



# KEAMANAN DATA & INFORMASI

Keamanan Komputer ■  
Kejahatan Komputer ■  
Teknik Kriptografi ■  
Keamanan Web ■  
Keamanan Email ■  
Keamanan Jaringan Komputer ■  
Keamanan Sistem Operasi ■  
Keamanan Informasi ■  
Keamanan Komputer Secara Fisik ■  
Kode Etik Profesi IT & Cyber Law ■

Ika Yusnita Sari • Muttaqin • Jamaludin • Janner Simarmata  
M. Arif Rahman • Akbar Iskandar • Andrew Fernando Pakpahan  
Abdul Karim • Sugianto • Yo Ceng Giap • Hazriani  
Devi Yendrianof • Sardjana Orba Manullang





# KEAMANAN DATA & INFORMASI

- Keamanan Komputer ■
- Kejahatan Komputer ■
- Teknik Kriptografi ■
- Keamanan Web ■
- Keamanan Email ■
- Keamanan Jaringan Komputer ■
- Keamanan Sistem Operasi ■
- Keamanan Informasi ■
- Keamanan Komputer Secara Fisik ■

## UU 28 tahun 2014 tentang Hak Cipta

### Fungsi dan sifat hak cipta Pasal 4

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

### Pembatasan Perlindungan Pasal 26

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

- a. penggunaan kutipan singkat Ciptaan dan/atau produk Hak Terkait untuk pelaporan peristiwa aktual yang ditujukan hanya untuk keperluan penyediaan informasi aktual;
- b. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk kepentingan penelitian ilmu pengetahuan;
- c. Penggandaan Ciptaan dan/atau produk Hak Terkait hanya untuk keperluan pengajaran, kecuali pertunjukan dan Fonogram yang telah dilakukan Pengumuman sebagai bahan ajar; dan
- d. penggunaan untuk kepentingan pendidikan dan pengembangan ilmu pengetahuan yang memungkinkan suatu Ciptaan dan/atau produk Hak Terkait dapat digunakan tanpa izin Pelaku Pertunjukan, Produser Fonogram, atau Lembaga Penyiaran.

### Sanksi Pelanggaran Pasal 113

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

# **Keamanan Data dan Informasi**

Penulis:

Ika Yusnita Sari, Muttaqin, Jamaludin, Janner Simarmata  
M. Arif Rahman, Akbar Iskandar, Andrew Fernando Pakpahan  
Abdul Karim, Sugianto, Yo Ceng Giap, Hazriani  
Devi Yendrianof, Sardjana Orba Manullang

Penerbit Yayasan Kita Menulis



# Keamanan Data dan Informasi

Copyright © Yayasan Kita Menulis, 2020

Penulis:

Ika Yusnita Sari, Muttaqin, Jamaludin, Janner Simarmata  
M. Arif Rahman, Akbar Iskandar, Andrew Fernando Pakpahan  
Abdul Karim, Sugianto, Yo Ceng Giap, Hazriani  
Devi Yendrianof, Sardjana Orba Manullang

Editor: Ronal Watrianthos

Desain Sampul: Tim Kreatif Kita Menulis

Sampul: pexels.com

Penerbit

Yayasan Kita Menulis

Web: [kitamenulis.id](http://kitamenulis.id)

e-mail: [press@kitamenulis.id](mailto:press@kitamenulis.id)

WA: 0821-6453-7176

Ika Yusnita Sari, dkk.

Keamanan Data dan Informasi

Yayasan Kita Menulis, 2020

xiv; 188 hlm; 16 x 23 cm

ISBN: 978-623-6761-80-9

Cetakan 1, Desember 2020

- I. Keamanan Data dan Informasi
- II. Yayasan Kita Menulis

## Katalog Dalam Terbitan

Hak cipta dilindungi undang-undang

Dilarang memperbanyak maupun mengedarkan buku tanpa

izin tertulis dari penerbit maupun penulis

# Kata Pengantar

Dengan mengucapkan Puji Syukur kepada Tuhan Yang Maha Esa, kami persembahkan kemampuan yang ada pada kami dalam bentuk Buku Keamanan Data dan Informasi. Buku ini dibuat agar dapat membantu para mahasiswa bidang Teknik Informatika untuk mempelajari dan mengetahui tentang Keamanan Data dan Informasi serta ikut dalam meningkatkan mutu pendidikan di Indonesia sehingga meningkatkan pengetahuan kita dengan diterbitkannya buku ini.

Buku ini terdapat banyak materi dalam memahami hal-hal dalam keamanan data dan informasi di mana perkembangan teknologi komputer saat ini sangat berkembang pesat. Maka dibutuhkan suatu keamanan data dan informasi serta pengetahuan berbagai macam kejahatan-kejahatan yang ditimbulkan oleh pemanfaatan komputer yang salah penggunaannya.

Secara rinci buku ini membahas tentang :

Bab 1 Keamanan Komputer dan Kejahatan Komputer

Bab 2 Prinsip Dasar Keamanan Komputer

Bab 3 Cryptosystem dan Cryptography

Bab 4 Teknik Kriptografi

Bab 5 Keamanan Web

Bab 6 Keamanan Email

Bab 7 Keamanan Jaringan Komputer

Bab 8 Keamanan Sistem Operasi

Bab 9 Sistem Keamanan Informasi

Bab 10 Keamanan Komputer Secara Fisik

Bab 11 Evaluasi Keamanan Sistem Informasi

Bab 12 Kode Etik Profesi IT

Bab 13 Perspektif Cyber Law dan UU ITE Dalam Sistem Hukum Di Indonesia.



Akhir kata Kami Ucapkan terima kasih kepada semua teman-teman dan mahasiswa yang sudah memberikan umpan balik atas naskah yang kami persiapkan. Sehingga, hal tersebut menjadi cara agar pada bagian-bagian yang sulit dapat lebih mudah dipahami.

Meskipun demikian, kami menyadari bahwa di dalam penyusunan buku ini masih memiliki kekurangan yang membutuhkan perhatian. Oleh karena itu, kami akan sangat berterima kasih jika ada kritik dan saran untuk perbaikan kedepannya pada edisi yang akan datang.

Semoga buku ini dapat memberikan manfaat. Terima kasih

Kisaran, 18 November 2020  
Penulis

# Daftar Isi

|                      |      |
|----------------------|------|
| Kata Pengantar ..... | v    |
| Daftar Isi .....     | vii  |
| Daftar Gambar .....  | xi   |
| Daftar Tabel.....    | xiii |

## **Bab 1 Keamanan Komputer dan Kejahatan Komputer**

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| 1.1 Pendahuluan.....                                                    | 1  |
| 1.2 Definisi Keamanan Komputer.....                                     | 2  |
| 1.3 Aspek-Aspek Keamanan Komputer .....                                 | 3  |
| 1.4 Model Penyerangan Keamanan .....                                    | 4  |
| 1.5 Kejahatan Komputer .....                                            | 6  |
| 1.5.1 Faktor-Faktor Penyebab Kejahatan Komputer (Cybercrime) .....      | 7  |
| 1.5.2 Macam-Macam Kejahatan Komputer.....                               | 8  |
| 1.6 Definisi Cybercrime .....                                           | 9  |
| 1.6.1 Denial Of Service Attack / DOS Attack .....                       | 9  |
| 1.6.2 Hacking.....                                                      | 10 |
| 1.6.3 Menulis dan Menyebarkan Virus/Trojan .....                        | 10 |
| 1.6.4 Cyberterrorism .....                                              | 11 |
| 1.6.5 Fraud dan Pencurian Identitas / Phising (Carding, Spoofing) ..... | 11 |

## **Bab 2 Prinsip Dasar Keamanan Komputer**

|                                                       |    |
|-------------------------------------------------------|----|
| 2.1 Pendahuluan.....                                  | 13 |
| 2.2 Definisi Keamanan Komputer.....                   | 14 |
| 2.2.1 Kerahasiaan .....                               | 17 |
| 2.2.2 Integritas .....                                | 18 |
| 2.2.3 Ketersediaan .....                              | 18 |
| 2.3 Tantangan Keamanan Komputer .....                 | 19 |
| 2.4 Model untuk Keamanan Komputer .....               | 21 |
| 2.5 Teknologi dan Prinsip Keamanan Komputer .....     | 24 |
| 2.5.1 Kerahasiaan Dengan Enkripsi Simetris .....      | 24 |
| 2.5.2 Otentikasi Pesan Dan Fungsi Hash .....          | 26 |
| 2.5.3 Otentikasi Menggunakan Enkripsi Symmetric ..... | 27 |

**Bab 3 Cryptosystem dan Cryptography**

|                                     |    |
|-------------------------------------|----|
| 3.1 Pendahuluan.....                | 29 |
| 3.2 Cryptosystem .....              | 30 |
| 3.3 Cryptography .....              | 30 |
| 3.3.1 Definisi Cryptography .....   | 31 |
| 3.3.2 Sejarah Cryptography .....    | 32 |
| 3.3.3 Tujuan Cryptography.....      | 34 |
| 3.3.4 Klasifikasi Cryptography..... | 34 |
| 3.3.5 Keamanan Cryptography.....    | 37 |

**Bab 4 Teknik Kriptografi**

|                                         |    |
|-----------------------------------------|----|
| 4.1 Apa itu Kriptografi .....           | 39 |
| 4.2 Teknik Kriptografi.....             | 42 |
| 4.2.1 Teknik Watermarking .....         | 42 |
| 4.2.2 Steganografi .....                | 46 |
| 4.3 Kriptografi Klasik dan Modern ..... | 48 |

**Bab 5 Keamanan Web**

|                                 |    |
|---------------------------------|----|
| 5.1 Pendahuluan.....            | 51 |
| 5.2 Keamanan Web .....          | 53 |
| 5.3 Metode Penyerangan Web..... | 55 |
| 5.4 Metode Pertahanan Web.....  | 57 |
| 5.4.1 Keamanan melalui XML..... | 59 |
| 5.4.2 Web Service .....         | 60 |

**Bab 6 Keamanan Email**

|                                                                                            |    |
|--------------------------------------------------------------------------------------------|----|
| 6.1 Pendahuluan.....                                                                       | 63 |
| 6.2 Memahami Keamanan Email.....                                                           | 64 |
| 6.3 Jenis Kejahatan Lewat Email .....                                                      | 67 |
| 6.3.1 Spoofing email .....                                                                 | 67 |
| 6.3.2 Mengirim Kode Berbahaya Melalui Email Seperti Virus.....                             | 68 |
| 6.3.3 Mengirim Email Mengancam .....                                                       | 69 |
| 6.3.4 Catfishing.....                                                                      | 69 |
| 6.3.5 Bom Email.....                                                                       | 69 |
| 6.3.6 Email Fitnah .....                                                                   | 69 |
| 6.3.7 Penipuan email .....                                                                 | 70 |
| 6.4 Strategi Keamanan Email Efektif.....                                                   | 70 |
| 6.4.1 Kembangkan Keamanan Email Sesuai Perkembangan IT .....                               | 71 |
| 6.4.2 Manfaatkan Multifactor Authentication (MFA) dan Mobile Device Management (MDM) ..... | 72 |
| 6.4.3 Bagaimana Phishing Terjadi? .....                                                    | 74 |



**Bab 7 Keamanan Jaringan Komputer**

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 7.1 Pendahuluan.....                                                 | 77 |
| 7.2 Ancaman, Kerentanan, Serangan di Jaringan Komputer .....         | 76 |
| 7.2.1 Virus .....                                                    | 76 |
| 7.2.2 Worm .....                                                     | 77 |
| 7.2.3 Trojan Horses .....                                            | 77 |
| 7.2.4 Port Scanning.....                                             | 77 |
| 7.2.5 Spoofing.....                                                  | 77 |
| 7.2.6 DNS poisoning .....                                            | 78 |
| 7.2.7 Sniffing .....                                                 | 79 |
| 7.2.8 Denial of Service .....                                        | 79 |
| 7.3 Metode Proteksi .....                                            | 81 |
| 7.3.1 Kontrol Akses .....                                            | 81 |
| 7.3.2 Autentikasi .....                                              | 82 |
| 7.3.3 Kerahasiaan .....                                              | 82 |
| 7.3.4 Integritas.....                                                | 83 |
| 7.4 Mengamankan Jaringan Komputer.....                               | 83 |
| 7.4.1 Mengamankan Perangkat Keras .....                              | 83 |
| 7.4.2 Mengamankan Perangkat Lunak .....                              | 84 |
| 7.4.3 Firewall .....                                                 | 84 |
| 7.4.4 Network Intrusion Detection dan Network Intrusion Prevention.. | 85 |

**Bab 8 Keamanan Sistem Operasi**

|                                             |    |
|---------------------------------------------|----|
| 8.1 Sistem Operasi .....                    | 87 |
| 8.2 Fungsi Sistem Operasi.....              | 88 |
| 8.3 Jenis - Jenis Sistem Operasi .....      | 89 |
| 8.3.1 Sistem Operasi Berbasis Dekstop ..... | 89 |
| 8.4 Keamanan .....                          | 95 |
| 8.5 Keamanan Sistem Operasi .....           | 98 |
| 8.6 Meningkatkan Keamanan Komputer.....     | 99 |

**Bab 9 Sistem Keamanan Informasi**

|                                                          |     |
|----------------------------------------------------------|-----|
| 9.1 Definisi Keamanan Informasi.....                     | 103 |
| 9.2 Aspek Keamanan Sistem Informasi.....                 | 104 |
| 9.3 Mengapa Keamanan Informasi Sangat Diperlukan ? ..... | 106 |
| 9.4 Dasar-dasar Keamanan Sistem Informasi.....           | 110 |

## **Bab 10 Keamanan Komputer Secara Fisik**

|                                  |     |
|----------------------------------|-----|
| 10.1 Pendahuluan.....            | 113 |
| 10.2 Sisi Lingkungan .....       | 114 |
| 10.3 Sisi Manajemen .....        | 117 |
| 10.4 Sisi Fisika dan Kimia ..... | 119 |
| 10.5 Sisi Perangkat Keras.....   | 121 |

## **Bab 11 Evaluasi Keamanan Sistem Informasi**

|                                                               |     |
|---------------------------------------------------------------|-----|
| 11.1 Pendahuluan.....                                         | 123 |
| 11.2 Keamanan Sistem Informasi .....                          | 124 |
| 11.2.1 Statistik Keamanan Sistem Informasi .....              | 126 |
| 11.2.2 Jenis Ancaman Keamanan Informasi.....                  | 128 |
| 11.2.3 Tipe Serangan Terhadap Keamanan Sistem Informasi ..... | 129 |
| 11.2.4 Sumber Lubang Keamanan (Security Hole) .....           | 130 |
| 11.2.5 Mengamankan Sistem Informasi.....                      | 130 |
| 11.3 Evaluasi Keamanan Sistem Informasi .....                 | 131 |
| 11.3.1 Cara Pengujian Keamanan Sistem Informasi.....          | 132 |
| 11.3.2 Kriteria Evaluasi Keamanan Sistem Informasi .....      | 133 |

## **Bab 12 Kode Etik Profesi IT**

|                                                      |     |
|------------------------------------------------------|-----|
| 12.1 Pentingnya Kode Etik Profesi IT .....           | 135 |
| 12.2 Sejarah dan Perkembangan Etika Profesi IT ..... | 136 |
| 12.3 Pengertian Kode Etik Profesi .....              | 137 |
| 12.4 Tujuan dan Fungsi Kode Etik Profesi.....        | 138 |
| 12.5 Prinsip Dasar Kode Etik Profesi.....            | 139 |
| 12.6 Organisasi Profesi IT Indonesia .....           | 141 |
| 12.6.1 Komunitas IT di Indonesia.....                | 144 |
| 12.7 Organisasi Profesi IT Internasional.....        | 145 |
| 12.8 Kode Etik Profesi Bidang IT .....               | 148 |

## **Bab 13 Perspektif Cyber Law dan UU ITE Dalam Sistem Hukum Di Indonesia**

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| 13.1 Pendahuluan.....                                                    | 151 |
| 13.2 Cyber Law dan Undang-Undang Informasi dan Transaksi Elektronik..... | 153 |
| 13.2.1 Pengertian Cyber Law .....                                        | 153 |
| 13.3 Teori Sistem Hukum .....                                            | 159 |
| 13.4 Contoh Kasus Cyber Law di Indonesia .....                           | 161 |
| 13.5 Kesimpulan.....                                                     | 162 |
| Daftar Pustaka .....                                                     | 165 |
| Biodata Penulis .....                                                    | 229 |

# Daftar Gambar

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| Gambar 2.1: Triad Persyaratan Keamanan .....                        | 15  |
| Gambar 2.2: Triad Persyaratan Keamanan .....                        | 23  |
| Gambar 2.3: Model Enkripsi Simetris yang Disederhanakan .....       | 25  |
| Gambar 3.1: Skema kriptografi kunci simetris.....                   | 35  |
| Gambar 3.2: Skema kriptografi kunci asimetris .....                 | 37  |
| Gambar 4.1: Public Key Encryption .....                             | 40  |
| Gambar 4.2: Private Key Encryption .....                            | 41  |
| Gambar 4.3: Proses Watermarking .....                               | 44  |
| Gambar 4.4: Steganografi Citra .....                                | 47  |
| Gambar 5.1: Gambar alur akses web .....                             | 52  |
| Gambar 5.2: Gambar ilustrasi ancaman keamanan web .....             | 53  |
| Gambar 5.3: Gambar ilustrasi server side attack .....               | 57  |
| Gambar 5.4: Gambar Penerapan Cyber Security .....                   | 59  |
| Gambar 5.5: Gambar Ilustrasi Web Service .....                      | 60  |
| Gambar 7.1: Jaringan Komputer Dengan Firewall .....                 | 85  |
| Gambar 8.1: Ms Dos .....                                            | 89  |
| Gambar 8.2: Windows .....                                           | 89  |
| Gambar 8.3: MacOS .....                                             | 90  |
| Gambar 8.4: Linux.....                                              | 90  |
| Gambar 8.5: UNIX .....                                              | 91  |
| Gambar 8.6: Android .....                                           | 93  |
| Gambar 8.7: iOS .....                                               | 93  |
| Gambar 8.8: Symbian .....                                           | 94  |
| Gambar 8.9: Symbian.....                                            | 94  |
| Gambar 8.10: Blackberry .....                                       | 95  |
| Gambar 9.1: Elemen-elemen keamanan informasi .....                  | 105 |
| Gambar 10.1: Gempa bumi.....                                        | 116 |
| Gambar 11.1: The Security Triad .....                               | 126 |
| Gambar 11.2: Perbandingan Kasus Vulnerability pada Tahun 2019 ..... | 127 |
| Gambar 11.3: Perbandingan Rata-rata Waktu Pemulihan .....           | 127 |



# Daftar Tabel

|                                                |    |
|------------------------------------------------|----|
| Tabel 2.1: Terminologi Keamanan Komputer ..... | 21 |
|------------------------------------------------|----|





# **Bab 1**

## **Keamanan Komputer dan Kejahatan Komputer**

### **1.1 Pendahuluan**

Perkembangan teknologi informasi merupakan media yang efektif dalam menghasilkan dan memperluas informasi yaitu dengan menggunakan media teknologi komputer dalam bisnis. Oleh karena itu, komputer merupakan hal yang dibutuhkan manusia dan berperan penting dalam berbagai macam manfaat. Salah satu nya yaitu, dapat digunakan oleh banyak ahli untuk mengakses komputer bertukar file, kirim email, namun komputer tidak hanya sebatas melakukan hal tersebut. Komputer mampu menghasilkan sistem informasi secara global yang membuat dunia semakin kecil (Yanti dkk, 2017). Dengan adanya teknologi informasi komputer sebagai media dalam bertukar informasi maka dibutuhkan suatu keamanan untuk menjaga kerahasiaan informasi.

Keamanan merupakan bagian terpenting dalam sistem informasi karena informasi hanya diserahkan pada bagian golongan tertentu. Jadi, pentingnya melakukan pencegahan agar tidak salah dipergunakan oleh golongan-golongan yang tidak memiliki hak dalam kepentingan (Situmorang, 2016). Oleh karena itu dibutuhkan suatu keamanan komputer agar informasi dapat terjaga dengan

baik. Keamanan komputer adalah sesuatu yang berguna sehingga perlu diamati dalam berkembang pesatnya dunia internet. Dunia internet adalah jaringan global yang dipublikasikan kepada umum. Jaringan internet terdapat berbagai jenis dampak baik dan buruk. Disebabkan jaringan internet merupakan lintasan informasi yang sangat efisien. Dikarenakan saat ini jaringan komputer menjadi tren maka dibutuhkan keamanan untuk mencegah sesuatu yang tidak baik dari jaringan internet. Dengan cara selalu hati-hati dan teliti dalam menempati dan memahami sesuatu dari internet dan selalu mengawasi kerahasiaan dan memakai Anti virus agar melindungi sistem komputer yang dimiliki dan berbagai teknik untuk menangkal sesuatu yang akan terjadi saat melancarkan kegiatan menggunakan koneksi internet seperti menembusnya berbagai jenis virus antara lain adware, spyware, malware dan lain-lain ke dalam komputer dan mengamati semua kegiatan surfing dalam dunia internet (Hermawan, 2016). Dengan adanya keamanan komputer maka dapat memberikan perlindungan terhadap kemungkinan yang timbul dari berbagai macam kejahatan komputer.

## 1.2 Definisi Keamanan Komputer

Komputer adalah barang teknologi terpenting yang diperlukan. Sebagian kalangan masyarakat, secara langsung atau tidak langsung ikut menggunakan komputer. Hampir kalangan masyarakat tampaknya melihat komputer dari wujud yang nyata yaitu persegi dan mempunyai monitor, tetapi pada dasarnya komputer memiliki dua buah perangkat utama meliputi perangkat keras (hardware) dan perangkat lunak (software). Komponen dari hardware yaitu monitor, keyboard, mouse dan Central Processing Unit (CPU) yang terdiri dari komponen motherboard, VGA card, processor, harddisk, RAM serta power supply. Sementara pada unit Software memuat program pendukung seperti Operating System (OS) dan perangkat lunak lainnya.

Persoalan keamanan adalah sesuatu sudut pandang yang perlu dari sistem informasi. Kadang-kadang posisi keamanan diletakan di posisi kedua bahkan diposisikan terakhir dalam susunan masalah yang dianggap penting. Jika mengganggu kinerja sistem, kadang-kadang keamanan dikurangi atau dihilangkan. Terkoneksinya LAN atau komputer ke internet memberikan peluang adanya lubang keamanan yang sebelumnya dapat ditutup dengan prosedur keamanan secara fisik. Hal ini merupakan pandangan bahwa

mudahnya dalam akses informasi terbalik dengan tingkat keamanan sistem informasi tersebut.

Keamanan informasi yaitu bagaimana seseorang dapat mencegah penipuan atau menemukan adanya penipuan di suatu sistem berbasis informasi, yang mana informasi tersebut tidak mempunyai arti fisik. Keamanan komputer dipakai untuk memantau risiko yang berkaitan dengan pemakaian komputer. Keamanan komputer tersebut artinya yaitu keamanan sebuah komputer yang terkoneksi ke dalam sebuah jaringan (Internet) (Hartiwati, 2014). Arti mengenai keamanan komputer memiliki banyak makna, dapat dilihat dari pengertian keamanan komputer menurut para ahli, yaitu:

1. Menurut Howard (1997) dalam bukunya “An analysis of security incidents on the internet” mengungkapkan bahwa: “Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab” (Hasibuan, 2016).
2. Menurut Gollmann (1999) dalam bukunya “Computer Security” mengungkapkan bahwa: “Keamanan komputer adalah berhubungan dengan pencegahan diri dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer”.

## 1.3 Aspek-Aspek Keamanan Komputer

Keamanan komputer memiliki delapan aspek yang terdiri dari (Hasibuan, 2016):

1. *Authentication* yaitu penerima informasi menentukan aslinya pesan, yang masuk dari seseorang yang dimintai informasi. Istilahnya, informasi tersebut masuk dari orang yang dikehendaki.
2. *Integrity* merupakan keotentikan sebuah pesan yang dikirim melalui jaringan dan dipastikan bahwa informasi yang dikirim tidak diubah orang yang tidak memiliki hak akses.
3. *Non-repudiation* yaitu sesuatu yang berhubungan dengan si pengirim. Pengirim tidak dapat menghindar bahwa dialah yang mengirim informasi itu.

4. *Authority*, adalah informasi yang ada pada sistem jaringan tidak dapat diubah oleh bagian yang memiliki hak aksesnya.
5. *Confidentiality* adalah cara dalam melindungi informasi dari seseorang yang tidak memiliki hak akses. Kerahasiaan ini berkaitan dengan informasi yang diperoleh ke pihak lain.
6. *Privacy*, merupakan sesuatu yang berkaitan dengan hal yang bersifat pribadi
7. *Availability*, adanya bagian yang berkaitan dengan kecepatan informasi saat diinginkan. Sistem informasi yang diserang atau dibobol dapat menghalangi atau menolak akses ke informasi.
8. *Access Control*, aspek ini berkaitan dengan aturan hak akses ke informasi. Sehingga seringkali berkaitan dengan suatu permasalahan kerahasiaan dan privasi. Maka dilakukannya pengontrolan dalam pengaksesan dengan digunakannya penggabungan user id dan Password Id atau cara lain.

Cara meningkatkan keamanan komputer dengan melakukan tindakan mencegah yaitu dengan cara memakai penggunaan Password untuk mencegah kemungkinan pemakai yang tidak memiliki hak akses terhadap data (confidentiality) dan mencegah data tidak dimanipulasi (integrity) dan memberi authentication pada pihak yang memiliki hak akses data (Pratiwi dan Atmojo, 2016).

## 1.4 Model Penyerangan Keamanan

Penyerangan di dalam keamanan memiliki beberapa model. Menurut Stalling (1995), model penyerangan keamanan meliputi:

1. *Interruption*, yaitu perangkat sistem yang membuat rusak atau tidak ada. Serangan ini disampaikan kepada ketersediaan (Availability) dari sistem.
2. *Interception* merupakan seseorang yang tidak berhak sukses dalam masuk ke dalam aset atau informasi.

3. *Modification*, adalah seseorang yang tidak berhak tidak saja berhasil mengakses, namun dapat melakukan perubahan aset.
4. *Fabrication* yaitu seseorang yang tidak berhak melakukan penyisipan suatu objek palsu ke dalam sistem

Pada dasarnya sistem keamanan komputer mempunyai lima macam keamanan komputer yang membentengi sistem keamanan komputer meliputi (Dhika dan Hanipah, 2020):

1. Keamanan Fisik. Jenis keamanan ini didukung dengan perangkat keras. Tujuannya adalah dapat menjaga perangkat keras agar keadaan menjadi stabil dan dapat dipakai dalam mengerjakan operasi jaringan.
2. Keamanan Jaringan. Keamanan jaringan adalah sesuatu yang masih hipotesis . Hal ini diakibatkan jenis keamanan dilaksanakan oleh barang yang tidak dapat dilihat, yang memakai Software ataupun perintah yang lain. Misalnya, seperti keamanan jaringan adalah dengan memakai proxy dan firewall untuk mengerjakan filter pada user yang akan memakai akses dalam jaringan.
3. Otorisasi Akses. Jenis keamanan jaringan atau otorisasi akses adalah keamanan jaringan dengan memakai Password atau kunci, saat mengkoneksikan perangkat dalam jaringan. Ini dikerjakan supaya administrator dapat memberikan batasan akses kepada User yang telah dipilih saja yang dapat terkoneksi pada jaringan.
4. Proteksi Virus. Virus dapat mengerjakan metode penyerangan pada sistem komputer dengan memakai program, dan membuat sistem yang terdapat di dalam komputer menjadi berubah dan membuat rusak sistem. Sehingga membutuhkan penanganan terhadap serangan virus, dapat memakai atau instal Software anti virus pada komputer sehingga dilakukan update dengan database baru.
5. Penanganan rencana. Penanganan Rencana adalah tahap-tahap yang wajib dipilih jika terjadi bencana yang mengakibatkan rusaknya dan hilangnya data penting pada seluruh sistem jaringan komputer. Perencanaan bencana ini mempunyai tujuan agar saat terjadinya rusaknya pada sistem dapat dengan efisien terselesaikan.

Keamanan dalam sistem komputer memiliki pengaruh pada berbagai macam faktor yang terdiri dari (Harliana, Perdana dan Prasetyo,2008) :

1. *Social engineering*
2. Security hole pada sistem operasi dan servis
3. Keamanan fisik
4. Serangan pada jaringan
5. DOS attack
6. Serangan via aplikasi berbasis web
7. *Trojan, backdoor, rootkit, keylogger*
8. *Virus, worm- Anatomy of A Hack*

Di dalam komputer terdapat suatu data penting atau rahasia yang perlu dijaga maka hal tersebut membutuhkan suatu keamanan komputer. Alasan membutuhkan keamanan komputer akan lebih dijelaskan sebagai berikut (Wirdasari,2008):

1. Information-Based Society, alasan ini dikarenakan nilai informasi mempunyai nilai yang penting dan kinerja dalam proses dituntut serta menyajikan informasi dengan efisien dan nilai akurat menjadi sangat penting untuk suatu organisasi
2. Infrastruktur jaringan komputer, misalnya LAN dan internet, mengharuskan untuk menyajikan informasi secara efisien, bersamaan membuka kemungkinan terdapatnya lubang keamanan (security hole)

## 1.5 Kejahatan Komputer

Populernya aksi kejahatan yang berkaitan dengan pemakaian teknologi yang berbasis komputer dan jaringan telekomunikasi yang berkembang menjadikan banyaknya golongan pemakai jaringan telekomunikasi menjadi khawatir. Berbagai macam kejahatan atau ancaman (threats) diklasifikasikan dalam berbagai bentuk sesuai dengan teknik yang jelas (Abidin, 2015).

Menurut Hamzah (2004) menuliskan dalam buku yang judulnya *Aspek-aspek Pidana di Bidang Komputer*”, mendefinisikan kejahatan komputer sebagai: berbagai kegiatan yang ilegal dengan menggunakan komputer untuk tindakan

pidana. Sekecil apapun pengaruh yang muncul dari pemakaian komputer yang modern (Hasibuan, 2016).

Kejahatan komputer mengalami peningkatan dikarenakan (Wirdasari, 2008):

1. Aplikasi bisnis yang berbasis IT dan jaringan komputer yang mengalami peningkatan yang meliputi online banking, e-commerce, Electronic data Interchange (EDI).
2. Desentralisasi server.
3. Transisi dari single vendor menjadi sulti Vendor.
4. Naiknya kinerja pengguna (user).
5. Kesulitan pendiri hukum dan tidak adanya ketetapan yang benar
6. Bertambah rumitnya sistem yang dipakai, bertambahnya meningkatnya *source code* program yang dipakai.
7. Berkaitan dengan internet.

### 1.5.1 Faktor-Faktor Penyebab Kejahatan Komputer (Cybercrime)

Beberapa faktor yang menyebabkan kejahatan komputer yang semakin berkembang meliputi (Hasibuan, 2016):

1. Jalan masuknya Internet yang tidak memiliki batas.
2. Kecerobohan pemakai komputer. Hal ini adalah penyebab utama kejahatan komputer.
3. Tidak sulit dilakukan dengan ancaman keamanan yang kecil dan tidak dibutuhkan perlengkapan yang sangat canggih. Meskipun kejahatan komputer tidak sulit untuk dijalankan namun akan sangat sulit untuk mencarinya. Jadi, hal ini memaksa para pelaku kejahatan untuk terus menjalankan hal tersebut.
4. Para pelaku adalah sebagian kalangan yang cerdas, memiliki keinginan penasaran yang tinggi dan mengerti terhadap teknologi komputer.
5. Sistem keamanan jaringan yang tidak kuat
6. Tidak adanya kepedulian masyarakat. Masyarakat dan pendiri hukum sekarang memberikan kepedulian yang tinggi pada kejahatan



konvensional. Pada faktanya para pelaku kejahatan komputer masih menjalankan tindakan kejahatan tersebut.

7. Tidak terbentuknya Undang- Undang atau Hukum yang mengatur mengenai kejahatan komputer.

### 1.5.2 Macam-Macam Kejahatan Komputer

Macam-macam bentuk kejahatan komputer yang terdiri dari (Hasibuan, 2016):

1. **Illegal Access/Akses Tanpa ijin ke Sistem Komputer.** Dengan sengaja dan tanpa izin mengakses pada semua atau separuh dari sistem komputer dalam arti untuk memperoleh data komputer maupun tujuan-tujuan yang buruk dan berhubungan dengan sistem komputer yang dikaitkan pada sistem komputer lainnya. Penyusupan adalah bagian dari kejahatan yang sering dilakukan.
2. **Illegal Content/ Konten yang Ilegal atau melanggar hukum** yang artinya masuknya suatu data atau informasi ke Internet mengenai berita yang tidak benar dan dinilai telah melakukan pelanggaran hukum.
3. **Data Forgery/ Pemalsuan Data** adalah kejahatan dengan meniru data pada file-file penting pada tempat penyimpanan sebagai scriptless document melalui internet. Kejahatan tersebut ditargetkan pada file-file e-commerce dengan merekayasa seakan-akan membuat kesalahan pada pengetikan yang hasilnya akan memberikan keuntungan pada penyusup.
4. **Spionase Cyber/ Mata-mata** adalah kejahatan yang menggunakan jaringan internet dengan untuk melancarkan aktivitas mata-mata pada sasaran dengan melibatkan sistem jaringan komputer pada target.
5. **Data Theft / Mengambil data.** Aktivitas ini mendapatkan data komputer dengan tidak sah.
6. **Misuse Of Devices / memanipulasi Perlengkapan komputer** dengan niat sengaja dan tidak memiliki izin akses melakukan berbagai kegiatan produksi, jual, memakai dan menyebarkan untuk keperluan tersebut.

Kejahatan komputer dikaitkan dengan yang dikenal dengan istilah hacker yang memiliki arti yang tidak baik. Hacker merupakan pekerja di suatu perusahaan yang setia dan perusahaan sangat mempercayainya dan orang tersebut tidak perlu melakukan kejahatan komputer. Para Hacker tersebut merupakan orang-orang yang tergiur pada lubang-lubang yang ada pada sistem komputer. Oleh karena itu, kesempatan adalah faktor utama para Hacker menjadi penjahat cyber (Arifah, 2011).

## 1.6 Definisi Cybercrime

Cybercrime adalah istilah yang dipakai untuk mendeskripsikan kegiatan kejahatan yang memakai media komputer maupun internet. Kegiatan-kegiatan kejahatan ini sudah mempunyai hukum yang mana di negara-negara masih sebagian terdapat perdebatan mengenai bentuk dan status hukumnya. Pengertian ini dapat didefinisikan bahwa cybercrime suatu aktivitas yang menggunakan komputer atau internet sebagai media atau tujuan kejahatan.

Aktivitas yang dapat dikategorikan menjadi aktivitas kejahatan komputer atau dunia maya (Cybercrime) terdiri dari (Murti, 2005):

1. Melancarkan Denial of Service Attack / DOS Attack
2. Hacking
3. Menulis dan menyebarkan virus /trojan
4. Cyberterrorism
5. Fraud dan Pencurian Identitas/ Phising (meliputi Carding dan Spoofing)

### 1.6.1 Denial Of Service Attack / DOS Attack

*Denial of Service Attack / DOS Attack* merupakan suatu serangan pada suatu sistem komputer atau jaringan yang mengakibatkan jaringan atau sistem itu sendiri tidak dapat berfungsi seperti email, web dan sebagainya. Tindakan kejahatan DOS melancarkan aksi kejahatannya dengan menyerang bandwidth yang terdapat di jaringan atau dengan mengirimkan berita palsu pada system secara terus-menerus yang akhirnya system akan menjadi *overloading*.

Aksi dalam meluncurkan DOS dengan mencoba banyak cara, namun secara umum dapat dikelompokkan menjadi 3 kelompok, yang terdiri dari:

1. Menghabiskan sumber daya komputer/jaringan, contohnya *bandwidth*, *disk space* atau CPU Time
2. Merusak informasi konfigurasi jaringan contohnya informasi routing
3. Merusak secara fisik/ perangkat keras pada komponen jaringan

### 1.6.2 Hacking

Hacker adalah istilah yang dipakai untuk mendeskripsikan sebagian tipe kecerdasan di komputer. Di Dalam media massa dan opini orang banyak ditimbulkan oleh tulisan di media massa, selain itu Hacker dapat diartikan sebagai kejahatan komputer. Namun sebenarnya yang terjadi yaitu Hacker adalah programmer yang pandai di bidang keamanan komputer. Hacker dapat didefinisikan suatu pengakuan pada orang yang mempunyai keahlian dan pemahaman yang di atas rata-rata orang pada umumnya dalam ilmu pengetahuan komputer.

### 1.6.3 Menulis dan Menyebarluaskan Virus/Trojan

Virus Komputer merupakan program komputer yang melakukan aplikasikan diri dan penyalurannya dengan proses melakukan infeksi terhadap file program binary atau file dokumen. Dan bila hal itu tersalurkan dibuka dan dieksekusi akan terjadi maka terotomatis virus akan aktif di dalam komputer yang membuka atau menjalankan program tersebut. Untuk menciptakan virus saat ini tidak sulit, karena sudah terdapat program yang dirancang dengan target dapat memperoleh virus. Contohnya, *VBS Worm Generator* yang berarti seseorang tidak lagi kesulitan dalam mempelajari program untuk menciptakan virus dikarenakan semua sudah tersedia dan hanya memakai program yang sudah dapat menciptakan virus.

Trojan adalah suatu program yang seakan-akan adalah program yang bagus, namun mempunyai kode-kode program yang sangat bahaya. Apabila kode-kode program itu diproses akan mengakibatkan sistem komputer menjadi rusak atau mengakibatkan back door yang digunakan oleh orang yang mengirimkan trojan itu. Jadi, si pengirim trojan bisa masuk ke sistem komputer dan meluncurkan berbagai tindakan yang diinginkan.

### 1.6.4 Cyberterrorism

*Cyberterrorism* merupakan aktivitas yang memakai jaringan komputer atau internet sebagai media melancarkan terorisme. Dengan semakin berkembang pesatnya internet dan teknologi komputer hingga sekarang, oleh karena itu berkembangnya hal ini digunakan untuk melakukan aktivitas terorisme. Contohnya menyalurkan virus/trojan yang berbahaya, menjalankan DOS pada sistem tersebut hingga akhirnya membuat terhenti sementara, sabotase pada media atau infrastruktur jaringan komputer dan data yang telah disimpan di server tempat lawan dari teroris dan lainnya. Hal ini menjadikan ancaman yang sangat perlu diperhatikan jika tidak diawali diantisipasi saat ini, disebabkan dalam internet/jaringan komputer tidak mudah untuk mengawasi seluruh pihak yang melakukan kegiatan di dalam jaringan.

### 1.6.5 Fraud dan Pencurian Identitas / Phising (Carding, Spoofing)

Dunia komputer, Phising (Carding, Spoofing) adalah aktivitas yang mencuri informasi penting contohnya password, nama user, nomor kartu kredit dan lainnya oleh seorang yang tidak mempunyai hak akses. Salah satu teknik yang dipakai yaitu memakai email, yang mana melewati email dikirim informasi yang seakan-akan dari orang-orang yang terpercaya untuk mendapatkan data-data dari korban karena saat korban dengan mudah mempercayainya maka korban dengan cepat memberikan data yang penting ke orang pengirim email. Bentuk email yang selalu dikirim yaitu penawaran yang menarik perhatian korban sehingga korban langsung percaya saat diminta untuk mengirim data yang penting atau pengumuman bahwa sistem yang digunakan korban sedang mengalami masalah sehingga administrator memerlukan data dari pelanggan sistem tersebut atau bisa juga dengan melewati website untuk mudah memperoleh data (Murti, 2005).



## **Bab 2**

# **Prinsip Dasar Keamanan Komputer**

## **2.1 Pendahuluan**

Kami mulai dengan diskusi tentang apa yang kami maksud dengan keamanan komputer. Intinya, keamanan komputer berkaitan dengan aset terkait komputer yang tunduk pada berbagai ancaman dan berbagai tindakan diambil untuk melindungi aset tersebut (Stallings and Bauer, 2012). Oleh karena itu, bagian selanjutnya memberikan gambaran singkat tentang kategori aset terkait komputer yang ingin dipertahankan dan dilindungi oleh pengguna dan manajer sistem, dan melihat berbagai ancaman dan serangan yang dapat dilakukan pada aset tersebut.

Ada tiga pertanyaan mendasar terkait dengan keamanan:

1. Aset apa yang perlu kita lindungi?
2. Bagaimana aset tersebut terancam?
3. Apa yang dapat kita lakukan untuk melawan ancaman tersebut?

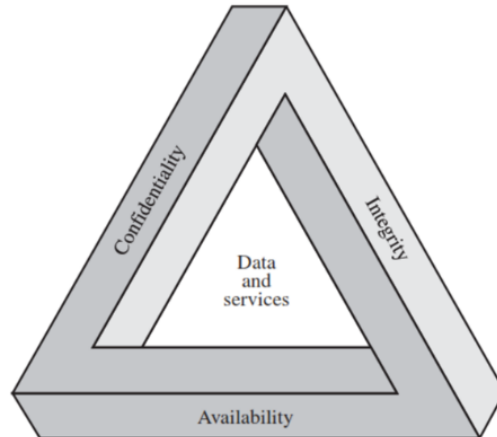
## 2.2 Definisi Keamanan Komputer

Keamanan komputer merupakan perlindungan yang diberikan pada sistem informasi otomatis untuk mencapai tujuan yang berlaku untuk menjaga integritas, ketersediaan, dan kerahasiaan sumber daya sistem informasi (termasuk perangkat keras, perangkat lunak, *firmware*, informasi / data, dan telekomunikasi).

Definisi ini memperkenalkan tiga tujuan utama yang menjadi inti dari keamanan komputer (Stallings and Bauer, 2012):

1. Kerahasiaan: istilah ini mencakup dua konsep terkait:
  - a. Kerahasiaan Data: Menjamin bahwa informasi pribadi atau rahasia tidak tersedia atau diungkapkan kepada individu yang tidak berwenang.
  - b. Privasi: Menjamin bahwa individu mengontrol atau memengaruhi informasi yang terkait dengan mereka yang dapat dikumpulkan dan disimpan dan oleh siapa dan kepada siapa informasi tersebut dapat diungkapkan.
2. Integritas: Istilah ini mencakup dua konsep terkait:
  - a. Integritas Data: Menjamin bahwa informasi dan program diubah hanya dengan cara yang ditentukan dan diotorisasi.
  - b. Integritas Sistem: Menjamin bahwa sistem melakukan fungsi yang dimaksudkan dengan cara yang tidak terganggu, bebas dari manipulasi sistem yang disengaja atau tidak disengaja.
3. Ketersediaan: Menjamin bahwa sistem bekerja dengan segera dan layanan tidak ditolak untuk pengguna yang berwenang.

Ketiga konsep ini membentuk apa yang sering disebut sebagai triad CIA (Gambar 2.1). Ketiga konsep tersebut mewujudkan tujuan keamanan fundamental untuk data dan untuk layanan informasi dan komputasi. Misalnya, standar NIST FIPS 199 (Standar untuk Kategorisasi Keamanan dari Sistem Informasi dan Informasi Federal) mencantumkan kerahasiaan, integritas, dan ketersediaan sebagai tiga tujuan keamanan untuk informasi dan untuk sistem informasi. FIPS PUB 199 memberikan karakterisasi yang berguna dari ketiga tujuan ini dalam hal persyaratan dan definisi kehilangan keamanan di setiap kategori:



**Gambar 2.1:** Triad Persyaratan Keamanan (Stallings and Bauer, 2012)

- **Kerahasiaan:** Menjaga pembatasan resmi atas akses dan pengungkapan informasi, termasuk cara untuk melindungi privasi pribadi dan informasi hak milik. Hilangnya kerahasiaan adalah pengungkapan informasi yang tidak sah.
- **Integritas:** Menjaga dari modifikasi atau kerusakan informasi yang tidak patut, termasuk memastikan informasi non-penyangkalan dan keaslian. Kehilangan integritas adalah modifikasi yang tidak sah atau penghancuran informasi.
- **Ketersediaan:** Memastikan akses dan penggunaan informasi yang tepat waktu dan dapat diandalkan. Hilangnya ketersediaan adalah terganggunya akses atau penggunaan informasi atau sistem informasi.

