



KEAMANAN SIBER TANTANGAN DI ERA REVOLUSI INDUSTRI 4.0

Yose Indarta • Fadhly Ranuhardja • Ilham Firman Ashari
Jay Idoan Sihotang • Janner Simarmata • Harmayani
M Habib Algifari • Muhammad Takdir Muslihi • Jamaludin
A. Aviv Mahmudi • Aslam Fatkhudin • Zelvi Gustiana
Edy Subowo • Mohamad Idris



KEAMANAN SIBER
TANTANGAN DI ERA
REVOLUSI INDUSTRI
4.0

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 Siber

Tantangan di Era Revolusi Industri 4.0

Yose Indarta, Fadhly Ranuhardja, Ilham Firman Ashari
Jay Idoan Sihotang, Janner Simarmata, Harmayani
M Habib Algifari, Muhammad Takdir Muslihi, Jamaludin
A. Aviv Mahmudi, Aslam Fatkhudin, Zelvi Gustiana
Edy Subowo, Mohamad Idris



Penerbit Yayasan Kita Menulis

Keamanan Siber

Tantangan di Era Revolusi Industri 4.0

Copyright © Yayasan Kita Menulis, 2022

Penulis:

Yose Indarta, Fadhly Ranuhardja, Ilham Firman Ashari
Jay Idoan Sihotang, Janner Simarmata, Harmayani
M Habib Algifari, Muhammad Takdir Muslihi, Jamaludin
A. Aviv Mahmudi, Aslam Fatkhudin, Zelvi Gustiana
Edy Subowo, Mohamad Idris

Editor: Ronal Watrianthos

Desain Sampul: Devy Dian Pratama, S.Kom.

Penerbit

Yayasan Kita Menulis

Web: kitamenulis.id

e-mail: press@kitamenulis.id

WA: 0821-6453-7176

IKAPI: 044/SUT/2021

Yose Indarta., dkk.

Keamanan Siber: Tantangan di Era Revolusi Industri 4.0

Yayasan Kita Menulis, 2022

xiv; 196 hlm; 16 x 23 cm

ISBN: 978-623-342-595-7 (print)

E-ISBN: 978-623-342-596-4 (online)

Cetakan 1, Oktober 2022

- I. Keamanan Siber: Tantangan di Era Revolusi Industri 4.0
- 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

Atas berkat rahmat dan karunia Allah SWT, Tuhan yang Maha Pengasih dan Penyayang, buku hasil karya kolaborasi dari beberapa penulis yang berjudul “Keamanan Siber: Tantangan di Era Revolusi Industri 4.0” ini telah selesai disusun dan berhasil diterbitkan. Semoga memberikan sumbangsih keilmuan dan menambah wawasan bagi semua pihak terutama para akademisi, praktisi, dan pihak-pihak yang tertarik terutama dalam bidang keamanan siber.

Secara lengkap buku ini membahas:

- Bab 1 Keamanan Siber
- Bab 2 Hukum dan Regulasi Siber
- Bab 3 Ancaman Keamanan Siber
- Bab 4 Arsitektur Keamanan Siber
- Bab 5 Keamanan Jaringan
- Bab 6 Keamanan Aplikasi
- Bab 7 Keamanan Privasi
- Bab 8 Keamanan Web
- Bab 9 Keamanan Mobile
- Bab 10 Keamanan Sistem Informasi
- Bab 11 Keamanan Perangkat Keras
- Bab 12 Siber Terorisme
- Bab 13 Spionase Siber
- Bab 14 Pencegahan Kejahatan Siber

Terima kasih kami sampaikan kepada semua pihak yang telah mendukung dan turut andil dalam seluruh rangkaian proses penyusunan

dan penerbitan buku ini, sehingga buku ini bisa hadir dihadapan sidang pembaca.

Semoga kehadiran buku ini membawa manfaat yang sebesar-besarnya serta dapat memberikan kontribusi bagi pengembangan ilmu pengetahuan.

Tim Penulis

Daftar Isi

Kata Pengantar	v
Daftar Isi	vii
Daftar Gambar	xi
Daftar Tabel	xiii

Bab 1 Keamanan Siber

1.1 Pendahuluan	1
1.2 Konsep Keamanan Siber.....	4
1.3 Elemen dan Tantangan Keamanan Siber.....	6

Bab 2 Hukum dan Regulasi Siber

2.1 Pendahuluan.....	11
2.2 Hukum Siber Dalam Perspektif Internasional.....	13
2.3 Hukum dan Regulasi Siber Indonesia.....	19

Bab 3 Ancaman Keamanan Siber

3.1 Pendahuluan.....	25
3.2 Sirkulasi/ Infeksi	27

Bab 4 Arsitektur Keamanan Siber

4.1 Pendahuluan.....	41
4.2 Arsitektur Keamanan Informasi	44
4.3 Arsitektur Keamanan Siber.....	47
4.4 Framework Keamanan Siber	49

Bab 5 Keamanan Jaringan

5.1 Pendahuluan.....	53
5.2 Keamanan Jaringan Internet dan Firewall	55
5.2.1 Mengidentifikasi Kebutuhan Firewall	59
5.2.2 Membangun Firewall	60
5.3 Bentuk Ancaman Keamanan Komputer.....	62

Bab 6 Keamanan Aplikasi

6.1 Pendahuluan.....	65
6.2 Jenis Keamanan Aplikasi.....	66
6.3 Alat Buat Keamanan Software.....	68

Bab 7 Keamanan Privasi

7.1 Pendahuluan.....	73
7.2 Privasi Digital dan Risikonya	75
7.3 Keamanan Informasi Pengguna	76
7.3.1 Menyimpan Informasi Online	76
7.3.2 Username dan Password Pada Aplikasi.....	79
7.3.3 Mengunggah Informasi Secara Online	82
7.3.4 Langkah-Langkah Melindungi Informasi Yang Diunggah Secara Online.....	84
7.3.5 Permintaan Akses Aplikasi.....	86
7.3.6 Berinternet Menggunakan Mode Pribadi	88
7.4 Kebijakan Privasi Penyelenggara Sistem Elektronik.....	89
7.4.1 Bagaimana Penyelenggara Sistem Elektronik Menjaga Data Anda?	89
7.4.2 Alasan Penerapan Kebijakan Privasi	90
7.4.3 Kebijakan Privasi.....	92

Bab 8 Keamanan Web

8.1 Pendahuluan.....	95
8.2 Serangan Pada Web.....	98
8.3 Metodologi Serangan Web	100
8.4 Teknik Perlindungan Keamanan Web.....	103

Bab 9 Keamanan Mobile

9.1 Pendahuluan.....	107
9.2 Ancaman Pada Perangkat Mobile.....	108
9.3 Celah Keamanan Perangkat Mobile.....	111
9.4 Teknik Keamanan Perangkat Mobile	113
9.5 Mobile Device Management	116

Bab 10 Keamanan Sistem Informasi

10.1 Pendahuluan.....	119
10.2 Tujuan Keamanan Sistem Informasi	120
10.3 Bentuk Ancaman Keamanan Sistem Informasi	124

10.4 Pencegahan/Mitigasi Serangan Pada Sistem Informasi	126
10.5 Isu Keamanan Sistem Informasi	128
Bab 11 Keamanan Perangkat Keras	
11.1 Pendahuluan.....	133
11.2 Ancaman Utama Perangkat Keras Saat Ini	135
11.3 Best Practices Keamanan Hardware	138
Bab 12 Siber Terorisme	
12.1 Pendahuluan.....	143
12.2 Bentuk-Bentuk Komunikasi, Perencanaan, dan Penyerangan Siber Terorisme.....	145
Bab 13 Spionase Siber	
13.1 Pendahuluan.....	153
13.2 Proses Spionase Siber	157
13.2.1 Social Engineering.....	157
13.2.2 Espionage-As-A-Service.....	159
13.2.3 Peran Malware Dalam Spionase Dunia Maya	160
13.3 Pencegahan Spionase Siber	165
Bab 14 Pencegahan Kejahatan Siber	
14.1 Pendahuluan.....	171
14.2 Tantangan Pengembangan Kebijakan Keamanan Siber Di Indonesia..	172
14.3 Langkah Pencegahan Kejahatan Siber Dari Sisi Pengguna	174
14.4 Pencegahan Kejahatan Siber Dari Sisi Email.....	176
14.5 Perlindungan Situs Web Dari Kejahatan Siber	177
Daftar Pustaka	179
Biodata Penulis	189

Daftar Gambar

Gambar 1.1: Ukuran Pasar Keamanan Siber Di Seluruh Dunia Dalam US Dolar.....	2
Gambar 1.2: Triad CIA	4
Gambar 1.3: Elemen Keamanan Siber.....	6
Gambar 1.4: Contoh Disaster Recovery Plan Untuk IT Perusahaan	7
Gambar 2.1: Kerugian Finansial Karena Kejahatan Siber Tahun 2021 (US Dolar).....	12
Gambar 2.2: Negara Paling Berisiko Terhadap Serangan Siber	14
Gambar 2.3: Arsitektur Serangan Distributed Denial of Service (DDoS) ...	16
Gambar 2.4: Perbandingan Delik Terhadap Muatan Konten Pornografi Anak dan UU ITE	19
Gambar 3.1: Appender Infection	27
Gambar 3.2: Komputer Terinfeksi Dengan Rootkit.....	31
Gambar 3.3: Perangkat Keras Keylogger	31
Gambar 3.4: Pesan Ransomware.....	33
Gambar 3.5: Infeksi Ransomware Komputer.....	34
Gambar 3.6: E-Mail Phising	37
Gambar 3.7: Gambar Spam	39
Gambar 4.1: Tiga Serangkai Keamanan Informasi.....	42
Gambar 4.2: Manajemen Risiko Keamanan Informasi	43
Gambar 4.3: Hubungan Antar Arsitektur	45
Gambar 4.4: Kerangka Kerja EISA	50
Gambar 4.5: Alur Informasi dan Keputusan Dalam Organisasi	51
Gambar 5.1: Jaringan Komputer	54
Gambar 5.2: Ilustrasi Firewall	61
Gambar 6.1: Platform Monitoring OSINT dan WHOIS dan IP-Geolocation.....	68
Gambar 6.2: Google Dorks.....	69
Gambar 6.3: Maltego Tools Security Analyst.....	69
Gambar 6.4: FOCA Tools Security Analyst Dan Spybot Tools Security Analyst	70
Gambar 6.5: Qualys Tools Security Analyst.....	71

Gambar 6.6: Atera Tools Security Analyst dan Webroot Tools Security Analyst.....	71
Gambar 7.1: Jenis Data Pribadi Yang Umum Diambil Oleh Perusahaan.....	77
Gambar 7.2: Hasil Survei Privasi dan Keamanan Data	79
Gambar 7.3: Hasil Survei Kegunaan Aplikasi Duo	80
Gambar 7.4: Langkah-Langkah Proteksi Tweet (Twitter)	84
Gambar 7.5: Pengaturan Pemirsa Postingan (Facebook)	85
Gambar 7.6: Pengaturan Aktivitas (Facebook)	86
Gambar 7.7: Hak Akses Pada Android (Facebook).....	87
Gambar 7.8: Kebijakan Privasi (WhatsApp).....	92
Gambar 8.1: Bagan Aplikasi Web.....	97
Gambar 8.2: IDS/ IPS.....	103
Gambar 10.1: Confidentially, Integrity, dan Availability (CIA).....	120
Gambar 13.1: Proses Spionase Dunia Maya	163
Gambar 13.2: Cookies Meminta Ijin Akses Kepada Pengguna.....	166
Gambar 13.3: Kerentanan Sistem Terhadap Serangan Spionase Siber.....	167
Gambar 14.1: Perkembangan Jumlah Pengguna Internet dalam 10 (sepuluh) Tahun Terakhir di Indonesia.....	173
Gambar 14.2: Heat Map Global Cybersecurity Index Tahun 2017.....	174

Daftar Tabel

Tabel 2.1: Pokok-Pokok Perubahan UU ITE	21
Tabel 3.1: Tipe Ekstensi File Yang Dapat Di Infeksi	28
Tabel 3.2: Perbedaan Antara Virus, Worm, dan Trojan	30
Tabel 3.3: Efektivitas Social Engineering.....	36
Tabel 7.1: Kebijakan Privasi Penyelenggara Sistem Elektronik.....	93
Tabel 13.1: Contoh Kasus Spionase Siber.....	162
Tabel 14.1: Kerugian Akibat Kejahatan Siber di Indonesia dan Global	172

Bab 1

Keamanan Siber

1.1 Pendahuluan

Teknologi informasi dan komunikasi saat ini digunakan di banyak bidang kehidupan, termasuk sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintah, keamanan, dan pertahanan. Hal ini menjadikan keamanan siber telah mendapat perhatian utama bagi semua negara di dunia. Tingkat bahaya dan ancaman penyalahgunaan teknologi informasi dan komunikasi semakin meningkat dan menjadi lebih rumit karena berbanding lurus dengan tingginya tingkat penggunaan teknologi tersebut.

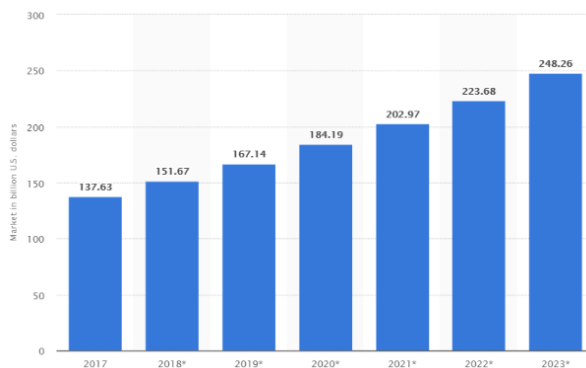
Saat ini sangat penting untuk memahami apa itu keamanan siber dan bagaimana menggunakannya di dunia yang tidak dapat ada tanpa teknologi dan koneksi jaringan. Tanpa perlindungan yang memadai, sistem, file, data, dan aset virtual penting lainnya mungkin bisa dalam keadaan bahaya. Dalam bisnis, baik perusahaan IT atau bukan, harus sama-sama dilindungi terhadap ancaman peretas.

Keamanan siber adalah proses mempertahankan diri dari serangan siber pada jaringan, perangkat lunak, dan data sensitif. Serangan ini dapat diklasifikasikan sebagai eksploitasi sumber daya, akses tidak sah ke sistem, seperti serangan *ransomware* untuk mengenkripsi data melakukan serangan perangkat untuk tujuan pemerasan (M, 2022).

Bahaya yang terkait dengan ancaman siber sangat tinggi. Keamanan siber sangat penting untuk semua organisasi, tidak hanya untuk organisasi komersial dan pemerintah. Namun, mereka yang memanfaatkan gadget digital seperti komputer, smartphone, tablet, dll juga harus menyadari hal ini. Banyak informasi pribadi yang ada di perangkat ini mungkin menarik bagi penjahat dunia maya.

Bisnis menghadapi ancaman sehari-hari dari kerentanan keamanan siber. Meskipun lanskap keamanan siber terus bergeser, terbukti bahwa ancaman siber semakin buruk dan lebih sering terjadi. Selama lima tahun ke depan, biaya yang terkait dengan kejahatan dunia maya diperkirakan akan meningkat sebesar 15% setiap tahun menurut analisis di Cybersecurity Ventures.

Dengan menganalisis dampak keuangan dari serangan siber sebelumnya dan lanskap ancaman potensial, perkiraan pengeluaran \$10.5 triliun ini termasuk biaya untuk penghancuran data, uang curian, dan pencurian kekayaan intelektual (Matt Ahlgreen, 2022).



Gambar 1.1: Ukuran Pasar Keamanan Siber Di Seluruh Dunia Dalam US Dolar (Jann Chambers, 2021)

Masalah keamanan siber sudah menjadi kejadian sehari-hari yang umum bagi banyak individu dan bisnis. Untuk memenangkan perang melawan ancaman keamanan siber, penting bagi orang-orang untuk memahami ancaman tersebut dan cara mencegahnya. Diperkirakan ukuran pasar keamanan siber di seluruh dunia akan mencapai \$223,68 miliar pada tahun 2022 seperti yang ditunjukkan pada gambar 1.1 (Jann Chambers, 2021).

Menurut studi oleh Cybersecurity Ventures, kerusakan *ransomware* dapat merugikan perusahaan \$ 265 miliar per tahun dan terjadi pada kecepatan satu

serangan setiap 10 detik untuk individu dan perusahaan. Klinik Universitas Düsseldorf di Jerman mengalami serangan *ransomware* pada September 2020, memaksa karyawan untuk mengalihkan pasien darurat ke lokasi lain. Karena seluruh jaringan TI rumah sakit lumpuh oleh serangan siber, dokter dan perawat tidak dapat berinteraksi satu sama lain atau mengakses catatan pasien (Matt Ahlgreen, 2022).

Menurut analisis yang lebih baru oleh *Australian Cyber Security Center* (ACSC), ada 59.806 laporan kejahatan dunia maya antara Juli 2019 dan Juni 2020 (kejahatan dilaporkan, bukan diretas), atau rata-rata 164 kejahatan dunia maya setiap tahun. Perusahaan kecil adalah target 43% dari serangan siber baru-baru ini, menurut Cybint Solutions. Banyak perusahaan kecil kurang berinvestasi dalam keamanan siber yang menarik peretas yang ingin memanfaatkan kelemahan mereka untuk keuntungan finansial.

Keamanan siber juga menjadi masalah yang serius di Indonesia dengan kebocoran data sering terjadi di Indonesia selama 2020-2021. Menurut riset Trend Micro, Indeks Risiko Siber (CRI) Indonesia untuk tahun 2020 adalah 0,26, yang menunjukkan tingkat bahaya yang moderat. Sebaliknya, turun menjadi -0,12 pada tahun 2021, menunjukkan bahwa bahayanya meningkat walau belum dalam risiko tinggi (Nita Azhar, 2021).

Menurut sebuah studi yang dilakukan beberapa waktu lalu oleh Reboot Digital PR Service yang berbasis di Inggris, Indonesia memiliki peringkat keamanan siber terburuk di Asia dan seluruh dunia. Analisis statistik keamanan siber dilakukan oleh Reboot sendiri pada berbagai serangan siber, termasuk *drive-by*, *phishing*, *hosting malware*, dan pelanggaran komputer.

Indonesia dilaporkan menempati peringkat pertama atau tertinggi dengan skor 82,8 dari 100 menurut temuan penelitian. Reboot menemukan bahwa Indonesia memiliki 643 mesin yang disusupi, 1.080 situs *phishing*, dan 1.050 situs web yang dipenuhi malware. Karena itu, Indonesia memiliki indeks keamanan siber termiskin di Asia dan seluruh dunia.

Siprus, yang memiliki skor yang sama dengan Indonesia (82,8), adalah negara dengan keamanan siber terburuk di dunia, berada di posisi kedua. Malaysia, yang berada di samping Indonesia dan dengan skor 79,9, berada di posisi ketiga. Korea Selatan, yang menerima skor 19,8 dari 100, memiliki keamanan siber tertinggi di Asia (Feradhita NKD, 2022).

1.2 Konsep Keamanan Siber

Sejumlah kemajuan teknologi terbaru, termasuk sistem siber fisik, teknologi informasi dan komunikasi, jaringan komunikasi, *big data* dan komputasi awan, pemodelan, virtualisasi, simulasi, dan alat yang dirancang untuk interaksi manusia sederhana dengan komputer, digabungkan membentuk karakteristik model Industri 4.0.

Permasalahan ke depan untuk Industri 4.0 antara lain berurusan dengan isu-isu perubahan paradigma bisnis, keamanan, masalah hukum, standardisasi, dan kesulitan dalam perencanaan sumber daya manusia (Fauzan, 2018). CIA Triad adalah kerangka kerja atau panduan umum yang digunakan praktisi keamanan untuk menilai persyaratan keamanan informasi di lingkungan mereka, dan dengan perluasan, fitur keamanan dan fungsi sistem yang mendasarinya (Adam Boone, 2018).



Gambar 1.2: Triad CIA (Adam Boone, 2018)

CIA Triad meliputi:

1. Kerahasiaan (Confidentiality)
Bagaimana informasi sensitif atau diatur akan dirahasiakan?
2. Integritas (Integrity)
Bagaimana informasi dijaga agar bebas dari manipulasi oleh orang yang tidak berwenang?

3. Ketersediaan (Availability)

Bagaimana informasi akan tersedia bagi pengguna yang berwenang saat dibutuhkan?

Arti keamanan siber sangat bervariasi dan sering kali berkisar pada lingkungan digital sehingga membuat frasa itu sendiri sangat luas. Tiga ide mendasar yang disebut sebagai "Triad CIA" diperlukan untuk memahami apa itu keamanan siber. *Confidentiality*, *Integrity* and *Availability* (CIA) merupakan kerangka kerja keamanan yang diciptakan untuk membantu orang-orang dalam memikirkan keamanan TI.

Kadang-kadang, praktisi keamanan memberikan "A" di triad sebagai *Authentication*, otorisasi atau akses, yang semuanya memiliki implikasi penting untuk fungsi yang mendasari di sekitar kredensial pengguna, kontrol akses, dan sebagainya. Tetapi *Availability* juga mencakup persyaratan seperti mencegah serangan Denial of Service, memblokir serangan Ransomware, dan sebagainya (Adam Boone, 2018).

Persyaratan keamanan tingkat tinggi ini menyaring persyaratan tingkat sistem. Mereka memandu bagaimana suatu perusahaan dapat menyebarkan sistem dan fungsi keamanan untuk melindungi mereka, tetapi mereka juga dapat menunjukkan bagaimana sistem itu sendiri harus dirancang.

Confidentiality

Sangat penting saat ini bagi orang-orang untuk melindungi informasi sensitif dan data pribadi mereka dari akses yang tidak sah. Melindungi kerahasiaan bergantung pada kemampuan untuk mendefinisikan dan menetapkan tingkat akses tertentu untuk informasi.

Dalam beberapa kasus, pemisahan informasi ke diatur oleh siapa yang membutuhkan akses ke informasi dan seberapa sensitif informasi itu sebenarnya. Beberapa cara paling umum yang digunakan untuk mengelola kerahasiaan adalah daftar kontrol akses, enkripsi volume dan file, dan izin file Unix.

Integrity

Ini adalah komponen penting dari CIA Triad dan dirancang untuk melindungi data dari penghapusan atau modifikasi dari pihak yang tidak berwenang, dan memastikan bahwa ketika orang yang berwenang membuat perubahan yang seharusnya tidak dilakukan, kerusakan dapat diperbaiki.

Proses dari integritas menjamin data yang ada di dalam sistem agar selalu konsisten, terverifikasi, akurat dan terpercaya. Artinya data tersebut tidak bisa diganti, diubah, dihapus, atau diakses tanpa adanya izin.

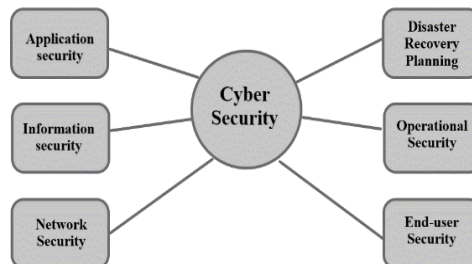
Availability

Ini adalah komponen terakhir dari Triad CIA dan mengacu pada ketersediaan data. Mekanisme otentikasi, saluran akses, dan sistem semuanya harus berfungsi dengan baik untuk informasi yang mereka lindungi dan memastikannya tersedia saat dibutuhkan.

Dalam hal komponen yang dibutuhkan seperti perangkat keras, jaringan, perangkat lunak, perangkat, dan peralatan, ketersediaan artinya semua hal yang disebutkan tadi harus ditingkatkan dan dipertahankan. Alasan kenapa hal itu penting adalah karena komponen tersebut dapat memberikan kinerja yang lancar dan akses ke data tanpa adanya gangguan.

1.3 Elemen dan Tantangan Keamanan Siber

Keamanan siber adalah perlindungan sistem terkait web, misalnya, perangkat keras, perangkat lunak, dan informasi dari bahaya dunia maya. Layanan keamanan siber yang baik mencakup berbagai lapisan perlindungan yang menangani semua sudut penggunaan teknologi. Keamanan siber sekarang menjadi bagian penting dari setiap operasi bisnis karena serangan dunia maya dapat membuat bisnis hancur secara finansial.



Gambar 1.3: Elemen Keamanan Siber (swarnavo09, 2022)

Gambar 1.3 menunjukkan elemen-elemen penting dalam keamanan siber:

Application Security

Keamanan aplikasi adalah komponen kunci utama dari keamanan siber yang menambahkan sorotan keamanan di dalam aplikasi selama jangka waktu perbaikan untuk mempertahankan diri dari serangan siber. Ini melindungi situs dan aplikasi online dari berbagai macam bahaya keamanan siber yang mengeksploitasi kelemahan dalam kode sumber. Keamanan aplikasi terkait dengan menjaga aplikasi perangkat lunak dari bahaya. Fokus umum keamanan aplikasi adalah pada organisasi berbasis layanan cloud.

Information Security

Keamanan Informasi adalah komponen keamanan siber yang menunjukkan metode untuk mempertahankan akses, penggunaan, pengungkapan, interupsi, modifikasi, atau penghapusan informasi yang tidak disetujui. Perlindungan data, kode, dan informasi perusahaan yang dikumpulkan oleh perusahaan dari klien dan pengguna mereka dilindungi oleh keamanan informasi. Standar dan prinsip utama keamanan Informasi adalah Kerahasiaan, Integritas, dan Ketersediaan yang disebut sebagai CIA (Confidentiality, Integrity, and Availability).

Network Security

Keamanan jaringan adalah keamanan yang diberikan kepada jaringan dari akses dan bahaya yang tidak disetujui. Adalah kewajiban kepala jaringan untuk mengambil langkah-langkah pencegahan untuk melindungi jaringan mereka dari potensi bahaya keamanan. Keamanan jaringan adalah satu lagi elemen keamanan TI yang merupakan metode untuk mempertahankan dan mencegah akses yang tidak disetujui ke dalam jaringan komputer.



Gambar 1.4: Contoh Disaster Recovery Plan Untuk IT Perusahaan

Disaster Recovery Planning

Perencanaan yang menggambarkan kelangsungan pekerjaan secara cepat dan efisien setelah terjadinya bencana dikenal dengan istilah *Disaster Recovery Planning* atau *Business Continuity Planning*. Teknik pemulihan bencana harus dimulai pada tingkat bisnis dan mencari tahu aplikasi mana yang umumnya penting untuk menjalankan aktivitas asosiasi. *Business Continuity Planning* (BCP) terkait dengan kesiapan menghadapi bahaya dunia maya dengan membedakan bahaya ke institusi sesuai jadwal dan memeriksa bagaimana kegiatan mungkin terpengaruh dan bagaimana mengatasinya.

Tujuan utama dari perencanaan pemulihan bencana meliputi:

1. melindungi organisasi selama bencana;
2. memberikan keyakinan keamanan;
3. membatasi risiko penundaan;
4. memastikan keandalan sistem cadangan;
5. memberikan standar untuk menguji rencana;
6. membatasi pengambilan keputusan selama bencana.

Operational Security

Proses yang mendorong para manajer untuk melihat aktivitas menurut sudut pandang seorang peretas untuk melindungi data sensitif dari berbagai ancaman dikenal sebagai *Operational Security* (OPSEC) atau keamanan operasional dan digunakan untuk mempertahankan fungsi institusi.

Ada lima tahapan dalam menghadapi program pengamanan operasional, yaitu:

1. mencirikan data asosiasi;
2. membedakan jenis-jenis ancaman;
3. menginvestigasi celah keamanan dan kelemahannya;
4. mengevaluasi risiko;
5. mengeksekusi tindakan pencegahan yang akurat.

End User Education

Pelatihan pengguna akhir adalah elemen yang paling signifikan dari keamanan komputer. Pengguna akhir berubah menjadi ancaman keamanan terbesar dalam asosiasi apa pun karena itu bisa terjadi kapan saja. Salah satu kesalahan utama yang menyebabkan kerusakan informasi adalah kesalahan manusia.

Sebuah asosiasi harus mempersiapkan pekerjanya tentang keamanan siber. Setiap perwakilan harus mengetahui tentang serangan *phishing* melalui pesan dan antarmuka dan mungkin dapat mengelola bahaya dunia maya.

Untuk memastikan evaluasi tersebut lebih adil lagi, perusahaan atau organisasi juga dapat menyusun tim evaluasi kinerja yang dianggap adil baik untuk menilai kinerja individu maupun menilai kinerja kelompok, unit, atau bagian lain dari perusahaan (Sofyan Tsauri, 2014).

Sedangkan tantangan yang akan dihadapi oleh perusahaan-perusahaan dalam keamanan siber di era Revolusi Industri 4.0 (Rahmawati, 2019) menurut Eset adalah:

Target Serangan

Pada titik tertentu, 48% produsen mengalami peristiwa keamanan, dan 50% dari bisnis ini menghadapi kerugian finansial atau gangguan bisnis, menurut survei *Enterprise Environmental Factor* (EEF). Sektor manufaktur, sektor publik, dan bisnis keuangan adalah salah satu yang paling sering diserang oleh serangan siber, menurut jajak pendapat tersebut.

Dalam hal solusi keamanan perusahaan, *Industrial Control System* (ICS) atau *Supervisory Control and Data Acquisition* (SCADA) adalah perangkat lunak yang paling banyak digunakan di sektor infrastruktur, manufaktur, dan lainnya.

Ransomware

Ransomware adalah jenis malware yang paling umum, menurut analisis Verizon 2018. Perkembangan yang paling mengkhawatirkan adalah bahwa peretas berfokus pada server dan sistem penting lainnya daripada perangkat pribadi karyawan. Karena sulitnya berurusan dengan *ransomware*, kebutuhan perusahaan akan teknologi keamanan *ransomware* tidak dapat dinegosiasikan. Ini karena *ransomware* tidak pernah memilih korban mana yang akan ditargetkan.

Sumber Daya Manusia

Eset mengklaim bahwa ada ke terputusan antara kesadaran staf dan kemajuan dalam keamanan siber. penyebab utama kerentanan, 52% di antaranya diakibatkan oleh kesalahan karyawan yang tidak disengaja, seperti mengirimkan file yang salah, menyalinnya secara tidak benar, membiarkan komputer terbuka saat tidak digunakan, dll. Menurut sebuah penelitian oleh Ponemon Institute, orang dalam dengan sengaja membocorkan data untuk

keuntungan finansial, spionase, atau persaingan bisnis dalam satu dari setiap empat kasus.

Bab 2

Hukum dan Regulasi Siber

2.1 Pendahuluan

Untuk mempertahankan kedaulatan dan stabilitasnya di dunia modern, suatu negara harus mengubah pendekatannya terhadap diplomasi dan keamanan nasional. Munculnya kejahatan dunia maya memerlukan pertimbangan yang cukup besar dalam pengembangan keamanan siber suatu negara. Keberadaan dunia maya bukan lagi sekadar isu nasional; sekarang menjadi masalah global (Dinanda Diadeska Diara, 2020).

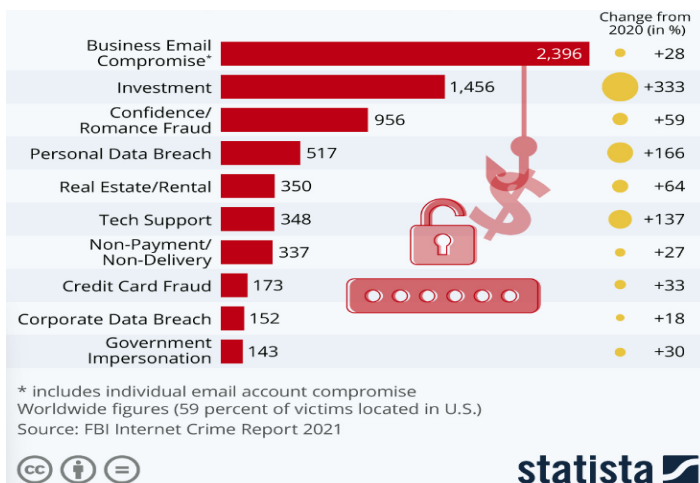
Kehadiran *cybercrime* telah menjadi ancaman bagi kehidupan manusia. Hal ini akibat dari pesatnya perkembangan teknologi informasi yang pada hakikatnya memiliki dampak positif dan negatif. Salah satu dampak negatifnya adalah penyalahgunaan data dan informasi pribadi (Aswandi, Muchsin and Sultan, 2020).

Di era digital, serangan siber memberikan dilema bagi para pengambil kebijakan. Sejak tahun 2003, telah terjadi peningkatan kejahatan yang dilakukan dengan menggunakan teknologi komputer seperti mendistribusikan konten terlarang, ujaran kebencian, dan bentuk kejahatan dunia maya lainnya. Dengan meningkatnya kejahatan siber, negara-negara seperti Indonesia harus memperhatikan dan menganggap serius keamanan siber (Dewan Teknologi dan Komunikasi Nasional, 2018).

Karena web dianggap sebagai platform global, siapa pun dapat mengakses sumber daya internet dari mana saja. Namun teknologi internet telah digunakan oleh segelintir orang untuk kegiatan kriminal seperti akses tidak sah ke jaringan orang lain, penipuan, dan lain-lain. Kegiatan kriminal ini atau pelanggaran/kejahatan yang terkait dengan internet disebut sebagai kejahatan dunia maya.

Untuk menghentikan atau menghukum para penjahat cyber istilah "cyber law" diperkenalkan. Kita dapat mendefinisikan *cyber law* sebagai bagian dari sistem hukum yang berhubungan dengan Internet, dunia maya, dan dengan masalah hukum. Ini mencakup area yang luas, mencakup banyak sub topik serta kebebasan berekspresi, akses ke dan pemanfaatan Internet, dan keamanan online atau privasi online.

Hukum merupakan salah satu kebijakan pemerintah yang dibuat untuk kepentingan negara. Hukum diyakini dapat mengontrol dan mengatur masyarakat. Namun, atas nama kebebasan banyak yang tidak menyukainya. Dalam konteks Internet, undang-undang siber dibuat untuk memastikan para pengguna internet menggunakan ruang siber dengan baik dan hati-hati. Salah satu langkah untuk mengatasi ancaman siber adalah melalui penegakan hukum siber. Namun, netizen masih belum menyadari keberadaan *cyber law* dan meningkatnya jumlah kasus *cyber crime* di setiap tahunnya (Pitchan and Omar, 2019).



Gambar 2.1: Kerugian Finansial Karena Kejahatan Siber Tahun 2021 (US Dolar) (Buchholz, 2022)

Menurut laporan yang dirilis oleh FBI, kerugian akibat kejahatan dunia maya meningkat secara signifikan pada tahun 2021. Kerugian diperkirakan mencapai \$6,9 miliar tahun lalu, naik dari \$4,2 miliar pada tahun 2020. Kejahatan paling mahal yang dicatat oleh FBI adalah penyusupan email bisnis dan penyusupan email pribadi, yang menargetkan bisnis dan individu yang terlibat dalam transfer dengan membobol email mereka. Pada tahun 2021, hampir \$2,4 miliar hilang dengan cara ini (Buchholz, 2022).

2.2 Hukum Siber Dalam Perspektif Internasional

Tema utama keamanan siber adalah praktik melindungi sistem kritis dan data sensitif dari serangan digital. Sifat perkembangan Internet yang ekspansif telah memicu pembentukan badan legislatif siber dengan tujuan untuk memastikan keamanan dunia maya. Pada awal tahun 2021, jumlah orang yang menggunakan internet lebih dari 4,66 miliar dan indeks ini meningkat sekitar 7% setiap tahun, yang berarti jumlah ini meningkat sekitar 8.75.000 pengguna baru setiap hari.

Hukum siber adalah salah satu tambahan terbaru pada sistem hukum. Definisi hukum siber merupakan sistem hukum yang diterapkan untuk menangani komputasi, dunia maya, dan masalah hukum terkait seputar internet dengan memberikan perlindungan. Lanskap kejahatan dunia maya yang berkembang dan kesenjangan keterampilan yang dihasilkan merupakan tantangan penting bagi lembaga penegak hukum (Odishvili, 2021).

Hukum siber mencakup aspek kekayaan intelektual, kontrak, yurisdiksi, undang-undang perlindungan data, privasi, dan kebebasan berekspresi. Ini interkoneksi ke sirkulasi digital perangkat lunak, informasi, keamanan online, dan e-Commerce. Ini berarti bahwa penyedia layanan Internet perlu memperlakukan semua komunikasi Internet secara setara dan mereka tidak dapat melakukan diskriminasi berdasarkan pengguna, konten, platform, peralatan, alamat sumber, atau metode komunikasi.

Menurut prinsip ini, penyedia layanan Internet dilarang dengan sengaja memblokir, memperlambat layanan, atau mengenakan biaya untuk konten tertentu. Pasal 19 Deklarasi Universal Hak Asasi Manusia menuntut kebebasan

berekspresi dalam segala bentuk media. Postingan internet yang mengandung konten negatif, fitnah, dan distribusi konten ilegal semuanya telah menjelaskan batasan kebebasan berbicara di internet. Selain itu, sensor internet mengacu pada apa yang dapat diakses, dipublikasikan, atau dilihat di internet. Pengguna internet dapat disensor karena beberapa alasan: moral, bisnis, intimidasi, dan ketakutan akan konsekuensi hukum (Odishvili, 2021).

Mempertimbangkan sifat dinamis, terstruktur, dan interaktif dari dunia maya, pendekatan legislatif untuk bidang ini bersifat konstruktif. Dalam konteks Hukum Siber Internasional, perlu ditonjolkan beberapa kekurangan terkait metode pendekatan. Misalnya, karena perkembangan teknologi adalah bidang yang berkembang pesat, implementasi standar mungkin berada jauh di belakang kemajuan teknologi.



Gambar 2.2: Negara Paling Berisiko Terhadap Serangan Siber (Varga, 2022)

Tantangan utama mengenai hukum siber internasional tetap pada kenyataan bahwa hukum internasional yang mengikat dan terarah dengan baik sering kali tidak berlaku efektif bagi negara-negara yang diberikan akses terhadap tantangan yang terjadi di luar bidang hukum internasional publik dalam hal yurisdiksi, arbitrase, instrumen hukum, dan yurisprudensi. Sebagai contoh, hukum internasional di dunia maya saat ini terbelakang dalam lingkup kewajibannya terhadap peran negara.

Berdasarkan statistik yang diterbitkan oleh Konferensi PBB tentang Perdagangan dan Pembangunan, Eropa memiliki tingkat adopsi undang-undang dunia maya tertinggi (93 persen), sementara Asia dan Pasifik memiliki tingkat adopsi terendah (55 persen). 154 negara (79 persen) telah memberlakukan undang-undang kejahatan dunia maya, 5% negara memiliki

undang-undang tingkat rancangan, 13% negara tidak memiliki pendekatan legislatif sama sekali, sementara kami tidak memiliki informasi mengenai 2% negara (Odishvili, 2021).

Di seluruh dunia, hampir setiap hari laporan berita telah diajukan merinci hasil serangan siber yang sangat efektif mulai dari perusahaan kecil hingga negara-bangsa. Jumlah total serangan ini secara permanen dan dramatis mengubah lanskap ancaman keamanan informasi. Serangan siber telah menjadi ancaman eksistensial bagi banyak negara seperti layanan keuangan, fasilitas pembangkit listrik, dan integritas berbagai segmen industri (Herberger, 2018).

Akibatnya, regulator di seluruh dunia turun tangan untuk mencoba dan mendorong tindakan yang diperlukan. Berikut beberapa regulasi yang sudah pernah dilakukan:

National Institute of Standards and Technology's (NIST) Cybersecurity Framework

NIST meletakkan tiga pilar utama untuk kerangka kerja yang dirancang untuk memberikan industri dan pemerintah sama dengan taksonomi keamanan siber umum, menetapkan tujuan, target yang diinginkan, mengidentifikasi dan memprioritaskan peluang untuk peningkatan, menilai kemajuan, dan meningkatkan komunikasi di antara para pemangku kepentingan.

Kerangka kerja terakhir diumumkan pada bulan Februari 2014. Banyak yang mengatakan kerangka kerja ini dipandang sebagai pionir yang akan menelurkan banyak kerangka kerja untuk kebutuhan industri di seluruh AS.

Office of the Superintendent of Financial Institutions (OSFI) DDoS Memorandum

Pada tanggal 28 Oktober 2013, *Office of the Superintendent of Financial Institutions* (OSFI) merilis sebuah memorandum kepada *Federal-Regulated Canadian Financial Institution* (FRFIs) yang membahas langkah-langkah yang harus diambil FRFI untuk mencegah, mengelola, dan memulihkan serangan siber. Memorandum tersebut menyatakan bahwa keamanan siber semakin penting.

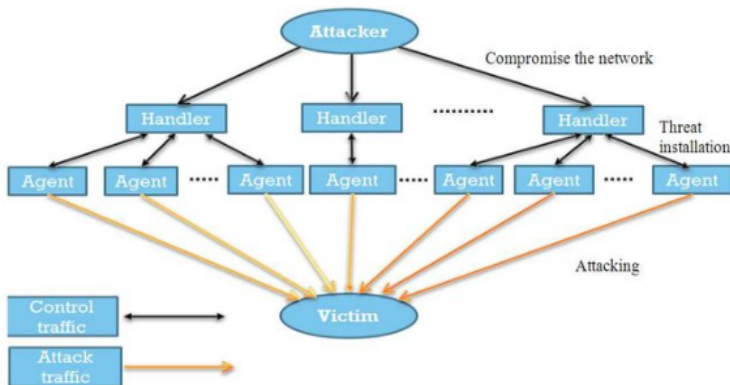
Kembali pada tahun 2005, OSFI mendirikan *Canadian Cyber Incident Response Center* (CCIRC) dengan mandat untuk berkolaborasi dengan sektor swasta dalam menanggapi ancaman serangan cyber (Herberger, 2018).

FFIEC Joint Statement: Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources (US)

Anggota Dewan Pemeriksa Lembaga Keuangan Federal (FFIEC) mengeluarkan pernyataan untuk memberi tahu lembaga keuangan tentang risiko yang terkait dengan serangan siber pada Anjungan Tunai Mandiri (ATM), sistem otorisasi kartu, dan serangan penolakan layanan (DDoS) terdistribusi yang berkelanjutan terhadap publik.

Pernyataan-pernyataan tersebut menjelaskan langkah-langkah yang dapat diharapkan oleh para anggota lembaga untuk mengatasi serangan-serangan ini dan menyoroti sumber daya yang dapat digunakan lembaga-lembaga untuk membantu mengurangi risiko yang ditimbulkan oleh serangan-serangan tersebut.

