MANAJEMEN ASET DIGITAL

Apa itu aset digital? Aset digital merupakan kepemilikan dengan jenis data apa pun dalam bentuk biner yang disimpan di komputer atau di internet dalam suatu server (cloud). Aset digital adalah setiap item teks atau media yang telah diformat menjadi sumber biner yang mencakup hak untuk menggunakannya. Pada titik ini, konsep "Aset Digital" lahir bukan hanya karena dorongan dari Teknologi Informasi, tetapi juga karena dorongan dari "Warga Digital" yang juga mendorong konsep "Aset Digital" menjadi nyata. Buku ini membahas tentang Konsep Dasar Manajemen Aset Digital, Konsep Aset Digital, Konsep Data dan Informasi, Manajemen Dokumen, Manajemen Konten, Manajemen Media, Sistem Informasi Aset Digital, Katalogisasi Aset Digital, Database Aset Digital, Server Aset Digital, dan Sistem Keamanan Aset Digital.

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

MANAJEMEN
ISBN 978-623-8575-20-6
9 786238 575206

MANAJEMEN ASET DIGITAL

MANAJEMEN ASET DIGITAL

Andi Asari, Muthia, Sri Ayu Ashari, Maemunah M., Eka Vickraien Dangkua, Huzaima Mas'ud, Indhitya R. Padiku, Nikmasari Pakaya, Robby Irsan, Mohamad Syafri Tuloli, Alfian Zakaria

MANAJEMEN ASET DIGITAL

Sanksi Pelanggaran Pasal 113
Undang-Undang No. 28 Tahun 2014 Tentang Hak Cipta

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 (1) 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 Rp 1.000.000.000,00 (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).

MANAJEMEN ASET DIGITAL

Andi Asari
Muthia
Sri Ayu Ashari
Maemunah M.
Eka Vickraien Dangkua
Huzaima Mas'ud
Indhitya R. Padiku
Nikmasari Pakaya
Robby Irsan
Mohamad Syafri Tuloli
Alfian Zakaria

MAFY media literasi INDONESIA

MANAJEMEN ASET DIGITAL

Penulis:
Andi Asari, Muthia, Sri Ayu Ashari, Maemunah M., Eka Vickraien Dangkua, Huzaima Mas'ud, Indhitya R. Padiku, Nikmasari Pakaya, Robby Irsan, Mohamad Syafri Tuloli, Alfian Zakaria

Editor:
Andi Asari

Desainer:
Mafy Media

Sumber Gambar Cover:
www.freepik.com

Ukuran:
vi, 166 hlm, 15,5 cm x 23 cm

ISBN:
978-623-8575-20-6

Cetakan Pertama:
Februari 2024

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

Kata Pengantar

Segala puji syukur kami panjatkan kepada Tuhan yang maha Esa, karena atas pertolongan dan limpahan rahmatnya sehingga penulis bisa menyelesaikan buku yang berjudul **Manajemen Aset Digital**. Buku ini di susun secara lengkap dengan tujuan untuk memudahkan para pembaca memahami isi buku ini. Buku ini membahas tentang Konsep Dasar Manajemen Aset Digital, Konsep Aset Digital, Konsep Data dan Informasi, Manajemen Dokumen, Manajemen Konten, Manajemen Media, Sistem Informasi Aset Digital, Katalogisasi Aset Digital, Database Aset Digital, Server Aset Digital, dan Sistem Keamanan Aset Digital.

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

Penulis, 31 Januari 2024

Daftar Isi

BAB 1

KONSEP DASAR MANAJEMEN ASET DIGITAL

Oleh Andi Asari

1.1 Pendahuluan

Karena kemajuan teknologi informasi yang sangat pesat, setiap organisasi didorong untuk menggunakan dan menerapkan teknologi, khususnya dalam pengelolaan informasi. Teknologi informasi bermanfaat bagi organisasi dengan mempermudah pengorganisasian, pengambilan, dan berbagi informasi. Dalam suatu organisasi, tata kelola informasi didefinisikan sebagai pendekatan strategis terintegrasi untuk mengelola, memproses, mengendalikan, menyimpan, dan mengambil bukti seluruh transaksi (Franks, 2013).

Pemanfaatan teknologi informasi dalam tata kelola informasi yang baik akan membantu organisasi dalam upaya pengelolaan pengetahuannya dengan tujuan memperkuat prinsip dan praktik terbaik untuk menanamkan solusi dalam setiap permasalahan penggunaan informasi untuk memenuhi kebutuhan organisasi dan pengguna layanan (Hendrawan, 2016). Hal ini bertujuan untuk mencapai keseimbangan antara komitmen organisasi terhadap keterbukaan,transparansi dan akuntabilitas yang efektif (Hendrawan & Ulum, 2017).

Sebagai sarana transfer ilmu pengetahuan kepada guru atau siswa, perpustakaan perguruan tinggi tidak bisa lepas dari dukungan teknologi informasi. Tentu saja seiring kemajuan teknologi, pustakawan harus kreatif dan imajinatif agar mampu menjawab kebutuhan informasi, baik secara langsung maupun melalui layanan elektronik. Beradaptasi dengan era digital dan era globalisasi, sumber daya perpustakaan tidak hanya ada dalam bentuk buku, namun keberadaan perpustakaan digital juga untuk menghemat ruang dan waktu. Perpustakaan digital adalah perpustakaan dengan koleksi dan pengelolaan digital. Menurut Sismanto, “perpustakaan digital” adalah “suatu sistem layanan dan objek informasi yang dapat diakses dengan menggunakan perangkat digital”. Sismanto (2008).

1.2 pengertian manajemen aset digital

Untuk mendukung perpustakaan digital diperlukan tempat penyimpanan data digital yang sering disebut database. Dalam perpustakaan sering dikenal dengan Digital Asset Management (DAM). Perpustakaan menciptakan manajemen aset digital karena beberapa alasan.

Menurut Pfister dan Zimmermann (2008), “Perpustakaan menerapkan manajemen sumber daya digital karena tiga alasan utama, antara lain meningkatkan visibilitas dan dampak keluaran penelitian, membuka akses kepada masyarakat luas sehingga

dapat memvisualisasikan pencapaian Intelektual universitas dan terciptanya sumber daya manusia yang unggul, sistem pengarsipan. Sehingga informasi atau keterangan ilmiah pada bahan karya dapat tersimpan dan mudah diakses saat dibutuhkan."

Karena universitas memiliki hak kekayaan intelektual, koleksi digital publikasi ilmiah para profesor universitas merupakan aset penting bagi perpustakaan universitas. Mengingat koleksi digital merupakan aset yang sangat penting dan berharga, maka perpustakaan akademik harus mampu mengelolanya secara efektif dan efisien melalui pemanfaatan DAM.

Amit Sawarkar (2001) mendefinisikan manajemen aset digital (DAM) sebagai serangkaian aktivitas yang menghasilkan sistem, ruang penyimpanan (repositori), dan alur kerja untuk mengelola multimedia yang diterbitkan dalam bentuk foto, grafik, dokumen, audio, informasi video. dan komponen lainnya yang bersifat non-digital (fisik).

Pengelolaan aset digital mengacu pada proses hulu dan hilir materi, mulai dari pemilihan format, pemilihan media penyimpanan, konversi ulang ke format baru, dan tentunya metode distribusi konten terkait. Tujuannya adalah untuk mempertahankan akses terhadap informasi ini selama mungkin, atau bahkan selamanya. (Furau'ki & Sukmana, 2018).

Analisis dari waktu ke waktu diperlukan untuk memastikan materi selalu dapat diakses. Seiring dengan penelitian format media, analisis teknologi merupakan pertimbangan utama dalam memastikan keterbacaan konten. Penerapan manajemen aset digital memerlukan data dan informasi sensitif, dan jelas diperlukan sistem keamanan yang andal untuk melindungi data dan informasi tersebut. Dapat disimpulkan bahwa manajemen aset digital (DAM) dapat membawa manfaat bagi pekerjaan yang didukung perangkat lunak seperti penyedia informasi dan sistem penyimpanan data. Manajemen aset digital banyak digunakan

tidak hanya di perpustakaan tetapi juga dalam bisnis (Furau'ki & Sukmana, 2018).

1.3 Tujuan Manajemen Aset Digital

Tujuan Manajemen Aset Digital. Beberapa tujuan dapat dicapai dengan menggunakan ide DAM ini, beberapa di antaranya adalah sebagai berikut:

a. Menjaga dan mengelola kepemilikan aset.
b. Menjamin keaslian dan integritas data dan dokumen.
c. Memanfaatkan data digital yang ada.
d. Meningkatkan efisiensi pengelolaan aset, meningkatkan produksi dan profitabilitas.
e. Menjaga integritas data selama penyimpanan dantransfer.
f. Meningkatkan kecepatan akses aset digital.