Meskipun penggunaan triad CIA untuk menentukan tujuan keamanan telah ditetapkan dengan baik, beberapa di bidang keamanan merasa bahwa konsep tambahan diperlukan untuk menyajikan gambaran yang lengkap. Dua dari yang paling sering disebutkan adalah sebagai berikut (Stallings and Bauer, 2012):

Pembelajaran sejatinya dilakukan melalui interaksi guru dengan siswa dalam suasana lingkungan belajar. Esensi pembelajaran ini merupakan pendampingan yang dilakukan pendidik untuk mentransmisikan ilmu kepada peserta didik. Oleh karena itu, secara sederhana pembelajaran dapat dimaknai



sebagai suatu proses pencerahan yang dilakukan guru untuk membantu siswa mendapatkan pembelajaran dan mampu memahami bahan pembelajaran yang diberikan (Mansyur, 2020).

- Keaslian: Properti yang asli dan dapat diverifikasi dan dipercaya; keyakinan terhadap validitas transmisi, pesan, atau pembuat pesan. Ini berarti memverifikasi bahwa pengguna adalah yang mereka katakan dan bahwa setiap masukan yang masuk ke sistem berasal dari sumber terpercaya.
- Akuntabilitas: Tujuan keamanan yang menghasilkan persyaratan untuk tindakan suatu entitas untuk ditelusuri secara unik ke entitas tersebut. Ini mendukung *non repudiation, deterrence, fault isolation, intrusion detection and prevent, and after-action recovery and legal action*. Karena sistem yang benar-benar aman belum menjadi tujuan yang dapat dicapai, kami harus dapat melacak pelanggaran keamanan ke pihak yang bertanggung jawab. Sistem harus menyimpan catatan aktivitas mereka untuk memungkinkan analisis forensik nanti melacak pelanggaran keamanan atau untuk membantu dalam sengketa transaksi. Perhatikan bahwa FIPS PUB 199 menyertakan keaslian dibawah integritas.

Contoh: Sekarang kami menyediakan beberapa contoh aplikasi yang menggambarkan persyaratan yang baru saja disebutkan. Untuk contoh-contoh ini kami menggunakan tiga tingkat dampak pada organisasi atau individu jika ada pelanggaran keamanan (yaitu, hilangnya kerahasiaan, integritas, atau ketersediaan). Tingkat ini ditentukan dalam FIPS PUB 199:

- Rendah: Kerugian dapat diharapkan memiliki efek merugikan yang terbatas pada operasi organisasi, aset organisasi, atau individu. Efek merugikan yang terbatas berarti bahwa, sebagai contoh, hilangnya kerahasiaan, integritas, atau ketersediaan dapat (i) menyebabkan penurunan kapabilitas misi sejauh dan lamanya organisasi mampu menjalankan fungsi utamanya, tetapi efektivitas organisasi. fungsi berkurang secara nyata; (ii) mengakibatkan kerusakan kecil pada aset organisasi; (iii) mengakibatkan kerugian finansial kecil; atau (iv) menghasilkan minor merugikan individu.

- Sedang: Kerugian dapat diharapkan memiliki efek buruk yang serius pada operasi organisasi, aset organisasi, atau individu. Efek merugikan yang serius berarti bahwa, sebagai contoh, kerugian tersebut dapat (i) menyebabkan penurunan yang signifikan dalam kapabilitas misi sejauh dan lamanya organisasi tersebut mampu menjalankan fungsi utamanya, tetapi efektivitas fungsi tersebut berkurang secara signifikan; (ii) mengakibatkan kerusakan signifikan pada aset organisasi; (iii) mengakibatkan kerugian finansial yang signifikan; atau (iv) mengakibatkan kerugian yang signifikan bagi individu yang tidak melibatkan korban jiwa atau cedera serius yang mengancam jiwa.
- Tinggi: Kerugian dapat diperkirakan memiliki dampak buruk yang parah atau bencana besar pada operasi organisasi, aset organisasi, atau individu. Efek merugikan yang parah atau bencana berarti bahwa, sebagai contoh, kerugian tersebut dapat (i) menyebabkan degradasi yang parah atau hilangnya kemampuan misi sejauh dan lamanya organisasi tidak dapat melakukan satu atau lebih fungsi utamanya; (ii) mengakibatkan kerusakan besar pada aset organisasi; (iii) mengakibatkan kerugian finansial yang besar; atau (iv) mengakibatkan cedera parah atau bencana bagi individu yang melibatkan hilangnya nyawa atau cedera serius yang mengancam jiwa.

### 2.2.1 Kerahasiaan

Informasi nilai siswa merupakan aset yang kerahasiaannya dianggap sangat penting oleh siswa. Di Amerika Serikat, rilis informasi tersebut diatur oleh *Family Educational Rights and Privacy Act* (FERPA). Informasi nilai seharusnya hanya tersedia untuk siswa, orang tua, dan karyawan yang memerlukan informasi tersebut untuk melakukan pekerjaan mereka. Informasi pendaftaran siswa mungkin memiliki peringkat kerahasiaan sedang. Meskipun masih dicakup oleh FERPA, informasi ini dilihat oleh lebih banyak orang setiap hari, cenderung tidak ditargetkan dari pada informasi kelas, dan menghasilkan lebih sedikit kerusakan jika diungkapkan. Informasi direktori, seperti daftar siswa atau fakultas atau daftar departemen, dapat diberi peringkat

kerahasiaan rendah atau bahkan tidak ada peringkat. Informasi ini biasanya tersedia secara gratis untuk umum dan dipublikasikan di situs web sekolah.

### 2.2.2 Integritas

Beberapa aspek integritas diilustrasikan oleh contoh informasi alergi pasien rumah sakit yang disimpan dalam database. Dokter harus dapat mempercayai bahwa informasi tersebut benar dan terkini. Sekarang anggaplah seorang karyawan (mis., Seorang perawat) yang diberi wewenang untuk melihat dan memperbarui informasi ini dengan sengaja memalsukan data untuk membahayakan rumah sakit. Basis data perlu dikembalikan ke basis terpercaya dengan cepat, dan kesalahan harus dapat dilacak kembali ke orang yang bertanggung jawab. Informasi alergi pasien adalah contoh aset dengan persyaratan integritas yang tinggi. Informasi yang tidak akurat dapat mengakibatkan cedera serius atau kematian bagi pasien dan membuat rumah sakit menghadapi tanggung jawab besar.

Contoh aset yang dapat diberikan persyaratan integritas tingkat sedang adalah situs Web yang menawarkan forum untuk pengguna terdaftar untuk membahas beberapa topik tertentu. Baik pengguna terdaftar atau peretas dapat memalsukan beberapa entri atau merusak situs Web. Jika forum hanya ada untuk kesenangan pengguna, menghasilkan sedikit atau tidak ada pendapatan iklan, dan tidak digunakan untuk sesuatu yang penting seperti penelitian, maka potensi kerusakan tidak parah. Master Web mungkin mengalami kehilangan beberapa data, keuangan, dan waktu.

Contoh persyaratan integritas rendah adalah polling online anonim. Banyak situs Web, seperti organisasi berita, menawarkan polling ini kepada pengguna mereka dengan sedikit pengamanan. Namun, sifat tidak akurat dan tidak ilmiah dari jajak pendapat tersebut dipahami dengan baik.

### 2.2.3 Ketersediaan

Semakin penting suatu komponen atau layanan, semakin tinggi tingkat ketersediaan yang diperlukan. Pertimbangkan sistem yang menyediakan layanan otentikasi untuk sistem, aplikasi, dan perangkat penting. Gangguan layanan mengakibatkan ketidakmampuan pelanggan untuk mengakses sumber daya komputasi dan staf untuk mengakses sumber daya yang mereka butuhkan untuk melakukan tugas-tugas penting. Hilangnya layanan diterjemahkan

menjadi kerugian finansial yang besar dalam kehilangan produktivitas karyawan dan potensi kehilangan pelanggan.

Contoh aset yang biasanya dinilai memiliki persyaratan ketersediaan yang moderat adalah situs web publik untuk universitas; situs Web menyediakan informasi untuk siswa dan pendonor saat ini dan yang akan datang. Situs semacam itu bukanlah komponen penting dari sistem informasi universitas, tetapi ketidaktersediaannya akan membuat malu. Aplikasi pencarian direktori telepon online akan diklasifikasikan sebagai persyaratan ketersediaan rendah. Meskipun kehilangan aplikasi sementara mungkin mengganggu, ada cara lain untuk mengakses informasi, seperti direktori hardcopy atau operator.

## 2.3 Tantangan Keamanan Komputer

Keamanan komputer itu menarik dan kompleks. Beberapa alasannya adalah sebagai berikut (Stallings and Bauer, 2012):

1. Keamanan komputer tidak sesederhana yang mungkin pertama kali terlihat oleh pemula. Persyaratannya tampaknya langsung; memang, sebagian besar persyaratan utama untuk layanan keamanan dapat diberikan label satu kata yang cukup jelas: kerahasiaan, otentikasi, non repudiation, integritas. Tetapi mekanisme yang digunakan untuk memenuhi persyaratan tersebut bisa sangat kompleks, dan memahaminya mungkin melibatkan penalaran yang agak halus.
2. Dalam mengembangkan mekanisme atau algoritma keamanan tertentu, seseorang harus selalu mempertimbangkan potensi serangan pada fitur keamanan tersebut. Dalam banyak kasus, serangan yang berhasil dirancang dengan melihat masalah dengan cara yang sama sekali berbeda, oleh karena itu memanfaatkan kelemahan mekanisme yang tidak terduga.
3. Karena poin 2, prosedur yang digunakan untuk menyediakan layanan tertentu seringkali berlawanan dengan intuisi. Biasanya, mekanisme keamanan itu kompleks, dan dari pernyataan persyaratan tertentu tidak jelas bahwa tindakan yang rumit semacam itu diperlukan.

Hanya ketika berbagai aspek ancaman dipertimbangkan, mekanisme keamanan yang rumit menjadi masuk akal.

4. Setelah merancang berbagai mekanisme keamanan, perlu diputuskan di mana akan menggunakannya. Ini benar baik dalam hal penempatan fisik (misalnya, pada titik mana dalam jaringan diperlukan mekanisme keamanan tertentu) dan dalam arti logis [misalnya, pada lapisan atau lapisan apa dari arsitektur seperti TCP / IP (Transmission Control Protocol / Protokol Internet) harus ditempatkan mekanisme].
5. Mekanisme keamanan biasanya melibatkan lebih dari satu algoritma atau protokol tertentu. Mereka juga mengharuskan peserta untuk memiliki beberapa informasi rahasia (misalnya, kunci enkripsi), yang menimbulkan pertanyaan tentang pembuatan, distribusi, dan perlindungan informasi rahasia tersebut. Mungkin juga ada ketergantungan pada protokol komunikasi yang perilakunya dapat mempersulit tugas mengembangkan mekanisme keamanan. Misalnya, jika mekanisme keamanan berfungsi dengan baik memerlukan pengaturan batas waktu pada waktu transit pesan dari pengirim ke penerima, maka protokol atau jaringan apa pun yang memasukkan variabel, penundaan tak terduga dapat membuat batas waktu tersebut menjadi tidak berarti.
6. Keamanan komputer pada dasarnya adalah pertarungan kecerdasan antara pelaku yang mencoba menemukan lubang dan perancang atau administrator yang mencoba menutupinya. Keuntungan besar yang dimiliki penyerang adalah dia hanya perlu menemukan satu kelemahan sementara perancang harus menemukan dan menghilangkan semua kelemahan untuk mencapai keamanan yang sempurna.
7. Ada kecenderungan alami di pihak pengguna dan manajer sistem untuk melihat sedikit manfaat dari investasi keamanan sampai terjadi kegagalan keamanan.
8. Keamanan membutuhkan pemantauan yang teratur, bahkan konstan, dan ini sulit dilakukan dalam lingkungan jangka pendek yang kelebihan beban saat ini.

9. Keamanan masih terlalu sering menjadi renungan untuk dimasukkan ke dalam sistem setelah desain selesai daripada menjadi bagian integral dari proses desain.
10. Banyak pengguna dan bahkan administrator keamanan melihat keamanan yang kuat sebagai penghalang untuk pengoperasian sistem informasi atau penggunaan informasi yang efisien dan mudah digunakan.

## 2.4 Model untuk Keamanan Komputer

Kami sekarang memperkenalkan beberapa terminologi yang akan berguna, dengan mengandalkan RFC 2828, Daftar Istilah Keamanan Internet. Tabel 2.1 mendefinisikan istilah dan Gambar 2.2 menunjukkan hubungan antara beberapa istilah ini. Kita mulai dengan konsep sumber daya sistem, atau 3 aset, yang ingin dilindungi oleh pengguna dan pemilik. Aset sistem komputer dapat dikategorikan sebagai berikut (Stallings and Bauer, 2012):

- **Hardware:** Termasuk sistem komputer dan pemrosesan data lainnya, penyimpanan data, dan perangkat komunikasi data.
- **Perangkat Lunak:** Termasuk sistem operasi, utilitas sistem, dan aplikasi.
- **Data:** Termasuk file dan database, serta data terkait keamanan, seperti file sandi.

**Tabel 2.1:** Terminologi Keamanan Komputer (Stallings and Bauer, 2012)

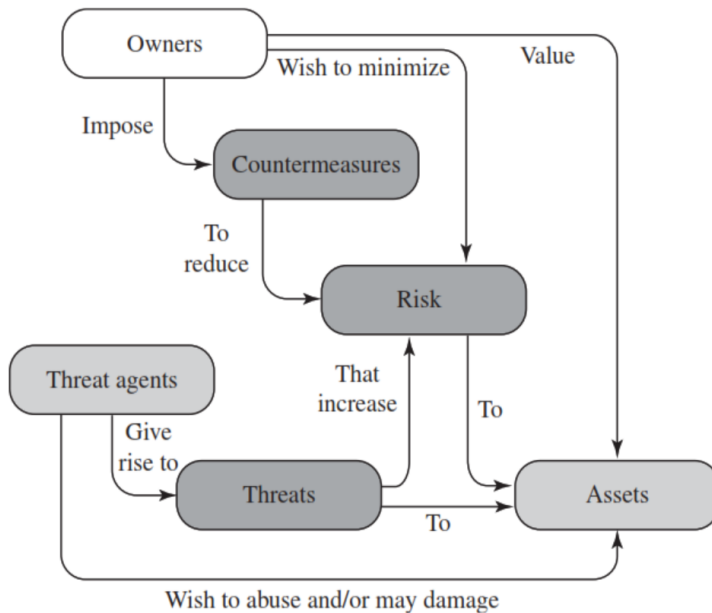
|                                 |                                                                                                                                                                                                                                                             |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Musuh<br/>(Agen Ancaman)</b> | Entitas yang menyerang, atau merupakan ancaman bagi, sistem.                                                                                                                                                                                                |
| <b>Menyerang</b>                | Serangan terhadap keamanan sistem yang berasal dari ancaman cerdas; Artinya, tindakan cerdas yang merupakan upaya yang disengaja (terutama dalam arti metode atau teknik) untuk menghindari layanan keamanan dan melanggar kebijakan keamanan suatu sistem. |
| <b>Tindakan</b>                 | Tindakan, perangkat, prosedur, atau teknik yang mengurangi                                                                                                                                                                                                  |

|                                  |                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Balasan</b>                   | ancaman, kerentanan, atau serangan dengan menghilangkan atau mencegahnya, dengan meminimalkan kerugian yang dapat ditimbulkan, atau dengan menemukan dan melaporkannya sehingga tindakan korektif dapat diambil.                                                                                                                                       |
| <b>Risiko</b>                    | Ekspektasi kerugian dinyatakan sebagai kemungkinan bahwa ancaman tertentu akan mengeksploitasi kerentanan tertentu dengan akibat berbahaya tertentu.                                                                                                                                                                                                   |
| <b>Kebijakan Keamanan</b>        | Serangkaian aturan dan praktik yang menentukan atau mengatur bagaimana suatu sistem atau organisasi menyediakan layanan keamanan untuk melindungi sumber daya sistem yang sensitif dan kritis.                                                                                                                                                         |
| <b>Sumber Daya Sistem (Aset)</b> | Data yang terdapat dalam sistem informasi; atau layanan yang disediakan oleh sistem; atau kemampuan sistem, seperti daya pemrosesan atau bandwidth komunikasi; atau item perlengkapan sistem (yaitu, komponen sistem— perangkat keras, firmware, perangkat lunak, atau dokumentasi); atau fasilitas yang menampung pengoperasian dan peralatan sistem. |
| <b>Ancaman</b>                   | Potensi pelanggaran keamanan, yang muncul ketika ada keadaan, kemampuan, tindakan, atau peristiwa, yang dapat melanggar keamanan dan menyebabkan kerugian. Artinya, ancaman adalah kemungkinan bahaya yang mungkin mengeksploitasi kerentanan.                                                                                                         |
| <b>Kerentanan</b>                | Cacat atau kelemahan dalam desain, implementasi, atau operasi dan manajemen sistem yang dapat dimanfaatkan untuk melanggar kebijakan keamanan sistem.                                                                                                                                                                                                  |

- Fasilitas dan jaringan komunikasi: Tautan komunikasi jaringan area lokal dan luas, bridge, router, dan sebagainya. Dalam konteks keamanan, perhatian kami adalah pada kerentanan sumber daya sistem. Kategori umum kerentanan sistem komputer atau aset jaringan berikut:
- Dapat dirusak, sehingga melakukan hal yang salah atau memberikan jawaban yang salah. Misalnya, nilai data yang disimpan mungkin berbeda dari yang seharusnya karena telah dimodifikasi dengan tidak benar.

- Bisa bocor. Misalnya, seseorang yang seharusnya tidak memiliki akses ke beberapa atau semua informasi yang tersedia melalui jaringan mendapatkan akses tersebut.
- Ini bisa menjadi tidak tersedia atau sangat lambat. Artinya, menggunakan sistem atau jaringan menjadi tidak mungkin atau tidak praktis.

Ketiga jenis kerentanan umum ini sesuai dengan konsep integritas, kerahasiaan, dan ketersediaan, yang disebutkan sebelumnya di bagian ini.



**Gambar 2.2:** Triad Persyaratan Keamanan (Stallings and Bauer, 2012)

Berkaitan dengan berbagai jenis kerentanan terhadap sumber daya sistem adalah ancaman yang mampu memanfaatkan kerentanan tersebut. Ancaman menunjukkan potensi bahaya keamanan pada suatu aset. Serangan adalah ancaman yang dilakukan (tindakan ancaman) dan, jika berhasil, mengarah pada pelanggaran keamanan yang tidak diinginkan, atau konsekuensi ancaman. Agen yang melakukan serangan disebut sebagai penyerang, atau agen ancaman.



Kita dapat membedakan dua jenis serangan:

- Serangan aktif: Upaya untuk mengubah sumber daya sistem atau memengaruhi operasinya.
- Serangan pasif: Upaya untuk mempelajari atau memanfaatkan informasi dari sistem yang tidak memengaruhi sumber daya sistem.

Kami juga dapat mengklasifikasikan serangan berdasarkan asal serangan:

- Serangan dari dalam: Dimulai oleh suatu entitas di dalam perimeter keamanan ("orang dalam"). Orang dalam diberi wewenang untuk mengakses sumber daya sistem tetapi menggunakannya dengan cara yang tidak disetujui oleh mereka yang diberi otorisasi.
- Serangan luar: Dimulai dari luar batas, oleh pengguna sistem yang tidak sah atau tidak sah ("orang luar"). Di Internet, penyerang luar potensial berkisar dari orang iseng amatir hingga penjahat terorganisir, teroris internasional, dan pemerintah yang bermusuhan.

## 2.5 Teknologi dan Prinsip Keamanan Komputer

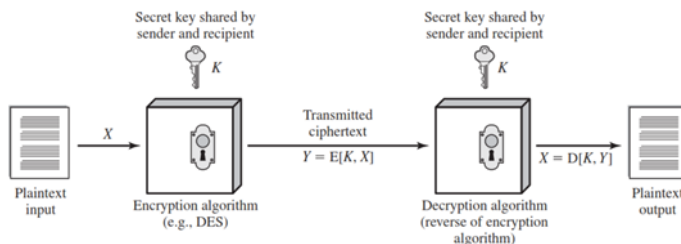
Elemen penting dalam banyak layanan dan aplikasi keamanan komputer adalah penggunaan algoritma kriptografi. Penjelasan berikut ini memberikan gambaran umum dari berbagai jenis algoritma, bersama dengan diskusi tentang penerapannya. Untuk setiap jenis algoritma, kami memperkenalkan algoritma standar terpenting yang umum digunakan. Kami mulai dengan enkripsi simetris, yang digunakan dalam berbagai macam konteks, terutama untuk memberikan kerahasiaan. Selanjutnya, kami memeriksa fungsi hash yang aman dan mendiskusikan penggunaannya dalam otentikasi pesan.

### 2.5.1 Kerahasiaan dengan Enkripsi Simetris

Teknik universal untuk memberikan kerahasiaan untuk data yang dikirim atau disimpan adalah enkripsi simetris.

a. Enkripsi Simetris

Enkripsi simetris, juga disebut sebagai enkripsi konvensional atau enkripsi kunci tunggal, adalah satu-satunya jenis enkripsi yang digunakan sebelum diperkenalkannya enkripsi kunci publik pada akhir 1970-an. Individu dan kelompok yang tak terhitung jumlahnya, dari Julius Caesar hingga pasukan U-boat Jerman hingga pengguna diplomatik, militer, dan komersial saat ini, telah menggunakan enkripsi simetris untuk komunikasi rahasia. Itu tetap yang lebih banyak digunakan dari dua jenis enkripsi. Skema enkripsi simetris memiliki lima bahan (Gambar 2.3):



**Gambar 2.3:** Model Enkripsi Simetris yang Disederhanakan (Stallings and Bauer, 2012)

- Plaintext: Ini adalah pesan atau data asli yang dimasukkan ke dalam algoritma sebagai input.
- Algoritma enkripsi: Algoritma enkripsi melakukan berbagai substitusi dan transformasi pada teks biasa.
- Kunci rahasia: Kunci rahasia juga dimasukkan ke dalam algoritma enkripsi. Substitusi dan transformasi tepat yang dilakukan oleh algoritma bergantung pada kuncinya.
- Ciphertext: Ini adalah pesan acak yang dihasilkan sebagai keluaran. Itu tergantung pada teks biasa dan kunci rahasia. Untuk pesan tertentu, dua kunci berbeda akan menghasilkan dua teks sandi yang berbeda.

- Algoritma dekripsi: Ini pada dasarnya adalah algoritma enkripsi yang dijalankan secara terbalik. Ini mengambil teks sandi dan kunci rahasia dan menghasilkan teks biasa asli.

Ada dua persyaratan untuk penggunaan yang aman dari enkripsi simetris:

1. Kami membutuhkan algoritma enkripsi yang kuat. Minimal, kami ingin algoritma sedemikian rupa sehingga lawan yang mengetahui algoritme dan memiliki akses ke satu atau lebih ciphertext tidak akan dapat memecahkan ciphertext atau mengetahui kuncinya. Persyaratan ini biasanya dinyatakan dalam bentuk yang lebih kuat: Lawan harus tidak dapat mendekripsi ciphertext atau menemukan kuncinya bahkan jika dia memiliki sejumlah ciphertext bersama dengan plaintext yang menghasilkan setiap ciphertext.
2. Pengirim dan penerima harus mendapatkan salinan kunci rahasia dengan cara yang aman dan harus menyimpan kunci tersebut dengan aman. Jika seseorang dapat menemukan kunci dan mengetahui algoritmanya, semua komunikasi yang menggunakan kunci ini dapat dibaca. Ada dua pendekatan umum untuk menyerang skema enkripsi simetris. Serangan pertama dikenal sebagai pembacaan sandi. Serangan kriptanalitik bergantung pada sifat algoritma ditambah mungkin beberapa pengetahuan tentang karakteristik umum dari teks biasa atau bahkan beberapa contoh pasangan teks-teks-teks biasa. Jenis serangan ini memanfaatkan karakteristik algoritma untuk mencoba menyimpulkan teks biasa atau menyimpulkan kunci yang digunakan. Jika serangan berhasil menyimpulkan kunci tersebut, efeknya adalah bencana: Semua pesan masa depan dan masa lalu yang dienkripsi dengan kunci tersebut akan disusupi.

## 2.5.2 Otentikasi Pesan dan Fungsi Hash

Enkripsi melindungi dari serangan pasif (menguping). Persyaratan yang berbeda adalah untuk melindungi dari serangan aktif (pemalsuan data dan transaksi). Perlindungan terhadap serangan semacam itu dikenal sebagai otentikasi pesan atau data. Sebuah pesan, file, dokumen, atau kumpulan data lainnya dikatakan otentik jika itu asli dan berasal dari sumber yang diduga.

Otentikasi pesan atau data adalah prosedur yang memungkinkan pihak yang berkomunikasi untuk memverifikasi bahwa pesan yang diterima atau disimpan adalah asli. Dua aspek penting tersebut adalah untuk memverifikasi bahwa isi pesan belum diubah dan bahwa sumbernya asli. Kami juga mungkin ingin memverifikasi ketepatan waktu pesan (belum ditunda dan diputar ulang secara artifisial) dan urutan yang terkait dengan pesan lain yang mengalir di antara dua pihak.

### 2.5.3 Otentikasi Menggunakan Enkripsi Symmetric

Tampaknya mungkin untuk melakukan otentikasi hanya dengan menggunakan enkripsi simetris. Jika kami berasumsi bahwa hanya pengirim dan penerima yang berbagi kunci (sebagaimana mestinya), maka hanya pengirim asli yang dapat berhasil mengenkripsi pesan untuk peserta lain, asalkan penerima dapat mengenali pesan yang valid. Lebih lanjut, jika pesan tersebut menyertakan kode deteksi kesalahan dan nomorurut, penerima yakin bahwa tidak ada perubahan yang dilakukan dan urutannya benar. Jika pesan juga menyertakan stempel waktu, penerima yakin bahwa pesan tidak ditunda melebihi yang biasanya diharapkan untuk transit jaringan. Nyatanya, enkripsi simetris saja bukanlah alat yang cocok untuk otentikasi data. Sebagai contoh sederhana, dalam mode enkripsi ECB, jika penyerang menyusun ulang blok ciphertext, maka setiap blok akan tetap berhasil didekripsi. Namun, pengubahan urutan dapat mengubah arti dari keseluruhan urutan data. Meskipun nomorurut dapat digunakan di beberapa tingkat (misalnya, setiap paket IP), biasanya nomorurut terpisah tidak akan dikaitkan dengan setiap blok b-bit teks biasa. Jadi, penyusunan ulang blok merupakan ancaman.



## **Bab 3**

# **Cryptosystem dan Cryptography**

### **3.1 Pendahuluan**

Perkembangan teknologi dan informasi yang begitu pesat telah membawa manfaat untuk peradaban manusia. Hal tersebut sejalan dengan kebutuhan terhadap keamanan data dari pihak-pihak yang ingin mengambil atau mencuri data-data penting sehingga merugikan pemilik data tersebut. Salah satu pengamanan data yang digunakan yaitu menggunakan kriptografi. Menurut Munir Rinaldi (2006), ada beberapa seni pengamanan data yang melalui suatu saluran, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang sangat rahasia akan disandikan sedemikian rupa sehingga walaupun data tersebut dicuri oleh pihak yang tidak berhak, namun mereka tidak dapat mengetahui data yang sebenarnya, karena data yang mereka curi merupakan data yang sudah disandikan. Data asli yang akan dikirimkan dan dalam kriptografi sebagai plaintext, dan data yang telah disandikan disebut sebagai ciphertext.

Untuk menjamin keamanan dan keutuhan dari suatu data, dibutuhkan suatu proses penyandian. Dengan cara penyandian tersebut, data asli tidak akan terbaca oleh pihak yang tidak berkepentingan. Pertimbangan bahwa sebuah standard algoritma yang baru sangatlah diperlukan untuk tetap menjaga kerahasiaan suatu data. Dalam hal ini, kunci yang lebih panjang juga merupakan keharusan.

## 3.2 Cryptosystem

*Cryptosystem* atau sistem kriptografi adalah kumpulan algoritma kriptografi yang terdiri dari plaintext, ciphertext dan kunci yang digunakan (Schneier, 1996). *Cryptosystem* adalah seperangkat algoritma kriptografi yang diperlukan untuk mengimplementasikan layanan keamanan tertentu, paling umum untuk mencapai kerahasiaan. *Cryptosystem* terdiri dari tiga algoritma: pembuatan kunci, proses enkripsi, dan proses dekripsi. Menurut William Stallings (2005), sistem kriptografi dapat diklasifikasikan menjadi tiga yaitu :

1. Tipe operasi yang digunakan untuk mentransformasikan plaintext ke ciphertext.
2. Jumlah kunci yang digunakan.
3. Cara memproses plaintext

*Cryptosystem* (seperti enkripsi RSA) didesain untuk menyediakan fungsi tertentu (seperti enkripsi kunci publik) untuk menjamin sifat keamanan tertentu keamanan (seperti serangan teks-terpilih) seperti pada model Oracle acak. *Cryptosystem* menggunakan sifat kriptografi sederhana utama untuk mendukung sifat keamanan sistem. Tentu saja, karena perbedaan antara kriptosistem dan kriptografi, *cryptosystem* yang canggih dapat diperoleh dari kombinasi beberapa kriptosistem sederhana. Beberapa *cryptosystem* yang terkenal termasuk enkripsi RSA, tanda tangan Schnorr, enkripsi Elgamal, PGP, dan lain-lain. *Cryptosystem* yang lebih rumit melibatkan sistem uang elektronik, sistem tanda-tangan enkripsi, dan lain-lain. Beberapa *cryptosystem* teoritikal termasuk sistem pembuktian interaktif, seperti pembuktian pengetahuan-nol), sistem untuk pembagian rahasia (Blakley, 1979).

## 3.3 Cryptography

Salah satu teknik yang digunakan dalam keamanan data adalah *cryptography* (kriptografi). Dalam *cryptography*, data yang sangat rahasia akan disandikan sedemikian rupa sehingga walaupun data tersebut dicuri oleh pihak yang tidak berhak, namun mereka tidak dapat mengetahui data yang sebenarnya, karena data yang mereka curi merupakan data yang sudah disandikan.

### 3.3.1 Definisi Cryptography

Beberapa aspek integritas diilustrasikan oleh contoh informasi alergi pasien rumah sakit yang disimpan dalam database. Dokter harus dapat mempercayai bahwa informasi tersebut benar dan terkini. Sekarang anggaplah seorang karyawan (mis., Seorang perawat) yang diberi wewenang untuk melihat dan memperbarui informasi ini dengan sengaja memalsukan data untuk membahayakan rumah sakit. Basis data perlu dikembalikan ke basis terpercaya dengan cepat, dan kesalahan harus dapat dilacak kembali ke orang yang bertanggung jawab. Informasi alergi pasien adalah contoh aset dengan persyaratan integritas yang tinggi. Informasi yang tidak akurat dapat mengakibatkan cedera serius atau kematian bagi pasien dan membuat rumah sakit menghadapi tanggung jawab besar.

Contoh aset yang dapat diberikan persyaratan integritas tingkat sedang adalah situs Web yang menawarkan forum untuk pengguna terdaftar untuk membahas beberapa topik tertentu. Baik pengguna terdaftar atau peretas dapat memalsukan beberapa entri atau merusak situs Web. Jika forum hanya ada untuk kesenangan pengguna, menghasilkan sedikit atau tidak ada pendapatan iklan, dan tidak digunakan untuk sesuatu yang penting seperti penelitian, maka potensi kerusakan tidak parah. Master Web mungkin mengalami kehilangan beberapa data, keuangan, dan waktu. Contoh persyaratan integritas rendah adalah polling online anonim. Banyak situs Web, seperti organisasi berita, menawarkan polling ini kepada pengguna mereka dengan sedikit pengamanan. Namun, sifat tidak akurat dan tidak ilmiah dari jajak pendapat tersebut dipahami dengan baik.

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Kriptografi menurut terminologinya adalah sebuah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara istilah kriptografi didefinisikan sebagai ilmu dan seni untuk menjaga kerahasiaan pesan baik berupa data maupun informasi yang mempunyai arti atau nilai dengan cara menyamarkan (mengacak) menjadi bentuk yang tidak dapat dimengerti dan hanya menerima yang dapat mengubah kode-kode tersebut menjadi pesan asli yang dapat dimengerti (Mollin, 2007). Menurut Schneier (1996), menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*cryptography is the art science of keeping message secure*). Menurut Sentot Kromodimoeljo (2010), kriptografi adalah ilmu mengenai teknik enkripsi di mana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang



sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter.

Menurut Abidin dkk, (2016), dalam kriptografi ada beberapa istilah yang sering digunakan, antara lain sebagai berikut :

1. Plaintext adalah informasi asli sebelum dienkripsi atau teks terang.
2. Enkripsi adalah proses kriptografi dari plaintext menjadi ciphertext.
3. Ciphertext adalah informasi acak yang berasal dari plaintext yang telah dimasukkan ke dalam fungsi kriptografi atau enkripsi.
4. Dekripsi adalah proses pengubahan ciphertext menjadi plaintext.
5. Kriptanalisis adalah studi yang mempelajari teknik matematika untuk memecahkan teknik kriptografi.
6. Kriptanalisis adalah orang yang melakukan kriptanalisis.
7. Kriptologi adalah ilmu tentang kriptografi dan kriptanalisis.

### 3.3.2 Sejarah Cryptography

Kriptografi memiliki sejarah yang panjang dan sangat mengagumkan. Penulisan rahasia ini dapat dilacak kembali pada 3000 tahun SM saat digunakan oleh bangsa Mesir. Mereka menggunakan hieroglyphs untuk menyembunyikan tulisan mereka yang tidak diharapkan. Hieroglyphs diturunkan dari Bahasa Yunani hieroglyphica yang berarti ukiran rahasia. Hieroglyphs berevolusi menjadi hieratic, yaitu stylized script yang lebih mudah untuk digunakan. Sekitar tahun 400 SM, kriptografi militer digunakan oleh bangsa Sparta dalam bentuk sepotong papyrus atau perkamen dibungkus dengan batang kayu, sistem ini disebut Scytale (Simarmata, 2020). Kriptografi sudah digunakan sekitar 4000 abad yang lalu oleh orang-orang Mesir untuk mengirim pesan ke pasukan yang berada di medan perang dan agar pesan tersebut tidak terbaca oleh musuh walaupun pembawa pesan tersebut tertangkap oleh musuh. Pada zaman Romawi, Julius Caesar telah menggunakan teknik kriptografi yang sekarang dianggap kuno dan sangat mudah dibobol untuk keperluan militernya. Metode yang digunakan oleh Julius Caesar ini sering dianggap awal dari kriptografi.

Informasi lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul *The Codebreakers*. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari

penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa hieroglyph yang tidak standar pada pyramid) hingga penggunaan kriptografi pada abad ke-20 sampai akhir Perang Dunia I, kriptografi merupakan disiplin ilmu matematika yang hanya dipelajari oleh orang-orang tertentu saja. Penelitian bidang ini tidak pernah sampai ke umum. Kriptografi juga digunakan di kalangan militer. Pada perang dunia ke 2, pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan Enigma. Mesin yang menggunakan beberapa buah rotor (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun Enigma cipher berhasil dipecahkan oleh pihak sekutu dan keberhasilan memecahkan Enigma sering dikatakan sebagai faktor yang memperpendek Perang Dunia II (Rinaldi, 2006).

Perkembangan komputer dan sistem komunikasi pada tahun 60-an berdampak pada permintaan dari sektor-sektor privat sebagai sarana untuk melindungi informasi dalam bentuk digital dan untuk menyediakan layanan keamanan. Dimulai dari usaha Feistel pada IBM di awal tahun 70-an dan mencapai puncaknya pada tahun 1977 dengan pengangkatan DES (Data Encryption Standard) sebagai standar pemroses informasi federal US untuk mengenkripsi informasi yang unclassified. DES merupakan mekanisme kriptografi yang paling dikenal sepanjang sejarah. Pengembangan paling mengejutkan dalam sejarah kriptografi terjadi pada tahun 1976 saat Whitfield Diffie dan Martin Hellman mempublikasi *New Directions in Cryptography*. Tulisan ini memperkenalkan konsep revolusioner kriptografi kunci public dan juga memberikan metode baru dan jenius untuk pertukaran kunci, keamanan yang berdasar pada kekuatan masalah logaritma diskrit. Walaupun penulis tesis tersebut tidak mempunyai praktek yang nyata akan bentuk skema enkripsi kunci public pada saat itu, tetapi ide tersebut memicu minat dan aktivitas yang besar dalam komunitas kriptografi. Pada tahun 1978, Rivest, Shamir, dan Adleman menemukan enkripsi kunci publik yang pertama dan sekarang ini dikenal dengan nama RSA (Rivest, Shamir, and Adleman). Skema RSA didasarkan pada permasalahan matematika sulit yang terdiri dari pemfaktoran terhadap bilangan besar. Skema kunci public yang kuat dan praktis ditemukan oleh El Gamal. Skema ini juga didasarkan masalah algoritma diskrit (Rinaldi, 2006).

### 3.3.3 Tujuan Cryptography

Menurut Janner Simarmata dkk (2020), kriptografi sering diminta untuk melakukan pekerjaan sebagai berikut :

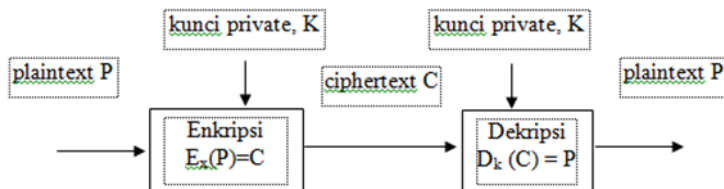
1. Kerahasiaan (confidentiality) adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi pesan yang tidak bisa terbaca oleh pihak yang berhak.
2. Autentikasi (authentication) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication) maupun mengidentifikasi kebenaran dari sumber pesan (data origin authentication). Dua pihak yang saling berkomunikasi harus dapat mengidentifikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diautentikasi sumbernya.
3. Integritas data (data integrity) adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama dalam pengiriman. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan yang dilakukan oleh pihak-pihak yang tidak berhak, antara lain perubahan, penghapusan dan penyisipan data lain ke dalam pesan yang sebenarnya. Di dalam kriptografi layanan ini direalisasikan dengan menggunakan tanda tangan digital (digital signature).
4. Tidak ada penyangkalan (non-repudiation) adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

### 3.3.4 Klasifikasi Cryptography

Menurut Munir Rinaldi (2006), berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi kriptografi kunci simetris (symmetric-key cryptography) dan kriptografi kunci asimetris (asymmetric-key cryptography).

### 1. Kriptografi Kunci Simetris

Pada sistem kriptografi kunci simetris, kunci untuk enkripsi sama dengan kunci untuk dekripsi, oleh karena itu dinamakan kriptografi kunci simetris atau kriptografi simetris. Istilah lain untuk kriptografi simetris adalah kriptografi kunci privat (private key cryptography), kriptografi kunci rahasia (secret key cryptography), atau kriptografi konvensional (conventional cryptography). Sistem kriptografi simetris mengasumsikan pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan kriptografi simetris terletak pada kerahasiaan kuncinya. Kriptografi simetris merupakan satu-satunya jenis kriptografi yang dikenal dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetris. Di sisi lain, ada puluhan algoritma kriptografi modern yang termasuk ke dalam sistem kriptografi simetris, diantaranya adalah DES (Data Encryption Standard), Blowfish, Twofish, Triple-DES, IDEA, Serpent dan yang terbaru adalah AES (Advanced Encryption Standard) (Rinaldi, 2006). Aplikasi kriptografi simetris yang utama adalah melindungi kerahasiaan data yang dikirim melalui media telekomunikasi dan melindungi kerahasiaan data yang disimpan pada media penyimpanan. Kelemahan dari sistem ini adalah baik pengirim maupun penerima pesan harus memiliki kunci yang sama, sehingga pengirim pesan harus mencari cara yang aman untuk memberitahukan kunci kepada penerima pesan.



**Gambar 3.1:** Skema kriptografi kunci simetris (Rinaldi, 2006)

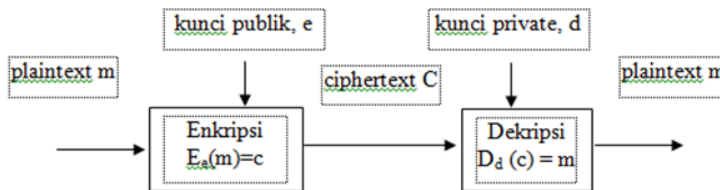
## 2. Kriptografi Kunci Asimetris

Jika kunci untuk enkripsi tidak sama dengan kunci untuk dekripsi, maka kriptografinya dinamakan kriptografi kunci asimetris atau kriptografi asimetris. Nama lainnya adalah kriptografi kunci publik (public key cryptography), sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun (diumumkan ke publik), sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan. Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan. Hanya penerima pesan yang dapat mendeskripsikan pesan karena hanya dia yang mengetahui kunci privatnya sendiri.

Menurut Munir Rinaldi (2006), keuntungan kriptografi kunci publik ada dua. Pertama tidak ada kebutuhan untuk mendistribusikan kunci privat sebagaimana pada kriptografi simetris. Kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirimkan pesan. Perhatikan bahwa saluran untuk mengirim pesan umumnya tidak aman. Kedua, jumlah kunci dapat ditekan. Untuk berkomunikasi secara rahasia dengan banyak orang, tidak perlu kunci rahasia sebanyak jumlah orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengenkripsikan pesan dan kunci privat bagi penerima pesan untuk mendeskripsikan pesan. Berbeda dengan kriptografi kunci simetris di mana jumlah kunci yang dibuat adalah sebanyak jumlah pihak yang diajak untuk berkorespondensi. Contoh algoritma kriptografi kunci publik diantaranya RSA, Elgamal, DSA, Knapsack, Elliptic Curve dan lain sebagainya.

Konsep kriptografi kunci asimetris sederhana dan elegan, tetapi mempunyai konsekuensi penggunaan yang hebat. Seperti yang telah dijelaskan pada bagian awal, pada kriptografi kunci publik, setiap pengguna memiliki sepasang kunci, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Kunci untuk enkripsi diumumkan kepada publik sehingga dinamakan dengan kunci publik dan disimbolkan

dengan  $e$ . Kunci untuk dekripsi bersifat rahasia sehingga dinamakan dengan kunci privat dan disimbolkan dengan  $d$ .



**Gambar 3.2:** Skema kriptografi kunci asimetris (Rinaldi, 2006)

Perbedaan kriptografi simetris dan asimetris menurut Schneier (1996), adalah kunci asimetris atau kunci publik dan kunci simetris merupakan dua jenis kriptografi yang berbeda dan memecahkan jenis permasalahan yang berbeda pula. Proses enkripsi pada kriptografi simetris sangat baik namun sangat rentan pada pengamanan datanya yang dienkripsi. Kunci asimetris dapat mengerjakan apa yang tidak dapat dikerjakan pada kriptografi simetris yaitu sangat baik pada manajemen kunci.

### 3.3.5 Keamanan Cryptography

Tugas utama kriptografi adalah untuk menjaga agar baik plaintext maupun kunci keduanya tetap terjaga kerahasiaannya dari penyadap (disebut juga sebagai lawan, penyerang, pencegat, penyelundup pesan, musuh, attacker dan sebagainya). Penyadap pesan diasumsikan mempunyai akses yang lengkap ke dalam saluran komunikasi antara pengirim dan penerima. Ini sangat mudah terjadi pada jalur internet dan saluran telepon (Yusuf, 2004).

Menurut Janner Simarmata (2020), sebuah algoritma kriptografi dikatakan aman apabila memenuhi tiga kriteria :

- Persamaan matematis yang menggambarkan operasi algoritma cryptography yang sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik
- Biaya untuk memecahkan ciphertext melebihi nilai informasi yang terkandung di dalam ciphertext tersebut,
- Waktu yang diperlukan untuk memecahkan ciphertext melebihi lamanya waktu informasi tersebut harus dijaga kerahasiaannya.

Algoritma kriptografi yang berbeda menawarkan tingkat keamanan yang berbeda pula, tergantung pada bagaimana sulitnya algoritma tersebut dipecahkan. Jika biaya yang diperlukan untuk memecahkan suatu algoritma lebih besar dari nilai data yang akan dienkripsi, maka ini tidak akan menjadi masalah. Jika waktu yang diperlukan untuk memecahkan suatu algoritma lebih lama dibanding waktu yang dienkripsi harus meninggalkan rahasia maka ini aman. Jika jumlah data yang dienkripsi dengan kunci tunggal kurang dari jumlah data yang diperlukan untuk memecahkan algoritma, maka ini juga aman (Simarmata, 2020).

