkait penggunaan perangkat, seperti pembatasan aplikasi yang dapat diinstal, kewajiban memasang perangkat lunak keamanan, serta aturan pemisahan antara data pribadi dan data bisnis. Dengan langkah-langkah ini, perusahaan dapat memanfaatkan fleksibilitas BYOD tanpa mengorbankan keamanan sistem dan data mereka. Salah satu tantangan terbesar dalam implementasi BYOD adalah penggunaan aplikasi pribadi yang tidak terkontrol. Aplikasi yang diunduh karyawan di perangkat mereka mungkin tidak disesuaikan dengan standar keamanan perusahaan. Hal ini membuka celah bagi akses tidak sah ke data perusahaan, yang dapat mengakibatkan kebocoran informasi penting. Kebutuhan untuk memantau dan mengelola aplikasi ini menjadi sangat penting.

Keamanan Perangkat Seluler Milik Pribadi (BYOD - Bring Your Own Device)

Jika organisasi mengizinkan penggunaan perangkat pribadi untuk keperluan bisnis, langkah-langkah berikut harus diterapkan:

a) Pemisahan Penggunaan Perangkat untuk Keperluan Pribadi dan Bisnis
    - Gunakan solusi containerization untuk memisahkan data bisnis dari data pribadi.
    - Terapkan kebijakan bahwa data bisnis harus tetap terenkripsi dan hanya bisa diakses melalui aplikasi yang disetujui.
b) Persyaratan Akses dan Penghapusan Data Jarak Jauh
    - Pengguna harus menandatangani perjanjian yang mengizinkan organisasi untuk menghapus data bisnis dari perangkat mereka jika diperlukan.
    - Kebijakan ini harus mematuhi hukum privasi yang berlaku di masing-masing negara.
c) Tanggung Jawab Pengguna Perangkat
   Setiap pengguna yang menggunakan perangkat titik akhir harus mematuhi kebijakan keamanan dan bertanggung jawab atas perlindungan perangkatnya, termasuk:
    - Menutup sesi dan logout setelah selesai bekerja.
    - Mengamankan perangkat dengan kata sandi atau metode autentikasi lainnya.
    - Tidak meninggalkan perangkat yang menyimpan data bisnis tanpa pengawasan.
    - Menggunakan perangkat dengan hati-hati di tempat umum untuk menghindari pengintaian (shoulder surfing).
    - Melindungi perangkat dari pencurian, terutama saat bepergian atau di tempat umum.
d) Jika perangkat hilang atau dicuri, pengguna harus segera melaporkannya sesuai dengan prosedur organisasi.
e) Diwajibkan untuk melakukan backup data perusahaan pada penyimpanan berbasis awan/online milik perusahaan untuk mencegah terjadinya kehilangan data
f) Dilarang meninggalkan laptop tanpa pengawasan. Selalu lakukan penguncian laptop saat tidak digunakan
g) Menonaktifkan *removable drive* untuk menghindari aktivitas pemindahan data perusahaan tanpa izin
h) Pembaruan perangkat lunak secara rutin untuk mendapatkan tingkat keamanan yang lebih baik seperti menggunakan antivirus.

i) Tidak diperbolehkan untuk meminjamkan laptop kepada pihak eksternal perusahaan. Peminjaman atau penggunaan laptop kepada pihak internal perusahaan harus dengan persetujuan atasan langsung.
j) Tidak diperbolehkan untuk mengganti dan membongkar perangkat keras laptop tanpa sepengetahuan dan persetujuan

Keuntungan BYOD

Dirangkum dari berbagai sumber, keuntungan BYOD meliputi:

- **Peningkatan produktivitas:** dengan BYOD, karyawan bisa bekerja dari mana pun dan kapan pun, sehingga meningkatkan fleksibilitas dan produktivitas. Mereka bisa langsung menggunakan perangkat pribadi yang sudah familiar, sehingga mengurangi waktu yang diperlukan untuk beradaptasi dengan perangkat baru.
- **Penghematan biaya**: BYOD mengurangi biaya yang harus dikeluarkan perusahaan untuk menyediakan perangkat kerja bagi karyawan.
- **Kepuasan karyawan**: dengan menggunakan perangkat pribadi, karyawan merasa lebih nyaman dan percaya diri. Ini juga memungkinkan mereka menyesuaikan perangkat dengan kebutuhan dan preferensi masing-masing.
- **Aksesibilitas data yang lebih baik**: BYOD memudahkan karyawan mengakses data perusahaan dari mana pun, sehingga kolaborasi lebih mudah dan respons lebih cepat terhadap kebutuhan bisnis. Hal ini juga memfasilitasi kerja *remote* yang semakin populer.
- **Inovasi teknologi**: perusahaan dapat memanfaatkan inovasi dan tren terbaru dalam teknologi melalui perangkat yang dimiliki karyawan. Ini membantu bisnis tetap *up-to-date* dengan perkembangan teknologi, tanpa harus berinvestasi besar dalam *hardware* baru.