1.4 Manfaat Manajemen Aset Digital

Manfaat manajemen aset digital. Berikut manfaatmenggabungkan ide penyimpanan aset dengan konsep DAM:

a. Produktivitas dalam proses produksi.
b. Efektivitas biaya.
c. Cari aset digital dengan cepat.
d. Atur publisitas.
e. Memperkuat standardisasi perusahaan.

1.5 Alih Media Digital

Perpustakaan universitas mendapat manfaat dari kemajuan teknologi digital. Sumber informasi akan lebih mudah disajikan kepada pengguna, terutama untuk memenuhi kebutuhan informasi. Pengguna dapat mengakses informasi dari mana saja. Untuk memudahkan pengguna memperoleh informasi, salah satu caranya adalah dengan mengubah media penyimpanan kertas menjadi arsip elektronik, dengan upaya menjaga keutuhan dan keaslian arsip sekaligus mempermudah pengambilan arsip (Wahyuni, 2013).

Alat media transmisi yang paling dasar adalah alat perekam (scanner) atau kamera. Akibatnya, transfer media merupakan kegiatan yang melibatkan pengubahan materi cetak menjadi format digital (CD, DVD, mikrofiksi, dll). Bertambahnya koleksi perpustakaan yang terus meningkat melatarbelakangi perlunya penyelenggaraan alih media informasi, khususnya dari bentuk cetak ke bentuk digital. Tentu saja akan memakan banyak tempat karena perpustakaan memperoleh bahan perpustakaan setiap tahun; Namun demikian, dengan banyaknya bahan pustaka yang ada di perpustakaan, maka koleksi-koleksi tersebut dianggap berharga, sehingga harus ditransfer agar memberikan pengaruh yang bermanfaat bagi perpustakaan.(Furau'ki & Sukmana, 2018)

Tujuan dari kegiatan transfer media digital adalah untuk melestarikan nilai informasi yang terkandung dalam bahan perpustakaan, menghemat tempat, meningkatkan jumlah dan variasi koleksi informasi, mempercepat pencarian informasi, pertukaran informasi antar perpustakaan, memanfaatkan koleksi bersama, dan memaksimalkan aksesibilitas informasi yang diberikan kepada pengguna. Menurut Ajie (2013), proses transfer media digital harus melalui tahapan sebagai berikut:

a. Mengumpulkan dan memilih sumber perpustakaan untuk digunakan dalam program transfer media digital. Anda dapat memperoleh item perpustakaan dari sumber internal dan eksternal.
b. Memperjelas kepemilikan dan hak cipta atas sumber daya perpustakaan yang dikelola. Jika berada dalam domain publik atau dimiliki oleh suatu institusi, tidak memerlukan izin jelas dari penulis/pengarang atau penerbit.
c. Memeriksa keadaan fisik sumber daya perpustakaan. Jika terjadi kerusakan maka bahan perpustakaan akan rusak jika dilakukan prosedur pemindahan media; Misalnya jika bahan pustaka dipindai maka keadaan kertas aslinya akan rusak. Untuk menghindari hal tersebut, diperlukan penanganan

yang cermat melalui perawatan, pelestarian, dan restorasi (konservasi).

d. Setiap sumber koleksi dicatat dengan data bibliografi sehingga dapat diketahui jumlah dan statusnya secara pasti.
e. Melakukan tugas transfer media, seperti memindai atau memotret dengan kamera digital, pada setiap halaman dokumen dan gambar yang dicetak serta slidedan mikrofilm. Kamera digital digunakan untuk menangkap item perpustakaan dalam tiga dimensi. Begitu pula sumber perpustakaan untuk rekamanaudio dan video dibuat dengan bantuan perangkat dan aplikasi pendukung.
f. File digital dengan resolusi tinggi dihasilkan sebagai konsekuensi dari prosedur transfer media dan dapat digunakan sebagai file master. Selanjutnya untuk alasan pengeditan dan publikasi, prosedur konversi dilakukan ke jenis file yang sesuai, seperti menyalin file master TIFF atau RAW ke format JPEG atau GIF. Demikian pula format audio WAV diubah menjadi MP3, sedangkan format video AVI diubah menjadi MPEG atau WMV.
g. Melakukan proses pengeditan file digital seperti gambar, audio, dan video untuk pengemasan dan distribusi. Edit dengan perangkat lunak khusus seperti Adobe Photoshop dan Macromedia. Langkah pengeditan ini biasanya melibatkan penskalaan, perubahan kedalaman dan kontras warna, serta pembersihan area tertentu jika ada noda atau efek lain yang terjadi selama transfer media.
h. Setiap gambar harus diberi *watermark* dan berisi logo dengan transparansi tertentu. Berikut beberapa kriteria yang digunakan dalam proses *watermarking*:
    1) Kekuatan citra. Logo *watermark* tidak dapat langsung dihapus atau diubah tanpa melakukan perubahan signifikan pada dokumen atau filegambar terkait.
    2) Tidak terlihat. Bentuk gambar *watermark* yang digunakan tidak perlu terlihat sehingga tidak mempengaruhi

tampilan atau estetika sumber dokumen aslinya. Berbagai metode saat ini tersedia, termasuk holografi, atau hologram.

3) Keamanan. Artinya, dokumen yang diberi *watermark* tidak akan dapat dikenali dan diedit oleh orang yang tidak berkepentingan. Penggunaan *watermark* atau indikasi angkadimaksudkan untuk menjamin keabsahan atau keandalan asal dokumen.

i. Kompilasi file untuk setiap judul yang mencakup beberapa halaman teks atau dokumen yang telah diedit dan diberi *watermark*. Format kompilasi yang digunakan bisa berbeda-beda tergantung kebutuhan, seperti PDF untuk dokumen teks dan gambar atau MPEG atau MP4 untuk audio dan video.

j. Masukkan metadata dan unggah file digital menggunakan sistem perpustakaan digital atau sistem manajemen aset digital. Ini diperlukan untuk mengarsipkan setiap kumpulan file digital yang Anda buat. Sistem ini dimaksudkan untuk melakukan pengelolaan aset digital agar perkembangan hasil kegiatan transfer media dapat diketahui secara pasti, serta dilengkapi dengan fungsi indeks dan mesin pencari sebagai alat pencariannya.

k. Kemas dan publikasikan file digital yang dihasilkan ke dalam media yang mudah diakses oleh pengguna. Cara pengemasan yang paling umum adalah dengan menggunakan media disk yang dapat diakses secara mandiri oleh pengguna, seperti CD/DVD ROM. Publikasi diproduksi melalui Internet dengan akses tidak terbatas, dan gaya tampilan halaman web serta animasi multimedia dapat disesuaikan dengan kebutuhan.

DAFTAR PUSTAKA

Ajie, M.D. (2013). *Renstra Tata Kelola Digital Asset Management Perpustakaan UPI*. 8-10.

Furau'ki, N., & Sukmana, E. (2018). Implementation Of Digital Asset Management In Bandung Institute Of Technology Library. *Library and Information Science*, *8*(2), 2582–2182.

Sawarkar, A. (2001). *Digital Asset Management*. Cognizant Technology Solutions. 3-19.

Wahyuni, Tri & Bakhtaruddin Nst. (2013). *Alih Media Arsip Konvensional di kantor Perpustakaan, Arsip, dan Dokumentasi Kota Bukittinggi*. Jurnal Ilmu Informasi Perpustakaan dan Kearsipan, 2(1).

BIODATA PENULIS

Andi Asari, yang mempunyai nama lengkap Andi Muhammad Asari sebagai nama pemberian orang tua, dan memilki nama pena atau panggilan akrab Anas adalah dosen di Universitas NegeriMalang yang saat ini sedang melanjutkan studi doctoral (S3) di jurusan Information ManagementUiTM Malaysia. Lahir di desa Brongkal kabupaten Malang, semasa di Malang pernah mengenyam pendidikan di MI Azharul Ulum 02 Brongkal, kemudian lanjut di MTsN Malang 3 Sepanjang gondanglegi, dan lanjut di SMK Turen Malang. Kemudian melanjutkan belajar di perguruan tinggi di beberapa perguruan tinggi dikota Malang dan kemudian pindah ke kota pendidikan Daerah Istimewa Yogyakarta, dan sekarang domisili di Malang Jawa Timur. Penulis merupakan alumni dari Magister Kajian Budaya dan Media sekolah pasca sarjana Universitas Gadjah Mada Yogyakarta, dan juga alumni dari jurusan Ilmu Perpustakaan UIN Sunan Kalijaga Yogyakarta, serta alumni jurusan Teknik Informatika STMIK. Dan juga pernah belajar di kampus UM, UNISMA dan UMM semasa pencarian jati diri di tanah kelahiran Kota Malang. Semasa kuliah pernah aktif di beberapa organisasi internal kampus dan eksternal kampus.