Menurut Schneier (1996), algoritma yang terbaik adalah algoritma yang telah dipublikasikan dan telah “diserang” oleh para kriptografer dan kriptanalis yang terbaik di dunia dan hingga kini belum berhasil dipecahkan. Dengan mempublikasikan algoritma kriptografi, kriptografer memperoleh konsultasi gratis dari sejumlah kriptologis akademisi yang ingin sekali memecahkan algoritma sehingga mereka dapat mempublikasikan paper yang memperlihatkan kecerdasan mereka. Jika banyak pakar telah mencoba memecahkan algoritma selang lima tahun setelah dipublikasikan dan tidak seorangpun berhasil, maka mungkin algoritma tersebut tangguh. Karena keamanan sistem secara eksklusif ditentukan oleh kunci, maka panjang kunci menentukan keamanan sistem. Semakin panjang kunci, maka jumlah kemungkinan diterka semakin besar. Kunci sepanjang 32 bit berarti memiliki kemungkinan diterka sebanyak  $2^{32} = 4,3 \times 10^9$  buah terkaan. Semakin panjang kunci, maka faktor kerja (work factor) untuk menemukan kunci semakin besar.

## Bab 4

# Teknik Kriptografi

### 4.1 Apa itu Kriptografi

Kriptografi (Cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu krypto dan graphia. Krypto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi (Ariyus, 2006; Simarmata, Sriadhi dan Rahim, 2020).

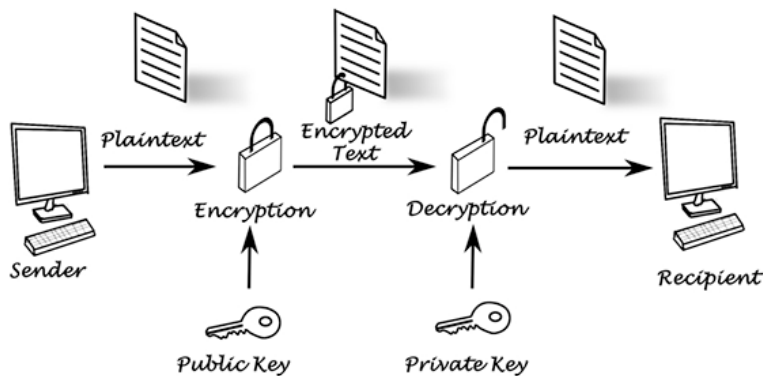
Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut.

Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses di mana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai

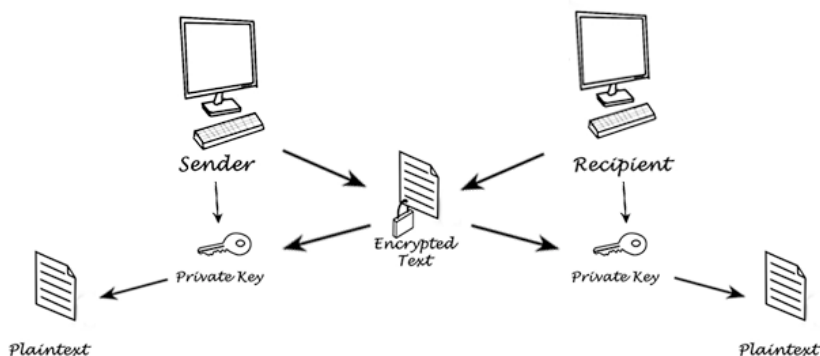


informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah plaintext. Kemudian setelah disamarkan dengan suatu cara penyandian, maka plaintext ini disebut sebagai ciphertext. Proses penyamaran dari plaintext ke ciphertext disebut enkripsi (encryption), dan proses pengembalian dari ciphertext menjadi plaintext kembali disebut dekripsi (decryption) (Pabokory, Astuti dan Kridalaksana, 2016).

Dua metode enkripsi yang paling banyak digunakan adalah Public key (asymmetric) encryption dan Private key (symmetric) encryption. Keduanya sama dalam arti bahwa keduanya memungkinkan pengguna untuk mengenkripsi data untuk menyembunyikannya dari orang lain, dan kemudian mendekripsi data tersebut dalam rangka untuk mengakses plaintext asli. Namun, mereka berbeda dalam cara mereka menangani langkah antara enkripsi dan dekripsi.



**Gambar 4.1:** Public Key Encryption



**Gambar 4.2:** Private Key Encryption

Berbagai algoritma kriptografi telah diciptakan oleh para ahli kriptografi, namun berbagai usaha dilakukan oleh cracker untuk memecahkannya tidak sedikit yang membawa keberhasilan. Hal ini mendorong para kriptografi untuk menciptakan algoritma-algoritma yang lebih aman (Surian, 2006).

Dalam kriptografi, pesan atau informasi yang dapat dibaca disebut sebagai plaintext atau cleartext. Proses yang dilakukan untuk mengubah teks asli (plaintext) ke dalam teks rahasia (chiphertext) disebut enkripsi. Pesan yang tidak terbaca disebut teks rahasia (chiphertext). Proses kebalikan dari enkripsi disebut dekripsi. Dekripsi akan mengembalikan teks rahasia (chiphertext) menjadi teks asli (plaintext). Kedua proses enkripsi dan dekripsi membutuhkan penggunaan sejumlah informasi rahasia, yang sering disebut kunci (key).

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu (Simarmata, 2006):

1. Kerahasiaan (confidentiality)

Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

2. Integritas data

Integritas adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang

tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3. Autentikasi

Autentikasi adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

4. Non-repudiasi atau nirpenyangkalan

Non-repudiasi atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

## 4.2 Teknik Kriptografi

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Salah satu usaha untuk mengamankan data di antaranya dengan menggunakan kriptografi. Berbagai macam algoritma kriptografi dapat diimplementasikan untuk mewujudkan sistem keamanan data.

Terdapat sejumlah teknik yang dapat digunakan untuk mengamankan data, antara lain: watermarking, steganografi dan kriptografi. Ketiga teknik tersebut mempunyai kesamaan operasi yaitu operasi untuk menyembunyikan data dan operasi untuk mengekstraksi kembali data yang semula telah disembunyikan. Secara umum, kriptografi merupakan teknik suatu metode dengan suatu kunci tertentu menggunakan mengolah informasi awal (plain text) yang tidak dapat dibaca baru (cipher text) suatu informasi menghasilkan enkripsi tertentu sehingga menjadi informasi awal (plain text) melalui tersebut dapat dikembalikan cipher text secara langsung sehingga orang lain tidak dapat mengenali data tersebut (Susantol dan Tritanto, 2011).

### 4.2.1 Teknik Watermarking

Watermarking atau tanda air dapat diartikan sebagai suatu teknik penyisipan dan atau penyembunyian informasi yang bersifat rahasia pada suatu data lainnya

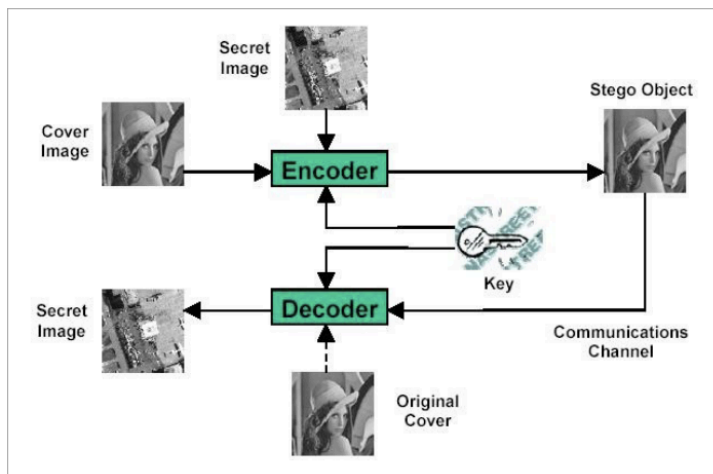
untuk "ditumpangi" (kadang disebut dengan host data), tetapi orang lain tidak menyadari adanya kehadiran data tambahan pada data host-nya (Istilah host digunakan untuk data atau sinyal digital yang disisipi), sehingga seolah-olah tidak ada perbedaan berarti antara data host sebelum dan sesudah proses watermarking (Supangkat dan Kuspriyanto, 2000).

Masalah muncul jika citra digital tersebut merupakan karya yang perlu dilindungi, misalnya citra hasil seni fotografi, citra hasil penginderaan jauh, citra medis, dan sebagainya. Contoh-contoh masalah yang muncul misalnya masalah kepemilikan (ownership), pelanggaran copyright, dan masalah keaslian. Permasalahan semacam ini dapat diatasi dengan menggunakan digital watermarking. Digital watermarking adalah teknik untuk menyisipkan informasi tertentu ke dalam data digital yang disebut watermark. Watermark dapat berupa teks seperti informasi copyright, gambar berupa logo, data audio, atau rangkaian bit yang tidak makna. Penyisipan watermark dilakukan sedemikian rupa sehingga watermark tidak merusak data digital yang dilindungi. Selain itu watermark yang telah disisipkan tidak dapat dipersepsi oleh indra manusia, namun ia dapat dideteksi oleh komputer dengan menggunakan kunci yang benar. Watermark yang telah disisipkan tidak dapat dihapus dari dalam data digital, sehingga bila data digital ber-watermark disebar dan digandakan, maka otomatis watermark di dalamnya ikut terbawa. Watermark di dalam data digital dapat dideteksi atau diekstraksi kembali. Watermarking berguna untuk membuktikan kepemilikan, copyright protection, otentikasi, fingerprinting tamper proofing, distribution tracing, dan sebagainya (Munir, 2006).

Digital watermarking dikembangkan sebagai salah satu jawaban untuk menentukan keabsahan pencipta atau pendistribusi suatu data digital dan integritas suatu data digital. Teknik watermarking bekerja dengan menyisipkan sedikit informasi yang menunjukkan kepemilikan, tujuan, atau data lain, pada media digital tanpa memengaruhi kualitasnya. Jadi pada tidak. Demikian pula jika diterapkan pada audio atau musik, telinga tidak bisa mendengar sisipan informasi tadi. Sehingga pada teknologi ini dikenal suatu persyaratan bahwa watermark haruslah imperceptible atau tidak terdeteksi oleh indera penglihatan (human visual system / HVS) atau indera pendengaran (human auditory system / HAS).

Dari pengertian tersebut, terdapat dua proses utama dalam watermarking, yaitu proses menyisipkan data (encode) dan proses mengekstrak data (decode).

Secara umum proses yang terjadi dalam watermarking terlihat dalam gambar berikut ini (Solichin, 2010).



**Gambar 4.3:** Proses Watermarking

Dari gambar tersebut terlihat bahwa gambar asli akan di-encode dengan menambahkan gambar rahasia dan kunci tertentu. Gambar yang sudah di-encode, selanjutnya dapat ditransfer melalui suatu jalur komunikasi dan jika akan diperiksa keasliannya atau ingin mendapatkan gambar aslinya, maka dilakukan proses decoder. Proses decoder key (kunci) yang sama dengan kunci pada proses encode.

Teknik digital watermarking dapat diaplikasikan dalam berbagai hal, antara lain:

1. **Ownership Assertion.** Kepemilikan dari dokumen multimedia dapat dilindungi dengan menambahkan watermark yang berisi informasi pemilik dari dokumen multimedia. Pemilik juga dapat mempublikasikan dokumen multimedia yang sudah disisipi watermark dengan aman tanpa harus mempublikasikan dokumen multimedia yang asli. Jika terjadi klaim dari orang lain mengenai dokumen multimedia tersebut, tentu dapat diketahui secara otentik siapa pemilik sebenarnya.
2. **Fingerprinting.** Watermarking dan fingerprinting pada dasarnya sama, hanya saja pada fingerprinting, penyisipan watermark biasanya

bersifat unik untuk suatu dokumen multimedia. Dokumen multimedia yang sama dapat memiliki fingerprint yang berbeda.

3. Copy prevention or control. Teknik watermarking juga dapat dilakukan untuk mencegah dokumen multimedia untuk diduplikasi dengan hardware atau software tertentu. Misalnya untuk mencegah suatu dokumen multimedia yang tersimpan dalam CD atau DVD agar tidak diduplikasi dengan CD atau DVD copier.
4. Fraud and tamper detection. Watermarking juga dapat digunakan untuk mendeteksi adanya pembajakan terhadap suatu dokumen digital.
5. ID card security. Informasi berupa passport atau ID juga dapat disertakan sebagai watermark ke dalam foto orang yang bersangkutan, sehingga jika suatu saat dokumen seperti passport dimanipulasi oleh orang lain dengan mengganti fotonya maka dapat dideteksi.

Metode audio watermarking yang sering dikaji dapat dibagi menjadi (Rumondang, 2002):

1. Domain waktu Metode ini bekerja dengan cara mengubah data audio dalam domain waktu yang akan disisipkan watermark. Contohnya dengan mengubah LSB (Least Significant Bit) dari data tersebut. Secara umum metode ini rentan terhadap proses kompresi, transmisi dan encoding.

Beberapa teknik algoritma yang termasuk dalam metode ini adalah:

- a. Compressed-domain watermarking Pada teknik ini hanya representasi data yang terkompresi yang diberi watermark. Saat data di uncompressed maka watermark tidak lagi tersedia.
- b. Bit dithering Watermark disisipkan pada tiap LSB, baik pada representasi data terkompresi atau tidak. Teknik ini membuat derau pada sinyal.
- c. Amplitude modulation Cara ini membuat setiap puncak sinyal dimodifikasi agar jatuh ke dalam pita-pita amplitudo yang telah ditentukan.
- d. Echo hiding Dalam metode ini salinan-salinan terputus-putus dari sinyal dicampur dengan sinyal asli dengan rentang waktu yang

- cukup kecil. Rentang waktu ini cukup kecil sehingga amplitudo salinannya cukup kecil sehingga tidak terdengar.
2. Domain frekuensi Metode ini bekerja dengan cara mengubah spectral content dalam domain frekuensi dari sinyal. Misalnya dengan cara membuang komponen frekuensi tertentu atau menambahkan data sebagai derau dengan amplitudo rendah sehingga tidak terdengar. Beberapa teknik yang bekerja dengan metode ini:
    - a. Phase coding Bekerja berdasarkan karakteristik sistem pendengaran manusia (Human Auditory System) yang mengabaikan suara yang lebih lemah jika dua suara itu datang bersamaan. Secara garis besar data watermark dibuat menjadi derau dengan amplitudo yang lebih lemah dibandingkan amplitudo data audio lalu digabungkan.
    - b. Frequency band modification Informasi watermark ditambahkan dengan cara membuang atau menyisipkan ke dalam pita-pita (band) spectral tertentu.
    - c. Spread spectrum Dalam metode ini, sinyal yang membawa data watermark dimodulasikan ke dalam derau pita lebar (widebandnoise) setelah sebelumnya di multiplikasi dengan suatu pseudorandom sequence.

## 4.2.2 Steganografi

Seiring dengan pesatnya kebutuhan informasi pada manusia seperti yang terjadi pada saat ini tentu diperlukan kewanala terhadap pesan yang dikirim maupun diterima. Keamanan tersebut diperlukan untuk menghindari adanya penyadapan atau pembajakan terhadap gambar yang mengandung informasi penting bagi penggunaanya. Keamanan diperlukan untuk menjaga integritas gambar tersebut agar tetap aman. Terdapat beberapa cara untuk mengamankan pesan gambar tersebut, yaitu dengan kriptografi dan steganografi. Kriptografi dan steganografi dapat diimplementasikan pada aplikasi untuk mengamankan gambar (Bhaudhayana dan Widiartha, 2015).

Teknik penyembunyian informasi yang cukup terkenal adalah steganografi. Teknik mengurangi kekurangan dari kriptografi yang dapat dengan mudah menimbulkan kecurigaan. Steganografi menyembunyikan informasi rahasia di

dalam informasi lain sehingga informasi tersebut tidak dapat diketahui oleh orang lain yang tidak bersangkutan. Teknik ini mempunyai beberapa metode yang digunakan untuk mengenkripsinya. Salah satunya adalah LSB (Least Significant Bit) dan EOF (End Of File). Kedua metode tersebut mempunyai kelemahan dan kelebihan masing-masing dalam proses enkripsi. Untuk menjaga keamanan file yang berupa pesan tentunya perlu suatu cara agar enkripsi file tidak mudah untuk dipecahkan oleh orang lain serta hasil dari stego image tidak menimbulkan kecurigaan (Aditya, Pratama dan Nurlifa, 2010).

Penggunaan steganografi bertujuan untuk menyembunyikan atau menyamarkan suatu data sehingga sulit untuk dideteksi (encoding). Data yang disembunyikan dapat diekstraksi kembali sama seperti keadaan aslinya (decoding) (Pamungkas, 2020).



**Gambar 4.4:** Steganografi Citra

Menurut Ariyus, (2006), ada tujuh teknik dasar yang digunakan dalam steganografi, yaitu :

1. Injection, merupakan suatu teknik menanamkan pesan rahasia secara langsung ke suatu media. Salah satu masalah dari teknik ini adalah ukuran media yang diinjeksi menjadi lebih besar dari ukuran normalnya sehingga mudah dideteksi. Teknik ini sering juga disebut embedding.
2. Substitusi, data normal digantikan dengan data rahasia. Biasanya, hasil teknik ini tidak terlalu mengubah ukuran data asli, tetapi tergantung pada file media dan data yang akan disembunyikan. Teknik substitusi bisa menurunkan kualitas media yang ditumpangi.



3. Transform Domain, teknik ini sangat efektif. Pada dasarnya, transformasi domain menyembunyikan data pada transform space. Akan sangat lebih efektif teknik ini diterapkan pada file berekstensi JPG.
4. Spread Spectrum, sebuah teknik pentransmisian menggunakan pseudo-noise code, yang independen terhadap data informasi sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (bandwidth) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika pseudo-noise code tersinkronisasi.
5. Statistical Method, teknik ini disebut juga skema steganographic 1 bit. Skema tersebut menanamkan satu bit informasi pada media tumpangan dan mengubah statistik walaupun hanya 1 bit. Perubahan statistik ditunjukkan dengan indikasi 1 dan jika tidak ada perubahan, terlihat indikasi 0. Sistem ini bekerja berdasarkan kemampuan penerima dalam membedakan antara informasi yang dimodifikasi dan yang belum.
6. Distortion, metode ini menciptakan perubahan atas benda yang ditumpangi oleh data rahasia.
7. Cover Generation, metode ini lebih unik daripada metode lainnya karena cover object dipilih untuk menyembunyikan pesan. Contoh dari metode ini adalah Spam Mimic.

## 4.3 Kriptografi Klasik dan Modern

Pada dasarnya, baik kriptografi klasik maupun modern sama-sama menggunakan ilmu matematika dalam proses enkripsi dan dekripsi, hanya saja ilmu matematika yang digunakan pada kriptografi modern lebih rumit dari pada kriptografi klasik. Contoh kriptografi klasik seperti Caesar Cipher, hanya menggunakan konsep substitusi sederhana pada proses enkripsinya, sedangkan pada enkripsi kriptografi modern, seperti RSA memanfaatkan keunikan bilangan prima dalam proses enkripsinya. Adapula yang memakai konsep Ring, Polinom, dan lain-lain.

Banyak di antara kriptografi klasik yang sudah tidak digunakan lagi, alasannya tentu masalah keamanan. Semakin banyak kunci enkripsi yang mungkin dari suatu enkripsi, maka semakin sulit suatu teknik enkripsi untuk dibobol. Contoh enkripsi kriptografi klasik yang sangat mudah dibobol adalah Caesar Cipher, sebab hanya memiliki kunci yang mungkin sebanyak 26 buah saja (termasuk kunci 0/tanpa pergeseran). Sehingga banyak peneliti yang tertarik untuk meningkatkan keamanan kriptografi klasik seperti Caesar Cipher ini.

Dari segi penggunaan kunci, kriptografi klasik masih menggunakan kunci simetris dalam proses enkripsinya, sedang kriptografi modern sudah banyak menggunakan kunci asimetris. Kunci simetris adalah di mana kunci untuk enkripsi dan dekripsi menggunakan kunci yang sama, sedang kunci asimetris adalah di mana kunci untuk enkripsi dan dekripsi menggunakan kunci yang berbeda. Dari segi perkembangan, kriptografi modern terus mengalami perkembangan beriringan dengan berkembangnya ilmu matematika. Sedangkan kriptografi klasik, berkembang dengan penggabungan-penggabungan dengan teknik enkripsi lain yang saat ini banyak dilakukan oleh peneliti (Kriptografi, 2017).



# **Bab 5**

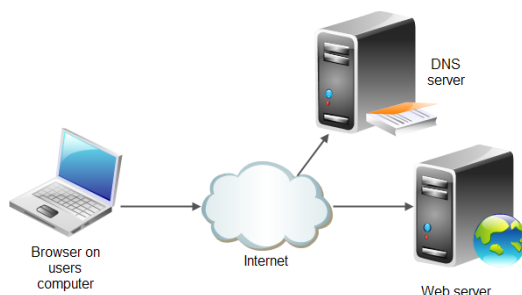
## **Keamanan Web**

### **5.1 Pendahuluan**

Web/ Website yaitu suatu halaman yang berisi kumpulan informasi yang saling terhubung ke sebuah perangkat atau sebuah program komputer. Semenjak ditemukannya Website oleh Sir Timothy John "Tim" Berners-Lee pada Tahun 1991 yang terhubung dengan jaringan sampai saat ini, website menjadi media komunikasi penting yang digunakan hampir seluruh orang didunia (Achyani dan Saumi, 2019). Web/ website dapat diakses melalui jaringan seperti internet ataupun jaringan lokal (LAN) dengan alamat yang diberikan berupa URL/ Uniform Resource Locator (format standar pengalamatan sebuah web). Semua gabungan situs yang ada didunia dapat diakses melalui World Wide Web atau yang dikenal dengan WWW, semua halaman web yang diakses bersifat publik atau diberikannya kebebasan kepada seseorang dalam pengaksesannya tetapi dalam kegiatannya beberapa dari situs web ini mengharuskan pengunjung melakukan pendaftaran atau bahkan meminta pembayaran untuk dapat mengakses isi situs yang terdapat dalam situs web tersebut, contohnya web berita, layanan surat menyurat elektronik dan lain nya (Zabar dan Novianto, 2015).

Sekarang ini, sebuah Web ditulis dalam bentuk HTML/ Hypertext Language yang merupakan kombinasi antara text dan informasi yang terdiri simbol atau kode yang terdapat dalam sebuah file guna menampilkan halaman situs.

HTML dibuat menggunakan software yang disebut editor, terdapat 3 kategori software editor yaitu: (1) Text Editor yaitu software yang umum digunakan programmer dalam menulis kode program yang berisikan syntax highlighting, search dan lain- lain contoh software: Notepad, Notepad ++ dan Sublime Text. (2) WYSIWYG artinya What You See is What You Get artinya apa yang kamu lihat apa yang kamu dapatkan. Jadi editor ini mempunyai kemampuan menghasilkan output yang sama seperti yang terlihat dengan hasil akhirnya.



**Gambar 5.1:** Gambar alur akses web (Josi, 2017)

Dalam penggunaannya tidak menuliskan Text ataupun Symbol HTML tetapi langsung menggunakan GUI (Graphical User Interface) contohnya: Macromedia Dreamweaver dan Microsoft frontpage. (3) Editor yaitu situs yang menyediakan Template atau web sebagai tempat editor sendiri (Sidik, 2014). dalam perancangan sebuah website contohnya: iWeb atau Rapidweaver. Setelah dituliskan pada editor kemudian file HTML tersebut dieksekusi melalui Browser, browser merupakan sebuah aplikasi untuk menerima, menampilkan, dan menerjemahkan informasi dari world wide web. Terdapat macam- macam browser yang sering digunakan user pada saat sekarang ini yaitu Google Chrome, Opera, Mozilla Firefox dan Microsoft Edge. Tahun 1995 diperkenalkan PHP (Hypertext Preprocessor) oleh Rasmus Lerdorf digunakan untuk keperluan dinamisasi sebuah web agar tidak terlihat monoton seperti sebelumnya. Berbeda dengan halnya html hanya digunakan untuk membangun kerangka pada sebuah website, tetapi jika PHP berfungsi sebagai pengatur alur program, bentuk tampilan serta konektivitas dengan berbagai database server (Nazwita, 2017).

Saat ini sangat pesat sekali perkembangan teknologi website membuat mobilitas kegiatan orang- orang yang beralih ke internet yang menyebabkan traffic akses terhadap internet dan web serta situs semakin tinggi. Maka tidak

bisa dielakkan lagi munculnya beberapa ancaman terhadap keamanan web itu sendiri. Berbagai keamanan web seperti kerahasiaan yang sering diincar hacker, Masquerader, virus- virus dari internet maupun dari media transfer data seperti flashdisk, hardisk eksternal, melalui jaringan Internet, download file tanpa proteksi keamanan, Trojan horse, Aktivitas pengguna yang tidak terotorisasi dan masih banyak lagi ancaman keamanan yang kadang tidak sadari.

## 5.2 Keamanan Web

Keamanan suatu website atau web security system merupakan salah satu prioritas yang sangat utama bagi seorang pengelola/ pengguna situs. Kebanyakan pengguna hanya mengutamakan design tampilan dan konten apa supaya menarik pengunjung sebanyak-banyaknya. Jika seorang pengelola atau pengguna mengabaikan keamanan suatu website, maka yang dirugikan adalah pengguna itu sendiri karena seseorang dapat mengambil data-data penting pada suatu website dan bahkan pula dapat mengacak-acak tampilan website (deface) tersebut. Paling utama keamanan sebuah situs adalah melindungi komputer, aplikasi dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya.



**Gambar 5.2:** Gambar ilustrasi ancaman keamanan web (Achyanil, 2016)

Keamanan web sendiri meliputi beberapa aspek, antara lain (Han, 2012) :

1. Privacy, adalah suatu kegiatan yang bersifat rahasia (private). Sebuah kegiatan pencegahan agar data atau informasi di dalam sebuah situs tidak diakses oleh sembarang orang. Contohnya adalah email yang

berisikan file-file yang tidak boleh dibaca, digunakan dan diedit orang lain tanpa seizin pemilik file. Pencegahan yang bisa dilakukan seperti menggunakan teknologi keamanan enkripsi, jadi hanya pemilik informasi yang dapat mengetahui informasi yang sesungguhnya.

2. Confidentiality adalah merupakan kegiatan memberikan data ke orang lain untuk tujuan khusus tetapi tetap dijaga penyebarannya. Contohnya data yang bersifat pribadi seperti : No. id, nama, alamat, nama ibu kandung dan sebagainya. Confidentiality terjadi apabila diminta untuk membuktikan kejahatan seseorang, apakah pemegang informasi akan memberikan informasinya kepada orang yang memintanya atau menjaga kliennya.
3. Integrity adalah penekanannya adalah sebuah informasi tidak diizinkan kecuali sepengetahuan pemilik informasi/ user. Data yang terenkripsi kemungkinan yang tidak terjaga integritasnya keamanannya karena ada kemungkinan chipertext dari enkripsi tersebut berubah. Contoh : Pembaharuan Integritas ketika sebuah email dikirimkan di tengah jalan disadap dan diganti/ fake email, sehingga email yang sampai ke tujuan sudah berubah.
4. Authentication adalah kegiatan ini dilakukan sewaktu user melakukan login pada sebuah situs dengan menggunakan nama user dan passwordnya, apakah sesuai atau tidak, jika sesuai diterima untuk melanjutkan dan tidak akan ditolak. Hal ini berhubungan dengan hak akses seseorang, apakah dia mengakses yang sah atau tidak.
5. Availability adalah aspek ini berkaitan dengan ketersediaan sebuah data saat dibutuhkan. Apabila sebuah data atau informasi terlalu rumit ada kalanya pengamanannya akan menyulitkan pengguna dalam mengakses situs itu sendiri. Disamping itu akses yang lambat juga menghambat terpenuhinya aspek availability. Serangan yang dilakukan pada hal ini adalah denial of service (DoS), yaitu pembatalan service ketika adanya permintaan data sehingga komputer tidak bisa melayaninya. Contoh lain dari denial of service ini adalah mengirimkan request/ request boom yang berlebihan

sehingga menyebabkan komputer tidak bisa lagi menampung beban tersebut dan akhirnya komputer down.

Jadi berdasarkan uraian pada paragraf sebelumnya, kita tahu bahwa sebenarnya web/ internet belumlah benar-benar aman. Beberapa alasan utama ketidakamanan internet adalah sebagai berikut:

1. Internet adalah wilayah bebas, belum adanya hukum atau aturan yang mengaturnya. Hukum dan aturan masing-masing jaringan diserahkan sepenuhnya kepada penanggung jawab jaringan (administrator jaringan internet). Pada kenyataan tidak semua administrator jaringan, memahami dengan baik tentang keamanan internet .
2. Masih banyaknya terdapat celah (hole) di sistem komputer, jaringan maupun pada sebuah web yang bisa dimanfaatkan oleh cracker demi keuntungan/ kepentingan pribadinya.
3. Akses user dari tempat yang lemahnya pengawasan dari orang lain, sehingga muncul keinginan untuk ingin mencoba- coba
4. Kurangnya kesadaran adanya celah (hole) kejahatan di internet oleh kebanyakan user.
5. Belum adanya standar yang mengatur keamanan manajemen jaringan internet.

## 5.3 Metode Penyerangan Web

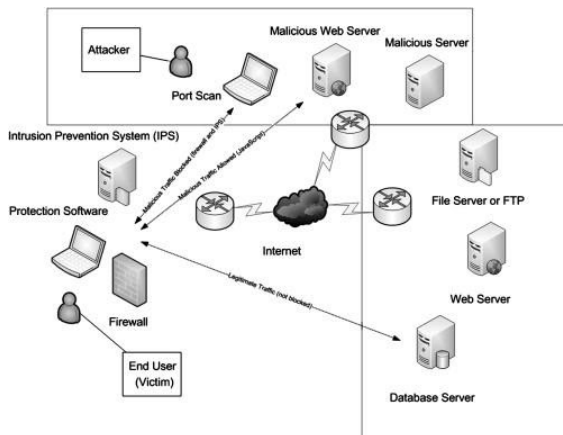
Terdapat beberapa metode yang biasa dan sering digunakan para hacker/ cracker untuk menyerang suatu website:

1. Remote File Inklusi (RFI) adalah Sebuah metode yang menggunakan script PHP `include_once()`, `include()`, `require_once()`, `require()` yang variabel nya tidak dideklarasikan dengan sempurna. Seorang attacker memanfaatkan RFI untuk meng include kan file yang berada di luar server yang bersangkutan (Sun dkk., 2018). Cara paling aman bagi seorang administrator dalam mengatasi hal ini adalah selalu memperhatikan usaha-usaha infiltrasi dan usaha eksploitasi lokal.



Penggunaan firewall dapat mencegah penyusupan orang-orang yang tidak bertanggung jawab dan serta memperhatikan port-port server yang sedang berjalan.

2. Local File Inclusion (LFI) adalah Metode yang memanfaatkan kelemahan script PHP `include_once()`, `require()`, `include()`, `require_once()` yang variabel nya tidak dideklarasikan dengan sempurna. Penyerang biasanya menggunakan LFI dengan mengincludekan file yang berada di dalam server yang bersangkutan (Sun dkk., 2018).
3. SQL injection adalah kode injeksi teknik yang memanfaatkan kelemahan keamanan yang terjadi pada aplikasi database (Dahlan M., Latubessy A., 2015). Hal ini terjadi ketika masukan pengguna tidak benar baik disaring untuk menghindari karakter string literal yang dibuat dalam pernyataan SQL atau masukan pengguna tidak kuat diketik dan dengan demikian tereksekusi. Ini adalah sebuah kerentanan yang dapat terjadi kapanpun salah satu bahasa pemrograman atau script yang tertanam di dalam yang lain. Serangan ini lebih dikenal sebagai serangan penyisipan SQL.
4. Cross Site Scripting (XSS) adalah jenis kerentanan keamanan komputer yang terdapat di aplikasi web yang memungkinkan penyerang berbahaya untuk memasukkan script sisi klien ke dalam halaman web dilihat oleh pengguna lain (Ziegler dan Ziegler, 2014). Cross-site scripting merupakan istilah lain yang merupakan kelemahan sebuah aplikasi web yang yang diserang dengan cara mem-bypass mekanisme klien-sisi keamanan biasanya dikenakan pada konten web oleh browser modern. Dengan cara menginjeksi bad script ke dalam halaman web, kemudian penyerang mendapatkan hak akses diangkat ke konten halaman tertentu, cookie sesi, dan berbagai informasi lainnya yang dikelola oleh browser atas nama pengguna. Serangan Cross-site scripting ini terjadi pada kasus khusus injeksi kode. XSS data diatasi dengan menggunakan Open Source Libraries mengenai pencegahan XSS attack seperti PHP AntiXSS, HTMLPurifier, xssprotect, XSS HTML Filter (OWASP, 2014).



**Gambar 5.3:** Gambar ilustrasi server side attack ( dkk., 2017)

## 5.4 Metode Pertahanan Web

Umumnya web saat sekarang ini dibuat sudah menggunakan beberapa keamanan tambahan yang didapatkan menggunakan certificate, merupakan sebuah protokol keamanan menggunakan enkripsi modern untuk mengirimkan dan menerima informasi penting. Prinsip kerjanya *end to end* atau ujung ke ujung. Berikut contohnya:

### 1. SSL (Secure Sockets Layer)

Protokol yang dikembangkan oleh Netscape untuk komunikasi dokumen yang memiliki privasi melalui jaringan internet. SSL mempunyai sistem enkripsi yang menggunakan dua kunci untuk melakukan enkripsi data. SSL terdiri dari 4 jenis, yaitu (A. Freier, 2015):

- a. SSL web server certificate with EV, SSL jenis ini digunakan bila pengunjung harus input data sensitif seperti credit cards, PIN number, dst yang membutuhkan keamanan ekstra. Bila menggunakan SSL jenis ini, address bar pada browser akan berwarna hijau dan menunjukkan nama organisasi bersangkutan yang telah diverifikasi.

- b. SSL web server certificates, SSL jenis ini digunakan bila pengunjung harus login atau sign in. SSL jenis ini menggunakan enkripsi sekuat SSL web server certificate with EV namun tidak adanya warna hijau pada address bar browser.
  - c. SGC SuperCert, SSL ini mempunyai kompatibilitas pada browser lama. Jika pengunjung menggunakan browser lama, atau cara lain untuk mengunjungi suatu website, maka SSL jenis ini cocok untuk diterapkan di browser tersebut, karena SSL jenis ini memungkinkan kompatibilitas browser lama untuk enkripsi 128 atau 256 bit.
  - d. SSL123 Certificate, SSL ini diterapkan pada komunikasi internal dan intranet private. Cara kerja dari SSL ini yaitu dengan enkripsi untuk pegawai dan user di dalamnya. Hanya nama domain yang akan diverifikasi.
2. IDS (Intrusion Detection System)
- Intrusion Detection System diterapkan untuk pendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Aktivitas tidak sah atau tidak diinginkan yang mengganggu konfidensialitas, integritas dan atau ketersediaan dari informasi yang terdapat di sebuah sistem. IDS akan memantau lalu lintas data pada sebuah jaringan atau mengambil data dari berkas log. IDS akan menganalisa dengan algoritma tertentu untuk memutuskan memberi peringatan kepada seorang administrator jaringan atau tidak (Liao dkk., 2013).
3. IPS (Intrusion Prevention System)
- Intrusion Prevention System (IPS) adalah aplikasi yang bekerja untuk memantau lalu lintas sebuah jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. Produk dari IPS ini sendiri meliputi perangkat keras (hardware) atau perangkat lunak (software). Secara umum IPS terbagi dalam dua jenis yaitu Host-based Intrusion Prevention System (HIPS) dan Network-based Intrusion Prevention System (NIPS) (Panda dkk., 2016).



**Gambar 5.4:** Gambar Penerapan Cyber Security (Sahtyawan, 2019)

### 5.4.1 Keamanan melalui XML

XML signatures merupakan dokumen XML yang berisi informasi tanda tangan digital. Tanda tangan digital dapat dilakukan terhadap dokumen dengan tipe apapun, termasuk dokumen XML. XML signatures dapat ditambahkan pada dokumen XML yang ditandatangani ataupun dapat berupa sebuah dokumen XML tersendiri. Secara garis besar, struktur XML signatures adalah sebagaimana (di mana “?” menandakan nol atau satu kemunculan, “+” menandakan satu atau lebih kemunculan, dan “\*” menandakan nol atau lebih (Deviana, 2011).

#### 1. Kode XML

Salah satu keuntungan penggunaan standar XML signature adalah dapat dilakukannya penandatanganan sebuah dokumen XML oleh lebih dari satu pihak. Pihak tertentu hanya akan menandatangani elemen XML yang menjadi tanggung jawabnya (Triawan dan Prasetyo, 2019).

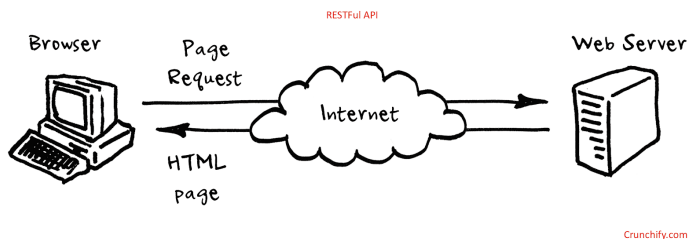
#### 2. XML Encryption

Pengamanan terhadap data yang dipertukarkan merupakan salah satu kebutuhan yang muncul pada proses pertukaran data. Beberapa komunitas telah merekomendasikan Enkripsi XML sebagai metode alternatif untuk pengamanan data dengan menggunakan format XML. Enkripsi XML dirancang untuk dapat diterapkan baik pada data XML maupun data non XML. Implementasi Enkripsi XML memungkinkan

penggabungan data yang telah dienkripsi dengan data yang tidak dienkripsi di dalam satu dokumen XML. Dengan demikian, proses enkripsi maupun dekripsi dapat dilakukan hanya pada data yang memang perlu diamankan saja (Widodo dkk., 2012).

### 5.4.2 Web Service

Web service adalah sistem perangkat lunak yang dirancang untuk mendukung interaksi yang bisa beroperasi machine to machine di atas jaringan. Web service mempunyai alat penghubung yang diuraikan pada format machine processible (secara spesifik WSDL). Sistem lain saling berhubungan dengan web service di dalam cara yang telah ditentukan oleh deskripsinya yang menggunakan pesan soap, secara khas di sampaikan menggunakan HTTP dengan XML serialization, bersama dengan standar lain yang terkait dengan web (Harismawan dkk., 2018).



**Gambar 5.5:** Gambar Ilustrasi Web Service (Robinson dkk., 2015)

Disebut web service karena database dari web tersebut tersimpan dalam sebuah web server berbayar, dan dapat di akses dengan berbagai platform yang tentunya harus terkoneksi dengan internet (Saputra1 dan Aji, 2018). Beda halnya dengan URL web pada umumnya, URL web service hanya mengandung kumpulan informasi, perintah, konfigurasi atau syntax yang berguna membangun sebuah fungsi-fungsi tertentu dari aplikasi. Sebuah teknologi web service merupakan salah satu cara setiap fungsi kegiatan bisnis untuk berkomunikasi. Bukan seperti model client-server tradisional, seperti web server atau sistem halaman web, web service tidak menyediakan GUI untuk para pengguna. Web service hanya menyediakan *business logic*, proses, dan data dalam antarmuka pemrograman antar jaringan. Web service tidak memerlukan browser atau HTML. Sehingga web service dapat ditambahkan ke sebuah GUI (seperti laman web atau aplikasi desktop).

Dari tulisan di atas perlu kita sadari semua bahwa untuk mendapatkan keamanan itu adalah suatu hal yang sangat mustahil, hal ini bisa dibandingkan dengan keadaan yang sebenarnya di dunia nyata. Tidak ada suatu tempat pun yang benar-benar aman kondisinya, walaupun sudah dijaga dengan ketat sekalipun. Begitu juga dengan keamanan sebuah web. Namun yang bisa kita lakukan adalah untuk meminimalisir gangguan keamanan tersebut dengan merancang sebuah pencegahan yang membantu menghentikan pengguna yang tidak sah (penyusup) untuk mengakses setiap bagian dari sistem. Tujuan pengamanan web ini adalah untuk mengantisipasi risiko gangguan seperti ancaman fisik maupun logik baik langsung maupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam situs.



# **Bab 6**

## **Keamanan Email**

### **6.1 Pendahuluan**

Keamanan email adalah istilah untuk prosedur apa pun yang melindungi konten email dan akun dari akses tidak sah. Penyedia layanan email memiliki langkah-langkah keamanan email untuk mengamankan akun klien dan informasi dari peretas (Banday, 2011); (Al-Fedaghi & Alnasser, 2020). Jika anda perlu mengirimkan beberapa informasi kepada klien, email adalah pilihan yang tepat. Jika Anda ingin mengirim klien anda sesuatu yang membuat mereka tetap terinformasi atau berbagi sudut pandang perusahaan Anda, seperti laporan atau studi kasus, email adalah pilihan yang tepat. Email sebagai media komunikasi dan dirancang agar terbuka dan dapat diakses semaksimal mungkin. Ini memungkinkan orang dalam organisasi untuk berkomunikasi satu sama lain dan dengan orang di organisasi lain.

Masalahnya adalah email tidak aman. Hal ini memungkinkan penyerang untuk menggunakan email sebagai cara untuk menimbulkan masalah dalam upaya mendapatkan keuntungan. Baik melalui kampanye spam, serangan malware atau penyusupan email bisnis, penyerang mencoba memanfaatkan kurangnya keamanan email untuk melakukan tindakan mereka, karena sebagian besar organisasi mengandalkan email untuk berbisnis, penyerang mengeksploitasi email dalam upaya mencuri informasi sensitif (Choudhary, 2013); (Lam & Kettani, 2019).



Kebijakan keamanan email ini bisa sesederhana menghapus semua konten yang dapat dijalankan dari email hingga tindakan yang lebih mendalam, seperti mengirim konten yang mencurigakan ke alat sandboxing untuk analisis mendetail (Nghu Phu, Dai Tho, Le Hoang, Ngoc Toan, & Ngoc Binh, 2020); (Mahajan & Goyal, 2020). Organisasi/perusahaan perlu memiliki intelijen yang dapat menindaklanjuti tentang ruang lingkup serangan. Ini akan membantu menentukan kerusakan apa yang mungkin disebabkan oleh serangan tersebut. Setelah organisasi/perusahaan memiliki visibilitas ke semua email yang dikirim, mereka dapat memberlakukan kebijakan enkripsi email untuk mencegah informasi email sensitif jatuh ke tangan yang orang yang tidak bertanggung jawab.

Penting juga untuk menerapkan solusi enkripsi email otomatis sebagai praktik terbaik. Solusi ini harus dapat menganalisis semua lalu lintas email keluar untuk menentukan apakah materi tersebut sensitif. Jika konten sensitif, itu perlu dienkripsi sebelum dikirim melalui email ke penerima yang dituju. Karena ini akan mencegah penyerang melihat email, meskipun mereka mencegatnya. Phishing dapat dilakukan melalui pesan teks, media sosial, atau melalui telepon, tetapi istilah 'phishing' terutama digunakan untuk menggambarkan serangan yang datang melalui email. Email phishing dapat menjangkau jutaan pengguna secara langsung, dan bersembunyi di antara sejumlah besar email jinak yang diterima pengguna yang sibuk. Beberapa penjahat dunia maya menggunakan informasi yang dikumpulkan oleh email phishing untuk memulai serangan dunia maya (Hu, 2020); (Lallie et al., 2020).

## 6.2 Memahami Keamanan Email

Keamanan email adalah serangkaian metode yang digunakan untuk menjaga korespondensi email dan akun aman dari serangan ini (Alabady, Al-Turjman, & Din, 2020). Gerbang email yang aman yang diterapkan di lokal atau di cloud harus menawarkan perlindungan berlapis dari email yang tidak diinginkan, berbahaya. Kontrol ini memungkinkan tim keamanan memiliki keyakinan bahwa mereka dapat mengamankan pengguna dari ancaman email dan memelihara komunikasi email jika terjadi pemadaman. Solusi yang lebih baik adalah dengan menerapkan gateway email aman yang menggunakan pendekatan berlapis-lapis.