Para anggota juga mengharapkan lembaga keuangan untuk mengatasi kesiapan DDoS sebagai bagian dari keamanan informasi. Lebih khusus lagi, setiap institusi diharapkan untuk memantau lalu lintas masuk ke situs web publiknya, mengaktifkan rencana respons insiden jika mencurigai bahwa serangan DDoS sedang terjadi, dan memastikan staf yang memadai selama serangan, termasuk penggunaan pihak ketiga yang telah dikontrak sebelumnya.



Gambar 2.3: Arsitektur Serangan Distributed Denial of Service (DDoS)
(Bhaya and Manaa, 2014)

Securities and Exchange Commission Cyber Exams (U.S.)

SEC mengatur sebagian besar layanan keuangan yang tidak termasuk dalam yurisdiksi FFIEC. Jadi, semua reksa dana, manajemen kekayaan, dan dana lindung nilai (di antara banyak lainnya) diatur bukan oleh pedoman FFIEC,

melainkan pedoman SEC. Tidak seperti FFIEC dan badan pengaturnya (OCC, FDIC, OTS, & NCUA), hingga saat ini SEC melakukan tinjauan ad-hoc, namun tinjauan keamanan rutin tetap dipertahankan.

Office of the Comptroller of the Currency Guidance (U.S.)

Pada bulan Desember 2012, *Office of the Comptroller of the Currency* (OCC) memberi tahu lembaga keuangan anggotanya bahwa serangan DDoS sedang meningkat dan mereka mengharapkan anggotanya mengambil langkah untuk mengidentifikasi risiko yang terkait dengan serangan tersebut dan untuk memberikan pemberitahuan kepada OCC dan lain-lain jika mereka diserang.

OCC mengharapkan bank yang menjadi korban atau terkena dampak buruk dari serangan DDoS untuk melaporkan informasi ini kepada otoritas penegak hukum dan untuk memberi tahu kantor pengawasan mereka. Selain itu, bank harus secara sukarela mengajukan Laporan Aktivitas Mencurigakan (SAR) jika serangan DDoS memengaruhi informasi penting lembaga termasuk informasi akun pelanggan, atau merusak, menonaktifkan, atau memengaruhi sistem penting bank.

National Credit Union Administration Risk Alert (U.S)

Pada bulan Februari 2013, *National Credit Union Administration* (NCUA) mengeluarkan Peringatan Risiko kepada lembaga serikat kredit anggota tentang “Mengurangi Serangan Denial-of-Service Terdistribusi”. Urgensi dan keganasan serangan muncul dalam peringatan dan memberikan pemahaman tentang masalah yang lebih luas daripada ketersediaan sistem serikat kredit.

European Union Security of Network Information Systems (NIS) Directive 2016/ 2018

Pada Juli 2016, Parlemen Eropa menetapkan kebijakan *Directive on Security of Network and Information Systems* (NIS Directive). Arahan tersebut mulai berlaku pada Agustus 2016, dan semua negara anggota Uni Eropa diberi waktu 21 bulan untuk memasukkan peraturan arahan tersebut ke dalam undang-undang nasional mereka sendiri.

Tujuan dari NIS Directive adalah untuk menciptakan tingkat keamanan siber yang lebih tinggi secara keseluruhan di UE. Arahan tersebut secara signifikan mempengaruhi penyedia layanan digital (DSP) dan operator layanan penting (OES). Operator layanan penting termasuk organisasi yang operasinya akan

sangat terpengaruh jika terjadi pelanggaran keamanan jika mereka terlibat dalam kegiatan sosial atau ekonomi yang kritis (Herberger, 2018).

European Union General Protection Regulation (GDPR)

Peraturan Perlindungan Data Umum (GDPR) UE mulai berlaku pada 25 Mei 2018. GDPR bertujuan untuk menghadirkan standar tunggal untuk perlindungan data di antara semua negara anggota di UE. Perubahan termasuk pendefinisian ulang batas-batas geografis. Ini berlaku untuk entitas yang beroperasi di UE atau menangani data penduduk UE mana pun. Di mana pun data diproses, jika data warga negara Uni Eropa sedang diproses, entitas tersebut kini tunduk pada GDPR.

European Union Ban on Geo-IP Blocking of Member States 2018

Pada Februari 2018, Dewan Eropa mengadopsi peraturan untuk melarang pemblokiran geografis yang tidak dapat dibenarkan di pasar internal. Dewan Eropa telah berulang kali menekankan pentingnya strategi pasar tunggal digital dan menyerukan percepatan pelaksanaan strategi, yang mencakup penghapusan hambatan yang tersisa untuk sirkulasi bebas barang dan jasa yang dijual secara online dan untuk mengatasi diskriminasi yang tidak dapat dibenarkan pada alasan letak geografis.

UE menyatakan pemblokiran geografis sebagai praktik diskriminatif yang mencegah pelanggan online mengakses dan membeli produk atau layanan dari situs web yang berbasis di negara anggota lain. Undang-undang baru akan menghilangkan hambatan terhadap e-Commerce dengan menghindari diskriminasi berdasarkan kewarganegaraan pelanggan, tempat tinggal atau tempat pendirian

Growth of Country-Specific Cybersecurity Regulations such as Korean Cyber Laws

Di Korea, ada berbagai undang-undang, peraturan, dan pedoman yang mempromosikan keamanan siber: dua undang-undang umum (Undang-Undang Jaringan dan Undang-Undang Perlindungan Informasi Pribadi (PIPA)) dan undang-undang lain yang menargetkan area tertentu.

Protection of Information and Communications Infrastructure Act (PICIA) lebih terlibat dengan perlindungan infrastruktur informasi dan komunikasi terhadap 'intrusi elektronik', yang didefinisikan sebagai tindakan menyerang infrastruktur informasi dan komunikasi dengan cara meretas, virus komputer,

bom logika, email bom, penolakan layanan, gelombang elektromagnetik berdaya tinggi dan cara lainnya (Herberger, 2018).

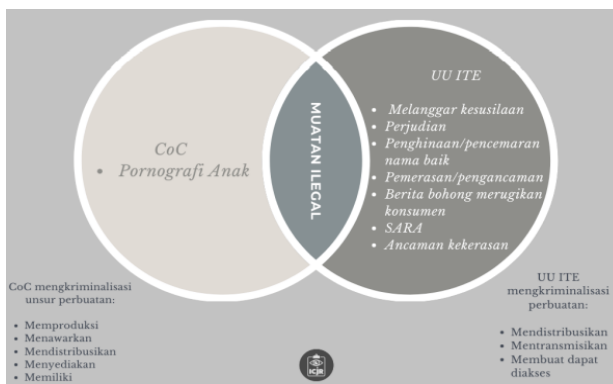
2.3 Hukum dan Regulasi Siber Indonesia

Perkembangan Teknologi Informasi dan Komunikasi (TIK) di sejumlah daerah telah mengubah cara pandang budaya Indonesia. Pertama, modifikasi budaya dalam teknologi informasi untuk modernisasi informasi. Kedua, pergeseran budaya masyarakat ke dalam siber kultur (cyberculture).

Dalam kerangka budaya modern, menjamurnya handphone dan penggunaan media sosial dan mesin pencari merupakan fenomena yang tak terhindarkan. Semua ini didasarkan pada kecenderungan orang-orang terhadap kebutuhan akan koneksi dan informasi yang konstan, yang telah mengarah pada pengembangan sistem budaya komunitas global (Sahri, 2018).

Kebijakan Pidana dan Pengaturan Dalam UU ITE 2008

Dalam hal regulasi, UU ITE 2008 melampaui ruang lingkup Konvensi Kejahatan Siber. Berbeda dengan Konvensi Kejahatan Siber, yang semata-mata melarang Pornografi Anak, UU ITE mencakup lebih luas lagi seperti konten terlarang, perjudian, kesusilaan, fitnah, pencemaran nama baik, mendistribusikan informasi palsu, menyebabkan kerugian konsumen, dan sebagainya.



Gambar 2.4: Perbandingan Delik Terhadap Muatan Konten Pornografi Anak dan UU ITE (A. Budiman *et al.*, 2021)

Dalam beberapa rumusannya, peraturan non-pidana dalam UU ITE 2008 masih belum jelas karena terbuka terhadap berbagai penafsiran, yang bertentangan dengan dasar-dasar hukum pidana. Ini juga menyentuh aspek pribadi individu. Selain fakta bahwa larangan pengiriman konten kesusilaan telah diatur dalam Undang-Undang Nomor 44 Tahun 2008 tentang Pornografi, larangan distribusinya, misalnya, tidak memiliki batasan yang sesuai dan berdampak pada interpretasi yang luas dan beragam.

UU ITE juga memasukkan frasa "tanpa hak" sebagaimana didefinisikan dalam Pasal 9 Konvensi Kejahatan Siber, yang relevan dengan peraturan beberapa kejahatan ilegal. Frasa "tanpa hak" didefinisikan secara ketat dalam Konvensi Kejahatan Dunia Maya karena ada beberapa contoh di mana suatu tindakan dapat dibenarkan, seperti ketika ada otoritas hukum, eksekutif, administratif, yudisial, kontraktual, atau konsensual.

Namun, "tanpa hak" adalah salah satu faktor dalam berbagai kejahatan kriminal yang diatur yang tidak dijelaskan oleh Undang-Undang ITE, yang mengarah pada interpretasi yang berbeda dari bagian "tanpa hak" ini (A. Budiman *et al.*, 2021).

UU ITE 2016: Dinamika dan Arah Perubahan Kebijakan

UU ITE 2008 telah mengalami beberapa revisi terbatas sebagai akibat dari berbagai kritik terhadap isu-isu yang dihasilkan. Pemerintah kemudian membuat usulan amandemen UU Informasi dan Transaksi Elektronik (UU ITE) 2008, dan pada Desember 2015, Presiden Joko Widodo secara resmi mempresentasikan Rancangan Undang-Undang tentang Perubahan atas Undang-Undang tentang Informasi dan Transaksi Elektronik (RUU Revisi UU ITE) kepada Dewan Perwakilan Rakyat (DPR).

Pemerintah dan DPR menyepakati revisi beberapa materi UU pada 27 Oktober 2016, sepuluh tahun setelah UU ITE 2008 disahkan. Amandemen ini akhirnya disahkan dalam UU ITE 2016. UU ini menambahkan lebih banyak klarifikasi dan mengatur sejumlah bagian baru, amandemen ini berfokus pada ketentuan pidana. Pasal-pasal tindak pidana telah direvisi dengan definisi baru, termasuk untuk pencemaran nama baik yang mengacu pada KUHP Pasal 27 ayat 3, yang berhubungan dengan fitnah dan pencemaran nama baik (A. Budiman *et al.*, 2021).

Tabel 2.1: Pokok-Pokok Perubahan UU ITE (A. Budiman *et al.*, 2021)

No.	Isu	Perubahan
1	Perubahan dalam Pasal 27 ayat (3) tentang penghinaan dan / atau pencemaran nama baik	<ul style="list-style-type: none"> ▪ Menambahkan penjelasan tentang istilah mendistribusikan, mengirimkan dan/atau membuat dapat diaksesnya informasi elektronik. ▪ Menambah penjelasan bahwa ketentuan Pasal 27 ayat (3) mengacu pada ketentuan pencemaran nama baik dan/atau fitnah yang diatur dalam KUHP. ▪ Tambahan penjelasan tersebut mempertegas pada ketentuan Pasal 27 ayat (3) merupakan delik aduan.
2	Menurunkan ancaman pidana	<ul style="list-style-type: none"> ▪ Tindak pidana pencemaran nama baik dalam Pasal 27 ayat (3) yang sebelumnya maksimum enam tahun penjara diubah menjadi maksimum empat tahun penjara. ▪ Tindak pidana kekerasan dalam Pasal 29, yang sebelumnya paling lama 12 tahun, diubah menjadi empat tahun dan denda Rp 2 miliar menjadi Rp 750 juta.
3	Perundungan di dunia siber (cyber bullying)	Penjelasan pasal 45B memasukkan perundungan di dunia siber (cyber bullying) yang mengandung unsur ancaman kekerasan atau menakut-nakuti dan mengakibatkan kekerasan fisik, psikis, dan/atau kerugian materiil.
4	Intersepsi (penyadapan)	<ul style="list-style-type: none"> ▪ Tata cara intersepsi diatur dengan Undang-Undang, yang sebelumnya dapat diatur dalam Peraturan Pemerintah. ▪ Perubahan ini melaksanakan putusan MK atas Pasal 31 ayat (4) yang menyatakan bahwa tata cara intersepsi diatur dengan Undang-Undang
5	Hasil penyadapan sebagai alat bukti	Menambahkan penjelasan ketentuan Pasal 5 ayat (1) dan (2) mengenai hasil penyadapan atau rekaman hasil penyadapan informasi sebagai alat bukti hukum jika dilakukan secara sah dalam rangka penegakan hukum.
6	Hukum Acara	Sinkronisasi hukum acara pengeledahan, penyitaan, penangkapan, dan penahanan dengan hukum acara dalam KUHP yang mana memberikan kemunduran bagi penguatan fair trial.
7	Penyidik pegawai negeri sipil (PPNS)	Memperkuat peran penyidik pegawai negeri sipil (PPNS) dalam Pasal 43 ayat (5) UU ITE untuk memutus akses, ke tindak pidana yang terkait dengan

		teknologi informasi.
8	Penghapusan informasi	<ul style="list-style-type: none"> ▪ Pasal 26 ditambahkan ketentuan tentang kewajiban untuk menghapus Informasi Elektronik dan/atau Dokumen Elektronik yang tidak relevan bagi penyelenggara sistem elektronik berdasarkan surat perintah pengadilan. ▪ Ketentuan ini hampir mirip dengan konsep hak untuk dilupakan (right to be forgotten).
9	Pencegahan konten negatif di internet	<ul style="list-style-type: none"> ▪ Pasal 40 memperkuat peran Pemerintah untuk mencegah penyebaran konten negatif di internet. ▪ Pemerintah memiliki wewenang besar untuk memutus akses dan/atau memerintahkan Operator Sistem Elektronik menghentikan akses ke informasi elektronik yang memiliki tuduhan melanggar hukum.

Permasalahan Dalam Pelaksanaan Pasal UU ITE

Pasal-pasal pidana UU ITE 2008 memiliki sejumlah masalah yang berdampak pada bagaimana penerapannya, yang sangat berkontribusi pada situasi yang tidak boleh diadili, diselesaikan di pengadilan, atau bahkan mengakibatkan penjara. Sebenarnya, meski setelah diperbaharui pada 2016, pasal-pasal pidana UU ITE masih berdampak. Dari 2016 hingga Februari 2020, *Institute for Criminal Justice Reform* (ICJR) melakukan penelusuran putusan berkaitan dengan kasus-kasus yang melibatkan penerapan Pasal 27 hingga 29 UU ITE dan menghasilkan setidaknya 768 kasus.

Tindak pidana pencemaran nama baik dengan tuntutan pidana berdasarkan Pasal 27 ayat (3) menyumbang persentase tertinggi dari 768 kasus (37,2%), diikuti dengan tindak pidana kesusilaan dengan tuntutan pidana berdasarkan Pasal 27 ayat (1) (31,5%), dan tindak pidana penyebaran kebencian dengan tuntutan pidana berdasarkan Pasal 28 ayat (2) (8,2%). Data tersebut juga menunjukkan bahwa tingkat pidanaan UU ITE sangat tinggi, dengan tingkat keyakinan terdakwa mencapai 96,8%. (744 kasus) (A. Budiman *et al.*, 2021).

Statistik menunjukkan masalah yang signifikan dalam penerapan UU ITE. Pertama, tingkat keyakinan yang sangat tinggi menunjukkan betapa sederhananya menetapkan unsur-unsur kejahatan dan seberapa cepat narapidana dinilai bersalah. Penyusunan pasal-pasal pidana dalam Pasal 27

ayat (1) dan (3), Pasal 28 ayat (2), dan Pasal 29, yang sangat permisif dan tidak ditegakkan secara ketat, memiliki dampak substansial terhadap proses pembuktian dalam kasus-kasus aktual.

Kedua, tingginya jumlah bentuk hukuman penjara dalam kasus-kasus UU ITE menunjukkan hukuman secara ekssesif digunakan. Padahal, terdapat berbagai opsi hukuman lain yang bila dikenakan, misalnya pidana bersyarat dengan masa percobaan ataupun pidana denda karena rumusan dalam UU ITE memuat pidana denda secara alternatif-kumulatif (A. Budiman *et al.*, 2021).

Dalam kasus pencemaran nama baik (Pasal 27 ayat 3), hukuman penjara sangat tinggi yang mencapai 87%, padahal sifat tindak pidana pencemaran nama baik ini adalah delik aduan yang seharusnya ruang-ruang untuk melakukan penyelesaian dengan mekanisme pemulihan, perdamaian, penggantian kerugian yang mempertimbangkan hak korban lebih bermanfaat dan dapat diterapkan untuk menghindari pemenjaraan yang ekssesif.

Ketiga, tingginya *conviction rate* dan hukuman penjara tersebut didukung oleh masalah-masalah dalam proses peradilan. Dalam sejumlah kasus, terjadi pelanggaran hak-hak atas *fair trial*, misalnya tidak terpenuhinya secara baik prinsip *equality of arms* di dalam pemeriksaan perkara yang disebabkan ketiadaan pendampingan hukum, kualitas pendampingan hukum yang buruk, ataupun peradilan yang tidak imparsial (A. Budiman *et al.*, 2021).

Bab 3

Ancaman Keamanan Siber

3.1 Pendahuluan

Ashari et al (2022) Mengatakan bahwasanya berbagai jenis malware telah muncul dari waktu ke waktu sebagai akibat dari pertahanan keamanan menjadi lebih canggih dan serangan yang semakin lebih kompleks. Salah satu metode untuk mengklasifikasikan berbagai jenis malware adalah dengan menggunakan sifat primer yang dimiliki malware.

Menurut Ciampa (2015) ciri-ciri malware dapat dilihat dari sifatnya yaitu *circulation, infection, concealment, dan payload capabilities*.

1. Circulation

Beberapa malware memiliki sifat utama yang dapat menyebar dengan cepat ke sistem lain sehingga dapat mempengaruhi sejumlah besar pengguna. Malware dapat beredar melalui berbagai media, ini berarti: menyebar dengan menggunakan jaringan dimana semua perangkat terhubung, melalui flash USB drive yang dibagikan di antara pengguna, atau dengan mengirimkan malware sebagai lampiran E-Mail. Malware dapat diedarkan secara otomatis atau mungkin memerlukan tindakan atau aksi yang dilakukan oleh pengguna.

2. Infection

Setelah malware mencapai sistem melalui fase sirkulasi, maka malware harus "menginfeksi" atau menanamkan dirinya ke dalam sistem tersebut. Malware bisa saja hanya berjalan satu kali dan kemudian menyimpan dirinya sendiri dalam memori komputer. Beberapa malware menempel pada program yang tidak berbahaya, sementara malware lainnya berfungsi sebagai proses yang berdiri sendiri yang dimana nantinya dapat melakukan instruksi atau perintah berbahaya.

3. Concealment

Beberapa malware memiliki sifat utama yaitu menghindari deteksi dengan menyembunyikan kehadirannya dari aplikasi pemindai. Malware polimorfik berusaha menghindari deteksi dengan mengubah dirinya sendiri, sementara malware lain dapat menempatkan dirinya dalam proses yang ada atau memodifikasi sistem operasi host yang mendasarinya.

4. Payload Capabilities

Ketika *payload capabilities* menjadi fokus utama malware, maka yang jadi perhatian adalah tindakan jahat apa yang bisa dilakukan malware. Apakah itu mencuri kata sandi? dan data berharga lainnya dari sistem pengguna? Apakah itu menghapus program sehingga komputer tidak bisa lagi berfungsi dengan baik? Atau apakah malware dapat melakukan modifikasi sistem pengaturan keamanan? Dalam beberapa kasus, tujuan malware adalah untuk menginfeksi sistem dan untuk meluncurkan serangan terhadap komputer lain.

Bagian berikut memberikan rincian lebih lanjut dan contoh malware yang diklasifikasikan berdasarkan sirkulasi/ kemampuan infeksi, *concealment*, dan *payload capabilities*.

3.2 Sirkulasi/ Infeksi

Tiga jenis malware memiliki ciri utama sirkulasi dan/atau infeksi. Ini adalah virus, worm, dan Trojan.

Virus

Secara istilah, virus biologis adalah agen yang berkembang biak di dalam sel. Ketika sel terinfeksi oleh virus, virus akan mengambil alih operasi pada sel itu, mengubahnya menjadi pabrik virtual untuk membuat lebih banyak salinannya. Sel dipaksa untuk menghasilkan ribuan atau ratusan ribu identik salinan virus asli dengan sangat cepat (virus polio dapat membuat lebih dari satu juta salinan dirinya sendiri di dalam satu sel manusia yang terinfeksi). Ahli biologi sering mengatakan bahwa virus hanya ada untuk membuat lebih banyak virus lainnya lagi.

Virus komputer (virus) adalah kode komputer berbahaya yang dapat mereproduksi dirinya sendiri di komputer yang sama. Sebenarnya virus komputer dapat bereplikasi sendiri (atau salinan yang berkembang dari dirinya sendiri) tanpa campur tangan manusia. Hampir semua virus “menginfeksi” dengan memasukkan dirinya ke dalam file komputer. Virus yang menginfeksi file program yang dapat dieksekusi disebut program virus. Saat program dijalankan, virus diaktifkan.

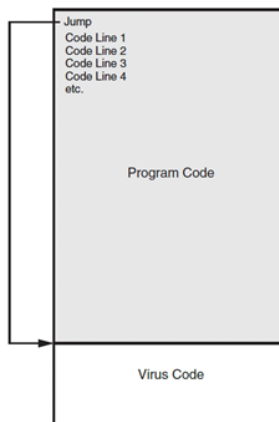


Figure 2-1 Appender infection

Gambar 3.1: Appender Infection (Ciampa, 2015)

Virus juga dapat menginfeksi data file. Salah satu virus data file yang paling umum adalah virus makro yang ditulis dalam skrip yang dikenal sebagai makro. Makro adalah serangkaian instruksi yang dapat dikelompokkan bersama sebagai satu instruksi perintah. Sering kali makro digunakan untuk mengotomatisasi serangkaian tugas yang kompleks atau serangkaian tugas yang berulang.

Makro dapat ditulis dengan menggunakan bahasa makro, seperti *Visual Basic for Applications* (VBA), dan disimpan dalam dokumen pengguna (seperti pada lembar kerja (spreadsheet) Excel .XLSX atau file Word .DOCX). Setelah dokumen dibuka, instruksi perintah makro kemudian dijalankan, apakah instruksi itu tidak berbahaya atau virus makro. Sejumlah besar jenis ekstensi file yang berbeda-beda dapat berisi virus. Tabel 3.1 mencantumkan beberapa dari 70 perbedaan Jenis file Microsoft Windows dapat terinfeksi virus.

Virus relatif mudah dalam menginfeksi file. Salah satu tipe dasar infeksi adalah *appender infection*. Virus pertama-tama menempel atau menambahkan dirinya ke ujung yang terinfeksi mengajukan. kemudian menyisipkan di awal file instruksi "lompat" yang menunjuk ke akhir file, yang merupakan awal dari kode virus. Saat program diluncurkan, instruksi lompat mengalihkan kontrol ke virus. Gambar 3.1 menunjukkan cara kerja infeksi appender.

Tabel 3.1: Tipe Ekstensi File Yang Dapat Di Infeksi (Ciampa, 2015)

Ekstensi File	Deskripsi
.DOCX, .XLSX Microsoft Office user documents	.DOCX, .XLSX Microsoft Office user documents
.EXE Executable program file	.EXE Executable program file
.MSI Microsoft installer file	.MSI Microsoft installer file
.MSP Windows installer patch file	.MSP Windows installer patch file
.SCR Windows screen saver	.SCR Windows screen saver
.CPL Windows Control Panel file	.CPL Windows Control Panel file
.MSC Microsoft Management Console file	.MSC Microsoft Management Console file
.WSF Windows script file	.WSF Windows script file
.REG Windows registry file	.REG Windows registry file
.PS1 Windows PowerShell script	.PS1 Windows PowerShell script

Worm

Worm adalah jenis malware kedua yang tujuan utamanya adalah menyebar. Worm adalah program jahat yang menggunakan jaringan komputer untuk mereplikasi (worm kadang-kadang disebut virus jaringan). Worm dirancang untuk memasuki komputer melalui jaringan dan kemudian memanfaatkan

kerentanan dalam suatu aplikasi atau sistem operasi pada komputer host. Setelah worm mengeksploitasi kerentanan pada satu sistem, ia segera mencari komputer lain di jaringan yang memiliki kerentanan yang sama.

Salah satu serangan secara masal worms pertama terjadi pada tahun 1988. worms ini mengeksploitasi kesalahan konfigurasi dalam program yang mengizinkan perintah di email ke sistem jarak jauh untuk dieksekusi pada sistem itu, dan itu juga membawa muatan yang berisi program yang berusaha untuk menentukan password pengguna. Hampir 6000 komputer, atau 10 persen perangkat yang terhubung ke Internet pada waktu itu, adalah terpengaruh. Serangan worms itu dikaitkan dengan Robert T. Morris, Jr., yang kemudian dihukum karena kejahatan federal sehubungan dengan kejadian serangan ini.

Pada awalnya worm dibuat tidak untuk merusak secara fatal dan dirancang hanya untuk menyebar dengan cepat dan tidak membuat kerusakan sistem yang diinfeksi. Worms ini memperlambat jaringan yang mereka lewati dengan mereplikasi dirinya dengan begitu cepat sehingga mereka menghabiskan semua sumber daya di jaringan. Saat ini worm dapat meninggalkan dirinya pada sistem yang mereka infeksi dan menyebabkan kerusakan, seperti virus. Tindakan yang dilakukan worm termasuk menghapus file di komputer atau mengizinkan komputer yang akan dikendalikan dari jarak jauh oleh penyerang.

Trojan

Menurut legenda kuno, orang Yunani memenangkan Perang Troya dengan menyembunyikan tentara di sebuah kuda kayu berongga besar yang dikirimkan untuk menyerang kota Troy. Kuda didorong ke benteng kota, para prajurit merayap keluar dari kuda pada malam hari dan menyerang pasukan yang berjaga.

Kuda Trojan komputer (atau hanya Trojan) adalah program komputer yang dapat dieksekusi dan menyamar untuk melakukan aktivitas yang tidak berbahaya tetapi juga melakukan sesuatu yang berbahaya. Misalnya, pengguna mungkin unduh apa yang diiklankan di E-Mail sebagai aplikasi kalender, tetapi ketika di instal, selain menginstal kalender, aplikasi juga menginstal malware yang dapat memindai sistem untuk pelacakan nomor kartu kredit dan kata sandi, kemudian menghubungkan melalui jaringan ke sistem jarak jauh, dan kemudian mentransmisikannya informasi kepada penyerang.

Tabel 3.2: Perbedaan Antara Virus, Worm, dan Trojan (Ciampa, 2015)

Aksi	Virus	Worm	Trojan
Apa yang dapat dilakukan?	Memasukkan kode berbahaya ke dalam program atau data file	Eksplorasi kerentanan di dalam aplikasi atau pada sistem operasi	Melakukan penyamaran tetapi juga dapat langsung melakukan serangan berbahaya
Bagaimana penyebaran ke komputer lain	Pengguna mentransfer file yang terinfeksi ke perangkat lain	Menggunakan jaringan untuk berpindah dari satu komputer ke komputer lain	Pengguna mentransfer file trojan untuk ke komputer lain
Apakah menginfeksi file	Ya	Tidak	Ya
Apakah membutuhkan aksi dari <i>user</i> untuk menyebar	Tidak	Tidak	Ya

Concealment

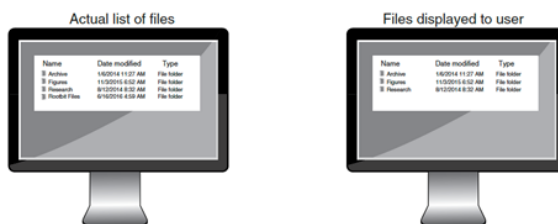
Beberapa jenis malware dapat menghindari deteksi dari anti-malware (Ashari, 2021). Jenis yang paling umum dari *concealment* malware pertama kali yang menarik perhatian publik adalah malware pada media CD musik. Pada akhir tahun 2005, Sony BMG Music Entertainment mengejutkan dunia komputer dan musik, dengan menginstal secara diam-diam perangkat lunak tersembunyi di komputer yang memutar salah satu dari 50 CD musik Sony.

Perangkat lunak yang dipasang Sony dimaksudkan untuk mencegah penyalinan CD musik. CD ini membuat direktori tersembunyi, menginstal perangkat lunak driver perangkat mereka sendiri di komputer, dan kemudian mengalihkan fungsi normal dari Microsoft Windows ke rutinitas Sony sendiri. Setelah perilaku jahat ini terungkap, Sony terpaksa mundur dan menarik CD dari pasar.

Apa yang dilakukan Sony adalah menginstal *rootkit* di komputer tempat CD diputar. Sebuah *rootkit* adalah perangkat lunak yang digunakan untuk menyembunyikan tindakan atau keberadaan jenis perangkat lunak lain yang diikutsertakan. *Rootkit* dapat mengubah konfigurasi sistem operasi untuk memaksanya mengabaikan file atau aktivitas berbahaya yang sedang dilakukan. *Rootkit* juga dapat menyembunyikan atau menghapus semua jejak bukti yang dilakukan oleh malware, seperti entri log.

Salah satu pendekatan yang digunakan oleh *rootkit* adalah mengubah atau mengganti file sistem operasi dengan yang dimodifikasi versi yang secara khusus dirancang untuk mengabaikan bukti berbahaya. Misalnya, pemindaian perangkat lunak dapat diinstruksikan untuk memindai semua file dalam direktori tertentu. Untuk melakukan ini, perangkat lunak pemindaian akan menerima daftar file tersebut dari sistem operasi. Sebuah *rootkit* akan mengganti daftar file akurat sistem operasi dengan rutinitas *rootkit* sendiri sehingga tidak menampilkan file berbahaya.

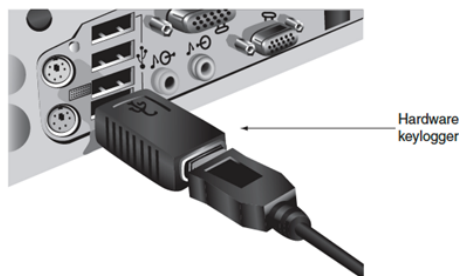
Hal ini diilustrasikan pada Gambar 3.2 Antivirus mengasumsikan tidak tahu bahwa komputer hanya menyediakan file yang telah disetujui rootkit. intinya, pengguna tidak bisa lagi mempercayai bahwasanya komputer mereka berisi *rootkit*.



Gambar 3.2: Komputer Terinfeksi Dengan Rootkit (Ciampa, 2015)

Payload Capabilities

Kekuatan merusak dari malware ditentukan oleh muatan yang dibawa oleh malware tersebut. Muatan utama dari malware kemampuannya adalah mengumpulkan data, menghapus data, mengubah pengaturan keamanan sistem, dan meluncurkan serangan (Ashari, 2018).



Gambar 3.3: Perangkat Keras Keylogger (Ciampa, 2015)

Adware

Adware dapat mengirimkan konten iklan dengan cara yang tidak disangka-disangka dan tidak diinginkan oleh pengguna. Setelah malware dari adware terinstal, biasanya akan menampilkan iklan popup atau bahkan bisa membuka jendela browser web baru secara acak. Pengguna umumnya menolak adware karena:

Adware dapat menampilkan konten yang tidak pantas, seperti situs perjudian atau pornografi. Iklan popup yang sering muncul dapat mengganggu produktivitas pengguna. Iklan popup dapat memperlambat komputer atau bahkan menyebabkan crash dan hilangnya data.

Beberapa adware lebih dari sekadar memengaruhi pengalaman komputer pengguna. Ini karena adware program juga dapat melakukan fungsi pelacakan, yang memantau dan melacak pengguna lewat aktivitas online dan kemudian mengirimkan log aktivitas ini ke pihak ketiga tanpa izin pengguna atau pengetahuan.

Misalnya, pengguna yang mengunjungi situs mobil online untuk melihat jenis mobil dapat dilacak oleh adware dan diklasifikasikan sebagai seseorang yang tertarik untuk membeli mobil yang baru. Berdasarkan urutan dan jenis situs web yang dikunjungi, adware juga dapat menentukan: apakah perilaku pengguna menunjukkan bahwa mereka memiliki ketertarikan terhadap sesuatu. Informasi ini dikumpulkan oleh adware dan kemudian dijual ke showroom mobil pengiklan.

Ransomware

Salah satu jenis malware terbaru dan paling cepat berkembang adalah ransomware. Ransomware mencegah perangkat pengguna beroperasi dengan benar sampai pengguna menebus dengan biaya tertentu. Ransomware dapat mengunci komputer pengguna dan kemudian menampilkan pesan seolah berasal dari lembaga penegak hukum.

Pesan ini, menggunakan citra resmi, menyatakan bahwa pengguna telah melakukan tindakan ilegal seperti mengunduh pornografi dan harus segera membayar denda online dengan memasukkan nomor kartu kredit. Komputer tetap dikunci (kecuali keyboard) sampai tebusan pembayaran dilakukan. Gambar 3.4 menunjukkan pesan ransomware dari situs web Symantec di Pusat Respon Keamanan.



Gambar 3.4: Pesan Ransomware (Sumber: <https://www.knowbe4.com/locker-ransomware>)

Malware Ransomware dapat sangat menguntungkan. Dengan perkiraan hampir 3 persen dari pengguna tersebut yang telah terinfeksi dan membayar uang tebusan dapat menghasilkan hampir 5\$ juta per tahun dari korban yang diperas. Karena tingkat keberhasilannya yang tinggi, penyerang memperluas kemampuan malware ini. Bukan hanya menampilkan pesan di layar, bahkan ada varian ransomware yang dapat memutar pesan yang direkam melalui speaker komputer menggunakan pesan suara regional dan semipersonal.

Variasi lain menampilkan peringatan fiktif bahwa ada masalah dengan komputer seperti infeksi malware atau kegagalan hard-drive yang terjadi. Tidak penting bagaimana kondisi komputer yang sebenarnya, ransomware selalu melaporkan bahwa ada masalah. Variasi ransomware ini memberi tahu pengguna bahwa mereka harus segera membeli tambahan software online untuk memperbaiki masalah yang sebenarnya tidak ada.

Peringatan itu tampaknya sah karena meniru tampilan asli dan secara tidak sah menggunakan merek dagang atau ikon yang sah. Contoh ransomware pada Gambar 3.5 menggunakan skema warna dan ikon serupa dengan yang ditemukan pada perangkat lunak Windows yang sah. Pengguna yang memberikan nomor kartu kredit mereka untuk melakukan pembelian menemukan bahwa penyerang hanya menangkap informasi itu dan kemudian menggunakan nomor kartu untuk tujuan mereka sendiri.



Gambar 3.5: Infeksi Ransomware Komputer (Sumber:

<https://www.zdnet.com/article/wannacry-ransomware-attack-at-lg-electronics-takes-systems-offline/>)

Modifikasi Keamanan Sistem

Beberapa jenis malware mencoba untuk memodifikasi pengaturan keamanan sistem sehingga serangan yang lebih berbahaya dapat dilakukan. Salah satu jenis malware dalam kategori ini disebut backdoor.

Backdoor memberikan akses ke komputer, program, atau layanan untuk menghindari aplikasi deteksi keamanan. Pintu belakang yang dipasang di komputer memungkinkan penyerang untuk kembali di lain waktu dan melewati pengaturan keamanan.

Social Engineering Attack

Suatu pagi sekelompok kecil orang asing berjalan ke kantor perusahaan pengiriman dan segera keluar dengan akses ke seluruh jaringan komputer perusahaan, yang berisi informasi yang berharga dan sangat sensitif.

Mereka mampu mencapai ini tanpa alat atau keterampilan teknis:

1. Sebelum memasuki gedung, satu orang dari kelompok itu memanggil Sumber Daya Manusia (SDM) di kantor dan menanyakan nama-nama karyawan yang penting. Kantor dengan sukarela memberikan informasi tanpa mengajukan pertanyaan.
2. Saat kelompok berjalan ke gedung, salah satu dari mereka berpura-pura kehilangan akses kode kunci ke pintu, jadi karyawan yang

ramah membiarkan mereka masuk. Ketika mereka memasuki area aman di lantai tiga, mereka mengaku salah menaruh lencana identitas mereka, jadi karyawan yang lain membuka pintu untuk mereka.

3. Karena orang asing ini tahu bahwa *Chief Financial Officer* (CFO) sedang berada di luar kota karena pesan suaranya, mereka berjalan tanpa hambatan ke kantornya dan mengumpulkan informasi dari komputernya yang tidak terlindungi. Mereka juga menggali informasi dari tempat sampah dan mengambil dokumen yang berguna. Seorang penjaga bahkan dihentikan dan meminta sebuah kotak untuk meletakkan dokumen-dokumen ini agar bisa dibawa keluar bangunan.
4. Salah satu anggota kelompok kemudian menelepon *helpdesk* perusahaan dari kantor CFO dan berpura-pura menjadi CFO (mereka telah mendengarkan suaranya dari salam pesan suaranya dan tahu bagaimana dia berbicara). CFO penipu mengklaim bahwa dia putus asa untuk menemukan kata sandinya karena dia lupa dan sedang dalam perjalanan ke tempat pertemuan yang penting. *Help desk* memberikan kata sandi, dan kelompok itu meninggalkan gedung dengan akses penuh ke jaringan. Kisah nyata ini menggambarkan bahwa teknologi tidak selalu dibutuhkan untuk menyerang. Sosial Engineering adalah sarana mengumpulkan informasi untuk serangan dengan mengandalkan kelemahan dari sisi psikologis individu. *Social Engineering Attack* dapat melibatkan pendekatan psikologis serta prosedur fisik.

Psychology Approach

Banyak *social engineering attacks* mengandalkan dari aspek psikologi, yaitu mental dan emosional daripada serangan berbasis fisik. Pada intinya, *social engineering* bergantung pada penyerang untuk melakukan manipulasi dengan memanfaatkan sifat manusia untuk membujuk korban sehingga memberikan informasi atau mengambil tindakan.

Beberapa “prinsip” atau alasan dasar membuat psikologis sosial rekayasa ini berjalan efektif. Ini tercantum dalam Tabel 3.3 dengan contoh penyerang yang

berpura-pura untuk menjadi *Chief Executive Officer* (CEO) memanggil *helpdesk* untuk memiliki pengaturan ulang kata sandi.

Tabel 3.3: Efektivitas Social Engineering (Ciampa, 2015)

Prinsip	Deskripsi	Contoh
<i>Authority</i>	Meniru identitas seseorang yang memiliki wewenang dan jabatan tertentu.	“Panggilan saya adalah CEO
<i>Intimidation</i>	Intimidasi untuk menakuti dan mengancam seseorang untuk melakukan aksi sesuai perintah	“ Jika kamu tidak reset password saya, saya akan panggil supervisor kamu“
<i>Consensus/ Social Proof</i>	Dipengaruhi oleh apa yang orang lain lakukan	“saya menelepon rekan anda minggu lalu dan rekan Anda mengatur ulang kata sandi saya“
<i>Urgency</i>	Berdasarkan tindakan yang perlu segera dilakukan	Rapat saya akan segera dimulai 5 menit lagi
<i>Trust</i>	Kepercayaan diri	„kamu tahu kan saya siapa“

Karena banyak pendekatan psikologis melibatkan kontak orang-ke-orang, penyerang menggunakan berbagai teknik untuk mendapatkan kepercayaan tanpa bergerak cepat sehingga menjadi curiga.

Peniruan Identitas

Social Engineering berarti menyamar sebagai individu nyata atau fiktif karakter dan kemudian memainkan peran orang itu pada korban. Misalnya, penyerang dapat menyamar sebagai teknisi *help desk* yang memanggil korban, berpura-pura bahwa ada masalah dengan jaringan, dan meminta nama pengguna dan kata sandinya untuk mengatur ulang akun.

Peran umum yang sering ditiru termasuk tukang reparasi, dukungan TI, manajer, pihak ketiga yang terpercaya, atau sesama karyawan. Sering kali penyerang akan menyamar sebagai individu yang perannya otoritatif karena korban umumnya menolak mengatakan "tidak" kepada siapa pun di kekuasaan.

Salah satu bentuk *social engineering* yang paling umum adalah phishing. Phishing adalah mengirim E-Mail atau menampilkan pengumuman web yang mengklaim berasal dari perusahaan yang sah dalam upaya untuk mengelabui pengguna agar menyerahkan informasi pribadi. Pengguna diminta untuk menanggapi E-Mail atau diarahkan ke situs web tempat mereka diminta untuk memperbarui informasi pribadi, seperti kata sandi, nomor kartu kredit, Nomor Jaminan Sosial, nomor rekening bank, atau informasi lainnya.

Namun, E-Mail atau situs web sebenarnya adalah penipuan dan diatur untuk mencuri informasi apa yang pengguna masuk. Salah satu alasan keberhasilan phishing adalah karena E-Mail dan situs web palsu tampak menjadi sah. Gambar 3.6 mengilustrasikan pesan E-Mail phishing aktual yang mengklaim korban baru-baru ini melakukan pembayaran dengan jumlah yang besar kepada seseorang.

Pesan berisi logo, warna skema, dan kata-kata yang digunakan oleh situs yang sah sehingga tampak asli. Korban secara alami akan bingung dengan pesan ini dan mengklik tautan, yang kemudian akan meminta nama pengguna dan kata sandi untuk masuk, tetapi alih-alih mengakses situs yang sah, informasi ini ditangkap oleh penyerang.



Figure 2-8 Phishing email message
Source: Email sent to Dr. Mark Revets

Gambar 3.6: E-Mail Phising

Banyak serangan phishing memiliki fitur umum berikut:

1. Tautan web yang menipu
Phisher suka menggunakan variasi alamat yang sah, seperti www.ebay_secure.com, www.ebay.com, atau www.e-baynet.com.
2. Logo. Phisher sering menyertakan logo vendor dan mencoba membuat E-Mail terlihat seperti situs web vendor sebagai cara untuk meyakinkan penerima bahwa itu asli.

3. Permintaan yang penting

Banyak E-Mail phishing menyertakan instruksi bagi penerima untuk bertindak segera atau akun mereka tidak akan tersedia atau sejumlah besar uang akan dipotong dari akun mereka.

Beberapa variasi serangan phishing adalah:

1. Pharming

Bukannya meminta pengguna untuk mengunjungi situs web palsu, pharming secara otomatis mengarahkan pengguna ke situs palsu. Hal ini dilakukan oleh penyerang untuk menembus server di Internet dan mengarahkan lalu lintas atau mengubah file di komputer host.