Mulai tahun 2015 sampai sekarang penulis aktif mengajar di Jurusan Sastra Indonesia, Prodi S1 Ilmu Perpustakaan dan D4 Perpustakaan Digital Universitas Negeri Malang. Disamping kesibukan di dunia akademis juga memiliki kegiatan sebagai nara sumber pada kegiatan seminar, workshop, konsultan lembaga pendidikan dan perpustakaan.

Riwayat Pekerjaan:

- ❖ Ketua Asosiasi Peneliti dan Penulis Indonesia (APEPINDO)
- ❖ Ketua Yayasan Pondok Penulis Indonesia
- ❖ Sekretaris Yayasan Roudlotul Muhsinin Al-huffadz
- ❖ Dosen Universitas Negeri Malang
- ❖ Dewan Penasehat Lembaga EduArsip Yogyakarta
- ❖ Direktur PT Samudera Media Nusantara
- ❖ Penasihat PT Samudera Media Internasional
- ❖ Editor Jurnal Nasional dan Internasional
- ❖ Reviewer Jurnal
- ❖ Editor Ratusan Buku
- ❖ Penulis Puluhan Buku

Riwayat Mengajar:

https://pddikti.kemdikbud.go.id/data_dosen/RjEyRkFENzYtMEYx OS00QjE3LThFMzQtNTY1 RkYwOTA3MzM1

Riwayat Publikasi Artikel:

https://sinta.kemdikbud.go.id/authors?q=andi+asari

Riwayat Penerbitan Buku:

https://www.google.com/search?q=andi+asari&tbm=bks&ei=WE HEYpa1OdWh4t4PkI2jqAw& ved=0ahUKEwiWwf3w8eH4AhXVkNgFHZDGCMUQ4dUDCAg&oq =andi+asari&gs_lcp=Cg1nd3Mtd2l6LWJvb2tzEAxQAFgAYABoAHA AeACAAQCIAQCSAQCYAQA&sclient=gws- wiz-books

Riwayat Penelitian dan Pengabdian:

https://pakar.um.ac.id/Data/Peneliti/view/eyJpdiI6Ikt5bFNGRVQ yOURKVWdkNHFJUzVjR0E9PSIsInZhbHVlIjoiUjhJNGtKUDA4OVIx Q0ZkR3hRRUR2RGZWbU9HMlc2dGMvRHVSOG4zSW93QT0iLCJtY WMiOiI4ZGYxNTlmYjYwZTZmOWNmYjk4YTRiMGY1OGJiNTZkND IwNTc5ZThkY2YxMzk3OWU0MWRkMjk1MWRjZjc3YWRkIn0

Scopus ID : 57213605546
Publons ID : AAX-3077-2021
Sinta ID : 6027586
Garuda ID : 2677652
Google scholar:
https://scholar.google.co.id/citations?hl=id&user=YVa5GeIAAAAJ
Researchgate :
https://www.researchgate.net/profile/Andi-Asari/research
Email :
andi.asari.fs@um.ac.id
publishing.smn@gmail.com
Youtube:
https://youtube.com/channel/UCnNHvnNWspDB1pRQmBoI6ZQ
https://youtube.com/channel/UCJBO0b8pPXR86HuLrv7tn-Q
Facebook:
https://www.facebook.com/andiasari.official/@SMI PRESS
Instagram:
@andiasari.official
@smn.press
Twitter:
andiasari_um

BAB 2

KONSEP ASET DIGITAL

Oleh Muthia

2.1 Pendahuluan

Apa itu aset digital? Aset digital merupakan kepemilikan dengan jenis data apa pun dalam bentuk *biner* yang disimpan di komputer atau di internet dalam suatu *server* (cloud). Aset digital adalah setiap item teks atau media yang telah diformat menjadi sumber *biner* yang mencakup hak untuk menggunakannya (Niekerk, 2016). Pada titik ini, konsep "Aset Digital" lahir bukan hanya karena dorongan dari Teknologi Informasi, tetapi juga karena dorongan dari "Warga Digital" yang juga mendorong konsep "Aset Digital" menjadi nyata. Pendekatan lain yang akan dibahas adalah apa yang membuat file digital menjadi aset? (Moon, 2019). Repositori tidak lagi memandang gambar digital sebagai objek, tetapi lebih sebagaiaset digital.

Materi digital memiliki nilai jangka panjang dan dapat digunakan ulang seperti jenis aset lainnya. Selain itu, materi digital dapat dikenali dan digunakan ulang oleh orang lain, bukan hanya oleh pemilik atau pembuat aset digital tersebut. Siapa sebenarnya yang memiliki aset digital Anda? (Warwick- Ching, 2022). Saat ini, aset digital telah menjadi bagian dari kehidupan dan telah tertanam secara permanen dalam masyarakat digital, termasuk segala bentuk informasi digital yang disimpan di komputer, ponsel pintar, media digital, atau awan (*cloud*). Tidak lama yang lalu, aset dianggap hanya sebagai aset berwujud dalam bentuk fisik seperti uang tunai, mesin, bangunan, tanah, hewan ternak, dll., serta aset tidak berwujud yang dianggap sebagai aset nonfisik, seperti properti intelektual, hak cipta, paten, merek dagang, rahasia dagang, dan *goodwill* (Best, 2020). Mulai dari akhir abad ke-20, revolusi digital secara dramatis mengubah kehidupan masyarakat. Meskipun beberapa menganggap aset digital sebagai bagian dari aset tidak berwujud (Goldfinger, 2017). Fakta-fakta menunjukkan bahwa Teknologi Informasi yang berkembang pesat, inovatif, dan independen membuat "Aset Digital" benar-benar unik dan terpisah dari aset tidak berwujud.

Teknologi Informasi yang inovatif dan independen menciptakan bentuk baru dari populasi dunia digital atau "Warga Siber." Banyak warga dunia digital (Warga Siber) secara umum menyadari dan menerima bahwa "Aset Digital" sebagai kenyataan dan memiliki nilai, nilai signifikan, atau uang yang mungkin; seperti album foto digital dan album musik digital. Beberapa akun digital, misalnya *eBay* dan *PayPal*, mungkin memiliki nilai moneter setelah pemilik akun meninggal. Email dan akun media sosial mungkin berisi informasi pribadi penting yang erat hubungannya dengan keluarga dan teman pengguna, dan akun-akun ini mungkin sangat berharga bagi pemilik akun dan ahli waris mereka.

Dunia "*Cyber*" yang berkembang pesat dan konsep "aset digital" bersama dengan nilai-nilai ekonomi dan sosial yang semakin meningkat membawa ketidakpastian dan hambatan baru ke dalam masyarakat digital.

"Aset digital" adalah konsep baru yang sebanding dengan aset berwujud dan tidak berwujud. Definisi hukum, undang- undang, dan regulasi saat ini belum cukup untuk secara tepat mendefinisikan, melindungi, dan mengatur aset digital. Misalnya, apa yang akan terjadi pada aset digital setelah seseorang meninggal? Apakah orang dapat menyimpan, mentransfer, menjual, atau mewarisi aset digital mereka? Misalnya, apakah kerabat dapat mengakses *email*, akun *Facebook*, *Flickr*, *eBay*, atau *PayPal* orang yang sudah meninggal? Apakah ada hukum dan regulasi tentang konsep aset digital baru ini? Bagaimana orang akan menentukan nasib aset digital mereka? Bagaimana dengan ponsel pintar, file musik digital, data keuangan, *blog*, akun *Twitter*, atau informasi di penyimpanan awan (*cloud*)?Apakah kita memerlukan regulasi hukum untuk mengakses aset digital? Haruskah surat wasiat disusun khusus mengenai aset digital atau biarkan di tangan penyedia layanan digital dan berharap belas kasihan? Apa hukum dan referensi mendasar yang akan membantu dan memandu pihak-pihak seperti penyedia layanan akun digital, pemilik aset digital, dan ahli waris mereka? Di mana aset digital dimulai dan berakhir? Ini adalah beberapa pertanyaan penting yang menunggu jawaban pada saat ini. Untuk memulai mengidentifikasi jawaban dari banyaknya hal terkait aset digital dapat dimulai dengan memahami terkait konsep aset digital.