Kekurangan BYOD

Selain kelebihannya, BYOD memiliki beberapa kekurangan:

- **Keamanan data**: salah satu tantangan utama dari kebijakan BYOD adalah risiko keamanan data. Perangkat pribadi bisa menjadi titik lemah dalam sistem keamanan perusahaan, memungkinkan akses tidak sah, pencurian data, atau *cyber attack* jika perangkat tersebut tidak dilindungi dengan baik.
- **Pengelolaan perangkat**: dengan BYOD, perusahaan menghadapi tantangan dalam mengelola berbagai perangkat dengan konfigurasi yang berbeda. Ini bisa menyulitkan pengaturan dan pemantauan, terutama jika perangkat tersebut memiliki sistem operasi atau versi aplikasi berbeda.
- **Privasi karyawan**: kebijakan BYOD dapat memicu kekhawatiran privasi karyawan, karena perusahaan perlu mengakses atau memantau perangkat pribadi mereka untuk alasan keamanan. Ini bisa menimbulkan konflik antara kebutuhan perusahaan akan keamanan dan privasi individu karyawan.
- **Kesulitan teknis**: dukungan teknis bisa menjadi masalah dalam kebijakan BYOD, terutama ketika karyawan menggunakan perangkat yang berbeda. Perusahaan kemungkinan perlu memperluas dukungan teknis mereka untuk mencakup berbagai jenis perangkat dan aplikasi, yang bisa memakan waktu dan sumber daya.
- **Kesulitan dalam memisahkan pekerjaan dan kehidupan pribadi**: penggunaan perangkat pribadi untuk pekerjaan bisa mengaburkan batas antara kehidupan pribadi dan pekerjaan. Hal ini bisa menyebabkan karyawan kesulitan untuk beristirahat dari pekerjaan, yang pada akhirnya memengaruhi kesejahteraan dan keseimbangan hidup

C. RANGKUMAN

Keamanan aplikasi mobile penting untuk melindungi data pengguna dari ancaman seperti malware (Trojan, Spyware, Ransomware), serangan Man-in-the-Middle (MitM), dan Injection Attacks (SQL Injection, XSS). Pencegahan meliputi mengunduh aplikasi dari sumber resmi, menggunakan enkripsi TLS/SSL, VPN, autentikasi multifaktor, dan validasi input yang baik.

Kebijakan BYOD memungkinkan karyawan menggunakan perangkat pribadi untuk bekerja, meningkatkan fleksibilitas dan produktivitas. Namun, ini menambah risiko keamanan data. Langkah pencegahan mencakup pemisahan penggunaan pribadi dan bisnis, pengelolaan akses, serta penguncian dan pengawasan perangkat. Keuntungan BYOD termasuk penghematan biaya dan kepuasan karyawan, sementara kekurangannya adalah risiko keamanan dan pengelolaan perangkat yang rumit.

Secara keseluruhan, kebijakan dan teknologi yang tepat diperlukan untuk menjaga keamanan data dan perangkat.

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

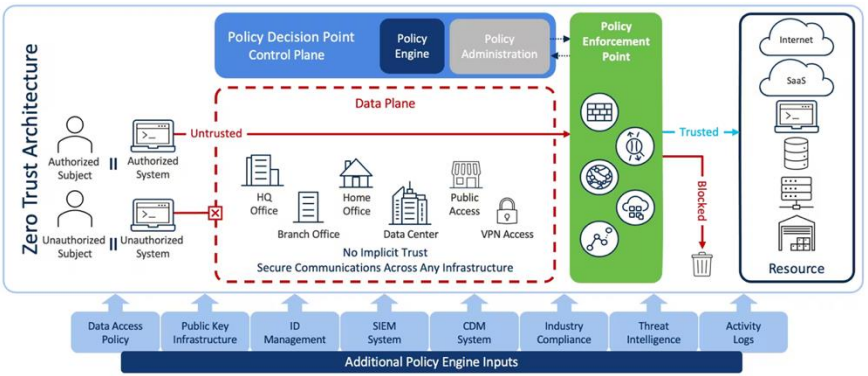
c. Adversarial Attacks
Penyerang dapat menggunakan teknik adversarial machine learning untuk menyisipkan input yang dimodifikasi secara halus agar dapat mengelabui model AI, membuatnya gagal dalam mengidentifikasi serangan dengan benar

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.