2. Spear Phishing

Phishing melibatkan pengiriman jutaan pesan E-Mail secara acak kepada pengguna, *spear phishing* hanya menargetkan kepada pengguna tertentu. E-Mail yang digunakan dalam *spear phishing* disesuaikan dengan penerima, termasuk nama dan informasi pribadi mereka, sehingga membuat pesan tampak sah.

3. Whaling

Salah satu jenis *spear phishing* adalah *whaling*. Tidak memancing "ikan kecil", *whaling* menargetkan "ikan besar", yaitu, seseorang yang kaya atau eksekutif dalam bisnis yang biasanya memiliki jumlah uang yang lebih besar di rekening bank yang dapat diakses penyerang jika serangan berhasil.

4. Vishing

Bukannya menggunakan E-Mail untuk menghubungi calon korban, melainkan menggunakan panggilan telepon yang dapat digunakan sebagai gantinya. Dikenal sebagai *phishing* (phishing suara), penyerang menelepon korban, saat menjawab, mendengar pesan rekaman yang berpura-pura dari pengguna bank yang menyatakan bahwa kartu kreditnya telah mengalami aktivitas penipuan atau bahwa dia rekening bank memiliki aktivitas yang tidak biasa.

Korban diinstruksikan untuk memanggil nomor telepon tertentu segera (yang telah diatur oleh penyerang). Ketika panggilan korban, dijawab dengan instruksi otomatis yang menyuruhnya memasukkan

nomor kartu kreditnya, nomor rekening bank, nomor Jaminan Sosial, atau informasi lainnya pada papan tombol telepon.

Spam

Spam adalah E-Mail yang tidak diminta. Google memperkirakan bahwa 9 dari setiap 10 pesan E-Mail adalah spam. Alasan mengapa pengguna menerima begitu banyak pesan spam yang mengiklankan produk atau item untuk dijual, karena mengirim spam adalah bisnis yang menguntungkan dan murah. Spammer membutuhkan biaya yang sangat kecil untuk mengirim jutaan E-Mail spam.

Di masa lalu, spammer akan membeli daftar alamat E-Mail yang valid (\$100 untuk 10 juta alamat) dan sewa kamar motel dengan koneksi internet berkecepatan tinggi (\$85 per hari) sebagai basis untuk meluncurkan serangan. Namun, hari ini, hampir semua spam dikirim dari botnet, spammer yang tidak memiliki botnetnya sendiri dapat menyewa dari penyerang lain (\$40 per jam) untuk menggunakan botnet hingga 100.000 komputer yang terinfeksi untuk meluncurkan serangan spam.

Bahkan jika spammer hanya menerima persentase tanggapan yang sangat kecil, mereka tetap mendapat untung besar. Sebagai contoh, jika seorang spammer mengirim spam ke 6 juta pengguna untuk produk dengan harga jual \$50 yang harganya hanya \$5 untuk membuat, dan jika hanya 0,001 persen dari penerima yang menanggapi dan membeli produk (biasanya bergantung dari tingkat respons pengguna), spammer masih dapat menghasilkan keuntungan lebih dari \$270.000.



Gambar 3.7: Gambar Spam

Pesan spam berbasis teks menyertakan kata-kata seperti Viagra atau investasi dapat dengan mudah dipindai oleh spam filter yang dapat mencari kata-kata ini dan memblokir E-Mail. Karena peningkatan penggunaan spam filter ini, spammer telah beralih ke spam gambar, yang menggunakan gambar grafis teks dalam untuk menghindari filter berbasis teks. Spam gambar tidak dapat di filter berdasarkan konten tekstual pesan karena muncul sebagai gambar, bukan teks. Gambar 3.7 menunjukkan contoh spam gambar.

Selain mengganggu, spam secara signifikan mengurangi produktivitas kerja saat pengguna menghabiskan waktu membaca dan menghapus pesan spam. Salah satu risiko terbesar dari spam adalah spam dapat digunakan untuk menyebarkan malware secara luas.

Bab 4

Arsitektur Keamanan Siber

4.1 Pendahuluan

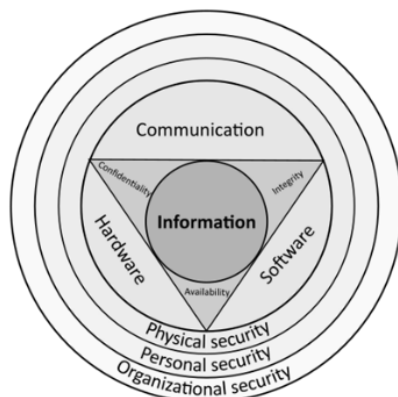
Pada beberapa bab sebelumnya, kita sudah membahas mengenai dasar-dasar keamanan siber, hukum dan regulasi siber, hingga ancaman keamanan siber. Dan mengapa hal tersebut penting? Dikarenakan dengan semakin meningkatnya pengguna internet jaman sekarang (Kemp, 2021), dibutuhkan sebuah rancangan regulasi yang dapat menjaga keamanan informasi yang dibagikan melalui Internet (Sepis, 2022).

Beberapa serangan umum yang mungkin terjadi biasanya dikarenakan adanya kesalahan dari pengguna, di mana pengguna lalai untuk menjaga informasi pribadi atau informasi sensitif. Atau dengan kurangnya literasi terhadap cara melakukan pertukaran informasi yang aman di internet (Sihotang, 2021). Ancaman terhadap keamanan informasi berasal dari berbagai sumber dan dengan berbagai variasi.

Ancaman yang paling umum sekarang ini adalah pencurian properti intelektual, pencurian identitas, sabotase, hingga kebocoran informasi. Beberapa serangan yang terencana seperti *Distributed Denial of Service*, *Brute Force*, *Adware*, *Ransomware*, *Trojan*, *Spam*, *Worm*, *Botnet*, dan lainnya. Keamanan informasi adalah sebuah praktek melindungi informasi dari berbagai ancaman yang mungkin terjadi. Umumnya keamanan informasi

termasuk ke dalam manajemen risiko informasi yang mencakup pencegahan akses tidak sah terhadap data, penggunaan informasi yang tidak sesuai hukum, penghancuran atau perubahan data tanpa otoritas, hingga pencegahan lebih lanjut yang melibatkan keamanan jaringan secara fisik dan tata kelola teknologi informasi (Gold, 2004).

Fokus utama dari keamanan informasi adalah untuk mencapai perlindungan yang seimbang terhadap kerahasiaan, integritas, dan ketersediaan data, sementara berfokus kepada aturan implementasi tanpa mengurangi produktivitas organisasi.



Gambar 4.1: Tiga Serangkai Keamanan Informasi (Kennedy, 2009)

Gambar 4.1 di atas menjelaskan mengenai pentingnya keseimbangan dari tiga serangkai keamanan informasi yaitu Kerahasiaan, Integritas, dan Ketersediaan baik dari aspek perangkat keras, perangkat lunak, hingga jalur komunikasi yang dibungkus dalam keamanan secara fisik, keamanan secara personal, dan keamanan secara organisasi.

1. Kerahasiaan adalah sebuah properti dari informasi yang tidak tersedia atau tertutup hanya untuk individu yang memiliki otoritas terhadap data tersebut.
2. Integritas dalam sebuah data terbentuk dengan adanya pengawasan dan penjaminan akurasi dan kelengkapan data dalam setiap transmisi data. Dalam hal ini, integritas dari data melibatkan individu, proses, komersial, dan juga mencakup beberapa aspek seperti kredibilitas,

konsistensi, kejujuran, kelengkapan, akurasi, ketepatan waktu, dan penjaminan mutu dari informasi tersebut.

3. Ketersediaan bukan hanya berarti ada ketika dibutuhkan. Namun hal ini mencakup sistem komputasi yang digunakan dalam menyimpan, dan mendistribusikan informasi dalam lingkungan kontrol keamanan informasi baik secara fisik, individu, atau aturan dalam organisasi.

Dewasa ini, ketersediaan dari informasi merupakan hal yang vital dan kerap dijadikan sebuah parameter terhadap kesuksesan implementasi tata Kelola TI, manajemen risiko, dan Teknik lainnya dalam mengamankan data. Bahkan di perusahaan perbankan, hilangnya akses terhadap data beberapa detik dapat mengakibatkan kerugian yang besar bagi perusahaan tersebut. Bagi orang awam, reliabilitas dari sebuah situs atau sistem akan dinilai terlebih dahulu dari seberapa jarang sistem/situs tersebut tidak dapat diakses.



Gambar 4.2: Manajemen Risiko Keamanan Informasi

Keseimbangan antara tiap komponen dalam tiga serangkai keamanan informasi dapat terjadi dengan melakukan proses manajemen risiko (Randall, 2011) berikut:

1. melakukan identifikasi terhadap informasi dan aset terkait, termasuk potensi ancaman, kelemahan dari sistem, hingga dampak dari ancaman tersebut;

2. melakukan evaluasi dari setiap risiko tersebut;
3. mengambil keputusan terhadap bagaimana cara mengatasi masing-masing ancaman yang sudah dievaluasi;
4. melakukan implementasi mitigasi risiko dengan memilih atau merancang kontrol keamanan yang sesuai;
5. melakukan pengawasan terhadap aktivitas manajemen risiko, dan secara berkala melakukan penyesuaian terhadap tingkat ancaman yang ada.

4.2 Arsitektur Keamanan Informasi

Menurut (NIST, 2012), arsitektur keamanan informasi adalah sebuah struktur dan sikap dari proses keamanan perusahaan, sistem keamanan informasi, personal dan organisasional dalam penyesuaian terhadap misi dan rencana strategis perusahaan. Arsitektur keamanan informasi juga dapat diartikan sebagai sebuah praktik dari aplikasi metode yang komprehensif terhadap proses dan sistem keamanan informasi yang bertujuan untuk mendukung operasional bisnis, manajemen operasi, hingga proses arsitektur keamanan itu sendiri.

Adapun yang menjadi tujuan dari arsitektur keamanan informasi adalah:

1. memberikan struktur, koherensi dan kohesivitas;
2. mengaktifkan penyesuaian bisnis-ke-keamanan;
3. ditetapkan secara top-down dimulai dengan strategi bisnis;
4. memastikan bahwa semua model dan implementasi dapat ditelusuri kembali ke strategi bisnis, persyaratan bisnis spesifik, dan prinsip-prinsip utama;
5. berikan abstraksi sehingga faktor-faktor yang memperumit, seperti geografi dan prinsip teknologi, dapat dihapus dan dikembalikan pada tingkat detail yang berbeda hanya jika diperlukan;
6. menetapkan "bahasa" umum untuk keamanan informasi di dalam organisasi.

Dalam praktiknya, dibutuhkan sebuah metodologi dalam mengembangkan arsitektur keamanan informasi guna menentukan kondisi sekarang, kondisi yang seharusnya, dan target aktual yang diselaraskan dengan manajemen perubahan dalam bisnis tersebut. Kerangka kerja ini akan memberikan taksonomi dan ontologi yang ketat yang secara jelas mengidentifikasi proses apa yang dilakukan bisnis dan informasi terperinci tentang bagaimana proses tersebut dijalankan dan diamankan.

Produk akhir dari kerangka kerja ini adalah seperangkat artefak yang menjelaskan dalam berbagai tingkat detail persis apa dan bagaimana bisnis beroperasi dan kontrol keamanan apa yang diperlukan. Artefak ini sering digambarkan dalam bentuk grafik (NIST, 2012).



Gambar 4.3: Hubungan Antar Arsitektur

Menerapkan arsitektur keamanan informasi perusahaan umumnya dimulai dengan mendokumentasikan strategi organisasi dan detail lain yang diperlukan seperti di mana dan bagaimana operasinya. Proses kemudian mengalir ke bawah untuk mendokumentasikan kompetensi inti yang terpisah, proses bisnis, dan bagaimana organisasi berinteraksi dengan dirinya sendiri dan dengan pihak eksternal seperti pelanggan, pemasok, dan entitas pemerintahan.

Beberapa komponen yang didokumentasikan adalah alir proses bisnis, aktivitas bisnis, siklus hidup bisnis, manajemen rantai persediaan, inventori dari perangkat lunak, jaringan komunikasi, klasifikasi data dan basis data, komponen fisik keamanan jaringan komunikasi, dan lainnya.

Hasil antara dari proses arsitektur adalah inventaris yang komprehensif dari strategi keamanan bisnis, proses keamanan bisnis, bagan organisasi, inventaris keamanan teknis, diagram sistem dan antarmuka, dan topologi jaringan, dan hubungan eksplisit diantara komponen yang sudah disebutkan. Inventarisasi dan diagram hanyalah alat yang mendukung pengambilan keputusan. Tapi hal ini tidak cukup. Proses arsitektur harus menjadi proses yang hidup.

Dalam hal ini, Organisasi harus merancang dan mengimplementasikan proses yang memastikan pergerakan terus-menerus dari keadaan saat ini ke keadaan masa depan.

Hal ini dapat tercapai dengan cara:

1. Menutup kesenjangan yang ada antara strategi organisasi saat ini dan kemampuan dimensi keamanan TI untuk mendukung strategi organisasi
2. Menutup kesenjangan yang ada antara strategi organisasi “masa depan” yang diinginkan dan kemampuan dimensi keamanan untuk mendukungnya
3. Peningkatan dan penggantian yang diperlukan yang harus dilakukan pada arsitektur keamanan TI berdasarkan kelangsungan hidup pemasok, usia dan kinerja perangkat keras dan perangkat lunak, masalah kapasitas, persyaratan peraturan yang diketahui atau diantisipasi, dan masalah lain yang tidak didorong secara eksplisit oleh manajemen fungsional organisasi.
4. Secara teratur, keadaan saat ini dan keadaan yang diharapkan (masa depan) didefinisikan ulang untuk memperhitungkan evolusi arsitektur, perubahan strategi organisasi, dan faktor eksternal murni seperti perubahan dalam hal teknologi dan persyaratan pelanggan/vendor/pemerintah, dan perubahan baik internal maupun eksternal. lanskap ancaman eksternal dari waktu ke waktu.

4.3 Arsitektur Keamanan Siber

Arsitektur keamanan siber, juga dikenal sebagai arsitektur keamanan jaringan, adalah praktik merancang sistem komputer untuk memastikan keamanan data. Secara umum, arsitektur keamanan siber adalah fondasi pertahanan organisasi terhadap ancaman keamanan.

Bekerja sebagai salah satu komponen arsitektur keamanan organisasi secara keseluruhan, arsitektur keamanan siber biasanya dirancang menggunakan kerangka arsitektur keamanan siber – yaitu, kerangka kerja yang menentukan struktur, standar, kebijakan, dan perilaku fungsional jaringan komputer, termasuk tindakan keamanan dan jaringan. fitur.

Kerangka kerja akan membantu organisasi dalam mengidentifikasi risiko keamanan dan kemudian memosisikan kontrol keamanan untuk mengatasinya (National Institute of Standards and Technology, 2018). Kerangka ini juga akan menunjukkan kepada perusahaan bagaimana kontrol keamanan perusahaan berhubungan dengan bisnis secara keseluruhan.

Idealnya, kerangka arsitektur keamanan siber akan memungkinkan organisasi untuk menjaga kerahasiaan, integritas, dan ketersediaan data dalam operasi bisnisnya. Kerangka arsitektur keamanan siber harus cukup fleksibel untuk beradaptasi dan menyediakan cakupan keamanan untuk bisnis meskipun lanskap ancaman siber terus berkembang. Ini harus mencakup tiga elemen utama, yang akan kita jelajahi lebih lanjut sebentar lagi: elemen prosedural dan terkait kebijakan, standar dan kerangka kerja, dan elemen keamanan dan jaringan.

Sebagian besar bisnis sudah memiliki setidaknya beberapa elemen keamanan siber, termasuk *firewall*, program antivirus, dan sistem deteksi intrusi. Arsitektur keamanan siber yang terperinci harus mengintegrasikan elemen-elemen ini untuk memelihara dan memaksimalkan alat-alat ini di samping kebijakan dan prosedur bisnis.

Meskipun demikian, *firewall*, program antivirus, dan sistem deteksi intrusi hanya mengatasi ancaman eksternal – yang tidak cukup di lingkungan ancaman modern. Untuk alasan ini, banyak organisasi menggunakan model “zero trust”, yang meminta verifikasi setiap permintaan terlepas dari apakah pengguna berada di dalam atau di luar perimeter. Dengan menggunakan

kontrol akses dan membangun beberapa pos pemeriksaan dalam jaringan, organisasi dapat membatasi paparan mereka terhadap infiltrasi malware.

Meskipun bisnis dapat dan harus berbuat lebih banyak untuk membangun sistem keamanan jaringan secara mandiri, banyak yang tidak memiliki teknologi yang diperlukan untuk melakukannya. Jika hal ini terdengar kompleks, perusahaan mungkin ingin mempertimbangkan untuk menyewa seorang arsitek keamanan siber: seorang profesional keamanan yang akan membantu perusahaan mengantisipasi potensi ancaman siber, dan merancang struktur dan sistem yang akan mencegahnya. Bagi banyak organisasi, menyewa arsitek keamanan siber adalah cara terbaik untuk mengidentifikasi kerentanan sistem dan memulihkannya secepat mungkin.

Berdasarkan Ross, McEvilley and Oren (2018), Arsitektur keamanan siber yang efektif dan efisien terdiri dari tiga komponen utama. Yaitu orang, proses, dan alat yang bekerja sama untuk melindungi aset perusahaan. Untuk menyelaraskan komponen ini secara efektif, arsitektur keamanan perusahaan perlu didorong oleh kebijakan keamanan. menyatakan ekspektasi arsitektur keamanan perusahaan, rencana implementasi, dan proses penegakan hukum.

Kebijakan keamanan adalah pernyataan yang menguraikan bagaimana setiap entitas mengakses satu sama lain, operasi apa yang dapat dilakukan oleh berbagai entitas, tingkat perlindungan yang diperlukan untuk suatu sistem serta tindakan yang harus diambil ketika persyaratan keamanan ini tidak terpenuhi.

Komponen yang tercantum di bawah ini adalah bagian dari arsitektur keamanan yang efektif dan direncanakan dengan cermat:

1. pengarahan di bidang respons insiden terhadap ancaman, pemulihan bencana, konfigurasi sistem, pembuatan dan pengelolaan akun, dan pemantauan keamanan siber;
2. manajemen identitas;
3. memutuskan penyertaan dan pengecualian dari mereka yang tunduk pada domain arsitektur keamanan;
4. akses dan kontrol perbatasan;
5. validasi dan penyesuaian arsitektur, dan;
6. pelatihan.

Tujuan arsitektur keamanan siber hanyalah untuk memastikan bahwa arsitektur jaringan utama perusahaan, termasuk data sensitif dan aplikasi

penting terlindungi sepenuhnya dari ancaman dan pelanggaran saat ini atau di masa mendatang. Penting bagi perusahaan untuk sepenuhnya memahami berbagai titik lemah dalam sistem perusahaan agar dapat menawarkan solusi secara efektif dan cepat.

Cara terbaik untuk mengidentifikasi titik lemah sistem perusahaan adalah dengan menggunakan jasa arsitek keamanan siber. Arsitek keamanan siber akan mengevaluasi kerentanan permukaan secara menyeluruh untuk topologi jaringan dan serangan siber yang berbeda untuk secara efektif mempertahankan data sensitif dan aplikasi penting perusahaan.

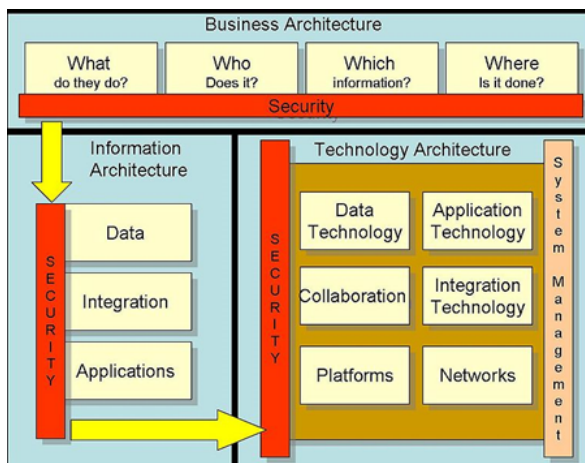
Tujuan utama dari arsitektur keamanan siber yang efektif adalah:

1. Untuk memastikan bahwa semua serangan siber diminimalkan, dimitigasi, baik yang tersembunyi atau dinamis.
2. Untuk memastikan bahwa permukaan serangan siber harus berukuran relatif kecil, disimpan secara rahasia, sehingga mereka diam-diam bergerak menuju target ancaman dan sulit untuk dideteksi dan ditembus oleh ancaman siber.
3. Untuk memastikan semua data rahasia dan sensitif Anda dienkripsi dengan kuat, dan tunduk pada teknik enkripsi ujung ke ujung selama transfer.
4. Semua serangan siber secara agresif dideteksi, dimitigasi, dan dilawan menggunakan tindakan pencegahan seperti *Moving-Target Defenses* (MTD).

4.4 Framework Keamanan Siber

Beberapa kerangka kerja (Framework) dari arsitektur keamanan siber adalah bagian kerangka kerja arsitektur perusahaan. Berikut ini adalah contoh dari beberapa kerangka kerja arsitektur perusahaan yang kerap digunakan: *The Open Group Architecture Framework* (TOGAF), *SABSA Framework & Methodology*, *NIST*, *ITIL*, *ISACA COBIT*, *Open Security Architecture*, *Zachman Framework*, dan lainnya.

Gambar 4.4 di bawah ini adalah contoh kerangka kerja keamanan dari *Enterprise Information Security Architecture (EISA)*.

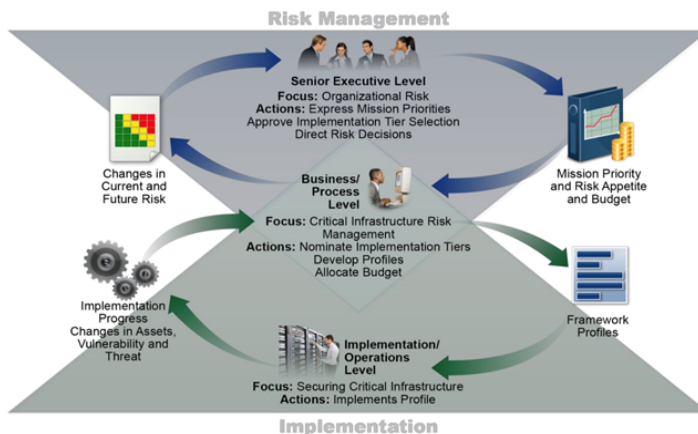


Gambar 4.4: Kerangka Kerja EISA (Huxham, 2006)

Alasan utama terbentuknya Framework Keamanan Siber adalah dikarenakan meningkatnya ancaman keamanan siber, yang menjadikan proteksi terhadap informasi vital menjadi lebih kompleks. Baik perlindungan aset informasi yang tidak terlihat atau pun sistem repositori atau sistem manajemen informasi secara virtual maupun perlindungan secara fisik terhadap infrastruktur aset vital tersebut (National Institute of Standards and Technology, 2018).

Anggota dari setiap sektor infrastruktur kritis menjalankan fungsi yang didukung oleh kategori luas teknologi, termasuk teknologi informasi (TI), sistem kontrol industri, sistem siber-fisik, dan perangkat yang terhubung secara lebih umum, termasuk *Internet of Things* (IoT).

Ketergantungan pada teknologi, komunikasi, dan interkoneksi ini telah mengubah dan memperluas potensi kerentanan dan meningkatkan potensi risiko terhadap operasi. Misalnya, karena teknologi dan data yang dihasilkan serta prosesnya semakin banyak digunakan untuk memberikan layanan penting dan mendukung keputusan bisnis/misi, potensi dampak insiden keamanan siber pada organisasi, kesehatan dan keselamatan individu, lingkungan, komunitas, dan ekonomi dan masyarakat yang lebih luas harus dipertimbangkan.



Gambar 4.5: Alur Informasi dan Keputusan Dalam Organisasi (National Institute of Standards and Technology, 2018)

Untuk mengelola risiko keamanan siber, diperlukan pemahaman yang jelas tentang penggerak bisnis organisasi dan pertimbangan keamanan khusus untuk penggunaan teknologinya. Karena risiko, prioritas, dan sistem setiap organisasi adalah unik, alat dan metode yang digunakan untuk mencapai hasil yang dijelaskan oleh kerangka kerja akan bervariasi.

Kerangka kerja tersebut akan tetap efektif dan mendukung inovasi teknis dikarenakan kerangka kerja bersifat netral dalam teknologi, sekaligus merujuk pada berbagai standar, pedoman, dan praktik yang ada yang berkembang seiring dengan perkembangan teknologi.

Dengan mengandalkan standar, pedoman, dan praktik global yang dikembangkan, dikelola, dan diperbarui oleh industri, maka alat dan metode yang tersedia untuk mencapai hasil kerangka kerja akan berskala lintas batas, mengakui sifat global risiko keamanan siber, dan berkembang seiring kemajuan teknologi dan bisnis persyaratan.

Penggunaan standar yang ada dan yang muncul akan memungkinkan skala ekonomi dan mendorong pengembangan produk, layanan, dan praktik efektif yang memenuhi kebutuhan pasar yang teridentifikasi. Persaingan pasar juga mendorong difusi yang lebih cepat dari teknologi dan praktik ini serta realisasi banyak manfaat oleh para pemangku kepentingan di sektor-sektor ini. Dibangun dari standar, pedoman, dan praktik tersebut,

Kerangka ini menyediakan taksonomi dan mekanisme umum bagi organisasi untuk:

1. menjelaskan status keamanan siber perusahaan saat ini;
2. menjelaskan status target perusahaan terhadap keamanan siber;
3. mengidentifikasi dan memprioritaskan peluang untuk perbaikan dalam konteks proses yang berkelanjutan dan berulang;
4. menilai kemajuan menuju keadaan target perusahaan;
5. berkomunikasi di antara pemangku kepentingan internal dan eksternal tentang risiko keamanan siber.

Bab 5

Keamanan Jaringan

5.1 Pendahuluan

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Perkembangan teknologi komputer, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke Internet. Sebagai akibat dari serangan itu, banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan kita.

Dalam perkembangan teknologi dewasa ini, sebuah informasi menjadi sangat penting bagi sebuah organisasi. Informasi tersebut biasanya dapat diakses oleh para penggunanya. Akan tetapi, ada masalah baru yang berakibat dari keterbukaan akses tersebut.

Masalah-masalah tersebut antara lain adalah sebagai berikut (Khasanah, 2016):

1. Pemeliharaan validitas dan integritas data atau informasi tersebut.
2. Jaminan ketersediaan informasi bagi pengguna yang berhak.
3. Pencegahan akses sistem dari yang tidak berhak.
4. Pencegahan akses informasi dari yang tidak berhak.

Dengan adanya masalah-masalah tersebut, maka secepat mungkin kita harus segera mengamankan jaringan komputer dari serangan. Dengan memanfaatkan berbagai teknik, khususnya Teknik keamanan dan pemeliharaan (maintenance), maka hadirilah solusi untuk pemeliharaan (maintenance) dengan menggunakan sistem operasi manajemen jaringan yang menyediakan berbagai fasilitas yang mendukung keamanan dan akses data jaringan. Sistem operasi ini juga menyediakan fasilitas dalam pengelolaan sistem dan network infrastruktur. Sistem operasi ini dinamakan “Untangle”.

Pada dasarnya segala kegiatan penyampaian informasi bisa saja dilakukan secara manual seperti yang sudah berlangsung jauh sebelum sistem jaringan khususnya jaringan secara lokal atau LAN (Local Area Network) dikembangkan dan direalisasikan dalam per komputeran kegiatan perkantoran perusahaan.



Gambar 5.1: Jaringan Komputer

Namun mengingat semakin terbatasnya waktu dalam menyajikan informasi maka sistem jaringan khususnya jaringan secara lokal atau LAN adalah alternatif yang tepat dan baik untuk dibangun pada sebuah perusahaan yang memiliki jumlah komputer yang banyak dan terletak dengan jarak yang berjauhan keberadaannya satu dengan lainnya. Komunikasi antar komputer secara jaringan lokal cukup dapat diandalkan untuk saling berbagi data dan informasi.

Banyak manfaat yang bisa diperoleh dengan pemanfaatan teknologi jaringan secara lokal atau Local Area Network ini di antaranya adalah efisiensi dan efektivitas, yaitu efisiensi waktu dan biaya serta efektivitas pemanfaatan informasi yang disampaikan (Gani, 2019).

Garfinkel, Spafford dan Schwartz (2003) bahwa keamanan komputer melingkupi empat aspek, yaitu:

1. Privacy
Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.
2. Integrity
Informasi tidak boleh diubah tanpa seizin pemilik informasi.
3. Authentication
Metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.
4. Availability
Ketersediaan hubungan dengan ketersediaan informasi ketika dibutuhkan.

5.2 Keamanan Jaringan Internet dan Firewall

Serangan terhadap keamanan sistem informasi (security attack) dewasa ini sering kali terjadi. Kejahatan computer (cyber crime) pada dunia maya sering kali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan (Tashiha, 2017).

Ada beberapa kemungkinan tipe dari serangan yang dilakukan oleh penyerang yaitu:

1. Interception yaitu pihak yang tidak mempunyai wewenang telah berhasil mendapatkan hak akses informasi.
2. Interruption yaitu penyerang telah dapat menguasai sistem, tetapi tidak keseluruhan. Admin asli masih bisa login.

3. Fabrication yaitu penyerang telah menyisipkan objek palsu ke dalam sistem target.
4. Modification yaitu penyerang telah merusak sistem dan telah mengubah secara keseluruhan.

Menurut David Icové, dilihat dari lubang keamanan yang ada pada suatu sistem, keamanan dapat diklasifikasikan menjadi empat macam:

Keamanan Fisik (Physical Security)

Suatu keamanan yang meliputi seluruh sistem beserta peralatan, periferal, dan media yang digunakan. Biasanya seorang penyerang akan melakukan *wiretapping* (proses pengawasan dan penyadapan untuk mendapatkan password agar bisa memiliki hak akses).

Jika gagal, maka DOS (Denial Of Service) akan menjadi pilihan sehingga semua servis yang digunakan oleh komputer tidak dapat bekerja. Sedangkan cara kerja DOS biasanya mematikan servis apa saja yang sedang aktif atau membanjiri jaringan tersebut dengan pesan-pesan yang sangat banyak jumlahnya.

Secara sederhana, DOS memanfaatkan celah lubang keamanan pada protokol TCP/IP yang dikenal dengan *Syn Flood*, yaitu sistem target yang dituju akan dibanjiri oleh permintaan yang sangat banyak jumlahnya (flooding), sehingga akses menjadi sangat sibuk.

Keamanan Data dan Media

Pada keamanan ini penyerang akan memanfaatkan kelemahan yang ada pada software yang digunakan untuk mengolah data. Biasanya penyerang akan menyisipkan virus pada komputer target melalui *attachment* pada e-mail. Cara lainnya adalah dengan memasang *backdoor* atau *trojan horse* pada sistem target.

Tujuannya untuk mendapatkan dan mengumpulkan informasi berupa password administrator. Password tersebut nantinya digunakan untuk masuk pada account administrator.

Keamanan Dari Pihak Luar

Memanfaatkan faktor kelemahan atau kecerobohan dari orang yang berpengaruh (memiliki hak akses) merupakan salah satu tindakan yang

diambil oleh seorang hacker maupun cracker untuk dapat masuk pada sistem yang menjadi targetnya.

Hal ini biasa disebut social engineering. Social engineering merupakan tingkatan tertinggi dalam dunia hacking maupun cracking. Biasanya orang yang melakukan social engineering akan menyamar sebagai orang yang memakai sistem dan lupa password, sehingga akan meminta kepada orang yang memiliki hak akses pada sistem untuk mengubah atau mengganti password yang akan digunakan untuk memasuki sistem tersebut.

Keamanan Dalam Operasi

Merupakan salah satu prosedur untuk mengatur segala sesuatu yang berhubungan dengan sistem keamanan pasca serangan. Dengan demikian, sistem tersebut dapat berjalan baik atau menjadi normal kembali. Biasanya para penyerang akan menghapus seluruh log-log yang tertinggal pada sistem target (log cleaning) setelah melakukan serangan.

Firewall atau tembok-api adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya. Tembok-api umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar ataupun pencuri data lainnya,

Di samping itu Firewall merupakan suatu cara/sistem/mechanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya.

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkungannya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau Local Area Network (LAN).

Penggunaan firewall secara umum diperuntukkan untuk melayani:

1. Mesin/computer setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.
2. Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang dimiliki oleh perusahaan, organisasi dsb.

Firewall adalah sebuah pembatas antara suatu jaringan lokal dengan jaringan lainnya yang sifatnya publik sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik. Firewall juga dapat memantau informasi keadaan koneksi untuk menentukan apakah ia hendak mengizinkan lalu lintas jaringan. Umumnya hal ini dilakukan dengan memelihara sebuah tabel keadaan koneksi (dalam istilah *firewall: state table*) yang memantau keadaan semua komunikasi yang melewati firewall.

Secara umum fungsi firewall adalah untuk:

1. mengatur dan mengontrol lalu lintas;
2. melakukan autentikasi terhadap akses;
3. melindungi sumber daya dalam jaringan privat;
4. mencatat semua kejadian, dan melaporkan kepada administrator.

Jenis firewall dapat dikelompokkan menjadi empat yakni:

1. Personal firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total misalnya: Microsoft Windows Firewall
2. Network firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. Misalnya: *Internet Security and Acceleration Server (ISA Server)*, Cisco PIX.

3. IP Filtering Firewall

Sebuah IP Filtering firewall bekerja pada level paket

4. Proxy Server

Cara kerja proxy server, terlihat saat user terhubung dengan proxy server dengan perangkat lunak client, proxy server akan menduplikasi komunikasi tersebut.

5.2.1 Mengidentifikasi Kebutuhan Firewall

Untuk membangun sebuah jaringan yang memiliki pengamanan firewall, maka dibutuhkan hardware yang digunakan sebagai server. Selain hardware, sistem operasi harus diinstalasi agar jaringan dapat berfungsi dengan baik, seperti: Windows Server 2000, Windows Server 2003, Linux, Fedora, Mandriva, Debian, Ubuntu, FreeBSD dan Sun Solaris. Selanjutnya pada server tersebut di instalasi Paket program Firewall, seperti: WinGate, Microsoft ISA, Firestarter, dan Shorewall.

1. High level risk assessment

Pengujian terhadap keamanan jaringan juga harus memenuhi berbagai macam kriteria, termasuk sampai ke dalam *high level risk* atau tingkat ancaman paling tinggi. Sebuah firewall yang baik seharusnya dapat menahan serangan sampai tingkat yang paling tinggi, walaupun peran seorang administrator jaringan dan sistem administrator diperlukan untuk memantau kinerja dan kinerja sistem jaringan termasuk kinerja server yang dimiliki.

2. Menentukan perangkat keras yang diperlukan

Sebuah server adalah komputer yang memiliki kapasitas lebih besar dari workstation. Dari segi memori, hal ini untuk mendukung *multiple task* yang aktif pada saat yang bersamaan. Harddisk yang lebih besar juga dibutuhkan untuk menyimpan data. Server juga harus memiliki *extra expansion slots* pada *system board* nya untuk memasang beberapa device seperti printer dan beberapa NIC.

3. Inspeksi paket

Stateful Packet Inspection merupakan proses inspeksi paket yang tidak dilakukan dengan menggunakan struktur paket dan data yang

terkandung dalam paket, tapi juga pada keadaan apa host-host yang saling berkomunikasi tersebut berada.

4. Melakukan autentikasi terhadap akses

Firewall dilengkapi dengan fungsi autentikasi dengan menggunakan beberapa mekanisme autentikasi, sebagai berikut:

- a. Firewall dapat meminta input dari pengguna mengenai nama pengguna (user name) serta kata kunci (password).
- b. Metode kedua adalah dengan menggunakan sertifikat digital dan kunci publik.
- c. Metode selanjutnya adalah dengan menggunakan *Pre-Shared Key* (PSK) atau kunci yang telah diberitahu kepada pengguna.

Salah satu tugas firewall adalah melindungi sumber daya dari ancaman yang mungkin datang. Proteksi ini dapat diperoleh dengan menggunakan beberapa peraturan pengaturan akses (access control), penggunaan SPI, application proxy, atau kombinasi dari semuanya untuk mencegah host yang dilindungi dapat diakses oleh host-host yang mencurigakan atau dari lalu lintas jaringan yang mencurigakan.

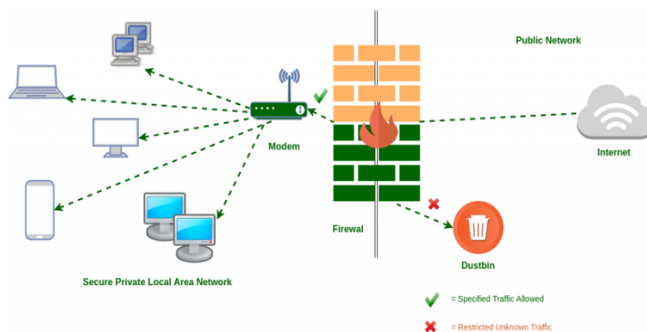
Firewall juga mampu mencatat semua kejadian, dan melaporkan kepada administrator, mencatat apa-apa saja yang terjadi di firewall amatlah penting, sehingga bisa membantu kita untuk memperkirakan kemungkinan penjeblolan keamanan atau memberikan umpan balik yang berguna tentang kinerja firewall

5.2.2 Membangun Firewall

Ada beberapa langkah yang harus dilakukan untuk membangun Firewall, yaitu (Bundet, 2010):

1. Mengidentifikasi bentuk jaringan yang dimiliki
Mengetahui bentuk jaringan yang dimiliki khususnya topologi yang digunakan serta protokol jaringan, akan memudahkan dalam mendesain sebuah firewall.
2. Menentukan Policy atau kebijakan
Penentuan kebijakan atau policy merupakan hal yang harus dilakukan, baik atau buruknya sebuah firewall yang di bangun sangat di tentukan oleh policy/kebijakan yang diterapkan, di antaranya:

- a. menentukan apa saja yang perlu di layani. artinya, apa saja yang akan dikenai policy atau kebijakan yang akan kita buat;
 - b. menentukan individu atau kelompok-kelompok yang akan dikenakan policy atau kebijakan tersebut;
 - c. menentukan layanan-layanan yang dibutuhkan oleh tiap-tiap individu atau kelompok yang menggunakan jaringan;
 - d. berdasarkan setiap layanan yang digunakan oleh individu atau kelompok tersebut akan ditentukan bagaimana konfigurasi terbaik yang akan membuatnya semakin aman;
 - e. menerapkan kan semua policy atau kebijakan tersebut.
3. Menyiapkan software atau hardware yang akan digunakan
Baik itu *operating system* yang mendukung atau software-software khusus pendukung firewall seperti IPchains, atau Iptables pada Linux, dsb. Serta konfigurasi hardware yang akan mendukung firewall tersebut.
4. Melakukan tes konfigurasi
Pengujian terhadap firewall yang telah selesai di bangun haruslah dilakukan, terutama untuk mengetahui hasil yang akan kita dapatkan, caranya dapat menggunakan tool-tool yang biasa dilakukan untuk mengaudit seperti *nmap*.



Gambar 5.2: Ilustrasi Firewall (Triyadi, 2019)

5.3 Bentuk Ancaman Keamanan Komputer

Ada banyak faktor yang mengancam keamanan jaringan komputer, yang dapat dibagi menjadi faktor subyektif dan faktor obyektif. Untuk menggambarkan faktor-faktor yang mengancam keamanan jaringan komputer agar lebih komprehensif (Munawar dan Putri, 2020).

Spam dan Spyware

Dalam bentuk komunikasi yang biasa, berkirim email adalah cara yang lebih umum digunakan. Terutama di semua jenis pekerjaan sering kali, email memainkan peran yang sangat penting dalam melakukan pekerjaan. Karena alasan ini, maka banyak penjahat ingin menggunakan email untuk mencuri privasi pengguna atau ada tujuan lain.

Mereka terutama memaksa pengguna untuk menerima spam dengan memasukkannya ke dalam email yang mereka kirimkan. Jika pengguna tidak memperhatikan validitas email ini, mereka dapat mengeklik atau mengunduh perangkat lunak khusus yang mereka masukkan, maka akan terjadi kehilangan informasi.

Serangan dan Ancaman Hacker

Peretas merujuk pada sekelompok orang dengan kecerdasan dan kemampuan tinggi, yang akrab dengan pengetahuan komputer dan sangat pandai dalam keamanan jaringan komputer, dibandingkan dengan orang biasa, peretas menunjukkan ketakutan kepada pengguna.

Peretas dapat memilih serangan destruktif dan serangan non-destruktif jika ingin memenuhi kebutuhan mereka sendiri melalui jaringan komputer. Serangan destruktif, seperti menghancurkan sistem pengguna sehingga komputer benar-benar tidak dapat digunakan.

Serangan non-destruktif berarti peretas hanya mengambil informasi yang mereka butuhkan tanpa mempengaruhi penggunaan normal pengguna. Peretas umum menggunakan cara serangan: serangan kuda Trojan, serangan phishing terhadap situs web, serangan email dan sebagainya.

Implantasi Virus

Pengguna komputer takut terhadap virus komputer, karena virus dapat disisipkan ke berbagai jenis aplikasi program, pengguna dengan tidak sengaja akan mengklik virus tersebut, selanjutnya virus dengan cepat menyebar ke seluruh bagian sistem komputer. Setelah sistem inti pengguna terinfeksi oleh virus, akan mempengaruhi kerja normal pengguna dalam waktu singkat, sehingga menyebabkan kerugian yang tak terhindarkan bagi pengguna.

Pintu Belakang dan Kebocoran Perangkat Lunak Komputer

Tidak ada perangkat lunak di dunia yang sempurna, sehingga banyak peretas suka memilih peranti lunak untuk diserang. Disebut "backdoor" berarti programmer meninggalkan pintu untuk di awal perancangan perangkat lunak, sehingga turut "memfasilitasi" operasi masa depan mereka.

Backdoor semacam itu jelas bukan karena programmer tidak cukup kompeten, akan tetapi karena justru terlalu kompeten untuk memikirkan cara yang tidak masuk akal tersebut. Singkatnya, perilaku tersebut adalah tidak masuk akal atau tidak direkomendasikan.

Sistem Serangan Langsung

Dengan perkembangan ilmu pengetahuan dan teknologi, beberapa orang yang akrab dengan komputer langsung menyerang sistem komputer orang lain melalui jaringan komputer yang dimiliki. Jenis kejahatan ini muncul dengan pengembangan bidang komputer. Serangan secara langsung pada sistem ini lebih canggih, bahkan tanpa meninggalkan beberapa jejak.