2.2 Pengertian Aset Digital

2.2.1 Definisi Aset Digital

a. Gartner, Inc.
   Menurut Gartner, aset digital mencakup beragam jenis data dan konten yang memiliki nilai ekonomi. Ini mencakup lebih dari sekadar file digital. [Gartner, 2023].

b. Brian Solis, Penulis dan Analis Digital
   Brian Solis menekankan beragam jenis konten dan entitas yang ada dalam format digital dalam definisinya. (Solis, 2016).
c. Jason Bloomberg, Ahli Transformasi Digital
   "Aset digital adalah segala sesuatu yang memiliki nilai ekonomi dan diwakili dalam format digital." menyoroti nilai ekonomi dan representasi digital dalam definisinya. [Toygar et al, 2013]
d. TechTarget
   "Aset digital adalah segala sesuatu yang bisa disimpan dalam format digital dan memiliki nilai." Definisi TechTarget menitikberatkan pada penyimpanan dalam format digital dan nilai yang dimiliki oleh aset tersebut. [TechTarget, 2019].

Aset digital adalah segala sesuatu yang memiliki nilai ekonomidan direpresentasikan dalam format digital. Aset ini mencakup beragam jenis data, teks, gambar, video, dan suara. Pemahaman yang mendalam tentang aset digital sangatpenting dalam konteks ekonomi digital yang berkembang pesat dan bisnis modern.

2.2.2 Pentingnya Aset Digital dalam Dunia Modern

Dalam era digital yang semakin berkembang pesat, aset digital memiliki peran sentral dalam berbagai aspek kehidupan kita. Penjelasan ini akan membahas mengapa aset digital menjadi begitu penting dalam dunia modern.

a. Transformasi Bisnis
   Aset digital adalah pendorong utama transformasi bisnis modern. Bisnis yang mengelola dan memanfaatkan aset digital dengan baik cenderung lebih kompetitif dan inovatif (Bughin, et al, 2016). Mereka dapat menciptakan model bisnis baru dan meraih pangsa pasar yang lebih besar.
b. Ekonomi Digital
   Aset digital adalah salah satu fondasi ekonomi digital. Mereka menciptakan peluang baru untuk perdagangan, layanan, dan investasi (Bughin, et al, 2016). Ekonomi digital telah

menciptakan jutaan pekerjaan baru di seluruh dunia.

c. Inovasi dan Kreativitas
   Aset digital mendukung inovasi dan kreativitas. Mereka memungkinkan pengembang, seniman, dan perusahaan untuk menciptakan konten baru, aplikasi, dan solusi teknologi yang merubah dunia.
d. Akses Global
   Aset digital memungkinkan akses global ke informasi dan layanan (Anderson, 2018). Mereka membantu menjembatani kesenjangan akses digital di berbagai negara dan menghubungkan orang-orang dari berbagai budaya.
e. Efisiensi Operasional
   Dalam dunia bisnis, aset digital membantu meningkatkan efisiensi operasional (Parley & Gasser, 2018). Mereka memungkinkan otomatisasi, analisis data real-time, dan pengelolaan rantai pasokan yang lebih efisien.
f. Pendidikan dan Pembelajaran
   Aset digital digunakan dalam pendidikan modern. Mereka memungkinkan pembelajaran jarak jauh, kursus online, dan akses ke berbagai sumber pendidikan dari seluruh dunia.

2.3 Jenis-jenis Aset Digital

Aset digital mencakup beragam jenis konten dan data yang memiliki nilai ekonomi. Dalam materi ini, kita akan mengeksplorasi beberapa jenis utama aset digital yang digunakan dalam dunia modern.

a. Aset Digital Tangible
   Aset digital tangible adalah aset yang memiliki wujud fisik dalam dunia digital. Contohnya termasuk perangkat keras komputer seperti laptop, ponsel, dan tablet. Aset digital tangible adalah fondasi dari perangkat keras yang digunakan dalam produksi dan pengaksesan aset digital lainnya (Nakamoto, 2018).

b. Aset Digital Non-Tangible
   Aset digital non-tangible adalah aset yang tidak memiliki wujud fisik. Ini termasuk dokumen digital, gambar, audio, video, dan perangkat lunak. Aset digital non-tangible mencakup konten digital yang sangat beragam, dari dokumen bisnis hingga hiburan multimedia (Lessig, 2014).
c. Aset Digital Finansial
   Aset digital finansial adalah bentuk digital dari uang, seperti cryptocurrency (contoh: Bitcoin) atau uang elektronik (e-money). Aset digital finansial telah mengubah cara kita bertransaksi dan berinvestasi, membuka peluang baru dan tantangan dalam ekonomi digital.
d. Aset Digital Kekayaan Intelektual
   Aset digital kekayaan intelektual mencakup hak cipta, paten, merek dagang, dan hak kekayaan intelektual lainnya dalam bentuk digital. Perlindungan dan pengelolaan aset digital kekayaan intelektual sangat penting dalam melindungi inovasi dan karya intelektual (Schneier, 2015).
e. Aset Digital Sumber Daya Manusia
   Aset digital sumber daya manusia mencakup profil, keterampilan, dan data pribadi individu yang digunakan dalam berbagai aplikasi, seperti platform media sosial atau pasar kerja daring. Aset digital sumber daya manusia memiliki peran penting dalam ekosistem media sosial dan perekrutan sumber daya manusia (Davenport et al, 2020).

Jenis-jenis aset digital yang beragam ini merupakan bagian integral dari dunia digital modern. Mereka memiliki nilai ekonomi dan peran yang berbeda dalam berbagai sektor, termasuk bisnis, keuangan, hiburan, dan teknologi. Pengelolaan dan perlindungan aset digital adalah tantangan yang harus diatasi dalam era digital yang semakin kompleks.

2.4 Hak Kepemilikan Aset Digital

Konsep hak kepemilikan aset digital adalah topik penting dalam era digital ini. Materi ini akan membahas berbagai jenis hak kepemilikan aset digital dan mengapa pemahaman tentang hal ini sangat penting.

a. Hak Kepimilikan Intelektual
   Hak kepemilikan intelektual (HKI) mencakup hak cipta, paten, merek dagang, dan hak kekayaan intelektual lainnya atas aset digital yang dihasilkan. HKI melindungi karya intelektual dan inovasi, mendorong kreasi baru, dan memberikan pemilik hak kontrol atas penggunaan aset mereka (Fama & French, 2022).
b. Hak Akses dan Penggunaan
   Hak akses dan penggunaan mengatur siapa yang memiliki izin untuk mengakses dan menggunakan aset digital tertentu. Hak ini menentukan siapa yang memiliki akses ke aset digital, seperti data, dan bagaimana mereka dapat menggunakannya.
c. Hak Transfer
   Hak transfer mengizinkan pemilik aset digital untuk mentransfer kepemilikan mereka kepada pihak lain (Boyle, 2018). Hak ini penting dalam transaksi jual beli aset digital dan dalam pengaturan warisan.
d. Hak Privasi dan Keamanan
   Hak privasi dan keamanan melibatkan hak individu untuk melindungi data pribadi mereka dan hak perusahaan untuk melindungi aset digital mereka dari ancaman siber (Boyle, 2018). Hak ini sangat penting dalam menjaga keamanan dan privasi dalam dunia digital yang semakin terkoneksi.

Pemahaman tentang hak kepemilikan aset digital adalah kunci dalam melindungi hak dan kepentingan individu, perusahaan, dan masyarakat dalam dunia digital yang semakin kompleks. Hak kepemilikan intelektual, hak akses dan penggunaan, hak transfer, serta hak privasi dan keamanan adalah elemen- elemen penting dalam pemahaman ini.

2.5 Licensi dan Penggunaan Aset Digital

Lisensi dan penggunaan aset digital adalah aspek penting dalam manajemen aset digital. Materi ini akan membahas konsep lisensi, jenis-jenis lisensi, dan pentingnya memahami bagaimana aset digital dapat digunakan dengan benar.

2.5.1 Licensi Aset Digital

Lisensi adalah izin yang diberikan oleh pemilik aset digital kepada pihak lain untuk menggunakan aset tersebut dalam batasan tertentu (Randles & Stam, 2020). Lisensi mengatur penggunaan aset digital, termasuk apa yang diizinkan dan apa yang tidak, serta apakah pengguna harus membayar royalti. Jenis-jenis license antara lain (Stallman, 2022).

a. Licensi Terbuka (*Open Source*)
   Memungkinkan pengguna untuk mengakses, menggunakan, dan memodifikasi aset digital dengan sedikit atau tanpa pembatasan.
b. Licensi Berbayar
c. Mengharuskan pengguna membayar untuk hak penggunaan aset digital.
   Licensi Kepemilikan
d. Memberikan hak kepemilikan penuh kepada pengguna, biasanya dalam kasus pembelian aset digital.