C. PENERAPAN ARSITEKTUR ZERO TRUST (ZERO TRUST ARCHITECTURE – ZTA)

Model keamanan tradisional yang berfokus pada perimeter jaringan ("trust but verify") kini dianggap tidak lagi memadai untuk mengamankan sistem informasi modern. Perubahan besar seperti migrasi ke cloud, mobilitas karyawan, peningkatan penggunaan perangkat BYOD (Bring Your Own Device), serta tingginya risiko dari *insider threats* menuntut adanya pendekatan baru yang lebih adaptif dan menyeluruh. Di sinilah konsep Zero Trust hadir sebagai paradigma yang merevolusi cara organisasi memandang dan menerapkan keamanan.

Arsitektur Zero Trust (ZTA) menghilangkan anggapan bahwa sistem internal selalu aman. Dengan prinsip "never trust, always verify", setiap entitas — baik pengguna, perangkat, maupun aplikasi — harus melalui proses autentikasi dan otorisasi yang ketat, tanpa memandang lokasi geografis atau posisi dalam jaringan. Konsep ini menekankan keamanan berbasis identitas, verifikasi dinamis, dan segmentasi mikro, yang seluruhnya sangat relevan di era digital dan cloud-native saat ini.



Gambar 17. 1. Arsitektur Zero Trust (ZTA)

Sumber: https://accuknox.com/blog/zero-trust-architechture

1. Prinsip-Prinsip Dasar Arsitektur Zero Trust

Berikut adalah prinsip-prinsip utama dari ZTA menurut National Institute of Standards and Technology (NIST SP 800-207):

a. Verifikasi secara terus-menerus (Continuous Verification): Setiap permintaan akses harus diautentikasi dan diotorisasi secara dinamis berdasarkan konteks (lokasi, perangkat, waktu, dll).
b. Minimalkan hak akses (Least Privilege Access): Pengguna atau perangkat hanya diberikan akses minimum yang diperlukan.
c. Asumsi pelanggaran (Assume Breach): Sistem harus dirancang dengan asumsi bahwa ancaman sudah ada di dalam jaringan.
d. Segmentasi Mikro (Microsegmentation): Memecah jaringan menjadi bagian-bagian kecil untuk membatasi pergerakan lateral penyerang.
b. Pemantauan dan logging terus-menerus: Seluruh aktivitas harus dicatat dan dianalisis untuk mendeteksi anomali atau pelanggaran.

2. Komponen Utama dalam Implementasi ZTA

Zero Trust Architecture (ZTA) merupakan paradigma keamanan modern yang menolak asumsi kepercayaan implisit dalam sistem informasi. Alih-alih mempercayai perangkat atau pengguna hanya karena mereka berada dalam jaringan internal, ZTA mengharuskan verifikasi secara eksplisit terhadap setiap entitas yang mengakses sumber daya digital, kapan pun dan dari mana pun. Berikut adalah komponen utama dalam implementasi ZTA :

a. Identitas sebagai Perimeter Baru
   Dalam konteks Zero Trust, identitas — baik manusia (user identity) maupun mesin (machine identity) — menggantikan posisi perimeter jaringan sebagai lapisan pertahanan utama. Hal ini mencerminkan pergeseran dari "network-based perimeter" ke "identity-based perimeter".
b. Kebijakan Berbasis Atribut (Attribute-Based Access Control / ABAC)
   Zero Trust menekankan pentingnya kebijakan akses yang fleksibel dan kontekstual. ABAC memungkinkan kontrol akses tidak hanya berdasarkan identitas pengguna, tetapi juga berdasarkan sejumlah atribut yang relevan.
c. Penggunaan Proxy atau Gateway Zero Trust
   Untuk menjamin bahwa seluruh trafik dipantau dan dikendalikan, ZTA mengandalkan komponen seperti proxy atau gateway yang menjadi titik inspeksi utama terhadap semua lalu lintas data yang masuk dan keluar.
d. Endpoint Security dan Posture Check

Dalam ZTA, setiap perangkat yang ingin mengakses sumber daya harus melalui proses evaluasi kondisi keamanan atau *posture assessment*. Sistem akan memeriksa apakah perangkat telah mendapatkan update keamanan terbaru, memiliki antivirus aktif, firewall menyala, serta tidak memiliki kerentanan yang dapat dieksploitasi.

3. Arsitektur Referensi dan Model Implementasi

NIST (2020) melalui dokumen SP 800-207 menyediakan referensi arsitektur ZTA. Model ini terdiri dari komponen berikut:

a. Policy Enforcement Point (PEP): Komponen yang mengizinkan atau menolak akses berdasarkan keputusan kebijakan.
b. Policy Decision Point (PDP): Tempat di mana keputusan akses dibuat berdasarkan informasi dari sumber data.
c. Policy Administrator (PA): Bertugas menyiapkan dan mengelola kebijakan yang diterapkan di PDP.
d. Trust Algorithm Engine: Mesin yang menghitung skor kepercayaan berdasarkan konteks permintaan.