Email ditemukan jauh di tahun 1960-an tetapi digunakan dengan kapasitas terbatas dan dengan cara yang terbatas dan populer pada tahun 1993 (Schultz, 2000). Komunikasi email memicu revolusi bisnis karena menghubungkan dunia. Meskipun banyak bentuk komunikasi modern telah ditemukan, email tetap menjadi yang paling populer di dunia korporat. Saat komunikasi email berkembang, itu menjadi bagian penting dari kehidupan pribadi dan profesional kita. Email adalah bagian penting dari penemuan dan investigasi forensik, terutama dengan meningkatnya kejahatan dunia maya. Keamanan email menjelaskan berbagai teknik untuk menjaga keamanan informasi sensitif dalam komunikasi email dan akun dari akses yang tidak sah, kehilangan, atau penyusupan. Email adalah media populer untuk penyebaran malware, spam, dan serangan phishing, menggunakan pesan yang menipu untuk membujuk penerima agar membocorkan informasi sensitif, membuka lampiran atau mengklik hyperlink yang menginstal malware di perangkat korban (Killoran, Graham, & others, 2020). Email juga merupakan vektor entri umum bagi penyerang yang ingin mendapatkan pijakan di jaringan perusahaan dan melangkah data perusahaan yang berharga.

Keamanan email diperlukan untuk akun email perorangan dan bisnis, dan ada beberapa langkah yang harus diambil organisasi untuk meningkatkan keamanan email. Karena popularitas email sebagai vektor serangan, sangat penting bagi perusahaan dan individu untuk mengambil tindakan untuk mengamankan akun email mereka dari serangan umum serta upaya akses tidak sah ke akun atau komunikasi. Malware yang dikirim melalui pesan email bisa sangat merusak. Email phishing yang dikirim ke karyawan seringkali berisi malware dalam lampiran yang dirancang agar terlihat seperti dokumen resmi atau menyertakan hyperlink yang mengarah ke situs web yang menyajikan malware. Membuka lampiran email atau mengeklik tautan di email dapat membuat akun atau perangkat disusupi (Jardine, 2020); (Qashqari, Alhbshi, Alzahrani, Ghwati, & Aljahdali, 2020).

Meskipun email media komunikasi yang sangat berharga namun tetap menciptakan beberapa tantangan bagi pengirim. Miskomunikasi dapat dengan mudah terjadi ketika orang-orang memiliki ekspektasi yang berbeda tentang pesan yang mereka kirim dan terima. Email digunakan untuk berbagai tujuan, termasuk menghubungi teman, berkomunikasi dengan profesor dan supervisor, meminta informasi, dan melamar pekerjaan, magang, dan beasiswa. Model komunikasi lewat email tergantung pada tujuan pesan yang anda kirim. Beberapa orang menganggap email sebagai bentuk komunikasi

yang cepat dan informal cara untuk mengatakan “halo” atau untuk mengajukan pertanyaan singkat. Selanjutnya pikirkan tentang pesan anda sebelum anda menulisnya. Serta jangan mengirim email dengan tergesa-gesa (Albert, 2020).

Hal yang dilakukan dengan tergesa-gesa biasanya akan berdampak buruk terlebih lagi dengan keamanan isi email yang akan kita kirim, karena email adalah format terbuka dan dapat dilihat oleh siapa saja bagi mereka yang tidak bertanggung jawab, sehingga menyebabkan masalah pada keamanan email. Hal tersebut sudah menjadi masalah bagi perusahaan maupun individu karena organisasi mulai mengirimkan informasi rahasia atau sensitif melalui email yang bisa membuat mereka dapat mengetahui informasi yang kita kirim ataupun yang kita terima. Maka dari itu, seorang penyerang dapat dengan mudah membaca isi email dengan mencegatnya. Selama bertahun-tahun, berbagai organisasi telah meningkatkan langkah-langkah keamanan email untuk mempersulit penyerang mendapatkan informasi sensitif atau rahasia. Email sangat penting dalam dunia bisnis saat ini, sehingga pemerintah pun turun tangan untuk menetapkan kebijakan tentang cara menangani arus informasi. Salah satu kebijakannya adalah Undang-undang ITE dan anjuran dari berbagai organisasi tentang melihat konten email yang mengalir melalui server email agar kita dapat memahami apa yang ada di seluruh email.

Email phishing juga dapat digunakan untuk mengelabui penerima agar membagikan informasi sensitif, seringkali dengan menyamar sebagai bisnis yang sah atau kontak tepercaya. Serangan phishing terhadap bisnis seringkali menargetkan departemen yang menangani informasi pribadi atau keuangan yang sensitif, seperti hutang dagang atau sumber daya manusia. Selain meniru vendor atau eksekutif perusahaan yang dikenal, penyerang akan mencoba menanamkan rasa urgensi dalam email phishing untuk meningkatkan peluang keberhasilan mereka. Email phishing yang ditujukan untuk mencuri informasi biasanya akan meminta penerima untuk mengkonfirmasi informasi login, kata sandi, nomor jaminan sosial, nomor rekening bank, dan bahkan informasi kartu kredit mereka (Basit et al., 2020). Beberapa bahkan menautkan ke situs web palsu yang terlihat persis seperti vendor atau mitra bisnis terkemuka untuk mengelabui korban agar memasukkan informasi rekening atau keuangan. Serangan phishing juga dapat digunakan untuk mendistribusikan program berbahaya, akan tetapi lampiran email masih menjadi metode utama untuk pengiriman program jahat (Alabdan, 2020).

## 6.3 Jenis Kejahatan Lewat Email

Email dengan cepat muncul sebagai bentuk komunikasi elektronik yang paling disukai dan berguna di dunia. Tentu saja, popularitasnya menyusut dengan munculnya SMS. Tetapi masih umum menggunakan email untuk berkomunikasi dengan individu dan tetap up to date dengan langganan ke situs web. Miliaran pesan email melintasi dunia setiap hari. Seperti bentuk komunikasi lainnya, email juga disalahgunakan oleh unsur kriminal. Kemudahan dan kecepatan telah menjadikannya alat yang ampuh untuk penjahat. Seperti halnya bentuk komunikasi online apa pun, email rentan terhadap penipuan dan aktivitas kriminal. Berikut adalah beberapa cara paling umum yang digunakan orang untuk menyalahgunakan email untuk tujuan kriminal. Pelanggaran keamanan dapat sangat merusak reputasi pelanggan atau perusahaan. Namun untuk menghentikan serangan penjahat dunia maya membutuhkan berbagai prosedur keamanan email yang berlapis-lapis. Salah satu alasannya adalah karena email secara default bukanlah alat komunikasi yang aman. Karena komunikasi kita berjalan melalui internet dari satu server ke server lainnya. Sebuah serangan phishing dapat merugikan perusahaan jutaan dolar. Oleh karena itu dengan melihat fakta tersebut, pengguna harus berupaya untuk memperdalam kesadaran keamanannya dengan membiasakan diri dengan tanda-tanda serangan phishing (Xiao & Jiang, 2020).

Beberapa kejahatan utama terkait email dapat kita ketahui seperti:

- Spoofing email
- Mengirim kode berbahaya melalui email seperti virus
- Mengirim email yang mengancam
- Catfishing
- Pemboman email
- Email yang memfitnah
- Penipuan email

### 6.3.1 Spoofing email

Email spoof adalah email yang sepertinya berasal dari sumber yang sah tetapi sebenarnya dari sumber yang tidak dapat diandalkan. Biasanya pengirim memalsukan nama atau alamat pembuatnya agar terlihat valid. Misalnya, seseorang mungkin mengirim email dengan berpura-pura menjadi teman dekat

atau situs web terpercaya untuk menipu penerima. Spoofing sering dilakukan dengan tujuan menipu penerima uang. Spoofing email/Email palsu adalah email yang tampaknya berasal dari satu sumber tetapi sebenarnya muncul dari sumber lain. Memalsukan nama dan / atau alamat email pengirim email biasanya melakukan spoofing email. biasanya untuk mengirim email pengirim harus memasukkan informasi berikut:

1. Alamat email penerima email
2. Alamat email orang yang akan menerima salinan email (disebut CC untuk salinan karbon).
3. Alamat email orang yang akan menerima salinan email (disebut CC untuk salinan karbon, tetapi identitasnya tidak akan diketahui oleh penerima email lainnya (dikenal sebagai BCC untuk orang buta kertas pengganda).
4. Subjek pesan (judul / deskripsi singkat dari pesan)
5. Pesan

Layanan email berbasis web tertentu seperti [www.sendfakemail.com](http://www.sendfakemail.com), menawarkan fasilitas di mana selain yang disebutkan di atas, pengirim juga dapat memasukkan alamat email pengirim email yang dimaksud.

### 6.3.2 Mengirim Kode Berbahaya Melalui Email Seperti Virus

Kode berbahaya dapat menyebar ke hampir semua aspek internet. Pesan email adalah beberapa cara yang paling umum terjadi. Seorang pengirim dapat menyebarkan virus, worm, atau Trojan ke jutaan komputer dalam rentang beberapa jam. Email merupakan cara tercepat dan termudah untuk menyebarkan kode berbahaya melalui Internet. Virus Love Bug, misalnya, mencapai jutaan komputer dalam waktu 36 jam setelah dirilis dari Filipina berkat email (Ciesla, 2020). Peretas sering kali mengikat Trojans, virus, worm, dan kontaminan komputer lainnya dengan kartu ucapan elektronik dan kemudian mengirimkannya melalui email kepada orang yang tidak menaruh curiga. Mereka memikat orang untuk membuka lampiran atau mengklik hyperlink yang menginstal malware (seperti virus email) di perangkat pengguna. Kontaminan semacam itu juga dapat terikat dengan perangkat lunak yang tampaknya merupakan tambalan anti-virus. Misalnya. Seseorang menerima email dari Compose From To CC BCC Subject.

### 6.3.3 Mengirim Email Mengancam

Email adalah salah satu metode elektronik paling umum bagi orang untuk mengirim ancaman. Ini mungkin termasuk ancaman penangkapan yang salah, mengungkapkan informasi atau masalah lain. Dalam kasus seperti ini, pengirim sering memeras penerima uang atau sesuatu yang lain sebagai imbalan karena tidak menindaklanjuti ancaman palsu tersebut. Di lain waktu, email dapat digunakan untuk membuat ancaman langsung berupa kekerasan atau jenis bahaya lainnya.

### 6.3.4 Catfishing

Beberapa orang menggunakan email sebagai salah satu cara untuk melakukan penipuan asmara yang biasa disebut dengan catfishing. Ini adalah saat seseorang berpura-pura menjadi orang lain dengan minat romantis pada penerimanya. Ini dapat berkembang menjadi pengirim yang mendapatkan akses ke informasi keuangan dan identifikasi dari penerima.

### 6.3.5 Bom Email

Bom email adalah bentuk penyalahgunaan yang terdiri dari pengiriman email dalam jumlah besar ke suatu alamat email dalam upaya untuk membanjiri kotak surat. Jenis bom surat ini sederhana untuk dirancang tetapi karena kesederhanaannya yang ekstrim membuat mereka dapat dengan mudah dideteksi oleh filter spam. Karena targetnya sering kali adalah host khusus yang menangani situs web dan akun email bisnis, jenis serangan ini bisa saja merusak layanan host tersebut.

### 6.3.6 Email Fitnah

Jika seseorang mempublikasikan komentar yang menghina anda dalam sosial media, anda mungkin dapat menuntut atas pencemaran nama baik, begitupun jika sebuah email berisi informasi palsu yang menurunkan reputasi anda, itu juga dapat dianggap mencemarkan nama baik secara hukum (Siddik & Rahi, 2020). Maka dari itu, sebaiknya kita harus menahan diri untuk tidak menyerang orang secara pribadi atau menyatakan hal-hal yang tidak seharusnya dikatakan atau dilakukan secara langsung baik melalui telepon atau email karena akan menjadi bukti jejak digital. Menghapus atau mencabut email tidak melindungi anda dari pencemaran nama baik karena pesan

disimpan di server perusahaan dan dapat ditarik kembali dari arsip oleh departemen TI atau spesialis TI.

### 6.3.7 Penipuan email

Penipuan lewat email adalah penipuan yang disengaja baik untuk keuntungan pribadi atau untuk merusak orang lain melalui email. bentuk penipuan bisa berupa prospek 'tawar-menawar' atau 'sesuatu yang gratis' dan sangat menggoda. Biasanya menargetkan individu yang naif yang menaruh kepercayaan pada skema untuk menjadi kaya dengan cepat. Email populer di kalangan peretas sebagai alat untuk menyebarkan serangan malware, spam, dan phishing. Mereka menggunakan pesan yang menipu untuk mengelabui penerima agar berbagi informasi sensitif, yang mengakibatkan pencurian identitas. Jenis penipuan email bisa juga berbentuk "permintaan bantuan" yang dikirim kepada calon korban untuk meminta bantuan dengan cara tertentu. Namun, hadiah disertakan untuk bantuan tersebut, yang bertindak sebagai "pengait". Hadiahnya bisa berupa uang dalam jumlah besar, harta karun, atau artefak yang seharusnya bernilai tinggi.

## 6.4 Strategi Keamanan Email Efektif

Mengetahui metode peretas sering kali menjadi kunci untuk mencegah serangan, tetapi bagaimana Anda dapat mencegah serangan yang bahkan tidak dapat Anda lihat? Jawabannya terletak pada penggunaan alat keamanan email paling canggih dan menggabungkannya dengan kesadaran dan proses keamanan. Email telah menjadi cara yang menguntungkan bagi peretas untuk menghasilkan uang dengan cepat. Bagaimanapun, platform komunikasi penting ini merupakan bagian integral dari setiap organisasi. Email dapat membuat atau menghancurkan bisnis kecil karena mereka adalah yang paling rentan dalam serangan cyber.

Bayangkan jika sebuah bisnis tidak memiliki perlindungan apapun saat seorang karyawan mengklik lampiran berbahaya dalam pesan yang menginfeksi jaringan dengan malware. Tetapi jika kita memiliki keamanan yang baik, meskipun penyerang dapat mengetahui sandinya email yang kita miliki, mereka masih tetap terkunci dari akun email tanpa informasi kedua

yang diperlukan (Boussios, 2020). Nah, strategi yang dapat dilakukan untuk melindungi email dari peretas seperti:

#### 6.4.1 Kembangkan Keamanan Email Sesuai Perkembangan IT

Kebanyakan dari kita menganggap diri kita paham akan email. Sayangnya, penipu email terus-menerus mengubah metode mereka dan mengembangkan teknik baru yang sangat canggih setiap hari. Penipuan phishing menjadi semakin canggih, dan cara lama untuk melindunginya tidak lagi memadai. Jika anda ingin memastikan bahwa anda menjaga organisasi anda tetap aman, maka langkah-langkah keamanan anda pun perlu dikembangkan seiring dengan perkembangan ancaman dalam dunia teknologi. Karena jika tidak, akun email akan mudah diretas, setelah peretas memiliki akses ke akun email, mereka sering kali menetapkan aturan tak terlihat yang meneruskan semua email ke akun luar di bawah kendali penyerang. Jika kedua belah pihak dalam percakapan atau kesepakatan tidak waspada atau tidak memiliki perlindungan email yang kuat, peretas dapat meyakinkan salah satu pihak untuk mentransfer ribuan atau bahkan jutaan dolar keluar dari organisasi dan ke kantong mereka sendiri. Perlu diketahui tentang bentuk serangan dunia maya yang terhormat dan semakin canggih. Seperti halnya email phishing di mana metode mencoba mengumpulkan informasi pribadi menggunakan email dan situs web yang menipu. Phishing ini merupakan serangan dunia maya yang menggunakan email terselubung sebagai senjata.

Tujuannya adalah untuk mengelabui penerima email agar percaya bahwa pesan tersebut adalah sesuatu yang mereka inginkan atau butuhkan, seperti permintaan dari bank atau catatan dari seseorang yang berasal dari perusahaan mitra sehingga mengarahkan pemilik email untuk mengklik link atau mendownload lampiran. Seperti kondisi dunia saat ini membuat peretas dan penipu siber memanfaatkan pandemi penyakit virus corona (COVID-19) dengan mengirimkan email palsu dan pesan WhatsApp yang berupaya mengelabui kita agar mengklik tautan berbahaya atau membuka lampiran (Eboibi, 2020). Tindakan ini dapat mengungkapkan nama pengguna dan sandi anda, yang dapat digunakan untuk mencuri uang atau informasi sensitif.



### 6.4.2 Manfaatkan Multifactor Authentication (MFA) dan Mobile Device Management (MDM)

Otentikasi multifaktor (MFA) adalah salah satu cara terbaik untuk mencegah peretas mendapatkan akses ke akun email. Dengan otentikasi multifaktor, akun email tidak dapat diakses kecuali memiliki dua informasi, bukan hanya kata sandi. Jadi meskipun penyerang dapat mengetahui sandinya, mereka masih terkunci dari akun email tanpa informasi kedua yang diperlukan. Selain menggunakan MFA kita juga dapat menggunakan Mobile Device Management (MDM) untuk mengurangi akses dari perangkat yang tidak dikenal atau lokasi yang tidak biasa (Agazzi, 2020). Solusi informasi keamanan dan manajemen menggunakan mobile dapat memantau dan memperingatkan kita tentang asal komunikasi yang tidak biasa dapat membantu mendeteksi jika akun email telah dibajak. Sistem ini memungkinkan organisasi untuk mengidentifikasi kapan email kita diakses oleh pengguna luar dan dari mana akses itu berasal, serta memberi tahu pemilik akun bahwa akun kemungkinan besar telah disusupi.

Selain strategi yang sudah dijelaskan di atas kita juga dapat melakukan pencegahan serangan dari peretas/phising lewat beberapa cara sederhana, seperti:

- Periksa alamat email pengirim
- Periksa link yang disertakan sebelum anda mengklik
- Selalu berhati-hati saat memberikan informasi pribadi.
- Jangan terburu-buru atau merasa tertekan.
- Jika anda memberikan informasi sensitif, jangan panik.
- Jika anda melihat scam atau praktik penipuan lainnya, segera dilaporkan.

Email merupakan media serangan umum untuk penjahat dunia maya, dan solusi keamanan email tradisional tidak cukup untuk melindungi dari ancaman tersebut (Mandal & Khan, 2020); (Alharbi, 2020). Sehingga perusahaan atau instansi memerlukan solusi keamanan email dengan beberapa kemampuan inti seperti:

- Anti phishing
- Perlindungan malware

- Pencegahan kehilangan data
- Pencegahan pengambilalihan akun

Meskipun demikian, penipu masih berhasil dengan bentuk serangan dunia maya ini dan penggunaannya tetap lazim. Selain itu, penjahat dunia maya mengubah taktik untuk menghindari tindakan anti phishing yang diterapkan oleh perusahaan. Seperti trik populer yang digunakan oleh penyerang adalah zombie phish. Penyerang selalu menemukan cara baru dan inovatif untuk melewati tindakan deteksi dan pemfilteran. Maka dari itu, kita tidak dapat memastikan apa yang akan terjadi di masa depan, tetapi kita dapat mengatakan dengan yakin bahwa phishing akan tetap menjadi ancaman yang signifikan bagi individu dan bisnis dalam waktu dekat. Peretas telah mengembangkan paket malware, masing-masing melakukan tugas khusus untuk berkontribusi terhadap kerusakan sistem anda atau pencurian data anda.

Jika anda ingin dilindungi dari serangan email phishing, ingin kolega anda terlindungi dari serangan email phishing dan anda ingin perusahaan anda terlindungi dari serangan email phishing. maka cara terbaik untuk melakukannya adalah dengan menciptakan budaya kesadaran keamanan dunia maya. Perlindungan sistem email adalah tugas yang rumit dan sangat sedikit produk keamanan di pasaran yang dapat memenuhi semua persyaratan secara memadai. Dalam email phishing, penjahat dunia maya biasanya akan menanyakan hal-hal seperti (Marion & Twede, 2020):

- Tanggal lahir
- Nomor jaminan sosial
- Nomor telepon
- Rincian kartu kredit
- Alamat rumah
- Informasi kata sandi (atau apa yang mereka butuhkan untuk mengatur ulang kata sandi anda)

Informasi ini kemudian digunakan oleh penjahat dunia maya untuk menyamar sebagai korban dan mengajukan permohonan kartu kredit atau pinjaman, membuka rekening bank, dan aktivitas penipuan lainnya.

### 6.4.3 Bagaimana Phishing Terjadi?

Phishing terjadi ketika korban membalas email penipuan yang menuntut tindakan segera. Contoh tindakan yang diminta dalam email phishing meliputi:

- Mengklik lampiran
- Memperbarui kata sandi
- Menangani permintaan koneksi media sosial, dll.
- sedang berlangsung dalam situs.

## **Bab 7**

# **Keamanan Jaringan Komputer**

### **7.1 Pendahuluan**

Jaringan komputer sekarang ini telah menjadi tulang punggung teknologi komunikasi di seluruh dunia. Berbagai aplikasi atau yang sistem tidak dapat diakses apabila jaringan komputer yang menghubungkannya tidak berfungsi dengan baik. Untuk memiliki jaringan komputer yang handal tidak hanya membutuhkan alat-alat yang dapat diandalkan, tenaga ahli di bidang jaringan yang berpengetahuan baik namun juga membutuhkan pemahaman yang baik tentang bagaimana mengamankan jaringan komputer itu sendiri. Keamanan jaringan komputer telah menjadi perhatian utama dalam dunia teknologi informasi saat ini. Seringkali terdengar berita tentang jaringan komputer yang diganggu karena serangan peretas (hacker). Ketika seorang peretas dapat menembus jaringan komputer suatu organisasi, maka dapat menimbulkan berbagai jenis kerugian seperti: diaksesnya informasi rahasia, resiko data hilang atau diganti, dan kehilangan kepercayaan dari para pemangku kepentingan.

Setiap organisasi harus mengawasi sistemnya dari kemungkinan serangan dari jaringan komputer, dan ini haruslah menjadi bagian sehari-hari dari aktivitas dari bagian TI (teknologi informasi) perusahaan. Cara yang paling dapat diandalkan untuk menghindari dari serangan jaringan komputer adalah dengan tidak menghubungkan sistem komputer perusahaan dengan jaringan komputer

dan meletakkannya di tempat yang terkunci. Sayangnya hal ini bukanlah solusi yang dapat dilakukan sekarang ini, di mana semua komputer harus terhubung satu dengan yang lain untuk membentuk jaringan yang dapat saling berbagi informasi dan sumber daya. Oleh karena itu organisasi yang menghubungkan sistem mereka dengan jaringan komputer haruslah mengetahui jenis-jenis ancaman, kerentanan dan serangan yang dapat terjadi di jaringan komputer sehingga dapat mengambil langkah-langkah yang dapat mengamankan jaringan komputer mereka dari gangguan dan bocornya informasi kepada pihak yang tidak berhak.

## 7.2. Ancaman, Kerentanan, Serangan di Jaringan Komputer

Dalam keamanan jaringan komputer kita harus dapat membedakan antara ancaman, kerentanan dan serangan. Ancaman berarti sesuatu yang dapat mengganggu operasi jaringan komputer yang dapat dalam bentuk niat jahat, tidak disengaja ataupun akibat kegiatan alam. Kerentanan berarti kelemahan yang terdapat di dalam desain, konfigurasi, implementasi atau manajemen dari jaringan komputer yang rawan dimanfaatkan terhadap ancaman. Serangan berarti teknik atau kegiatan yang digunakan untuk memanfaatkan kerentanan yang ada. Berbagai macam serangan yang dilakukan ke jaringan komputer dapat memanfaatkan kerentanan yang ada sehingga menimbulkan ancaman. Di bawah ini diberikan berbagai macam contoh dari serangan yang dapat terjadi pada jaringan komputer (Canavan, 2001).

### 7.2.1 Virus

Virus adalah program atau kode yang tidak hanya menyerang satu komputer, tapi dapat menyebar ke seluruh sistem. Kode ini dapat menyebar via email, usb drive, dan mengambil data atau merusak data yang ada di komputer. Kode ini dapat menyebar dengan mereplikasi dirinya dari satu komputer dan kemudian menyebar ke komputer-komputer yang lain. Infeksi yang terjadi ini dapat menjadi sangat berbahaya bila virus dapat menginfeksi banyak komputer di dalam jaringan. (Upadhyay and Singh, 2020).

### 7.2.2 Worm

Worm adalah program independen yang dapat berjalan sendiri yang didesain untuk menyebarkan dirinya dari sistem. Pada saat suatu worm aktif, dia akan mengaktifkan proses baru yang adalah replika dari worm tersebut. Setelah itu program ini akan mencari sistem lainnya yang mempunyai kerentanan yang sama dan menginfeksi sistem tersebut dan mereplikasi dirinya ke sistem jaringan tersebut. Dengan menggunakan mekanisme worm dapat menginfeksi banyak sistem dalam waktu yang cepat.

### 7.2.3 Trojan Horses

Trojan horse adalah program atau kode yang bersembunyi di dalam program yang seolah-olah melakukan fungsi yang lain. Tipe serangan ini mendapatkan namanya dari mitos Yunani dari cerita bagaimana kota Troya ditaklukan, di mana penyerang kota tersebut bersembunyi di dalam kuda kayu raksasa yang diletakkan di depan kota tersebut. Kemudian kuda kayu itu dibawa masuk ke dalam kota yang mengakibatkan takluknya kota tersebut dengan tentara musuh yang tidak terlihat tapi dibawa masuk secara sukarela oleh penduduk kota Troya. Aplikasi trojan horse seolah-olah mempunyai fungsi tertentu tetapi di dalamnya mempunyai fungsi yang dapat membahayakan penggunaannya seperti mencatat informasi sensitif dan menyediakan pintu akses kepada pihak yang tidak berhak. Pengguna biasanya melakukan instalasi perangkat lunak yang di dalamnya terdapat trojan horse secara sukarela, tanpa menyadari fungsi berbahaya yang ada di dalam aplikasi yang digunakan.

### 7.2.4 Port Scanning

Port scanning adalah kegiatan pengintaian yang dilakukan oleh peretas dalam fase awal dalam mengumpulkan informasi sebelum melakukan peretasan ke dalam sistem atau jaringan komputer. Aplikasi port scanner digunakan untuk mengetahui port-port yang aktif di suatu sistem yang nantinya dapat dieksploitasi untuk masuk ke dalam sistem. Salah satu aplikasi port scanning yang populer digunakan adalah Nmap, sebuah aplikasi yang digunakan untuk melakukan audit pada jaringan.

### 7.2.5 Spoofing

Spoofing adalah suatu kegiatan di mana seseorang atau suatu aplikasi melakukan pemalsuan identitas atau menyamarkan identitasnya agar dapat

memperoleh akses ke dalam sistem atau jaringan komputer dengan hak akses yang tidak seharusnya diperoleh. Di bawah ini adalah beberapa contoh kegiatan spoofing:

- a. IP Address spoofing, alamat IP (Internet Protocol) adalah alamat unik yang membedakan setiap alat di dalam satu jaringan komputer. IP address spoofing dapat memanfaatkan sistem atau jaringan komputer yang menggunakan autentikasi berdasarkan IP. Jika sumber daya di dalam sistem atau jaringan dapat diakses menggunakan alamat IP tertentu, maka peretas dapat melakukan spoofing dengan mengganti alamat komputer yang digunakan menjadi alamat suatu alamat IP yang mempunyai hak akses. Dalam melakukan IP address spoofing, seorang peretas dapat masuk ke dalam sistem dengan seolah-olah menjadi orang atau komputer lain.
- b. Sequence number spoofing, dalam jaringan komputer berbasis TCP/IP koneksi yang terjadi menggunakan nomor urut (sequence number), nomor urut ini dihasilkan menggunakan suatu algoritma tertentu. Peretas dapat menebak hasil nomor urut dari algoritma yang digunakan dan memasukkan data atau informasi yang diinginkan sehingga dia dapat memperoleh akses ke informasi tertentu.
- c. Session hijacking, dengan teknik yang hampir serupa dengan sequence number spoofing, peretas dapat mengambil alih session yang terjadi antara client dan server sehingga peretas dapat bertindak seolah menjadi pihak yang diinginkan. Dengan cara ini seorang peretas bisa mendapatkan akses ke sistem dengan hak akses yang tidak seharusnya dimilikinya.

Untuk mencegah terjadinya spoofing, salah satu cara yang dapat dilakukan adalah melakukan enkripsi terhadap setiap koneksi yang terjadi dan juga mengamankan aplikasi dan sistem yang terhubung dengan jaringan komputer.

### 7.2.6 DNS poisoning

Domain name system (DNS) adalah komponen penting dari Internet yang dapat dimanfaatkan oleh peretas untuk melakukan serangan ke sistem atau jaringan komputer yang ditargetkan. Salah satu metode yang dapat digunakan

untuk mengendalikan DNS adalah dengan melakukan DNS poisoning. Metode ini memanfaatkan kelemahan yang ada di dalam server DNS yang memungkinkan peretas untuk memasukkan informasi yang tidak benar ke dalam table catatan DNS di dalam server. Hal ini akan mengakibatkan pengguna DNS server mendapatkan IP address yang tidak benar, yang telah diatur oleh peretas untuk mengarahkan pengguna ke alamat IP address yang diinginkan oleh sang peretas. Pengguna seolah-olah mengakses website yang benar, padahal yang sedang diakses adalah website palsu yang sudah disiapkan oleh peretas untuk memperoleh informasi yang diinginkannya dari pengguna tersebut.

### 7.2.7 Sniffing

Sniffing adalah kegiatan pengawasan jaringan yang dapat dilakukan oleh peretas untuk memperoleh informasi dari suatu jaringan komputer. Dengan menggunakan aplikasi atau alat yang tepat, peretas dapat memperoleh informasi tentang komputer yang terhubung ke suatu jaringan, jenis dari sistem operasi, alamat IP ataupun kata sandi dan informasi lainnya yang dikirimkan di dalam jaringan. Untuk menghalangi dan mengurangi risiko informasi dapat bocor ke pihak yang tidak berhak, komunikasi di dalam jaringan sebaiknya menggunakan teknik enkripsi tertentu atau menggunakan aplikasi VPN (virtual private network) yang aman.

### 7.2.8 Denial of Service

Denial of Service adalah suatu serangan yang didesain sedemikian rupa dengan tujuan bahwa sistem atau jaringan komputer yang diserang tidak dapat berjalan dengan baik. Jenis serangan ini berbeda dengan jenis serangan yang telah dijelaskan sebelumnya, di mana jenis serangan ini tidak bertujuan untuk mendapatkan informasi atau mengakses suatu sistem yang tertutup. Denial of Service bertujuan agar sistem atau jaringan komputer yang diserang tidak dapat diakses oleh pengguna. Dengan demikian serangan ini biasanya dimanfaatkan untuk melakukan balas dendam atau meminta pemilik sistem atau jaringan komputer untuk membayar peretas agar serangan tidak dilakukan. Ada banyak jenis serangan denial of service yang ada, di antaranya adalah:

- a. Ping of Death. Jenis serangan ini memanfaatkan kelemahan yang ada di implementasi ICMP yang dilakukan vendor jaringan. Dengan



menggunakan perintah ping (yang digunakan untuk mengetahui apakah suatu host aktif atau tidak di dalam jaringan) dengan ukuran lebih besar dari normal seorang peretas dapat membuat alat jaringan atau komputer tidak dapat diakses atau mengalami crash. Untuk melakukan serangan ini diperlukan sumber daya komputer yang cukup besar dan biasanya apabila kelemahan ini ditemukan, maka vendor akan segera mengeluarkan patch untuk menghilangkan permasalahan.

- b. SYN Flooding. Jenis serangan ini mengeksploitasi proses three-way handshake yang digunakan dalam TCP/IP untuk membuat koneksi antar alat jaringan atau komputer. Dengan menggunakan SYN flooding, peretas melumpuhkan proses ini dengan menghalangi proses handshake selesai. Peretas dapat melakukan ini dengan terus menerus mengirimkan koneksi SYN yang tidak valid dan membuat server akan menunggu koneksi yang sengaja tidak diselesaikan, sehingga server tidak mempunyai waktu untuk melayani pengguna lainnya. Cara untuk mengurangi dampak dari serangan ini adalah dengan mengatur waktu tunggu dari server dalam merespon SYN menjadi lebih pendek.
- c. Serangan Smurf. Serangan ini memanfaatkan permintaan echo ICMP yang dikirimkan dalam broadcast suatu jaringan. Permintaan ini akan mengirimkan ICMP ECHO REQUEST palsu yang seolah-olah dilakukan oleh komputer atau alat jaringan yang ditargetkan. Setiap komputer yang menerima ECHO \_REQUEST ini akan menjawab permintaan ini dan akan membanjiri komputer target dengan jawaban yang sebenarnya tidak dilakukan. Hal ini dapat mengakibatkan komputer yang diserang tidak dapat mengakses jaringan.

## 7.3 Metode Proteksi

Dalam melakukan perlindungan terhadap objek vital kita harus melakukan pencegahan agar tidak ada akses yang dapat dilakukan oleh pihak-pihak yang berhak, hal ini dapat dicapai dengan menggunakan control akses, autentikasi, kerahasiaan, integritas dan *non repudiasi*.

### 7.3.1 Kontrol Akses

Perkembangan teknologi memungkinkan kontrol akses dapat dilakukan dengan berbagai macam cara, di antaranya di bawah ini:

- a. Akses dapat dilakukan di lokasi tertentu. Dengan memperbolehkan akses terhadap jaringan komputer dari lokasi tertentu akan meningkatkan keamanan jaringan. Lokasi yang ditentukan ini dapat dilindungi dengan lebih baik, dengan perangkat keras dan perangkat lunak yang dipersiapkan secara khusus untuk melakukan berbagai verifikasi terhadap pengakses sistem.
- b. Kartu identifikasi. Dengan menggunakan kartu identifikasi yang hanya dimiliki oleh pihak yang berhak, akses terhadap sistem dapat dilindungi secara lebih baik. Berbagai jenis kartu seperti kartu magnetik, barcode, kartu RFID (radio frequency identifier) dapat digunakan.
- c. Identifikasi biometrik. Ini merupakan metode akses kontrol yang paling banyak digunakan sekarang ini, karena menawarkan tingkat keamanan yang lebih tinggi dari kontrol akses menggunakan kartu. Metode identifikasi biometric yang diimplementasikan sekarang ini adalah dalam bentuk: sidik jari (fingerprint), iris (mata), wajah, dan pengenalan suara.

Selain dari melindungi jaringan komputer dengan kontrol akses secara fisik, hal ini dapat dilakukan pula dengan menggunakan perangkat lunak. Apabila sistem diakses dari jarak jauh (remote) maka dapat digunakan aplikasi yang dapat mengumpulkan dan menyimpan catatan lengkap mengenai identitas pengaksesnya, mulai dari waktu, IP address, nama komputer, jenis sistem operasi, jenis browser yang digunakan, dsb. Dengan demikian dapat dilakukan

pengawasan terhadap pihak-pihak yang melakukan akses ke dalam sistem atau jaringan komputer yang dilindungi.

### 7.3.2 Autentikasi

Autentikasi adalah langkah penting dalam memproteksi jaringan komputer di mana pada langkah ini dilakukan identifikasi terhadap pengguna. Identitas pengguna diverifikasi dengan cara dibandingkan dengan catatan atau informasi yang telah tersimpan sebelumnya. Di bawah ini merupakan beberapa cara autentikasi dapat dilakukan:

- a. Menggunakan username, kata kunci (password) atau kombinasi dari keduanya. Dalam melakukan autentikasi dapat dilakukan dengan meminta username tertentu yang mempunyai hak akses, atau meminta kata kunci yang sudah ditentukan sebelumnya. Seringkali untuk mengakses sumber daya yang dapat diakses dari jaringan yang diminta adalah merupakan kombinasi dari username dan kata kunci.
- b. Dengan menggunakan kartu identitas. Seperti telah dibahas di bagian kontrol akses, penggunaan kartu identitas yang terdaftar adalah salah satu cara yang dapat digunakan untuk melakukan autentikasi terhadap pengguna. Orang yang mempunyai kartu akan dapat mengakses sumber daya yang ditentukan. Penggunaan kartu ini juga biasanya dapat dikombinasikan dengan cara autentikasi lainnya.
- c. Dengan menggunakan biometrik. Penggunaan jenis-jenis biometrik sebagaimana dijabarkan di bagian kontrol akses dapat digunakan untuk melakukan autentikasi terhadap pengguna. Penggunaan biometrik dapat menawarkan tingkat keamanan yang lebih tinggi karena identitas melekat langsung kepada pengguna yang berhak dan tidak dapat dipindahtangankan.

### 7.3.3 Kerahasiaan

Kerahasiaan dari data atau informasi yang dapat diakses melalui jaringan komputer merupakan bagian yang tidak terpisahkan dari keamanan jaringan komputer itu sendiri. Keamanan data dapat dilakukan dengan melindungi data atau informasi dengan algoritma enkripsi tertentu sehingga ketika data itu berpindah tangan maka data itu tidak bisa diakses tanpa mengetahui kunci

yang telah ditentukan. Enkripsi juga digunakan dalam proses komunikasi yang terjadi ketika data dikirimkan dari satu titik ke titik yang lainnya. Dengan menggunakan enkripsi, pengiriman data terlindungi dari sniffers, suatu aplikasi yang dapat digunakan untuk menyadap komunikasi sedang berlangsung.

### 7.3.4 Integritas

Integritas dilakukan untuk meyakinkan bahwa data yang diakses atau dikirimkan merupakan informasi yang utuh dan benar sesuai dengan yang dikirimkan. Pada saat dikirimkan melalui jaringan komputer, data mungkin saja diakses oleh pihak yang berhak dan diubah sehingga tidak sama dengan data awal yang dikirimkan. Dengan menggunakan enkripsi dan algoritma hashing, meyakinkan bahwa integritas data yang dikirimkan adalah utuh.

## 7.4 Mengamankan Jaringan Komputer

Sebelum membahas mengenai bagaimana mengamankan jaringan komputer, kita harus mengerti bahwa keamanan merupakan sebuah proses yang dilakukan secara terus menerus untuk memproteksi sebuah objek dari akses yang tidak sah (Kizza, 2017). Objek ini bisa saja berupa orang, properti berupa tanah atau bangunan dan sistem komputer atau file. Oleh karena itu di dalam melakukan pengamanan terhadap jaringan komputer kita harus melakukan pengamanan terhadap fisik dari jaringan komputer itu sendiri dan juga terhadap perangkat lunak yang digunakan. Setelah perangkat keras dan lunak dapat digunakan, maka langkah selanjutnya adalah dengan menggunakan perangkat tambahan seperti Firewall ataupun Network Intrusion Detection/Network Intrusion Prevention yang memungkinkan kontrol terhadap lalu lintas jaringan dapat dilakukan secara mendetail dan pengawasan dapat dilakukan secara proaktif.

### 7.4.1 Mengamankan Perangkat Keras

Dalam melakukan pengamanan terhadap perangkat keras jaringan komputer, proteksi dilakukan secara berlapis. Perlindungan dilakukan terhadap area terluar dari lokasi di mana lokasi sistem yang perlu mendapatkan perlindungan. Area terluar dapat dilindungi dengan pagar kawat/besi/tembok beserta dengan sensor getaran/gerakan, lampu keamanan, dan closed-circuit

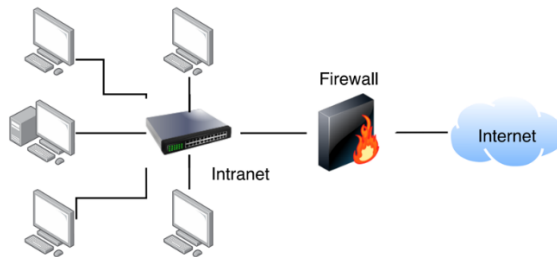
television (CCTV). Selanjutnya berbagai macam sekat keamanan seperti pintu dengan kunci khusus, gerbang pembatas, X-Ray/Body scanner harus ditempatkan di berbagai tempat untuk meyakinkan bahwa setiap bagian dari tempat yang diamankan hanya diakses oleh orang yang berhak dan mereka tidak membawa sesuatu yang dapat membahayakan sistem yang dilindungi. Melindungi perangkat keras juga berarti melindungi setiap alat atau komponen yang digunakan untuk melakukan input ke dalam sistem termasuk keyboard, mouse, touchscreen, dsb. Alat-alat jaringan juga haruslah dilindungi dengan baik seperti: firewall, hub, switch, router, gateway yang rentan diakses oleh peretas. Kemudian jaringan komunikasi seperti kabel, wireless haruslah dilindungi untuk mencegah jaringan diakses oleh penyadap.

### 7.4.2 Mengamankan Perangkat Lunak

Dalam melindungi perangkat lunak jaringan komputer berarti melindungi perangkat lunak yang digunakan oleh perangkat keras jaringan seperti: sistem operasi, server protocol browser, perangkat lunak aplikasi dan juga properti intelektual yang disimpan di dalam tempat disk atau database yang disimpan di dalam jaringan. Hal ini juga berarti melindungi aplikasi perangkat lunak yang digunakan seperti: portofolio investasi, data keuangan, gambar atau file pribadi yang disimpan (Kizza, 2017).

### 7.4.3 Firewall

Firewall dapat berupa perangkat keras atau perangkat lunak yang digunakan untuk mengontrol apa yang dapat masuk atau keluar dari jaringan komputer. Firewall biasanya ditempatkan di tempat di mana level kepercayaan berubah. Firewall biasanya ditempatkan di perbatasan antara jaringan internal dan Internet. Firewall juga dapat ditempatkan di dalam jaringan internal untuk membatasi akses ke sumber daya yang sensitif dan hanya dapat diakses oleh pengguna dengan hak akses tertentu. Firewall bekerja dengan memeriksa setiap paket yang datang dan keluar dari jaringan. Setiap paket dibandingkan dengan aturan yang telah dibuat di dalam Firewall dan hanya memperbolehkan paket yang sesuai dengan aturan untuk dapat melintasi Firewall. Sebagai contoh sebuah Firewall dapat membatasi lalu lintas di jaringan internal sehingga hanya memperbolehkan akses ke email atau web tetapi tidak memperbolehkan jenis lalu lintas lainnya.



**Gambar 7.1:** Jaringan Komputer Dengan Firewall

#### 7.4.4 Network Intrusion Detection dan Network Intrusion Prevention

Walaupun alat pengaman di dalam jaringan sudah terpasang dan berfungsi dengan baik, diperlukan suatu aplikasi network intrusion detection yang dapat mengawasi jaringan, komputer atau aplikasi yang digunakan terhadap adanya aktivitas yang tidak berizin. Aplikasi yang dapat mendeteksi terjadinya network intrusion bekerja dengan cara membandingkan aktivitas yang terjadi di jaringan dengan signatures yang sudah dikenali sebelumnya dan disimpan di dalam database. Pada dasarnya teknik ini dapat berfungsi dengan baik, kecuali ada jenis serangan yang baru yang belum ditemukan signaturenya. Jenis pengawasan berikutnya yang dapat dilakukan adalah deteksi berdasarkan terjadinya anomali. Apabila ada anomali di dalam jaringan, yang dapat membentuk pola lalu lintas tertentu di dalam jaringan, maka aplikasi dapat mendeteksi pola ini dan melaporkannya kepada administrator jaringan.



# **Bab 8**

## **Keamanan Sistem Operasi**

### **8.1 Sistem Operasi**

Sistem operasi adalah sebuah perangkat lunak yang bertugas untuk mengatur sumber daya perangkat keras (Hardware) dengan perangkat lunak (Software), sistem operasi juga sebagai penghubung antara Pengguna (Brainware) dengan perangkat keras (Hardware). Jika sebuah komputer tanpa sistem operasi hanya sekumpulan besi yang tidak berguna. Sistem Operasi adalah perangkat lunak sistem yang mengatur sumber daya dari perangkat keras (Hardware) dan perangkat lunak (Software), serta sebagai jurik (daemon) untuk program komputer. Tanpa sistem operasi, pengguna tidak dapat menjalankan program aplikasi pada komputer mereka, kecuali program booting (Rusmana, 2018).

Sistem operasi menurut para ahli:

- a. Menurut Iim Rusyamsi, Sistem operasi adalah perangkat lunak yang memiliki tugas mengontrol dan mengatur perangkat keras sekaligus operasi dasar sistem lainnya termasuk untuk menjalankan program aplikasi.
- b. Sama halnya, M. Suyanto pun berpendapat bahwa Sistem operasi adalah suatu sistem yang terdiri atas beberapa komponen perangkat



lunak atau software yang memiliki fungsi untuk mengontrol seluruh aktivitas yang sudah dilakukan komputer.