2.5.1 Penggunaan Aset Digital

Lisensi mengatur cara penggunaan aset digital, termasuk apakah pengguna dapat mengubah, menyalin, mendistribusikan, atau menjualnya (Moerland, 2018). Memahami penggunaan yang diizinkan membantu mencegah pelanggaran hak cipta dan penggunaan yang tidak sah. Beberapa lisensi mengharuskan pengguna membayar royalti atau biaya berlangganan untuk menggunakan aset digital. Pemahaman tentang biaya terkait dengan lisensi diperlukan untuk perencanaan anggaran.

Lisensi dan penggunaan aset digital adalah bagian penting dari manajemen aset digital yang efektif. Pemahaman tentang jenis lisensi, hak penggunaan yang diizinkan, dan kewajiban pembayaran royalti membantu individu dan perusahaan dalam memanfaatkan aset digital dengan benar, mematuhi hukum, dan mencegah pelanggaran hak cipta.

2.6 Pentinganya Memahami Konsep Aset Digital

Dalam dunia yang semakin terdigitalisasi, memahami konsepaset digital menjadi sangat penting. Dalam materi ini, kita akan menjelaskan mengapa pemahaman tentang aset digital adalah hal yang vital.

a. Transformasi Bisnis
   Aset digital adalah tulang punggung transformasi bisnis modern. Perusahaan yang memahami dan memanfaatkan aset digital dengan baik cenderung lebih kompetitif dan inovatif. Mereka dapat menciptakan model bisnis baru dan meraih pangsa pasar yang lebih besar.
b. Ekonomi Digital
   Aset digital adalah salah satu fondasi ekonomi digital. Mereka menciptakan peluang baru untuk perdagangan, layanan, dan investasi (Worl Economic Forum, 2016). Ekonomi digital telah menciptakan jutaan pekerjaan baru di seluruh dunia.
c. Inovasi dan Kreativitas
   Aset digital mendukung inovasi dan kreativitas. Mereka memungkinkan pengembang, seniman, dan perusahaan untuk menciptakan konten baru, aplikasi, dan solusi teknologi yang merubah dunia.
d. Perlindungan dan Keamanan
   Memahami konsep aset digital adalah langkah pertama dalam melindungi diri (Schneier, 2015). Keamanan aset digital menjadi semakin penting dalam menghadapi ancaman siber yang berkembang pesat.

e. Investasi dan Nilai
   Pemahaman aset digital memungkinkan individu dan perusahaan untuk mengelola dan menginvestasikan aset mereka dengan lebih bijak. Ini termasuk investasi dalam cryptocurrency, saham teknologi, atau bahkan domain web (Tapscott, 2016).
f. Pendidikan dan Kesadaran
   Dalam pendidikan modern, pemahaman tentang aset digital sangat penting. Ini memungkinkan generasi muda untuk menjadi pengguna yang cerdas dan bertanggung jawab dalam dunia digital.

Memahami konsep aset digital adalah esensial dalam dunia yang semakin terkoneksi ini. Aset digital adalah kunci untuk transformasi bisnis, inovasi, dan kemajuan ekonomi. Selain itu, pemahaman ini membantu dalam melindungi aset, mengelola investasi, dan mendukung pendidikan modern. Dalam era digital yang semakin kompleks, pemahaman tentang aset digital adalah modal yang berharga.

DAFTAR PUSTAKA

Anderson, C. (2018). The Long Tail: Why the Future of Businessis Selling Less of More. Hyperion.

Best, K. (2020). The Fundamentals of Design Management. Lausanne, Ava Publishing.

Boyle, J. (2018). The Public Domain: Enclosing the Commons of the Mind. Yale University Press.

Bughin, J., Hazan, E., Lund, S., Dahlström, P., Wiesinger, A., & Subramaniam, A. (2016). Digital Europe: Realizing the continent's potential. McKinsey & Company.

Davenport, T. H., Harris, J., & Shapiro, J. (2020). Competing on Talent Analytics. Harvard Business Review, 88(10), 52-58.

Fama, E. F., & French, K. R. (2022). The Cross-Section of Expected Stock Returns. Journal of Finance, 47(2), 427-465.

Goldfinger, C. (2017). Intangible economy and its implicationsfor statistics and statisticians. International Statistical Review.65(2), 1997.

https://www.briansolis.com/2016/01/digitaltransformation-its-about-people-first/ (accessed 8/31/2023)

https://www.gartner.com/en/informationtechnology/glossary/digital-asset (accessed 8/31/2023)

https://searchcontentmanagement.techtarget.com/definition/digital-asset (accessed 8/31/2023)

Lessig, L. (2014). Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity. Penguin Press.

Moerland, J., & Van Der Flier, H. (2018). The Impact of Open Source Software on the Use of Software Licenses. International Journal of Economics, Commerce, and Management, 6(8), 1-12.

Moon, M. (2019). Activity lifecycle of digital assets. Journal of Digital Asset Management, 3(3), 112-115.

Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.

Palfrey, J. G., & Gasser, U. (2018). Born Digital: Understanding the First Generation of Digital Natives. Basic Books.

Randles, M., & Stam, A. (2020). Open Source Software: A Primerfor Intellectual Property Attorneys. Intellectual Property & Technology Law Journal, 22(2), 14-16.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.

Toygar, Alp; Rohm, C.E. Taipe Jr.; and Zhu, Jake (2013) "A New Asset Type: Digital Assets," Journal of International Technology and Information Management: Vol. 22: Iss. 4, Article 7.

Stallman, R. M. (2022). Free Software, Free Society: Selected Essays of Richard M. Stallman. Free Software Foundation.

Van Niekerk, A. J. (2016). The Strategic Management of Media Assets; a Methodological Approach. Allied Academies, NewOrleans Congress.

Warwick-Ching, L. (2022). Who really owns your digital assets?

World Economic Forum. (2016). The Future of Jobs: Employment, Skills, and Workforce Strategy for the Fourth Industrial Revolution. World Economic Forum.

BIODATA PENULIS

Muthia, S.SI., M.Pd. MCE
Dosen Pendidikan Teknologi Informasi
Fakultas Teknik Universitas Negeri Gorontalo

Penulis lahir di Gorontalo tanggal 11 Desember 1991. Penulis adalah dosen pada Program Studi Pendidikan Teknologi Informasi Fakultas Teknik, Universitas Negeri Gorontalo. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika Prodi Sistem Informasi Universitas Negeri Gorontalo, dan melanjutkan S2 pada Universitas Negeri Semarang, Program Pasca Sarjana Jurusan Pendidikan Kejuruan Konsentrasi Pendidikan Teknologi dan Informasi. Penulis menekuni bidang Penelitian dan Pengabdian di bidang Teknologi Informasi khususnya Pendidikan.

BAB 11

SISTEM KEAMANAN ASET DIGITAL

Oleh Alfian Zakaria

Dalam era digital yang terus berkembang, aset digital telah menjadi bagian integral dari kehidupan kita. Aset-aset ini melibatkan data berharga, informasi rahasia, mata uang kripto, sumber daya perangkat lunak, infrastruktur jaringan, dan lebih banyak lagi. Sementara teknologi telah memberikan manfaat besar bagi masyarakat, pertumbuhan pesat ini juga membawa risiko baru yang signifikan. Untuk melindungi aset digital yang kita miliki, kita perlu memahami konsep dan praktik sistem keamanan aset digital.

11.1 Definisi Sistem Keamanan Aset Digital

Sistem keamanan aset digital adalah rangkaian strategi, prosedur, teknologi, dan kebijakan yang disusun dengan tujuan utama melindungi aset digital dari berbagai jenis ancaman dan potensi kerusakan. Aset digital dapat mencakup berbagai bentuk, seperti data pribadi, informasi bisnis, dokumen elektronik, dan elemen-elemen digital lainnya yang memiliki nilai atau relevansi tertentu.

Langkah-langkah dalam sistem keamanan aset digital mencakup identifikasi potensi risiko, penerapan kontrol keamanan, pemantauan secara terus-menerus, dan respons cepat terhadap insiden keamanan. Teknologi keamanan seperti firewall, enkripsi data, dan perangkat lunak keamanan siber dapat digunakan untuk memitigasi risiko dan menjaga integritas serta kerahasiaan aset digital.

Prosedur keamanan harus mencakup manajemen akses yang ketat, pengelolaan sandi yang aman, serta kebijakan keamanan yang jelas dan dapat diterapkan. Selain itu, pelibatan karyawan dalam pelatihan keamanan siber dan kesadaran keamanan menjadi bagian penting dari sistem ini, karena seringkali manusia merupakan sasaran utama dalam upaya peretasan.

Prinsip dasar dari sistem keamanan aset digital adalah mencegah, mendeteksi, dan merespons terhadap ancaman keamanan dengan cepat dan efektif. Melalui implementasi sistem ini, organisasi atau individu dapat meminimalkan risiko terhadap kebocoran data, pencurian identitas, atau kerusakan terhadap aset digital yang dapat berdampak padakeberlanjutan operasional dan reputasi.