4. Studi Kasus Implementasi Zero Trust

Berikut adalah beberapa studi kasus Implementasi Zero Trus yang sudah di lakukan :

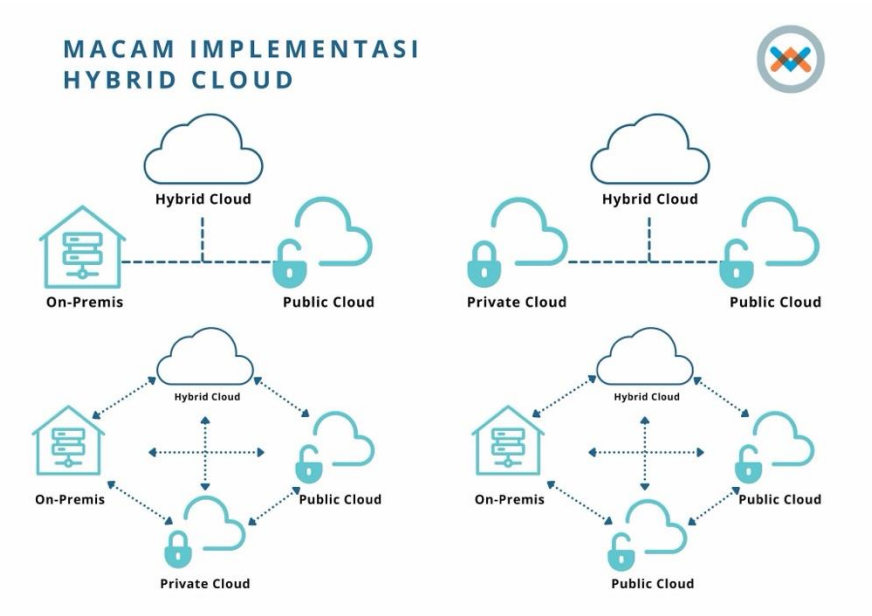
a. Google BeyondCorp: Salah satu pionir implementasi Zero Trust sejak 2011, memungkinkan karyawan mengakses aplikasi perusahaan dari jaringan apa pun tanpa VPN.
b. Microsoft Zero Trust Framework: Menerapkan ZTA pada skala besar dengan menggabungkan Azure AD, Microsoft Defender, dan Endpoint Manager.
c. US Department of Defense (DoD): Meluncurkan strategi Zero Trust pada 2021 sebagai kerangka kerja keamanan masa depan.

D. KEAMANAN DALAM ARSITEKTUR CLOUD DAN HYBRID

Transformasi digital yang masif telah mendorong organisasi di berbagai sektor untuk mengadopsi layanan cloud sebagai bagian integral dari infrastruktur teknologi informasi (TI) mereka. Layanan cloud tidak hanya menawarkan skalabilitas dan efisiensi operasional, tetapi juga memungkinkan organisasi untuk dengan cepat menerapkan dan memperluas aplikasi serta layanan tanpa investasi besar pada perangkat keras. Model cloud computing seperti public cloud, private cloud, dan

hybrid cloud memungkinkan fleksibilitas dalam pengelolaan sumber daya dan penyimpanan data.

Namun, adopsi arsitektur cloud membawa serta kompleksitas baru dalam pengelolaan keamanan. Perpindahan dari sistem on-premise ke lingkungan cloud mengharuskan organisasi menyesuaikan pendekatan keamanan mereka, karena model tanggung jawab bersama (shared responsibility model) mengharuskan pelanggan dan penyedia layanan berbagi tanggung jawab terhadap keamanan data dan infrastruktur.



Gambar 17. 2. Implementasi Hybrid Cloud

Sumber: https://www.wowrack.com/id-id/blog/cloud-id/apa-saja-tipe-arsitektur-hybrid-cloud-dan-implementasinya/

1. Tantangan Keamanan dalam Arsitektur Cloud dan Hybrid

Berikut beberapa tantangan yang dihadapi dalam Arsitektur Cloud dan Hybrid :

a. Konfigurasi yang Salah (Misconfiguration)

Salah satu penyebab utama insiden keamanan di cloud adalah konfigurasi yang tidak tepat dari layanan, seperti bucket penyimpanan publik atau aturan firewall yang terbuka lebar. Hal ini membuka celah bagi akses tidak sah dan kebocoran data.

b. Kehilangan Visibilitas dan Kontrol atas Data
Dalam lingkungan cloud, data sering kali tersebar di berbagai lokasi dan wilayah geografis, membuat organisasi kesulitan dalam memantau akses dan penggunaan data secara menyeluruh, terutama dalam konteks regulasi seperti GDPR atau UU Perlindungan Data Pribadi.

c. Ancaman dari Pihak Ketiga
Ketergantungan pada penyedia layanan cloud, integrator, atau vendor pihak ketiga memperluas permukaan serangan. Ancaman tidak hanya berasal dari luar, tetapi juga dari dalam, termasuk insider threat dari staf vendor.

d. Kompleksitas Integrasi Hybrid Cloud
Dalam arsitektur hybrid, organisasi menggabungkan lingkungan lokal (on-premise) dengan layanan cloud. Ini menciptakan tantangan dalam menyelaraskan kebijakan keamanan, mengelola identitas pengguna lintas lingkungan, serta memastikan enkripsi dan pemantauan yang konsisten.