Dengan mencuri privasi, menghancurkan informasi nyata dan menyebabkan masalah besar bagi orang lain. Karena sifatnya tidak terbatas dari jaringan komputer, para penjahat ini menjadi semakin dan semakin merajalela. Hanya dengan meluangkan sedikit waktu dan energi, tetapi mereka mendapatkan keuntungan yang besar, sehingga timbul keinginan menjadi lebih kuat.

Bencana Alam

Tidak peduli seberapa cerdas komputer itu, komputer hanyalah sebuah mesin, yang selalu lebih rendah daripada manusia. Karena itu, ada faktor eksternal lain yang akan berdampak besar pada keamanan komputer, yaitu bencana alam.

Bencana alam yang dimaksud merujuk pada penyebab yang tidak dapat dikendalikan seperti perubahan kelembaban, suhu, gempa bumi atau gempa bumi yang menyebabkan tsunami, pemadaman listrik yang tiba-tiba atau kecelakaan asupan air komputer. Penyebab alami ini berada di luar kendali manusia dan tidak bisa sepenuhnya dihindari.

Karena itu, jika ingin meningkatkan keamanan jaringan komputer, kita harus melakukannya mulai dari aspek lain.

Bab 6

Keamanan Aplikasi

6.1 Pendahuluan

Keamanan perangkat lunak mengacu pada tindakan pencegahan keamanan yang digunakan pada taraf software buat mencegah pencurian atau pembajakan data atau kode pada aplikasi. Ini mencakup duduk perkara keamanan yang didesain selama pengembangan dan desain perangkat lunak, serta metode dan prosedur buat melindungi software sesudah diterapkan (Bamai, 2022).

Apa Itu Keamanan Aplikasi?

seluruh tugas yang memperkenalkan siklus hayati pengembangan software yang aman ke tim pengembangan disertakan dalam keamanan perangkat lunak yang dikenal menjadi *AppSec*. Tujuan utamanya adalah buat menaikkan praktik keamanan dan, menjadi hasilnya, mendeteksi, memperbaiki, dan, idealnya, menghindari kelemahan keamanan dalam aplikasi. Ini meliputi semua siklus hidup aplikasi, termasuk analisis persyaratan, desain, implementasi, pengujian, serta pemeliharaan.

Perangkat keras, software, dan mekanisme yang mengidentifikasi serta mengurangi kerentanan keamanan bisa disertakan dalam keamanan aplikasi. Keamanan aplikasi perangkat keras mengacu pada router yang menghentikan siapa pun asal melihat alamat IP personal komputer melalui Internet.

Namun, kontrol keamanan tingkat perangkat lunak, seperti firewall perangkat lunak yang secara ketat membatasi tindakan yang diizinkan dan dilarang, sering kali diintegrasikan ke pada software. Rutinitas keamanan aplikasi yang mencakup protokol seperti pengujian reguler adalah contoh prosedur.

Mengapa Keamanan Aplikasi Penting?

software waktu ini tak jarang tersedia melalui beberapa jaringan serta terhubung ke *cloud*, perangkat lunak tadi lebih rentan terhadap serangan dan pelanggaran keamanan. terdapat peningkatan tekanan dan insentif buat memastikan keamanan tidak hanya di tingkat jaringan tetapi pula dalam software individu. keliru satu penjelasan buat ini merupakan sebab peretas lebih memfokuskan agresi mereka di software kini daripada pada masa kemudian. Pengujian keamanan perangkat lunak bisa mengekspos kelemahan taraf software, membantu dalam pencegahan serangan ini.

Semakin cepat serta dini Anda bisa mendeteksi serta menyelesaikan dilema keamanan pada proses pengembangan software, semakin safety perusahaan Anda nantinya. sebab setiap orang membuat kesalahan, triknya merupakan mengidentifikasinya sesegera mungkin. alat keamanan perangkat lunak yang terintegrasi dengan lingkungan pengembangan anda dapat menghasilkan proses dan alur kerja ini jauh lebih mudah serta efisien. indera-indera ini sangat bermanfaat buat audit kepatuhan, sebab dapat berhemat saat serta asal daya menggunakan mendeteksi problem sebelum auditor menyadarinya.

Sifat yang berubah dari bagaimana aplikasi perusahaan dibangun selama bertahun-tahun terakhir sudah membantu ekspansi yang cepat berasal industri keamanan perangkat lunak.

6.2 Jenis Keamanan Aplikasi

Otentikasi, otorisasi, enkripsi, logging, serta pengujian keamanan software merupakan model fitur keamanan perangkat lunak. Pengembang juga bisa menggunakan kode buat mengurangi kelemahan keamanan dalam aplikasi.

1. Autentikasi

Saat pengembang menyertakan protokol pada perangkat lunak buat memastikan bahwa hanya pengguna yang berwenang yang bisa mengaksesnya. prosedur otentikasi memverifikasi bahwa pengguna

adalah siapa yang mereka klaim. waktu masuk ke aplikasi, ini dapat dilakukan dengan meminta pengguna buat memasukkan nama pengguna dan kata sandi. Otentikasi multi-faktor memerlukan penggunaan aneka macam bentuk otentikasi, seperti sesuatu yang Anda ketahui (istilah sandi), sesuatu yang Anda miliki (perangkat seluler), serta sesuatu perihal diri Anda (biometrik).

2. Otorisasi

Seorang pengguna dapat diotorisasi untuk mengakses dan memakai perangkat lunak sesudah diautentikasi. menggunakan membandingkan identifikasi pengguna menggunakan daftar pengguna yang berwenang, sistem dapat memverifikasi bahwa pengguna memiliki biar untuk mengakses aplikasi. supaya software hanya mencocokkan kredensial pengguna yang divalidasi dengan daftar pengguna yang disetujui, otentikasi wajib dilakukan sebelum otorisasi.

3. Enkripsi

Tindakan keamanan lainnya dapat melindungi data sensitif agar tidak dilihat atau digunakan oleh penjahat dunia maya sehabis pengguna diverifikasi serta memakai software. kemudian lintas yang berisi data sensitif yang mengalir antara pengguna akhir serta cloud pada software berbasis cloud dapat dienkripsi buat menjaga keamanan data.

4. Pencatatan

Jika pelanggaran keamanan terjadi dalam suatu perangkat lunak, pencatatan dapat membantu pada menentukan siapa yang memperoleh akses ke data dan bagaimana mereka melakukannya. file log software melacak bagian mana berasal perangkat lunak yang telah diakses serta sang siapa.

5. Pengujian keamanan perangkat lunak

Metode yang memastikan bahwa seluruh kontrol keamanan ini berfungsi secara efektif.

6.3 Alat Buat Keamanan Software

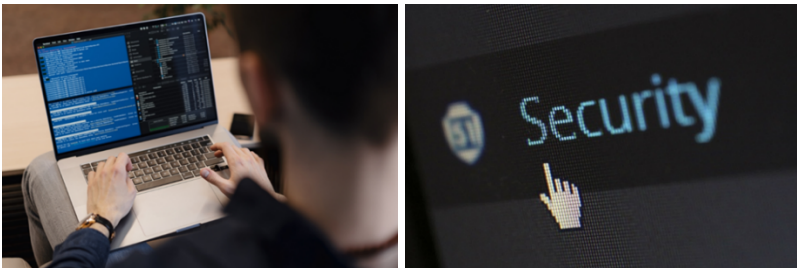
Pendekatan keamanan software yang lengkap membantu pada pendeteksian, perbaikan, serta penyelesaian banyak sekali kerentanan software serta tantangan keamanan. Solusi untuk menghubungkan dampak insiden terkait keamanan aplikasi menggunakan akibat bisnis disertakan dalam paket keamanan perangkat lunak yang paling efektif dan canggih.

Menemukan teknologi keamanan software yang sempurna buat perusahaan Anda sangat krusial buat efektivitas tindakan keamanan apa pun yang diterapkan sang *DevOps* atau tim keamanan Anda.

Tools Security Analyst

1. Platform monitoring OSINT

Penting untuk memiliki platform OSINT (Open Source Intelligence Tools) yang bisa mengumpulkan data dari sumber-sumber penting serta relevan untuk bisnis (Widyawinata, 2021).



Gambar 6.1: Platform Monitoring OSINT dan WHOIS dan IP-Geolocation (Freepik.com)

2. WHOIS dan IP-Geolocation tool biomimikri untuk bisnis

Tools *security analyst* yang satu ini bisa memberikanmu petunjuk berupa rekaman WHOIS dan informasi IP. Keduanya bisa memberikan kamu petunjuk siapa dalang di balik sebuah serangan, dan apakah serangan masih berlangsung. Informasi yang didapatkan juga bisa membantumu meriset dan melihat gambaran yang lebih jelas seputar serangan atau pelakunya.

3. Google dorks

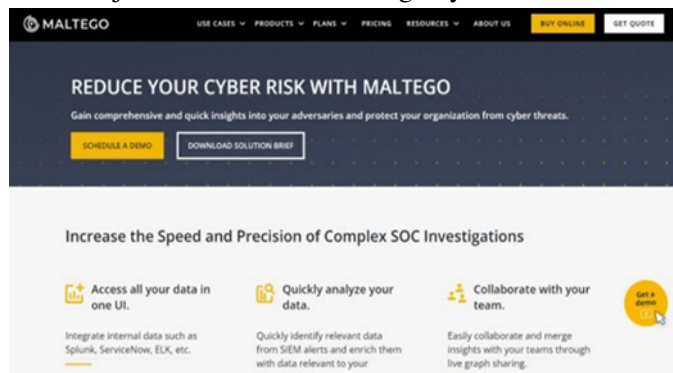
Jangan salah, Google banyak dipakai oleh analis dan juga pelaku tindak kejahatan untuk menggali informasi seputar keamanan sebuah situs atau sistem. Google dorks adalah kata kunci pencarian di Google yang digunakan penyerang untuk mengenali dan menemukan targetnya. Jadi, kamu bisa mencoba melakukan “Google hacking” untuk menelusuri sebuah kejadian atau menguji keamanan sistem yang kamu pakai.



Gambar 6.2: Google Dorks (9to5google.com)

4. Maltego tools security analyst

Maltego adalah sebuah data mining tool yang bersifat interaktif. Alat ini menunjukkan analisis link atau keterkaitan dan hubungan berbagai objek. Objek yang dianalisis bisa berupa orang, tempat, alat komunikasi, kejadian tertentu, dan sebagainya.



Gambar 6.3:Maltego Tools Security Analyst (maltego.com)

5. FOCA tools security analyst

FOCA adalah alat untuk menganalisis metadata dan informasi tersembunyi dalam dokumen yang dipindai (di-scan). Saat kamu membuat dan menayangkan dokumen Microsoft Office atau PDF secara online, hal tersebut berpotensi besar untuk diretas. FOCA adalah tools security analyst yang bisa mengekstrak data yang “bocor” dari dokumen-dokumen bersifat publik alias bisa diakses siapa saja.



Gambar 6.4: FOCA Tools Security Analyst Dan Spybot Tools Security Analyst (Foca Open Source)

6. SpyBot tools security analyst

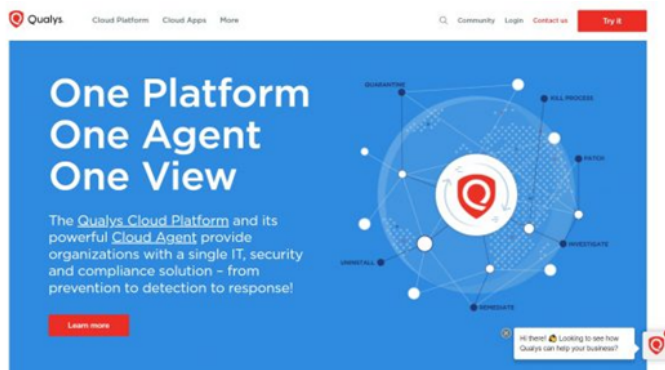
SpyBot adalah *tools security analyst* yang berfungsi sebagai *vulnerability management software*. Alat ini menggabungkan antivirus serta teknik uniknya untuk melindungi bisnismu dari spyware, keyloggers, trojans, adware, dan sebagainya.

7. Qualys tools security analyst

Qualys menawarkan berbagai fitur dan tools *security analyst*, di antaranya: manajemen, deteksi, dan respons terhadap kerentanan (*vulnerability*):

- a. perlindungan terhadap ancaman;
- b. container security;
- c. web app security;
- d. manajemen aset cybersecurity.

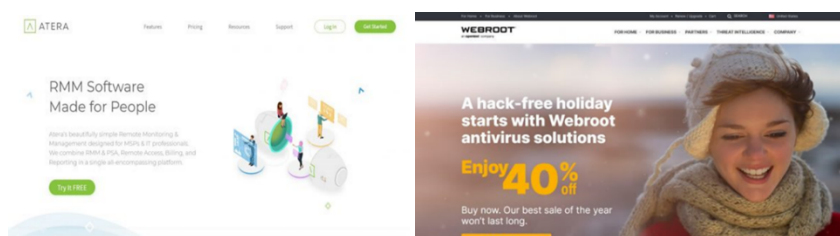
Menurut situsnya, Qualys VM (produk manajemen kerentanan mereka) dapat memindai dan mengenali kerentanan dengan tingkat keakuratan hingga 99,9 persen.



Gambar 6.5: Qualys Tools Security Analyst (Qualys.com)

8. Atera tools security analyst

Mirip seperti Qualys, Atera juga menawarkan software manajemen kerentanan (vulnerability management). Atera akan menyediakan secara *real-time status system resource*, siapa saja users yang masuk, pemantauan IP dan jaringan, dan masih banyak lagi. Ada berbagai pilihan yang bisa kamu sesuaikan sendiri, kejadian atau peringatan apa yang mau didapatkan melalui notifikasi email.



Gambar 6.6: Atera Tools Security Analyst dan Webroot Tools Security Analyst (Atera.com)

9. Webroot tools security analyst

Webroot juga menjadi tools yang perlu kamu telusuri sebagai security analyst. Produk Endpoints Protection dan antivirusnya bisa melindungimu dari serangan siber canggih tanpa mengorbankan system performance-mu. Tools security analyst ini juga menawarkan

perlindungan berlapis-lapis dari berbagai serangan seperti email, situs, file, URL, iklan, aplikasi, dan sebagainya.

Bab 7

Keamanan Privasi

7.1 Pendahuluan

Perkembangan teknologi informasi dan komunikasi yang pesat dewasa ini telah membawa dunia pada Revolusi Industri 4.0. Revolusi Industri 4.0 ditandai dengan munculnya berbagai Penyelenggara Sistem Elektronik baru yang mengadopsi penerapan layanan berbasis sistem cerdas dengan memanfaatkan jaringan internet.

Kesiapan infrastruktur dan kemudahan akses terhadap kebutuhan perangkat teknologi, mendorong peningkatan jumlah pengguna internet dan smartphone pada masyarakat di Indonesia. Menurut APJII pada profil internet Indonesia 2022, terdapat lebih dari 210 juta orang penduduk Indonesia yang terkoneksi menggunakan internet di tahun 2021-2022. Peningkatan penetrasi internet di Indonesia pada tahun 2021-2022 sebesar 77.02% dari jumlah total penduduk (APJII, 2022).

Peningkatan jumlah pengguna internet ini juga mendorong berkembangnya sistem elektronik berbasis web ataupun mobile seperti media sosial, pesan instan, panggilan video, augmented reality, dan lainnya. Berkembangnya aplikasi-aplikasi sistem elektronik, akan semakin memberikan kemudahan pada layanan yang diberikan. Pada sisi lain, terdapat dampak negatif dari

pemanfaatan data yang dilakukan oleh aplikasi-aplikasi sistem elektronik tersebut.

Penyelenggara Sistem Elektronik pada umumnya, sering kali mensyaratkan / meminta data-data pribadi dari penggunanya. Data-data pribadi tersebut kemudian digunakan untuk mendukung proses bisnis. Salah satu contoh pemanfaatan data pribadi pengguna digunakan sebagai “identitas utama pengguna” dalam proses pertukaran data yang terjadi pada sebuah sistem elektronik.

Adapun contoh umum data pribadi yang sering digunakan sebagai identitas adalah email. Email bersifat unik dan sensitif yang rentan untuk disalahgunakan oleh penyelenggara sistem elektronik dan berpotensi terjadinya pelanggaran privasi data pengguna.

Definisi privasi dinyatakan oleh (S. Warren dan L. Brandeis, 1890) bahwa:

“Privasi sebagai hak individu untuk menyimpan sesuatu sendiri, dan itu telah diakui sebagai hak asasi manusia yang mendasar.”

Ada dua cara untuk menghindari pelanggaran privasi oleh sebuah penyelenggara sistem elektronik. Cara pertama dilihat dari sisi pengguna sistem elektronik yang mana pengguna sistem elektronik dapat melakukan pengendalian/pembatasan penggunaan data pribadi miliknya. Pengguna sistem harus sadar akan pentingnya menjaga data pribadi dan pengguna sistem juga harus memahami pemanfaatan setiap data pribadi yang dititipkan kepada pihak penyelenggara sistem elektronik.

Cara lainnya dilihat dari sisi penyelenggara sistem elektronik, dimana data-data pribadi pengguna dapat dipelajari pengguna melalui pembuatan kebijakan privasi dengan menjelaskan secara terbuka pemanfaatan penggunaan data pribadi dari pengguna, sehingga dapat menumbuhkan kepercayaan dari pengguna. Perkembangan teknologi perlu diimbangi dengan kesadaran dalam penggunaan data-data sensitif pada sistem elektronik agar terhindar dari gangguan keamanan privasi yang tidak diinginkan.

7.2 Privasi Digital dan Risikonya

Ketika menggunakan aplikasi layanan elektronik berbasis online, sebuah perusahaan penyelenggara sistem elektronik akan mengumpulkan, menyimpan dan mengolah data pribadi dari penggunanya untuk kepentingan tertentu. Data-data pribadi yang dititipkan pada perusahaan tersebut, memiliki risiko untuk dicuri atau disalahgunakan.

Sebagai contoh, ancaman yang sering terjadi pada pengguna layanan kartu kredit adalah pencurian identitas. Pada penyelenggara sistem elektronik yang memiliki fitur pembayaran menggunakan kartu kredit, akan menyimpan data-data penting dari kartu kredit yang digunakan.

Data ini dapat ditemukan pada basis data perusahaan tempat pengguna melakukan transaksi bisnis secara online. Kondisi ini membuat dilema bagi pengguna dimana di satu sisi penyimpanan data pembayaran dapat memudahkan tetapi disisi lain terdapat konsekuensi keamanan pada data yang dititipkan.

Terdapat dua risiko utama yang kurang disadari pengguna dalam menggunakan aplikasi penyelenggara sistem elektronik, diantaranya:

Memberikan “Hackers” Informasi Yang Mereka Butuh kan

Saat pengguna semakin berbagi informasi tentang kehidupannya secara online di jejaring sosial seperti Facebook dan Twitter, pencuri identitas dapat membobol akun dan mengumpulkan informasi yang mereka butuh kan untuk membajak identitas. Sebagian besar situs web publik memiliki tautan yang memungkinkan pengguna menemukan kata sandi mereka atau mengatur ulang kata sandi mereka jika hilang.

Biasanya, ini dilakukan dengan mengajukan serangkaian pertanyaan yang hanya diketahui oleh pemegang akun. Ketika Internet pertama kali digunakan dan konsep jenis pertanyaan dan jawaban saat pengguna ingin mengatur ulang kata sandi, itu bekerja dengan cukup baik karena belum ada yang memposting informasi pribadi secara online.

Kenyataannya adalah bahwa jawaban atas pertanyaan-pertanyaan ini mungkin telah dibagikan secara online di situs jejaring sosial, seperti nama orang tua, tanggal lahir, alamat rumah, nomor telp, sekolah dll.

Memberitahu “Pencuri” Kapan Harus Masuk Rumah

Jejaring sosial adalah tempat yang bagus untuk memberi tahu teman dan kerabat tentang apa yang sedang terjadi dalam hidup seseorang. Saat memposting lebih banyak informasi di situs jejaring sosial, pengguna harus menyadari bahwa tidak hanya teman ataupun keluarga yang dapat melihatnya. pengguna harus sangat berhati-hati dalam memposting alamat rumah yang sebenarnya secara online.

Jika pengguna telah memposting di mana lokasi sebenarnya tinggal, dan waktu untuk berlibur ke luar kota, secara tidak langsung pengguna baru saja memberitahu siapa pun yang berpotensi melakukan pencurian di area rumahnya dimana rumah dia berada dan fakta bahwa rumah miliknya akan kosong setidaknya selama beberapa hari.

7.3 Keamanan Informasi Pengguna

7.3.1 Menyimpan Informasi Online

Di era digitalisasi saat ini, segala aktivitas transaksi belanja dan pertukaran informasi dapat dilakukan dengan mudah melalui internet. Untuk mempermudah dan menjamin kualitas kegiatan transaksi, diperlukan informasi pribadi dari pengguna sebagai penjamin kegiatan transaksi tersebut. Setiap perusahaan bisnis menyimpan informasi penting tentang penggunanya, termasuk informasi pribadi yang sensitif. Perusahaan penyedia jasa layanan elektronik, pada umumnya menyimpan informasi pengguna melalui data yang mereka dapatkan dari informasi yang diberikan oleh pengguna.

Kondisi bisnis saat ini, hampir seluruh perusahaan penyedia jasa layanan elektronik menyimpan dan melacak informasi pribadi penggunanya, sehingga sangat penting untuk diketahui bahwa pengguna harus mampu menjaga diri (informasi pribadi) dari pencuri data dan identitas online. pengguna harus mampu untuk memahami bagaimana perusahaan mengumpulkan dan menggunakan informasi pribadi, sehingga pengguna paham akan batasan dalam menyebarkan informasi pribadi untuk kepentingan tertentu.

Pada situasi tertentu yang dimana informasi pribadi tidak menjadi kepentingan utama dalam kegiatan yang pengguna lakukan secara online, pengguna bisa

juga memberikan informasi yang salah untuk menghindari terjadinya kejahatan keamanan data.

Sebenarnya ada berapa banyak informasi yang pengguna bagikan dengan perusahaan melalui internet? perlu diketahui bahwa perusahaan yang pengguna gunakan untuk berbisnis atau kegiatan transaksi secara online ini mengumpulkan informasi pribadi pengguna mereka dalam skala yang sangat besar. Tentunya ada alasan dibalik perusahaan-perusahaan ini mengumpulkan informasi pribadi pengguna mereka.

Alasan pertama yang paling umum adalah mempermudah mereka / perusahaan dalam menentukan target yang tepat untuk mengiklankan produk atau layanan mereka, sehingga mereka mendapatkan kesempatan yang baik dalam membuka peluang terjualnya produk mereka jika berhasil memberikan tawaran yang sesuai dengan keinginan calon pengguna.

Alasan kedua bagi perusahaan untuk mendapatkan data pengguna mungkin terasa ilegal dan kurang disenangi oleh pengguna, perusahaan mengumpulkan dan menyimpan data pribadi pengguna untuk bisa dijual kembali ke perusahaan lain yang memberikan layanan untuk mengiklankan produk / layanan perusahaan dengan iming-iming data pribadi pengguna.



Gambar 7.1: Jenis Data Pribadi Yang Umum Diambil Oleh Perusahaan

Berdasarkan Gambar 7.1 diatas, dapat dilihat terdapat berbagai jenis data pribadi yang sangat umum dan biasa diambil oleh perusahaan dari pengguna. Informasi seperti lokasi, kesehatan, nomor identitas, nama pribadi, informasi ekonomi dan identitas sosial, physical atribut, dan online identifier merupakan informasi yang sangat mudah untuk didapatkan oleh perusahaan tanpa pengguna sadari.

Sebagai contoh, aplikasi-aplikasi seperti Instagram, Facebook, dan Twitter sering kali meminta pengguna untuk memberikan akses informasi terkait data lokasi pengguna, hal ini sebenarnya bertujuan untuk memberikan konten yang sesuai pada halaman sosial media dengan peristiwa atau event yang sedang hits di sekitar lokasi pengguna.

Memberikan akses penuh kepada sosial media / layanan internet terkait lokasi pribadi secara real time tanpa disadari akan sangat membahayakan pengguna, karena dengan data lokasi ini siapa saja dapat mengetahui pola keseharian pengguna.

Pengguna tentunya memiliki pertimbangan yang besar dalam memberikan informasi pribadi, terlebih pada jaminan akan perusahaan untuk melindungi informasi dan data pribadi mereka. Perusahaan biasanya menjelaskan terkait jaminan keamanan data pribadi pengguna pada web informasi mereka, serta menjelaskan terkait bagaimana mereka memanfaatkan informasi pribadi pengguna.

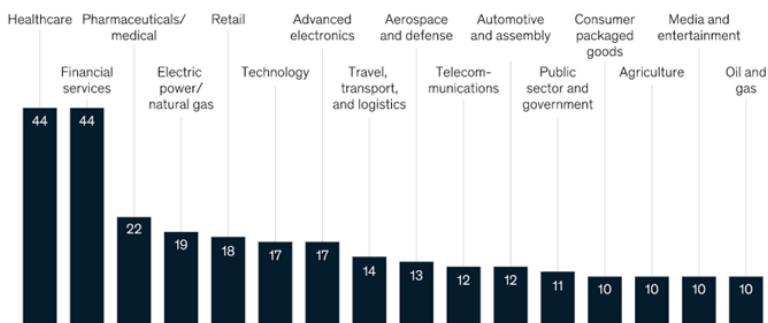
Tetapi, mereka tidak akan menjelaskan langkah-langkah atau metode enkripsi yang mereka gunakan untuk menjaga data pengguna agar tetap aman. Informasi-informasi tersebut tidak disebarluaskan karena akan memancing dan memberikan kesempatan bagi penjahat siber dalam membobol sistem perusahaan.

Negara Amerika Serikat memiliki hukum federal yang mengatur keseluruhan data dan informasi kesehatan penduduk setempat yang bernama HIPPA (Health Information Patient Protection Act). HIPPA mengatur seluruh perusahaan yang bergerak dibidang kesehatan untuk mengambil tindakan pencegahan kebocoran data kesehatan yang mereka miliki dengan hanya memberikan akses khusus kepada orang-orang yang benar-benar dapat mengakses informasi kesehatan tersebut.

Sebagai contoh, perusahaan biasanya mengharuskan seluruh informasi kesehatan pasien yang dicetak untuk dihancurkan setelah dokumen informasi kesehatan tersebut sudah tidak digunakan lagi, sedangkan untuk informasi kesehatan yang disimpan secara digital harus dipastikan diamankan dengan menggunakan kode enkripsi.

Berdasarkan survei yang dilakukan oleh McKinsey pada orang-orang Amerika Utara terkait privasi dan keamanan data, didapatkan bahwa untuk setiap perusahaan yang berlatar belakang kesehatan dan keuangan menduduki posisi

paling pertama sebesar 44% akan ke jaminannya dalam melindungi data pengguna.



Source: McKinsey Survey of North American Consumers on Data Privacy and Protection, 2019

Gambar 7.2: Hasil Survei Privasi dan Keamanan Data (McKinsey, 2019)

Survei ini membuktikan bahwa hukum HIPAA yang diterapkan di Amerika Serikat benar-benar menjadi pegangan dan dilaksanakan dengan baik oleh setiap perusahaan kesehatan di Amerika Serikat. Salah satu tujuan dari keamanan data adalah untuk membuat sistem keamanan menjadi sulit untuk diretas dan memakan waktu yang lama, sehingga menjadikan peretasan data sebagai kegiatan yang sia-sia yang berujung pada menyerahnya pelaku peretasan data.

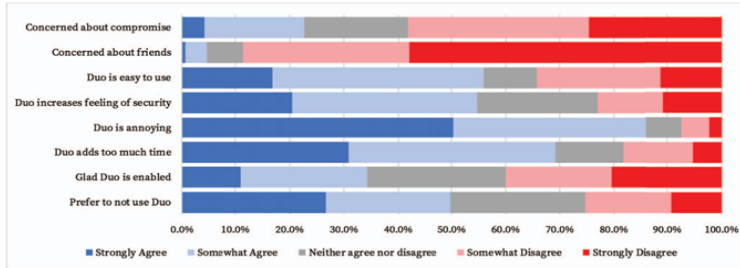
7.3.2 Username dan Password Pada Aplikasi

Cara lain untuk menjaga keamanan privasi pada aplikasi penyedia layanan elektronik adalah dengan memperkuat username dan password yang digunakan sebagai identitas utama pengguna. Memilih username dan password yang unik dan tidak mengandung keterkaitan dengan informasi pribadi mampu menghindari terjadinya peretasan.

Keamanan informasi pengguna pada aplikasi penyedia layanan elektronik bisa juga ditingkatkan juga dengan menambahkan fitur *two-factor authentication* setelah melakukan pengisian username dan password. Semakin banyaknya tahapan autentikasi yang dilakukan oleh pengguna, sebenarnya membuat informasi pribadi pengguna juga semakin terjaga dengan baik.

Tetapi, berdasarkan penelitian yang dilakukan oleh Duston, Egget, dan Seamons tentang mengukur perilaku pengguna dalam menggunakan *two-factor authentication* yang memanfaatkan aplikasi Duo. Mereka menemukan

bahwa terdapat beberapa pengguna yang kenyamanannya terganggu dengan fitur keamanan ini dalam mengakses situs yang dituju.



Gambar 7.3: Hasil Survei Kegunaan Aplikasi Duo (Duston, 2019)

Pada penelitian ini, mereka merekomendasikan terkait pemanfaatan layanan *two-factor authentication*, yang dimana sebaiknya layanan *two-factor authentication* diterapkan hanya pada bagian halaman yang memuat informasi sensitif dari pengguna.

Username dan password merupakan salah satu bentuk dari informasi sensitif pengguna yang keamanannya harus terjaga, sehingga hampir pada seluruh situs online yang menyediakan akun bagi penggunaannya pasti memiliki fitur keamanan tambahan dari *two-factor authentication*.

Username

Dimulai dengan memilih username, pengguna harus memastikan tidak ada informasi pribadi yang terkandung pada username, contohnya kombinasi nama dengan tahun kelahiran. Kombinasi nama dengan tahun kelahiran dapat membuka peluang yang besar bagi peretas dalam menebak pertanyaan-pertanyaan keamanan yang biasanya ada pada saat proses masuk kedalam akun pengguna.

Tetapi, dalam memilih username juga harus disesuaikan dengan tujuan pembuatan username itu sendiri, apakah username dibuat untuk akun sosial media atau untuk akun penyimpanan data keuangan? Sebagai contoh, Andi ingin membuka akun sosial media yang membutuhkan dibentuknya username dan password. Dalam memilih username, tentunya Andi ingin akun sosial mediana mudah untuk dijangkau oleh orang terdekat Andi melalui pencarian username.

Oleh karena itu, Andi harus memilih kombinasi username yang masih memiliki informasi terkait nama Andi, namun dengan batasan tidak mengandung informasi pribadi lainnya.

Password

Pemilihan password juga tidak kalah penting dengan pemilihan username, yang dimana pengguna juga harus memilih kombinasi yang unik dan tidak mudah ditebak oleh orang pada umumnya. Menentukan kombinasi password yang unik bisa dilakukan dengan melakukan parafrase dari kata-kata yang dipilih sebagai password.

Misalnya, kalimat yang ingin digunakan sebagai password adalah “kucing kecil manis” dapat di parafrase dengan mengganti kombinasi huruf yang ada pada kalimat dengan simbol spesial atau angka, sehingga parafrase menjadi “kuc1ngk3c!lm4n15”.

Perlu diingat juga bahwa penentuan password yang panjang dan unik memang sangat sulit untuk ditebak dan diingat, sehingga sebaiknya penerapan dari parafrase dilakukan dengan kalimat yang berasal dari konten kesukaan seperti musik, artis, film, dan quotes.

Two-Factor Authentication

Pemanfaatan *two-factor authentication* sudah semakin sering ditemukan pada setiap situs layanan elektronik yang membutuhkan pengisian informasi username dan password. Cara kerja *two-factor authentication* pada umumnya memanfaatkan dua jenis informasi yang dibutuhkan untuk autentikasi. Informasi pertama biasanya diberikan dan diketahui oleh pengguna yang sudah tersimpan pada situs (seperti password), sedangkan untuk informasi yang kedua berbentuk kombinasi angka acak yang dihasilkan dari *key fob*, aplikasi smartphone, website, atau pesan teks yang dikirimkan ke smartphone pengguna.

Pemanfaatan *two-factor authentication* tentunya sangat bermanfaat dan terjamin keamanannya karena kode yang digunakan hanya bisa digunakan sekali dan berlaku pada waktu yang sangat singkat. Sebagai contoh seperti dalam penggunaan *key fob* yang dimana *key fob* hanya akan memberikan kode / nilai baru pada setiap 60 detik, dan kode yang diberikan akan tidak berlaku lagi apabila tidak digunakan dalam waktu 60 detik.

Pengguna harus paham akan cara kerja dari *two-factor authentication* yang mereka temui, yang dimana mayoritas dari fitur keamanan tambahan ini memberikan kode rahasia mereka ke email atau pesan singkat pada smartphone pengguna.

Sehingga, pengguna harus memperhatikan dengan benar akan email dan nomor telepon yang mereka gunakan pada akun mereka untuk kegiatan autentikasi. Pengguna harus memastikan bahwa email dan nomor telepon yang digunakan benar-benar bisa mereka akses, karena jika tidak bisa, mereka akan kesulitan untuk masuk dalam akun situs layanan elektronik yang dituju.

7.3.3 Mengunggah Informasi Secara Online

Dalam mengunggah konten atau informasi secara online, pengguna harus paham akan jenis informasi seperti apa saja yang layak untuk diunggah. Setiap informasi yang diunggah secara online akan menjadi konsumsi khalayak ramai secara otomatis, tentunya pengguna tidak ingin informasi-informasi seperti data pribadi yang bersifat rahasia ini diketahui dan disalahgunakan oleh khalayak ramai.

Pada sub bab ini akan membahas terkait jenis-jenis informasi yang layak untuk diunggah dan dibagikan secara online, serta bagaimana langkah-langkah yang bisa dilakukan untuk melindungi informasi yang diunggah secara online.

Jenis Informasi Yang Tidak Boleh Diunggah Secara Online

Sebelum memahami lebih dalam terkait jenis informasi yang tidak layak dibagikan secara online kepada khalayak ramai, pengguna harus paham akan konsekuensi yang didapatkan setelah mengunggah informasi secara online. Informasi atau konten yang berbentuk teks, foto, video, ataupun audio yang diunggah secara online, secara otomatis akan kekal berada di internet walaupun nantinya informasi tersebut akan pengguna hapus.

Hal ini dikarenakan setiap situs seperti Twitter, Facebook, dll tidak akan langsung menghapus file yang mengandung informasi pengguna, padahal sebelumnya pengguna sudah membuat permintaan untuk melakukan penghapusan informasi.

Sebagai contoh, sejak tahun 2013 Facebook telah menyatakan bahwa untuk kebijakan *End User License Agreement* (EULA) tentang konten yang dihapus akan tetap tersimpan di situs mereka sampai waktu yang tidak ditentukan, tetapi informasi tersebut tidak tersedia untuk umum.

Dengan memahami kebijakan dari masing-masing situs online terkait informasi yang diunggah secara online, pengguna seharusnya bisa lebih bijak dalam memilih konten atau informasi yang akan mereka unggah.

1. Informasi pribadi

Jenis informasi seperti alamat, nomor telepon, informasi keluarga, tanggal lahir, password, dan lokasi terkini merupakan data pribadi yang harus dilindungi dan sebaiknya tidak diunggah di situs online.

2. Foto dan video

Sedangkan untuk konten seperti foto dan video juga pengguna harus hati-hati dalam membagikannya secara online, karena biasanya foto dan video yang diambil dari smartphone tertanam informasi seputar GPS pada saat foto dan video diambil.

3. Kartu kredit dan informasi keuangan lainnya

Membagikan informasi kartu kredit juga perlu dihindari, karena dapat memberikan akses bagi pencuri / penjahat identitas pada kartu kredit. Dampak yang bisa pengguna rasakan apabila pencuri identitas telah mengetahui informasi kartu kredit yaitu akun keuangan pengguna bisa saja dikunci oleh pihak bank atau bahkan pencuri identitas dapat memanfaatkan kartu kredit untuk kepentingan pribadinya (seperti mengambil uang dari kartu kredit).

4. Keluhan terkait pekerjaan

Burn out karena pekerjaan dan lingkungan kerja tentunya sudah biasa dialami oleh semua orang. Banyak pekerja yang melepaskan rasa gundah dan penatnya dengan mengeluarkan seluruh keluh kesahnya selama bekerja di sosial media. Dengan menceritakan keluh kesah akan pekerjaan, mungkin saja secara tidak sadar telah mengungkap pekerjaan yang sebenarnya bersifat rahasia bagi perusahaan.

Jika informasi tersebut dikonsumsi oleh banyak orang, termasuk kompetitor dari perusahaan, maka sudah memosisikan diri dan perusahaan pada posisi yang berbahaya. Dengan tulisan di situs online ini, bisa saja mengakibatkan perusahaan melakukan pemecatan pegawai dengan alasan menyebarkan informasi rahasia perusahaan.

7.3.4 Langkah-Langkah Melindungi Informasi Yang Diunggah Secara Online

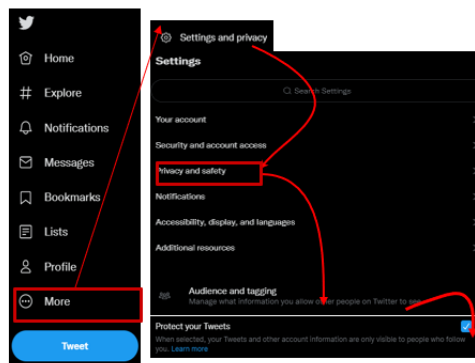
Dalam melindungi informasi yang diunggah secara online pada setiap situs online, tentunya memiliki cara yang berbeda-beda. Berikut langkah-langkah yang bisa dilakukan untuk melindungi informasi pada situs Twitter, Facebook, dan Instagram yang merupakan tiga aplikasi sosial media yang paling besar jumlah penggunaanya saat ini.

Twitter

Twitter memiliki layanan bagi pengguna untuk melindungi setiap tweet yang diunggah. Layanan perlindungan ini menjamin akan perlindungan konten dan informasi yang diunggah agar tidak muncul di fitur Search Twitter, dan membatasi orang-orang yang bisa melihat tweet hanya untuk pengguna yang saling mengikuti.

Untuk melakukan perlindungan tweet, pengguna dapat masuk kedalam akun twitter masing-masing dan memilih menu More pada sidebar Twitter seperti yang ada pada Gambar 7.4. Setelah memilih menu More, akan muncul menu tambahan yang di dalamnya terdapat submenu Settings and privacy, pengguna memilih submenu tersebut untuk memasuki pengaturan privasi akun Twitter.

Selanjutnya pengguna dapat memilih menu Privacy and safety pada halaman Settings Twitter. Layanan perlindungan tweet dapat ditemukan pada menu Audience and tagging setelah memasuki halaman Privacy and safety, aktifkan checkbox pada bagian Protect your tweets untuk mengaktifkan fitur perlindungan.

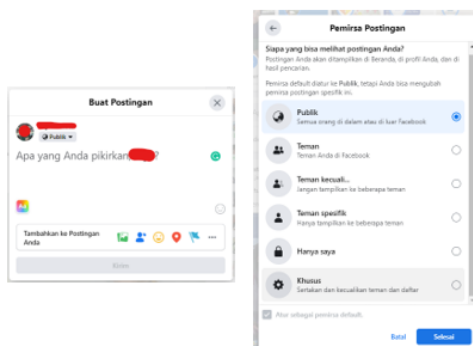


Gambar 7.4: Langkah-Langkah Proteksi Tweet (Twitter)

Facebook

Berbeda dengan Twitter, Facebook memiliki banyak cara dan pengaturan dalam melindungi privasi pengguna, baik dari melalui melindungi konten atau informasi yang akan diunggah secara satu persatu dan melalui pengaturan keamanan privasi akun Facebook secara keseluruhan.

Cara pertama untuk melindungi privasi pada Facebook dapat dilakukan dengan memberikan batasan hak akses untuk unggahan yang baru seperti pada Gambar 7.5. Terdapat enam kategori hak akses yang diberikan Facebook, yaitu Publik, Teman, Teman terkecuali, Teman spesifik, Hanya saya, dan Khusus.



Gambar 7.5: Pengaturan Pemirsa Postingan (Facebook)

Kategori Publik memberikan hak akses kepada seluruh orang yang berada di dalam atau luar lingkup pertemanan pengguna untuk bisa melihat unggahan terkait. Tentunya untuk memilih kategori Publik ini, pengguna harus bisa menjamin tidak ada informasi pribadi pengguna untuk menghindari kejahatan pencurian informasi pribadi.

Hak akses dengan kategori teman memberikan kebebasan pada setiap teman pengguna untuk bisa melihat postingan, tetapi tidak untuk orang di luar pertemanan Facebook. Hak akses Teman Terkecuali dan Teman Spesifik memiliki cara kerja yang sama, hanya berbeda kalau Teman Terkecuali ini mengecualikan teman yang dipilih, sedangkan Teman Spesifik memasukkan teman yang dipilih sebagai pengguna yang bisa mengakses unggahan.

Kategori Hanya Saya memberikan akses hanya untuk pengguna yang dapat melihat postingan, dan kategori yang terakhir memberikan hak kepada orang-

orang yang pengguna tambahkan secara khusus. Cara kedua adalah melakukan pengaturan privasi untuk keseluruhan akun Facebook yang dapat dilakukan dengan memilih menu tambahan yang ada pada profil pengguna. Menu yang dipilih adalah menu Pengaturan & Privasi lalu dilanjutkan dengan memilih submenu Privasi. Pilihan pengaturan privasi aktivitas akun Facebook biasanya akan ditampilkan seperti Gambar 7.6 berikut.



Gambar 7.6: Pengaturan Aktivitas (Facebook)

Instagram

Tidak berbeda dengan Facebook, untuk melakukan pengaturan privasi pada Instagram juga dapat dilakukan dengan mengakses menu pengaturan dan mengarah ke submenu Privacy and Security. Pengaturan privasi dan keamanan pada Instagram biasanya berupa mengatur siapa saja yang bisa melihat story dan postingan pengguna, melakukan komentar pada story dan postingan, mendapatkan mention, dan sebagainya. Pengaturan di Instagram terlihat lebih sederhana dan mudah untuk dilakukan dibandingkan dengan Twitter dan Facebook.