11.2 Mengapa Keamanan Aset Digital Penting

Keamanan aset digital menjadi penting karena peran yangkrusial dalam melindungi informasi dan data yang memiliki nilai besar, baik untuk individu, bisnis, maupun masyarakat pada umumnya.

Beberapa alasan mengapa keamanan aset digital sangat penting melibatkan konsekuensi keamanan, privasi, keuangan, dan reputasi. Berikut adalah pemahaman lebih lanjut mengenai mengapa keamanan aset digital sangat ditekankan:

a. **Perlindungan Terhadap Ancaman Siber:** Keamanan aset digital menjadi sangat penting karena meningkatnya ancaman siber di era digital ini. Serangan siber seperti malware, ransomware, phishing, dan serangan siber lainnya dapat merusak, mencuri, atau merusak data digital dengan cepat dan tanpa deteksi yang tepat waktu. Tanpa langkah-langkah keamanan yang memadai, aset digital menjadi rentan terhadap serangan yang dapat menyebabkan kerugian finansial, kehilangan informasi penting, atau bahkan gangguan operasional yang signifikan.
b. **Privasi dan Keamanan Data Pribadi:** Aset digital seringkali mencakup data pribadi, termasuk informasi identitas, riwayat keuangan, dan data sensitif lainnya. Kehilangan privasi ini dapat memiliki konsekuensi serius, termasuk potensi pencurian identitas, penipuan keuangan, atau eksploitasi data untuk kepentingan jahat. Dengan memastikan keamanan aset digital, individu dapat menjaga privasi mereka dan mengurangi risiko terhadap penyalahgunaan data pribadi.
c. **Keberlanjutan Operasional Bisnis:** Bagi bisnis, keamanan aset digital menjadi krusial untuk menjaga keberlanjutan operasional. Serangan terhadap sistem informasi atau pencurian data bisnis dapat menyebabkan gangguan layanan, kerugian finansial, dan merusak reputasi perusahaan. Dengan menerapkan sistem keamanan yang kokoh, perusahaan dapat melindungi informasi bisnis, menjaga produktivitas, dan meminimalkan dampak negatif terhadap operasional mereka.
d. **Kepatuhan Regulasi:** Banyak negara dan industri memiliki regulasi ketat terkait perlindungan data dan privasi. Kepatuhan terhadap regulasi ini bukan hanya tanggung jawab etika, tetapi juga dapat membawa konsekuensi hukum

dan keuangan jika tidak dipatuhi. Dengan memiliki sistem keamanan aset digital yang memadai, organisasi dapat memastikan bahwa mereka memenuhi standar keamanan yang ditetapkan oleh regulasi, mengurangi risiko sanksi dan denda.

e. **Kepercayaan Pelanggan dan Reputasi:** Keamanan aset digital juga berperan penting dalam membangun dan mempertahankan kepercayaan pelanggan. Konsumen modern cenderung memilih produk atau layanan yang menawarkan jaminan keamanan terhadap data mereka. Suatu kebocoran data atau pelanggaran keamanan dapat merusak reputasi perusahaan dan mengurangi kepercayaan pelanggan. Oleh karena itu, investasi dalam keamanan aset digital bukan hanya sebagai langkah perlindungan, tetapi juga sebagai investasi jangka panjang dalam menjaga kepercayaan pelanggan dan reputasi bisnis.
f. **Inovasi dan Pengembangan Teknologi:** Keamanan aset digital juga memungkinkan inovasi dan pengembangan teknologi yang lebih lanjut. Dengan memiliki rasa aman terhadap keamanan aset digital, organisasi dapat lebih leluasa untuk mengembangkan dan mengadopsi teknologi baru tanpa khawatir terhadap risiko yang terkait dengan serangan siber ataukebocoran data.

Dalam rangka untuk mengatasi kompleksitas dan intensitas ancaman siber yang terus berkembang, keamanan aset digital bukan hanya suatu keharusan, tetapi juga suatu investasi yang strategis. Kesadaran akan pentingnya keamanan digital harus diakui di semua lapisan masyarakat, mulai dari individu hingga perusahaan dan pemerintah, guna menciptakan lingkungan digital yang aman dan dapat diandalkan bagi semua pihak yangterlibat.

11.3 Langkah Pertama: Identifikasi Risiko

Identifikasi potensi risiko merupakan langkah kritis dalamupaya melindungi aset digital. Proses ini memungkinkan individu,

bisnis, atau organisasi untuk memahami dan mengevaluasi ancaman yang mungkin dihadapi aset digital mereka. Berikut adalah beberapa langkah yang dapat diambil dalam mengidentifikasi potensi risiko aset digital:

a. **Inventarisasi Aset Digital**: Pertama-tama, identifikasi semua aset digital yang dimiliki. Ini dapat mencakup data pelanggan, informasi keuangan, rancangan produk, kode sumber perangkat lunak, atau bahkan properti intelektual. Dengan mengetahui dengan jelas apa saja aset digital yang dimiliki, lebih mudah untuk mengidentifikasi potensi risiko yang terkait.
b. **Evaluasi Nilai Aset:** Tentukan nilai strategis dan finansial dari setiap aset digital. Aset yang memiliki nilai tinggi cenderung menjadi target yang lebih menarik bagi pihak yang tidak sah. Oleh karena itu, penilaian nilai membantu dalam menetapkan prioritas keamanan dan menentukan langkah-langkah perlindungan yang lebih cermat.
c. **Identifikasi Ancaman Potensial:** Analisis ancaman melibatkan identifikasi berbagai jenis ancaman yang dapat mengakibatkan kerugian terhadap aset digital. Ancaman tersebut bisa mencakup serangan siber, kebocoran data, pencurian fisik perangkat, atau tindakan insider yang tidak sah. Dengan mengetahui berbagai potensi ancaman, dapat dibuat strategi keamanan yang lebih komprehensif.
d. **Analisis Kerentanan:** Tinjau kerentanan potensial dalam infrastruktur teknologi, perangkat lunak, atau proses bisnis yang digunakan untuk mengelola aset digital. Kerentanan ini bisa berasal dari kekurangan keamanan dalam perangkat keras, perangkat lunak yang tidak terbarukan, atau kesalahan manusia dalam kebijakan keamanan.
e. **Pertimbangkan Faktor Internal dan Eksternal:** Faktor internal seperti praktik keamanan internal, tingkat kepatuhan karyawan, dan manajemen akses perlu dievaluasi. Selain itu, pertimbangkan faktor eksternal seperti perubahan

dalam regulasi keamanan siber, tren serangan terbaru, atau perkembangan teknologi yang dapat mempengaruhi risiko aset digital.

f. **Tinjau Kebijakan dan Kepatuhan:** Pastikan kepatuhan terhadap kebijakan dan regulasi keamanan yang berlaku. Tinjau apakah kebijakan keamanan yang ada masih relevan dan efektif atau perlu disesuaikan dengan perkembangan terbaru dalam dunia keamanansiber.
g. **Evaluasi Kelemahan dalam Sistem Keamanan:** Melakukan audit keamanan secara berkala untuk mengidentifikasi kelemahan dalam sistem keamanan yang ada. Ini mencakup evaluasi keefektifan kontrol akses, penggunaan enkripsi, pemantauan jaringan, danteknologi keamanan lainnya.
h. **Pertimbangkan Risiko dari Faktor Manusia:** Manusia seringkali merupakan faktor risiko signifikan. Tinjau kebijakan akses karyawan, tingkat kesadaran keamanan karyawan, dan pelibatan mereka dalam praktik keamanan siber. Pelatihan dan kesadaran keamanan dapat membantu mengurangi risiko yang disebabkan oleh tindakan kelalaian atau kecerobohan manusia.
i. **Tinjau Histori Keamanan:** Pelajari sejarah kejadian keamanan sebelumnya atau insiden serangan siber yang mungkin telah mempengaruhi organisasi atau individu. Hal ini membantu dalam memahami tren serangan dan meningkatkan kewaspadaan terhadap potensi ancaman yang serupa di masa depan.
j. **Kolaborasi dengan Ahli Keamanan:** Dalam mengidentifikasi risiko, bergabung dengan komunitas keamanan siber, atau bekerja sama dengan ahli keamanan dapat memberikan wawasan tambahan. Mereka dapat membantu mengidentifikasi risiko yang mungkin tidak terpikirkan sebelumnya dan memberikan solusi yang lebih efektif.

Melalui langkah-langkah ini, individu atau organisasi dapat memiliki pemahaman yang lebih baik tentang potensi risiko yang mungkin dihadapi aset digital mereka. Identifikasi risiko adalah langkah pertama yang kritis dalam mengembangkan strategi keamanan yang efektif dan responsif terhadap ancaman yang terus berkembang di dunia digital.