2. Pendekatan Keamanan Masa Depan untuk Cloud dan Hybrid

Menghadapi tantangan tersebut, pendekatan keamanan cloud yang modern harus:

a. Berbasis Cloud-Native Security
Mengintegrasikan kontrol keamanan langsung ke dalam arsitektur cloud, termasuk melalui container security, Kubernetes security, dan serverless function protection. Ini memungkinkan sistem untuk bersifat otomatis, elastis, dan mampu beradaptasi dengan lingkungan cloud yang dinamis.

b. Cloud Access Security Broker (CASB)
CASB bertindak sebagai jembatan antara pengguna dan penyedia layanan cloud dengan memberikan visibilitas, pengendalian kebijakan, dan perlindungan data dalam penggunaan layanan SaaS, PaaS, dan IaaS. CASB juga memungkinkan organisasi mendeteksi anomali, mencegah kebocoran data, dan memenuhi kepatuhan.

c. Cloud Workload Protection Platforms (CWPP)
CWPP menyediakan perlindungan untuk beban kerja yang dijalankan di lingkungan cloud, termasuk virtual machine, container,

dan fungsi serverless. Fitur-fitur seperti anti-malware, vulnerability scanning, dan runtime protection menjadi bagian penting dalam mekanisme perlindungan beban kerja modern.

d. Enkripsi End-to-End
Untuk menjaga kerahasiaan dan integritas data, enkripsi data dalam proses, saat transit, dan saat disimpan (at-rest) menjadi keharusan. Dalam konteks hybrid, organisasi harus memastikan bahwa kebijakan enkripsi dapat diterapkan konsisten di semua lingkungan.

E. OTOMATISASI DAN ORKESTRASI DALAM RESPONS INSIDEN.

Di era digital saat ini, jumlah insiden keamanan yang terjadi dalam suatu organisasi meningkat secara eksponensial. Mulai dari phishing, malware, hingga advanced persistent threats (APT), tim keamanan siber menghadapi beban kerja yang semakin besar dan kompleks. Dalam lingkungan seperti ini, kecepatan dan akurasi dalam mendeteksi, merespons, serta memitigasi ancaman menjadi kunci utama untuk mempertahankan keberlangsungan layanan dan menjaga kepercayaan pemangku kepentingan.

Namun, banyak organisasi masih bergantung pada proses manual dalam penanganan insiden, yang tidak hanya memakan waktu tetapi juga rawan kesalahan. Hal ini diperparah dengan keterbatasan sumber daya manusia di pusat operasi keamanan (Security Operations Center – SOC), yang mengakibatkan keterlambatan dalam respons dan eskalasi insiden. Untuk menjawab tantangan ini, pendekatan otomatisasi dan orkestrasi dalam respons insiden telah muncul sebagai solusi strategis yang krusial.

1. Konsep Otomatisasi dan Orkestrasi

Otomatisasi mengacu pada penggunaan sistem atau teknologi untuk menjalankan tugas-tugas tertentu secara mandiri tanpa intervensi manusia. Sementara itu, orkestrasi merujuk pada pengelolaan dan pengoordinasian berbagai proses serta alat keamanan yang berbeda agar bekerja secara terpadu dan efisien dalam satu alur kerja.

Kombinasi dari keduanya diimplementasikan melalui platform SOAR (Security Orchestration, Automation, and Response), yang merupakan teknologi canggih yang dirancang untuk membantu tim SOC dalam mengelola siklus hidup insiden secara lebih efisien.