Dari pengertian sistem operasi di atas, bisa kita simpulkan bahwa sistem operasi pada intinya adalah perangkat lunak yang punya tugas mengatur dan mengontrol cara beroperasinya sebuah perangkat bisa komputer, smartphone dan lainya (Italia, 2019).

## 8.2 Fungsi Sistem Operasi

Sistem Operasi memiliki banyak fungsi pada komputer. Fungsi inti inilah yang akan mengintegrasikan seluruh sumber daya yang ada dalam komputer Mulai dari hardware hingga software (Pagi, 2020).

1. Manajemen Sumber Daya Komputer

Sistem operasi sebagai pengatur waktu aplikasi yang dijalankan, membagi penggunaan CPU saat aplikasi berjalan bersamaan, memberi akses pada perangkat keras komputer.

2. Tampilan Antar Muka (Interface)

Dengan adanya tampilan antar muka akan lebih mudah untuk dipahami. Sehingga tidak perlu memasukkan perintah yang rumit untuk menjalankan hardware atau software di dalam komputer.

3. Koordinasi

Sistem operasi sebagai mengatur seluruh aktivitas yang berjalan dari berbagai perangkat lunak sesuai dengan urutan yang tepat. OS juga mengatur setiap kegiatan yang berhubungan dengan perangkat keras yang terhubung.

4. Pelindung File

Sistem operasi sebagai membatasi akses dan melakukan perubahan pada sistem atau aplikasi. melindungi Sebuah file sistem yang mengalami kerusakan atau hilang, jika ada kerusakan pada sistem maka komputer tidak dapat berjalan dengan baik. Begitu juga sebuah aplikasi, jika ada file yang error, aplikasi tersebut akan berjalan tidak normal.

#### 5. Penerjemah

Sistem operasi sebagai penerjemah dari bahasa manusia ke bahasa mesin dan sebaliknya. Komputer beroperasi dengan bahasa pemrograman yang sangat rumit, Sistem operasi menerjemahkan bahasa pemrograman tersebut agar pengguna dapat mengoperasikan komputer dengan mudah.

## 8.3 Jenis - Jenis Sistem Operasi

Jenis sistem operasi yang digunakan terbagi menjadi dua jenis yaitu Sistem Operasi Berbasis Desktop dan Sistem Operasi Berbasis Mobile, yang membedakan kedua sistem operasi ini adalah hardwarenya, sistem operasi berbasis desktop itu digunakan oleh komputer sedangkan sistem operasi berbasis mobile itu digunakan oleh gadget/HP/Smartphone.

### 8.3.1 Sistem Operasi Berbasis Dekstop

Berikut ini jenis – jenis sistem operasi berbasis desktop untuk perangkat komputer atau laptop yang sering digunakan.

#### 1. Microsoft DOS

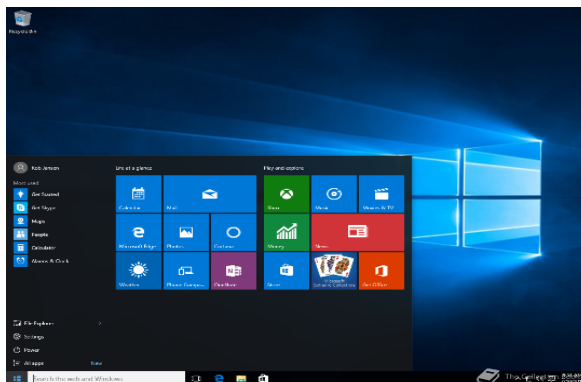
MS DOS merupakan generasi pertama sistem operasi buatan Microsoft. Sistem operasi ini banyak digunakan oleh komputer dari IBM-PC dan dirilis pada tahun 1981. User Interface dari sistem operasi ini masih berupa tulisan tanpa adanya gambar yang sekarang dikenal dengan istilah Command Prompt.



**Gambar 8.1:** Ms Dos (Hadi, 2020)

## 2. Windows

Sistem Operasi Windows pengembangan dari Microsoft DOS dengan tampilan yang sudah memiliki gambar atau GUI (Graphical User Interface). Dengan adanya tampilan grafik tersebut, pengguna akan jauh lebih mudah dalam mengoperasikan komputer.



**Gambar 8.2:** Windows (Wikipedia, 2020)

## 3. Macintosh atau MAC OS

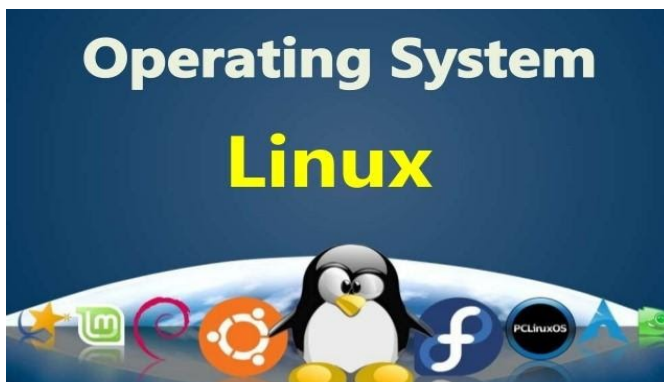
Sistem operasi Macintosh (MAC) adalah sistem operasi yang dibuat Khusus untuk perangkat Apple. Mulai dikembangkan pada tahun 1984 untuk proyek bernama LISA. MAC juga telah mengeluarkan beberapa versi hingga saat ini.



**Gambar 8.3:** MacOS (Bosman, 2020)

#### 4. Linux

Sistem operasi Linux merupakan sistem operasi yang bersifat open source. Artinya, pengguna bebas untuk mengembangkan sistem operasi ini sesuai dengan kebutuhannya. Tentu hal ini menjadi favorit bagi para pengembang mandiri, karena dengan linux mereka bisa mengubah, menambah atau mengurangi sistem di dalamnya.



**Gambar 8.4:** Linux (Anishkumardey, 2020)

#### 5. UNIX

Hampir sama dengan sistem operasi pada DOS. Memiliki beberapa versi yang sempat dirilis di publik secara gratis. OS ini juga terbilang

cukup aman dan susah terkena virus. Meski begitu, UNIX sudah mulai ditinggalkan dan belum mampu menandingi kelebihan dari sistem operasi kompetitor lainnya.



**Gambar 8.5:** UNIX (Pratiksha6294, 2020)

### 8.3.2. Sistem Operasi Berbasis Mobile

Sistem operasi ini yang sering digunakan smartphone, sistem operasi ini sudah banyak yang dirilis tetapi hanya sedikit yang masih bertahan di pasaran.

#### 1. Android

Sistem operasi ini digunakan oleh sebagian besar smartphone yang ada di pasaran. Awalnya Sistem operasi ini dikembangkan oleh perusahaan bernama Android Inc yang akhirnya dibeli oleh Google. Android adalah Sistem Operasi Mobile yang didasarkan pada versi modifikasi dari kernel Linux dan Software open source lainnya, yang dirancang terutama untuk *device mobile* touchscreen seperti smartphone dan tablet. Android dikembangkan oleh konsorsium pengembang yang dikenal sebagai Open Handset Alliance, dengan kontributor utama dan pemasar komersialnya Google



**Gambar 8.6:** Android (Raphael, 2020)

## 2. iOS

Sebelum adanya android, Apple lebih dulu memperkenalkan sistem operasi untuk perangkat mobilenya bernama iOS. Jika Macintosh adalah OS untuk perangkat komputer milik Apple, iOS hadir khusus untuk perangkat mobile mereka seperti iPhone dan iPad. Perkembangan selanjutnya, OS ini juga dijalankan pada perangkat Apple TV.



**Gambar 8.7:** iOS (Tillman, 2020)

## 3. Symbian

Anda pernah menggunakan ponsel genggam pada tahun sebelum maraknya HP berteknologi touchscreen, Anda pasti akan menjumpai

nama-nama besar seperti Nokia, Sony Ericson dan Siemens. Merk-merk besar tersebut menggunakan sistem operasi symbian dalam perangkatnya. Namun, OS ini kian ditinggalkan setelah munculnya Android, iOS dan Windows Phone.



**Gambar 8.8:** Symbian (Wowkeren, 2020)

#### 4. Windows Phone

Windows Phone atau yang sebelumnya disebut Windows Mobile merupakan sistem operasi yang dikembangkan Microsoft untuk dijalankan pada perangkat smartphone. Nokia sempat menggunakan OS ini, namun tidak terlalu berhasil karena dominasi Android dan iOS yang kian tak terbendung hingga kini.



**Gambar 8.9:** Symbian (Gewirtz, 2018)

### 5. Blackberry OS

Sama dengan Apple, Blackberry hadir cukup eksklusif dengan beberapa layanan dan juga sistem operasi milik mereka sendiri. Pada masanya, memang perangkat Blackberry adalah salah satu perangkat yang sangat populer. Bisa dikatakan menjadi perangkat peralihan antara model seluler lama era Nokia dengan ponsel terbaru milik Samsung. OS blackberry juga sempat disematkan pada ponsel terbaru mereka berteknologi touchscreen. Alih-alih mampu memberikan alternatif pilihan bagi dunia smartphone, Blackberry justru makin terpuruk dengan berkembangnya ponsel Android. Konsumen sudah terlalu nyaman dengan berbagai fitur dan aplikasi yang disediakan oleh Android dan Play Store.



**Gambar 8.10:** Blackberry (Blackberry, 2020)

## 8.4 Keamanan

Masalah keamanan merupakan salah satu aspek terpenting dari sistem komputer. Masalah keamanan seringkali kurang mendapat perhatian dari para pengelola sistem komputer. Seringkali masalah keamanan berada di urutan kedua, ketiga, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Konfigurasi keamanan sistem bisa mengganggu performansi dari sistem, namun seringkali masalah keamanan tidak begitu dipedulikan bahkan ditiadakan. Saat ini sistem komputer banyak terhubung dengan jaringan sehingga semakin mudah untuk diakses, sehingga sangat



rentan terhadap kelemahan komunikasi data, yaitu kejahatan komputer. Apalagi di masa ini masyarakat bergantung pada komputer untuk menciptakan, menyimpan dan mengatur informasi-informasi penting seperti informasi keuangan, informasi diri, informasi perusahaan dan sebagainya. Jadi pengguna dan pengelola sistem komputer perlu melindungi komputer dan data mereka agar tidak hilang, rusak ataupun disalahgunakan.

Istilah keamanan pada sistem komputer mengacu pada seluruh masalah keamanan agar sumber daya tidak digunakan atau dimodifikasi oleh orang yang tidak berhak. Pengamanan itu sendiri termasuk masalah teknis, manajerial, legalitas dan politis. (Wahid, 2019). Arti dari keamanan komputer telah berubah dalam beberapa tahun terakhir. Sebelum masalah keamanan data/informasi menjadi populer, kebanyakan orang berpikir bahwa keamanan komputer difokuskan pada alat alat komputer secara fisik.(Soewito, 2019). Secara tradisional, fasilitas komputer secara fisik dilindungi karena tiga alasan:

1. Untuk mencegah pencurian atau kerusakan hardware
2. Untuk mencegah pencurian atau kerusakan informasi
3. Untuk mencegah gangguan layanan

Banyak terjadi pertukaran informasi setiap detik di internet. Banyak terjadi pencurian informasi itu sendiri oleh pihak-pihak yang tidak bertanggung jawab. Ancaman keamanan yang terjadi terhadap informasi adalah :

1. Interruption : Ancaman terhadap availability; informasi, data yang ada dalam sistem komputer dirusak, dihapus, sehingga jika ada informasi yang dibutuhkan tidak ada lagi.
2. Interception : Ancaman terhadap kerahasiaan (secrecy). Informasi yang ada disadap atau orang yang tidak berhak mendapat akses ke komputer tempat informasi tersebut disimpan.
3. Modifikasi : Ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan diubah sesuai dengan keinginan orang tersebut.
4. Fabrication : Ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru (memalsukan) suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi.

Tujuan dari keamanan (Security) sistem tersendiri, sebagai berikut :

1. **Integritas Data**  
Seperti misalnya pengguna yang tidak memiliki otorisasi untuk mengakses data, maka tidak mungkin dapat mengubah atau memodifikasi data yang ada.
2. **Kerahasiaan Data**  
Sistem dapat menjamin bahwa data yang telah ditentukan atau yang tersimpan untuk tidak dapat dibaca oleh pengguna lain pada sistem, data tersebut benar-benar aman aman dan rahasia.
3. **Ketersediaan Akses ke Sistem**  
Tidak ada seorangpun, sekalipun dengan akses ke sistem dapat menyebabkan sistem menjadi tidak dapat digunakan. Sebagai contoh, serangan denial of service melalui internet.

Keamanan pada komputer meliputi aspek berikut ini :

1. **Authentication** : Agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari orang yang dimintai informasi, dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki.
2. **Integrity** : Keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan bahwa dalam perjalanan, informasi yang dikirim tidak termodifikasi oleh orang yang tidak berhak.
3. **Non Repudiation**: Merupakan hal yang bersangkutan dengan si pengirim, si pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. **Authority**: Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.
5. **Confidentiality**: Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Confidentiality biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
6. **Privacy**: Lebih kepada data-data yang sifatnya pribadi.
7. **Availability**: Berhubungan dengan ketersediaan informasi ketika dibutuhkan, sistem informasi yang diserang atau di jebol dapat menghambat atau meniadakan akses ke informasi.

8. Access Control: Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan masalah authentication dan juga privacy. Access Controll seringkali dilakukan dengan menggunakan kombinasi ID user dan password atau dengan menggunakan mekanisme lainnya

## 8.5 Keamanan Sistem Operasi

Pengamanan perangkat lunak cenderung memfokuskan pada pengamanan sistem operasi, karena perangkat lunak aplikasi juga memberi resiko keamanan. Keamanan sistem operasi merupakan bagian masalah keamanan sistem komputer secara total. Pengamanan sistem operasi berarti kecil jika setiap orang dapat melenggang di ruang sistem komputer. Pengamanan secara fisik dengan membatasi pengaksesan fisik secara langsung dengan fasilitas sistem komputer harus dilakukan juga (Wahid, 2019).

Keamanan dari segi sistem itu sendiri terbagi menjadi tiga, yaitu :

1. Keamanan Eksternal  
Berkaitan dengan pemakaian fasilitas komputer dari penyusup (seperti hacker) dan bencana seperti kebakaran dan banjir.
2. Keamanan Interface Pemakai  
Berkaitan dengan identifikasi pemakai sebelum memakai diizinkan mengakses program dan data yang disimpan.
3. Keamanan Internal  
Berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tidak terkorupsi untuk menjaga integritas program dan data. Istilah keamanan (security) dan proteksi (protection) sering digunakan secara bergantian. Untuk menghindari kesalahpahaman, istilah keamanan mengacu ke seluruh masalah keamanan dan istilah mekanisme proteksi mengacu ke mekanisme sistem yang digunakan untuk memproteksi atau melindungi informasi pada sistem komputer.

## 8.6 Meningkatkan Keamanan Komputer

Ada beberapa cara yang bisa Anda gunakan untuk meningkatkan keamanan komputer:

1. Gunakan antivirus dan antispam  
Sudahkah Anda menginstall antivirus? Antivirus memiliki fungsi menjaga, mengamankan, menemukan, dan memusnahkan virus yang mengancam sistem komputer. Di Indonesia, persebaran virus justru lebih banyak terjadi melalui flashdisk. Karenanya proteksi menggunakan antivirus sangat penting. Tidak perlu menggunakan antivirus mahal. Antivirus yang gratis pun sudah cukup. Meski demikian, tidak ada salahnya menggunakan dua sistem keamanan sekaligus, selama fungsinya tidak berkonflik. (Andi, 2018)
2. Update patch OS Anda bila tersedia  
OS atau Operating System adalah sistem pengoperasian komputer yang Anda gunakan. Misalnya Windows 7 atau Windows 10. Secara berkala, pihak pengembang OS menambahkan update patch untuk operating systemnya. Jika saat Anda sedang menggunakan komputer dan muncul notifikasi update, maka lakukanlah pembaruan di OS Anda. Setiap pembaruan berarti ada perbaikan, dan tidak menutup kemungkinan ada peningkatan keamanan yang ditambah.
3. Gunakan Firewall  
Ibaratkan komputer sebagai perumahan. Maka, firewall adalah satpamnya. Firewall bertugas mengawasi keluar masuknya data, dari internet ke komputer, maupun dari komputer ke internet. Fungsi pengawasan ini adalah untuk memastikan bahwa file yang datang adalah file yang aman, dan juga memastikan file keluar bukanlah file yang diambil secara paksa/curian. Jika data yang keluar menuju ke internet terjadi tanpa seizin, maka firewall dengan segera akan menghalangi proses pengiriman data tersebut, dan memblokir pemohon file. Secara umum, firewall juga efektif dalam menyaring virus, trojan, penyadapan email, serta spyware yang merekam input data di komputer. Firewall juga menyaring dan memeriksa lalu lintas

data yang keluar masuk, memastikan semua lalu lintas data terjadi karena seizin.

4. Jangan Login Akun Penting Dari Wifi Umum

Wifi publik tentu saja menyenangkan. bisa mengakses internet tanpa terpotong kuota. Namun, hotspot di tempat umum bisa sangat beresiko. Tidak menutup kemungkinan, seseorang di tempat umum tersebut memasang software perekam data, yang bisa merekam alamat situs yang diakses, username, serta password. Jika sekadar login ke akun sosmed mungkin tidak masalah. Namun sebaiknya jangan mengakses akun e-banking atau e-mail di tempat umum. Karena informasi penting yang kita miliki bisa dicuri orang, lalu digunakan untuk kepentingannya sendiri.

5. Gunakan Kombinasi Password Yang Rumit

Salah satu tips keamanan lainnya adalah dengan menggunakan kombinasi password yang rumit. Apabila kata kunci yang digunakan adalah kosakata yang ada di kamus, password semacam itu akan terbongkar menggunakan program hanya dalam waktu 2 detik. Sementara kombinasi berupa angka, tanda baca, dan huruf besar huruf kecil baru bisa dibongkar dengan estimasi sekitar jutaan tahun.

6. Menggunakan ACL (Access Control List)

Tips meningkatkan keamanan komputer lainnya adalah menggunakan ACL. ACL, atau Access control list, adalah penyortiran lalu lintas data berdasarkan kategori. Hal ini akan krusial ketika butuh kendali dalam lalu lintas data.

7. Lakukan Back Up Secara Rutin

Ransomware Wannacry beberapa waktu lalu punya kemampuan mengunci data hingga tidak bisa diakses. Jika mau dibuka, harus membayar sejumlah uang. Sebenarnya hal ini tidak perlu dilakukan jika kita melakukan backup data secara rutin. Backup maksudnya adalah mengcopy data ke suatu tempat sebagai data cadangan, jika sewaktu-waktu data utama rusak atau hilang. Hal ini tergolong mudah dilakukan jika Anda berlangganan penyimpanan data berbasis

cloud dan wifi. Data Anda jadi terbackup secara otomatis. Cara manualnya bisa menggunakan CD,DVD, atau harddisk eksternal.

#### 8. Upgrade Sistem Operasi

Jika Anda masih menggunakan sistem operasi lama, seperti XP atau Windows 7, ada baiknya mulai mempertimbangkan ganti sistem operasi. Pasalnya, sistem operasi yang sudah lama tidak mendapatkan pembaruan keamanan. Ditakutkan sistem operasi yang Anda gunakan rentan terserang virus atau dibajak.

#### 9. Waspada Spyware

Spyware adalah sebuah program kecil yang mampu merekam dan menyadap aktivitas yang dilakukan di komputer. Program ini ukurannya mungil, nyaris tak terlihat, dan menggunakan nama samaran yang mirip dengan nama program dalam sistem. Spyware biasanya didapat dari mengakses situs porno, menggunakan software bajakan, atau salah install aplikasi. Namun spyware dapat dicegah menggunakan program antivirus atau antispyware.

#### 10. Amankan Koneksi Nirkabel (Wireless)

Jika di rumah atau di kantor menggunakan wifi, selalu pasang password untuk wifi. Lebih bagus jika password itu diganti secara berkala. Dengan demikian, orang tidak bisa sembarangan mengakses wifi.

#### 11. Waspada Email Dari Kotak Spam

Di kotak spam email, kita sering mendapati adanya email seolah-olah dari perempuan yang mengajak berkenalan. Di dalam email ia melampirkan link ke suatu alamat atau sebuah program. Jangan buka email tersebut! Karena, ditakutkan bahwa link atau program tersebut berisi virus. Jika tidak kenal siapa pengirimnya dan sedang tidak menunggu ada e-mail dari suatu pihak, sebaiknya jangan buka e-mail tersebut.



## **Bab 9**

# **Sistem Keamanan Informasi**

### **9.1 Definisi Keamanan Informasi**

Saat ini informasi merupakan sumber aset yang begitu penting dan sangat berharga bagi keberlangsungan hidup suatu lembaga organisasi, perusahaan/bisnis, pertahanan keamanan dan keutuhan serta kedaulatan sebuah negara, di mana kepercayaan masyarakat dan konsumen menjadi indikator integritas suatu organisasi tersebut. Untuk menjaga kepercayaan publik maka sebagai organisasi harus mampu menjaga ketersediaan informasi, ketepatan dan keutuhan informasinya. Sebuah informasi tentu dapat disajikan kepada publik dalam berbagai format seperti : teks, gambar, audio, maupun video. Di mana manajemen pengelolaan informasi menjadi begitu penting. Informasi ini menjadi sangat penting apabila terkait dengan kredibilitas dan kelangsungan hidup jutaan manusia. Tujuan dari manajemen informasi adalah untuk melindungi kerahasiaan, integritas dan ketersediaan informasi tersebut.

Keamanan data elektronik menjadi sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun lembaga pemerintahan industri lainnya, seperti perusahaan ekspor-impor, transportasi, lembaga pendidikan, media pemberitaan, lembaga kesehatan, perbankan, hingga militer yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur yang kritis (penting). Informasi atau data adalah aset bagi perusahaan. Di mana keamanan data dan informasi secara tidak langsung memastikan kontinuitas

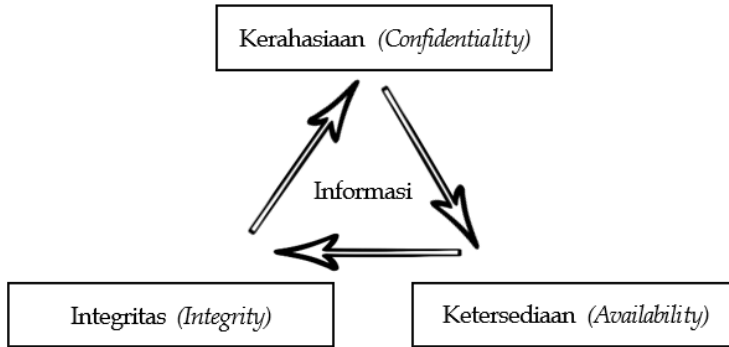


bisnis, mengurangi risiko-risiko, mengoptimalkan return of investment dan sebagai acuan mencari kesempatan dalam bisnis. Apabila semakin banyak informasi yang mampu diperoleh dan disimpan oleh sebuah organisasi atau perusahaan, kemudian dikelola dan dibagikan (sharing) kepada publik maka semakin besar pula risiko terjadinya kerusakan atau bahkan sampai hilangnya data penting sehingga tereksposnya data tersebut kepada pihak-pihak eksternal organisasi atau perusahaan yang tidak kita inginkan. (Syafrizal, 2007).

Di era digital saat ini, semakin mudahnya mengakses informasi melalui layanan internet menyebabkan informasi sangat mudah diperoleh dan disebarluaskan, sehingga informasi memiliki nilai dan harus dilindungi, karena keamanan informasi sudah menjadi prioritas. Menurut G.J. Simons, keamanan informasi adalah bagaimana usaha yang dapat dilakukan untuk mencegah terjadinya penipuan (cheating) atau paling tidak mampu mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Sistem keamanan informasi bisa juga diartikan sebagai suatu kebijakan, prosedur dan pengukuran teknis yang dapat digunakan untuk mencegah masuknya akses yang tidak sah atau ilegal ke dalam sistem informasi. Melakukan perubahan program, menghapus data, pencurian data, atau bahkan sampai terjadi kerusakan fisik terhadap sistem informasi tersebut. Semakin berkembang teknologi maka sistem pengamanan terhadap teknologi informasi dapat dikembangkan dan ditingkatkan dengan menggunakan teknik-teknik pengamanan dan peralatan-peralatan (tools) untuk mengamankan hardware (perangkat keras) dan software (perangkat lunak), jaringan komunikasi dan data.

## 9.2 Aspek Keamanan Sistem Informasi

Informasi saat ini sudah menjadi komoditi yang sangat penting. Bahwa kita sudah berada dalam kondisi information-based society. Di mana kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi esensial bagi sebuah lembaga organisasi, baik itu organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (perorangan). Hal ini dimungkinkan dengan perkembangan teknologi yang cukup pesat dan update di bidang teknologi komputer dan telekomunikasi. Penggunaan perangkat komputer dan layanan informasi yang terus berkembang setiap saat. (Budi Rahardjo, 1998)



**Gambar 9.1:** Elemen-elemen keamanan informasi

Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (right information), informasi dipegang oleh orang yang berwenang (right people), dapat diakses dan digunakan sesuai dengan kebutuhan (right time), dan memberikan informasi pada format yang tepat (right form). Dalam membuat program keamanan informasi ada prinsip dasar yang harus dipenuhi agar sistem tersebut handal. Prinsip dasar tersebut adalah:

1. Kerahasiaan (confidentiality) merupakan aspek yang menjamin kerahasiaan data dan informasi. Artinya memastikan bahwa informasi hanya dapat diakses dan hanya tersedia bagi orang yang berwenang sehingga pihak yang tidak berhak tidak bisa mengakses informasi. Contoh kerahasiaan adalah seorang administrator tidak boleh membuka atau membaca email milik pengguna (user). Selain itu kerahasiaan juga harus menjamin data-data yang harus dilindungi penggunaan dan penyebarannya baik oleh pengguna maupun administrator, seperti nama, alamat, tempat tanggal lahir, nomor kartu kredit, penyakit yang diderita, dan sebagainya.
2. Integritas (Integrity) merupakan aspek yang menjamin bahwa data dan informasi tidak mengalami perubahan/diubah tanpa ada izin dari pihak yang memiliki kewenangan (authorized). Artinya informasi dijaga agar selalu akurat dan menjaga keutuhan informasi tersebut maka informasi hanya boleh diubah dengan izin pemilik informasi. Virus trojan merupakan contoh dari informasi yang integritasnya

terganggu karena virus telah mengubah informasi tanpa izin. Integritas informasi ini dapat dijaga dengan melakukan enkripsi data atau membuat tanda tangan digital (digital signature).

3. Ketersediaan (Availability) merupakan aspek yang menjamin bahwa data dan informasi akan tersedia ketika dibutuhkan. Artinya adanya jaminan ketika pihak berwenang membutuhkan informasi, maka informasi dapat diakses dan digunakan. Memastikan pengguna (user) yang berhak dapat menggunakan data atau informasi melalui perangkat terkait. Hambatan dalam ketersediaan ini contohnya adalah adanya Denial of Service Attack (DoS). DoS merupakan serangan yang ditujukan ke server, di mana banyak sekali permintaan yang dikirimkan ke server dan biasanya permintaan tersebut palsu yang menyebabkan server tidak sanggup lagi melayani permintaan karena tidak sesuai dengan kemampuan sehingga server menjadi down bahkan error.

Keamanan informasi diperoleh dengan melakukan mengimplementasikan seperangkat alat kontrol yang layak, dapat berupa kebijakan-kebijakan, praktik-praktik, prosedur-prosedur, struktur organisasi dan peranti lunak (software). Dengan terpenuhinya aspek-aspek sistem keamanan informasi dan prinsip dasar penyusunan program keamanan informasi tersebut maka seluruh sumber daya informasi terjamin dan terlindungi dari ancaman pihak-pihak yang tidak berwenang untuk memanfaatkan data dan informasi untuk kepentingan yang akan merugikan organisasi atau perusahaan. (BPPTIK, 2014).

## 9.3 Mengapa Keamanan Informasi Sangat Diperlukan?

Karena begitu pentingnya nilai sebuah data dan informasi di era saat ini menyebabkan seringkali data dan informasi diinginkan hanya boleh diakses oleh pihak-pihak yang berwenang atau orang tertentu saja. Jatuhnya data dan informasi ke pihak yang tidak berwenang atau pihak lain sebagai contoh misalnya pihak kompetitor bisnis tentu hal ini akan sangat merugikan bagi

organisasi atau perusahaan yang memiliki data dan informasi tersebut. Sebagai contoh misalnya data dan informasi dari sebuah organisasi komersial (perusahaan), di mana biasanya banyak informasi yang hanya diperbolehkan diakses dan digunakan oleh kalangan internal perusahaan tersebut atau bahkan hanya boleh diketahui oleh orang-orang tertentu saja di perusahaan yang memiliki kepentingan. Misalnya informasi tentang sebuah produk unggulan baru yang sedang dikerjakan oleh tim dari perusahaan, teknik-teknik khusus yang digunakan dalam mendvelop produk baru tersebut, atau mungkin bahan baku tambahan khusus yang dipakai untuk menghasilkan produk yang berkualitas sehingga hanya pihak yang berwenang saja dari perusahaan tersebut yang berhak mengetahui data dan informasinya.

Untuk itu keamanan sistem informasi yang digunakan dalam perusahaan tersebut harus memiliki jaminan dan kerahasiaan bahwa data dan informasi hanya bisa di akses oleh pihak yang memiliki akses tertentu saja di internal perusahaan. Hal ini penting kenapa ? tentu saja untuk mencegah terjadinya kebocoran informasi ke pihak yang tidak diinginkan yaitu pihak lawan bisnis. Apabila data dan informasi ini sampai jatuh ke pihak lain, tentu akan membawa kerugian bagi perusahaan. Saat ini jaringan komputer, seperti LAN (Local Area Network) dan mudahnya akses internet, tentu saja memungkinkan bagi sebuah organisasi atau perusahaan untuk menyediakan data dan informasi secara cepat dan akurat.

Meningkatnya kejahatan komputer (computer crime), terutama yang berhubungan dengan data dan sistem informasi akan terus mengalami peningkatan ini dikarenakan beberapa hal, di antaranya adalah :

1. Aplikasi bisnis yang berbasis teknologi informasi dan jaringan komputer akan terus mengalami peningkatan yang cukup cepat. Sebagai contoh saat ini banyak sekali aplikasi bisnis yang terus hadir dan berkembang seperti e-commerce, online banking, fintech, ticketing online, termasuk electronic data interchange dan sebagainya. Apalagi saat ini aplikasi bisnis seperti e-commerce menjadi primadona dan sangat populer. Industri e-commerce dunia terus mengalami perkembangan di mana masing-masing platform belanja online terus bersaing memberikan pelayanan promo menarik dilengkapi dengan inovasi layanan yang tentu saja memberikan kemudahan dan kenyamanan bagi penggunaanya.

2. Desentralisasi server yang akan membuat lebih banyak sistem yang harus ditangani. Hal ini tentunya membutuhkan lebih banyak operator dan administrator yang handal. Mencari operator dan administrator yang memiliki kompetensi yang baik tidaklah mudah. Problem yang akan dialami adalah biasanya menyebabkan server-server di daerah (bukan pusat) tidak dikelola dan di maintenance dengan baik, sehingga akan menjadi lebih rentan mendapat serangan yang mengakibatkan kebocoran data dan informasi ke pihak yang tidak diinginkan. Bahkan memungkinkan untuk kehilangan data dan informasi.
3. Mudahnya mendapatkan sumber informasi dan akses internet saat ini tentu saja membawa dampak dengan meningkatnya kemampuan pengguna (user) di bidang komputer. Saat ini banyak pengguna yang mulai melakukan percobaan atau iseng-iseng bermain dan membongkar sistem yang digunakannya (atau sistem milik orang lain), jika dahulu akses ke komputer sangat sulit. Berbeda dengan era saat ini komputer dan akses internet sudah merupakan kebutuhan dan barang mudah diperoleh dan semakin banyak dipergunakan bukan hanya di perkantoran saja akan tetapi menjadi kebutuhan hampir setiap individu (pribadi).
4. Perubahan transisi dari single vendor ke multi vendor.
5. Mudahnya memperoleh software atau tools untuk melakukan percobaan menyerang jaringan komputer dan sistem komputer sebuah organisasi atau perusahaan. Saat ini banyak di internet ditemukan situs-situs yang menyediakan software atau tools hacking yang langsung dapat di unduh (download) dan langsung dapat dipergunakan untuk melakukan percobaan menyerang (attack) ke jaringan dan sistem komputer.

Manajemen sistem informasi yang baik tentunya sangat memungkinkan data dan informasi terdistribusi secara elektronik, sehingga diperlukan sebuah sistem untuk memastikan apakah data dan informasi telah terkirim dan diterima oleh pengguna (user) yang tepat sesuai dengan keinginan pengirim data dan informasi. Menurut W. Stallings, serangan terhadap sistem keamanan

sistem informasi (security attack) dapat dilihat dari sudut peranan komputer atau jaringan komputer yang memiliki fungsi sebagai penyedia informasi. Berikut beberapa kemungkinan serangan (attack) yang dapat terjadi pada sistem keamanan informasi, di antaranya adalah :

1. *Interruption*, di mana serangan ini akan menyebabkan perangkat sistem menjadi rusak atau tidak tersedia. Jenis serangan ini ditujukan kepada availability atau ketersediaan data dan informasi dari sistem. Contoh jenis serangan adalah DoS Attack
2. *Interception*, di mana jenis serangan ini memungkinkan pihak yang tidak berwenang mampu menembus dan berhasil mengakses aset baik data dan informasi. Contoh jenis serangan ini pada umumnya adalah proses penyadapan (wiretapping).
3. *Modification*, di mana jenis serangan ini menyebabkan perubahan data dan informasi karena pihak yang tidak berwenang bukan saja berhasil mengakses aset tetapi juga mampu melakukan perubahan pada data dan informasinya. Contoh dari jenis serangan ini sering terjadi pada halaman website, biasanya mengubah isi dari website tentunya mengganti dengan isi pesan-pesan yang bisa menyebabkan kerugian bagi pemilik website dan juga pengguna lainnya.
4. *Fabrication*, di mana jenis serangan ini juga sangat berbahaya karena pihak yang tidak berwenang yang berhasil mendapatkan hak akses biasanya akan menyisipkan objek palsu ke dalam sistem. Contoh dari jenis serangan ini biasanya pihak yang tidak bertanggung jawab memasukkan pesan-pesan palsu seperti yang sering terjadi email palsu ke dalam jaringan komputer dan tentu saja hal ini akan menyebabkan dampak kerugian bagi perusahaan terkait.

## 9.4 Dasar-Dasar Keamanan Sistem Informasi

Sebelum membahas lebih luas mengenai hal hal yang praktis dalam pengamanan sistem informasi, sebaiknya kita pahami terlebih dahulu yang menjadi dasar-dasar dan teori yang biasanya digunakan untuk melakukan pengamanan sistem informasi.

Apa itu kriptografi, enkripsi dan dekripsi ?

1. Kriptografi, adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integritas data dan autentikasi keaslian data. (Menezes, dkk). Fakta sejarah bahwa setiap orang mempunyai cara masing-masing untuk mengamankan data, sehingga sebuah pesan itu memiliki nilai estetika tersendiri yang memiliki hubungan dengan seni dan kebudayaan, jika diperhatikan secara lebih mendalam kata Grafy dalam kriptografi memiliki makna sebuah seni. Di mana keamanan juga membutuhkan teknik dan seni demikian pula halnya dengan keamanan data, kehandalan dalam mengamankan data sangat tergantung dari cara masing-masing dalam memahami pentingnya dari sebuah data tersebut.

Perkembangan teknologi saat ini terus mengalami perubahan yang cukup cepat, sehingga mengubah perilaku setiap penggunanya. Perubahan ini dimulai dari cara pikir pengguna (user) yang cenderung untuk lebih maju dalam penguasaan teknologi. Di era sekarang ini hampir tidak ada satu sisi kehidupan kita yang tidak menggunakan pengolahan data komputer, mulai dari hal pengolahan data yang bersifat sederhana hingga pengolahan data yang memiliki kompleksitas yang cukup rumit. Di mana internet mampu memanjakan penggunanya baik dalam hal sebagai sarana tukar informasi dan memudahkan pengguna untuk berkomunikasi dan terhubung dengan berbagai pengguna komputer dari berbagai negara di dunia.

Di era sekarang ini, semakin berkembangnya pemanfaatan layanan komunikasi internet maka timbul permasalahan baru seperti munculnya hacker dan cracker. Banyak pengguna merasa sangat terganggu atas kehadiran pihak-pihak yang tidak bertanggung jawab yang mengganggu kenyamanan pengguna dalam layanan atau berkomunikasi melalui internet. Ada beberapa cara yang dilakukan pengguna dalam menjaga keaslian data dan informasi agar terhindar dari gangguan pihak-pihak yang tidak bertanggung jawab. Maka hal ini yang mendasari muncul berbagai metode atau ilmu pengkodean dalam pengiriman pesan di antaranya adalah kriptografi. Kriptografi adalah bidang ilmu yang paling banyak diminati orang, karena jika mampu memahami dan menguasai bidang ilmu kriptografi seseorang tentu akan mampu menjaga keaslian dan kerahasiaan data dan informasi yang akan dikirimkan kepada orang lain. Di mana kriptografi adalah ilmu dan seni yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data dan autentikasi.

Dalam perkembangannya kriptografi, muncul istilah dalam kriptografi yang dipergunakan untuk menandai dalam aktivitas rahasia untuk pengiriman pesan. Di mana proses acak mengirim pesannya disebut enkripsi (encryption) dan saat proses merapikan pesan yang teracak dikenal dengan istilah dekripsi (decryption) dan pesan awal yang belum diacak ataupun yang sudah dirapikan disebut dengan plaintext, sedangkan ciphertext adalah sebutan untuk pesan yang telah diacak. (Mukhtar, 2018).

2. Enkripsi, adalah merupakan sebuah proses di mana kita bisa mengubah pesan asli ke dalam bentuk pesan yang tidak bisa dikenali (acak), sehingga pesan yang akan dikirimkan benar-benar berbeda dengan pesan aslinya. Atau proses perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang sulit untuk dipahami. Enkripsi sudah ada sejak zaman perang romawi, namun sudah tentu dari segi teknologinya pasti sudah sangat berbeda dengan saat ini dan teknik enkripsi sudah mengalami perubahan dan kemajuan dengan



adanya komputer. (Kristianto, 2003). Bagi yang ingin mendalami lebih jauh mengenai kriptografi, disarankan untuk mencari sumber buku yang dijadikan referensi dalam menulis bab ini.

3. Dekripsi, adalah proses di mana perubahan data yang terenkripsi sebelumnya menjadi data yang mudah untuk dibaca kembali sehingga bisa dimengerti oleh manusia (pengguna) atau komputer.

Alasan mengapa enkripsi dan dekripsi digunakan, di antaranya adalah agar menjaga kerahasiaan data atau informasi pribadi, membantu memastikan bahwa data dan informasi yang dikirimkan asli tidak mengalami perubahan dari data yang asli apabila diakses oleh orang-orang yang tidak memiliki kepentingan.

# **Bab 10**

## **Keamanan Komputer Secara Fisik**

### **10.1 Pendahuluan**

Sistem keamanan data dan informasi sebagai upaya yang dilakukan untuk melindungi dan mengamankan kinerja, fungsi ataupun proses kerja sistem komputer (Aswar 2020). Walaupun terkadang upaya tersebut gagal karena kepandaian para hacker yang berupaya menyusup sistem kerja jaringan. Upaya-upaya tersebut wajib kita lakukan guna meminimalisir terjadinya serangan dari pihak luar. Dalam melakukan keamanan data dan informasi, salah satu hal yang sangat penting dalam melakukan pengamanan yaitu keamanan komputer secara fisik. Keamanan komputer secara fisik sebagai lapisan pertama dalam melakukan keamanan data dan informasi. Secara tradisional, keamanan komputer secara fisik dilindungi karena untuk mencegah pencurian atau kerusakan hardware, untuk mencegah pencurian atau kerusakan data dan informasi serta untuk mencegah gangguan layanan (Suwito 2019). Dalam bab ini akan dijelaskan cara melakukan keamanan komputer secara fisik dari berbagai sisi, seperti sisi lingkungan, sisi manajemen, sisi fisika dan kimia, serta sisi perangkat keras.

## 10.2 Sisi Lingkungan

Dalam melakukan keamanan komputer secara fisik, hal pertama yang wajib kita lakukan yaitu dari sisi lingkungan. Berikut ini hal-hal yang perlu kita waspadai dari sisi lingkungan:

### 1. Manusia

Manusia sebagai pengguna yang rentan terhadap faktor keamanan komputer (Ridwan Lubis 2020). Dari sisi lingkungan, hal yang pertama wajib kita waspadai adalah dari sisi manusia yaitu :

- a. Mencuri, manusia dapat melakukan pencurian seperti mencuri perangkat keras, mencuri data dan informasi, mengubah data.
- b. Merusak, manusia dapat merusak sistem komputer dan jaringan yang dapat mengakibatkan sebagian atau keseluruhan sistem rusak.
- c. Mengganggu, manusia dapat mengganggu sistem kerja komputer dan jaringan sehingga sebagian atau keseluruhan sistem menjadi terganggu.

Cara penanggulangan :

- Khusus ruang server, buat area terbatas hanya untuk orang-orang tertentu.
- Kunci ruangan dengan sistem pengamanan seperti penggunaan password atau ID, biometric ataupun RFID.
- Pasang CCTV di area-area terbatas.

### 2. Binatang

Agar ruangan sistem kerja komputer dan jaringan terbebas dari binatang-binatang berbahaya yang dapat merusak sistem kerja komputer dan jaringan seperti:

- a. Semut
- b. Lalat
- c. Laba-laba
- d. Tikus
- e. Cicak

- f. Rayap
- g. Tawon
- h. Nyamuk

Bahaya dari binatang-binatang tersebut seperti urine, kotoran, sarang, bangkai. Urine dari binatang mengandung zat-zat yang bersifat asam sehingga dapat melarutkan materi yang bersifat logam yang tidak tahan zat asam. Misalnya urine terkena motherboard, maka ada kemungkinan bagian-bagian tertentu dari motherboard tersebut akan rusak karena zat asam.

Cara penanggulangan:

- Tutup bagian dari lubang angin ataupun yang lainnya dengan kasa.
- Menangkap serangga yang masuk ke dalam ruangan.
- Membersihkan ruangan dan perangkat komputer secara berkala.
- Tidak menggunakan kapur barus karena akan merusak perangkat keras komputer dan jaringan.

### 3. Iklim dan cuaca

Kondisi iklim sangat berpengaruh terhadap perangkat sistem komputer dan jaringan. Iklim yang panas akan mengakibatkan perangkat akan memuai sedangkan pada suhu dingin perangkat akan mengalami lembab dan menyusut. Kondisi lembab, penyusutan dan pemuaian akan mengakibatkan perangkat menjadi rusak. Selain iklim, cuaca juga sangat berpengaruh terhadap perangkat sistem komputer dan jaringan. Kondisi angin yang kencang akan membawa debu, debu yang masuk ke dalam ruangan server akan merusak perangkat komputer. Hujan yang turun terus menerus akan mengakibatkan lembab dan banjir. Pengaturan suhu ruangan sangat penting agar tidak menimbulkan lembab. Selain itu, pengaruh lain dari cuaca adalah petir. Petir dapat menyambar perangkat sistem komputer sehingga dapat merusak perangkat. Cara penanggulangan adalah dengan cara mengatur suhu ruangan stabil pada suhu yang sesuai dan menggunakan AC. Agar terhindar dari petir kita wajib

memasang anti petir di gedung yang baik serta menggunakan arde yang baik yang ditanam ke dalam tanah.

#### 4. Bencana alam

Di Indonesia, beberapa daerah rawan sekali terhadap bencana alam, bencana alam merupakan bencana yang diakibatkan oleh suatu peristiwa alam seperti banjir, gempa bumi, angin topan, kekeringan, tsunami dan gunung meletus. Dalam membuat ruang pusat data, kita wajib mencari lokasi yang tidak rentan terhadap bencana alam.



**Gambar 10.1:** Gempa bumi (Aryadita Umasugi 2018)

Cara penanggulangan adalah dengan cara memilih lokasi yang aman dari bencana alam, membuat bangunan yang tidak rentan terhadap gempa bumi, meletakkan perangkat di ruang yang aman dari bencana banjir (misalnya lantai 2).