11.4 Klasifikasi Aset: Data yang Sensitif dan Perlindungan Ekstra

Tidak semua aset digital sama. Beberapa data mungkin lebih sensitif daripada yang lain. Misalnya, data pribadi seperti nomor KTP, nomor rekening bank, atau riwayat medis adalah data yang sangat sensitif. Oleh karena itu, penting untuk mengklasifikasikan aset digital Anda berdasarkan tingkat sensitivitasnya. Data yang sangat sensitif harus diberikan perlindungan ekstra. Ini termasuk penggunaan enkripsi yang kuat untuk data ini saat disimpan atau ditransmisikan.

Klasifikasi aset, khususnya data yang sensitif, merupakan langkah kunci dalam membangun strategi keamanan yang efektif. Data yang sensitif mencakup informasi yang jika jatuh ke tangan yang salah, dapat mengakibatkan konsekuensi serius seperti pencurian identitas, penipuan, atau pelanggaran privasi. Dalam melindungi data yang sensitif, perlindungan ekstra dan pendekatan yang cermat diperlukan. Berikut adalah klasifikasi aset dan langkah-langkah perlindungan ekstra yangdapat diambil:

Klasifikasi Aset:

a. **Data Pribadi:** Termasuk informasi identitas pribadi seperti nama, alamat, nomor telepon, nomor identifikasi, dan informasi keuangan.
b. **Informasi Keuangan:** Melibatkan data terkait keuangan seperti nomor kartu kredit, rekening bank, atau informasi pembayaran lainnya.

c. **Data Kesehatan:** Informasi medis dan kesehatan individu, yang sering kali dilindungi oleh regulasi kesehatan seperti HIPAA (Health Insurance Portability and Accountability Act).
d. **Properti Intelektual:** Melibatkan hak cipta, paten, atau informasi bisnis eksklusif yang memiliki nilai strategis.
e. **Data Pelanggan:** Informasi terkait pelanggan, preferensi mereka, dan riwayat pembelian yang dapat memberikan wawasan bisnis yang berharga.
f. **Rancangan Produk dan Riset:** Data terkait pengembangan produk, rancangan, dan hasil riset yangbelum dipublikasikan.
g. **Informasi Konfidensial Perusahaan:** Informasi strategis atau operasional yang dapat memberikan keuntungan bersaing dan harus dijaga dengan ketat.

11.5 Enkripsi: Menjaga Data Anda Tetap Rahasia

Enkripsi adalah suatu proses yang digunakan untuk menjaga kerahasiaan dan keamanan data dengan mengonversi informasi menjadi bentuk yang tidak dapat dimengerti tanpa kunci dekripsi yang sesuai. Dengan menerapkan enkripsi, bahkan jika data tersebut dicuri atau diakses oleh pihak yang tidak berwenang, mereka tidak akan dapat membaca atau memahaminya. Ini merupakan langkah kunci dalam menjaga privasi dan keamanan informasi di dunia digital yang terus berkembang. Berikut adalah beberapa aspek penting terkait enkripsi dan cara menjaga data Anda tetap rahasia:

Cara Kerja Enkripsi:

Enkripsi melibatkan proses mengubah teks biasa (plaintext) menjadi teks terenkripsi (ciphertext) menggunakan algoritma enkripsi dan kunci. Hanya dengan kunci dekripsi yang sesuai, data dapat dikembalikan ke bentuk aslinya. Terdapat dua jenis utama enkripsi:

a. Enkripsi Simetris: Menggunakan kunci yang sama untuk enkripsi dan dekripsi. Contoh algoritma simetris termasuk AES (Advanced Encryption Standard).

b. Enkripsi Asimetris: Menggunakan sepasang kunci, yaitu kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. RSA adalah salah satu contoh algoritma asimetris.

Perlindungan Data Selama Penyimpanan dan Selama Transmisi:

Berikut adalah jenis-jenis enkripsi yang dapat digunakan saat data disimpan dalam suatu media penyimpanan

c. Disk Encryption: Mengenkripsi seluruh disk atau volume penyimpanan. Misalnya, BitLocker untuk Windows atau FileVault untuk macOS.
d. Database Encryption: Melibatkan enkripsi data yang disimpan di dalam database, sehingga bahkan jika database dicuri, data tetap aman.

Sedangkan untuk enkripsi yang dapat digunakan selama Transmisi adala sebagai berikut :

e. SSL/TLS Protokol: Digunakan untuk mengenkripsi data yang dikirim antara server dan pengguna melalui web. Memastikan keamanan transmisi data saat melakukan transaksi online.
f. End-to-End Encryption (E2EE): Mengenkripsi konten email dari pengirim hingga penerima, sehingga hanya penerima yang dapat membaca isinya. ProtonMail adalah contoh penyedia layanan email dengan E2EE. End-to-End Encryption untuk Pesan Instan: Aplikasi seperti WhatsApp dan Signal menggunakan E2EE untuk melindungi pesan teks dari akses yang tidak sah. Panggilan Suara yang Aman: Aplikasi seperti Signal dan Telegram menawarkan panggilan suara yang dienkripsi untuk menjaga privasi percakapan.

Kekuatan enkripsi selain pada algoritma enkripsi yang digunakan juga di tentukan oleh kekuatan kunci (*key*) yang digunakan, kunci yang panjang dan kompleks lebih sulit untuk dipecahkan. Melalui penerapan enkripsi yang tepat, organisasi dan individu dapat menjaga data mereka tetap rahasia dan melindungi informasi sensitif dari akses yang tidak sah. Enkripsi merupakan salah satu

lapisan keamanan yang paling efektif dalam upaya melindungi integritas dan kerahasiaan data di era digital saat ini.

11.6 Otentikasi: Mencegah Akses yang Tidak Sah

Sistem keamanan harus memastikan bahwa hanya orang yang berwenang yang dapat mengakses aset digital. Ini melibatkan penggunaan otentikasi yang kuat. Kata sandi kuat, otentikasi dua faktor (2FA), dan bahkan teknologi biometrik seperti sidik jari atau pemindaian wajah dapat digunakan untuk memastikan otentikasi yang kuat. Otentikasi adalah pintu gerbang pertama dalam menjaga keamanan informasi dan sumber daya digital. Ini merupakan proses kritis yang memverifikasi identitas pengguna atau sistem sebelum memberikan akses ke data atau layanan tertentu. Tujuannya adalah mencegah akses yang tidak sah dan memastikan bahwa hanya pihak yang berwenang yang dapat menggunakan atau mengakses suatu sistem. Di bawah ini adalah pemaparan lebihrinci mengenai konsep dan strategi otentikasi:

Jenis Otentikasi:

a. **Kata Sandi (Password):** Pengguna memberikan kombinasi karakter unik sebagai bukti identitasnya.
b. **Otentikasi Dua Faktor (2FA):** Kombinasi kata sandi dengan faktor tambahan seperti kode yang dikirimkan melalui pesan teks.
c. **Biometrik:** Penerapan fitur fisik atau perilaku unik, seperti sidik jari atau pengenalan wajah.
d. **Otentikasi Multi-Faktor (MFA):** Penggunaan dua atau lebih metode otentikasi secara bersamaan.

Keamanan Kata Sandi:

a. **Kekuatan Kata Sandi:** Mendorong pengguna untukmembuat kata sandi yang kuat dengan kombinasi karakter yang beragam.
b. **Rotasi Kata Sandi:** Menggugah pengguna untuk secara berkala mengubah kata sandi mereka.

Penggunaan Token dan Kode Unik:

a. **Token:** Menghasilkan kode dinamis untuk memberikan otorisasi akses.
b. **Kode Unik:** Penggunaan kode yang dikirimkan melalui pesan teks atau aplikasi otentikasi.

Biometrik dan Pengenalan Wajah:

a. **Sidik Jari:** Menggunakan pemindaian sidik jari untuk verifikasi identitas.
b. **Pengenalan Wajah:** Menilai fitur wajah untukmengotentikasi pengguna.

Manajemen Sesi:

a. **Logout Otomatis:** Mengakhiri sesi pengguna secara otomatis setelah periode inaktivitas.
b. **Token Sesi yang Kuat:** Memastikan token sesi yang digunakan pengguna cukup kuat dan sulit diakses oleh pihak tidak berwenang.

Otentikasi di Tingkat Aplikasi dan Perangkat:

a. **Otentikasi Perangkat:** Memverifikasi perangkat atau terminal yang digunakan pengguna untuk mengakses suatu layanan.
b. **Otentikasi Aplikasi:** Memastikan aplikasi yang digunakan oleh pengguna dapat dipercaya dan belumdimanipulasi.