2. Fungsi dan Manfaat SOAR dalam Respons Insiden

Berikut adalah beberapa Fungsi dan Manfaat dari SOAR (Security Orchestration, Automation, and Response) dalam response insiden :

a. Integrasi Alat Keamanan
   SOAR mampu mengintegrasikan berbagai komponen seperti SIEM (Security Information and Event Management), endpoint detection and response (EDR), threat intelligence platform, serta firewall dan email gateway ke dalam satu sistem pusat.
b. Otomatisasi Proses Respons
   Tindakan seperti isolasi perangkat, penghapusan file berbahaya, pemblokiran alamat IP, dan pembuatan tiket insiden dapat diotomatisasi, mengurangi waktu tanggap dan menghindari kelalaian manusia.
c. Orkestrasi Alur Kerja
   SOAR menyederhanakan dan menyelaraskan alur kerja antar tim keamanan dengan mendefinisikan playbook atau runbook untuk berbagai jenis insiden, yang menjamin konsistensi dalam penanganan insiden.
d. Peningkatan Efisiensi Tim SOC
   Dengan mengurangi beban kerja manual, tim SOC dapat lebih fokus pada analisis strategis dan investigasi terhadap insiden tingkat lanjut, bukan sekadar menangani volume alert yang tinggi.
e. Pengambilan Keputusan yang Lebih Cepat dan Akurat
   Dengan data yang sudah dikorelasikan dan playbook yang terotomatisasi, SOAR mendukung pengambilan keputusan secara cepat berdasarkan konteks yang lengkap dan akurat.

F. PENGGUNAAN BLOCKCHAIN UNTUK INTEGRITAS DAN OTENTIKASI.

Dalam ekosistem digital modern, salah satu pilar utama dari keamanan informasi adalah menjaga integritas data serta memastikan otentikasi identitas yang dapat diandalkan. Sistem tradisional cenderung bergantung pada model tersentralisasi, seperti server pusat atau otoritas sertifikat digital, yang pada dasarnya menciptakan titik kepercayaan tunggal (single point of trust). Ketika titik ini disusupi atau gagal, maka seluruh sistem bisa terancam. Hal ini menjadi kerentanan besar terutama dalam sistem berskala besar atau lintas entitas.

Sebagai respons terhadap tantangan tersebut, teknologi blockchain muncul sebagai alternatif yang menjanjikan. Awalnya dikenal sebagai tulang punggung dari mata uang kripto seperti Bitcoin dan Ethereum, blockchain kini berkembang menjadi platform yang dapat diandalkan

untuk memastikan integritas, transparansi, dan otentikasi dalam berbagai konteks keamanan informasi.

1. Karakteristik Keamanan Blockchain

Teknologi blockchain memiliki beberapa karakteristik yang membuatnya ideal untuk digunakan dalam sistem keamanan informasi:

a. Desentralisasi
   Tidak ada entitas tunggal yang mengendalikan seluruh sistem, sehingga mengurangi risiko sentralisasi dan kerentanan tunggal.
b. Immutability (Ketidakbisaan Diubah)
   Data yang sudah tercatat dalam blok akan sangat sulit untuk diubah tanpa konsensus dari jaringan, menjamin integritas data.
c. Transparansi dan Auditabilitas
   Seluruh aktivitas yang tercatat di blockchain dapat diaudit kapan saja, meningkatkan akuntabilitas.
d. Kriptografi Tingkat Tinggi
   Seluruh transaksi dan identitas dalam blockchain dilindungi oleh algoritma kriptografi canggih yang menjamin otentikasi dan kerahasiaan.

2. Aplikasi Blockchain dalam Keamanan Informasi

Berikut beberapa aplikasi Blockchain dalam Keamanan Informasi, antara lain :

a. Log Aktivitas dan Audit Trail
   Blockchain dapat digunakan untuk mencatat log aktivitas sistem secara real-time dan tidak dapat diubah, sehingga mempermudah proses audit serta mendeteksi potensi manipulasi atau pelanggaran kebijakan.
b. Digital Identity Management (Identitas Terdesentralisasi)
   Dengan pendekatan Decentralized Identifiers (DIDs) dan Verifiable Credentials (VCs), pengguna dapat mengelola identitas digitalnya secara mandiri tanpa bergantung pada otoritas pusat, sehingga meningkatkan privasi dan keamanan.
c. Verifikasi Keaslian Dokumen
   Blockchain dapat digunakan untuk menyimpan hash dari dokumen resmi, ijazah, kontrak, atau dokumen penting lainnya untuk memastikan keasliannya. Siapa pun dapat memverifikasi dokumen tersebut tanpa harus memiliki akses langsung ke isinya.
d. Smart Contracts untuk Kebijakan Keamanan

Kontrak pintar dapat digunakan untuk mengotomatiskan kontrol keamanan seperti manajemen hak akses, persetujuan transaksi, atau penegakan kebijakan tertentu secara aman dan dapat diaudit.