#### 5. Tumbuhan

Tumbuhan yang perlu diwaspadai karena faktor lembab yaitu:

- a. Lumut
- b. Jamur
- c. Ganggang biru

Cara penanggulangan:

- Bersihkan lumut atau jamur yang berada diruangan sistem komputer.
- Gunakan silica gel untuk mengurangi lembab.

- Gunakan ruangan ber-AC dengan suhu yang sesuai agar menghindari lembab.

## 10.3 Sisi Manajemen

Dalam melakukan keamanan komputer secara fisik, kita perlu memperhatikan dan pengelolaan dari sisi manajemen. Sisi manajemen yang dimaksud adalah melakukan pengelolaan seperti pemberian hak otorisasi, pemberian kata sandi dan pengelolaan password sehingga mendukung tercapainya keamanan komputer secara fisik. Berikut ini akan dijelaskan cara melakukan keamanan dari sisi manajemen:

### 1. Pemberian hak otorisasi

Dalam melakukan keamanan komputer secara fisik, kita perlu memperhatikan pula pemberian hak otorisasi. Pemberian hak otorisasi ini akan berjalan dengan baik jika didukung dengan penerapan kebijakan dan prosedur manajerial. Contoh pemberian hak otorisasi: masing-masing bagian atau personel memiliki hak akses sesuai dengan bagian atau bidangnya. Misalnya saja bagian keuangan hanya dapat melakukan hak akses di sisi keuangan, bagian sales hanya dapat melakukan hak akses penjualan. Masing-masing menggunakan hak akses sesuai dengan bagiannya dan tidak diperkenankan memberikan account ke orang lain.

### 2. Pemberian kata sandi

Setiap bagian atau personil yang memiliki account harus menggunakan kata sandi yang unik dan berbeda. Kita harus memperhatikan aturan penggunaan kata sandi yang baik sebagai berikut:

- a. Tidak menggunakan abjad huruf atau angka secara berurut misalnya abcde atau 12345.
- b. Minimal 8 karakter dengan kombinasi huruf (besar dan kecil), angka dan simbol.
- c. Tidak menggunakan identitas diri (misalnya tanggal lahir).
- d. Tidak menggunakan password default.

Kendala penggunaan kata sandi:

- Mudah disadap oleh orang lain.
- Security lemah.
- Mudah dibaca oleh orang lain (pada saat mengetik menggunakan keyboard).

Permasalahan penggunaan kata sandi secara manual dapat digantikan dengan menggunakan perangkat seperti biometric.

3. Penggunaan perangkat keamanan

Permasalahan dalam penggunaan kata sandi secara manual dapat digantikan dengan penggunaan perangkat keamanan seperti:

a. Kartu magnetic

Kartu magnetic adalah sebuah kartu yang menyimpan data dengan modifikasi magnetik berbasis besi kecil pada pita magnetik pada kartu strip. Contohnya adalah kartu kredit, kartu identitas, kartu transportasi.

b. Signal suara

Signal suara atau speech recognition merupakan suatu teknik yang digunakan untuk memberikan suatu input data dalam bentuk sinyal suara. Signal suara dapat berbentuk ucapan-ucapan yang digunakan sebagai pengganti kata sandi.

c. Retina mata

Retina mata salah satu perangkat biometric yang dapat digunakan sebagai suatu input data dengan cara membaca pola retina pada mata.

d. Sidik jari atau telapak tangan.

Sidik jari biasanya digunakan untuk melakukan verifikasi identitas dengan membaca pola sidik jari yang tersimpan dalam suatu database. Misalnya mesin absensi fingerprint, access door dan lain-lain.

e. Wajah

Wajah juga digunakan untuk melakukan verifikasi identitas dengan membaca pola wajah seseorang yang sudah disimpan dalam database.

f. Tanda tangan

Tanda tangan digunakan untuk melakukan verifikasi identitas dengan melihat pola tanda tangan yang dibuat.

## 10.4 Sisi Fisika dan Kimia

Dari sisi fisika dan kimia, ada 5 hal yang dapat merusak atau mengganggu perangkat komputer secara fisik yaitu:

1. Panas

Panas yang terjadi dapat diakibatkan dari kerusakan pada fisik komponen dan ruangan. Berikut ini hal-hal yang dapat menyebabkan kerusakan akibat panas yang ditimbulkan:

- a. Suhu ruangan, agar suhu ruangan tidak menimbulkan panas maka kita wajib menggunakan pendingin udara (AC). Agar tidak terjadi lembab maka wajib diatur temperatur udaranya agar tetap stabil.
- b. Thermal paste mengering, jika perangkat yang digunakan sudah lebih dari 2 tahun maka wajib kita lakukan pengecekan terhadap thermal untuk memastikan paste dalam thermal tidak mengering. Thermal paste yang mengering dapat menimbulkan panas pada perangkat.
- c. Penggunaan perangkat non stop, jika perangkat yang kita gunakan bekerja secara nonstop dengan beberapa aplikasi yang berjalan maka perlu dilakukan istirahat untuk perangkat tersebut agar perangkat tersebut tidak menimbulkan panas.
- d. Overclocking, proses overclocking perangkat akan dipaksa bekerja keras dengan hasil overclocking yang digunakan. Misalnya CPU 2.2 Ghz di overclocking menjadi 4.4 Ghz.



- e. Heatsink tidak sesuai atau rusak, heatsink dalam perangkat CPU sangat berpengaruh terhadap panas, pastikan menggunakan heatsink yang sesuai, periksa apakah kondisi heatsink menyala atau tidak. Jika terdapat heatsink yang rusak segera lakukan pergantian perangkat tersebut.
2. Suara

Getaran suara didalam perangkat ataupun dalam ruangan akan berpengaruh terhadap head yang ada dalam perangkat hardisk. Untuk menghindari getaran suara kita dapat melakukan pemeriksaan apakah dalam perangkat ada komponen yang berbenturan sehingga mengakibatkan getaran suara atau apakah dalam ruangan tersebut ada benda yang akan menimbulkan getaran suara. Saat ini sudah ada perangkat SSD yang lebih tahan terhadap getaran suara.
3. Magnet

Di dalam ruang perangkat komputer sedapat mungkin kita menghindari dari penggunaan magnet, magnet akan merusak komponen yang ada dalam hardisk. Agar terhindar dari kerusakan akibat dari medan magnet maka kita tidak boleh menggunakan atau mendekatkan magnet ke CPU.
4. Listrik

Pada saat kita menggunakan perangkat komputer, listrik yang kita gunakan sangat berpengaruh terhadap tingkat kerusakan perangkat komputer tersebut. Listrik yang tidak stabil atau tiba-tiba sering mati akan merusak misalnya power supply terbakar, hardisk terbakar dan komponen motherboard terbakar. Untuk menanggulangnya dapat menggunakan stabilizer atau UPS.
5. Kimia

Di dalam perangkat motherboard terdapat baterai CMOS, baterai tersebut mengandung logam berat seperti merkuri, mangan, kadmium, nikel dan litium yang berbahaya bagi lingkungan dan kesehatan manusia. Kebocoran baterai CMOS pada komputer juga dapat merusak komponen motherboard atau komponen lainnya.

Untuk menanggulanginya dengan cara melakukan pengecekan secara berkala dan mengganti baterai CMOS yang sudah mulai rusak.

## 10.5 Sisi Perangkat Keras

Perangkat keras komputer adalah komponen fisik pada komputer yang digunakan oleh sistem komputer untuk menjalankan program yang telah diperintah (Rahayu 2016). Perangkat keras komputer dibagi menjadi 3 kategori yaitu:

1. Militer(-400 s/d 1200C) digunakan oleh pemerintahan
2. Industri (normal s/d 900 s/d 1000C) atau komputer bermerek
3. Jangkrik (normal s/d 600 s/d 700C) atau komputer rakitan

Kategori komputer tersebut sangat berpengaruh terhadap kualitas dari perangkat, perangkat komputer bermerek akan lebih berkualitas dibandingkan dengan komputer rakitan.



# **Bab 11**

## **Evaluasi Keamanan Sistem Informasi**

### **11.1 Pendahuluan**

Isu tentang keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Keterpenuhan aspek keamanan memastikan seluruh sumber daya sistem informasi pada sebuah organisasi atau perusahaan hanya dapat diakses oleh pihak-pihak yang berhak, serta menjamin sistem informasi berperilaku sebagaimana mestinya. Untuk menjamin kondisi keamanan senantiasa terpenuhi, maka kegiatan evaluasi keamanan sistem informasi merupakan sebuah kebutuhan. Evaluasi keamanan sistem informasi harus dilaksanakan secara terencana dan berkesinambungan untuk mengetahui tingkat keandalan serta integritas sebuah sistem informasi. Evaluasi ditujukan untuk menginvestigasi keterpenuhan standar kontrol keamanan yang telah ditetapkan oleh organisasi dalam mengatasi berbagai tingkat risiko keamanan yang mungkin terjadi. Dengan kata lain, evaluasi keamanan sistem informasi berperan untuk meyakinkan tidak adanya lubang keamanan (security hole) pada sebuah sistem informasi. Secara garis besar lubang keamanan pada sebuah sistem informasi disebabkan oleh empat hal, yaitu: Kesalahan desain (desain flaw), implementasi yang kurang baik, kesalahan konfigurasi dan kesalahan penggunaan program atau sistem (Rahardjo, 2005).

Berdasarkan laporan statistik keamanan oleh Edgescan ('BCC030 Vulnerability Stats Report (2020)\_WEB.pdf', 2020), mengidentifikasi sebelas (11) sumber kerentanan keamanan (security vulnerability) yang terjadi pada tahun 2019, yaitu crypto weaknesses (kelemahan crypto) 39.7%, cross-site scripting 12%, system patching related 8%, disclosure/ directory listing 7.1%, exposed system & services (sistem dan servis yang terbuka) 3.5%, poor configuration (kelemahan konfigurasi) 2.9%, authorization & session weaknesses (otorisasi dan session yang lemah) 2.4%, injection exploits 2.2%, XML external entity attack 1.8%, remote code execution 1.7%, password management and authentication weaknesses (kelemahan autentikasi) 1.3%, serta kategori lainnya sebanyak 17.4%. Laporan tersebut mengindikasikan bahwa setidaknya 46.3% potensi kerentanan disebabkan oleh kelemahan pengelolaan internal. Hal tersebut perlu menjadi perhatian serius dalam mengantisipasi potensi terjadinya gangguan keamanan informasi baik dalam skala keamanan informasi individu maupun organisasi.

Lebih lanjut Edge Scan melaporkan bahwa rata-rata waktu yang dibutuhkan oleh sebuah sistem internal (non-public facing) untuk kembali pulih setelah mengalami gangguan keamanan kurang lebih 75.29 hari, sedangkan untuk sistem yang terkoneksi ke internet (public internet-facing) membutuhkan rata-rata waktu 84.59 hari. Waktu pemulihan (recovery time) yang lumayan lama tersebut tentu saja sangat merugikan. Olehnya itu tindakan pencegahan berupa kegiatan evaluasi secara berkala sangat diperlukan agar kerugian akibat serangan keamanan dapat dihindari.

## 11.2 Keamanan Sistem Informasi

Keamanan sistem informasi merupakan satu sub kajian penting dalam bidang teknologi informasi yang berfokus pada bagaimana melindungi komputer, jaringan, serta para pengguna dari ancaman keamanan. Baik berupa ancaman pengambilalihan/ duplikasi hak akses maupun fabrikasi data. Secara spesifik definisi keamanan sistem informasi dinyatakan dalam (Information systems security, 2005) bahwa :

*“The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users”.*

Serta dikemukakan pula oleh (Fruhlinger, 2020b) bahwa:

*“Information security, sometimes abbreviated to infosec, is a set of practices intended to keep data secure from unauthorized access or alterations, both when it’s being stored and when it’s being transmitted from one machine or physical location to another”.*

Berdasarkan kedua definisi tersebut, dapat disimpulkan bahwa keamanan sistem informasi merupakan serangkaian kegiatan yang ditujukan untuk memproteksi sistem informasi, informasi, data dan sumber data dari pengaksesan oleh pihak-pihak yang tidak berhak baik pada media penyimpanan maupun pada saat ditransmisikan. Secara rinci, sasaran keamanan sistem informasi adalah terpenuhinya tiga elemen kunci keamanan informasi pada sebuah organisasi yang dikenal dengan istilah CIA Triad (Fruhlinger, 2020a), yang meliputi:

1. Confidentiality (kerahasiaan). Aspek confidentiality mencakup proses untuk mengamankan dan memastikan kerahasiaan data/ informasi, yakni mencegah pihak yang tidak berwenang mengakses dan memodifikasi data/ informasi. Dengan kata lain, jaminan bahwa hanya pengguna dan proses terotorisasi (sah) yang dapat mengakses maupun memodifikasi data/ informasi.
2. Integrity (integritas). Merupakan jaminan bahwa data tersedia dalam keadaan utuh dan tidak termodifikasi oleh pihak-pihak yang tidak berhak.
3. Availability. Kepastian bahwa data dapat diakses setiap saat (jika dibutuhkan) tanpa delay dan utuh (tanpa cacat). Dengan kata lain memastikan bahwa orang-orang yang tepat dapat memperoleh data/ informasi yang dibutuhkan dengan tepat waktu.

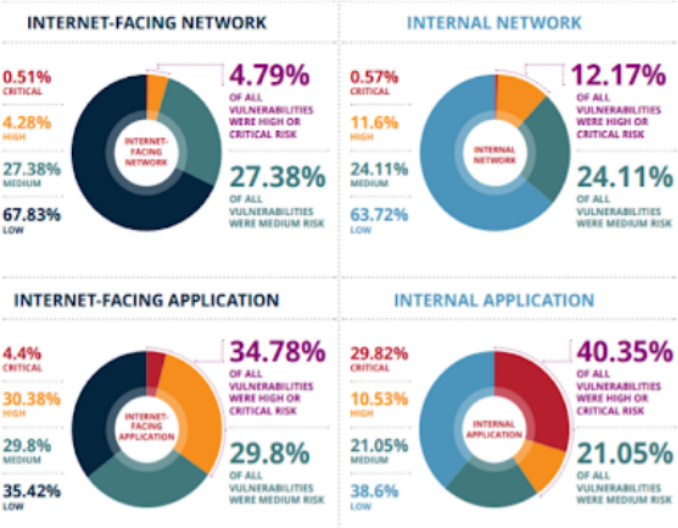
Hubungan antara ketiganya sebagaimana diilustrasikan pada gambar 11.1 berikut ini.



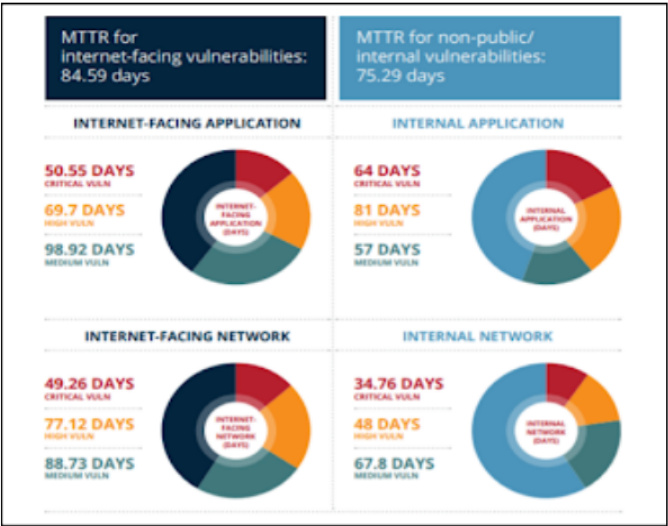
**Gambar 11.1:** The Security Triad (Bourgeois and Bourgeois, 2014)

### 11.2.1 Statistik Keamanan Sistem Informasi

Laporan statistik kerentanan (vulnerability) keamanan oleh Edgescan ('BCC030 Vulnerability Stats Report (2020) menampilkan berbagai hal terkait karakteristik vulnerability pada tahun 2019. Dua di antaranya yang menarik untuk diketahui adalah perbandingan jenis risiko keamanan pada tahun 2019 serta rata-rata waktu pemulihan setelah mengalami gangguan keamanan antara internet-facing network/ application dengan internal network/ application, sebagaimana tertera pada Gambar 11.2 dan 11.3. Gambar 11.2 menunjukkan bahwa intranet (internal network) memiliki angka high atau critical risk yang lebih tinggi yakni 12.17% dibandingkan dengan internet-facing network yang hanya 4.19%. Demikian halnya internal application dengan angka high/ critical risk sebesar 40.35%, sedangkan internet-facing application 5.57% lebih rendah, yakni sebesar 34.78%. Hal ini merupakan fenomena yg menarik, mengingat secara umum internet-facing network dan application cenderung sangat strategis menjadi sasaran ancaman keamanan. Namun di sisi lain, internet-facing vulnerability membutuhkan rata-rata waktu pemulihan yang terbilang lebih lama, yakni 84.59 hari dibandingkan dengan internal vulnerability yang memiliki waktu pulih 9.3 hari lebih cepat, yakni 75.29 hari sebagaimana ditampilkan pada Gambar 11.3.



**Gambar 11.2:** Perbandingan Kasus Vulnerability pada Tahun 2019 (‘BCC030 Vulnerability Stats Report, 2020)



**Gambar 11.3:** Perbandingan Rata-rata Waktu Pemulihan (‘BCC030 Vulnerability Stats Report, 2020)



### 11.2.2 Jenis Ancaman Keamanan Informasi

Whitman, Mattord dan Green (2014) mengidentifikasi dua belas (12) jenis ancaman keamanan informasi, sebagai berikut:

1. Kesalahan manusia. Merupakan ancaman keamanan yang diakibatkan oleh kesalahan manusia tanpa unsur kesengajaan (Human error or failure).
2. Ancaman hak kekayaan intelektual. Yakni ancaman terhadap pelanggaran hak cipta (compromises to intellectual property).
3. Pelanggaran yang disengaja. Tindakan dengan sengaja mengakses secara tidak sah data/ informasi yang bersifat rahasia (deliberate acts of trespass). Salah satu contoh, tindakan hacker untuk mengakses informasi secara ilegal.
4. Tindakan pemerasan. Berupa tindakan oknum untuk menuntut kompensasi untuk mengembalikan informasi rahasia yang diperoleh kepada individu/ lembaga pemilik informasi tersebut.
5. Tindakan sabotase. Kegiatan yang secara sengaja mengakses informasi/ data dengan tujuan merusak aset ataupun citra individu/ organisasi.
6. Tindakan pencurian. Secara sengaja mengambil informasi/ data individu/ organisasi secara ilegal untuk memperoleh keuntungan pribadi.
7. Serangan dengan perangkat lunak jahat (Malicious Program). Berupa perangkat lunak berbahaya yang ditujukan untuk merusak atau menghancurkan sumber daya sistem informasi. Di antaranya berupa: virus, worm, backdoors, serangan Denial of Service (DoS) dan Distributed Denial of Service (DDoS).
8. Kejadian alam/ bencana. Ancaman keamanan yang diakibatkan oleh bencana/ kejadian alam. Meskipun hal ini di luar kekuasaan manusia, tindakan antisipatif harus dipersiapkan.
9. Penyimpangan kualitas pelayanan. Gangguan yang diakibatkan oleh berhentinya/ tidak berfungsinya suatu layanan. Contoh: gangguan jaringan dapat mempengaruhi akses pengguna ke server

10. Kerusakan atau kesalahan teknis peralatan (perangkat keras). Cacat bawaan dari peralatan berpotensi menyebabkan sistem tidak bekerja sebagaimana mestinya, sehingga menyebabkan layanan tidak tersedia/ tidak berjalan sesuai harapan.
11. Kesalahan/ kegagalan perangkat lunak. Kondisi perangkat lunak yang belum bebas dari bug maupun kondisi tertentu yang belum melewati proses pengujian sebagaimana mestinya dapat menjadi sumber ancaman keamanan.
12. Peralatan yang ketinggalan jaman (outdated devices). Kondisi infrastruktur yang ketinggalan zaman dapat mempengaruhi keandalan sistem.

### 11.2.3 Tipe Serangan Terhadap Keamanan Sistem Informasi

Serangan keamanan dapat mengakibatkan berbagai kemungkinan gangguan, mulai dari yang dampaknya ringan hingga yang berakibat fatal. Menurut (Stallings, 1995), serangan keamanan (security attack) terhadap sistem informasi terdiri atas empat (4) kemungkinan serangan, yaitu:

1. Interupsi (interruption). Serangan yang mengakibatkan perangkat sistem menjadi rusak atau tidak tersedia. Serangan ini ditujukan untuk mengganggu ketersediaan (availability) dari sistem. Sebagai contoh serangan denial of service (DoS).
2. Intersepsi (Interception). Pihak yang tidak terotorisasi berhasil mengakses sumber daya sistem dan melakukan penyadapan (eavesdropping). Sebagai contoh
3. Modifikasi (Modification). Setelah berhasil mengakses sistem, pihak yang tidak berwenang mengubah isi/ konten (aset) sistem informasi sehingga dapat menimbulkan kerugian. Sebagai contoh pihak tidak terotorisasi mengubah nominal transaksi pada rekening tertentu sehingga mengakibatkan kerugian bagi pemilik rekening ataupun bank.
4. Fabrikasi (Fabrication). Setelah berhasil mengakses sistem, pihak yang tidak berwenang menyisipkan konten atau objek palsu sehingga

dapat berakibat fatal. Sebagai contoh pihak tidak terorisasi menambahkan transaksi debit maupun kredit pada rekening nasabah bank sehingga mengakibatkan kerugian fatal bagi pemilik rekening ataupun bank.

### 11.2.4 Sumber Lubang Keamanan (Security Hole)

Lubang keamanan berarti titik atau bagian yang dapat menjadi sumber kerentanan keamanan pada sebuah sistem. Dengan kata lain bagian yang rentan untuk menjadi objek serangan keamanan. (Rahardjo, 2005) mengemukakan empat faktor yang menjadi sumber lubang keamanan (security hole), yaitu:

1. Kesalahan desain (design flaw). Lubang keamanan karena kesalahan desain sulit diperbaiki, namun jarang terjadi. Meskipun diimplementasi dengan baik, kelemahan akan tetap ada sepanjang desain tidak diubah. Sebagai contoh sistem yang menerapkan algoritma caesar cipher lemah terhadap serangan karena siapapun yang mengetahui algoritmanya dapat memecahkan enkripsinya.
2. Kesalahan implementasi. Lubang keamanan yang diakibatkan oleh kesalahan implementasi sering terjadi. Program yang diimplementasikan secara terburu-buru dan kurang cermat kadangkala meninggalkan peluang untuk dieksploitasi.
3. Kesalahan konfigurasi. Kesalahan konfigurasi dapat menjadi salah satu potensi lubang keamanan. Sebagai contoh, konfigurasi sebuah berkas yang seharusnya hanya "read-only" secara tidak sengaja terkonfigurasi "writeable".
4. Kesalahan Penggunaan. Kesalahan penggunaan program atau sistem juga dapat menyebabkan terjadinya lubang keamanan. Sebagai contoh, seorang sistem administrator yang lalai dalam menggunakan command yang berakibat fatal pada sistem.

### 11.2.5 Mengamankan Sistem Informasi

Berikut ini enam cara yang dapat ditempuh untuk mengamankan sistem informasi (Rahardjo, 2005):

1. Mengatur akses (access Control), sebagai upaya untuk memastikan sistem hanya diakses oleh pihak-pihak yang terotorisasi dengan menerapkan mekanisme user authentication yang sesuai standar.
2. Menutup servis yang tidak digunakan. Memastikan bahwa servis-servis yang tidak digunakan maupun yang berpotensi menjadi objek serangan dalam keadaan tertutup.
3. Memasang proteksi. Keamanan sistem informasi dapat ditingkatkan dengan memasang proteksi tambahan. Proteksi tambahan dapat berupa firewall, pemantau serangan (intruder detection system), pemantau integritas sistem, dll.
4. Audit dengan mengamati berkas log. Berkas log sangat berguna untuk mengamati dan menganalisis histori penyimpangan/ serangan yang terjadi. Berdasarkan hasil analisis log, administrator dapat mengidentifikasi potensi serangan maupun kelemahan sistem.
5. Backup secara rutin. Backup merupakan hal yang esensial pada sebuah sistem informasi. Hal ini untuk mengantisipasi terjadinya kehilangan data pada sistem utama baik yang diakibatkan oleh kelalaian internal maupun karena serangan dari intruder.
6. Penggunaan Enkripsi untuk meningkatkan keamanan. Teknologi enkripsi membantu mengamankan data/ informasi agar tidak mudah disadap oleh pihak yang tidak berhak.

## 11.3 Evaluasi Keamanan Sistem Informasi

Meskipun telah dirancang memiliki perangkat keamanan, sebuah sistem informasi harus selalu diuji/ dievaluasi. Hal ini diperlukan, agar pemilik ataupun pihak manajemen memiliki keyakinan akan jaminan tingkat keamanan/ kehandalan sistem informasi yang dimiliki. (Rahardjo, 2005) mengemukakan tiga (3) hal yang menjadi penyebab perlunya evaluasi dan monitoring dilakukan, yaitu:

1. Ditemukannya lubang keamanan (security hole) baru. Sistem yang kompleks kadangkala belum melewati proses pengujian secara menyeluruh (seratus persen) pada saat implementasi awal sehingga memungkinkan adanya potensi lubang keamanan.
2. Kesalahan konfigurasi. Kelalaian dalam mengkonfigurasi sebuah sistem dengan benar dapat menimbulkan lubang keamanan. Sebagai contoh, kesalahan penetapan mode kepemilikan (permission) ataupun sharing option sebuah berkas sehingga dapat diubah/ diedit oleh pihak yang tidak berhak.
3. Penambahan perangkat (keras/ lunak) baru. Penambahan perangkat baru dapat menjadi salah satu penyebab menurunnya tingkat keamanan atau berubahnya teknik pengoperasian sebuah sistem. Sebagai contoh software ataupun server yang masih menggunakan konfigurasi dan password vendor akan menjadi sasaran serangan keamanan.

### 11.3.1 Cara Pengujian Keamanan Sistem Informasi

Terdapat berbagai pendekatan yang dapat dilakukan untuk menguji keamanan sistem. (Rahardjo, 2005) mengemukakan empat cara untuk melakukan pengujian keamanan, yaitu:

1. Pengujian dengan perangkat pembantu otomatis (automated tools). Untuk menguji sebuah sistem informasi yang kompleks, maka administrator membutuhkan perangkat otomatis agar memudahkan proses pengujian atau proses evaluasi keamanan sistem informasi yang dikelola. Beberapa contoh tools untuk platform UNIX di antaranya: cops, tripwire, satan, SBScan. Selain itu ada banyak pula program-program yang dibuat secara parsial, seperti crack, winuka, dll.
2. Probing Services. Probing service ditujukan untuk meraba/ memeriksa (probe) servis apa saja yang tersedia pada sistem. Hal ini untuk menemukan dan memastikan tidak ada servis yang berpotensi menjadi media bagi pihak-pihak yang tidak terotorisasi untuk melakukan serangan. Salah satu program yang biasa digunakan untuk melakukan probe adalah telnet.

3. Penggunaan program penyerang (attacker programs). Menyerang diri sendiri dengan paket program penyerang merupakan salah satu cara untuk mengetahui kelemahan sistem informasi yang dimiliki. Sehingga kelemahan sistem maupun titik-titik rentan yang bisa menjadi objek eksploitasi oleh pihak yang tidak bertanggung jawab dapat diidentifikasi.
4. Penggunaan sistem pemantau jaringan (network monitoring software). Sistem pemantau jaringan dapat digunakan untuk menemukan adanya lubang keamanan pada sistem informasi. Selain itu, pemantau jaringan berfungsi pula untuk mengawasi ancaman-ancaman keamanan dari luar yang berusaha untuk melumpuhkan sistem dengan upaya denial of service (DoS) attack.

### 11.3.2 Kriteria Evaluasi Keamanan Sistem Informasi

Hingga saat ini telah dirumuskan berbagai metode pengujian keamanan sistem informasi berikut kriterianya masing-masing. Salah satu rumusan standar internasional adalah *common criteria* (CC) yang secara formal dikenal dengan "common criteria for information technology security evaluation". Common Criteria memiliki dua komponen kunci, yaitu profil perlindungan (protection profil) dan level jaminan evaluasi (evaluation assurance levels). Protection profile (Ppro) mendefinisikan rangkaian standar terkait syarat keamanan dari sebuah produk (misal: firewall, dll). Sedangkan evaluation assurance level yang terdiri atas 7 level (level 1 hingga level 7), mendefinisikan seberapa teliti dan bagaimana sebuah produk/ sistem dievaluasi. Versi terbaru common criteria yang telah dirilis adalah versi 3.1 (cc v3.1 Release 5) sebagaimana tertera pada ('CCPART1V3.1R5.pdf', 2017).



# **Bab 12**

## **Kode Etik Profesi IT**

### **12.1 Pentingnya Kode Etik Profesi IT**

Dalam pergaulan sehari-hari seringkali kita mendengar istilah kode etik, namun apakah kita mengerti tentang istilah kode etik tersebut? Kode Etik terdiri dari dua kata yaitu “kode” dan “etik”. Kode merupakan tanda-tanda atau simbol-simbol yang berupa kata-kata, tulisan atau benda yang disepakati untuk maksud-maksud tertentu. Sedangkan etik (atau etika) berasal dari kata ethos (bahasa Yunani) yang berarti karakter, watak kesusilaan atau adat. Sebagai suatu subjek, etika akan berkaitan dengan konsep yang dimiliki oleh individu ataupun kelompok untuk menilai apakah tindakan-tindakan yang telah dikerjakannya itu salah atau benar, buruk atau baik. Kode etik merupakan suatu norma, nilai, tata cara dan aturan yang dibuat secara tertulis, di dalamnya berisi tentang hal-hal baik dan tidak baik yang harus ditaati oleh seorang profesional. Kode etik disusun untuk memberikan batasan yang jelas agar seorang profesional dapat melakukan pekerjaan/jasa dengan baik dan sebagai pelindung bagi pemberi pekerjaan/jasa agar terhindar dari perbuatan yang tidak profesional.

Karena itu maka dapat disimpulkan bahwa etika sangat dibutuhkan bagi para profesional khususnya di bidang IT agar selalu mengutamakan etika dalam melakukan tindakan-tindakan, apalagi terkait dengan jasa profesinya.



## 12.2 Sejarah dan Perkembangan Etika Profesi IT

Sesuai awal penemuan teknologi komputer di era 1940–an, perkembangan etika profesi IT juga dimulai dari era tersebut dan secara bertahap berkembang menjadi sebuah disiplin ilmu baru di masa sekarang ini. Perkembangan tersebut akan dibagi menjadi beberapa tahap seperti yang akan dibahas berikut ini (Wahyono, 2006):

### **Era 1940-1950-an**

Munculnya etika komputer sebagai sebuah bidang studi dimulai dari pekerjaan profesor Norbert Wiener yang mengembangkan suatu meriam anti pesawat yang mampu menembak jatuh sebuah pesawat tempur yang melintas di atasnya. Pada perkembangannya, penelitian di bidang etika dan teknologi tersebut akhirnya menciptakan suatu bidang riset baru yang disebut cybernetics atau the science of information feedback. Konsep cybernetics tersebut dikombinasikan dengan komputer digital yang dikembangkan pada waktu itu, membuat Wiener akhirnya menarik beberapa kesimpulan etis tentang pemanfaatan teknologi.

### **Era 1960-an**

Pada pertengahan tahun 1960, Donn Parker dari SRI International Menlo Park California melakukan berbagai riset untuk menguji penggunaan komputer yang tidak sesuai dengan profesionalisme di bidang komputer. Selanjutnya, Parker melakukan riset dan mengumpulkan berbagai macam contoh kejahatan komputer dan aktivitas lain yang menurutnya tidak pantas dilakukan para profesional komputer. Dalam perkembangannya, ia menerbitkan “Rules of Ethics in Information Processing” atau peraturan tentang etika dalam pengolahan informasi. Parker juga dikenal menjadi pelopor kode etik profesi bagi profesional di bidang komputer, yang ditandai dengan usahanya pada tahun 1968 ketika ditunjuk untuk memimpin pengembangan Kode Etik Profesional yang pertama dilakukan untuk Association for Computing Machinery (ACM).

### **Era 1970-an**

Perkembangan etika komputer di era 1970-an juga diwarnai dengan karya Walter Maner yang sudah mulai menggunakan istilah “computer ethics” untuk

mengacu pada bidang pemeriksaan yang berhadapan dengan masalah etis yang diciptakan oleh pemakaian teknologi komputer waktu itu.

### **Era 1980-an**

Pertengahan 80-an, James Moor dari Dartmouth College menerbitkan artikel menarik yang berjudul “What is computer Ethics?” sebagai isu khusus pada Jurnal *Metaphilosophy* (Moor, 1985). Deborah Johnson dari Rensselaer Polytechnic Institute menerbitkan buku teks *Computer Ethics* (Johnson, 1985), sebagai buku teks pertama yang digunakan lebih dari satu dekade dalam bidang itu.

### **Era 1990-an sampai sekarang**

Sepanjang tahun 1990, berbagai pelatihan baru di universitas, pusat riset, konferensi, jurnal, buku teks dan artikel menunjukkan suatu keanekaragaman yang luas tentang topik di bidang etika komputer. Sebagai contoh, pemikir seperti Donald Gotterbarn, Keith Miller, Simon Rogerson, dan Dianne Martin. Para ahli komputer di Inggris, Polandia, Belanda, dan Italia menyelenggarakan ETHICOMP sebagai rangkaian konferensi yang dipimpin oleh Simon Rogerson. Terdapat pula konferensi besar tentang etika komputer CEPE yang dipimpin oleh Jeroen van Hoven, serta di Australia terjadi riset terbesar etika komputer yang dipimpin oleh Chris Simpson dan Yohanes Weckert.

### **Etika Komputer di Indonesia**

Sebagai negara yang tidak bisa dilepaskan dari perkembangan teknologi komputer, Indonesia pun tidak mau ketinggalan dalam mengembangkan etika di bidang tersebut. Mengadopsi pemikir dunia di atas, etika di bidang komputer berkembang menjadi kurikulum wajib yang dilakukan hampir semua perguruan tinggi di bidang komputer di Indonesia.

## **12.3 Pengertian Kode Etik Profesi**

Kode Etik Profesi merupakan bagian yang tak terpisahkan dari etika profesi. Kode etik profesi merupakan lanjutan dari norma-norma yang lebih umum yang telah dibahas dan dirumuskan dalam etika profesi. Kode etik ini lebih memperjelas, mempertegas dan merinci norma-norma ke bentuk yang lebih sempurna walaupun sebenarnya norma-norma tersebut sudah tersirat dalam etika profesi. Berikut ini beberapa pengertian kode etik menurut para ahli,

terdiri atas: Sonny Keraf dalam Rosady (2011), menyatakan bahwa kode etik merupakan kaidah moral yang berlaku khusus untuk orang-orang profesional di bidang tersebut. Prof. Dr. R. Soebekti, S.H. menyatakan bahwa kode etik suatu profesi berupa norma-norma yang harus diindahkan oleh orang-orang yang menjalankan tugas profesi tersebut. Cutlip, Carter dan Broom (2000) menjelaskan bahwa etika profesi merupakan perilaku yang disarankan secara efektif dalam bertindak sesuai dengan pedoman nilai-nilai moral yang diterima secara umum di masyarakat atau kebudayaan tertentu. Menurut profesional, aplikasi nilai moral pada implementasinya didasarkan pada etika pelaksanaannya. Membangun etika perilaku profesi tersebut, akan sangat ideal apabila sejalan dengan kode etik normatif (formal) dan mendapatkan pengakuan secara profesional, yang berdasarkan cara pelaksanaannya dan penerapan sanksinya jika terjadi pelanggaran pada pelaksanaannya.

Berdasarkan pengertian-pengertian tersebut diatas, maka dapat disimpulkan bahwa kode etik profesi merupakan nilai-nilai moral atau norma yang harus dipatuhi oleh semua yang menjalankan profesi tersebut, mendapatkan pengakuan secara profesional dan mendapatkan sanksi ketika melakukan pelanggaran sesuai dengan aturan yang berlaku.

## 12.4 Tujuan dan Fungsi Kode Etik Profesi

Berikut ini akan diuraikan beberapa tujuan dan fungsi kode etik profesi (Farid dan Riyadi, 2019)

### **Tujuan Kode Etik Profesi**

Pada dasarnya tujuan merumuskan kode etik suatu profesi adalah untuk kepentingan organisasi profesi dan anggotanya. Beberapa tujuan kode etik profesi, yaitu sebagai berikut:

1. Untuk menjunjung tinggi martabat profesi.
2. Untuk menjaga dan memelihara kesejahteraan para anggota.
3. Untuk meningkatkan pengabdian para anggota profesi.
4. Untuk meningkatkan mutu profesi.
5. Untuk meningkatkan mutu organisasi profesi.

6. Meningkatkan layanan diatas keuntungan pribadi.
7. Mempunyai organisasi profesional yang kuat dan terjalin erat.
8. Menentukan baku standarnya sendiri.

### **Fungsi Kode Etik Profesi**

Ada tiga hal pokok yang merupakan fungsi dari kode etik profesi (Firmansyah, 2019), yaitu sebagai berikut:

1. Kode etik profesi adalah pedoman bagi setiap anggota profesi tentang prinsip profesionalitas. Sehingga pelaksana profesi dapat mengetahui suatu hal yang boleh dilakukan dan yang tidak boleh dilakukan.
2. Kode etik profesi adalah kontrol sosial bagi masyarakat atas profesi yang dijalankan. Artinya etika profesi dapat memberikan suatu pengetahuan kepada masyarakat agar juga dapat memahami arti pentingnya suatu profesi, sehingga memungkinkan pengontrolan terhadap para pelaksana di tempat kerja.
3. Kode etik profesi mencegah campur tangan pihak luar organisasi profesi tentang hubungan etika dalam keanggotaan profesi. Artinya bahwa pelaksana profesi pada suatu instansi atau perusahaan yang lain tidak boleh mencampuri pelaksanaan profesi di lain instansi atau perusahaan.

Sebagai seorang profesional di bidang IT mempunyai tanggung jawab untuk mempromosikan dan menerapkan kode etik di lokasi kerja masing-masing. Contohnya: penerapan kode etik profesi IT ketika kita membuat sebuah program aplikasi dari pengguna, maka kita harus memperhatikan masalah privasi pengguna, keamanan data pengguna, dan sebagainya.

## **12.5 Prinsip Dasar Kode Etik Profesi**

Prinsip dasar kode etik profesi sebagai berikut:

1. Prinsip standar teknis  
Setiap anggota profesi harus melaksanakan jasa profesional yang relevan dengan bidang profesinya

2. Prinsip kompetensi  
Setiap anggota profesi harus melaksanakan pekerjaan sesuai dengan kehati-hatian, kompetensi dan ketekunan
3. Prinsip tanggung jawab profesi  
Dalam melaksanakan tanggung jawabnya sebagai profesional, setiap anggota harus senantiasa menggunakan pertimbangan moral dan profesional dalam semua kegiatan yang dilakukan
4. Prinsip kepentingan publik  
Setiap anggota berkewajiban untuk senantiasa bertindak memberikan jasa profesionalnya dalam kerangka pelayanan kepada publik, menghormati kepercayaan publik, dan menunjukkan komitmen atas profesionalisme
5. Prinsip integritas  
Pelaku profesi menjunjung nilai tanggung jawab profesional dengan integritas setinggi mungkin untuk memelihara dan meningkatkan kepercayaan publik yang menggunakan jasa profesionalnya
6. Prinsip obyektivitas  
Setiap anggota harus menjaga obyektivitas dari benturan kepentingan dalam pemenuhan kewajiban profesionalnya
7. Prinsip kerahasiaan  
Setiap anggota harus menghormati kerahasiaan informasi yang diperoleh selama melakukan jasa profesional dan tidak boleh memakai atau mengungkapkan informasi tersebut tanpa persetujuan, kecuali bila ada hak atau kewajiban profesional atau hukum untuk mengungkapkannya
8. Prinsip perilaku profesional  
Setiap anggota harus perilaku konsisten dengan reputasi profesi yang baik dan menjauhi tindakan yang dapat mendiskreditkan profesi yang diembannya

## 12.6 Organisasi Profesi IT Indonesia

### **Ikatan Profesi Komputer dan Informatika Indonesia (IPKIN)**

Pada tanggal 18 April 1974 didirikan organisasi Himpunan Pemakai Komputer Indonesia (HPKI), kemudian seiring dengan perjalanan waktu, tanggal 30 Juli 1974 organisasi ini berganti nama menjadi Ikatan Pengguna Komputer Indonesia (IPKIN). Pada tahun 1975 secara resmi dokumen hukum IPKIN telah tersusun. Logo IPKIN didesain oleh Soenarjono Danoedjo. IPKIN merupakan organisasi profesi IT pertama di Indonesia. Pada tahun 1999 singkatan IPKIN berubah menjadi Ikatan Profesi Komputer dan Informatika Indonesia. Sejak tahun 2003 IPKIN berkembang ke berbagai daerah dan mulai dibukanya beberapa cabang, hingga saat ini ada 7 cabang yang sudah dibuka yaitu: Medan, Palembang, Bandung, Semarang, Yogyakarta, Surabaya dan Denpasar.

Jumlah anggota aktif tercatat hingga saat ini berjumlah 233 orang. IPKIN bertujuan untuk meningkatkan pemanfaatan dan pengembangan teknologi Komputer dan Informatika di Indonesia guna menunjang Pembangunan Nasional. Untuk itu IPKIN berupaya berperan sebagai wadah komunikasi, konsultasi dan koordinasi antar anggota. Untuk informasi selengkapnya mengenai Ikatan Ahli Profesi Komputer dan Informatika (IPKIN) dapat dilihat di website resminya <http://www.ipkin.co.id>

### **Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)**

Dalam Musyawarah Nasional Pertama tanggal 15 Mei 1996, Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dinyatakan berdiri, dewan pengurus yang ditunjuk untuk masa jabatan 3 tahun pertama diminta untuk melakukan beberapa program kunci yang dinilai strategis untuk pengembangan jaringan internet di Indonesia. Program-program tersebut adalah:

1. Tarif Jasa Internet
2. Pembentukan Indonesia-Network Information Center [ID-NIC]
3. Pembentukan Indonesia Internet Exchange [IIX]
4. Negosiasi Tarif Infrastruktur Jasa Telekomunikasi
5. Usulan Jumlah dan Jenis Provider

APJII memiliki misi dan tujuan sebagai berikut:

1. Membantu para anggota dalam menyediakan jasa Internet yang berkualitas bagi masyarakat Indonesia.
2. Memasyarakatkan Internet dalam menunjang pengembangan sumber daya manusia di Indonesia.
3. Mendukung terciptanya peluang bisnis pengusaha Indonesia melalui penyediaan sarana informasi dan komunikasi global.
4. Membantu pemerintah dalam usaha pemerataan ekonomi di tanah air melalui kesempatan akses terhadap informasi dan komunikasi secara merata di seluruh pelosok Indonesia.
5. Membantu para anggota dalam menyediakan sumber-sumber informasi mengenai Indonesia.
6. Meningkatkan partisipasi masyarakat Indonesia dalam kerjasama Internasional. (APJII, 2019)

### **Ikatan Ahli Informatika Indonesia (IAII)**

Ikatan Ahli Informatika Indonesia (IAII) didirikan di Bandung tanggal 15 Nopember 2014 oleh 300 profesional di bidang IT. IAII adalah organisasi profesi, yaitu organisasi nirlaba (non profit organization) yang menghimpun ahli-ahli Informatika Indonesia dalam satu wadah untuk bersatu padu untuk meningkatkan daya saing Indonesia melalui keahlian dan profesi Informatika (computing, yaitu bidang yang meliputi informatika/ilmu komputer, rekayasa perangkat lunak, sistem informasi, teknologi informasi, sistem/teknik komputer, manajemen dan tata kelola teknologi informasi). Ikatan Ahli Informatika Indonesia (IAII) adalah organisasi profesi yang bertujuan meningkatkan kualitas teknologi informasi di Indonesia, melindungi masyarakat dari praktik buruk layanan ahli informatika, meningkatkan kemakmuran, martabat, kehormatan, dan peran ahli informatika Indonesia dalam rangka mencapai tujuan Negara Kesatuan Republik Indonesia yang tercantum pada Pembukaan UUD 1945 (IAII, 2014).