Monitoring dan Analisis Otentikasi:

a. **Pemantauan Aktivitas Otentikasi:** Melacak dan memonitor aktivitas otentikasi untuk mendeteksi pola atau aktivitas mencurigakan.
b. **Analisis Risiko:** Menggunakan alat analisis risiko untuk menilai tingkat risiko otentikasi pada waktutertentu.

Pemulihan Akun yang Aman:

a. **Proses Pemulihan yang Aman:** Menetapkan prosedur yang aman untuk pemulihan akun jika pengguna lupa kata sandi atau menghadapi masalahotentikasi.

Otentikasi adalah garda pertama yang kokoh dalam menjaga keamanan informasi dan data sensitif. Dengan mengadopsi metode otentikasi yang cermat, organisasi dan individu dapat memastikan bahwa akses yang tidak sah diminimalkan, dan keamanan informasi terjaga dengan baik.

11.7 Manajemen Akses: Pengaturan Hak Aksesyang Tepat

Manajemen akses adalah tentang mengatur siapa yang memiliki akses ke aset digital Anda dan sejauh mana akses tersebut diberikan. Setiap pengguna atau anggota tim harus diberikan hak akses yang sesuai dengan peran dan tanggung jawab mereka. Ini memastikan bahwa hanya orang yang memerlukan akses yang dapat mengakses aset digital yang relevan. Dalam mengatur hak akses sebaiknya memperhatikanbeberapa hal berikut ini :

a. **Pengenalan Pengguna:** Setiap pengguna atau entitas yang mengakses sistem harus diidentifikasi secara unik.
b. **Otentikasi:** Proses verifikasi identitas pengguna atau entitas sebelum diberikan akses.
c. **Penetapan Hak Akses:** Menentukan hak akses yang sesuai dengan tugas atau tanggung jawab individu atauentitas.
d. **Pembaruan Secara Berkala:** Melakukan evaluasi dan pembaruan terhadap hak akses sesuai perubahan peran atau tanggung jawab.
e. **Model Kebutuhan Priciple (*Principle of Least Privilege* - PoLP):** Memberikan hak akses hanya yang diperlukan untuk melakukan tugas tertentu.
f. **Model Kebutuhan Priciple (*Need-to-Know Principle*):** Memberikan akses hanya kepada individuyang membutuhkan informasi tersebut untuk melaksanakan tugasnya.
g. **Pemisahan Tugas:** Memastikan bahwa tugas atau wewenang tertentu dipisahkan untuk mencegah penyalahgunaan akses.
h. **Prinsip Keempat Mata:** Sistem diatur sedemikian rupa sehingga satu entitas tidak memiliki hak aksespenuh.
i. **Pemantauan Aktivitas Akses:** Memonitor aktivitas

pengguna untuk mendeteksi pola atau tindakan yang mencurigakan.

j. **Audit Hak Akses:** Melakukan audit secara berkala terhadap hak akses untuk memastikan kepatuhan dengan kebijakan keamanan.

11.8 Monitoring dan Deteksi: MendeteksiAncaman Segera

Monitoring dan deteksi menjadi pilar penting dalam upaya menjaga keamanan informasi, memungkinkan organisasi untuk mengidentifikasi potensi serangan atau pelanggaran keamanan dengan segera. Proses ini melibatkan pemantauan aktivitas sistem dan jaringan, termasuk log aktivitas dan lalu lintas jaringan, dengan tujuan mendeteksi tanda-tanda awal ancaman khususnya yang mencurigakan atau tidak sah. Analisis log dan peristiwa dilakukan secara real-time, dengan korelasi peristiwa dari berbagai sumber untuk mengidentifikasi pola serangan yang mungkin terkait. Deteksi anomali menjadi fokus utama, baik dalam perilaku pengguna maupun aktivitas jaringan, dengan penggunaan algoritma untuk mengenali perubahan atau aktivitas yang tidak biasa.

Penerapan Sistem Deteksi Intrusi (IDS) dan Sistem Deteksi Ancaman (IPS) memberikan langkah proaktif dalam mendeteksi dan merespons ancaman. Sensor keamanan pada endpoint dan jaringan memperkuat upaya monitoring dengan fokus pada deteksi malware dan perilaku mencurigakan. Pengenalan tanda-tanda awal ancaman, seperti pola serangan atau tanda-tanda malware, menjadi kunci dalam upaya deteksi dini. Manajemen ancaman memainkan peran vital dengan memprioritaskan ancaman dan merespons dengan cepat untuk mengatasi potensi dampak dan kerentanan sistem.

11.9 Kesadaran dan Pelatihan: MengedukasiPengguna

Kesadaran dan pelatihan dalam konteks keamanan informasi menjadi aspek krusial dalam menjaga integritas, kerahasiaan, dan

ketersediaan data. Membangun kesadaran keamanan di kalangan pengguna adalah langkah awal untuk mencegah insiden keamanan yang disebabkan oleh kelalaian atau ketidaktahuan. Pelatihan rutin dan edukasi yang efektif membantu pengguna memahami risiko keamanan, mengidentifikasi tindakan yang dapat meningkatkan keamanan, dan memberikan dasar pengetahuan yang diperlukan untuk menghadapi ancaman siber.

a. **Pengenalan Risiko dan Ancaman:** Melibatkan pengguna dalam pemahaman risiko keamanan dan ancaman siber yang mungkin mereka hadapi. Ini mencakup pemahaman tentang phishing, malware, dan serangan siber lainnya yang dapat merugikan organisasi.
b. **Praktik Keamanan Umum:** Memastikan bahwa pengguna memahami dan menerapkan praktik keamanan umum, seperti pembuatan kata sandi yang kuat, menghindari klik tautan yang mencurigakan, dan memperbarui perangkat lunak secara teratur.
c. **Identifikasi Serangan Phishing:** Memberikan pelatihan khusus untuk mengenali serangan phishing, yang sering kali menjadi pintu masuk utama bagi ancaman siber. Pengguna perlu dapat membedakan email atau pesan palsu yang mencoba mendapatkaninformasi pribadi atau login.
d. **Tindakan dalam Kasus Serangan:** Menyediakan panduan yang jelas tentang tindakan yang harus diambil jika seorang pengguna menyadari atau mencurigai adanya serangan siber. Hal ini mencakup pelaporan kepada tim keamanan atau administrator sistem.
e. **Kebijakan Keamanan Organisasi:** Menyampaikan dan menjelaskan kebijakan keamanan organisasi kepada pengguna. Pengguna perlu memahami batasan dan kewajiban mereka dalam menjaga keamanan informasi organisasi.
f. **Pelatihan Menggunakan Simulasi:** Menggunakan simulasi serangan siber dalam pelatihan untuk memberikan pengalaman praktis kepada pengguna. Ini membantu mereka

merespons situasi nyata dan meningkatkan kemampuan mereka untuk menghadapiancaman.

g. **Kesadaran Mengenai Kebijakan Keamanan Data:** Memahamkan pengguna tentang kebijakan keamanan data, termasuk penggunaan data pribadi dan informasi bisnis yang sensitif. Kesadaran ini penting untuk melibatkan pengguna dalam upaya menjaga integritas dan kerahasiaan data.
h. **Pelatihan Berkelanjutan:** Menyelenggarakan pelatihan berkelanjutan secara rutin untuk menjaga kesadaran keamanan dan memperbarui pengguna tentang perkembangan terkini dalam ancaman siber. Pelatihan ini dapat disesuaikan dengan tren dan teknikserangan baru.
i. **Kesadaran akan Keamanan Mobile:** Menekankan pentingnya keamanan pada perangkat mobile, yang sering digunakan untuk mengakses data bisnis. Pengguna perlu memahami risiko dan praktik keamanan yang sesuai untuk perangkat mobile mereka.

Kesadaran dan pelatihan efektif bukan hanya tentang memberikan informasi tetapi juga memberikan keterampilan dan pemahaman yang mendalam kepada pengguna. Dengan membangun budaya keamanan yang kuat di seluruh organisasi, dapat diharapkan bahwa pengguna akan menjadi mitra aktif dalam menjaga keamanan informasi dan melawan ancaman siber.

BIODATA PENULIS

Alfian Zakaria, S.SI., M.T
Dosen Teknik Informatika
Fakultas Teknik Universitas Negeri Gorontalo

Penulis lahir di Gorontalo tanggal 20 Mei 1990. Penulis adalah dosen pada Program Studi Sistem Informasi Fakultas Teknik, Universitas Negeri Gorontalo. Menyelesaikan pendidikan S1 pada Jurusan Sistem Informasi Universitas Negeri Gorontalo dan melanjutkan S2 pada Teknik Infomatika Institut Teknologi Bandung. Penulis menekuni bidang pengembangan perangkat lunak dan keamanan informasi.