3. Keunggulan dan Nilai Tambah

Penggunaan blockchain dalam keamanan informasi menawarkan keunggulan signifikan dalam memastikan integritas dan otentikasi data melalui mekanisme yang desentralistik, transparan, dan tidak dapat diubah. Teknologi ini menghilangkan kebutuhan akan otoritas pusat, sehingga meminimalkan risiko manipulasi atau kegagalan sistem tunggal. Selain itu, integrasi smart contract memungkinkan otomasi kebijakan keamanan yang lebih aman dan efisien. Berikut adalah beberapa keunggulan dan nilai tambah yang ditawarkan oleh penerapan blockchain dalam konteks keamanan sistem informasi :

a. Meningkatkan Kepercayaan Antar Entitas, Dalam sistem lintas organisasi, blockchain mengurangi kebutuhan terhadap perantara dan membangun kepercayaan berbasis teknologi.
b. Mencegah Manipulasi, Tidak memungkinkan pihak tertentu untuk mengubah catatan tanpa konsensus, sangat cocok untuk data sensitif.
c. Mendukung Kepatuhan Regulasi, Log yang transparan dan tidak berubah memudahkan organisasi memenuhi standar keamanan dan audit seperti GDPR, HIPAA, dan ISO 27001.

G. KEAMANAN PERANGKAT IOT DAN SISTEM SIBER-FISIK.

Perkembangan teknologi Internet of Things (IoT) dan Sistem Siber-Fisik (CPS) telah membawa transformasi besar dalam berbagai sektor industri dan kehidupan sehari-hari. Dari smart home, sistem pengelolaan lalu lintas, pabrik berbasis otomasi (Industry 4.0), hingga perangkat medis yang terhubung, integrasi antara dunia fisik dan digital semakin tak terelakkan. Menurut laporan oleh Statista (2023), jumlah perangkat IoT yang terkoneksi secara global telah melampaui 15 miliar unit dan diprediksi mencapai lebih dari 29 miliar pada tahun 2030.

Namun, pertumbuhan eksponensial ini tidak diiringi dengan kesiapan sistem keamanan yang memadai. Banyak perangkat IoT dirancang untuk efisiensi biaya dan daya rendah, sehingga produsen sering kali mengabaikan lapisan keamanan seperti enkripsi data, pembaruan firmware otomatis, serta pengelolaan identitas dan otentikasi yang kuat. Hal ini menciptakan "attack surface" yang sangat luas dan kompleks, di mana satu titik celah saja dapat dimanfaatkan untuk mengakses jaringan yang lebih luas.

Lebih lanjut, ketika sistem ini terhubung dengan CPS yang mengontrol proses fisik secara real-time—seperti katup pipa industri, aktuator pada kendaraan otonom, atau alat pacu jantung digital—maka pelanggaran keamanan tidak hanya berdampak pada data, tetapi juga berisiko terhadap keselamatan jiwa manusia dan stabilitas operasional.

1. Tantangan Utama dalam Keamanan IoT dan CPS

Meskipun Internet of Things (IoT) dan sistem siber-fisik (Cyber-Physical Systems/CPS) memberikan manfaat besar dalam otomatisasi, efisiensi, dan konektivitas lintas sektor, keduanya juga menghadirkan risiko keamanan yang kompleks. Banyak perangkat IoT dirancang dengan kapabilitas komputasi terbatas dan tidak dilengkapi dengan mekanisme keamanan yang memadai, sementara CPS mengintegrasikan proses digital dan fisik yang rawan terhadap serangan siber berdampak langsung pada keselamatan dan operasional. Kurangnya standar keamanan universal, keterbatasan dalam pembaruan perangkat lunak, serta lemahnya autentikasi menjadi persoalan yang sering ditemukan. Berikut beberapa tantangan utama dalam keamanan IoT dan CPS:

a. Sumber Daya Terbatas pada Perangkat IoT
   Perangkat IoT umumnya memiliki CPU dan memori terbatas, sehingga sulit untuk menjalankan algoritma keamanan kompleks seperti enkripsi tingkat tinggi atau proteksi berbasis AI.
b. Kurangnya Standar Keamanan Global
   Tidak ada standar universal untuk keamanan perangkat IoT. Setiap produsen cenderung menggunakan protokol dan sistem sendiri-sendiri yang tidak selalu kompatibel dan aman.
c. Tidak Adanya Pembaruan (Firmware Update) yang Konsisten
   Banyak perangkat tidak mendukung pembaruan firmware otomatis, sehingga ketika ada celah keamanan yang ditemukan, perangkat tersebut tetap rentan sepanjang masa pakainya.
d. Koneksi Langsung ke Dunia Fisik
   CPS memiliki konsekuensi langsung terhadap realitas fisik, sehingga serangan terhadap sistem ini bisa menyebabkan kecelakaan kerja, gangguan transportasi, atau bahkan bencana industri.
e. Ketiadaan Segmentasi Jaringan
   Banyak sistem IoT terhubung langsung ke jaringan utama tanpa segmentasi, membuat seluruh sistem rentan jika satu perangkat disusupi.