7.3.5 Permintaan Akses Aplikasi

Semakin majunya teknologi saat ini hampir seluruh aspek layanan baik yang diberikan pemerintah maupun swasta sudah berbasis aplikasi android atau IOS. Contohnya seperti layanan pembuatan paspor online yang sudah terintegrasi dengan aplikasi android bernama M-Pasport yang mempermudah masyarakat dalam membuat jadwal dan perjanjian pembuatan paspor. Tentunya dalam menggunakan aplikasi layanan seperti ini, pengguna harus memberikan hak akses kepada aplikasi apabila dibutuhkan.

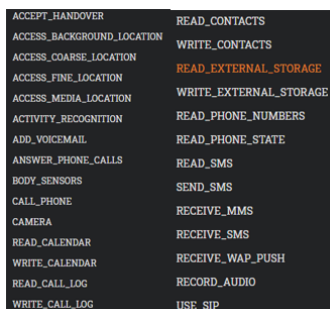
Seperti pada M-Pasport, pengguna diminta untuk memberikan akses kamera agar bisa merekam gambar dari dokumen yang diminta. Pengguna tentunya

akan mematuhi arahan dari aplikasi untuk memberikan akses kamera agar bisa menyelesaikan prosedur penjadwalan pembuatan paspor.

Aplikasi-aplikasi yang berasal dari pemerintah sebenarnya tidak perlu dikhawatirkan akan jaminan keamanan data dan perangkat apabila aplikasi meminta untuk mengakses beberapa layanan di smartphone, karena sudah ada aturan dan hukum yang mengatur layanan tersebut. Berbeda dengan aplikasi yang berlatar belakang seperti aplikasi layanan pemesanan makanan, antar jemput, atau aplikasi berbasis hiburan, pengguna harus waspada apabila aplikasi-aplikasi seperti ini meminta akses pada layanan smartphone. Sebagai pengguna aplikasi android atau iOS, tentunya sudah sangat sering mendapatkan permintaan hak akses kamera, GPS, dan bahkan daftar kontak. Pengguna harus sangat berhati-hati dalam memberikan hak akses apabila aplikasi yang digunakan sangat tidak relevan dengan permintaan hak akses layanan yang ada.

Sangat berbahaya apabila pengguna selalu menuruti permintaan hak akses dari aplikasi, karena bisa saja aplikasi yang sedang digunakan ini akan memanfaatkan informasi tersebut untuk kepentingan pribadi perusahaannya (seperti penjualan informasi pribadi). Setelah sudah mengetahui seberapa berbahayanya dampak dari penjualan informasi pribadi yang dimana bisa dijadikan bahan untuk penipuan. Oleh karena itu, sebagai pengguna yang bijak, pengguna harus paham akan dua jenis hak akses yang telah ditentukan oleh android, yaitu normal dan berbahaya. Jenis-jenis hak akses yang ada pada android dapat dilihat pada halaman *manifest permission* dan diantara banyaknya hak akses hampir 30 diantaranya berkategori kan berbahaya.

Hak akses yang dikategorikan pada kategori berbahaya dapat dilihat pada Gambar 7.7 berikut:



ACCEPT_HANDOVER	READ_CONTACTS
ACCESS_BACKGROUND_LOCATION	WRITE_CONTACTS
ACCESS_COARSE_LOCATION	READ_EXTERNAL_STORAGE
ACCESS_FINE_LOCATION	WRITE_EXTERNAL_STORAGE
ACCESS_MEDIA_LOCATION	READ_PHONE_NUMBERS
ACTIVITY_RECOGNITION	READ_PHONE_STATE
ADD_VOICEMAIL	READ_SMS
ANSWER_PHONE_CALLS	SEND_SMS
BODY_SENSORS	RECEIVE_MMS
CALL_PHONE	RECEIVE_SMS
CAMERA	RECEIVE_WAP_PUSH
READ_CALENDAR	RECORD_AUDIO
WRITE_CALENDAR	USE_SIP
READ_CALL_LOG	
WRITE_CALL_LOG	

Gambar 7.7: Hak Akses Pada Android (Facebook)

Pengguna harus melihat konteks dan hubungan antara hak akses yang diminta oleh aplikasi dengan layanan yang diberikan oleh aplikasi. Apabila pengguna mematikan seluruh hak akses aplikasi karena takut akan terjadinya kejahatan privasi, tentunya tidak ada aplikasi yang bisa berjalan sesuai dengan fungsinya.

Dalam menentukan wajar atau tidaknya hak akses yang diminta oleh aplikasi, mungkin bisa saja dianalogikan dengan permasalahan yang sederhana. Aplikasi dapat dianalogikan sebagai tukang bangunan yang akan memperbaiki rumah, tentunya hanya beberapa bagian dalam rumah yang bisa diakses oleh tukang bangunan untuk diperbaiki. Jika pengguna meminta tukang bangunan untuk memperbaiki ruang makan, sudah sepantasnya pemilik rumah memberikan akses bagi mereka untuk bisa masuk ke ruang makan.

Tetapi, apabila tukang bangunan meminta akses untuk masuk ke kamar pribadi, pengguna harus curiga dan sebisa mungkin untuk tidak memberikan akses tersebut karena tidak ada hubungannya dengan pekerjaan yang dilakukan tukang bangunan. Pola pengkondisian seperti ini sama dengan kondisi dimana pengguna dalam menghadapi permintaan hak akses aplikasi.

7.3.6 Berinternet Menggunakan Mode Pribadi

Selain memahami tentang memberikan hak akses kepada aplikasi yang digunakan, pengguna juga harus paham akan kemungkinan data pribadi yang dimiliki dapat diambil saat menggunakan browser. Melakukan aktivitas di browser merupakan kegiatan yang mungkin hampir setiap hari dilakukan dan secara tidak sadar browser juga sebenarnya mendapatkan beberapa data pribadi di saat pengguna menggunakannya.

Data atau informasi yang memungkinkan untuk didapatkan oleh browser adalah berupa informasi perangkat keras dan perangkat lunak yang digunakan, informasi koneksi (seperti IP), lokasi, sejarah pencarian, dan bahkan sampai informasi terkait pergerakan kursor. Dari data dan informasi tersebut, beberapa diantaranya sebenarnya bersifat rahasia seperti informasi lokasi, IP, dan sejarah pencarian.

Pengguna tentunya tidak ingin informasi yang bersifat rahasia ini dapat diakses oleh orang yang tidak bertanggung jawab. Oleh karena itu, untuk menghindari kekhawatiran dan permasalahan yang mungkin dialami pengguna, terdapat fitur pada beberapa browser untuk melindungi keamanan data pengguna, yaitu fitur *incognito*.

Fitur incognito dapat pengguna gunakan di browser seperti Chrome, Mozilla, Edge, dan lainnya. Cara kerja fitur incognito ini secara garis besar adalah memberikan layanan kepada pengguna untuk melakukan browsing atau pencarian di browser tanpa harus takut akan tersimpannya data aktivitas pencarian pada perangkat dan akun Google.

Selain itu, fitur incognito juga memberikan layanan yang dimana browser akan secara otomatis menghapus informasi terkait data situs dan cookies yang ada pada saat melakukan aktivitas pencarian, dan juga browser tidak akan menginformasikan kepada situs bahwa pengguna sedang melakukan pencarian secara rahasia dengan mode incognito.

Disamping dari beberapa kinerja fitur incognito yang dapat melindungi data pengguna, terdapat juga beberapa batasan yang dimiliki fitur ini. Fitur incognito tidak dapat merahasiakan data yang dimasukkan pada saat melakukan Sign In pada suatu website walaupun sudah dilakukan dengan fitur incognito, sehingga situs akan tetap bisa melacak dan mengambil data apabila melakukan sign in ke dalam situs.

Fitur incognito juga tidak menutup kemungkinan akan situs tetap mengambil informasi aktivitas dan lokasi pengguna. Sehingga secara garis besar, fitur incognito hanya akan melindungi pengguna melalui merahasiakan sejarah pencarian dan cookies.

7.4 Kebijakan Privasi Penyelenggara Sistem Elektronik

7.4.1 Bagaimana Penyelenggara Sistem Elektronik Menjaga Data Anda?

Salah satu kekhawatiran terbesar saat memberikan informasi online kepada penyelenggara sistem elektronik adalah mengetahui bagaimana perusahaan melindungi informasi yang pengguna titipkan. Banyak penyelenggara sistem elektronik menyebarkan informasi melalui situs web perusahaan mereka yang memberikan informasi dasar kepada pengguna tentang bagaimana perusahaan menangani dan melindungi informasi rahasia pengguna.

Di bawah ini terdapat dua contoh kasus dari perusahaan teknologi yang berkaitan dengan perlindungan data penggunanya:

Kasus Apple VS FBI

Pada halaman berita yang dilansir pada website The Guardian tahun 2016, yang berjudul “*Apple vs the FBI: what's the beef, how did we get here and what's at stake?*”, bercerita tentang perseteruan perusahaan teknologi Apple dengan badan investigasi pada departemen pertahanan Amerika (FBI). Permasalahan bermula saat ditemukannya ponsel pembunuh yang menggunakan iPhone 5C.

Pihak FBI meminta Apple untuk membantu mereka membuka data pelaku pembunuhan untuk proses penyelidikan lebih lanjut. Permintaan tersebut ditolak karena bertentangan dengan prinsip Apple yang berkomitmen untuk menjaga kerahasiaan privasi penggunanya.

Skandal Privasi Data Facebook

Pada tahun 2018, Facebook dituntut karena gagal melindungi data pribadi pengguna dalam pelanggaran Cambridge Analytica. Terdapat 87 juta data pengguna yang telah dimiliki perusahaan konsultasi politik asal Inggris tanpa izin. Penyalahgunaan data penggunanya oleh perusahaan konsultasi tersebut digunakan untuk memenangkan Presiden AS Donald Trump dalam pemilu presiden.

Kedua contoh kasus privasi data pengguna diatas dapat menjadi pelajaran bagi pengguna dimana penting untuk memahami penerapan kebijakan privasi yang diterapkan oleh setiap penyelenggara sistem elektronik.

7.4.2 Alasan Penerapan Kebijakan Privasi

Setelah mengetahui akan beberapa permasalahan yang terjadi karena kebijakan privasi, baik itu menguntungkan ataupun merugikan pengguna. Tentunya, sebagai perusahaan penyedia layanan elektronik tetap harus menyediakan layanan terkait kebijakan privasi pengguna.

Alasan mengapa penerapan kebijakan privasi ini penting, diantaranya karena:

Membangun Kepercayaan Pengguna

Diberikannya jaminan akan keamanan dan perlindungan privasi pada suatu layanan elektronik, membuat banyak pengguna menjadi tertarik dan memilih

untuk menggunakan layanan elektronik yang jelas akan penerapan kebijakan privasinya. Berdasarkan survei yang dilakukan oleh Price Waterhouse Cooper

Pada tahun 2018, kepercayaan termasuk ke dalam tiga faktor utama yang dicari pengguna untuk menentukan perusahaan bisnis yang diinginkan. Untuk meningkatkan rasa kepercayaan pengguna, tentunya perusahaan harus menjamin akan keamanan kerahasiaan data pengguna.

Selain menjamin kerahasiaan dan keamanan data, perusahaan juga bisa memberikan akses dan kontrol yang baik kepada pengguna untuk mengelola data pribadi yang mereka berikan kepada penyedia layanan elektronik (Geller, 2019).

Privasi Data Diatur Dalam Hukum

Banyaknya permasalahan yang terjadi tentang kebijakan privasi mengakibatkan hampir seluruh negara memiliki hukum yang mengatur keamanan data pribadi masyarakatnya. Di Indonesia sendiri, perlindungan atas privasi dan data pribadi dalam sistem elektronik diatur pada Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Permenkominfo 20/2016).

Sanksi yang dapat didapatkan bagi pelanggar berupa sanksi administratif dan gugatan ganti rugi dari pengguna yang menjadi korban. Sedangkan di Amerika Serikat, seperti yang sudah diketahui sebelumnya, mereka memiliki hukum yang mengatur akan jaminan keamanan data kesehatan di setiap fasilitas kesehatan. Amerika Serikat juga memiliki kebijakan terkait *Children's Online Privacy Protection Act Compliance Guide* yang melindungi informasi pengguna berusia di bawah 12 tahun.

Data Pribadi Dibutuhkan Oleh Pihak Ketiga

Data pribadi tentunya harus dilindungi dengan disediakannya kebijakan privasi pada setiap layanan sistem elektronik. Khususnya pada layanan-layanan seperti Google Analytics ataupun Google AdSense yang selalu membutuhkan data pribadi pengguna berupa history browser pengguna untuk menampilkan iklan.

Dengan diaturnya kebijakan privasi pengguna, layanan pihak ketiga seperti Google Analytics ataupun Google AdSense, tentunya tidak bisa menyalahgunakan kemampuan mereka dalam mengakses data pribadi pengguna. Hampir keseluruhan layanan pihak ketiga seperti ini memiliki

pernyataan khusus yang mengatur keamanan data pribadi pengguna pada dokumen kebijakan privasi layanan.

Oleh karena itu, pengguna juga harus teliti dalam membaca dokumen kebijakan privasi setiap layanan elektronik yang digunakan, apakah layanan tersebut benar-benar menjamin keamanan data pribadi pengguna atau tidak.

7.4.3 Kebijakan Privasi

Pada profil internet Indonesia yang dilansir dari APJII 2022, terdapat 13.03% pengguna internet di Indonesia pernah mengalami permasalahan keamanan saat berinternet. Terdapat 14.87% pengguna tidak tahu bagaimana cara mengamankan data miliknya. Tingkat pengetahuan dan kesadaran terkait keamanan data pengguna yang tidak baik akan berakibat pada permasalahan keamanan privasi dari data pengguna.

Berikut merupakan contoh penerapan kebijakan privasi pada aplikasi Whatsapp (WA):



Gambar 7.8: Kebijakan Privasi (WhatsApp)

Beberapa konfigurasi terkait privasi dapat diatur di menu pengaturan aplikasi Whatsapp, diantaranya:

1. Fitur sekali lihat dimana pengguna dapat mengirimkan foto dan video yang dapat menghilang setelah dilihat sekali.
2. Fitur verifikasi dua langkah yaitu fitur keamanan tambahan ketika masuk ke akun.
3. Fitur kunci akun pengguna dimana pengguna dapat menambahkan *face id* atau sidik jari yang terdaftar pada smartphone.

4. Fitur status laporan dibaca dimana pengguna dapat menghilangkan status sudah dibaca.
5. Fitur terakhir dilihat dimana pengguna dapat memilih apakah hanya kontak, semua orang, atau tidak seorang pun yang dapat melihat kapan terakhir kali pengguna membuka Whatsapp.
6. Fitur privasi foto profil dimana pengguna dapat menentukan apakah hanya kontak, semua orang, atau tidak seorang pun yang dapat melihat foto profil.
7. Fitur privasi status dimana pengguna dapat memilih siapa yang dapat melihat pembaruan status.
8. Fitur privasi grup dimana pengguna dapat memilih apakah semua orang, semua kontak, atau hanya sebagian kontak yang dapat menambahkan dirinya ke chat grup.

Berikut beberapa contoh kebijakan privasi dari penyelenggara sistem elektronik, diantaranya:

Tabel 7.1: Kebijakan Privasi Penyelenggara Sistem Elektronik

No	PSE	Jenis	Sumber
1	Google	Mesin Pencarian	https://safety.google/intl/id_id/principles/
2	Safari	Browser	https://www.apple.com/id/safari/docs/Safari_White_Paper_Nov_2019.pdf
3	Facebook	Media Sosial	https://www.facebook.com/privacy/policy/
4	Whatsapp	Pesan Instan	https://www.whatsapp.com/privacy
5	Instagram	Aplikasi berbagi foto dan video	https://help.instagram.com/811572406418223
6	Uber	Taxi online	https://privacy.uber.com/privacy/center
7	Tokopedia	marketplace	https://www.tokopedia.com/privacy?lang=id
8	Epic Games	Game Online	https://www.epicgames.com/site/en-US/privacypolicy
9	Traveloka	Tiket pesawat online	https://www.traveloka.com/en-id/privacypolicy

Bab 8

Keamanan Web

8.1 Pendahuluan

Fakta mendasar dalam keamanan Internet dan keamanan aplikasi web adalah ketidakmungkinan jaminan 100 persen bahwa sistem komputer dapat diandalkan. Keamanan Internet adalah proses mempertahankan dan melestarikan sumber daya dan data organisasi yang dibagikan di Internet. Keamanan Internet adalah salah satu subjek terpenting yang dapat memengaruhi berbagai pengguna Internet. Orang-orang menggunakan Internet untuk menjual, membeli, dan bahkan untuk berkomunikasi membutuhkan komunikasi atau produk mereka untuk diautentikasi, dapat diandalkan, dan aman (Von Solms and Van Niekerk, 2013).

Saat ini, penggunaan web menjadi semakin penting dalam kehidupan sehari-hari. Hal ini dapat dilihat dari bertambahnya jumlah organisasi atau perusahaan yang mengimplementasikan penggunaan web dalam organisasi mereka. Web menjadi fasilitas untuk menarik orang yang biasanya digunakan untuk bisnis atau perdagangan. Hal tersebut sekaligus menjadikan web sebagai target yang bagus oleh hacker.

Oleh karena itu, World Wide Web (WWW) telah dikembangkan dari halaman web statis ke platform dinamis, yang terhubung ke database untuk

menyediakan aplikasi yang berbeda, yang dikenal sebagai aplikasi web (Andress, 2019).

Aplikasi web ini digunakan di banyak bidang bisnis, bisa berupa situs web yang menyediakan informasi tentang bidang tertentu atau banyak bidang, atau situs web e-Commerce untuk memungkinkan pelanggan menjual dan membeli barang, atau aplikasi solusi di ekstranet dan/atau intranet organisasi. Aplikasi web juga dapat berupa server email atau mesin pencari.

Sistem berbasis komputer berada di belakang semua aplikasi ini, dan celah keamanan ada di sini. Jika penyerang berhasil meretas aplikasi web ini dan berhasil mencapai sistem berbasis komputer atau database, server, atau pengaturan sistem operasi maka perusahaan akan berada dalam masalah kritis. Jika penyerang tidak dapat mencapai ke sistem berbasis komputer, penyerang mungkin mengirim kueri yang salah yang merusak perangkat keras dan perangkat lunak; mengarah ke akses data yang tidak sah, dan operasi bisnis menjadi terganggu (Pan et al., 2019).

Banyak penelitian yang membahas tentang kerentanan aplikasi web, membuktikan bahwa hampir semua aplikasi web tidak aman, beberapa penelitian menunjukkan bahwa setengah dari aplikasi web memiliki tingkat risiko tinggi dan lainnya menunjukkan bahwa 80% dari aplikasi web memiliki setidaknya satu ancaman keamanan kritis.

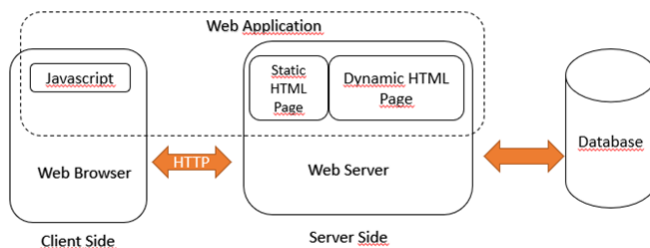
Selama beberapa tahun terakhir, ada banyak teknologi yang diperkenalkan oleh lembaga dan industri pemerintah untuk melindungi sistem mereka. Teknologi ini harus cukup untuk melindungi sistem elektronik. Namun, teknologi tersebut tidak terlalu efisien karena kurangnya alat eksperimental yang dipercaya untuk melindungi sistem dan kurangnya penelitian dan studi untuk meningkatkan pengembangan dan pengujian alat keamanan generasi berikutnya.

Selain itu, beberapa penelitian percaya bahwa mengamankan Internet berkecepatan tinggi dari virus merupakan faktor penting saat ini untuk melindungi aplikasi web. Studi-studi ini juga mempertimbangkan manfaat alat pemindai virus untuk melindungi komputer pribadi, server, proxy, dan gateway dari banyak virus yang terkenal dan bagaimana cara menghapusnya dari data, file, dan paket yang akan mencapai aplikasi web. Tingginya biaya alat keamanan juga merupakan alasan penting lain dari tidak amannya server web.

Dalam bab ini akan dibahas terkait jenis serangan, metodologi, dan teknik perlindungan dalam keamanan web. Akan dibahas juga tentang teknik keamanan profesional yang dapat digunakan untuk melindungi aplikasi web yang rentan terhadap serangan injeksi SQL, dan untuk memperjelas mekanisme yang benar yang harus diterapkan untuk melindungi dari injeksi SQL dan masalah validasi input. secara umum. Injeksi SQL sebagai teknik peretasan, yang merupakan teknik penting, juga dibahas secara rinci.

Kelemahan Keamanan Web

Aplikasi web terdiri dari tiga bagian utama seperti yang ditunjukkan pada Gambar 8.1. Bahasa pemrograman digunakan untuk mendesain sisi klien dan untuk membuat kueri basis data. Protokol transfer Hypertext (http) digunakan untuk menghubungkan sisi klien dengan sisi server. Hal ini juga digunakan untuk proses bisnis yang merupakan bagian pembeda dari setiap aplikasi web.



Gambar 8.1: Bagan Aplikasi Web

Ancaman utama lainnya dalam keamanan internet dan aplikasi web yang dijelajahi pengguna melalui *port default* nomor 80 menggunakan protokol http dan nomor port 443 menggunakan protokol lapisan aman https. Penyerang mulai menggunakan web sebagai pengguna normal situs web kemudian port ini digunakan untuk menyerang situs dan mengakses data dan file pelanggan. Ukuran serangan tergantung pada pentingnya data dan bisnis perusahaan yang memiliki situs web ini.

Semua website bisnis pada akhirnya akan mengalami serangan siber. Dalam beberapa kasus seperti situs Western Union dan Walt Disney Company, penyerang menggunakan masalah keamanan bawaan dalam aplikasi web untuk mengakses data web atau untuk mendapatkan data dari sistem atau basis data terkait.

Perlu diketahui bahwa menggunakan metode pencegahan keamanan tidak cukup untuk mengamankan aplikasi web, metode tersebut terdiri dari:

1. Enkripsi dan Dekripsi.
2. Lapisan HTTP atau Secure Socket.
3. Akun dan kata sandi.
4. Memindai program.
5. Firewall.
6. Sistem Deteksi Intrusi.

Dalam serangan siber, penyerang akan mulai menggunakan aplikasi web sebagai pengguna atau pelanggan biasa. Kemudian dia dapat melewati beberapa alat pencegahan seperti firewall atau sistem deteksi intrusi hingga mencapai lapisan aplikasi di mana dia akan memulai serangannya.

Melindungi Situs Web

Keamanan bukanlah hal yang mudah untuk diterapkan. Biaya mengamankan situs web statis kecil untuk beberapa organisasi bisa lebih besar daripada yang bisa dibayar. Biaya tinggi ini berasal dari pertimbangan bahwa kita tidak hanya perlu melindungi data pelanggan tetapi juga kita perlu melindungi sistem dari serangan yang sering terjadi seperti serangan *Denial of Service*, yang membuat situs web menjadi down. Serangan-serangan ini dapat mencegah beberapa organisasi yang bergantung pada e-business atau e-Commerce untuk melakukan pekerjaan mereka.

Oleh karena itu, sebagian besar aplikasi web perusahaan cenderung berada di bawah risiko serangan. Untuk melindungi aplikasi web ini, pakar keamanan harus memiliki kemampuan untuk mendeteksi ancaman keamanan dan pintu belakang dalam aplikasi web mereka. Setelah itu, mereka dapat memberikan solusi mulai dari masalah yang mendesak dan prioritas tertinggi seperti *Denial of Service* hingga mencakup semua ancaman keamanan.

8.2 Serangan Pada Web

Anatomi Serangan Web

Struktur serangan pada aplikasi web umumnya melalui langkah-langkah berikut (Li and Xue, 2011):

1. Pemindaian
Awalnya sebagian besar penyerang memulai dengan memindai semua *port default* yang terbuka pada alamat IP aplikasi web atau database yang dimulai dengan *port default*.
2. Mengumpulkan informasi
Setelah pemindaian, penyerang mencoba mengetahui versi dan edisi server web dan Sistem Manajemen Basis Data (DBMS) yang digunakan dalam aplikasi web yang ditargetkan. Kemudian penyerang mencoba menggunakan pengaturan dan kata sandi publik dan default.
3. Pengujian kode
Penyerang akan mulai setelah itu mencari kesalahan pengembangan atau apa pun yang dapat membuat menyerang aplikasi web. Kesalahan ini dapat ditemukan melalui menjalankan proses pengujian normal untuk kode dan skrip yang digunakan di web.
4. Perencanaan serangan
Setelah semua langkah sebelumnya, penyerang dapat merancang rencana lengkap untuk meluncurkan serangannya pada aplikasi web.
5. Peluncuran serangan
Berdasarkan informasi yang dikumpulkan dan rencana yang diajukan penyerang menyerang situs web mencoba merusak semua data atau mendapatkan data aplikasi kita yang rentan.

Teknik Serangan Web

Banyak teknik serangan yang digunakan terhadap berbagai macam aplikasi web. Tetapi ada beberapa teknik yang menargetkan lapisan pengembangan (development layer) aplikasi web seperti berikut ini:

1. Melewati Parameter
Berarti mengirim beberapa tipe parameter ke aplikasi web untuk mendapatkan lebih banyak data daripada apa disediakan web. Melewati parameter bisa dalam format sederhana dan hanya meneruskan parameter ke halaman web untuk mendapatkan beberapa data internal atau bisa juga dalam format tertentu dan mengirim

parameter ini melalui query SQL untuk mendapatkan data yang lebih sensitif dari database.

2. Memaksa program

Dalam situasi ini, penyerang memaksa aplikasi web ke untuk mendapatkan beberapa parameter debugging dan pengujian sehingga penyerang dapat melihat lingkungan tersembunyi pada aplikasi atau dapat membuat situs web down.

3. Mengakses cookie

Beberapa penyerang mencoba mengakses konten cookie yang telah ditransfer antara klien dan aplikasi web. Penyerang dapat memperoleh akses ke aplikasi web terbatas menggunakan informasi dalam cookie.

4. Pencarian file default

penyerang dapat meminta file default dari lingkungan pemrograman yang mungkin tetap dapat diakses oleh pemrogram. File-file ini dapat digunakan untuk mengakses informasi koneksi yang tidak sah.

8.3 Metodologi Serangan Web

Pada umumnya terdapat dua metodologi utama serangan terhadap web, serangan statis dan dinamis. Penyerang biasanya menggunakan metode serangan yang umum dan terkenal dalam mengeksekusi serangannya dalam metode yang disebut sebagai metodologi serangan statis. Sedangkan, menggunakan metode serangan yang kompleks yang sulit untuk dicegah dan dideteksi disebut metodologi serangan dinamis.

Metode Serangan Statis.

Ada banyak metode terkenal yang digunakan dalam metodologi serangan statis seperti metode berikut:

1. Exploits

Dalam metode statis ini, penyerang mencoba menerapkan metode serangan yang sudah umum karena telah digunakan dalam menyerang aplikasi web semacam itu. Penyerang mendapatkan

metode ini dari penyerang yang sudah ahli atau dari forum dan mesin pencari.

2. Directory Enumeration

Penyerang mencoba metode ini untuk mendapatkan peta aplikasi web dan struktur direktori web untuk memahami hierarki aplikasi web. Dalam metode ini, penyerang mencoba menggunakan file dan folder tersembunyi yang umum digunakan dalam struktur web serupa untuk mengakses informasi penting di dalam situs.

3. Debugging

Menemukan backdoors dan kesalahan kode untuk mendapatkan informasi yang berguna untuk menyerang aplikasi web. Sebagian besar pengembang aplikasi web meninggalkan kesalahan kode dan backdoors di dalam aplikasi mereka.

Metodologi Serangan Dinamis

Metode dinamis lebih kompleks daripada metode statis dan dapat diubah dari satu aplikasi ke aplikasi lainnya.

Seperti metode berikut:

1. Link traversal

Penyerang melacak URL situs web tertentu untuk mengetahui beberapa tautan dan URL yang tidak lagi tersedia atau ada. Tautan ini mungkin masih menjangkau beberapa informasi berharga yang belum dihapus dari aplikasi web.

2. Path truncation

Sebagian besar halaman galat situs web mengarahkan penyerang untuk mengetahui struktur direktori dalam aplikasi web tersebut.

3. Session hijacking

Penyerang mendapatkan informasi dan parameter nilai sesi dalam metode ini. Dengan menggunakan metode ini, penyerang mendapatkan izin untuk data yang tidak sah.

4. Hidden web tracks

Penyerang memeriksa kode html halaman web tertentu untuk mengetahui beberapa jalur tersembunyi di aplikasi web atau jalur direktori lama.

5. Java Applet Reverse Engineer

Beberapa penyerang mendekompilasi kode Java Applet pada login situs klien. Metode ini mendapatkan informasi yang tidak sah dari situs web dan membiarkan penyerang mengakses situs web.

6. Memeriksa folder cadangan dan ekstensi file default

Penyerang memulai serangan dari ekstensi file umum dan folder cadangan.

7. Melewati parameter

Sebagian besar aplikasi Web memungkinkan penggunaanya mengirimkan parameter ke sistem mereka melalui formulir web. Penyerang mengirimkan parameter yang tidak valid melalui formulir ini untuk menyalahgunakan aplikasi web.

8. Mengeksekusi scripts

penyerang memaksa server web untuk mengeksekusi skrip yang tidak ada di dalam aplikasi webnya. Tujuan mengeksekusi skrip asing ini adalah untuk mencuri beberapa informasi dan cookie pengguna.

9. SQL Injection

Injeksi SQL, di mana penyerang memasukkan pernyataan dan perintah SQL ke server web untuk menyerang database dan mendapatkan informasi yang berguna (Valeur, Mutz and Vigna, 2005).

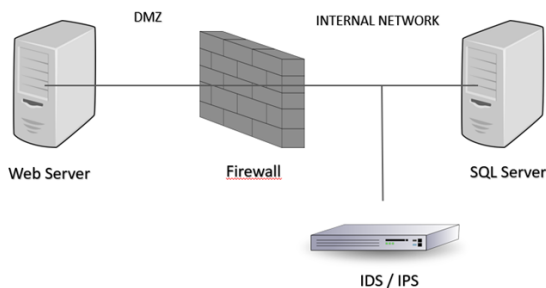
8.4 Teknik Perlindungan Keamanan Web

Intrusion Detection System

Intrusion Detection System (IDS) digunakan untuk mendeteksi berbagai jenis serangan yang dapat membahayakan keamanan sistem aplikasi web (Cao, Qiao and Lyu, 2018). Jenis serangan yang dapat dideteksi oleh IDS termasuk Worms, Virus, login yang tidak sah, akses ke file dan folder sensitif, dan yang terkait hak akses.

Intrusion Prevention System

Perlindungan otomatis lainnya disebut *Intrusion Prevention System* (IPS). IPS biasanya merupakan perangkat yang memantau jaringan untuk memantau perilaku pengguna yang berwenang dalam jaringan (Vinayakumar et al., 2019). Oleh karena itu, IPS akan mencegah pengguna yang tidak berwenang mengakses aplikasi web dan sumber daya jaringan.



Gambar 8.2: IDS/IPS

Kata Sandi

Kekuatan keamanan kata sandi tergantung pada pengguna yang membuatnya dan juga kombinasi karakter, huruf, dan angka. Secara umum, metode termudah untuk mengakses kata sandi adalah dengan pengetahuan orang dalam. Penyerang dapat melacak profil seseorang dari situs web sosial untuk mendapatkan informasi tentang dia untuk menebak kata sandi aplikasi web organisasinya.

Saat ini, sebagian besar aplikasi web mencoba menunjukkan kepada klien tingkat kerumitan kata sandi mereka saat pembuatan akun. Aplikasi web lain juga memilih kata sandi acak secara default yang sangat kompleks dan sulit diingat dari pengguna itu sendiri, yang membuat mereka menuliskannya di mana saja dan hal itu menyebabkan kemungkinan ancaman lain. Kata sandi itu sendiri tidak bisa menjadi satu-satunya teknik perlindungan yang digunakan oleh perusahaan.

SSL dan Enkripsi Data

Protokol Socket Secure Layer (SSL) dan enkripsi data dapat mengamankan data pengguna selama transmisi data tersebut dari server web ke mesin klien. Namun, server dan sistem klien perlu mendekripsi data ini begitu mereka ingin membacanya atau memodifikasinya.

Enkripsi data yang sama seperti password tidak dapat bekerja sendiri tanpa teknik proteksi lainnya. Biasanya enkripsi dan dekripsi ini didasarkan pada kunci bersama yang perlu diketahui oleh klien dan server. Oleh karena itu, pendistribusian *shared key* ini juga harus dilakukan melalui proses yang aman.

Firewall

Seperti yang ditunjukkan pada Gambar 8.2 firewall seperti penghalang di dalam jaringan yang memungkinkan hanya orang yang memiliki akses resmi untuk melewati gerbang ini. Firewall dapat berupa perangkat keras atau perangkat lunak yang dapat dikonfigurasi untuk mengizinkan dan memblokir pengguna, paket, port, atau bahkan alamat internet (IP) tertentu (Babiker, Karaarslan and Hoscan, 2018).

Penyerang dapat melakukan proses untuk meyakinkan firewall bahwa dia adalah pengguna yang berwenang untuk melewatinya dan inilah yang biasanya terjadi pada virus Trojan horse. Dalam jaringan komputer, firewall bekerja dengan router. Firewall memindai setiap paket jaringan untuk memutuskan apakah akan meneruskannya ke tujuannya di dalam jaringan perusahaan atau melarang pengirimannya.

Firewall juga bekerja dengan server proxy yang membuat permintaan jaringan atas nama sistem pengguna. Firewall sering dipasang di komputer khusus yang terpisah dari jaringan lainnya sehingga tidak ada paket yang datang langsung ke sistem server di jaringan perusahaan.

Program Pemindaian Standar

Serangan dan ancaman keamanan yang telah teridentifikasi disimpan di dalam sebuah pemindai otomatis untuk memindai semua program dan paket yang dikirim atau diterima pada sistem klien. Sebagian besar pemindai otomatis ini melindungi jaringan organisasi dari serangan yang sudah diketahui sebelumnya. Pemindaian dilakukan pada perangkat keras dan perangkat lunak. Sebagian besar pemindai ini mengamankan sistem dari daftar ancaman yang sudah ditetapkan.

Oleh karena itu, tidak ada jaminan untuk melindungi aplikasi dan sistem dari jenis serangan baru yang belum pernah terjadi. Terkadang pemindai dapat memperingatkan pengguna bahwa dengan melakukan beberapa tindakan atau mengakses beberapa file yang rentan dan memiliki risiko keamanan. Biasanya aplikasi ini memerlukan pembaruan harian untuk memperbarui daftar ancaman untuk memasukkan ancaman baru yang baru saja terjadi pada sistem komputer lain.

Penyedia Layanan Internet (ISP)

Sebagian besar teknik perlindungan terutama untuk menjamin pengamanan sistem dan data dilakukan secara mandiri oleh organisasi atau perusahaan, bukan oleh ISP. Namun demikian, saat ini sebagian besar pihak ketiga mulai bekerja sama dengan ISP dalam hal peningkatan keamanan untuk meningkatkan atau mempertahankan reputasi ISP di pasaran.

Implementasi Kode

Pemrogram / programmer bukanlah pakar keamanan sehingga mereka tidak terlalu mempertimbangkan ancaman keamanan saat mengembangkan aplikasi. Beberapa perusahaan software besar menerapkan pengujian keamanan untuk aplikasi mereka setelah fase pengembangan. Sementara sebagian besar perusahaan ini hanya berurusan dengan keamanan setelah aplikasi mereka menghadapi serangan.

Namun, untuk melindungi sistem tidak hanya harus menguji kode program tetapi perlu diterapkan semua validasi dan verifikasi yang diperlukan dalam fase pengembangan kode. Selain itu, hal ini bertujuan untuk mengamankan semua server dan database yang bekerja di latar belakang aplikasi ini. Penguji bukan seorang penyerang sehingga dia tidak bisa membayangkan secara lengkap cara menyerang sebuah sistem.

Oleh karena itu, perusahaan harus mulai merekrut pengujian dari kalangan penyerang yang biasa disebut *white hat hacker*, menyerang sistem yang direkrut secara resmi untuk menguji keamanan sebuah sistem.

Bab 9

Keamanan Mobile

9.1 Pendahuluan

Perkembangan teknologi yang semakin canggih membuat semua berubah, saat ini orang-orang lebih memilih untuk melakukan segala aktivitasnya menggunakan smartphone. Saat ini smartphone menjadi perangkat yang penting dan hampir setiap orang memiliki smartphone dengan fitur dan aplikasi yang berbeda-beda.

Dengan perangkat yang canggih tersebut, orang-orang tidak hanya melakukan panggilan telepon, mengirimkan SMS saja, namun orang dapat mengirimkan e-mail, chatting, internet browsing, games, GPS, menyimpan gambar atau video ataupun melakukan pembayaran secara online. Perangkat mobile seperti smartphone saat ini tak hanya berfungsi sebagai telepon dan SMS atau chat semata. Kini, banyak aktivitas yang berhubungan dengan internet bisa dilakukan menggunakan smartphone yang ada di genggaman kita.

Oleh sebab itu, tak heran jika penggunaan perangkat mobile kian meningkat. Meski begitu, seiring peningkatan perangkat mobile itu ternyata terjadi peningkatan bahaya online yang mengintai pengguna (Listiyani, 2017). Aplikasi para smartphone sangatlah rentan terhadap berbagai macam kejahatan pada dunia cyber. Oleh karena itu, keamanan perangkat ini perlu diperhatikan karena pengguna mungkin saja mengakses Wireless yang tidak aman ataupun

mendownload aplikasi yang sudah terdapat malware atau virus yang menjadi celah untuk melakukan serangan.

Keamanan merupakan aspek penting dari sebuah sistem, namun masalah keamanan sering kurang mendapat perhatian. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima (Rohmansyah and Nurwasito, 2018).

9.2 Ancaman Pada Perangkat Mobile

Menurut Yong Wang dan Yazan Alshboul (2015), beberapa ancaman dan serangan pada smartphone seperti *malware*, *sniffing*, *spamming*, *spoofing*, *phishing*, *pharming*, *vishing*, *data leakage*, DOS, dll. Namun pertumbuhan serangan malware lebih tinggi dibandingkan serangan lainnya.

Menurut Darko Hrestak, dkk (2015), malware dapat menyebabkan kerusakan seperti mengubah data (menghapus, menyembunyikan, mencuri), menghabiskan bandwidth, menginstal aplikasi tanpa sepengetahuan kita atau mendapatkan akses ke sumber sistem tanpa seizin pengguna. Oleh karena itu, malware dikatakan berbahaya.

Malware terdiri dari beberapa elemen yang memiliki kapabilitas untuk melakukan berbagai macam tugas seperti (Hrestak et al., 2015):

1. Trojan merupakan program yang terlihat legal namun setelah kita menginstalnya maka akan menyebabkan kerugian bagi user.
2. Worm merupakan program mencurigakan yang mereplikasi dirinya sendiri. Contoh worm yaitu Selfmite.b yang menyebarkan pesan berisi link url address yang sudah ditanami malicious code.
3. Spyware merupakan malware yang tujuan utamanya yaitu mengakses dan mengintai data personal dari perangkat user.
4. Adware merupakan program dimana banner iklan ditampilkan namun ternyata terdapat program lain yang berjalan di belakangnya

Menurut Persin Kaur Granthi dan S. M. Bansode (2017), setidaknya ada empat ancaman pada keamanan perangkat mobile seperti:

1. Kebocoran data
Data atau informasi sensitif yang bocor menyebabkan perangkat menjadi kondisi kritis. Eksploitasi kerentanan ini sangat mudah karena penyerang dapat memperoleh akses tempat data sensitif disimpan.
2. Eskalasi hak istimewa
Kekurangan keamanan mekanisme izin android dapat menyebabkan peningkatan eskalasi hak istimewa yang disebabkan oleh aplikasi yang dikompromikan. Pelanggaran hak istimewa di android membuat jutaan pengguna berisiko dibajak smartphonenya.
3. Pengemasan ulang aplikasi
Proses pembongkaran atau dekompile file .apk menggunakan teknik rekayasa balik (reverse engineering) dan menyusupkan kode berbahaya ke dalam kode sumber utama dikenal sebagai pengemasan ulang aplikasi android. Untuk pengguna android, menjadi sulit untuk membedakan antara aplikasi palsu yang di paket ulang dan aplikasi normal karena aplikasi yang dikemas ulang biasanya berfungsi dengan cara yang sama dengan yang sah.
4. Serangan DDos
Dalam serangan DDos, penyerang berusaha membuat perangkat atau sumber daya tidak tersedia untuk penggunaan yang dimaksudkan dengan mengganggu layanan perangkat host untuk sementara atau tidak terbatas.

Menurut I Gusti Gede Krisna Dewanta (2020), jenis-jenis ancaman siber yang umum terjadi dan dapat membahayakan perangkat mobile pengguna, seperti:

1. Serangan dari aplikasi ilegal
Umumnya para pengguna perangkat mobile tertarik menggunakan aplikasi ilegal yang tersebar di banyak tempat untuk dapat menggunakan aplikasi secara gratis atau tanpa melakukan pembelian terhadap aplikasi tersebut pada toko aplikasi resmi. Namun, tidak

semua aplikasi ilegal tersebut bersih dari celah serangan siber yang dapat masuk ke perangkat mobile, justru banyak pihak yang dengan sengaja memasukkan program jahat ke perangkat mobile anda melalui aplikasi ilegal tersebut.

2. Serangan phishing

Phishing merupakan salah satu dari ancaman serangan siber dengan tingkat keberhasilan paling tinggi. Pada umumnya, metode phishing dilakukan oleh para penjahat siber melalui email pribadi maupun email kantor dari calon korbannya, umumnya penjahat siber akan memancing calon korbannya untuk mengklik sebuah link untuk kemudian mengarahkan calon korbannya ke sebuah website palsu, tanpa sadar calon korban pun mengisi data-data personal, sehingga penjahat siber dapat dengan leluasa menggunakan data-data tersebut untuk memperoleh keuntungan serta akan menimbulkan kerugian hingga finansial kepada korbannya.

3. Serangan Man-in-The-Middle (MiTM)

Melalui perangkat mobile, pengguna dapat saling berkomunikasi dan terkoneksi ke berbagai belahan dunia. Setiap hari, ribuan bahkan jutaan informasi saling bertukar melalui perangkat mobile. Melalui peluang inilah para penjahat siber memanfaatkan dengan melakukan serangan *Man-in-The-Middle* (MiTM). Para penjahat siber melakukan tindakan yang dinamakan intercept, yaitu kegiatan ini akan mencegah lalu lintas data antara perangkat mobile dengan access point. Tujuannya adalah, agar penjahat siber dapat membaca semua komunikasi data yang terjadi tanpa diketahui oleh pengguna perangkat mobile tersebut.