### **Perkumpulan Profesional Teknologi Informasi (PPTI)**

Perkumpulan Profesional Teknologi Informasi (PPTI) adalah organisasi keprofesian di bidang Teknologi Informasi (TI) yang didirikan pada tanggal 1 Juni 2018 di Jakarta. PPTI merupakan organisasi para profesional Teknologi Informasi dan merupakan lembaga mandiri. Mengingat keprofesian TI di

Indonesia memiliki kompetensi yang sesuai untuk mengisi pembangunan nasional di bidang Teknologi Informasi sejajar dengan kemampuan internasional. Berdirinya PPTI bertujuan untuk membina dan mengembangkan profesi Teknologi Informasi di Indonesia untuk mendukung pembangunan nasional (PPTI, 2018).

### **Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM)**

Semakin banyak dan berkembangnya sekolah dan perguruan tinggi di bidang Information Technology (IT), menyebabkan peningkatan persaingan antara lembaga-lembaga pendidikan tersebut untuk menghasilkan lulusan yang berkualitas. Atmosfer persaingan yang sehat dibutuhkan untuk memacu perkembangan IT di Indonesia. Saat ini tercatat lebih dari 500.000 mahasiswa D1 hingga S3 yang sedang aktif belajar di lebih dari 850 Perguruan Tinggi di Indonesia dibawah naungan sekitar 1.500 program studi Kampus Informatika dan Komputer di seluruh Indonesia, dengan jumlah lulusan sekitar 40.000 hingga 50.000 alumni per tahunnya. APTIKOM sebagai sebuah asosiasi yang merupakan kerjasama antara perguruan tinggi di bidang IT diharapkan dapat menjadi wadah untuk dapat meningkatkan kerjasama baik antar perguruan tinggi, maupun antar perguruan tinggi dengan pemerintah dan pelaku usaha.

Semuanya bermula pada tahun 1983, yaitu ketika 8 perguruan tinggi penggagas pendirian Program Studi informatika dan komputer membentuk sebuah forum yang diberi nama Badan Kerja Sama Perguruan Tinggi Sejenis Ilmu Komputer (BKS PERTINIS I-K). Sejalan dengan perkembangan pesat ilmu komputer dan informatika, anggota BKS PERTINIS I-K bertambah menjadi 78 anggota pada tahun 1987. Puncaknya adalah pada tahun 1996, ketika BKS PERTINIS I-K berubah nama menjadi Perguruan Tinggi Informatika dan Komputer (PERTIKOM) jumlah anggota menjadi lebih dari 250 Program Studi dari seluruh wilayah di tanah air.

Sesuai dengan kebutuhan dan perkembangan zaman, maka pada Rapat Koordinasi Nasional (Rakornas) 2002 di Kota Malang, diusulkan oleh perubahan bentuk organisasi dari PERTIKOM menjadi Asosiasi Perguruan Tinggi Informatika dan Ilmu Komputer (APTIKOM). Sampai dengan saat ini, jumlah anggota APTIKOM terdiri dari 850 Perguruan Tinggi Informatika dan Komputer serta 1.560 Program Studi. (Kominfo, 2019)



### 12.6.1 Komunitas IT di Indonesia

Selain organisasi dan asosiasi, di Indonesia juga terdapat komunitas-komunitas di bidang IT. Beberapa komunitas yang ada tersebut, antara lain (Wahyono, 2006):

- Indonesia Internet Society : Organisasi Infrastruktur Informasi & Industri Teknologi Internet
- PHPID : Komunitas Pemrograman Berbasis Bahasa Scripting PHP
- MUGI : Microsoft User Group Indonesia)
- KPLI : Komunitas Pengguna Linux Indonesia
- Indonesia Oracle Application Users Group
- Indonesia Oracle Fans Site
- KIOSS : Komunitas Informasi Outsourcing
- Kesini : Kumpulan Networker & Instalasi Jaringan
- Komunikasi Postnuke Indonesia : Komunitas Web Designer, Web Programmer, atau Pemerhati Web.
- Apache Software : Organisasi Proyek Software
- Delphi Indonesia : Komunitas Delphi
- Indonesia Cisco Study Group : Kelompok Studi Pengguna Internetworking, khususnya Cisco
- Linux User Group Ujung Pandang
- Pelmongers : Kelompok Pengguna Perl
- Programmers Online
- Toekang Web : komunitas web designer berisi tip-tip, berita, revisi site pilihan dan profil web designer.

## 12.7 Organisasi Profesi IT Internasional

Beberapa organisasi profesi IT internasional yaitu sebagai berikut (wikipedia, 2020):

### **ACM (Association for Computing Machinery)**

ACM singkatan dari Association for Computing Machinery (Asosiasi untuk Permesinan Komputer), adalah sebuah serikat ilmiah dan pendidikan komputer pertama di dunia yang didirikan pada tanggal 15 September 1947. Anggota ACM sekitar 78.000 terdiri dari para profesional dan para pelajar yang tertarik akan komputer. Dia bermarkas besar di Kota New York. ACM diatur menjadi 170 bagian (chapter) lokal dan 34 grup minat khusus (Special Interest Group, SIG), di mana mereka melakukan kebanyakan kegiatan mereka.

Banyak dari SIG, seperti SIGGRAPH, SIGPLAN dan SIGCOMM, mensponsori konferensi teratur yang menjadi terkenal sebagai acara utama untuk memperkenalkan inovasi baru dalam bidang tertentu. SIG juga menerbitkan sejumlah jurnal khusus, majalan, dan surat berita. ACM juga mensponsori acara yang berhubungan dengan ilmu komputer seperti ACM International Collegiate Programming Contest (ICPC) yang mendunia, dan telah mensponsori beberapa acara lainnya, seperti pertandingan catur antara Garry Kasparov dan komputer IBM Deep Blue.

### **IEEE (Institute of Electrical and Electronics Engineers)**

Sebelumnya IEEE memiliki kepanjangan yang dalam Indonesia berarti Institut Insinyur Listrik dan Elektronik (Institute of Electrical and Electronics Engineers). Namun kini kepanjangan itu tak lagi digunakan, selain untuk keperluan legal; sehingga organisasi ini memiliki nama resmi IEEE saja. IEEE memiliki lebih dari 415.000 anggota individu yang tersebar dalam lebih dari 150 negara. Aktivitasnya mencakup beberapa panitia pembuat standar, publikasi terhadap standar-standar teknik, serta mengadakan konferensi.

IEEE Indonesia Section berada pada IEEE Region 10 (Asia-Pasifik). Section ini dinyatakan berdiri pada 16 Februari 1988. Saat ini IEEE Indonesia Section memiliki beberapa chapter, yaitu:

- Computer Society Chapter
- Communications Society Chapter
- Circuits and Systems Chapter

- Engineering in Medicine and Biology Chapter
- Join Chapter of Education Society / Electron Devices Society / Power Electronics Society / Signal Processing Society
- Join chapter of Microwave Theory / Antennas & Propagation
- Join chapter of Control System / Robotics & Automation

### **South East Asia Regional Computer Confederation (SEARCC)**

SEARCC adalah asosiasi nirlaba dari asosiasi profesional komputer nasional di wilayah Asia-Pasifik. SEARCC adalah forum perkumpulan profesional teknologi informasi nasional di kawasan Asia Pasifik. Piagam dan konstitusi SEARCC ditandatangani di Singapura tanggal 28 Februari 1978. Enam perkumpulan nasional dari kawasan itu: Masyarakat Komputer Hongkong, Masyarakat Komputer Indonesia, Konfederasi Komputer Nasional Malaysia, Masyarakat Komputer Filipina, Asosiasi Komputer Singapura dan Asosiasi Komputer Thailand adalah para penandatangan pendiri. SEARCC adalah anggota IFIP (International Federation for Information Processing). IFIP adalah organisasi internasional untuk masyarakat nasional yang bergerak di bidang teknologi informasi. Ini adalah organisasi non-pemerintah, nirlaba berkantor pusat di Laxenburg, Austria. IFIP didirikan pada tahun 1960 dibawah naungan UNESCO.

SEARCC juga menyelenggarakan Kompetisi Perangkat Lunak Sekolah Internasional Tahunan, Kompetisi Pemrograman Tim, biasanya diperebutkan oleh Tim Pemenang berasal dari Kompetisi Pemrograman Nasional dari Negara tersebut. Strategi SEARCC yaitu:

1. Untuk mendorong kemakmuran ekonomi dan sosial di seluruh wilayah melalui peningkatan profesi TIK.
2. Memfasilitasi penyampaian program dan layanan yang relevan dan berharga untuk kepentingan asosiasi anggotanya.
3. Berkolaborasi dan membangun hubungan dengan pemangku kepentingan internasional utama untuk mencapai tujuan dan kepentingan bersama.
4. Teladan pemerintahan yang baik dan kepemimpinan pemikiran dengan membangun dan mencapai hasil.

Komitmen SEARCC yaitu:

1. Berbagi pendekatan terbaik untuk kebijakan teknologi, strategi, dan implementasi.
2. Menginspirasi generasi berikutnya melalui kompetisi coding internasional kami.
3. Mempromosikan keunggulan dalam industri melalui Penghargaan ICT Global kami.
4. Membantu anggota dengan dukungan advokasi untuk ekonomi domestik, pemerintah dan industri mereka.
5. Menetapkan tolok ukur profesional di kawasan ini untuk meningkatkan peluang perdagangan di seluruh negara anggota.
6. Menyampaikan proyek kerja sama yang menunjukkan kepemimpinan kepada pemerintah dan industri dalam pendidikan teknologi baru dan pembangunan kapasitas. (SEARCC, 2017)

## 12.8 Kode Etik Profesi Bidang IT

Etika profesi bidang IT itu mengatur bagaimana seorang profesional di bidang IT harus melakukan pekerjaannya dengan mengedepankan kode etik, karena jika bertentangan dengan kode etik, maka akan menjadi masalah yang besar di kemudian hari nanti. Itulah sebabnya maka setiap asosiasi atau organisasi profesi di bidang IT membuat kode etik untuk dipatuhi dan dilaksanakan oleh para anggotanya. Jika ada anggota profesi tidak menjalankan kode etik dengan baik dan bertanggung jawab, maka dapat mencemarkan nama baik profesi atau organisasi.

### **Kode Etik ACM (Association for Computing Machinery)**

Tindakan profesional komputasi mengubah dunia. Untuk bertindak secara bertanggung jawab, mereka harus merefleksikan dampak yang lebih luas dari pekerjaan mereka, secara konsisten mendukung kepentingan publik. Kode Etik dan Perilaku Profesional ACM ("Kode") mengungkapkan hati nurani profesinya. Kode ini dirancang untuk menginspirasi dan memandu perilaku etis semua profesional komputasi, termasuk praktisi, instruktur, pelajar, pemberi pengaruh, dan siapa pun yang menggunakan teknologi komputasi

dengan cara yang berdampak. Selain itu, Kode berfungsi sebagai dasar untuk perbaikan saat pelanggaran terjadi. Kode ini mencakup prinsip-prinsip yang dirumuskan sebagai pernyataan tanggung jawab, berdasarkan pemahaman bahwa kepentingan umum selalu menjadi pertimbangan utama. Setiap prinsip dilengkapi dengan pedoman, yang memberikan penjelasan untuk membantu para profesional komputasi dalam memahami dan menerapkan prinsip tersebut.

Adapun kode etik yang ada pada ACM secara garis besar dibagi menjadi 4 bagian, yaitu sebagai berikut (ACM, 2020):

1. Prinsip Etis Umum, seorang profesional komputasi harus:
  - Berkontribusi pada masyarakat dan kesejahteraan manusia.
  - Hindari “Bahaya”.
  - Jujur dan dapat dipercaya.
  - Bersikap Adil dan tidak bersikap diskriminatif.
  - Menghargai hak cipta.
  - Hargai Privasi.
  - Hormati Kerahasiaan.
2. Tanggung Jawab Profesional, seorang profesional komputasi harus:
  - Berusaha keras untuk mencapai kualitas tinggi baik dalam proses maupun produk dari pekerjaan profesional.
  - Pertahankan standar tinggi kompetensi profesional, perilaku, dan praktik etis.
  - Mengetahui dan menghormati aturan yang terkait dengan pekerjaan profesional.
  - Menerima dan memberikan ulasan profesional yang sesuai.
  - Berikan evaluasi yang komprehensif dan menyeluruh terhadap sistem komputer dan dampaknya, termasuk analisis risiko yang mungkin terjadi.
  - Lakukan pekerjaan hanya di bidang kompetensi.
  - Menumbuhkan kesadaran publik dan pemahaman tentang komputasi, teknologi terkait, dan konsekuensinya.
  - Mengakses sumber daya komputasi dan komunikasi hanya jika diizinkan atau ketika dipaksa oleh publik.

- Desain dan implementasi sistem yang kuat dan dapat digunakan dengan aman.
3. Prinsip Kepemimpinan Profesional
- Kepemimpinan dapat berupa sebutan formal atau muncul secara informal dari pengaruh atas orang lain. Dalam bagian ini, "pemimpin" berarti setiap anggota organisasi atau kelompok yang memiliki pengaruh, tanggung jawab pendidikan, atau tanggung jawab manajerial. Sementara prinsip-prinsip ini berlaku untuk semua profesional komputasi, para pemimpin memikul tanggung jawab yang tinggi untuk menegakkan dan mempromosikannya, baik di dalam maupun melalui organisasi mereka. Seorang profesional komputasi, terutama yang bertindak sebagai pemimpin, harus:
- Memastikan bahwa barang publik adalah perhatian utama selama semua pekerjaan komputasi profesional.
  - Mengartikulasikan, mendorong penerimaan, dan mengevaluasi pemenuhan tanggung jawab sosial oleh anggota organisasi atau kelompok.
  - Mengelola personel dan sumber daya untuk meningkatkan kualitas kehidupan kerja.
  - Mengartikulasikan, menerapkan, dan mendukung kebijakan dan proses yang mencerminkan prinsip-prinsip kode etik.
  - Menciptakan peluang bagi anggota organisasi atau kelompok untuk tumbuh sebagai profesional.
  - Berhati-hatilah saat memodifikasi atau menghentikan sistem.
  - Mengenali dan merawat secara khusus sistem yang terintegrasi ke dalam infrastruktur masyarakat.
4. Kepatuhan Dengan Kode Etik, seorang profesional komputasi harus:
- Menjunjung tinggi, mempromosikan, dan menghormati prinsip-prinsip kode etik.
  - Menangani pelanggaran kode etik sebagai tidak konsisten dengan keanggotaan dalam ACM.



## **Bab 13**

# **Perspektif Cyber Law dan UU ITE Dalam Sistem Hukum Di Indonesia**

### **13.1 Pendahuluan**

Sebagai wujud dari ilmu pengetahuan modern dalam era revolusi industri, maka perkembangan teknologi saat ini terjadi sangat pesat. Identifikasi perkembangan teknologi tersebut dapat terlihat dari munculnya inovasi-inovasi teknologi. (Phyllis Deane, 1979) Salah satu kemajuan teknologi ialah dibidang teknologi informasi yang berkembang seiring dengan globalisasi yang berlangsung hampir di semua bidang kehidupan. (Juwono Sudarsono, 1990) Pengaruh globalisasi terjadi pada industri yang berakibat lahirnya revolusi industri. Revolusi industri 2.0 terjadi di awal abad ke-20. Revolusi industri ini ditandai dengan perkembangan teknologi di bidang baja, bahan kimia, listrik dan di berbagai bidang lainnya (Harshit Agarwal dan Rashi Agarwal, 2017: 1963). Setelah revolusi industri kedua, manusia masih berperan sangat penting dalam proses produksi berbagai macam jenis barang. Tetapi, setelah revolusi industri yang ketiga, manusia tidak lagi memegang peranan penting. Setelah revolusi ini, abad industri pelan-pelan berakhir dan abad informasi dimulai (Ning Rahayu, 2019). Menurut Jeremy Rifkin bahwa pada pertengahan tahun



1990-an, mulai terjadi konvergensi komunikasi dan energi, di mana teknologi internet dan energi terbarukan bergabung untuk menciptakan infrastruktur yang kuat untuk revolusi industri ketiga. (Jeremy Rifkin: 2011) Perkembangan internet yang pesat baru-baru ini dan kemampuannya untuk menawarkan berbagai jenis layanan telah menjadikannya teknologi yang paling cepat berkembang, dengan dampak besar pada kehidupan sosial dan lingkungan bisnis (Mohamed Abomhara dan Geir M. Kjøen: 2015).

Sejak tahun 2011, era industri 4.0 telah dimulai, yang ditandai meningkatnya konektivitas, interaksi, dan batas antara manusia, mesin, dan sumber daya lainnya yang semakin konvergen melalui teknologi informasi dan komunikasi. (Kementerian Perindustrian RI: 2019) Secara pesat, teknologi ini mengubah cara hidup masyarakat, di mana batas ruang dan waktu sudah tidak menjadi kendala besar (borderless). Bahkan kehadiran internet yang sangat fenomenal ini semakin mengukuhkan pendapat bahwa teknologi informasi dan komunikasi telah menjadi *mainstream* budaya masyarakat dunia saat ini. (Jimy Asshiddiqie 2005) Padahal di sisi lain, Informasi media massa (baik media cetak, media elektronik, maupun cybermedia) memiliki pengaruh yang lebih besar dari apapun. Terjadinya revolusi informasi dan dominasi kebebasan informasi internasional yang luar biasa telah membawa masalah etika, budi pekerti dan kearifan manusia dalam mengelola masalah informasi. Globalisasi menyebabkan terjadinya konvergensi dari tatanan hukum (legal order) atau sistem hukum. (Muhadjir Effendy: 2016) Sistem hukum mendapat pengaruh dari teknologi, sehingga tatanan hukum akan bergerak ke arah yang lebih memadai. Implikasi dari globalisasi yang ditandai dengan perkembangan teknologi yang semakin pesat, terutama teknologi informasi dan komunikasi, akan memaksa tatanan hukum untuk berkonvergensi sehingga tercapainya efisiensi secara ekonomis. Hal ini karena tatanan regulasi terkait dari suatu tatanan hukum akan membuat satu sistem hukum saja tidak akan mampu memberikan solusi yang optimal dari permasalahan-permasalahan yang muncul. (Danrivanto Budhijanto: 2014).

Saat ini era digitalisasi dan pengaruh industri 4.0 di Indonesia membawa pengaruh yang cukup besar pada semua bidang kehidupan masyarakat Indonesia. Keberadaan Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik menunjukkan hukum teknologi informasi diperlukan guna mencegah akses

negatif dari penggunaan teknologi informasi yakni mencegah terjadinya penyalahgunaan teknologi informasi internet seperti facebook, instagram, whatsapp, twitter, telegram untuk tujuan penyebaran berita bohong (hoax), pencemaran nama baik, ujaran kebencian (hate speech), penghinaan yang melanggar hak asasi manusia dan lain sebagainya. Pada sisi lain berkenaan dengan pembangunan teknologi, maka melalui internet, peradaban manusia dihadapkan pada fenomena baru yang mampu mengubah setiap aspek kehidupan manusia (Dikdik M. Arief Mansur dan Elisatris Gultom: 2009).

Menurut Gustav Radbruch sebagaimana dikutip oleh Brian Bix (Brian H. Bix: 2011) terdapat tiga aspek tujuan hukum, yaitu: keadilan, kemanfaatan, dan kepastian hukum. Tujuan hukum tersebut dapat dicapai dengan didukung oleh sistem hukum yang baik. Untuk menciptakan sistem hukum yang baik, maka diperlukan adanya pengembangan sistem hukum tersebut. Namun, pengembangan sistem hukum seringkali terhambat karena sejak dulu paradigma dan kondisi hukum harus diakui tidak banyak mengalami perubahan yang signifikan. Padahal hukum sebagai panglima tertinggi seharusnya mampu menghadapi perkembangan zaman dan bisa beradaptasi sesuai dengan tantangan yang ada termasuk perkembangan teknologi yang pesat. Hukum sebagai sarana yang penting untuk memelihara ketertiban dan sekaligus pembaharuan masyarakat dan Negara harus dikembangkan sedemikian rupa, sehingga dapat memberi ruang gerak bagi perubahan, dan bukan sebaliknya, menghambat usaha-usaha pembaharuan karena semata-mata ingin mempertahankan nilai-nilai ortodoks. (Mochtar Kusumaatmadja: 2002) Pembaharuan sistem hukum dilakukan dengan memperhatikan tiga bidang yang saling terkait yakni struktur hukum (legal structure), substansi hukum (legal substance), budaya hukum (legal culture).

## 13.2 Cyber Law dan Undang-Undang Informasi dan Transaksi Elektronik

### 13.2.1 Pengertian Cyber Law

Kehadiran hukum sebagai sarana pembaharuan didasarkan atas pemikiran bahwa adanya keteraturan atau ketertiban dalam pembangunan dan peningkatan kesejahteraan masyarakat adalah mutlak adanya. Berbagai kaidah

dan peraturan dapat berfungsi sebagai alat pengatur kegiatan manusia ke arah yang dikehendaki oleh pembangunan dimaksud. Fungsi hukum menurut teori hukum pembangunan adalah selain untuk mencapai ketertiban dan keadilan, juga dapat berfungsi sebagai sarana pembaharuan dalam masyarakat. Pandangan ini dikemukakan oleh Mochtar Kusumaatmadja yang merupakan modifikasi terhadap pandangan Roscoe Pound tentang *law as a tool of social engineering* (hukum sebagai alat pembaharuan masyarakat).

Cyber Law adalah aspek hukum yang istilahnya berasal dari Cyberspace Law, yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet/elektronik yang dimulai pada saat mulai “online” dan memasuki dunia cyber atau maya. Pada negara yang telah maju dalam penggunaan internet/elektronik sebagai alat untuk memfasilitasi setiap aspek kehidupan mereka, perkembangan hukum dunia maya sudah sangat maju. Pembagian ruang lingkup Cyber Law dalam beberapa hal di antaranya: Copyright (hak cipta), Trademark (hak merek), Defamation (pencemaran nama baik), Hate Speech (penistaan, penghinaan, fitnah), Hacking, Viruses, Illegal Access, (penyerangan terhadap komputer lain), Regulation Internet Resource (pengaturan sumber daya internet), Privacy (kenyamanan pribadi), Duty Care (kehati-hatian), Criminal Liability (kejahatan menggunakan IT), Procedural Issues (yuridiksi, pembuktian, penyelidikan, dll.), Electronic Contract (transaksi elektronik), Pornography, Robbery (pencurian lewat internet), Consumer Protection (perlindungan konsumen), dan E-Commerce, E-Government (pemanfaatan internet dalam keseharian) .

Disisi lain, dibentuknya Undang-undang Informasi dan Transaksi Elektronik adalah agar penggunaan teknologi informasi dalam cyber law (aspek hukum yang ruang lingkupnya meliputi semua aspek yang berhubungan dengan orang perorangan atau subjek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki dunia cyber atau maya) tidak disalahgunakan sehingga menimbulkan hoax, ujaran kebencian atau pencemaran nama baik dan sebagainya. Pengaturan hukum dalam bentuk sanksi pidana tidak saja merupakan ultimum remedium namun juga diharapkan menciptakan efek jera agar setiap masyarakat Indonesia pengguna teknologi dalam dunia maya tidak melakukan perbuatan pidana. Undang-undang Informasi dan Transaksi Elektronik diharapkan memberikan jaminan kepastian hukum (kepastian dalam pelaksanaannya. Setiap orang dianggap mengetahui adanya hukum dan hukum dapat ditegakkan) dan

memberikan keadilan (menuntut kepada setiap orang dalam situasi yang sama untuk diperlakukan sama). (Bambang Priyambodo dan Arif Awangga: 2020) Pada hakekatnya hukum (perundang-undangan) mempunyai fungsi sebagai sarana pembaharuan kehidupan masyarakat dan mengubah pola perilaku lama menjadi perilaku yang baru, yaitu: (Arif Awangga: 2020):

1. Hukum harus dapat mengemban fungsi ekspresif yakni mengungkapkan filosofis hidup bangsa, nilai-nilai budaya dan nilai-nilai sosial/kemasyarakatan yang berkembang.
2. Hukum harus dapat mengemban fungsi instrumental yakni sarana untuk menciptakan dan memelihara ketertiban, sarana untuk melestarikan nilai-nilai budaya dan mewujudkan keadilan. Sarana-sarana tersebut dijadikan suatu cara untuk melakukan pembaharuan masyarakat atau perubahan masyarakat menjadi lebih teratur dalam hidup dan kehidupannya.

Kebutuhan akan hukum dan peraturan perundang-undangan yang dapat mengakomodasi dan memfasilitasi konvergensi telematika saat ini sangat mendesak. Sementara peraturan perundang-undangan yang eksisting dalam bidang-bidang yang berhubungan dengan teknologi informasi, penyiaran, dan telekomunikasi belum mampu mengakomodasi tren dimaksud yang bersifat “ubiquitous”, artinya, sebuah teknologi yang memudahkan user dan dapat melakukan segala sesuatu seperti yang user inginkan, serta dapat dijangkau kapan saja, di mana saja, dan oleh siapa saja. (Pengertian Teknologi yang bersifat “ubiquitous”, memungkinkan user untuk memanfaatkan layanan aplikasi melalui internet, yaitu pemanfaatan jasa telekomunikasi, melalui jaringan telekomunikasi berbasis protokol internet yang menyediakan layanan komunikasi dalam bentuk pesan singkat, panggilan suara, panggilan video, dan daring percakapan (chatting), transaksi finansial dan komersial, penyimpanan dan pengambilan data, permainan (game), jejaring dan media sosial, serta turunannya).

Keberadaan konvergensi menjadikan fungsi pemerintah selaku pemegang otoritas kebijakan masih tetap diperlukan untuk memantau, mengawasi, dan memfasilitasi peralihan dari sistem yang cenderung anti kompetitif menuju ke sistem yang kompetitif dan berorientasi pada kepentingan konsumen (Danrivanto Budiharto: 2014). Peranan pemerintah tersebut antara lain meliputi (Danrivanto Budiharto 2014):

1. Mencegah para incumbent agar tidak menyalahgunakan posisi dominannya untuk meniadakan kompetisi, dan menjaga agar tidak terjadi peralihan monopoli dan perusahaan milik negara.
2. Mengatur kewajiban para operator agar tetap memberikan pelayanan universal. Prinsip-prinsip Kewajiban Pelayanan Universal (KPU) atau Universal Service Obligation (USO) ini diatur dalam Pasal 16 ayat (1) UU Telekomunikasi Tahun 1999, yang telah mewajibkan kepada semua operator, tanpa kecuali untuk memberikan kontribusi dalam pelayanan universal;
3. Mendorong inovasi dalam menciptakan daya saing bangsa dalam sektor TIK; dan;
4. Melindungi kepentingan konsumen dan/atau kepentingan publik.

Secara umum, hukum meliputi segala macam ketentuan hukum yang ada, baik materi hukum tertulis (tertuang dalam peraturan perundang-undangan) maupun materi hukum tidak tertulis (berupa kebiasaan yang dipraktekkan sebagai sebuah kelaziman). Dalam ilmu perundang-undangan, pembentukan aturan hukum dalam wujud undang-undang, yakni yang berorientasi pada melakukan perbuatan dalam hal pembentukan peraturan perundang-undangan, dan bersifat normatif, maka pembentukan hukum dalam wujud undang-undang ini dibagi dalam tiga bagian yaitu (Arif Awangga: 2020):

1. Proses perundang-undangan,
2. Metode perundang-undangan,
3. Teknik perundang-undangan

Sejak disahkannya Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Indonesia telah memiliki apa yang disebut dengan Cyber Law atau Cyberspace Law, yang mengatur peristiwa dan perbuatan hukum dengan medium ruang maya (cyberspace). Dengan makin masifnya pemanfaatan teknologi digital, maka regulasi di bidang ini juga akan terus berkembang. Hukum telematika adalah hukum terhadap perkembangan konvergensi telematika yang berwujud dalam penyelenggaraan suatu sistem elektronik, baik yang terkoneksi dengan internet maupun tidak. (Sugeng 2020, 14). Secara ideal, hukum telematika dapat melakukan harmonisasi semua asas dan tujuan yang telah ada di dalam UU Telekomunikasi, UU Penyiaran, UU ITE, dan UU Keterbukaan Informasi Publik (KIP). Beberapa aspek yang perlu

dilindungi dan cyberspace adalah sistem informasi yang baik (terjaga keutuhan dan keamanan sistemnya) dan perbuatan yang dilarang, yaitu illegal content, illegal access, illegal interception, data interference, system interference, misuse of device, dan computer related fraud.

Saat ini, pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika sedang dalam proses menyiapkan rancangan undang-undang yang akan mengatur mengenai Konvergensi Telematika. Rancangan Undang-Undang (RUU) Konvergensi Telematika diproyeksikan sebagai payung hukum utama yang merupakan legislasi negara kesatuan Republik Indonesia dalam melaksanakan reformasi kebijakan sektor komunikasi dan informatika. Undang-undang ini akan menggantikan UU Nomor 36 Tahun 1999 tentang Telekomunikasi, dan mengakomodasi hal-hal yang belum diatur terkait dengan konvergensi dalam UU Nomor 32 Tahun 2002 tentang Penyiaran dan UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, beserta semua aturan perundangan di bawahnya. (Sugeng 2020, 15). Dalam Rencana Strategis Kementerian Komunikasi dan Informatika Tahun 2015-2019, pembangunan bidang komunikasi dan informatika lima tahun ke depan diprioritaskan pada upaya mendukung pencapaian kedaulatan pangan, kecukupan energi, pengelolaan sumber daya maritim dan kelautan, pembangunan infrastruktur, percepatan pembangunan daerah perbatasan, dan peningkatan sektor pariwisata dan industri, berlandaskan keunggulan sumber daya manusia dan kemampuan ilmu pengetahuan dan teknologi.

Sebagai leading sector di bidang komunikasi dan informatika, Kementerian Komunikasi dan Informatika dalam Renstra tahun 2015-2019 akan berfokus membangun sektor telekomunikasi, tata kelola internet, dan digitalisasi siaran televisi. Adapun sasaran strategis pembangunan di bidang komunikasi dan informatika meliputi (Sugeng 2020):

1. Terwujudnya ketersediaan dan meningkatnya kualitas layanan komunikasi dan informatika untuk mendukung fokus pembangunan pemerintah sebagai wujud kehadiran negara dalam menyatakan kedaulatan dan pemerataan pembangunan.
2. Tersedianya akses broadband nasional, internet dan penyiaran digital yang merata dan terjangkau untuk meningkatkan pertumbuhan ekonomi, pendidikan, sosial, budaya, pertahanan, dan keamanan
3. Terselenggaranya tata kelola Komunikasi dan Informatika yang efisien, berdaya saing, dan aman.

Mengiringi perkembangan konvergensi telematika, maka yang dibutuhkan adalah regulasi yang berpijak pada suatu aturan yang memungkinkan hadirnya beberapa hal, sebagai berikut (Sugeng 2020):

1. Fleksibel dan tanggap terhadap perkembangan teknologi komunikasi yang cepat;
2. Memungkinkan persaingan yang sehat antara operator yang masih berpatron kepada pemerintah dan operator swasta murni;
3. Layanan yang mampu mendorong tumbuhnya produktivitas masyarakat dalam berkomunikasi untuk semua kepentingannya;
4. Kualitas jasa dan layanan yang dapat dipertanggungjawabkan, baik oleh operator maupun masyarakat kemudahan dan keluasaan akses;
5. Efektivitas dan efisiensi berkomunikasi; dan
6. Berbiaya murah dan terjangkau.

Kajian hukum dalam terhadap konvergensi telematika mencakup seluruh aspek ataupun bidang hukum yang terkait dengan perkembangan dan penerapan teknologi tersebut, antara lain (Edmon Makarim, 2005):

1. Aspek hak asasi manusia (HAM) terhadap informasi dan komunikasi;
2. Aspek perlindungan hukum terhadap privasi dan perlindungan data;
3. Aspek media;
4. Aspek komunikasi;
5. Aspek perikatan;
6. Aspek hak atas kekayaan intelektual (intellectual property)
7. Aspek perlindungan konsumen;
8. Aspek persaingan perusahaan;
9. Aspek pidana
10. Aspek perpajakan
11. Peran pemerintah dan Konvensi Hukum Internasional

Konvergensi telematika termasuk didalamnya terdapat Undang-Undang Informasi dan Transaksi Elektronik dalam perspektif cyber law ditujukan agar penggunaan akses informasi elektronik melalui pemakaian internet dapat memberikan kesejahteraan rakyat dan mencegah kejahatan. Upaya konvergensi harus juga dilakukan melalui pendekatan teori sistem hukum Lawrence Meir Friedman.

## 13.3 Teori Sistem Hukum

Sistem merupakan satu kesatuan yang terdiri dari unsur-unsur atau elemen yang saling berinteraksi satu sama lain, dalam sistem tidak menghendaki adanya konflik antar unsur-unsur yang ada dalam sistem, kalau sampai terjadi konflik maka akan segera diselesaikan oleh sistem tersebut (Teguh Prasetyo dan Abdul Halim Barkatullah: 2017). Sistem hukum adalah suatu kesatuan yang terdiri dari unsur-unsur yang mempunyai interaksi satu sama lain dan bekerja sama untuk mencapai tujuan kesatuan tersebut (Sudikno Mertokusumo: 2002).

Menurut Raz, berbicara mengenai teori sistem hukum setidaknya membahas empat masalah dasar yaitu:

1. Keberadaan (existence). Apa kriteria untuk keberadaan sistem hukum?
2. Identitas (identity) dan keanggotaan (membership). Apa kriteria yang menentukan sistem yang dimiliki oleh hukum tertentu? Hukum mana yang membentuk sistem tersebut?
3. Struktur (structure). Apakah ada struktur yang umum untuk semua sistem hukum?
4. Konten (content). Apakah ada undang-undang yang berulang di semua sistem hukum? Apakah ada konten yang umum di semua sistem hukum? (Joseph Raz: 2003).

Menurut Friedman sebagaimana dikutip oleh Teguh Prasetyo, ada tiga elemen dari sistem hukum, yaitu struktur (structure), substansi (substance), budaya hukum (legal culture) (Teguh Prasetyo dan Abdul Halim Barkatullah: 2017). Dalam bukunya yang berjudul *The Legal System: A Social Science Perspective*, Friedmann menyatakan bahwa suatu sistem hukum dalam operasi aktualnya merupakan sebuah organisme kompleks di mana struktur (structure), substansi (substance), dan kultur (culture) berinteraksi untuk menjelaskan latar belakang dan efek dari setiap bagiannya diperlukan peranan dari banyak elemen sistem tersebut. (Lawrence M. Friedman: 2011).



Friedman lebih lanjut menjabarkan ketiga elemen sistem hukum tersebut sebagai berikut (Achmad Ali: 2012):

1. Komponen struktur hukum (legal structure), yaitu kelembagaan yang diciptakan oleh sistem hukum dengan berbagai macam fungsi dalam rangka mendukung bekerjanya sistem tersebut. Komponen ini dimungkinkan untuk melihat bagaimana sistem hukum memberikan pelayanan terhadap penggarapan bahan-bahan hukum secara teratur.
2. Komponen substantif hukum (legal substance), sebagai output dari sistem hukum, berupa peraturan-peraturan, keputusan-keputusan yang digunakan, baik oleh pihak yang mengatur maupun yang diatur.
3. Komponen kultur hukum (legal culture), terdiri dari nilai-nilai dan sikap-sikap yang memengaruhi bekerjanya hukum atau oleh Lawrence M. Friedman disebut kultur hukum. Kultur (budaya) hukum inilah yang berfungsi sebagai jembatan yang menghubungkan antara peraturan hukum dengan tingkah laku hukum seluruh warga masyarakat. Kultur hukum dibedakan antara internal legal culture yakni kultur hukumnya lawyers, judges dan external legal culture yakni kultur hukum masyarakat pada umumnya.

Pengembangan sistem hukum berarti membangun elemen-elemen dari sistem hukum itu sendiri. Pengembangan sistem hukum pada akhirnya bertujuan untuk mencapai tujuan hukum itu sendiri sebagaimana dikemukakan oleh Gustav Radbruch yaitu terdapat tiga aspek tujuan hukum: keadilan, kemanfaatan, dan kepastian hukum. (Brian H. Bix, 2011).

## 13.4 Contoh Kasus Cyber Law di Indonesia

Apabila ada pertanyaan apakah Indonesia pernah sudah ada kasus Cyber Law. Jawabannya dapat langsung dijawab ya sudah. (Sardjana Orba Manullang, 2020) Ada salah satu contoh kasus dalam kejahatan cyber adalah kasus yang dialami oleh Wakil Ketua MPR periode 2009-2014 yaitu Lukman Hakim Saifuddin, e-mail Lukman Hakim Saifuddin dibajak oleh seseorang untuk

mendapatkan kepentingan dengan sejumlah uang dengan mengirimkan surat kepada kontak-kontak yang ada di e-mail milik beliau. Bila kita menagacu ke UU ITE, Lukman Hakim Saifuddin memiliki hak sebagaimana diatur dalam Pasal 26 ayat (2) Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU ITE”) yang berisikan “setiap orang yang melanggar haknya sebagaimana yang di maksud pada ayat (1) dapat mengajukan gugatan atas kerugian yang ditimbulkan berdasarkan Undang-Undang ini.”

Dengan kata lain ada hak yang telah disebutkan di atas, dengan hak tersebut Lukman Hakim Saifuddin sebenarnya berhak untuk mengajukan gugatan yang didasarkan kepada Pasal 28 ayat (1) UU ITE yang berbunyi, “setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik”, hal tersebut merupakan perbuatan yang dilarang. Dalam kasus ini, sang pelaku dapat dikenakan pidana sesuai ketentuan Pasal 45A UU ITE yang berbunyi, “Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).”

Di dalam kasus yang menimpa Lukman Hakim Saifuddin tersebut, pelaku kejahatan dunia maya yang membajak e-mail beliau juga dapat diterapkan dengan pelanggaran Pasal 378 KUHP tentang penipuan yang berbunyi, “Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum dengan memakai nama palsu atau martabat (hoendangheid) palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, mengerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi utang maupun menghapus kan piutang, diancam karena penipuan, dengan pidana penjara paling lama 4 (empat) tahun.” Selain itu sudah ada beberapa kasus lagi yang berkaitan dengan Cyber Law. Salah satu kasus fenomenal yang berkaitan dengan Pidana (Cyber Law), adalah tuduhan Pidana melakukan “prostitusi online” kepada artis papan atas Indonesia dengan inisial VA, di Pengadilan Negeri Surabaya pada tahun pertengahan tahun 2019.

Kasus ini banyak menjadi sorotan, kata “prostitusi online” (lebih khusus adalah kata “online” menjadi bahan di seluruh media (baik cetak maupun

media online). Pada saat itu saksi ahli yang dilibatkan dalam kasus ini adalah Sardjana Orba Manullang dari Universitas Krisnadwipayana. Apa yang terjadi dalam kasus ini dengan jelas menunjuk adanya penggunaan Cyber Law di Indonesia. Jadi, terlihat dengan jelas telah terjadi kasus di dalam pengaturan mengenai Cyber Law di Indonesia”

## 13.5 Kesimpulan

### **Tujuan Cyber Law**

Dalam setiap masyarakat ada hukum yang mengaturnya, ini sudah menjadi diktum yang berlaku universal di mana pun (Sardjana Orba Manullang, 2019). Berarti diperlukan adanya hukum yang mengatur masyarakat dan rupa dari sistem hukum itu sendiri berbeda-beda. Cyber Law sangat dibutuhkan, kaitannya dengan upaya pencegahan tindak pidana, maupun penanganan tindak pidana. Cyber Law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme. Dengan kata lain, Cyberlaw diperlukan untuk menanggulangi kejahatan Cyber.

### **Alasan Cyber Law Penting Untuk Hukum Indonesia**

Cyber Law penting diberlakukan sebagai hukum di Indonesia. Hal tersebut disebabkan oleh perkembangan zaman. Menurut pihak yang pro terhadap Cyber Law, sudah saatnya Indonesia memiliki Cyber Law, mengingat hukum-hukum tradisional tidak mampu mengantisipasi perkembangan dunia maya yang pesat. Dalam pergaulan sehari-hari seringkali kita mendengar istilah kode etik, namun apakah kita mengerti tentang istilah kode etik tersebut? Kode Etik terdiri dari dua kata yaitu “kode” dan “etik”. Kode merupakan tanda-tanda atau simbol-simbol yang berupa kata-kata, tulisan atau benda yang disepakati untuk maksud-maksud tertentu. Sedangkan etik (atau etika) berasal dari kata ethos (bahasa Yunani) yang berarti karakter, watak kesusilaan atau adat. Sebagai suatu subjek, etika akan berkaitan dengan konsep yang dimiliki oleh individu ataupun kelompok untuk menilai apakah tindakan-tindakan yang telah dikerjakannya itu salah atau benar, buruk atau baik.

Kode etik merupakan suatu norma, nilai, tata cara dan aturan yang dibuat secara tertulis, di dalamnya berisi tentang hal-hal baik dan tidak baik yang harus ditaati oleh seorang profesional. Kode etik disusun untuk memberikan

batasan yang jelas agar seorang profesional dapat melakukan pekerjaan/jasa dengan baik dan sebagai pelindung bagi pemberi pekerjaan/jasa agar terhindar dari perbuatan yang tidak profesional. Karena itu maka dapat disimpulkan bahwa etika sangat dibutuhkan bagi para profesional khususnya di bidang IT agar selalu mengutamakan etika dalam melakukan tindakan-tindakan, apalagi terkait dengan jasa profesinya.



# Daftar Pustaka

‘BCC030 Vulnerability Stats Report (2020)\_WEB.pdf’ (no date). Available at: [https://cdn2.hubspot.net/hubfs/4118561/BCC030%20Vulnerability%20Stats%20Report%20\(2020\)\\_WEB.pdf](https://cdn2.hubspot.net/hubfs/4118561/BCC030%20Vulnerability%20Stats%20Report%20(2020)_WEB.pdf) (Accessed: 29 November 2020).

‘CCPART1V3.1R5.pdf’ (no date). Available at: <https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf> (Accessed: 30 November 2020).

A. Freier, P. K. (2015). The secure sockets layer (ssl) protocol version 3.0. RFC 6101

Abidin, A. M., Hardianti, F. dan Setiano, I. N. (2016) “Analisa Dan Implementasi Proses Kriptografi Encryption-Decryption Dengan Algoritma Advanced Encryption Standard ( Aes-128 ),” Jurnal Sarjana Teknik Informatika, Keamanan Komputer, hal. `1-20.

Abidin, D.Z. (2015).Kejahatan Dalam Teknologi Informasi dan Komunikasi,Jurnal Ilmiah Media Processor, Vol. 10, No.2, Hal:509-516

Achmad Ali. (2012), Mengungkap Teori Hukum (Legal Theory) dan Teori Peradilan (Judicial Prudence) Termasuk Interpretasi Undang-Undang (Legisprudence), Jakarta: Kencana.

Achyani, Y. E. dan S. Saumi. (2019). Penerapan metode waterfall pada sistem informasi manajemen buku perpustakaan berbasis web. Jurnal SAINTEKOM. 9(1):83.

Achyani1, Y. E. (2016). KEAMANAN jaringan dengan packet filtering firewall (studi kasus: pt. sukses berkat mandiri jakarta) siti. 입법학연구. 제13집 1호(May):31–48.

- Aditya, Y., Pratama, A. dan Nurlifa, A. (2010) “Studi pustaka untuk steganografi dengan beberapa metode,” in Seminar Nasional Aplikasi Teknologi Informasi (SNATI).
- Agazzi, A. E. (2020). Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them. ArXiv Preprint ArXiv:2006.00577.
- Al-Fedaghi, S., & Alnasser, H. (2020). Modeling network security: Case study of email system. ArXiv Preprint ArXiv:2003.13509.
- Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A novel security model for cooperative virtual networks in the IoT era. *International Journal of Parallel Programming*, 48(2), 280–295.
- Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10), 168.
- Albert, M. (2020). If These Emails Could Talk: The Pitfalls of Hastily Implementing a Teacher Mentoring Program. *Taboo: The Journal of Culture and Education*, 19(4), 3.
- Alharbi, F. S. (2020). Dealing with Data Breaches Amidst Changes In Technology. *International Journal of Computer Science and Security (IJCSS)*, 14(3), 108.
- Andi (2018) 10 Tips Cara Meningkatkan Keamanan Komputer.
- Andriasan Sudarso et.al., (2020), *Konsep E-Bisnis*, Medan: Kita Menulis.
- Anthon F. Susanto. (2007), *Hukum Dari Consilience Menuju Paradigma Hukum Konsruktif-Transgresif*, Jakarta: Refika Aditama.
- Arif Awangga. (2020), *Teknik Perancangan Perundang-Undangan*, Bandung: Cendekia Press.
- Ariyus, D. (2006) “Kriptografi keamanan data dan komunikasi,” Graha Ilmu, Yogyakarta.
- Aryadita Umasugi, Ryana. (2018). “Selama 2018, Gempa Di Indonesia Meningkat 4.648 Kali Dibanding 2017.” 2018. <https://megapolitan.kompas.com/>.

- Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2019). "Latar Belakang". [https://apjii.or.id/pengurus/latar\\_belakang](https://apjii.or.id/pengurus/latar_belakang). (Diakses tanggal 22 Nopember 2020).
- Association for Computing Machinery (ACM). (2020). "ACM Code of Ethics Professional Conduct". <https://www.acm.org/diversity-inclusion/code-of-ethics>. (Diakses tanggal 23 Nopember 2020).
- Aswar, Alfin. (2020). "Keamanan Komputer Secar Fisk." 2020. <https://www.pediainfo.com/>.
- B. Arief Sidharta. (2008), *Meuwissen Tentang Pengembangan Hukum, Ilmu Hukum, Teori Hukum dan Filsafat Hukum*, Jakarta: Refika Aditama.
- Bambang Priyambodo dan Arif Awangga. (2020), *Politik Hukum Badan Peradilan Tata Usaha Negara*, Bekasi: CV Intelektual Writer.
- Banday, M. T. (2011). Effectiveness and Limitations of E-Mail Security Protocols. *International Journal of Distributed and Parallel Systems*, 2. <https://doi.org/10.5121/ijdps.2011.2304>
- Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, 1–16.
- BBPTIK (2014). Keamanan Informasi. <https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/>
- Bhaudhayana, G. W. dan Widiartha, I. M. (2015) "Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap," *Jurnal ilmu komputer Universitas Udayana*, 8(2), hal. 15–25.
- Blakley, G. (1979) "Safeguarding cryptographic keys," in *Proceedings of AFIPS*, hal. 313–317.
- Bourgeois, D. and Bourgeois, D. T. (2014) 'Chapter 6: Information Systems Security', in *Information Systems for Business and Beyond*. Published through the Open Textbook Challenge by the Saylor Academy. Available at: <https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/> (Accessed: 29 November 2020).
- Boussios, E. G. (2020). Hacking Back: Trump's "Madman Theory" Approach to Cybersecurity. *Journal of Applied Security Research*, 1–12.



- Brian H. Bix, (2011). "Radbruch's Formula and Conceptual Analysis", American Journal of Jurisprudence, Vol. 56,.
- Briggs, A.. (1961). 'The Welfare State in Historical Perspective', European Journal of Sociology, 2: 221-58. Broberg, G. and Roll-Hansen, N. (eds) Eugenics and The Welfare State: Sterilization Policy in Denmark, Sweden, Norway and Finland, 1996, East Lansing: Michigan State University Press, 1961.
- Bryan A. Garner. (2004) Black's Law Dictionary, Eighth Edition, St. Paul, Minnosota, USA: West Publishing Co.
- Budi Setiyono. (2018), Model dan Desain Negara Kesejahteraan, Bandung: Nuansa Cendekia.
- C.F.G., Sunaryati Hartono. (1991), Politik Hukum Menuju Satu Sistem Hukum Nasional, Bandung: Alumnii.
- Canavan, J.E., (2001). Fundamentals of Network Security. Artech House.
- Carl Joachim Friedrich. (1969), The Philosophy of Law, in Historical Perspective, Chicago, The University of Chicago Press,
- Carl Joachim Friedrich. (2010), Filsafat Hukum, Perspektif Historis, Terjemahan: Rausul Muttaqien, Bandung: Nusa Media.
- Choudhary, S. (2013). E-mail Security: Issues and Solutions. International Journal of Computer Information Systems, 7, 42–46.
- Ciesla, R. (2020). Common Attacks Against Cryptographic Systems. In Encryption for Organizations and Individuals (pp. 75–101). Springer.
- Cutlip, S.M., M.A. Center dan G.M. Bloom. (2000). Effective Public Relation. 8 Edition. Penerbit Prentice Hall. Englewood Cliffs. New Jersey.
- Dahlan M., Latubessy A., N. M. (2015). Analisa keamanan web server terhadap serangan possibility sql injection. Prosiding SNATIF
- Danrivanto Budhijanto. (2014). Teori Hukum Konvergensi, Bandung: PT Refika Aditama.
- Darji Darmodihardjo. (2008), Pokok-pokok Filsafat Hukum, Jakarta: Gramedia Pustaka Utama.
- Deddy Wahyudin Purba, et.al., (2020), Pengantar Ilmu Pertanian, Medan: Kita Menulis.

- Deviana, H. (2011). Penerapan xml web service pada sistem distribusi barang. *Jurnal Generic*
- Dista Amalia Arifah. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi (JBE)*, 185-195
- E. Gunadhi dan A. P. Nugraha. (2017). Penerapan kriptografi base64 untuk keamanan url (uniform resource locator) website dari serangan sql injection. *Jurnal Algoritma*. 13(2):391–398.
- Eboibi, F. E. (2020). Cybercriminals and Coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: cyber hygiene and preventive enforcement measures. *Commonwealth Law Bulletin*, 1–30.
- Ertie Nur Hartiwati. (2014). Keamanan Jaringan Dan Keamanan Sistem Komputer Yang Mempengaruhi Kualitas Pelayanan Warnet. *Jurnal Ilmiah Informatika Komputer Universitas Gunadarma*, 27–33.
- Everipedia. (2017). SEARCC. [https://everipedia.org/wiki/lang\\_en/SEARCC](https://everipedia.org/wiki/lang_en/SEARCC) (Diakses tanggal 24 Nopember 2020).
- Febriani, R. dan Suci, A. (2015). Buku Ajar Etika Profesi Teknologi Informasi. [https://www.academia.edu/27022002/Buku\\_Ajar\\_ETIKA\\_PROFESI\\_TEKNOLOGI\\_INFORMASI\\_2015](https://www.academia.edu/27022002/Buku_Ajar_ETIKA_PROFESI_TEKNOLOGI_INFORMASI_2015) (Diakses 15 Nopember 2020).
- Firmansyah, Yoki. (2019). Modul Etika Profesi Teknologi Informasi & Komunikasi. <https://repository.bsi.ac.id/index.php/unduh/item/237184/Modul-EPTIK-Oke.pdf> (Diakses 22 Nopember 2020)
- Fruhlinger, J. (2020a) The CIA triad: Definition, components and examples, CSO Online. Available at: <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html> (Accessed: 29 November 2020).
- Fruhlinger, J. (2020b) What is information security? Definition, principles, and jobs, CSO Online. Available at: <https://www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html> (Accessed: 29 November 2020).
- H.L.A. Hart, (1977), *The Concept of Law*, Clarendon Press, Oxford, New York

- H.L.A. Hart, (2011), *The Concept of Law*, Penerjemah M. Khozim, Konsep Hukum, Bandung: Nusa Media.
- Hadi, R. (2020) *Mengenal Perintah Dasar MS-DOS - Kepo*. Tersedia pada: <https://kepo.co/mengenal-perintah-dasar-ms-dos/> (Diakses: 30 November 2020).
- Han, S. (2012). *Web 2.0*. Web 2.0.
- Hanipah, R & Dhika, H. (2020), "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark," *Journal of Computer and Information Technology*. Vol. 4, No.1, hal. 11-23.
- Hans Kelsen. (2008), *Teori Umum Tentang Hukum dan Negara*, Bandung: Nusa Media.
- Harismawan, A. F., A. P. Kharisma, dan T. Afirianto. (2018). Analisis perbandingan performa web service menggunakan bahasa pemrograman python , php , dan perl pada client berbasis android. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer (J-PTIIK) Universitas Brawijaya*. 2(January):237–245.
- Harold J. Berman (1996), *Segi-segi Filosofis Hukum Amerika*, Dalam *Ceramah Tentang Hukum Amerika Serikat*, Jakarta: Tata Nusa.
- Harshit Agarwal dan Rashi Agarwal, (2017). "First Industrial Revolution and Second Industrial Revolution: Technological Differences and the Differences in Banking and Financing of the Firms", *Saudi Journal of Humanities and Social Sciences*, Vol. 2, No. 11A,.
- Hasibuan, M. S. (2016). *Keylogger pada Aspek Keamanan Komputer*. Teknovasi, 3(1), 8–15.
- Hermawan, R. (2016). *Analisa Cara Kerja dan Dampak dari Serangan Virus Spyware*. *STRING (Satuan Tulisan Riset Dan Inovasi Teknologi)*, 1(1). <https://doi.org/10.30998/string.v1i1.964>
- Hu, H. (2020). *Characterizing and Detecting Online Deception via Data-Driven Methods*. Virginia Tech.
- Ikatan Ahli Informatika Indonesia (IAII). (2014). "Pengantar". [https://www.iaii.or.id/index.php?model=iaii\\_content&action=showContent&lang=id&id=c9f0f895fb98ab9159f51fd0297e236d&type=0&skip=0&title=Pengantar](https://www.iaii.or.id/index.php?model=iaii_content&action=showContent&lang=id&id=c9f0f895fb98ab9159f51fd0297e236d&type=0&skip=0&title=Pengantar). (Diakses tanggal 22 Npember 2020).

- Information systems security (2005) TheFreeDictionary.com. Available at: <https://www.thefreedictionary.com/Information+systems+security> (Accessed: 29 November 2020).
- Italia (2019) “Pengertian Sistem Operasi, Fungsi, Macam-macam & Contoh Sistem Operasi yang Perlu Kamu Ketahu.”
- J. Schlechtendahl, (2015 ).“Making existing production systems Industry 4.0-ready”, Jurnal Production Engineering, Vol. 9, Issue.1.,
- Jardine, E. (2020). The Case against Commercial Antivirus Software: Risk Homeostasis and Information Problems in Cybersecurity. Risk Analysis, 40(8), 1571–1588.
- Jeremy Rifkin (2011), The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World, New York: St. Martin.
- Jimly Asshiddiqie (2005), Hukum Tata Negara dan Pilar-pilar Demokrasi, Jakarta: Konpress.
- Jimly Asshiddiqie dan Ali Safa’at. (2012), Hans Kelsen Tentang Hukum, Jakarta: Konsitusi Press (Konpress).
- Jimly Asshiddiqie, (2004 ). Cita Negara Hukum Indonesia Kontemporer, Papper. Disampaikan dalam Wisuda Sarjana Hukum Fakultas Hukum Universitas Sriwijaya Palembang, 23 Maret 2004 dalam Simbur Cahaya No. 25 Tahun IX Mei 2004 ISSN No. 14110-0614.
- Jimly Asshiddiqie, (2006), Teori Hans Kelsen Tentang Hukum, Jakarta : Sekjen dan Kepaniteraan MK-RI, 2006.
- Jimly Asshiddiqie, (2009) Komentar Atas Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Jakarta: Penerbit Sinar Grafika, 2009.
- John Gillesen dan Frits Gorle. (2005), Sejarah Hukum, Suatu Pengantar, Terjemahan, Disadur Oleh: Freddy Tengker, Jakarta: Refika Aditama.
- Joseph Raz. (2003), The Concept of a Legal System: An Introduction to the Theory of Legal System, Edisi Kedua, Oxford: Clarendon.
- Josi, A. (2017). Penerapan metode prototyping dalam membangun website desa (studi kasus desa sugihan kecamatan rambang). Jti

- Kamus Besar Bahasa Indonesia Kementerian Pendidikan dan Kebudayaan Republik Indonesia. (2016). <https://kbbi.kemdikbud.go.id/entri/etika> (Diakses 17 Nopember 2020).
- Kementerian Komunikasi dan Informatika Republik Indonesia. (2019). Asosiasi Pendidikan Tinggi Informatika dan Komputer (APTIKOM). <https://aptika.kominfo.go.id/2019/08/asosiasi-pendidikan-tinggi-informatika-dan-komputer-aptikom/> (Diakses 21 Nopember 2020).
- Killoran, J. P., Graham, B., & others. (2020). Email-based authentication for account login, account creation and security for passwordless transactions. Google Patents.
- Kizza, J.M., (2017). Guide to Computer Network Security, Computer Communications and Networks. Springer International Publishing, Cham. <https://doi.org/10.1007/978-3-319-55606-2>
- Kriptografi (2017) Kriptografi Klasik dan Modern - KRIPTOGRAFI INDONESIA. Tersedia pada: <http://www.kriptografi.science/2017/07/kriptografi-klasik-dan-modern.html> (Diakses: 1 Desember 2020).
- Kristianto, A. (2003). Perancangan Sistem Informasi.
- Kromodimoeljo, S. (2010) Teori dan Aplikasi Kriptografi. SPK IT Consulting. Tersedia pada: <http://www.buku-e.lipi.go.id/utama.cgi?lihatarsip&sent001&1254672494>.
- Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of COVID-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. ArXiv Preprint ArXiv:2006.11929.
- Lam, T., & Kettani, H. (2019). PhAttApp: A Phishing Attack Detection Application. Proceedings of the 2019 3rd International Conference on Information System and Data Mining, 154–158.
- Lawrence M. Friedman (2011), The Legal System: A Social Science Perspective, terjemahan M. Khozim, Bandung: Nusamedia.
- Lawrence M. Friedman, American Law an Introduction (2001), Second Edition, terjemahan: Wishnu Basuki, Hukum Amerika, Sebuah Pengantar, Jakarta: Tatanusa, 2001.

- Liao, H. J., C. H. Richard Lin, Y. C. Lin, dan K. Y. Tung. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*. 2013.
- Lili Rasjidi dan Ida Bagus Wyasa Putra (2012), *Hukum Sebagai Suatu Sistem*, Bandung: Fikahati Aneska.
- Lili Rasjidi dan Ira Tania Rasjidi. (2002), *Pengantar Filsafat Hukum*, Bandung, Mandar Maju.
- Lita Sari Marita, (2019), *Cyber Crime dan Penerapan Cyver Law dalam Pemberantasan Cyver Law di Indonesia*.
- Mahajan, V., & Goyal, R. (2020). Enforcing security policies on mobile devices in a hybrid architecture. *Google Patents*.
- Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 837–842.
- Manullang, Sardjana Orba, (2019), *Sosiologi Hukum*, Jakarta: Bidik Phronesis Publishing.
- Manullang, Sardjana Orba, (2020), *Aspek Legal dalam E-Business*, Bab 4 Konsep E-Bisnis, Medan: Kita Menulis.
- Manullang, Sardjana Orba, (2020), *Ciri-ciri Pelayanan Birokrasi yang Berkualitas*, Bab 9 Pelayanan Birokrasi, Medan: Kita Menulis.
- Manullang, Sardjana Orba, (2020), *Hak Pemuliaan Varietas Tanaman/PVT*, Bab 14 Pengantar Ilmu Pertanian, Medan: Kita Menulis.
- Manullang, Sastrawan, (2018), *Teori dan Teknik: Analisis Stakeholder*, Bogor: IPB Press.
- Marion, N. E., & Twede, J. (2020). *Cybercrime: An Encyclopedia of Digital Crime*. ABC-CLIO.
- Mochtar Kusumaatmadja (2002), *Konsep-konsep Hukum Dalam Pembangunan*, Bandung: Alumni.
- Mochtar Kusumaatmadja (2006), *Hukum, Masyarakat, dan Pembangunan*, Bandung: Binacipta.
- Moh. Kusnadi dan Bintan R. Saragih. (2017), *Ilmu Negara*, Jakarta: Gaya Media Pratama.

- Mollin, R. A. (2007) *An Introduction to Cryptography*.
- Muhadjir Effendy. (2016), *Kamus Besar Bahasa Indonesia (KBBI)*, edisi kelima, Jakarta: Badan Pengembangan dan Pembinaan Bahasa Kemdikbud, 2016.
- Muhammad Fitri Rahmadana et.al., (2020), *Pelayanan Publik*, Medan: Kita Menulis.
- Mukhtar, Harun. (2018). *Kriptografi untuk Keamanan Data*. Deepublish,.
- Munir, R. (2006) "Sekilas image watermarking untuk memproteksi citra digital dan aplikasinya pada citra medis," in *International Conference on Telecommunication*.
- Murti, H. (2005), "Cybercrime," *Jurnal Teknologi Informasi DINAMIK* " , Vol. X, No.1, hal. 37-40.
- Nariza, Rinta. "Arti & Pengertian Etika (KBBI) dengan Sinonim / Antonim / Kata Turunan". <https://www.poskata.com/arti/etika/> (Diakses 21 Nopember 2020).
- Nazwita, S. R. (2017). Analisis Sistem Keamanan Web Server dan Database Server Menggunakan Suricata. *Seminar Nasional Teknologi Informasi Komunikasi dan Industri*. 0(0). 2017. 2579–5406.
- Nghi Phu, T., Dai Tho, N., Le Hoang, H., Ngoc Toan, N., & Ngoc Binh, N. (2020). An Efficient Algorithm to Extract Control Flow-Based Features for IoT Malware Detection. *The Computer Journal*.
- OWASP. 2014. *Cross-site Scripting (XSS) - OWASP*
- Pabokory, F. N., Astuti, I. F. dan Kridalaksana, A. H. (2016) "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 10(1), hal. 20–31.
- Pagi, S. (2020) *Pengertian Sistem Operasi*.
- Pamungkas, A. (2020) *Steganografi Citra Digital I Pemrograman Matlab*. Tersedia pada: <https://pemrogramanmatlab.com/2019/01/02/steganografi-citra-digital/> (Diakses: 1 Desember 2020).

- Panda, B. K., M. Pradhan, dan S. K. Pradhan. (2016). Intrusion prevention system. Dalam *Network Security Attacks and Countermeasures*
- Perkumpulan Profesional Teknologi Informasi (PPTI). (2018). <https://profesional-ti.id/> (Diakses 22 Nopember 2020).
- Phyllis Deane. (1979), *The First Industrial Revolution*, Second Edition, Cambridge: Cambridge University Press.
- Pratiwi, Atmojo D. WP (2016) "Peningkatan Keamanan Data Dengan Metode Cropping Selection Pseudorandom," *Jurnal TICOM*, 13(4), Vol. 4, No.3, hal. 132-138.
- Putri Harliana, D. (2008). Sniffing dan Spoofing Pada Aspek Keamanan Komputer. *Jurnal-Keamanan-Komputer*, 1–5.
- Qashqari, A., Alhbshi, D., Alzahrani, F., Ghwati, H., & Aljahdali, A. (2020). Electronic Mail Security. *International Journal of Computer Science and Information Security (IJCSIS)*, 18(5).
- Rabeh Morrar et.al, (2017 ). "The Fourth Industrial Revolution (Industry 4.0): A Social Innovation Perspective", *Technology Innovation Management Review*, Vol. 7, No. 11,.
- Rahardjo, B. (2005) 'Keamanan Sistem Informasi Berbasis Internet', p. 170.
- Rahardjo, Budi. (2005). "Keamanan sistem informasi berbasis internet." Jakarta: PT INDOCISC
- Rahayu, Sri. (2016). "Macam-Macam Perangkat Keras Pada Komputer." 2016. <http://blog.unnes.ac.id/>.
- Ridwan Lubis, Muhammad; d(kk. 2020). *Pengenalan Teknologi Informasi*. Sumatera Utara: Kita Menulis.
- Rinaldi, M. (2006) *Kriptografi*. Bandung: Informatika. Tersedia pada: [https://scholar.google.com/scholar?hl=th&as\\_sdt=0,5&cluster=16551445928354209324](https://scholar.google.com/scholar?hl=th&as_sdt=0,5&cluster=16551445928354209324).
- Robinson, M., K. Jones, dan H. Janicke. (2015). Cyber warfare: issues and challenges. *Computers and Security*. 49:70–94.
- Rosady, Ruslan. (2011). *Etika Kehumasan – Konsep & Aplikasi*. Penerbit Rajawali Press. Jakarta.



- Rumondang, M. (2002) "Perlindungan Hak Cipta Pada Data Audio Menggunakan Teknik Watermarking Phase Coding," Departemen Teknik Informatika Institut Teknologi Bandung Jalan Ganesha, 10.
- Rusmana, D. (2018) "Apa itu Sistem Operasi."
- Sahtyawan, R. (2019). Penerapan zero entry hacking didalam security misconfiguration pada vapt (vulnerability assessment and penetration testing). *Journal of Information System Management*
- Saputra<sup>1</sup>, D. dan R. F. Aji. (2018). ANALISIS perbandingan performa web service rest menggunakan framework laravel, django dan ruby on rails untuk akses data dengan aplikasi mobile (studi kasus: portal e-kampus stt indonesia tanjungpinang). *Jurnal Ilmiah Bangkit Indonesia*. 2(Vii):6.
- Saragih, Megasari Gusandra & Sardjana Orba Manullang, 2020, *Marketing Era Digital*, Medan: Penerbit Andalan.
- Satjipto Rahardjo (2009), *Hukum dan Perubahan Sosial, Suatu Tinjauan Teoretis Serta Pengalaman-Pengalaman di Indonesia*, Yogyakarta, Genta Publishing.
- Schneier, B. (1996) *Applied Cryptography Second Edition: Protocol, Algorithm and Souce Code in C*.
- Schultz, T. (2000). Mass media and the concept of interactivity: an exploratory study of online forums and reader email. *Media, Culture & Society*, 22(2), 205–221.
- Shidarta (2012), Mochtar Kusuma-Atmadja dan *Teori Hukum Pembangunan: Eksistensi dan Implikasi*, Jakarta: Epistema Institute.
- Shidarta. (2006), *Karakteristik Penalaran Hukum Dalam Konteks Ke-Indonesiaan*, Jakarta: CV Utomo
- Siddik, M. A. B., & Rahi, S. T. (2020). Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context. *BiLDBANGLADESH*, 68.
- Sidik, B. (2014). *Pemrograman web dengan php: edisi revisi kedua*. Pemrograman
- Simarmata, J. (2006) *Pengamanan Sistem Komputer*, Andi, Yogyakarta. Yogyakarta: Penerbit Andi.

- Simarmata, J., Sriadhi, S. dan Rahim, R. (2020) Kriptografi: Teknik Keamanan Data Dan Informasi. Jogjakarta: Andi Publisher.
- Situmorang, H., (2016). Keamanan Basis Data Dengan Teknik Enkripsi, *Jurnal Mahajana Inforamasi* Vol. 1, No.1, Hal:22-27
- Soerjono Soekanto (1986), Pengantar Penelitian Hukum, Cetakan ke-3, Jakarta: UI Press.
- Soerjono Soekanto dan Sri Mamudji (2006), Penelitian Hukum Normatif, Suatu Tinjauan Singkat, Jakarta: PT. Raja Grafindo Persada.
- Soewito, B. (2019) KEAMANAN KOMPUTER.
- Solichin, A. (2010) “Digital Watermarking untuk Melindungi Informasi Multimedia,” *Budi Luhur Information Technology (BIT)*, hal. 1–8.
- South East Asia Regional Computer Confideration (SEARCC). (2020). <https://searcc.org/> (Diakses tanggal 21 Nopember 2020)
- Stalling, W. (2005) *Cryptography and Network Securty Principles and Pratices* Fourth Edition. Prentice Hall.
- Stallings, W. (1995) *Network and internetwork security: principles and practice*. USA: Prentice-Hall, Inc.
- Stallings, W. and Bauer, M. (2012) *Computer Security Principles And Practice* (Second Edition). New York: Pearson. doi: 10.1016/0142-0496(87)90093-2.
- Sun, C. C., A. Hahn, dan C. C. Liu. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power and Energy Systems*. 2018.
- Sunaryati Hartono, Pembahasan Kertas Kerja (1981), Pemindahan Teknologi dan Pengaturannya dalam Peraturan Perundangan, Seminar Aspek-Aspek Hukum Pengalihan Teknologi, Bandung: BPFIN-Bina Cipta.
- Supangkat, S. H. dan Kuspriyanto, J. (2000) “Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital,” ITB, Bandung.
- Surian, D. (2006) “Algoritma Kriptografi AES Rijndael,” *TESLA Jurnal Teknik Elektro UNTAR*, 8(2), hal. 97–101.
- Susanto, A. dan Tritanto, R. (2011) “Kombinasi Algoritma RSA dan Algoritma Cipher Transposisi Untuk Keamanan Database,” *Jurnal Dian* Vol, 11(3).

- Suteki. (2013), Hukum dan Alih Teknologi, Yogyakarta: Thafa Media.
- Suwito, Benfano. (2019). "Keamanan Komputer." 2019. <https://mti.binus.ac.id/>.
- Syafrizal, Melwin. (2007). "ISO 17799: Standar Sistem Manajemen Keamanan Informasi." Seminar Nasional Teknologi. Vol. 10..
- Teguh Prasetyo dan Abdul Halim Barkatullah. (2017), Filsafat, Teori, dan Ilmu Hukum: Pemikiran Menuju Masyarakat yang Berkeadilan dan Bermartabat, Edisi 1, Cetakan 5, Depok: Rajawali Press.
- Triawan, A. dan M. A. Prasetyo. (2019). Penerapan web service (xml dan json) untuk meningkatkan performance pada informasi pembayaran uang kuliah. Teknois : Jurnal Ilmiah Teknologi Informasi dan Sains
- Undang-Undang Dasar Negara Republik Indonesia Tahun 1945
- Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik jo. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan jo. Undang-Undang Nomor 15 Tahun 2019 tentang Perubahan Atas Undang-Undang No. 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan.
- Upadhyay, R.K., Singh, P., (2020). Modeling and control of computer virus attack on a targeted network. Phys. Stat. Mech. Its Appl. 538, 122617. <https://doi.org/10.1016/j.physa.2019.122617>
- Wahid, A. A. (2019) "Analisis Sistem Keamanan Pada Sistem Operasi Microsoft Windows, Linux Dan Macintosh," Jurnal Teknik Informatika, 1(3).
- Wahyono, Teguh. (2006). Etika Komputer dan Tanggung Jawab Profesional di bidang Teknologi Informasi. Penerbit Andi. Yogyakarta.
- Whitman, M., Mattord, H. and Green, A. (2014) Principles of Incident Response and Disaster Recovery, 2nd Edition.
- Widodo, S., J. Teknik, K. Politeknik, dan N. Sriwijaya. (2012). Sistem keamanan transaksi data dengan menerapkan xml. Jurnal Fakultas Hukum UII. 2012(Snati):15–16.

- Wikipedia. (2020). "Association for Computing Machinery".  
[https://id.wikipedia.org/wiki/Association\\_for\\_Computing\\_Machinery](https://id.wikipedia.org/wiki/Association_for_Computing_Machinery)  
(Diakses tanggal 21 Nopember 2020)
- Wikipedia. (2020). "Institute of Electrical and Electronics Engineers".  
[https://id.wikipedia.org/wiki/Institute\\_of\\_Electrical\\_and\\_Electronics\\_Engineers](https://id.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers)  
(Diakses tanggal 21 Nopember 2020)
- William Stallings, 1(995). "Network and Internetwork Security," Prentice Hall
- Wirdasari, D. (2008). Mengenal Teknik-Teknik Keamanan Komputer Dan Model- Model Serangannya ( Security Attack Models ). Security Attack Models, 4(1), 111–119.
- Xiao, D., & Jiang, M. (2020). Malicious Mail Filtering and Tracing System Based on KNN and Improved LSTM Algorithm. 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCCom/CyberSciTech), 222–229.
- Yeni Yanti,D.(2017).Implementasi Sistem Keamanan Database Menggunakan Metode Triangle Chain. Serambi Engineering, 172-175
- Yusuf, K. (2004) Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika.
- Zabar, A. A. dan F. Novianto. (2015). Keamanan http dan https berbasis web menggunakan sistem operasi kali linux. Komputa: Jurnal Ilmiah Komputer dan Informatika. 4(2):69–74.
- Ziegler, M. dan M. Ziegler. (2014). Cross-Site-Scripting (XSS). Dalam Web Hacking



# Biodata Penulis



**Ika Yusnita Sari, S.Kom., M.Kom.** Lulusan S-1 dari Sekolah Tinggi Manajemen Informatika dan Komputer Royal Kisaran pada tahun 2015. Selanjutnya melanjutkan kuliah S-2 pada April 2018 di Universitas Putra Indonesia (UPI) YPTK Padang Dan Lulus pada Oktober 2019. Pengalaman bekerja, Saya pernah bekerja menjadi Dosen tidak Tetap di STMIK Royal Kisaran. Dan Sekarang bekerja di Universitas Imelda Medan sebagai Dosen Tetap.

Buku ini merupakan buku pertama saya mengenai pengetahuan saya tentang “Keamanan Data dan Informasi”. Semoga ini menjadi pintu pembuka saya dalam menulis buku-buku selanjutnya dan bermanfaat untuk orang lain dalam mencari ilmu tentang komputer.



**Muttaqin, S.T., M.Cs.** Lahir dan besar di Aceh. Pendidikan TK hingga SMA diselesaikan di Kabupaten Aceh Utara dan Kabupaten Bireun Provinsi Aceh. Menyelesaikan Pendidikan D3 Instrumentasi & Komputasi di Universitas Syiah Kuala, S1 Teknik Informatika Sekolah Tinggi Teknik Bina Cendikian Banda Aceh, dan S2 Ilmu Komputer Universitas Gadjah Mada. Mengajar mata kuliah Sistem Operasi Komputer, Kecerdasan Buatan, Sistem Informasi Geografis, Pemodelan Sistem Informasi, Teknik Digital, Pemrograman C++, Sistem

Basis Data, E-Commerce. Sukses menerbitkan buku kolaborasi sebanyak 6 buku dengan judul: Biometrika Teknologi Identifikasi, E-Commerce: Implementasi, strategi & Inovasinya, Panduan Belajar Manajemen Referensi dengan Mendeley, MOOC: Platform Pembelajaran Daring di Abad 21, Sistem Pendukung Keputusan: Metode & Implementasi, Sistem Informasi Manajemen. Semuanya diterbitkan oleh Penerbit Kita Menulis. Email penulis [muttaqin.ugm@gmail.com](mailto:muttaqin.ugm@gmail.com), Hp. +6285260409204, WA. +62895600515418



**Jamaludin, M.Kom**, seorang praktisi dan akademisi yang lahir di Bah Jambi, 11 Januari 1973 memiliki latar belakang sarjana teknik informatika dari Sekolah Tinggi Poliprofesi Medan dan magister komputer dari Universitas Sumatera Utara dengan peminatan komputer. Saat ini bertugas sebagai dosen di Politeknik Ganesha Medan sejak tahun 2013 sampai sekarang. Aktif dalam penelitian dan pengabdian kepada masyarakat untuk merealisasikan kerja dosen dalam Tri Dharma Perguruan Tinggi. Mulai aktif menulis buku sejak September 2019 sampai sekarang. Kemudian aktif juga menulis artikel di media cetak/online mulai sejak September 2020 sampai sekarang. Tema yang digemari dalam penulisan buku adalah komputer, bisnis online dan pendidikan.



**Dr. Janner Simarmata, S.T., M.Kom.** Sarjana Teknik Informatika dari STMIK Bandung, Magister Ilmu Komputer dari Universitas Gadjah Mada (UGM) dan Doktor Pendidikan Teknologi Kejuruan (PTK) diperoleh dari Universitas Pendidikan Indonesia (UPI) Bandung bidang kajian Blended Learning.

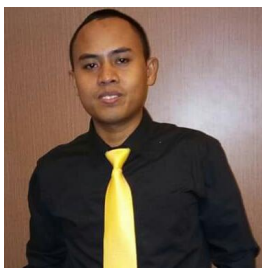
Menulis buku sejak tahun 2005. Dosen di Pendidikan Teknologi Informatika dan Komputer (PTIK) Fakultas Teknik Universitas Negeri Medan. Informasi lengkap dapat dilihat di web pribadi

[www.jannersimarmata.com](http://www.jannersimarmata.com) | surel: [jannersimarmata@junimed.ac.id](mailto:jannersimarmata@junimed.ac.id).



**M. Arif Rahman**, anak pertama dari 5 bersaudara, anak dari bapak seorang wiraswasta dan ibu seorang guru SD. Saya dibesarkan dikota kecil di sumatera barat yaitu Bukittinggi, kota yang mempunyai hawa dingin sekitaran gunung marapi. Dimana Agama, budaya dan makanan menjadi satu falsafah hidup masyarakat disana. Saya dari dahulu bercita- cita ingin mencerdaskan kehidupan bangsa, sehingganya sekarang terpanggil menjadi Dosen/ pengajar

dikampus swasta dan negeri di kota padang & medan. Sudah lebih 5 tahun saya menjalani karir sebagai dosen. Dan berharap teman-teman se profesi bisa tidak menyerah dengan keadaan. Suatu kebanggaan bisa menulis dan dibaca oleh orang lain, sungguh hal ini sangat berkesan bagi saya. Ini merupakan buku kedua penulis yang dikarang bersama- sama.



**Akbar Iskandar** dilahirkan di Jepuru pada tanggal 21 bulan Juli tahun 1986, jepuru terletak di desa Padang Kec. Gantarang kabupaten bulukumba, beralamat tinggal di Jalan Lembo dengan Nomor 175 Kota Makassar, pekerjaan nya sehari-hari menjadi salah satu dosen di STMIK AKBA – Makassar, riwayat pendidikan berawal di SD Negeri Nomor 232 Dampang (Bulukumba), melanjutkan ke SMP Negeri

Nomor 5 Gangking (Bulukumba), dan selanjutnya ke Sekolah Menengah Kejuruan di SMK Negeri 1 Bulukumba, beranjak remaja maka ia lanjutkan Pendidikan Tinggi pada Tahap Strata 1 (S1) di Jurusan Pendidikan Teknik Elektronika Universitas Negeri Makassar, dan Strata 2 (S2) diselesaikan di Jurusan Penelitian dan Evaluasi Pendidikan Universitas Negeri Makassar. Kemudian Ia kembali melanjutkan pendidikan S2 yang kedua kalinya pada bidang Sistem Komputer di makassar. Selain itu, ia juga aktif diberbagai kegiatan ilmiah/penelitian, beberapa Artikel Ilmiah nya sudah terindeks di Scopus dan WOS, aktif menjadi Reviewer diberbagai Jurnal baik Nasional maupun Internasional.

Selain itu ia aktif dlm kegiatan Konferensi Nasional dan Tingkat internasional, berkolaborasi dengan berbagai peneliti baik Nasional maupun Internasional sudah menjadi gaya hidupnya dalam melaksanakan Penelitian, ia juga aktif dalam berbagai kegiatan Pengabdian pada Masyarakat.





**Andrew Fernando Pakpahan, M.T., Ph.D.**, menyelesaikan pendidikan Sarjana Ilmu Komputer dari Universitas Advent Indonesia (UNAI), Bandung. Kemudian dia menyelesaikan program Magister Informatika dari Institut Teknologi Bandung (ITB) di tahun 2011. Di tahun 2014 dia melanjutkan studi ke jenjang Doktor (S3) dengan beasiswa di Yuan Ze University, Taiwan. Pada tahun 2018 dia menyelesaikan pendidikan S3 dengan memperoleh gelar Doctor of Philophy in Computer Science. Beliau merupakan penulis aktif yang telah mempublikasikan tulisannya di jurnal bereputasi internasional. Selain itu beliau juga dipercaya menjadi reviewer di berbagai jurnal bereputasi nasional dan internasional. Bidang penelitian yang ditekuninya adalah Passive Optical Network, Software-defined Networking and Network Quality of Service. Pada saat ini beliau aktif sebagai dosen di Fakultas Teknologi Informasi Universitas Advent Indonesia (UNAI), Bandung.



**Abdul Karim**, Lahir Pasar Bilah, 02 Juli 1988, menempuh pendidikan Diploma Tiga (DIII) AMIK STIEKOM Sumatera Utara, Strata Satu (S1) Universitas Pembangunan Panca Budi Medan, Strata Dua (S2) Universitas Bina Nusantara Jakarta. Saat ini mengajar di Universitas Budidarma dan AMIK STIEKOM Sumatera Utara, Sekaligus Tenaga Ahli Dinas Komunikasi dan Informatika Kabupaten Labuhanbatu. Aktif dalam berbagai organisasi kemasyarakatan,



**Sugianto, S.T, M.Kom**, asal dari kota Medan dan lahir pada tanggal 12 Mei 1982. Menyelesaikan kuliah dan mendapat gelar Sarjana Teknik pada tahun 2008. Pernah bekerja sebagai programmer di Edugames selama hampir 4 tahun. Memiliki pengalaman sebagai konsultan IT dan pengembangan layanan sistem informasi di beberapa instansi pemerintah daerah. Kemudian pada tahun

2011 mengikuti Program Magister Teknik Informatika dan lulus pada tahun 2014 dari Universitas Sumatera Utara. Pada akhir tahun 2014 diangkat menjadi Dosen Sekolah Tinggi Teknik Harapan dan ditempatkan di program studi Sistem Informasi. Selain menjadi dosen, juga aktif sebagai praktisi bisnis online dan pembicara digital marketing nasional. Sejak 2018 sebagai fasilitator program Google Gapura Digital di Indonesia. Buku yang telah terbit hasil kolaborasi dengan para penulis antara lain adalah Teaching From Home: Dari Belajar Merdeka Menuju Merdeka Belajar (2020), Smart Entrepreneur: Peluang Bisnis Kreatif dan Inovatif di Era Digital (2020). E-mail : soegi1703@gmail.com



**Yo Ceng Giap, S.Kom., M.Kom., CPS.** Penulis telah menempuh pendidikan Strata Satu (S1) di STMIK Buddhi Jurusan Teknik Informatika lulus pada tahun 2003 dan menempuh pendidikan Magister (S2) di STMIK Eresha Jurusan Teknik Informatika lulus pada tahun 2009.

Sejak tahun 2004 hingga saat ini penulis bekerja sebagai Dosen Tetap Yayasan di Universitas Buddhi Dharma Tangerang Banten, pada program studi Teknik Informatika. Buku-buku yang sudah

dipublikasikan pada tahun 2020 antara lain:

1. Optimasi desain toko online.
2. Cloud Computing: Teori dan Implementasi.
3. Belajar dari COVID-19: Perspektif Teknologi dan Pertanian.
4. Pembelajaran E-Learning di masa pandemi COVID-19.
5. Bisnis online: strategi dan peluang usaha.
6. Pengenalan Teknologi Informasi.

Penulis mendapatkan penghargaan bidang karya tulis yaitu

1. Mendapatkan hibah penulisan buku ajar dari Ristekdikti dengan judul buku Routing and Switching pada tahun 2018.
2. Juara 1 lomba penulisan artikel tema Waisak pada tahun 2020.



**Hazriani** lahir di Desa Tamaona Kabupaten Gowa, Provinsi Sulawesi-Selatan pada tanggal 5 Mei 1978. Menyelesaikan Pendidikan S1 Sistem Komputer di STMIK Handayani pada tahun 2001, S2 Teknik Informatika di Universitas Hasanuddin pada tahun 2007, dan S3 bidang Advanced Information Technology di Kyushu Univeristy pada tahun 2018. Sejak tahun 2005 hingga saat ini yang bersangkutan berstatus sebagai dosen tetap LLDIKTI WIL. IX dipekerjakan pada STMIK Handayani.



**Devi Yendrianof, S.Kom., M.Si.**, lahir di Medan, 22 Maret 1972. Penulis memperoleh gelar Ahli Madya di Indonesia Amerika Institut (IAI) Bandung (1995), Sarjana Komputer di STMIK Bandung (1998), Magister Ilmu Manajemen di Universitas Sumatera Utara (2006).

Pada tahun 2002 penulis diterima sebagai Dosen Tetap di STMIK Kaputama Binjai dan Dosen Tidak Tetap di STIE IBBI Medan, Universitas Dharmawangsa Medan, dan AKPER & AKBID Pemkab. Langkat. Mata kuliah yang pernah diampu yaitu: Paket Program Niaga, Algoritma dan Pemrograman, Struktur Data, Sistem Informasi Manajemen, E-Bisnis, Analisa dan Perancangan Sistem Informasi, serta Etika Profesi dan HAKI. Penulis juga pernah memimpin Tim Pengembangan Sistem Informasi Akademik Online STMIK Kaputama (2010) dan Tim Pengembangan Perpustakaan Online STMIK Kaputama (2012).

Penulis yang memiliki hobi membaca dan traveling ini beberapa kali mendapat kesempatan mengikuti studi ekskursi dan pelatihan ke luar negeri antara lain: Studi Ekskursi ke NTU Singapore dan UTM Malaysia (2008) dan Training Conference PUM Educating the Next Generation di Belanda (2013).

Sejak tahun 2009 penulis diterima sebagai ASN di BPKAD Kab. Langkat dan tahun 2016 ditempatkan di Inspektorat Kab. Langkat dengan jabatan Auditor Muda. Prestasi yang pernah diraih: Dosen Terbaik STMIK Kaputama Binjai (2008), Terbaik I Diklat Keprotokolan Pemkab. Langkat (2009), Terbaik III

Diklat Prajabatan CPNS Formasi Tahun 2008 dan Tanda Kehormatan “Satyalancana Karya Satya X Tahun” dari Presiden RI (2019).

Buku ini merupakan Buku Kolaborasi Kelima yang telah diterbitkan oleh Yayasan Kita Menulis. Penulis dapat dihubungi melalui email: [dyendrianof972@gmail.com](mailto:dyendrianof972@gmail.com).



**Sardjana Orba Manullang**, Lektor di Fakultas Hukum Universitas Krisnadwipayana, juga sebagai Advokat dan Aktif di bidang Konservasi/Lingkungan. Selepas pendidikan dasar di bidang sosiologi dan hukum di Universitas Indonesia berkecimpung sebagai Advokat / konsultan hukum khususnya bidang Keperdataan dan bisnis, juga sebagai anggota Konsultan Hukum Pasar Modal (HKHPM). Pengetahuan bisnis/manajemen dipelajari ketika menjadi peserta Wijayata Manajemen di PPM. dan diperkaya sewaktu mengikuti Hukum Bisnis di

Universitas Padjadjaran dan pendidikan kenotariatan di Universitas Diponegoro.

Ketertarikan untuk mempelajari Cyber Law ternyata berbuah hasil dengan mendapat kesempatan untuk menjadi saksi ahli pada salah satu kasus fenomenal di Indonesia, yaitu kasus Pidana berkaitan erat dengan Cyber Law, lebih khusus lagi tuduhan melakukan Prostitusi online pada salah satu artis terkenal di Indonesia dengan inisial VA, di Pengadilan Negeri Surabaya pada tahun 2019, selain kasus itu, juga beberapa kali sudah menjadi saksi-ahli baik di Pengadilan maupun di luar Pengadilan untuk bidang ilmu yang dikuasainya. Kegiatan lain saat ini adalah sebagai praktisi HKI (Hak Kekayaan Intelektual) dan mendalami masalah hukum dan sosial khususnya yang berkaitan dengan hal kekinian termasuk tetapi tidak terbatas pada teknologi informasi dan media sosial. (untuk korespondensi dapat dihubungi di [somanullang@gmail.com](mailto:somanullang@gmail.com) )





Pembahasan pada buku ini tentang keamanan data dan informasi di mana perkembangan teknologi komputer saat ini sangat berkembang pesat, maka dibutuhkan suatu keamanan data dan informasi serta pengetahuan berbagai macam kejahatan-kejahatan yang terjadi, baik dari pemanfaatan komputer serta dari sisi penggunaanya.

Secara rinci buku ini membahas tentang :

Bab 1 Keamanan Komputer dan Kejahatan Komputer

Bab 2 Prinsip Dasar Keamanan Komputer

Bab 3 Cryptosystem dan Cryptography

Bab 4 Teknik Kriptografi

Bab 5 Keamanan Web

Bab 6 Keamanan Email

Bab 7 Keamanan Jaringan Komputer

Bab 8 Keamanan Sistem Operasi

Bab 9 Sistem Keamanan Informasi

Bab 10 Keamanan Komputer Secara Fisik

Bab 11 Evaluasi Keamanan Sistem Informasi

Bab 12 Kode Etik Profesi IT

Bab 13 Perspektif Cyber Law dan UU ITE Dalam Sistem Hukum Di Indonesia.

# KEAMANAN DATA & INFORMASI



YAYASAN KITA MENULIS  
press@kitamenulis.id  
www.kitamenulis.id

ISBN 978-623-6761-80-9



9 786236 761809