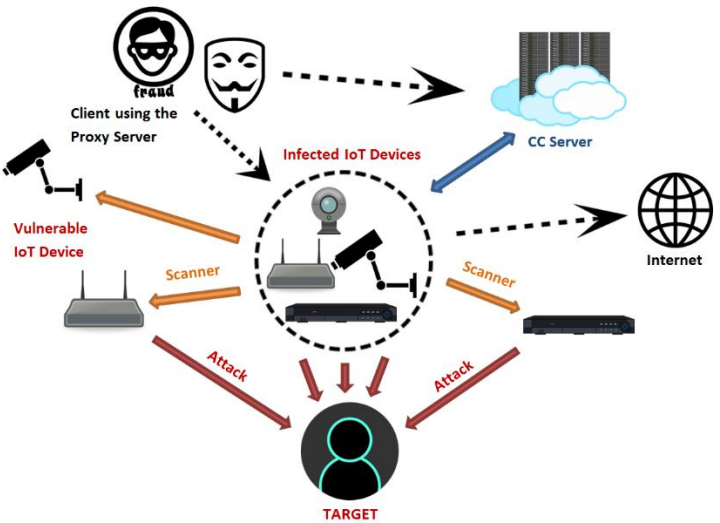
2. Komponen Kritis dalam Keamanan IoT dan CPS

Untuk menjawab tantangan tersebut, pendekatan keamanan terhadap IoT dan CPS harus bersifat **end-to-end** dan menyentuh seluruh siklus hidup perangkat serta jaringan. Berikut adalah beberapa komponen kunci:

a. Otentikasi dan Manajemen Identitas Perangkat
   Setiap perangkat harus memiliki identitas digital yang unik dan dapat diverifikasi agar tidak terjadi spoofing atau pemalsuan perangkat.
b. Enkripsi Data dan Komunikasi Aman
   Data yang dikirim antar perangkat atau ke cloud harus dienkripsi secara menyeluruh untuk mencegah penyadapan (sniffing) dan manipulasi data.
c. Pembaruan Firmware dan Patch Otomatis
   Sistem harus mendukung pembaruan keamanan jarak jauh (Over-The-Air Updates) untuk menutup celah kerentanan secara berkala.
d. Segmentasi Jaringan dan Zero Trust untuk IoT
   Perangkat IoT sebaiknya tidak berada di jaringan yang sama dengan aset utama organisasi. Segmentasi dan penggunaan prinsip Zero Trust akan membatasi penyebaran serangan.
e. Deteksi Anomali dan Pemantauan Real-Time
   Penggunaan machine learning atau IDS (Intrusion Detection System) untuk mendeteksi perilaku abnormal dari perangkat yang bisa mengindikasikan compromise.
f. Hardening Sistem dan Secure Boot
   Perangkat harus dirancang dengan sistem operasi yang aman (minimal attack surface) serta hanya bisa melakukan boot dari firmware yang terverifikasi.

3. Contoh Kasus Nyata

Salah satu kasus paling terkenal adalah **serangan Mirai botnet (2016)**, yang mengeksploitasi ribuan perangkat IoT seperti kamera CCTV dan router untuk meluncurkan serangan DDoS besar-besaran terhadap penyedia DNS Dyn, yang akhirnya melumpuhkan akses ke situs besar seperti Twitter, Netflix, dan Reddit. Ini menjadi pelajaran bahwa perangkat kecil sekalipun dapat dimanfaatkan dalam skala serangan global jika keamanannya diabaikan.



Gambar 17. 3. Serangan Mirai botnet (2016)

Sumber: https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers

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.
3. 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.
4. 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.

TENTANG EDITOR

NURHADI, S.KOM., M.KOM

lahir di Bekasi, Jawa Barat bulan Nopember 1978. Beliau menamatkan pendidikan dasar dan menengah di Bekasi, setelah lulus dari STM Negeri 1 Bekasi (sekarang SMK Neger 1 Cikarang Barat) melanjutkan kuliah D3 di STMIK Pranata Indonesia Jurusan Managemen Informatika.

kemudian melanjutkan S1 di STMIK Pranata Indonesia Jurusan Sistem informasi. Pada tahun 2015 lulus S2 di universitas Budi Luhur Jakarta Program studi Magister Ilmu Komputer.

Beliau banyak mengikuti workshop tentang editor dan penulis buku yang di selenggarakan oleh lembaga pemerintahan maupun lembaga swasta. Saat ini sebagai dosen jurusan sistem informasi di STMIK Pranata Indonesia, mengajar untuk mata Kuliah Bahasa Pemrograman 1 dan Bahasa Pemrograman 2. Penulis juga aktif membuat video pembelajaran, salah satunya tentang pemrograman visual basic dan SQL server yang dapat di lihat di channel youtube penulis di ***https.//bit.ly/PDMVBSQL.***