Biasanya dampak perangkat mobile yang terkena serangan, contohnya apabila smartphone kita terkena malware maka smartphone kita akan mengalami gangguan seperti performa yang menurun, adanya pesan spam, operasi berjalan lambat, atau yang parahnya mungkin kita tidak dapat menerima atau membuat panggilan serta besar kemungkinan kita dapat kehilangan data yang mungkin berpengaruh pada finansial kita.

Adapun skenario serangan yang pernah terjadi pada smartphone adalah sebagai berikut (Kaspersky, 2014):

1. Penyerang membuat suatu website dan mengundang user untuk membuka website tersebut.
2. Pada website tersebut ditampilkan halaman untuk mengunduh aplikasi yang telah ditanami malware.
3. Halaman website tersebut dibuat semenarik mungkin sehingga user mendownload aplikasi tersebut.
4. Setelah user mendownload aplikasi tersebut maka smartphone telah terinfeksi malware dan attacker dapat melakukan apa saja apabila smartphone telah terinfeksi.

9.3 Celah Keamanan Perangkat Mobile

Celah-celah keamanan yang terdapat di aplikasi mobile dapat digunakan penyerang untuk mencuri informasi penting di dalam smartphone, dimana informasi merupakan salah satu aset penting dan sangat berharga disajikan dalam berbagai format berupa: catatan, lisan, elektronik, pos, dan audio visual. (Hanifurohman and Hutagalung, 2020).

Menurut Yong Wang, dkk (2012), pada setiap perangkat, baik komputer maupun smartphone, pasti memiliki celah keamanan. Dengan adanya celah keamanan tersebut maka attacker dapat menjadikannya tempat untuk melakukan serangan.

Berikut merupakan celah keamanan yang mungkin ada pada smartphone:

1. Celah keamanan yang pertama dan merupakan celah keamanan yang ada pada perangkat pengguna. Dengan menggunakan *social engineering* mungkin penyerang memiliki informasi mengenai karakteristik atau cara kita dalam menggunakan smartphone sehingga membuat penyerang lebih mudah dalam merancang skenario untuk melakukan penyerangan.
2. Celah keamanan selanjutnya yaitu dari sistem operasi yang ditanamkan pada smartphone seperti iOS, Android, Blackberry, atau

Windows Phone. Untuk melakukan penyerangan biasanya penyerang mencari informasi mengenai kelemahan sistem operasi yang kita gunakan. Kelemahan sistem operasi ini yang akan digunakan penyerang untuk melakukan penyerangan seperti mencuri data.

3. Celah keamanan lainnya yaitu apabila smartphone kita terkoneksi dengan bluetooth atau terkoneksi ke jaringan 2G/3G/4G atau jaringan Wi-Fi sehingga dapat mengakses internet. Saat perangkat kita terkoneksi pada sebuah jaringan maka kemungkinan terdapat penyerang yang akan merekam lalu lintas pada jaringan tersebut.
4. Celah keamanan yang paling banyak mengancam smartphone kita yaitu celah keamanan yang ada pada aplikasi yang kita instal. Karena terdapat sistem operasi yang mengizinkan pihak ketiga dalam membuat aplikasinya, maka kemungkinan adanya bug pada aplikasi tersebut dapat menjadi celah keamanan bagi smartphone
5. Tempat penyimpanan data yang tidak aman juga dapat menjadi salah satu celah keamanan smartphone kita karena dapat menimbulkan aplikasi saling mencuri data.
6. Embedded sensor yang tertanam pada perangkat kita pun dapat dijadikan sebagai celah keamanan smartphone

Dengan adanya celah keamanan tersebut, maka penyerang dapat menjadikannya tempat untuk melakukan serangan. Dan untuk mengetahui apakah celah keamanan atau aplikasi berbahaya yang ada pada smartphone kita, kita dapat mengujinya. Pengujian ini berfokus pada aktivitas yang berbahaya atau mencurigakan, adanya celah keamanan dan kemungkinan adanya risiko keamanan (Wang and Alshboul, 2015).

1. Mobile forensik

Mobile forensik merupakan cara yang legal untuk mendapatkan dan memeriksa data pada smartphone. Data yang didapati dapat berupa salinan SMS/MMS, e-mails, call log, calendar events, web trafik, bookmark, gambar, voice mail, informasi lokasi, aplikasi data, dll.

2. Penetrasi tes

Penetration tes ini juga dapat digunakan untuk menguji keamanan dari sebuah smartphone. Penetration test ini terdiri dari konfigurasi

pengujian lingkungan, melakukan prosedur pengujian, membandingkan dan menganalisis hasil dari pengujian, dll.

3. Static analysis

Static analysis ini proses analisis aplikasi tanpa menjalankan aplikasi tersebut. Static analysis ini akan mereview kodingan dari aplikasi untuk menemukan fungsi yang mencurigakan. Keluaran dari proses ini yaitu signature yang dapat digunakan sebagai signature untuk software pendeteksi malware.

4. Dynamic analysis

Dynamic analisis merupakan proses analisis aplikasi saat menjalankan aplikasi tersebut pada lingkungan yang terlindungi. Analisis ini akan memonitor trafik jaringan dan komunikasi lainnya untuk mengetahui aktivitas yang mencurigakan.

9.4 Teknik Keamanan Perangkat Mobile

Perangkat mobile saat ini, memang sangat bermanfaat tapi juga mendatangkan risiko, karena perangkat mobile tersebut bukan saja sebagai alat komunikasi dan penyimpanan data, tapi juga berfungsi sebagai dompet dan pusat jaringan sosial kita. Untuk itu kita harus mencegah dari risiko keamanan perangkat mobile dari orang yang tidak bertanggung jawab.

Adapun tujuan dasar yang utama untuk melakukan keamanan pada perangkat mobile adalah sebagai berikut:

1. Confidentiality, menjamin bahwa data yang tersimpan di perangkat mobile tidak dapat diakses oleh pihak yang tidak berwenang.
2. Integrity, mendeteksi perubahan yang disengaja atau tidak disengaja pada data yang tersimpan.
3. Availability, menjamin bahwa pengguna dapat mengakses sumber daya menggunakan perangkat mobile ketika dibutuhkan.
4. Untuk mencapai tujuan tersebut, perangkat mobile harus diamankan dari berbagai ancaman dan kelemahan.

Menurut Advent Jose (2014), beberapa cara mengamankan jaringan internet di rumah dari ulah penyerang adalah:

1. Membentengi WiFi

Memproteksi jaringan internet yang berasal dari sinyal perangkat router mutlak dilakukan. Pengguna dapat mengubah nama login dan password yang digunakan untuk mengakses WiFi dari router tersebut. Selain itu, pengguna juga dapat menghidupkan WPA atau WPA encryption. Pengguna perlu memastikan software untuk router (firmware) tetap up-date.

2. Install antivirus

Perangkat yang tidak mengupdate program antivirus lebih rentan enam kali lipat terinfeksi virus. Oleh karena itu, antivirus perlu selalu diupdate demi keamanan program maupun data yang tersimpan di komputer dan perangkat mobile lainnya.

3. Update Sistem Operasi

Penyerang lebih suka menyerang perangkat yang belum memperbarui sistem operasinya. Itulah mengapa vendor teknologi terus melakukan upaya update untuk melindungi penggunanya.

Menurut Liana Threestayanti (2020), berikut beberapa teknik yang dilakukan untuk menghindari risiko keamanan melalui perangkat mobile, yaitu:

1. Autentikasi pengguna

Langkah atau tindakan pengamanan, seperti *screen locking* dengan password atau autentikasi biometrik penting untuk diterapkan. Langkah ini dapat membatasi akses dan menjadi benteng pertama untuk menjaga informasi pada perangkat.

2. Enkripsi data pada perangkat mobile

Enkripsi data merupakan solusi fundamental dalam melindungi informasi yang disimpan di perangkat maupun informasi yang dikirim oleh perangkat. Tanpa *decryption key*, orang yang tidak berhak tidak akan dapat mengakses data. Pertimbangkan pula penggunaan VPN demi koneksi yang aman ke internet. VPN memungkinkan perangkat terkoneksi melalui server-server khusus/privat sehingga koneksi akan lebih aman. Ketika

menggunakan enkripsi, semua data yang berada di jalur antara perangkat dan server VPN akan terenkripsi dengan aman.

3. Perbarui sistem operasi dan aplikasi

Lakukan pembaruan secara berkala untuk memastikan sistem operasi pada perangkat, program serta aplikasi yang terpasang di perangkat adalah selalu yang terbaru. Update terbaru sistem operasi dan aplikasi biasanya selalu disertai peningkatan keamanan dan patch.

4. Hindari terkoneksi ke jaringan WiFi publik

Koneksi seperti ini tidak aman karena tidak terlindungi dan mudah diretas dengan serangan *Man-in-the-middle* sehingga dapat membahayakan data perusahaan. Untuk itu, pengguna perangkat mobile disarankan untuk mematikan fungsi *automatic connection*.

5. Unduh aplikasi hanya dari sumber terpercaya

Mengunduh dan memasang program dari pihak ketiga dapat mendatangkan risiko terhadap privasi informasi perusahaan, juga terhadap integritas perangkat itu sendiri.

6. Melakukan backup data

Untuk mengantisipasi serangan malware yang bisa membuat data tidak bisa diakses atau ketika perangkat hilang, buatlah backup data di tempat lain sehingga data tetap bisa diakses dan diperbarui. Mengaktifkan fitur *automated backup* adalah bagian dari tugas rutin IT security.

7. Gunakan fitur remote data access dan data deletion

Ketika perangkat hilang atau dicuri, pemilik perangkat dapat mengunci perangkat dan bahkan menghapus data di perangkat dari jarak jauh. Dengan cara ini, akses-akses ilegal terhadap informasi sensitif milik perusahaan dapat dicegah.

8. Waspadai mobile phishing

Brand phishing report dari check point menyebutkan bahwa telepon genggam adalah target yang disukai penjahat maya. Hindari mengklik link atau file yang mencurigakan karena tindakan itu dapat memicu ter unduhnya malware tanpa disadari pengguna.

9. Berselancar hanya di situs-situs web yang aman

Ketika mengunjungi sebuah situs web menggunakan perangkat mobile, pastikan situs web tersebut terproteksi dengan *SSL security certificate* yang akan mengenkripsi data user. Periksa apakah ada kode HTTPS tertulis di depan nama domain situs web.

10. Lakukan security audit pada perangkat mobile

Periksa secara berkala perangkat mobile untuk mendeteksi adanya kerentanan (*vulnerability*) dan lubang keamanan (*security hole*) yang berpotensi membahayakan keseluruhan jaringan perusahaan

9.5 Mobile Device Management

Menurut Muhammad Afsal (2022) *Mobile Device Management* atau biasa disebut MDM adalah salah satu solusi dari *Enterprise Mobility Management* (EMM) yang berfungsi untuk mengelola, memonitor, mengintegrasikan dan mendukung perangkat mobile (smartphone, komputer tablet, perangkat POS, laptop ataupun komputer desktop/PC) baik *Corporate Owned, Business Only* (COBO) ataupun *Bring Your Own Device* (BYOD) yang mencakup pada pendistribusian aplikasi dan konfigurasi administrasi pada perangkat tersebut.

Menurut Gopal Tatted dan G. R. Bamnote (2013), *Mobile Device Management* merupakan tools yang digunakan untuk memonitor, mengontrol dan melindungi perangkat mobile. MDM mencakup keamanan perangkat, aplikasi, jaringan dan data. MDM mengacu kepada frameworks atau solusi yang mengontrol, memonitor dan mengatur penggunaan perangkat mobile di perusahaan atau penyedia layanan (Bergman et al., 2013).

Software MDM yang digunakan dapat diimplementasikan di platform Android, iOS dan Blackberry. Tujuan utama dibuatnya aplikasi mobile ini untuk meningkatkan kemudahan, kenyamanan, keamanan dan kegunaannya. Fungsi dari MDM yaitu menambahkan lapisan keamanan dan memastikan cara untuk memantau aktivitas pada suatu perangkat.

Adapun beberapa fitur MDM seperti *device encryption, platform specific policies, SD Card encryption. Geo-location tracking, connectivity profiles* (VPN, Wi-Fi, Bluetooth), *remote wipe* dan beberapa fitur lainnya yang merupakan bagian dari solusi MDM.(Datacomm, 2017)

Menurut Helios (2022), ada empat manfaat menerapkan MDM untuk bisnis yaitu:

1. Setting Policies

Perusahaan dapat menerapkan kebijakan khusus untuk meminimalisir gap antara kebutuhan pekerjaan dan tindakan lain. Untuk memudahkan dan mendukung berbagai kebijakan tersebut, MDM dapat memberikan batasan otomatis demi menjaga dan melindungi aset perusahaan.

2. Security Factors

Ketika sewaktu-waktu terjadi kehilangan atau kecurian perangkat yang digunakan oleh karyawan, maka semua data tetap bisa diamankan dengan menghapus secara remote. Faktor keamanan sangat membantu apabila perangkat mengalami kerusakan dan tidak bisa digunakan lagi. MDM dapat memastikan semua data tetap aman dan terlindungi.

3. Application Management

Perusahaan dapat memberikan berbagai aplikasi yang sesuai dengan kebutuhan dengan proses instalasi lebih mudah. Dengan begitu, kebutuhan perangkat yang digunakan sesuai dengan kebutuhan dan kegunaan bisnis untuk meminimalkan kemungkinan perangkat digunakan di luar kebutuhan perusahaan.

4. Inventory Needs

Penggunaan perangkat dapat dipantau secara real-time untuk memudahkan monitoring terhadap semua aplikasi dan penggunaan lain. Admin IT juga dapat melihat dan mengetahui posisi perangkat untuk memastikan keamanan dan terlacak agar lebih terlindungi.

Bab 10

Keamanan Sistem Informasi

10.1 Pendahuluan

Teknologi informasi saat ini memiliki peran yang sangat vital pada proses bisnis perusahaan maupun organisasi lainnya. Dalam implementasinya, teknologi informasi menjadi roda penggerak/alat bantu proses bisnis perusahaan. Sistem informasi merupakan implementasi dari pemanfaatan teknologi informasi tersebut, selain hal tersebut, informasi juga merupakan aset penting bagi perusahaan. Mengingat pentingnya sistem informasi serta terjaminnya integritas dan kerahasiaan informasi, maka dibutuhkan keamanan sistem informasi.

Keamanan informasi secara umum adalah seperangkat strategi, aturan, pedoman, praktik untuk melindungi kerahasiaan, ketersediaan, dan integritas data serta mencegah akses, penggunaan, modifikasi, pencatatan, dan penghancuran informasi yang tidak sah (Nasher, 2020). Keamanan informasi tidak hanya bisa diterapkan pada aspek teknologi informasi saja, akan tetapi perusahaan/instansi harus memiliki suatu pemahaman agar ketika terdapat suatu masalah yang muncul, perusahaan/instansi dapat secara cepat dan tepat menanganinya.

Dengan demikian kebutuhan akan keamanan informasi dapat terpenuhi melalui pengolahan secara menyeluruh di setiap aspek perusahaan/organisasi.

Keamanan informasi adalah menjaga informasi dari ancaman yang mungkin terjadi dalam upaya menjamin kelangsungan bisnis, mengurangi tingkat risiko dan mempercepat atau memaksimalkan pengambilan keputusan investasi serta peluang bisnis (Listyorini, 2021).

Tingkat keamanan pada informasi juga bergantung pada tingkat sensitivitas informasi dalam database, informasi yang tidak terlalu sensitif sistem keamanannya tidak terlalu ketat sedangkan untuk informasi yang sangat sensitif perlu pengaturan tingkat keamanan yang ketat untuk akses ke informasi tersebut.

10.2 Tujuan Keamanan Sistem Informasi

Keamanan sistem informasi bertujuan untuk menjamin keberlangsungan sistem informasi, adapun aspek yang harus diperhatikan diantaranya *Confidentiality*, *Integrity*, dan *Availability* (CIA).. Dalam menerapkan Keamanan Informasi, perusahaan/organisasi harus memperhatikan 3 aspek yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA) (Dwinanto and Setiyani, 2021).

Pada umumnya ketika serangan, masalah, risiko yang mengancam keamanan informasi muncul, maka setidaknya terdapat salah satu dari aspek CIA yang akan menjadi target dari serangan tersebut.



Gambar 10.1: Confidentially, Integrity, dan Availability (CIA)

Kerahasiaan (Confidentiality)

Ketika kita membahas mengenai aspek *confidentiality* atau kerahasiaan informasi, maka kita sedang berbicara mengenai serangkaian upaya perlindungan agar informasi tidak terakses oleh pihak yang tidak berwenang.

Informasi rahasia memang dianggap sebagai data yang bernilai oleh para cyber hacker. Informasi yang diincar biasanya berupa informasi pelanggan, data karyawan, kekayaan intelektual, atau informasi mengenai rahasia dagang. Oleh karena itulah para cyber hacker terus mencari kerentanan yang ada pada dalam sistem agar mereka bisa mengakses info-info penting tersebut.

Langkah-langkah kerahasiaan melindungi informasi dari akses dan penyalahgunaan yang tidak sah. Sebagian besar sistem informasi menampung informasi yang memiliki tingkat sensitivitas tertentu. Mungkin informasi bisnis eksklusif yang dapat digunakan pesaing untuk keuntungan mereka, atau informasi pribadi mengenai karyawan, pelanggan, atau klien organisasi. Informasi rahasia sering kali memiliki nilai dan oleh karena itu sistem sering diserang karena penjahat memburu kerentanan untuk dieksploitasi. Vektor ancaman termasuk serangan langsung seperti mencuri kata sandi dan menangkap lalu lintas jaringan, dan serangan yang lebih berlapis seperti rekayasa sosial dan phishing.

Tidak semua pelanggaran kerahasiaan disengaja. Beberapa jenis pelanggaran umum yang tidak disengaja termasuk mengirim email informasi sensitif ke penerima yang salah, mempublikasikan data pribadi ke server web publik, dan membiarkan informasi rahasia ditampilkan di monitor komputer tanpa pengawasan. Saat melindungi informasi, akses sedapat mungkin harus dibatasi hanya bagi yang memiliki hak untuk mengakses dan yang diizinkan untuk melihatnya; semua orang harus dilarang mempelajari apa pun tentang isinya. Inilah inti dari kerahasiaan.

Misalnya, peraturan dari perguruan tinggi mengharuskan pembatasan akses informasi pada mahasiswa. Perguruan tinggi harus yakin bahwa hanya yang berwenang yang memiliki akses untuk melihat catatan nilai.

Aspek ini bertujuan untuk:

1. pembatasan akses informasi sesuai dengan tingkat kerahasiaannya;
2. melindungi data dan informasi hanya bagi yang memiliki hak akses.

Integritas (Integrity)

Integritas adalah menyajikan informasi yang akurat, benar dan lengkap. Setiap organisasi perusahaan pasti ingin melindungi data dan informasi, serta sumber daya yang diatur dapat digunakan secara bersama karena sistem informasi menempatkan kerahasiaan yang sangat tinggi. Integritas merupakan salah satu

aspek yang sangat penting untuk menunjang kualitas informasi yang akan digunakan oleh pengguna sistem informasi.

Integritas berkaitan dengan sistem yang dibangun harus lengkap dan akurat dari sistem yang dimilikinya, yang mana isinya data-data yang akurat sehingga bisa mewakili informasi yang dibutuhkan.

Integritas ini bertujuan untuk:

1. melindungi data dan program komputer agar tidak terjadi perubahan oleh pihak yang tidak berwenang;
2. menjamin data dan informasi pada sistem informasi tetap data dipercaya.

Ada banyak tindakan pencegahan yang dapat dilakukan untuk melindungi integritas. Kontrol akses dan autentikasi yang ketat dapat membantu mencegah pengguna yang berwenang membuat perubahan yang tidak sah. Verifikasi hash dan tanda tangan digital dapat membantu memastikan bahwa transaksi adalah asli dan file tidak dimodifikasi atau rusak. Sama pentingnya untuk melindungi integritas data adalah kontrol administratif seperti pemisahan tugas dan pelatihan.

Aspek yang menjamin data tidak dapat diubah tanpa ada izin pihak yang berwenang, menjaga kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang bisa menyebabkan perubahan pada informasi atau data asli.

Langkah-langkah integritas melindungi informasi dari perubahan yang tidak sah. Langkah-langkah ini memberikan jaminan dalam akurasi dan kelengkapan data. Kebutuhan untuk melindungi informasi mencakup data yang disimpan pada sistem dan data yang dikirimkan antar sistem seperti email. Dalam menjaga integritas, tidak hanya diperlukan untuk mengontrol akses pada tingkat sistem, tetapi untuk lebih memastikan bahwa pengguna sistem hanya dapat mengubah informasi yang mereka otorisasi secara sah untuk diubah.

Seperti halnya perlindungan kerahasiaan, perlindungan integritas data melampaui pelanggaran yang disengaja. Penanggulangan integritas yang efektif juga harus melindungi dari perubahan yang tidak disengaja, seperti kesalahan pengguna atau kehilangan data yang disebabkan oleh kegagalan fungsi sistem. Sementara semua pemilik sistem memerlukan kepercayaan pada integritas data mereka, industri keuangan memiliki kebutuhan yang sangat

penting untuk memastikan bahwa transaksi di seluruh sistemnya aman dari gangguan.

Ketersediaan (Availability)

Ketersediaan artinya ketersediaan data kapan pun dimana pun data data yang boleh diakses oleh konsumen atau pengguna(user) bisa disediakan sehingga ketika mencari informasi maka dapat dengan cepat. Kerahasiaan adalah melindungi data dan informasi dari penggunaan yang tidak semestinya atau orang-orang yang tidak memiliki otoritas. Ketersediaan berarti bahwa informasi dapat diakses dan dimodifikasi oleh siapa pun yang berwenang untuk melakukannya dalam jangka waktu yang sesuai.

Tergantung pada jenis informasi, kerangka waktu yang tepat dapat berarti hal yang berbeda. Misalnya, seorang pedagang saham membutuhkan informasi untuk segera tersedia, sementara seorang tenaga penjualan mungkin senang mendapatkan angka penjualan untuk hari itu dalam laporan keesokan paginya. Perusahaan seperti Amazon.com akan mengharuskan server mereka tersedia dua puluh empat jam sehari, tujuh hari seminggu. Perusahaan lain mungkin tidak menderita jika server web mereka mati selama beberapa menit sesekali.

Beberapa faktor yang dapat mengganggu ketersediaan ini diantaranya adalah:

1. Kerusakan perangkat keras teknologi informasi.
2. Aktivitas penyusup, Hacker, Cracker.
3. Aktivitas user jahat (malicious user).

Tinjauan keamanan informasi sebagai berikut:

Contoh tinjauan keamanan informasi sebagai berikut (Nurul, Angrainy and Aprelyani, 2022):

1. Physical Security, strategi yang memfokuskan untuk mengamankan anggota organisasi, aset fisik, akses tanpa otorisasi dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran.
2. Personal Security, strategi yang lebih memfokuskan untuk melindungi orang-orang dalam organisasi.
3. Operation Security, strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan ancaman.

4. Communications Security, strategi yang bertujuan untuk mengamankan media informasi dan teknologi informasi.
5. Network Security, strategi yang memfokuskan pengamanan peralatan jaringan pada data organisasi.

10.3 Bentuk Ancaman Keamanan Sistem Informasi

Interruption

Interruption adalah penghentian sementara. Jadi secara umum interruption merupakan gangguan yang mengacu pada situasi dimana layanan atau data tidak tersedia, tidak dapat digunakan untuk sementara. Contoh interupsi adalah ketika file tidak dapat digunakan akibat hardisk di rusak atau kabel telekomunikasi dipotong.

Dalam pengertian ini, pihak yang tidak bertanggung jawab mencoba untuk membuat layanan tidak dapat di akses oleh pihak lain. Perangkat sistem menjadi rusak atau tidak tersedia karena instruksi serangan di tunjukan kepada ketersediaan (availability). Contoh serangan adalah “denial of service attack”

Interception

berarti pencegahan atau penyadapan. Jadi interception merupakan ancaman terhadap kerahasiaan (secrecy). Ancaman ini mengacu pada situasi bahwa pihak yang tidak sah telah memperoleh akses ke layanan atau data, sebuah contoh, tempat intersepsi komunikasi antara kedua pihak telah terdengar oleh pihak lain.

Interception juga terjadi ketika data secara ilegal disalin. Misalnya, informasi yang ada disadap oleh pihak yang tidak bertanggung jawab atau mengcopy data secara tidak sah. Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Sederhananya adalah penyadapan mereka berhasil menyadap transaksi yang kita lakukan/sistem informasi kita berhasil dia masuki misal menyadap dapat mengetahui yang terjadi di sistem informasi kita. Contoh dari serangan ini adalah penyadapan (wiretapping).

Modification

Berarti tindakan untuk mengubah suatu hal. Modification merupakan ancaman terhadap integritas, yang melibatkan perubahan data atau gangguan terhadap perintah sehingga isi dari data tersebut tidak sesuai dengan aslinya. Contoh dari ancaman ini termasuk mencegat dan mengubah data yang dikirimkan dan diubah menjadi keinginan pihak yang tidak bertanggung jawab.

Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari website dengan pesan-pesan yang merugikan pemilik website

Fabrication

berarti dugaan pemalsuan bukti, merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru dan memalsukan suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh si penerima informasi tersebut.

Sebagai contoh, orang yang tidak bertanggung jawab memasukkan pesan-pesan atau data palsu ke dalam file. Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya dari serangan ini adalah memasukkan pesan-pesan palsu seperti email palsu ke dalam jaringan komputer

Interception, interruption, modification dan *fabrication* masing-masing dapat dilihat sebagai bentuk pemalsuan data. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi atau sistem jaringan komputer. Masalah keamanan sering kali kurang mendapat perhatian dari para perancang dan pengelola sistem informasi.

Sering kali masalah keamanan berada di urutan setelah tampilan, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi dari sistem, sering kali masalah keamanan tidak begitu dipedulikan bahkan ditiadakan.

10.4 Pencegahan/Mitigasi Serangan Pada Sistem Informasi

1. Pencegahan serangan pada perangkat keras, memberikan pengamanan fisik di ruang server / data center:
 - a. Pengamanan fisik mulai dari akses kontrol terhadap ruang data center, tidak semua orang punya akses untuk masuk ke ruang pusat data/server.
 - b. Akses control terhadap server rack, dibatasi siapa saja yang boleh masuk dan mengakses data-data yang ada di rak server.
 - c. Akses control terhadap fisik server, Penggunaan resource yang ada di ruang server juga dibatasi tidak sembarangan orang.
2. Pencegahan serangan pada perangkat lunak

Mitigasi serangan pada sistem operasi Mitigasi serangan terhadap sistem operasi dapat dilakukan dengan melakukan update terhadap sistem informasi yang digunakan. Update akan memberikan perbaikan terhadap sistem operasi terutama dari sisi keamanan (selain perbaikan aspek lain seperti tampilan, penambahan fitur).

Dengan selalu mengikuti update yang disediakan oleh produsen sistem operasi, maka celah keamanan yang ada dapat tertutup. Selain itu penggunaan software bajakan akan dapat membahayakan sistem operasi. Sebagian besar aplikasi crack untuk membajak software akan membuka backdoor yang memungkinkan malware untuk masuk ke dalam sistem.

- a. Mitigasi serangan pada layanan (service) sistem operasi serangan pada layanan sistem operasi dapat disebabkan oleh celah keamanan (vulnerability) yang terdapat pada layanan tersebut maupun dari serangan (secara disengaja). Tujuan dari serangan terhadap layanan (service) sistem operasi adalah untuk mendapatkan akses terhadap layanan tersebut (pada layanan SSH, FTP) atau agar layanan tersebut tidak dapat di akses (DDoS). Mitigasi yang dapat dilakukan yaitu memasang dan

mengonfigurasi firewall pada server untuk mengurangi serangan – serangan tersebut.

- b. Mitigasi serangan pada aplikasi serangan pada aplikasi sering kali dilakukan dengan memanfaatkan celah keamanan yang tidak sengaja terekspos oleh pembuat aplikasi. Hal ini sering kali disebabkan oleh kesalahan logika pemrograman. Untuk memitigasi serangan pada aplikasi adalah dengan menerapkan teknik secure coding. Secure coding merupakan teknik pemrograman yang mempertimbangkan sisi keamanan dari kode program yang digunakan.
3. Pencegahan serangan pada jaringan komputer
Mitigasi serangan pada jaringan komputer dapat dilakukan mulai dari desain jaringan komputer yang benar serta pemasangan aplikasi monitoring jaringan yang memiliki fitur *Intrusion Detection System / Intrusion Prevention System*.
Desain jaringan yang direkomendasikan adalah desain jaringan komputer yang dapat berkembang mengikuti perkembangan organisasinya, serta dalam proses perkembangannya berdampak minimal terhadap jaringan existing. Terutama pada jaringan komputer nirkabel, harus memperhatikan faktor keamanan aksesnya. Autentikasi pengguna jaringan komputer juga perlu dilakukan untuk mengidentifikasi setiap pengguna jaringan komputer.
4. Pencegahan Serangan pada Basis data
SQL Injection dengan berbagai variannya merupakan serangan utama pada basis data. Penyebab dari serangan ini bukanlah merupakan kesalahan *Data Base Management System* namun lebih ke kesalahan logika pemrograman yang digunakan. Maka penggunaan kode SQL sebagai input pada sistem informasi harus dibatasi.
 - a. Pembatasan penggunaan kode SQL sebagai input pada sistem informasi.
 - b. Mengubah karakter spesial ke dalam format HTML kemudian pengecekan dilakukan menggunakan *regular expression* dan *exceptions*.

5. Pencegahan serangan pada pengguna sistem informasi

Edukasi merupakan cara yang paling efektif dalam memitigasi serangan terhadap pengguna sistem informasi. Dengan edukasi pengguna akan dapat mengetahui hal – hal yang boleh dilakukan serta hal – hal yang berpotensi bahaya. Untuk memperkuat edukasi, pada organisasi tertentu seperti pada perusahaan dapat menerapkan policy / aturan dalam penggunaan sistem informasi.

Di tunjang dengan *Standard Operational Procedure* baku akan sangat efektif dalam memitigasi serangan terhadap pengguna sistem informasi karena setiap hal harus dilakukan sesuai dengan prosedur.

10.5 Isu Keamanan Sistem Informasi

Isu keamanan sistem informasi dapat diklasifikasikan berdasarkan ancaman dan kelemahan sistem yang dimiliki:

Ancaman

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman yang mungkin timbul dari kegiatan pengolahan informasi berasal dari 3 hal utama, yaitu:

1. Ancaman alam

Termasuk dalam kategori ancaman alam terdiri atas:

- a. Ancaman air, seperti: banjir, tsunami, intrusi air laut, kelembaban tinggi, badai, pencairan salju.
- b. Ancaman tanah, seperti: longsor, gempa bumi, gunung meletus.
- c. Ancaman alam lain, seperti: kebakaran hutan, petir, tornado, angin ribut, dsb.

2. Ancaman manusia

dikategorikan sebagai ancaman manusia, diantaranya adalah:

- a. Malicious code.
- b. Virus, Logic bombs, Trojan horse, Worm, active contents, Countermeasures.

- c. Social engineering.
 - d. Hacking, cracking, akses ke sistem oleh orang yang tidak berhak, DDOS, dan backdoor.
 - e. Kriminalisasi.
 - f. Pencurian, penipuan, penyuapan, pengkopian tanpa izin, perusakan.
 - g. Teroris.
 - h. Peledakan, Surat kaleng, perang informasi, perusakan.
3. Ancaman lingkungan
- Dikategorikan sebagai ancaman lingkungan seperti:
- a. Penurunan tegangan listrik atau kenaikan tegangan listrik secara tiba-tiba dan dalam jangka waktu yang cukup lama.
 - b. Polusi udara.
 - c. Efek bahan kimia seperti semprotan obat pembunuh serangga, semprotan anti api, dll.
 - d. Kebocoran seperti A/C, atap bocor saat hujan.

Besar kecilnya suatu ancaman dari sumber ancaman yang teridentifikasi atau belum teridentifikasi dengan jelas tersebut, perlu diklasifikasikan secara matriks ancaman sehingga kemungkinan yang timbul dari ancaman tersebut dapat diminimalisir dengan pasti.

Setiap ancaman tersebut memiliki probabilitas serangan yang beragam baik dapat terprediksi maupun tidak dapat diprediksikan seperti terjadinya gempa bumi yang mengakibatkan sistem informasi mengalami *malfunction*.

Kelemahan (Vulnerability)

Adalah cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut.

Cacat sistem bisa terjadi pada prosedur, peralatan, maupun perangkat lunak yang dimiliki, contoh yang mungkin terjadi seperti: Setting firewall yang membuka telnet sehingga dapat diakses dari luar, atau setting VPN yang tidak diikuti oleh penerapan kerberos atau NAT.

Pendekatan Keamanan Sistem Informasi

Suatu pendekatan keamanan sistem informasi minimal menggunakan 3 pendekatan, yaitu:

1. Pendekatan preventif yang bersifat mencegah dari kemungkinan terjadinya ancaman dan kelemahan.
2. Pendekatan detective yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal.
3. Pendekatan Corrective yang bersifat mengoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal.

Tindakan tersebutlah menjadikan bahwa keamanan sistem informasi tidak dilihat hanya dari kacamata timbulnya serangan dari virus, malware, spyware dan masalah lain, akan tetapi dilihat dari berbagai segi sesuai dengan domain keamanan sistem itu sendiri.

Kontrol Pengamanan

Berkaitan dengan keamanan sistem informasi, diperlukan tindakan berupa pengendalian terhadap sistem informasi. Kontrol-kontrol untuk pengamanan sistem informasi antara lain:

1. Kontrol administratif
Kontrol administratif dimaksudkan untuk menjamin bahwa seluruh kerangka kontrol dilaksanakan sepenuhnya dalam organisasi berdasarkan prosedur-prosedur yang jelas.
2. Kontrol pengembangan dan pemeliharaan sistem
Auditor sistem informasi harus dilibatkan dari masa pengembangan hingga pemeliharaan sistem, untuk memastikan bahwa sistem benar-benar terkendali, termasuk dalam hal otorisasi pemakai sistem.
3. Kontrol operasi
Pembatasan akan akses terhadap data, Kontrol terhadap personel pengoperasi, Kontrol terhadap peralatan, Kontrol terhadap penyimpanan arsip

4. Proteksi fisik terhadap pusat data
Faktor lingkungan yang menyangkut suhu, kebersihan, kelembaban udara, bahaya banjir, dan keamanan fisik ruangan perlu diperhatikan dengan benar.
5. Kontrol perangkat keras
Jika komponen dalam sistem mengalami kegagalan maka komponen cadangan atau kembarannya segera mengambil alih peran komponen yang rusak
6. Kontrol akses terhadap sistem komputer
setiap pemakai sistem diberi otorisasi yang berbeda-beda. Setiap pemakai dilengkapi dengan nama pemakai dan password.
7. Kontrol terhadap akses informasi
cara mengubah suatu informasi ke dalam bentuk yang tak dapat dibaca oleh orang lain dikenal dengan istilah kriptografi.
8. Kontrol terhadap bencana
9. Kontrol terhadap perlindungan terakhir
Rencana pemulihan terhadap bencana dan asuransi.
10. Kontrol aplikasi
Kontrol yang diwujudkan secara spesifik dalam suatu aplikasi sistem informasi.

Virus

Suatu program dapat disebut sebagai suatu virus apabila memenuhi minimal 5 kriteria berikut:

1. kemampuan untuk mendapatkan informasi;
2. kemampuan untuk memeriksa suatu file;
3. kemampuan untuk menggandakan diri dan menularkan diri;
4. kemampuan melakukan manipulasi;
5. kemampuan untuk menyembunyikan.

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Worm atau cacing komputer dalam keamanan komputer, adalah sebutan untuk sebuah program yang

menyebarkan dirinya di dalam banyak komputer, dengan menggandakan dirinya dalam memori setiap komputer yang terinfeksi, worm juga menghabiskan bandwidth yang tersedia.

Trojan horse atau Kuda Troya, dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (malicious software/malware) yang dapat merusak sebuah sistem atau jaringan.

Enkripsi dan Dekripsi

Enkripsi adalah proses Sebuah proses data encoding untuk mencegah pihak yang tidak berwenang melihat atau memodifikasinya. Pada kebanyakan proses enkripsi, Anda harus menyertakan kunci sehingga data yang dienkripsi dapat dideskripsikan kembali.

Ilmu yang mempelajari teknik enkripsi disebut kriptografi. Gambaran sederhana tentang enkripsi, misalnya mengganti huruf a dengan n, b dengan m dan seterusnya. Yang perlu diketahui tentang enkripsi:

1. Mencegah akses yang tidak diinginkan pada dokumen dan pesan email.
2. Level enkripsi yang tinggi sukar untuk dibongkar.
3. Perubahan dalam peraturan ekspor teknologi kriptografi akan meningkatkan penjualan software enkripsi.

Data melewati sebuah formula matematis yang disebut algoritma, yang kemudian mengubahnya menjadi data terenkripsi yang disebut sebagai ciphertext. Dekripsi merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah ciphertext menjadi plaintext dengan menggunakan algoritma (Simarmata, 2006; Simarmata, Sriadhi dan Rahim, 2020)..

Bab 11

Keamanan Perangkat Keras

11.1 Pendahuluan

Sebagaimana kita ketahui bahwa Komponen Sistem Komputer ada tiga, yaitu Hardware (Perangkat Keras), Software (Perangkat Lunak) dan Brainware (Pengguna / user). Terkait dengan keamanan, biasanya kita, terutama sebagai pengguna umum, hanya memperhatikan keamanan dari sisi software nya saja, misalnya dengan memasukkan program antivirus di komputer kita, program maintenance seperti ccleaner dan lain-lain.

Akan tetapi jarang sekali kita bahkan mengabaikan keamanan perangkat keras ini. Perangkat keras kita pertimbangkan hanya saat akan membeli perangkat PC atau Laptop saja. Padahal keamanan hardware atau perangkat keras ini sama pentingnya dengan keamanan software. pada artikel ini akan dibahas ancaman umum yang dihadapi oleh perangkat keras dan solusi untuk mengatasinya.

Apa itu Keamanan Perangkat Keras? Keamanan perangkat keras adalah perlindungan perangkat fisik dari ancaman yang akan memfasilitasi akses tidak sah ke sistem Enterprise (Ashtari, 2022). Pada sebuah perusahaan, keamanan perangkat keras merupakan domain dari bagian/divisi keamanan yang berfokus pada perlindungan semua perangkat fisik, mesin, dan periferal. Perlindungan ini dapat berupa pengamanan pemantauan fisik seperti

menyediakan tenaga penjaga/security/satpam, mengamankan ruangan dengan menyediakan kunci, dan kamera CCTV.

Selain itu juga bisa dalam bentuk penyediaan komponen perangkat keras khusus, seperti sirkuit terpadu yang menyediakan fungsi kriptografi untuk melindungi perangkat keras dari kerentanan keamanan dan menangkis penyerang. Sederhananya, keamanan perangkat keras melibatkan perlindungan melalui perangkat fisik atau operasi daripada program keamanan seperti antivirus.

Dalam hal keamanan 'fisik' tersebut, keamanan perangkat keras pada dasarnya juga memerlukan perlindungan dari bencana alam selain gangguan dari manusia. Hal ini diperlukan karena saat ini dengan banyaknya adopsi dari penggunaan teknologi *Internet Of Things* (IoT), serangan yang menargetkan komputasi serta perangkat yang terhubung non-komputasi menjadi lebih sering terjadi.

Contoh umum dari keamanan perangkat keras adalah perangkat yang memantau lalu lintas jaringan, seperti firewall perangkat keras atau server proxy. Keamanan perangkat keras berbasis hardware juga dapat dicapai melalui *Hardware Security Modules* (HSM) atau Modul Keamanan Perangkat Keras, yaitu perangkat yang menghasilkan dan membantu pengelolaan kunci kriptografi untuk otentikasi dan enkripsi sistem perusahaan. Sistem perangkat keras semacam itu memungkinkan perusahaan untuk menambahkan lapisan keamanan lain ke arsitektur yang rentan di serang.

Celah keamanan dapat dieksploitasi ketika perangkat keras menerima input, menjalankan kode, atau terlibat dalam operasi apa pun. Setiap perangkat yang terhubung ke jaringan, baik secara langsung maupun tidak langsung, perlu dilindungi dari serangan. Bahkan sistem yang tampaknya tidak penting, seperti sistem pencahayaan, dapat ditargetkan oleh penyerang untuk memengaruhi produktivitas.

Perangkat keras penting seperti server memerlukan langkah-langkah keamanan yang kuat untuk memastikan kelancaran operasi harian. Pelaku ancaman juga dapat beroperasi dari dalam organisasi, dengan membuat kebijakan untuk keamanan perangkat keras internal yang bagus sama pentingnya dengan menciptakan strategi keamanan eksternal yang kuat.

11.2 Ancaman Utama Perangkat Keras Saat Ini

Berikut ini beberapa contoh ancaman utama perangkat keras:

Firmware Sudah Usang

Firmware adalah jenis perangkat lunak yang terukir langsung ke dalam perangkat keras (Chakraborty, 2021). Fungsi dari firmware ini adalah untuk memberikan instruksi dan panduan yang diperlukan untuk komunikasi antar perangkat keras. Perangkat keras yang tidak memiliki firmware, akan sama dengan perangkat lunak yang tidak memiliki sistem operasi. Sehingga perintah-perintah yang diberikan pada perangkat keras tidak akan berjalan seperti yang diperintahkan. Dengan kata lain perangkat keras tersebut tidak dapat dioperasikan.

Firmware yang sudah usang dapat berakibat pada menurunnya performa dari perangkat keras. Dengan firmware yang diperbarui selain dapat meningkatkan performa dari perangkat keras, juga dapat digunakan untuk memperbaiki kesalahan yang terjadi pada sebuah sistem.

Enkripsi Tidak Memadai

Semakin banyak perangkat komputer yang terhubung dalam jaringan, maka semakin rawan keamanannya. Informasi yang tidak terenkripsi dengan baik dapat dengan mudah diserang, sehingga data dapat dicuri dan diakses dengan mudah. Untuk itu diperlukan enkripsi terutama terkait dengan alamat protokol jaringan yang harus diatur dengan baik.

Akses Lokal Tidak Aman

Perangkat keras dengan aplikasi IoT dan IIoT sering kali dapat diakses melalui antarmuka lokal atau jaringan lokal. Perusahaan, terutama yang lebih kecil, mungkin lalai mengonfigurasi titik akses lokal ini dengan benar atau melindunginya secara fisik. Hal tersebut dapat membuat lingkungan perangkat keras perusahaan terbuka sehingga mudah diakses oleh orang jahat yang dapat merusak sistem perusahaan.

Kata Sandi Default Yang Tidak Diubah

Sebagian besar perangkat perusahaan dilengkapi dengan 'kata sandi default/bawaan dari perangkat kerasnya' yang dapat dan seharusnya diubah.

Namun, banyak perusahaan, bahkan perusahaan yang menerapkan sistem keamanan canggih pun lupa atau abai untuk merubah kata sandi perangkat komputernya. Pengguna / pegawai perusahaan tersebut mungkin terus menggunakan kata sandi default untuk perangkat IoT murah dan perangkat keras *turnkey*.

Sering kali, kata sandi ditulis pada perangkat itu sendiri dan dapat diakses oleh hampir semua orang dengan akses fisik yang sama. Padahal risikonya bisa fatal. Sebagai contoh kata sandi pada BIOS, jika tidak diubah, kemudian ada orang yang jahat masuk ke sistem BIOSnya dengan mengubah setting/pengaturan prosesor yang dimaksimalkan (overclock), padahal prosesor tersebut tidak kuat, maka dapat berakibat pada kerusakan prosesor tersebut.

Perangkat Keras Khusus Yang Rentan

Banyak organisasi mengandalkan solusi perangkat keras yang dibuat khusus untuk operasi bisnis khusus. Misalnya, pusat data perusahaan dan sistem yang disesuaikan untuk aplikasi teknik yang beroperasi menggunakan chipset yang dibuat khusus yang memungkinkannya memberikan hasil tertentu.

Produsen sering mengabaikan untuk meninjau postur keamanan chip dan perangkat yang dibuat khusus ini seketat yang mereka lakukan untuk perangkat keras yang memenuhi tujuan yang lebih umum.

Backdoors

Backdoors adalah kerentanan tersembunyi yang sering dimasukkan dengan sengaja selama tahap pembuatan perangkat. Backdoors memungkinkan pelaku ancaman untuk melewati proses otentikasi dan mendapatkan akses root ke perangkat tanpa persetujuan pemilik.

Tidak seperti backdoors perangkat lunak yang dapat ditambal dengan mudah, backdoors perangkat keras jauh lebih sulit untuk dipasang. Mereka dapat dimanfaatkan oleh penyerang untuk menginstal malware atau memasukkan kode berbahaya ke dalam sistem.

Eavesdropping

Serangan Eavesdropping cara kerjanya seperti penyadapan telepon, terjadi ketika pihak yang tidak disetujui mengakses perangkat keras dan menangkap datanya. Serangan Eavesdropping dapat dieksekusi tanpa penyerang memiliki koneksi konstan ke perangkat keras.

Misalnya, dalam kasus skimmer kartu yang dimasukkan ke dalam ATM atau terminal PoS, penyerang mengakses perangkat sesekali untuk mendapatkan salinan informasinya. Serangan penyadapan dapat dipicu dengan menyuntikkan program jahat ke perangkat yang sudah disusupi, sehingga memungkinkan akses tidak sah ke data, dan bahkan menyiapkan protokol untuk data yang akan dikirim ke penyerang pada interval yang telah ditentukan.

Serangan Modifikasi

Serangan modifikasi secara invasif merusak fungsi normal perangkat dan memungkinkan orang jahat mengesampingkan batasan pada pengoperasian perangkat keras. Serangan modifikasi mengambil sesuatu selangkah lebih maju dari serangan penyadapan dengan memodifikasi komunikasi yang digunakan perangkat.

Serangan modifikasi ini cara kerjanya yaitu komponen perangkat keras disuntikkan dengan perangkat lunak berbahaya, pihak yang tidak berwenang kemudian memperoleh kemampuan untuk mengeksekusi *serangan man-in-the-middle*, memungkinkan mereka untuk menerima dan memodifikasi paket sebelum mengirimkannya ke penerima yang dituju.

Contoh serangan modifikasi ini adalah Trojan, yaitu malware yang jago bersembunyi. Seramnya, malware ini bisa mencuri hingga mengacaukan data dan sistem pada device korbannya.

Triggering Faults

Penyerang 'trigger' atau 'menginduksi' kesalahan pada perangkat keras bertujuan untuk mengganggu perilaku sistem normal. Serangan kesalahan dapat membahayakan keamanan tingkat sistem melalui injeksi kesalahan yang dibuat secara tepat untuk memberikan hak istimewa yang tidak sah atau membocorkan data. Serangan ini dapat memiliki efek domino pada perangkat terhubung yang mengandalkan perangkat keras yang disusupi untuk operasi reguler.

Penyerang jarang membutuhkan pengetahuan yang tepat tentang perangkat yang ditargetkan dan kesalahannya untuk mengeksekusi serangan kesalahan yang berhasil. Namun, mengembangkan penanggulangan terhadap serangan kesalahan memerlukan tim keamanan untuk mendapatkan pemahaman yang tepat tentang vektor serangan. Ini bisa sulit karena mekanisme keduanya,

injeksi kesalahan dan propagasi perlu dipahami untuk setiap titik lemah yang tersedia dan diselesaikan tanpa kehilangan data atau gangguan operasi.

Perangkat Keras Palsu

Perangkat keras palsu adalah ancaman yang selalu ada yang memungkinkan penyerang menargetkan perusahaan dengan mudah. Perangkat yang dibuat atau dimodifikasi tanpa otorisasi dari *Original Equipment Manufacturer* (OEM) -suku cadang buatan pabrik dan orisinal- rentan disusupi keamanannya. Celah ini kemudian dapat dieksploitasi oleh penyerang pada waktu yang wajar untuk memicu operasi yang tidak sah dan memungkinkan akses berbahaya ke sistem perusahaan.

11.3 Best Practices Keamanan Hardware

Dengan banyaknya perusahaan di seluruh dunia saat ini yang beralih ke sistem bekerja dari rumah (Work From Home) atau model kerja hibrida, membuat pemantauan aset perangkat keras menjadi lebih rumit. Pada artikel ini akan kami berikan *best practices* terkait dengan keamanan hardware/perangkat keras.

Pelajari Pemasok Perangkat Keras

Mengevaluasi keamanan perangkat keras perusahaan memerlukan analisis kerentanan yang ada sepanjang siklus hidupnya, mulai dari tahap pra-manufaktur. Untuk meminimalkan risiko pengoperasian dengan perangkat keras palsu, mulailah dengan mengidentifikasi vendor yang memasok perangkat keras perusahaan Anda. Periksa pemasok vendor Anda dan pelajari pihak-pihak yang mengintegrasikan komponen dan memproduksi bagian-bagian individual yang digunakan sistem Anda. Juga, cari tahu siapa mitra sekunder vendor Anda jika jalur pasokan utama luas.

Setelah Anda memiliki gambaran menyeluruh tentang semua jalur pasokan perangkat keras Anda, periksa langkah-langkah keamanan yang mereka terapkan sebagai bagian dari operasi manufaktur dan pengiriman mereka. Jika Anda tidak memiliki sumber daya untuk segera melakukan studi menyeluruh, prioritaskan komponen yang paling rentan yang akan menyebabkan dampak terbesar jika terjadi gangguan.

Pertimbangkan untuk mengatur inspeksi produk secara mendalam pada interval acak untuk mendapatkan pemahaman yang tepat tentang operasi harian pemasok Anda. Ikuti langkah serupa untuk setiap vendor perangkat keras baru dan yang sudah ada.

Enkripsi Apa Pun Yang Bisa

Terapkan proses dan protokol enkripsi sedapat mungkin, bahkan untuk perangkat yang kecil seperti media penyimpanan eksternal dan antarmuka *Dynamic Random Access Memory* (DRAM). Sebagian besar prosesor yang diproduksi saat ini dilengkapi dengan komponen bawaan yang memfasilitasi enkripsi dan dekripsi tanpa mengorbankan kekuatan pemrosesan. Jika memungkinkan, data harus dienkripsi saat diam, bergerak, dan dalam pemrosesan.

Enkripsi yang buruk dapat menyebabkan data tidak terlindungi dengan baik. Oleh karena itu, hindari hanya mengandalkan proses enkripsi tingkat rendah saja. Manfaatkan langkah-langkah enkripsi yang sesuai dengan kebutuhan keamanan pemangku kepentingan Anda secara menyeluruh. Terapkan sistem enkripsi yang akan mencegah penyerang mencegat sistem Anda dari jarak jauh.

Bahkan jika perangkat yang dienkripsi dengan benar dicuri secara fisik, penyerang tidak akan dapat mengaksesnya dengan mudah tanpa mengetahui kredensial yang diperlukan.

Minimalnkan Permukaan Serangan

Amankan infrastruktur perusahaan dari serangan dengan menonaktifkan perangkat keras atau komponen yang tidak digunakan secara benar, seperti port debug. Pastikan Anda juga menonaktifkan universal *Asynchronous Receiver-Transmitters* (UART) pemancar penerima asinkron universal lainnya, yang tidak disertakan dalam desain perangkat keras akhir.

Ini termasuk port JTAG dan antarmuka *debugging* serta pemrograman lainnya, antarmuka nirkabel yang tidak digunakan, dan port Ethernet yang tidak perlu. Untuk komponen-komponen yang tidak dipakai tersebut, pertimbangkan untuk menerapkan pembatasan berbasis alamat MAC atau cara lain yang dapat digunakan untuk menggagalkan penyerangan.

Kesalahan konfigurasi adalah salah satu penyebab paling umum dari kerentanan perangkat keras. Hati-hati terhadap kesalahan dalam konfigurasi

sistem; misalnya, penggunaan kata sandi default secara berkelanjutan dapat membuat perangkat terbuka untuk diserang. Pelaku kejahatan dapat menggunakan celah tersebut untuk menyerang perangkat keras perusahaan Anda.

Meminimalkan kemungkinan kesalahan konfigurasi dengan mengaktifkan sistem dan prosedur yang dapat mencegah kesalahan dalam proses konfigurasi perangkat keras perusahaan Anda. Mengotomatiskan proses untuk meminimalkan kesalahan selama *commissioning* dan *decommissioning* perangkat keras. Pantau perangkat dan pengaturan aplikasi Anda secara teratur dan bandingkan dengan konfigurasi standar industri untuk menemukan dan memperbaiki kesalahan pada perangkat yang terhubung ke jaringan perusahaan.

Menerapkan Keamanan Elektronik Yang Memadai

Keamanan elektronik dapat didukung menggunakan elemen yang aman untuk menyimpan kunci utama. Ini memungkinkan pengguna dapat mengenkripsi atau mendekripsi kredensial dan data lain kapan pun diperlukan. Elemen yang aman melindungi sistem dari ancaman seperti ekstraksi kunci dan gangguan. Jika elemen keamanan perangkat keras bukan merupakan opsi yang layak, isolasi yang didukung perangkat keras atau tindakan keamanan perangkat keras lainnya dapat digunakan sebagai gantinya.

Metode lain untuk meningkatkan keamanan elektronik adalah menggunakan perangkat autentikator yang aman untuk perifer. Perangkat autentikator ini memanfaatkan kriptografi yang kuat untuk mengotentikasi setiap perangkat penghubung satu sama lain. Ini meminimalkan risiko jaringan Anda terpapar perangkat keras palsu yang menyamar sebagai perangkat terpercaya.

Untuk lebih meningkatkan keamanan elektronik, gunakan pemantauan lingkungan dan saklar perusak untuk perangkat keras yang kemungkinan besar akan dirusak. Dalam hal ini, kunci master diunggah ke unit SRAM bertenaga baterai yang akan dihapus jika sakelar tamper dipicu. Saklar pemicu juga dapat mendeteksi cahaya di bagian dalam unit yang gelap, sehingga mengunci perangkat jika mesin dibuka.

Pastikan Keamanan Fisik Yang Kuat

Menerapkan langkah-langkah dasar keamanan perangkat keras itu sebenarnya sederhana dan tidak membutuhkan banyak biaya. Misalnya, setting BIOS untuk perangkat keras. Oleh karena itu, disarankan melindungi BIOS dengan

kata sandi untuk mencegah orang lain yang tidak mempunyai hak atau orang jahat mengakses sistem. Workstation karyawan juga dapat dilindungi dari serangan jarak jauh dengan menemukannya di belakang firewall perangkat keras yang dikonfigurasi dengan benar.

Pencurian sistem dari kantor sebenarnya dapat dikurangi dengan mengunci perangkat keras Workstation / komputer client / komputer yang digunakan karyawan dengan menggunakan alat khusus. Di dunia korporat pasca pandemi, di mana pekerjaan jarak jauh masih menjadi tren, sasis laptop dapat diamankan dengan kunci khusus untuk mencegah pembongkaran perangkat.

Server adalah bagian penting dari infrastruktur perusahaan, dan setiap gangguan atau kerusakan pada perangkat keras ini dapat menyebabkan kerugian besar. Oleh karena itu, server harus diamankan dengan memasangnya di rak di ruang server khusus. 'Lemari server' ini harus dilengkapi dengan pintu yang dapat dikunci, dan bingkai depan masing-masing server juga harus diamankan dengan kunci untuk mencegah gangguan. Suhu dan iklim ruangan harus dijaga dengan benar untuk mencegah kerusakan pada server karena terlalu panas atau lembab.

Tempat harus diamankan dengan pintu terkunci, staf keamanan di lapangan, verifikasi identitas yang ketat, dan kamera CCTV. Pemantauan ruang server TI dan perangkat karyawan sangat penting. Akses ke area dengan perangkat keras sensitif (server) harus dibatasi, dan hak akses fisik harus diatur dengan cara yang sama seperti hak akses di bagian depan perangkat lunak. Solusi kontrol akses berbasis cloud membuat penyesuaian izin lebih mudah di tingkat individu, tim, departemen, dan organisasi.

Dengan berbagai pertimbangan di atas, penyedia co-location semakin populer saat ini. Vendor ini mampu menampung dan mengamankan server dan staf, serta menawarkan bantuan teknis sepanjang waktu. Layanan co-location terkemuka menyediakan cadangan daya, konektivitas internet, staf keamanan terlatih, dan langkah-langkah pemantauan yang kuat dengan biaya berulang yang kompetitif dan fleksibel.

Terapkan Pemantauan Real-Time

Pemantauan perangkat keras secara real-time memastikan keamanan yang memadai dan mencegah tindakan yang tidak sah, terutama untuk perusahaan dengan pekerja jarak jauh (Work From Home). Solusi pemantauan real-time berbasis cloud dapat memberi tahu tim keamanan jika terjadi pelanggaran

terhadap perangkat keras sehingga insiden tersebut dapat direspons dengan cepat.

Jika memungkinkan, terapkan tindakan verifikasi visual, pelaporan aktivitas, dan akses jarak jauh ke perangkat fisik. Ini akan membantu meminimalkan waktu respons jika terjadi pelanggaran keamanan.

Bekerja dari rumah, yang akhir-akhir ini banyak dilakukan oleh beberapa perusahaan karena adanya pandemi COVID-19, telah menyebabkan perusahaan membutuhkan sejumlah besar perangkat jaringan. Bagi perusahaan skala dunia yang karyawannya tersebar di berbagai negara, sistem kerja seperti ini dapat efektif dan efisien karena karyawan bisa bekerja menggunakan perangkatnya sendiri. Sebagai gantinya, perusahaan menyiapkan sistem jaringan (internet atau intranet) dengan baik.

Terakhir, pertimbangkan untuk menggunakan platform terintegrasi dan otomatisasi IoT untuk mendapatkan gambaran lengkap tentang postur keamanan perangkat keras perusahaan Anda. Informasi ini dapat diproses menggunakan analitik bertenaga AI untuk memungkinkan implementasi proaktif dari langkah-langkah keamanan perusahaan sesuai kebutuhan.

Lakukan Audit Rutin

Audit rutin terhadap keamanan perangkat keras dan postur keamanan siber hendaknya dilakukan secara berkala. Fungsi audit adalah untuk menemukan dan menangani risiko operasional. Dengan meningkatkan audit keamanan perangkat keras Anda dapat mengurangi kerentanan dan sistem dapat selalu dipantau. Ini akan membantu melindungi perusahaan Anda dari ancaman baru.

Dalam hal keamanan perangkat keras, audit harus menyeluruh, dari mulai pengadaannya (mencari vendor yang terpercaya), pengamanan fisiknya, pengamanan dan kondisi ruangan, setting perangkat kerasnya sampai jadwal pelaksanaan audit harus dilakukan. Jika diperlukan, lakukan prosedur menyeluruh lainnya untuk memastikan keamanan sempurna dari perangkat keras yang sangat penting secara strategis.

Terakhir, jika Anda tidak yakin harus mulai dari mana atau bagaimana melanjutkan, sewalah konsultan dengan rekam jejak yang terbukti bagus untuk membantu Anda.

Bab 12

Siber Terorisme

12.1 Pendahuluan

Cyber terrorism atau yang lebih dikenal dengan terorisme siber merupakan suatu Tindakan kekerasan yang dilakukan dalam internet yang dapat mengakibatkan atau dapat mengancam hilangnya nyawa atau kerugian fisik yang cukup signifikan yang bertujuan untuk mencapai keuntungan politik melalui cara intimidasi sasaran. Siber terorisme merupakan sebuah aktivitas atau metode yang dilakukan oleh sejumlah jaringan atau kelompok teroris. Tidak bisa dipungkiri jika kemajuan teknologi dan dunia maya bisa menjadi wadah yang sangat segar untuk mereka dalam melakukan aksinya.

Hal ini juga terkadang dianggap sebagai sebuah tindakan teroris internet dalam aktivitas yang dikerjakan oleh teroris, termasuk ke dalam tindakan yang disengaja, gangguan jaringan komputer dalam skala besar, terutama penyerangan komputer pribadi yang terkoneksi ke internet yang biasanya dilakukan dengan media seperti virus komputer.

Aktivitas cyber terrorism menjadi sebuah pilihan yang sangat menarik oleh teroris dalam mencapai tujuannya, dengan alasan sebagai berikut:

1. Metode ini memiliki biaya yang lebih murah dibandingkan dengan metode tradisional yang biasanya dilakukan oleh kelompok maupun

- organisasi teroris. Individu Atau kelompok teroris hanya membutuhkan komputer dan sambungan internet dalam menjalankan aksi mereka. Teroris tidak membutuhkan peralatan seperti senjata api atau peledak. Justru dengan adanya internet mereka berharap bisa menciptakan virus dan menyebarkannya melalui sambungan internet.
2. Cyber Terrorism dapat menjadi sebuah metode atau cara yang lebih bersifat rahasia daripada metode yang konvensional yang biasa digunakan. Individu ataupun kelompok teroris bisa menggunakan username ataupun kode identitas yang tidak asli atau bukan sebenarnya untuk masuk ke dalam website tertentu. Hal ini dapat mengelabui atau memanipulasi polisi atau aparat keamanan yang mencari identitas teroris yang sebenarnya. Melalui cyberspace, Gerakan pelaku teroris tidak bisa dibatasi atau mereka dapat bergerak dengan bebas.
 3. Dari aktivitas Cyber Terrorism tersebut mendapatkan jumlah target yang lebih banyak. Pelaku teroris akan membuat target untuk menyerang komputer milik individu, masyarakat, pemerintah, maskapai swasta dan lain-lain. Dalam melakukan pemilihan target secara kompleks, para terorisme dalam menemukan kelemahan dari target yang akan mereka eksploitasi.
 4. Aktivitas cyber terrorism bisa dilaksanakan secara mobile atau berpindah-pindah (tidak fokus pada suatu tempat). Cyber Terrorism tidak membutuhkan pelatihan baik secara fisik maupun psikologis. Keberadaan mereka yang berpindah dari suatu tempat ke tempat lain dapat membuatnya menjadi lebih leluasa dalam melakukan aksinya seperti melakukan perekrutan ataupun mendapatkan dukungan dari pihak tertentu.
 5. Cyber Terrorism selalu mendapat tanggapan untuk menghasilkan dampak yang lebih besar terhadap orang banyak. Oleh karenanya, metode ini mampu menggagang pihak media yang lebih besar juga dalam rangka publisitas mereka.

Pelaku teror mampu mengerjakan manuver dalam ruangan cyber, yaitu dengan cara melakukan serangan cyber (cyber attack) terhadap sasaran yang mereka

inginkan. Menurut Sieber dan Brunst, Cyber attack sebagai cyber terror menargetkan infrastruktur dengan internet melalui virus dan spyware yang berada di dalam jaringan komputer.

Salah satu contoh dari kasus penyerangan virus terhadap jaringan komputer adalah kasus pada tahun 1999 yang dilepas dari Filipina kepada Kementerian Keuangan Rumania yaitu serangan virus I Love You. Virus ini disinyalir mampu merubah nilai mata uang Rumania dan memberikan dampak yang merugikan bagi Rumania pada saat ini. Cyber terror tidak hanya menyerang infrastruktur vital negara tetapi juga pada aspek kehidupan manusia dalam bentuk peretasan terhadap jaringan komunikasi, kendali pesawat dan sebagainya.

Petrus R. Golose dalam bukunya yang berjudul “Invasi Terorisme Ke CyberSpace” menjelaskan adanya 9 aktivitas terorisme (9P) yang dilakukan dengan memanfaatkan teknologi informasi pada internet. Dimana 9 aktivitas tersebut adalah propaganda, perekrutan, penyediaan logistik, pelatihan, pembentukan paramiliter secara melawan hukum, perencanaan, pelaksanaan serangan teroris, persembunyian, dan pendanaan.

10.2 Bentuk-Bentuk Komunikasi, Perencanaan, dan Penyerangan Siber Terorisme

Perencanaan dan pelaksanaan cyber terorisme sebenarnya merupakan bentuk dari salah satu komunikasi juga, karena dilaksanakan melalui media, bahkan lokus, komunikasi kontemporer yaitu komunikasi dengan jejaring dengan menggunakan backbone-nya internet.

Dengan begitu dapat disimpulkan bentuk-bentuk komunikasi pada cyber terorisme, diantaranya adalah:

Propaganda

Propaganda dapat diartikan sebagai sebuah wawasan atau informasi yang ditujukan untuk mempengaruhi pendapat, Tindakan ataupun tingkah laku dari sebuah kelompok tertentu. Bentuk penyampaian dari propaganda dapat secara

langsung ataupun tidak langsung. Propaganda yang biasa dilakukan oleh teroris untuk menyampaikan sebuah pesan dengan tujuan meyakinkan, mengajak seseorang ikut serta untuk bergabung, ataupun menyebarkan rasa takut pada suatu kelompok atau individu.

Target penyampaian pesan itu sendiri adalah pelaku teroris lainnya, target melakukan rekrutmen atau pengaderan, serta simpatisan. Propaganda terorisme banyak ditemukan dalam berbagai media termasuk internet. Internet menjadi sebuah media yang akan memberikan peluang untuk pelaku atau kelompok terorisme dalam melakukan aktivitas propaganda yang dilakukannya.

Beberapa peluang tersebut adalah sebagai berikut:

1. Internet memberikan peluang kepada publik untuk menerima ideologi yang radikal. Jangkauan yang sangat luas menjadi sebuah peluang besar untuk pelaku, kelompok maupun organisasi terorisme
2. Internet sangat berkompetisi dalam mempercepat aksi radikalisme. Video yang berisi paham-paham radikal dengan cepat dapat diakses oleh publik melalui platform yang telah disediakan seperti Youtube atau website-website.

Internet berpengaruh besar dalam mendukung publik untuk melakukan aksi radikal secara mandiri. Publik akan mampu terpapar paham radikal tanpa harus melakukan interaksi langsung dengan pelaku teror maupun pelaku radikalisme (radicalizer) nya. Teknik propaganda yang banyak digunakan adalah dengan melakukan teknik propaganda *by deed* (propaganda yang dilakukan dengan Tindakan kekerasan), dehumanisasi bahkan sampai teknik menyalahi untuk meyakini.

Presentasi Perspektif

Bentuk dari propaganda ini adalah dengan cara memperlihatkan sudut pandang atau idealisme dari pelaku teror ke depan umum. Sudut pandang ini disampaikan sebagai pesan atau wasiat terhadap publik yang sedang disebarkan yang bertujuan untuk memperkuat kekuatan pelaku dengan cara menciptakan rasa takut (fear) dengan panik kepada mereka.

Salah satu contohnya adalah yang dilakukan oleh Mujahidin Indonesia Timur (suatu jaringan terorisme, yang populer di Poso) yang melakukan pemublikasian pesan melalui Youtube setelah melakukan aksi bom di Poso.

Indoktrinasi

Indoktrinasi ini biasanya dilakukan oleh sekelompok atau organisasi terorisme yang bertujuan untuk memprovokasi masyarakat agar ikut serta atau setidaknya memberikan dukungan untuk aksi terorisme mereka.

Hal ini dilaksanakan biasanya bersamaan dengan presentasi perspektif yang dilakukan oleh teroris sebelum ataupun sesudah melakukan aksi teror di dunia nyata.

Radikalisasi

Radikalisasi ini disangkut pautkan dengan indoktrinasi, dimana radikalisasi dipahami mengarah pada proses indoktrinasi. Ketika seseorang sudah mulai tertarik dengan ideologi radikal atau sudah masuk ke dalam paham tersebut, maka suatu individu akan lebih mudah untuk di doktrin agar percaya, yakin, dan mau melakukan suatu tindakan yang sesuai dengan keinginan pelaku teror atau radikalizernya. Hal ini biasanya berupa aksi kekerasan, turut dalam melakukan aksi bom dan lain sebagainya.

Propaganda Rekrutmen

Rekrutmen dalam pembahasan ini dapat diartikan sebuah pencapaian yang diinginkan oleh teroris yang telah melakukan aksi radikalisme dan indoktrinasi. Pada saat ini, rekrutmen justru saat aktif dilakukan di internet.

Contoh propaganda dalam hal ini adalah kasus perekrutan calon martir atau bom bunuh diri yang dilakukan oleh militan Iran melalui situs Insight Online Magazine. Tujuan dari hal tersebut adalah bom bunuh diri terhadap masyarakat Amerika Serikat dan Israel.

Rekrutmen

Dalam hal ini rekrutmen dilakukan dalam rangka penyebaran ideologi dan mencari dukungan ataupun simpatisan ditengah-tengah publik. Intensitas para pengunjung dari situs dan informasi online akan menjadi sasaran bagi teroris. Hal ini akan diskenariokan melalui interaksi dengan calon anggota melalui chat, email, dan lain-lain.

Rekrutmen merupakan sebuah agenda teroris untuk menggalang dukungan populasi atau masyarakat yang akan menjadi sasarannya. Seperti halnya bentuk dari propaganda, rekrutmen akan ditujukan untuk menarik simpatisan dalam bergabung dengan jaringan atau organisasi terorismenya. Kemudian

diharapkan juga kader teroris agar dapat melakukan pelatihan atau persiapan lainnya berupa materi-materi yang akan disebarluaskan melalui internet.

Pemanfaatan internet menjadi salah satu metode yang sering dilakukan teroris untuk merekrut para calon anggotanya. Media sosial seperti Facebook biasanya digunakan oleh teroris merekrut anggotanya. Contoh kasusnya adalah seorang saksi yang diperiksa setelah sebelumnya direkrut dan dikirim ke Suriah pada tahun 2014. Saksi ini memberi pengakuan bawa menjalin pertemanan dengan seseorang melalui wall-wall Facebook serta melakukan chat Facebook kemudian diimingi fasilitas untuk berangkat ke Suriah.

Penyediaan Logistik

Jaringan terorisme biasanya mereka menggunakan cyberspace sebagai media untuk melakukan akses terhadap kebutuhan logistik seperti senjata, bahan peledak maupun bom yang akan dipublikasikan. Biasanya jaringan teroris akan menggunakan cyberspace sebagai tool dalam penyusunan akomodasi keberangkatan, terutama jika jaringan teroris tersebut telah berhasil melakukan perekrutan terhadap calon kadernya melalui media sosial.

Pelatihan

Kelompok teroris akan menggunakan cyberspace sebagai media untuk mencapai tujuan mereka. Salah satunya adalah sebagai pelatihan. Model pelatihan dari terorisme secara garis besar dapat dikategorikan menjadi dua yaitu pengunggahan konten melalui e-book, tutorial melalui video serta tulisan di blog. Sementara model dari komunikasi antara calon ataupun mentor dalam kelompok teroris adalah dengan cara forum dan instant messenger.

Teroris menggunakan instant messenger sebagai media untuk promosi materi-materi pelatihan yang dapat diakses oleh publik atau netizen. Forum internet biasanya akan dieksploitasi dan ditampilkan link bertaut dengan situs yang berisikan materi.

Selain menggunakan instant messenger, biasanya teroris juga menggunakan blog dan E-Book yang dapat diunduh dengan file sharing seperti 4Shared dan Hotfile. Kemudian juga terdapat situs video broadcast seperti Youtube, dengan begitu teroris akan bebas mengunggah video yang berisi cara pembuatan detonator bom atau merakit bom untuk keperluan teroris.

Pembentukan Paramiliter Melawan Secara Hukum

Untuk melakukan penggalangan masyarakat dalam mendukung aksi mereka, biasanya teroris membutuhkan publisitas yang tinggi. Hal ini terkait dengan ajakan atau pun seruan yang ada di internet atau media sosial untuk melakukan mobilisasi, penggunaan senjata, serta kebutuhan dalam membentuk kelompok serang (combat group).

Perencanaan

Dalam hal perencanaan, kelompok teroris akan menggunakan teknologi informasi dalam penetapan strategi, taktik ataupun operasional yang akan diambil dan diaplikasikan. Perencanaan yang dilakukan oleh pelaku, kelompok, ataupun organisasi terorisme akan dimulai dengan cara komunikasi rahasia dan bebas akses, diantaranya adalah email, pesan terenkripsi, dan chat room, sedangkan untuk informasi bebas biasanya seperti peta satelit, informasi pemerintah, agenda transpor, dan laporan keamanan.

Penggunaan aplikasi internet pada hakikatnya merupakan sebuah ancaman yang berhubungan dengan pemanfaatan informasi yang digunakan untuk penyebaran teror yang dilakukan oleh teroris. Salah satu contoh kasusnya adalah penggunaan aplikasi bersifat open source seperti Google Earth dan Google Map oleh milisi di Irak yang digunakan untuk perencanaan penyerangan. Aplikasi bebas akses ini tergolong cukup mudah diakses karena gratis.

Pelaksanaan Serangan

Pelaksanaan atau eksekusi biasanya dijalankan oleh kelompok teroris melalui internet sebagai perantara. Secara umum, pola dari eksekusi adalah sebagai berikut:

1. Ancaman kekerasan yang memiliki sifat nyata dan meliputi penggunaan senjata dalam pelaksanaannya.
2. Diseminasi dilakukan lewat internet yang nanti pada akhirnya akan memunculkan kegelisahan, ketakutan serta kepanikan di tengah-tengah masyarakat.
3. Video call digunakan sebagai media pengawas atau kontrol pelaksanaan aksi yang dilakukan secara real time atau live.

Berdasarkan pola tersebut dapat disimpulkan jika pemanfaatan internet sangat menguntungkan untuk kelompok teroris. Aksi kekerasan biasanya dilakukan oleh kelompok teroris dan ditunjukkan melalui situs atau video broadcast.

Penggunaan dari senjata api juga diperlihatkan seolah hal tersebut mampu membangun rasa cemas dan khawatir bagi publik yang menontonnya. Penyebaran aksi terorisme ini ditujukan untuk mendapatkan perhatian dari publik tentang eksistensi mereka. Selain itu, memberi peringatan kepada masyarakat umum bahwa tidak lama lagi mereka akan melakukan sebuah aksi teror yang besar.

Sementara aksi terorisme yang dilaksanakan kepada target yang sudah ditentukan, monitor dan kontrol terhadap aksi tersebut dilakukan melalui video call juga dilakukan. Rancangan dari serangan disebarluaskan melalui situs seperti anshar.net. Situs ini menjelaskan bagaimana cara aksis teror dilakukan hingga urutan serta peta sasaran yang telah direncanakan.

Persembunyian

Setelah dilakukannya aksi eksekusi ataupun pelaksanaan dari aksi terorisme, akan dilakukan aksi persembunyian. Tahap ini ditujukan untuk mengaburkan identitas pelaku terorisme dari publik dan aparat penegak hukum.

Pendanaan

Pendanaan sangat penting bagi teroris karena ini merupakan sebuah aktivitas yang sangat vital mengingat pada tahap ini terjadi kontribusi penuh atas kelancaran eksekusi atau pelaksanaan aksi terorisme. Pendanaan terorisme akan digunakan untuk semua kebutuhan dalam aksi terorisme seperti penyediaan logistik, perencanaan Latihan, perekrutan, propaganda, pelarian, dan penyerangan.

Pendanaan yang dilakukan untuk terorisme dikategorikan ke dalam tiga bagian yaitu berdasarkan pendana, sumber dana, dan bagaimana cara memperolehnya. Sumber dana bisa berasal dari dalam dan luar negeri, sedangkan pemberi dana bisa berasal dari negara sponsor, kelompok atau organisasi teroris, individu teroris, ataupun masyarakat. Perolehan dana bisa didapatkan secara legal maupun ilegal tergantung pada subjek atau pendananya.

Terorisme dan kejahatan secara organisasi memiliki perbedaan yang signifikan, dimana kejahatan yang terorganisir (organized crime) dibangun untuk fokus khususnya untuk keuntungan ekonomi dan bisa menghasilkan

pasar ilegal sebanyak mungkin. Sementara itu, terorisme adalah tindakan yang dimotivasi oleh tujuan ideologis dan oleh hasrat untuk perubahan politik.

Dikotomi biner antara kejahatan terorganisir dan terorisme memiliki kesamaan, diantaranya adalah:

1. Keduanya merupakan aktor rasional.
2. Keduanya menggunakan ancaman dan kekerasan.
3. Sama-sama menggunakan penculikan dan pembunuhan.
4. Keduanya melakukan operasi secara diam-diam walaupun pada periode tertentu keduanya ter publikasikan di wilayah yang bersahabat bagi mereka.
5. Keduanya membawa ancaman asimetris untuk negara-negara.

Bab 13

Spionase Siber

13.1 Pendahuluan

Keamanan komputer sekarang menjadi area kepentingan internasional, akademi, teknologi, sosial, dan ekonomi bagi semua negara seiring dengan berkembangnya malware yang menjadi lebih canggih sehingga sering digunakan sebagai alat untuk menyebarkan spionase dunia maya (Wangen, 2015). Pada tahun 2020 terjadi peningkatan serangan *cyber security* akibat munculnya COVID-19 dimana jenis serangan meningkat lebih dari 86% (Pranggono and Arabo, 2021).

Spionase, menurut Merriam-Webster, adalah "praktik mata-mata atau menggunakan mata-mata untuk mendapatkan informasi tentang rencana dan kegiatan terutama pemerintah asing atau perusahaan pesaing." Pada dunia maya, mata-mata adalah pasukan peretas jahat dari seluruh dunia yang menggunakan perang dunia maya untuk keuntungan ekonomi, politik, atau militer.

Penjahat dunia maya tersebut memiliki pengetahuan teknis untuk melakukan kejahatan siber pada hal apapun, mulai dari infrastruktur pemerintah hingga sistem keuangan atau sumber daya utilitas. Tujuan mereka adalah mempengaruhi hasil pemilihan politik, menciptakan kekacauan di acara-acara internasional, dan membantu perusahaan untuk berhasil atau gagal.

Banyak dari penyerang ini menggunakan ancaman persisten lanjutan (APT) sebagai modus operandi mereka untuk diam-diam memasuki jaringan atau sistem dan tetap tidak terdeteksi selama bertahun-tahun. Spionase dunia maya terutama digunakan sebagai sarana untuk mengumpulkan data sensitif atau rahasia, rahasia dagang, atau alamat IP lainnya yang dapat digunakan oleh agresor dan dijual untuk keuntungan finansial.

Dalam beberapa kasus, pelanggaran hanya dimaksudkan untuk menyebabkan kerugian reputasi bagi korban dengan mengekspos informasi pribadi atau praktik bisnis. Serangan spionase dunia maya dapat dimotivasi oleh keuntungan moneter dan juga dapat dikerahkan dalam hubungannya dengan operasi militer atau sebagai tindakan terorisme dunia maya atau perang dunia maya. Dampak spionase dunia maya, terutama jika itu adalah bagian dari kampanye militer atau politik yang lebih luas, dapat menyebabkan terganggunya layanan dan infrastruktur publik, serta hilangnya nyawa.

Spionase dunia maya atau mata-mata dunia maya adalah tindakan memperoleh informasi pribadi, sensitif, atau hak milik dari individu tanpa sepengetahuan atau persetujuan mereka. Dalam masyarakat yang semakin transparan dalam hal teknologi, kemampuan untuk mengontrol informasi pribadi yang diungkapkan seseorang di Internet dan kemampuan orang lain untuk mengakses informasi itu menjadi perhatian yang berkembang seperti penyimpanan dan pengambilan email oleh pihak ketiga, media sosial, mesin pencari, penambangan data, pelacakan GPS, ledakan penggunaan smartphone, dan banyak pertimbangan teknologi lainnya.

Di era big data sekarang, ada kekhawatiran yang meningkat terhadap masalah privasi seputar penyimpanan dan penyalahgunaan data pribadi dan penambangan informasi pribadi tanpa persetujuan oleh perusahaan atau organisasi yang berkepentingan, dan atau penjahat siber.

Mengenai meningkatnya ancaman spionase dunia maya di dunia big data sekarang ini, perusahaan tidak dapat memanggil polisi dan berharap mereka mengejar penjahat dunia maya. Organisasi yang terkena dampak memainkan peran utama dalam setiap penyelidikan karena sistem dan data merekalah yang dicuri atau dimanfaatkan. Pertarungan melawan kejahatan dunia maya harus dilakukan secara kolektif, terlepas dari apakah penjahat itu adalah peretas jahat atau negara bangsa (Jhaveri et al., 2017).

Pada tahun 1968, pemerintah AS mengesahkan Omnibus Crime Control and Safe Streets Act, yang mencakup undang-undang penyadapan yang kemudian

dikenal sebagai Undang-Undang Penyadapan. Undang-undang ini melarang siapa pun untuk dengan sengaja menggunakan perangkat elektronik atau mekanis untuk mencegah komunikasi lisan kecuali jika ada persetujuan sebelumnya atau jika intersepsi terjadi selama kegiatan bisnis biasa.

Pada tahun 1986, Kongres Amerika meloloskan *Electronic Communications Privacy Act* (ECPA) dan juga memperkenalkan *Stored Communications Act* (SCA) yang terutama mencegah orang luar meretas fasilitas yang digunakan untuk menyimpan komunikasi elektronik.

Ada banyak jenis kasus spionase siber yang pernah terjadi di berbagai negara, berikut beberapa contohnya:

1. Pencurian dan penggunaan akun internet orang lain yaitu pencurian atau penggunaan yang tidak sah atas ID dan password orang lain, cukup dengan menangkap ID dan Password yang digunakan oleh pengguna di jaringan internet yang nantinya akan digunakan oleh pencuri tersebut. Akibat pencurian ini, pengguna dikenakan biaya penggunaan akun.
2. Membajak website, yaitu kegiatan yang sering dilakukan oleh cracker adalah merubah halaman web yang dikenal dengan istilah defacement. Pembajakan dapat dilakukan dengan memanfaatkan celah keamanan. Cracker adalah kejahatan dengan mencuri data seperti spoofing, dll, tidak seperti hacker cracker yang biasanya dilakukan dengan niat buruk.
3. Probing dan port scanning merupakan salah satu langkah yang dilakukan cracker sebelum masuk ke server yang dituju adalah dengan melakukan pengintaian. Caranya adalah dengan melakukan "port scanning" atau "probing" untuk melihat layanan apa saja yang tersedia di server target.

Probing dan port scanning merupakan salah satu langkah yang dilakukan cracker sebelum masuk ke server yang dituju adalah dengan melakukan pengintaian. Caranya adalah dengan melakukan "port scanning" atau "probing" untuk melihat layanan apa saja yang tersedia di server target. Misalnya, hasil pemindaian dapat menunjukkan bahwa server target

menjalankan program server web Apache, server email Sendmail, dan sebagainya.

Analoginya dengan dunia nyata adalah untuk melihat apakah pintu Anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar dikunci (menggunakan firewall atau tidak) dan sebagainya. Yang bersangkutan tidak melakukan kegiatan pencurian atau penyerangan, tetapi kegiatan yang dilakukan sudah mencurigakan. Untuk melakukan probing atau portscanning bisa didapatkan secara gratis di Internet.

Salah satu program yang paling populer adalah "nmap" (untuk sistem berbasis UNIX, Linux) dan "Superscan" (untuk sistem berbasis Microsoft Windows). Selain mengidentifikasi port, nmap bahkan dapat mengidentifikasi jenis sistem operasi yang digunakan. Virus. Seperti di tempat lain, virus komputer juga menyebar di Indonesia. Penyebaran umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terinfeksi virus tidak menyadari hal ini. Virus tersebut kemudian dikirim ke tempat lain melalui email.

Serangan *Denial of Service* (DoS) dan *Distributed DoS* (DDoS). Serangan DoS adalah serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan. Serangan ini tidak mencuri, menguping, atau memalsukan data. Efek yang dihasilkan lebih dahsyat dari serangan DoS saja. Kejahatan terkait nama domain. Nama domain digunakan untuk mengidentifikasi perusahaan dan merek dagang. Tetapi banyak orang mencoba untuk mendapatkan keuntungan dengan mendaftarkan nama domain perusahaan orang lain dan kemudian mencoba menjualnya dengan harga yang lebih tinggi.

Pekerjaan ini mirip dengan broker tiket. Istilah yang sering digunakan adalah *cybersquatting*. Masalah lain adalah menggunakan nama domain perusahaan saingan untuk merugikan perusahaan lain. (kasus: mustika-ratu.com) Kejahatan lain yang berkaitan dengan nama domain adalah membuat "domain bermain", yaitu domain yang mirip dengan nama domain orang lain (seperti kasus klikbca.com).

Istilah yang digunakan saat ini adalah typosquatting. IDCERT (Tim Tanggap Darurat Komputer Indonesia). Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat unit pelaporan kasus keamanan. Masalah keamanan di luar negeri ini mulai dikenali dengan

munculnya “sendmail worm” yang menghentikan sistem email internet saat itu.

Kemudian dibentuk *Computer Emergency Response Team* (CERT). Sejak itu, di negara lain, CERT juga dibentuk untuk menjadi titik kontak bagi orang-orang untuk melaporkan masalah keamanan. IDCERT adalah CERT Indonesia. UU ITE (UU Informasi dan Transaksi Elektronik) yang disahkan DPR pada 25 Maret 2008, menjadi bukti bahwa Indonesia tidak lagi tertinggal dari negara lain dalam membuat instrumen hukum di bidang hukum ruang siber. Undang-undang ini adalah cyberlaw di Indonesia, karena isi dan cakupannya yang luas dalam membahas regulasi di dunia maya

13.2 Proses Spionase Siber

Penjahat dunia maya selalu mencari teknik dan metode baru untuk melakukan kegiatan terlarang mereka, oleh karena itu setiap hari semakin banyak teknik yang digunakan dalam melakukan spionase pada dunia maya terutama dalam aspek manusia dan teknis. Aspek manusia didorong untuk menginisiasi spionase dengan kekuatan, politik, ekonomi dan memanipulasi pengetahuan masyarakat dengan menerapkan rekayasa sosial untuk mencapai tujuan mereka.

Di sisi lain, aspek teknis digunakan oleh spionase untuk mengembangkan malware yang canggih dan kompleks. Gabungan antara kedua aspek tersebut sering disebut sebagai social Engineering yang sekarang sudah berkembang menjadi *Espionage-as-a-Service* (Rivera et al., 2022).

13.2.1 Social Engineering

Social Engineering atau Rekayasa Sosial menargetkan mata rantai terlemah dari rantai keamanan informasi yaitu manusia. Sejauh ini, tidak ada kontrol yang diketahui untuk melindungi pengguna dari jenis serangan ini. Faktanya, serangan ini sangat efektif sehingga tidak memerlukan keahlian teknis untuk mendapatkan informasi yang berharga.

Rekayasa sosial adalah proses sosial dan psikologis ketika seorang individu mengekstrak informasi dari organisasi sasaran, bahkan sebagian kecil informasi yang dikumpulkan merupakan pintu untuk mengungkap

kerahasiaan, ketersediaan, dan integritas informasi organisasi korban (Ramadhani, 2018). Sasaran utama dari jenis serangan ini adalah manusia, sehingga menyerang menggunakan bujukan dan pengaruh untuk memanipulasi korbannya.

Serangan ini diklasifikasikan menjadi berikut:

1. Pendekatan fisik

Penyerang melakukan tugas untuk mencari informasi fisik, seperti mencari tempat sampah untuk “menyelam tempat sampah”. Perampokan atau pemerasan adalah jenis serangan lain yang sesuai dengan klasifikasi ini.

2. Pendekatan sosial

Hal ini didasarkan pada penciptaan hubungan dengan korban dan menggunakan persuasi untuk mendapatkan informasi sebanyak mungkin

3. Pembalikan rekayasa sosial

Dalam serangan ini korban meminta bantuan kepada penyerang. Untuk melakukannya, penyerang menyabotase sistem korban dan kemudian menghubungi mereka untuk menawarkan pemecahan masalah, akhirnya penyerang melakukannya, tetapi meminta informasi sensitif kepada korban (misalnya kredensial akses)

4. Pendekatan teknis

Tujuannya adalah untuk mencari informasi pribadi korban melalui Internet menggunakan alat seperti Maltego atau mengumpulkan informasi dari jejaring sosial.

5. Pendekatan sosio-teknis

Serangan ini adalah yang paling kuat, karena penyerang menggunakan umpan (perangkat USB yang ditinggalkan, situs web, atau email) untuk memanfaatkan keingintahuan korban dan mendapatkan informasi rahasia yang berharga. Serangan rekayasa sosial terutama terdiri dari 4 fase:

- a. penelitian;
- b. membangun hubungan saling percaya;
- c. memanfaatkan kepercayaan yang diperoleh;

- d. menggunakan informasi (Grimes, 2020).

Fase-fase ini berulang hingga memenuhi tujuan menggunakan informasi yang dikumpulkan.

13.2.2 Espionage-As-A-Service

Perkembangan teknologi, infrastruktur, dan layanan yang berorientasi pada cloud telah menciptakan pasar layanan teknologi dalam pertumbuhan yang konstan.

Pada awalnya, model dasar layanan di cloud hanya disajikan dalam tiga modalitas: *Platform-as-a-Service* (PaaS), *Infrastructure-as-a-Service* (IaaS) dan *Software-as-a-Service* (SaaS). Akan tetapi seiring berkembangnya teknologi dan kebutuhan akan layanan sehingga segala sesuatu atau apa pun menjadi layanan melalui Internet misalnya: *Monitor-as-a-Service* dengan akronimnya (MaaS), *Communications* (CaaS), *Security* (SecaaS). Spionase sebagai layanan dengan akronimnya (EaaS) menjadi model spionase terbaru memanfaatkan celah tersebut terutama pada industri kedirgantaraan dan pertahanan (Rivera et al., 2022).

Terdapat 5 fase kerja pada EaaS antara lain:

1. Fase 1
Tujuan, pelaku yang menawarkan layanan EaaS mungkin adalah penjahat dunia maya yang akan melakukan serangan itu sendiri. Dalam beberapa kasus, aktor mungkin memiliki pembeli untuk informasi yang dikumpulkan, atau sebaliknya, mereka sudah mengumpulkan informasi dan mencari pembeli.
2. Fase 2
Pengenalan, aktor model EaaS yang disebutkan di atas menggunakan berbagai teknik pengenalan untuk mengidentifikasi serangan. Aktor akan mencari teknologi atau produk tertentu yang ingin diperoleh pelanggan dan bersedia membayar untuk layanan yang diberikan
3. Fase 3
Infiltrasi, ada banyak cara untuk menyusup ke jaringan komputer bernilai tinggi, bahkan jika jaringan dipertahankan dengan baik. Menggunakan serangan phishing atau upaya untuk mendapatkan

informasi data seseorang dengan teknik pengelabuan adalah salah satunya. Dalam serangan ini, penyerang dapat menyamar sebagai karyawan jika diperlukan dan menggunakan beberapa teknik yang disebutkan di atas dalam Rekayasa Sosial.

4. Fase 4

Ekstraksi, setelah informasi diperoleh, penting untuk meninggalkan jaringan tanpa terdeteksi. Penjahat dunia maya profesional ingin terus menjaga akses ke jaringan korban selama bertahun-tahun, sehingga mereka akan membutuhkan kesabaran dan waktu untuk menemukan dan menguji metode terbaik untuk mengeksploitasi lubang keamanan.

5. Tahap 5

Penjualan, pembeli teknologi curian akan mempertimbangkan biaya ini sebagai biaya transfer pengetahuan karena mereka dapat memperoleh teknologi pihak ketiga dengan biaya lebih rendah. Selain banyak layanan model XaaS, versi uji coba produk juga ditawarkan. Pertama, aktor dapat menawarkan sampel data yang dicuri untuk memulai hubungan di masa mendatang dengan pelanggan potensial.

13.2.3 Peran Malware Dalam Spionase Dunia Maya

Malware adalah perangkat lunak berbahaya yang sengaja dirancang untuk mendapatkan akses atau menyebabkan kerusakan pada komputer atau bahkan jaringan. Program jahat ini dapat melakukan berbagai fungsi seperti mencuri, mengenkripsi atau menghapus data sensitif, mengubah atau membajak fungsi komputasi inti dan memantau aktivitas komputer pengguna tanpa izin mereka.

Malware menggunakan vektor penipu untuk mengeksekusi atau menginstal dirinya sendiri di mesin korban seperti unduhan yang tidak sah. Malware didistribusikan menggunakan eksploitasi kerentanan dan melakukan instalasi diam pada mesin korban.

Dalam kasus spionase dunia maya skala besar di mana negara atau aktor dengan sumber daya yang besar terlibat salah satu contohnya adalah kasus *worm Stuxnet* di Amerika Serikat dan Israel. Worm tersebut dirancang untuk menyerang dan menghancurkan sistem Pengawasan Kontrol dan Akuisisi Data (SCADA) Siemens dengan target tertentu dan tujuan destruktif. Worm ini dianggap sebagai salah satu malware paling canggih yang pernah dibuat untuk

spionase. Contoh Malware lain yang dikembangkan untuk spionase yang lebih canggih adalah: Duqu, Flame, Gauss yang merupakan penerus Stuxnet.

Untuk menganalisis kasus yang relevan, pada tahun 2014 pakar keamanan Symantec menghabiskan waktu sekitar delapan bulan untuk menyelidiki salah satu perkembangan paling canggih dari malware mata-mata komputer yang pernah ada hingga saat ini dan dikenal sebagai Regin. Malware tersebut memata-matai pemerintah, operator infrastruktur, perusahaan, peneliti dan individu seperti serangan terhadap Telcos untuk mendapatkan akses ke panggilan yang dialihkan melalui infrastruktur mereka.

Regin adalah alat yang kompleks, memiliki desain modular untuk memungkinkan penambahan dan penghapusan fungsi malware yang berbeda. Malware ini memiliki banyak modul seperti: akses jarak jauh, tangkapan layar, pencurian kata sandi, pemantauan lalu lintas jaringan, dan pemulihan file yang dihapus.

Pengembangan malware ini pasti memakan waktu berbulan-bulan atau bahkan bertahun-tahun dan investasi sumber daya yang besar dan dibuat oleh negara atau organisasi kejahatan dunia maya dengan tingkat kecanggihan yang tinggi untuk operasi spionase yang besar. Analisis yang dilakukan terhadap Regin oleh Symantec menyatakan bahwa malware ini tidak hanya beroperasi pada target tertentu atau fokus pada sektor industri tertentu akan tetapi juga dilakukan di berbagai organisasi, termasuk perusahaan telekomunikasi, usaha swasta dan kecil, entitas pemerintah dan lembaga penelitian.

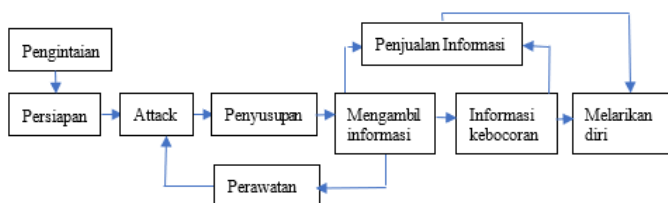
Serangan yang sering dilakukan dalam spionase cyber adalah jenis malware *Advanced Persistent Threat* (APT) yang beroperasi secara backdoor dalam sistem untuk menjaga spionase selama mungkin. Malware lain yang digunakan adalah trojan tipikal dengan fungsi *keylogger*, *backdoor*, dan *spyware*.

Pada perkembangannya, lima fase EaaS berkembang menjadi sembilan fase untuk memenuhi tujuan penyerang, antara lain: pengintaian, persiapan, serangan, infiltrasi, pengumpulan informasi, pemeliharaan, kebocoran informasi, penjualan informasi, dan pelarian.

Tabel 13.1 merangkum kasus-kasus spionase dunia maya yang relevan dan dilengkapi tahun laporan kasus tersebut yang sebagian besar karena malware dari berbagai jenis, seperti *backdoor*, *trojan*, *Remote Access Trojan* (RAT), malware multi-fitur, dan spyware.

Persiapan

Tergantung pada tujuannya terdapat dua vektor serangan berdasarkan teknik yang berbeda. Pertama, rekayasa sosial, keberhasilannya bergantung pada persiapan serangan yang membutuhkan banyak sumber daya, waktu, pengetahuan tentang psikologi manusia, bahasa, dan budaya. Kedua, eksploitasi komputer, keberhasilannya tergantung pada kecanggihan malware yang digunakan dan pengetahuan teknis penyerang untuk mengeksploitasi kemungkinan kerentanan yang sebelumnya terdeteksi pada sistem komputer yang ditargetkan.



Gambar 13.1: Proses Spionase Dunia Maya

Serangan

Setelah penyerang menganalisis kerentanan target dan memilih vektor serangan dan teknik dengan faktor keberhasilan tertinggi, maka serangan dapat dilakukan. Selanjutnya, penyerang akan mencoba untuk mendapatkan kredensial akses ke sistem target. Baik melalui malware, backdoor, atau APT, penyerang dapat menunggu beberapa saat untuk melanjutkan ke fase berikutnya atau segera memulai fase ini.

Setelah serangan berhasil, pengintaian internal dilakukan untuk mendapatkan username dan password yang memungkinkan akses ke lebih banyak sumber daya dengan memecahkan kata sandi hash pada serangan brute force. Selama infiltrasi, penyusup mencoba mengumpulkan informasi dari sistem, mirip dengan footprinting tetapi dilakukan secara lokal untuk mempelajari lingkungan korban.

Bahkan ada beberapa alat yang biasanya digunakan dalam peretasan misalnya *nmap*, *dnsenum*, dan *dimitry*. Fase ini adalah yang paling rumit, kesalahan sedikit saja dapat menyebabkan penyusup terdeteksi. Akan tetapi, setelah penyerang memiliki izin yang diperlukan, mereka dapat menginstal keyloggers atau malware spesifik lainnya yang sesuai dengan kebutuhan penyerang,

seperti memasang backdoors baru pada beberapa sistem, membuat koneksi VPN menggunakan kredensial palsu, serta mengautentikasi portal web. Semua ini untuk mempertahankan aksi penyerangan mereka ke dalam sistem secara diam-diam

Pengumpulan Informasi

Setelah penyerang mengetahui lingkungan yang dimata-matai, dia harus mengetahui jenis informasi apa yang dia cari, seperti gambar, dokumen teks, file email, dan database. Sangat Penting untuk mengetahui bahasa korban untuk memfasilitasi identifikasi file dan direktori sistem seperti kecenderungan penggunaan nama username dan juga password karena biasanya penyerang akan mencoba menggunakan informasi ini untuk melakukan *brute force attack* ke sistem korban yang lain.

Jenis malware tertentu untuk membantu tugas ini adalah advance keylogger yang memiliki fungsi untuk menangkap aktivitas yang dijalankan oleh pengguna, seperti percakapan VoIP, tangkapan layar, mengetik karakter apa pun, dan lainnya.

Pemeliharaan

Jika spionase akan dilakukan dalam waktu lama, penyerang harus beradaptasi dengan lingkungan yang berubah - ubah. Jika satu atau lebih backdoor yang diimplementasikan terdeteksi atau disusupi, penyerang akan mengidentifikasi dan menganalisis penyebabnya untuk mencegah hal ini terjadi dengan pada backdoor lain yang didistribusikan ke dalam sistem.

Setelah mereka menerapkan langkah-langkah yang tepat seperti membuat serangan baru untuk mempertahankan eksistensi mereka dalam sistem yang diserang, mereka akan memeriksa apakah mereka dapat melakukan lebih banyak serangan atau menyesuaikan infiltrasi mereka saat ini untuk melanjutkan pengumpulan informasi.

Kebocoran Informasi

Fase ini terjadi bersamaan dengan fase sebelumnya, atau terjadi setelah mengumpulkan semua informasi yang dibutuhkan. Penyerang biasanya mengompresi informasi menggunakan format seperti RAR atau 7z, melindunginya dengan kata sandi atau menerapkan algoritma enkripsi. Untuk mengekstrak informasi, penyerang dapat mengirimkan file tersebut menggunakan jaringan proxy, seperti jaringan Tor (juga dikenal sebagai deepweb), untuk menyembunyikan identitasnya.

Dalam kasus lain, informasi ditransmisikan menggunakan backdoor yang diterapkan pada fase sebelumnya atau bahkan mengunggah informasi di server yang sudah disiapkan untuk diunduh nanti.

Penjualan Informasi

Seperti yang dibahas di bagian sebelumnya, spionase juga ditawarkan sebagai Spionase-sebagai-Layanan (SaaS). Dalam hal ini, pelanggan dari informasi atau teknologi yang dicuri sering kali mencoba mengelola biaya R&D mereka sendiri melalui jenis transfer teknologi ini, karena biaya pembelian informasi hasil curian lebih murah dan effortless daripada membuat unit R&D mereka sendiri untuk mengambil informasi.

Akibatnya, penyerang menggunakan informasi yang dicuri sebagai alat tawar-menawar dengan pihak yang berkepentingan, untuk mendorong pembelian di masa depan dan dengan demikian memanfaatkan proses spionase yang mereka lakukan.

Melarikan Diri

Fase ini dapat terjadi karena beberapa alasan. Biasanya, setelah penyerang selesai mengumpulkan informasi yang dia cari dia akan meninggalkan sistem, atau mungkin membiarkan beberapa backdoor terbuka untuk spionase di masa depan.

Di sisi lain, jika penyerang terdeteksi dan harus meninggalkan misi, maka dia akan mencoba menghapus jejak yang mungkin dapat membahayakan identitasnya sebelum meninggalkan sistem.

13.3 Pencegahan Spionase Siber

Masyarakat saat ini telah tenggelam dalam hiruk-pikuk media yang canggih dan memudahkan pengguna, dan di sisi lain kecanggihan teknologi tersebut dapat menjadi pintu masuk kejahatan spionase siber. Mata-mata dunia maya tersebut bertujuan menyerang privasi dan individu, perusahaan, atau agensi yang menggunakan komputer, smartphone, pad, dan semua yang memiliki kamera terintegrasi seperti webcam.

Seorang mata-mata dunia maya sebenarnya dapat mengakses komputer Anda dengan menggunakan tautan dan jika dibuka, peretas dapat mengunduh akses

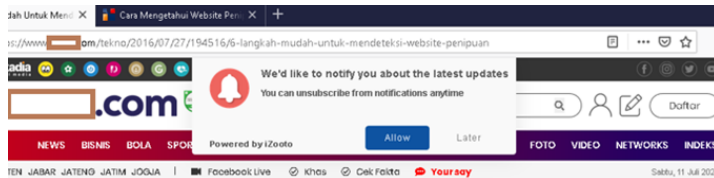
ke komputer. Mematikan perangkat saat tidak digunakan, menutupi kamera di rumah Anda menggunakan lembar catatan tempel untuk menutupi kamera web adalah solusi murah untuk menghindari mata-mata dunia maya di rumah.

Spionase siber dapat masuk melalui cookies yang sering kita temukan ketika mengakses internet. Gambar 13.2 menunjukkan bagaimana cookies meminta izin kepada pengguna untuk mengirimkan informasi terkait pengguna.

Mungkin Anda pernah mengalami hal-hal di bawah ini:

1. Login otomatis di sebuah website tanpa menulis kembali username dan kata sandi.
2. Anda mengunjungi kembali sebuah website dan website tersebut “mengingat” preferensi pengaturan yang Anda pilih sebelumnya.
3. Situs belanja online memberikan saran produk yang sesuai dengan preferensi Anda.

Hal-hal di atas dapat terjadi berkat bantuan cookies. Cookies memang membuat aktivitas browsing di internet lebih cepat, akan tetapi kita harus tetap waspada terhadap situs yang baru atau mencurigakan apalagi jika situs tersebut tidak aman seperti <http://> bukan <https://>

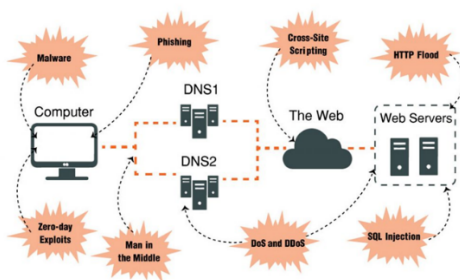


Gambar 13.2: Cookies Meminta Ijin Akses Kepada Pengguna

Spionase siber dapat dilakukan secara software maupun hardware sesuai dengan kerentanan sistem tersebut. Gambar 13.3 menunjukkan sistem yang rentan terhadap serangan spionase siber.

Dari Gambar 13.3 kita dapat melihat ada 5 serangan yang berkaitan dengan spionase siber. Antara lain malware yang mungkin ikut terinstal pada software yang tidak resmi atau dari link yang dikirimkan seperti phishing untuk memata-matai pengguna. Dari luaran komputer juga memungkinkan pencurian data seperti menggunakan keylogger atau packet squirrel. Pada bagian cloud serangan dapat terjadi dengan mengubah isi paket web seperti

cross-site scripting. Dan terakhir adalah serangan SQL-Injection dengan mengambil data yang tersimpan pada database.



Gambar 13.3: Kerentanan Sistem Terhadap Serangan Spionase Siber (Lewis, 2002)

Mata-mata dunia maya atau cyber espionage dapat mengungkap rahasia perusahaan yang dapat berupa informasi pribadi. Serangan itu bisa sangat parah sehingga dapat menjatuhkan perusahaan dengan merusak reputasi perusahaan. Mata-mata dunia maya terhadap pemerintah adalah untuk memperoleh informasi intelijen militer. Informasi ini dapat berupa lokasi unit tentara di perbatasan, keberadaan artileri, dan juga informasi sensitif lainnya mengenai negara.

Saat mendapatkan informasi, penjahat dunia maya dapat menggunakannya untuk keuntungan mereka. Akibatnya bisa berupa hilangnya nyawa. Biasanya target mata-mata cyber adalah: Informasi Internal Perusahaan Informasi yang dicuri dalam kategori ini termasuk data dalam paket penelitian, pengembangan, operasi, dan remunerasi karyawan. Informasi Intelektual/Kekayaan Intelektual Informasi yang dicuri dalam kategori ini adalah informasi berharga yang sedang diteliti seperti proyek rahasia, rencana, dan formula milik organisasi.

Data yang dicuri dapat dijual oleh mata-mata untuk mendapatkan keuntungan pribadi. Informasi tentang Klien dan Pelanggan Informasi detail klien dan pelanggan, layanan yang diberikan dan paket remunerasi yang ditawarkan termasuk dalam kategori data curian ini. Intelijen tentang Pasar dan pesaing Organisasi menetapkan tujuan jangka panjang dan jangka pendek untuk pertumbuhan mereka di pasar.

Tujuan dan perencanaan strategis untuk mencapai tujuan ini adalah rahasia perusahaan yang sangat dijaga. Informasi yang dicuri oleh pesaing

memberikan keunggulan di pasar untuk merencanakan dan tumbuh ke depan. Kehilangan data adalah masalah besar tetapi kehilangan reputasi dapat merusak perusahaan.

Dalam kasus spionase dunia maya, korporasi tidak hanya menghadapi risiko kerugian finansial dan kredibilitas, tetapi juga dari klien dan pemegang saham yang merupakan bagian dari korporasi. Perusahaan yang berurusan dengan pelanggan perlu melindungi data mereka dengan cara apa pun. Pelanggaran data oleh serangan dapat memastikan perusahaan kehilangan kredibilitasnya untuk dapat dipercaya. Ini akan menempatkan pelanggan di belakang kaki dengan pertanyaan yang muncul atas kebijakan keamanan yang diadopsi dan diikuti dalam perusahaan. Ini tidak berakhir di sini. Ini dapat mengakibatkan proses hukum terhadap perusahaan oleh pelanggan yang putus asa. Kerusakan reputasi korporasi sulit diperbaiki.

Komputer adalah buatan manusia. Perangkat lunak yang anda gunakan pasti memiliki kerentanan. Tidak ada keamanan 100% yang tersedia untuk melindungi perusahaan dan pemerintah dari spionase dunia maya. Perhatian utama bagi organisasi dan pemerintah saat ini adalah selalu mengikuti perkembangan kebijakan dan prosedur keamanan.

Untuk mengevaluasi risiko secara teratur dan memiliki kebijakan keamanan yang siap untuk melawan segala jenis kerentanan yang mungkin muncul secara tidak terduga. Banyak perusahaan menjalankan prosedur keamanan harian dan memiliki rencana respons siap untuk diikuti segera setelah serangan terungkap. Pencadangan tepat waktu, pembaruan keamanan, dan pembaruan perangkat lunak dan perangkat keras secara teratur harus diikuti.

Prosedur yang dijalankan ini dicatat dengan baik, dikonfirmasi, dan diaudit untuk prosedur kepatuhan lebih lanjut. Prosedur ini termasuk mengelola perangkat seluler juga. Profesional keamanan siber bekerja dengan departemen TI untuk memiliki firewall keamanan berlapis untuk perlindungan. Firewall dibangun dengan mempertimbangkan lingkungan virtual di tempat kerja. Lingkungan virtual dan perangkat lunak cloud yang banyak digunakan di mana-mana ini juga pasti akan diserang oleh malware dan virus.

Yang benar adalah bahwa tidak ada cara yang pasti untuk menghilangkan setiap serangan. Namun, umumnya disarankan bagi perusahaan dan organisasi lain untuk menilai keamanan dan prosedur mereka saat ini, mengevaluasi risiko, dan mengembangkan kebijakan keamanan yang kuat yang mencakup semua aspek keamanan siber.

Selain itu, proses seperti memiliki cadangan, memperbarui perangkat lunak dan perangkat keras secara teratur, dan pembaruan keamanan lainnya juga harus diikuti, dicatat, diverifikasi, dan diaudit untuk memastikan semuanya telah tercakup. Gunakan sistem keamanan seperti anti-virus, perangkat lunak anti-malware, dan sertifikat SSL untuk memastikan keamanan online. Karena mata-mata dunia maya ini mendapatkan akses melalui celah yang mereka temukan di keamanan online Anda, Anda harus menutup semua celah, dan sertifikat SSL adalah cara terbaik untuk memulai.

Biasanya, situs web yang tidak aman itu semuanya HTTP, tetapi HTTPS atau *Hypertext Transfer Protocol Secure* adalah bentuk HTTP yang lebih aman. SSL adalah kontak lapisan transfer antara server dan situs web Anda, pada dasarnya berfungsi sebagai pengawas untuk memastikan bahwa komunikasi aman dari serangan eksternal. Muncul dalam berbagai jenis dan pada tingkat validasi yang berbeda.

Jika Anda ingin mengamankan domain utama Anda selain beberapa sub domain tingkat pertama, sertifikat wildcard adalah pilihan terbaik Anda. Dengan sertifikat tunggal ini, Anda dapat terus menambahkan sub domain tingkat pertama di bawah domain utama yang dipilih tanpa biaya tambahan.

Misalnya, Anda dapat menggunakan SSL wildcard comodo premium namun murah untuk mengamankan semua sub domain dengan harga terjangkau. Pendekatan penting lainnya untuk membantu mengelola keamanan siber dapat dilakukan dengan menggunakan sistem operasi terbaru untuk perangkat Anda.

Sebagian besar perusahaan menggunakan platform Windows atau MAC tetapi mungkin tidak memperbarui untuk menjalankan versi perangkat lunak terbaru dan paling aman, yang meninggalkan celah keamanan. Versi terbaru biasanya menawarkan perlindungan paling banyak. Biasanya baik untuk menggunakan solusi keamanan TI yang komprehensif dengan penilaian dan pemahaman kerentanan yang mendalam. Itu harus menangani peningkatan dan tambalan perangkat lunak.

Bab 14

Pencegahan Kejahatan Siber

14.1 Pendahuluan

Saat ini Indonesia khususnya dan dunia pada umumnya mengalami perkembangan yang sangat cepat di dibidang informasi. Dalam bidang ini, data dan informasi memiliki peranan yang sangat penting dalam kehidupan bermasyarakat. Salah satu penemuan terbesar dalam perkembangan dunia informasi adalah internet. Seiring berjalannya waktu ketergantungan manusia terhadap internet semakin tinggi. Dewasa ini manusia hampir tidak dapat lepas dari arus informasi dan komunikasi. Hal ini tidak lepas dari perkembangan pesat internet di Indonesia.

Terkait dengan perkembangan yang sangat pesat dari internet, memunculkan sejumlah konsep baru yang saling terkait. Beberapa tahun yang lalu kita semua dikejutkan dengan munculnya Covid-19. Sebuah kondisi dan situasi yang memaksa lahirnya norma-norma baru dalam kehidupan masyarakat. Selama pandemi, terjadi peningkatan aktivitas yang dilaksanakan melalui internet, seperti pembelajaran daring, rapat daring, pelatihan, sertifikasi, transaksi jual beli, pembayaran, olah raga, hingga koordinasi yang dilakukan mulai dari masyarakat hingga pemerintah.

Peningkatan aktivitas daring ini juga menyebabkan masalah keamanan semakin bervariasi dan sering terjadi. Keamanan siber merupakan tindakan

yang dilakukan dalam rangka melindungi jaringan, sistem serta program dari pihak luar yang ingin melakukan serangan siber. Berbagai serangan ini biasanya dilakukan untuk dapat memperoleh keuntungan melalui meminta uang kepada pihak yang datanya berhasil diretas, mengganggu kenyamanan dan keamanan dengan cara mengganggu usaha bisnis berbasis siber, serta merusak data penting baik milik masyarakat, pengusaha hingga pemerintah [its.ac.id]. Meningkatnya kejahatan siber menyebabkan diperlukan pengembangan keamanan siber bagi setiap negara, tidak terkecuali Indonesia.

Dalam perkembangan, para ahli mendefinisikan media yang terdapat pada telematika sebagai multimedia. Seiring dengan perkembangannya, dalam penggunaan infrastruktur sistem telekomunikasi terbentuk dunia baru yang disebut sebagai dunia maya atau ruang siber. Kejahatan siber menimbulkan banyak kerugian baik dari sisi kenyamanan, keamanan, serta ekonomi.

Kerugian akibat dari kejahatan siber di Indonesia menurut data CIA sebesar 1,2% dari kerugian global seperti terlihat pada tabel berikut:

Tabel 14.1: Kerugian Akibat Kejahatan Siber di Indonesia dan Global (Handrini, 2014)

	Global	Indonesia
GDP:*	USD 71,620 bn	USD 895 bn
Percent of global GDP:*		1,2%
Cost of:**		
Genuine cyber crime:	USD 3,457 m	USD 43 m
Transitional Cybercrime:	USD 46,600 m	USD 582 m
Cybercriminal infrastructure:	USD 24,840 m	USD 310 m
Traditional crimes becoming cyber:	USD 150,200 m	USD 2,748 m

14.2 Tantangan Pengembangan Kebijakan Keamanan Siber Di Indonesia

Tantangan merupakan segala sesuatu yang meningkatkan kemauan dan kemampuan dalam mengatasi masalah atau kesulitan yang ada (KBBI, 2022). Terdapat 4 (empat) buah bagian penting untuk mendukung perkembangan dari teknologi informasi sebagai berikut (Handrini, 2014):

1. Perangkat lunak dan keras
2. Manajemen
3. Telekomunikasi
4. Perkembangan internet

Keamanan Siber

Keamanan siber dapat disebut sebagai tindakan dalam rangka melindungi informasi dari pihak yang tidak berhak. Serangan siber terhadap informasi dapat berupa segala jenis tindakan yang dilakukan dalam rangka untuk mengambil, merusak serta merubah data dan informasi dari suatu instansi ataupun perorangan.

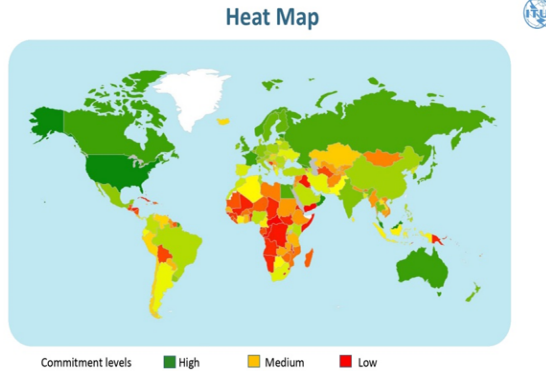
Seiring dengan pesatnya pertumbuhan pengguna internet global serta Indonesia seperti terlihat pada Gambar 14.1.



Gambar 14.1: Perkembangan Jumlah Pengguna Internet dalam 10 (sepuluh) Tahun Terakhir di Indonesia (<https://dataindonesia.id/digital/detail/pengguna-internet-di-indonesia-capai-205-juta-pada-2022>)

Usaha untuk meningkatkan kesadaran dunia dalam keamanan siber, salah satu yang menjadi tolak ukur dapat dilihat dari pemeringkatan *Global Cybersecurity Index (CGI)* oleh *International Telecommunication Union (ITU)* terhadap 193 negara yang menjadi anggota.

Berdasarkan lima pilar GCI framework, yaitu *legal, organizational, technical and procedure, international cooperation, dan capacity building*.



Gambar 14.2: Heat Map Global Cybersecurity Index Tahun 2017

Beberapa Istilah Dalam Keamanan Siber

Beberapa istilah yang biasa dipakai dalam keamanan siber di Indonesia adalah sebagai berikut (Siburian, 2020, hal. 14):

1. Ancaman (Threat).
2. Dampak (Impact).
3. Eksploitasi (Exploit).
4. Keamanan Siber (Cyber Security).
5. Kelemahan (Vulnerability).
6. Penilaian (Assessment).
7. Resiko (Risk).

14.3 Langkah Pencegahan Kejahatan Siber Dari Sisi Pengguna

Beberapa hal yang menjadi celah bagi kejahatan siber adalah adanya ketidakpahaman tentang pentingnya menjaga segala macam aktivitas siber dari sisi pengguna.

Berikut akan dibahas beberapa langkah yang diperlukan untuk mencegah terjadinya kejahatan siber:

Manajemen Kata Sandi

Kata sandi merupakan bagian penting yang dibutuhkan pengguna untuk masuk ke suatu akun tertentu di dunia siber. Dapat dikatakan kata sandi merupakan pintu gerbang untuk mengakses segala macam informasi yang bisa diakses oleh akun pengguna. Karena itu, perlu diperhatikan untuk membuat kata sandi yang cukup rumit sehingga akan menjadi sulit ditebak oleh pihak yang tidak berhak.

Hal yang bisa dilakukan adalah dengan cara membuat kata sandi dengan mengombinasikan angka, huruf dan simbol tertentu untuk meminimalkan kemungkinan terjadinya kejahatan siber. Pada sisi lain, dunia bisnis juga harus mewajibkan penggunanya untuk membuat kata sandi yang cukup panjang dan memuat angka, huruf serta simbol.

Melakukan Audit Terhadap Akun Yang Sudah Dinonaktifkan

Akun hiburan, pendidikan, dan pekerjaan seperti akun email yang sudah tidak digunakan oleh penggunanya dengan berbagai alasan dapat dikatakan sebagai akun yang nonaktif. Akun-akun nonaktif ini dapat menjadi celah bagi kejahatan siber untuk masuk ke dalam suatu sistem dan informasi bersamaan dengan mengakses data yang ada di dalamnya sambil menyamar sebagai pengguna yang sah.

Karena itu, diperlukan suatu tindakan terhadap akun yang sudah tidak digunakan dengan cara menutupnya. Melakukan tindakan penutupan terhadap akun ini dapat menutup salah satu celah bagi kejahatan siber untuk masuk ke sistem secara tidak sah.

Mencegah Adanya Akun dan Kata Sandi Bersama

Salah satu yang harus menjadi prioritas adalah masalah satu akun kerja yang digunakan lebih dari satu orang. Adanya satu akun untuk lebih dari satu orang akan menyulitkan bagi instansi/perusahaan untuk mengidentifikasi siapa yang bertanggung jawab jika terjadi percobaan kejahatan siber. Karena pengguna tersebut dapat mengelak dengan mengatakan bahwa ada pengguna lain yang dapat mengakses akun tersebut.

Sehingga memastikan bahwa tidak ada akun dan kata sandi bersama merupakan bagian upaya dari instansi/perusahaan tersebut untuk mencegah terjadinya kejahatan siber.

Pemakaian Website Yang Aman

Penting bagi instansi/perusahaan untuk memastikan bahwa seluruh bagian yang terlibat di dalamnya memiliki kewajiban untuk mengakses website dengan koneksi https. Hal ini dilakukan untuk memastikan bahwa transfer data dan informasi dapat berlangsung secara aman. Selain itu diperlukan upaya untuk mencegah pengguna dapat mengakses website yang tidak aman dengan koneksi http.

14.4 Pencegahan Kejahatan Siber Dari Sisi Email

Banyaknya celah yang menjadi pintu masuk bagi kejahatan siber, salah satunya melalui email. Sebagian besar komunikasi yang dilakukan individu, instansi, perusahaan, pemerintah dilakukan melalui komunikasi email. Hal ini menyebabkan pelaku kejahatan siber memanfaatkan email untuk mengirimkan virus dan malware melalui email. Sehingga penting bagi instansi/perusahaan untuk menjadikan keamanan email sebagai salah satu prioritas untuk mencegah terjadinya kejahatan siber.

Beberapa hal yang perlu menjadi perhatian dalam menjaga keamanan email adalah sebagai berikut:

Adanya Alat Penyaring

Dalam menjalankan kegiatannya, instansi, perusahaan, dan pemerintah tentu tidak terlepas dari berkomunikasi satu dengan lainnya. Komunikasi melalui email merupakan salah satu media yang banyak dipakai untuk berkomunikasi.

Pihak asing memanfaatkan hal ini untuk mengirimkan malware melalui media email. Mereka berupaya masuk ke dalam sistem komputer untuk mengakses data dan informasi perusahaan melalui malware yang disematkan dalam email. Sehingga diperlukan suatu alat yang berfungsi menyaring seluruh surat yang masuk untuk dapat mendeteksi apakah mengandung malware atau tidak.

Manajemen Kebijakan Email

Pedoman dan peraturan instansi/perusahaan terhadap kebijakan email bagi pengguna email yang berada di bawah naungannya merupakan salah satu upaya untuk menjaga keamanan siber. Hal ini disebabkan email dapat diretas tanpa sepengetahuan pemiliknya dan dapat masuk ke dalam sistem informasi instansi/perusahaan untuk mengambil dan mengirimkan data penting perusahaan seperti akun, password, informasi keuangan serta data pribadi karyawan yang berada di dalamnya.

14.5 Perlindungan Situs Web Dari Kejahatan Siber

Untuk memperluas jangkauan pemasaran, banyak bisnis yang memanfaatkan situs web untuk meningkatkan penjualan produk serta jasa yang mereka tawarkan. Dalam perkembangannya, beberapa bisnis mengumpulkan, menyimpan dan mengelola data pelanggan mereka pada situs web. Akibatnya, perlindungan dan keamanan situs web harus ditingkatkan untuk mencegah dari kejahatan siber.

1. Penyedia web hosting yang aman

Untuk mencari penyedia web hosting yang aman, beberapa hal yang bisa dilakukan diantaranya melalui rekomendasi orang lain yang kita percaya dan telah menggunakan jasa web hosting tersebut. Selain itu, Kita dapat berdiskusi dengan web developer serta menyesuaikannya dengan kebutuhan usaha kita.

2. Sertifikasi Secure Sockets layer (SSL)

Salah satu tanda bahwa suatu situs web aman adalah jika memiliki sertifikat SSL. Situs web dengan sertifikat SSL berarti situs tersebut menyediakan enkripsi dari klien ke server dan sebaliknya. Hal ini, menyebabkan pengguna menjadi nyaman dan percaya bahwa data pribadi yang akan dikirimkan ke situs web tersebut aman dari kejahatan siber.

Daftar Pustaka

- A. Budiman, A. et al. (2021) Mengatur Ulang Kebijakan Tindak Pidana di Ruang Siber: Studi Tentang Penerapan UU ITE di Indonesia. Jakarta: Institute for Criminal Justice Reform (ICJR) .
- Adam Boone (2018) Another Record Year for Vulnerabilities. Time to Join the CIA , embeddedcomputing.com. Available at: <https://embeddedcomputing.com/technology/software-and-os/ides-application-programming/another-record-year-for-vulnerabilities-time-to-join-the-cia> (Accessed: August 15, 2022).
- Andress, J. (2019) Foundations of Information Security: A Straightforward Introduction. No Starch Press.
- APJII. (2022). SURVEI PROFIL INTERNET INDONESIA 2022. Asosiasi Penyelenggara Jasa Internet Indonesia.
- Ashari, I. F. (2018) ‘Graph Steganography Based On Multimedia Cover To Improve Security and Capacity’, in 2018 International Conference on Applied Information Technology and Innovation (ICAITI). IEEE, pp. 194–201.
- Ashari, I. F. (2021) ‘The Evaluation of Image Messages in MP3 Audio Steganography Using Modified Low-Bit Encoding’, Telematika, 15.
- Ashari, I. F. et al. (2022) ‘Vulnerability Analysis and Proven On The neonime . co Website Using OWASP ZAP 4 and XSpear’, Jurnal Teknologi Komputer dan Sistem Informasi (JTKSI), 5(2), pp. 75–81.
- Ashtari , H., (2022). Spiceworks. [Online] Available at: <https://www.spiceworks.com/it-security/vulnerability->

- [management/articles/what-is-hardware-security/](#) [Accessed 20 July 2022].
- Aswandi, R., Muchsin, P.R.N. and Sultan, M. (2020) “Perlindungan Data dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS),” *LEGISLATIF*, 3(2).
- Babiker, M., Karaarslan, E. and Hoscan, Y. (2018) ‘Web application attack detection and forensics: A survey’, 6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding. IEEE, 2018-Janua, pp. 1–6..
- Bamai. (2022). Pengertian Keamanan Aplikasi. Retrieved from <https://bamai.uma.ac.id/2022/03/19/pengertian-keamanan-aplikasi-keamanan-perangkat-lunak-mengacu/>
- Bergman, N., Stanfield, M., Rouse, J., Scambray, J., (2013). *Hacking Exposed: Mobile Security and Solutions*. New York.
- Bhaya, W. and Manaa, M.E. (2014) “Review clustering mechanisms of distributed denial of service attacks,” *Journal of Computer Science*, 10(10). Available at: <https://doi.org/10.3844/jcssp.2014.2037.2046>.
- Buchholz, K. (2022) • Chart: The Costliest Types of Cyber Crime | Statista, Statista. Available at: <https://www.statista.com/chart/27097/most-expensive-types-of-cyber-crime-us/> (Accessed: August 16, 2022).
- Bundet (2010) Konfigurasi & Langkah Membangun Firewall - Bundet. Tersedia pada: <https://bundet.com/d/962-konfigurasi-langkah-membangun-firewall> (Diakses: 22 Agustus 2022).
- Cao, Q., Qiao, Y. and Lyu, Z. (2018) ‘Machine learning to detect anomalies in web log analysis’, 2017 3rd IEEE International Conference on Computer and Communications, ICC 2017, 2018-Janua, pp. 519–523..
- Chakraborty, K., (2021). Techopedia. [Online] Available at: <https://www.techopedia.com/definition/2137/firmware>[Accessed 21 Juli 2022].
- Chazar, C. (2017) ‘Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005’, *Jurnal Informasi*, VII(2), pp. 48–57.
- Cherry, D. (2013). *The basics of digital privacy: Simple tools to protect your personal information and your identity online*. Syngress.

- Ciampa, M. (2015) *Security+ Guide To Network Security Fundamentals*.
- Criddle, C. (2020). Facebook sued over Cambridge Analytica data scandal. *BBC News*.
- Czubik, A. (2016). "The Right to Privacy" by S. Warren and L. Brandeis—The Story of a Scientific Article in the United States. *Ad American*, 17, 211-219.
- Datacomm, (2017). Manfaat dan Solusi Mobile Device Management. URL <https://datacommcloud.co.id/manfaat-dan-solusi-mdm/>
- Dewan Teknologi dan Komunikasi Nasional (2018) "Pengembangan keamanan siber nasional," Policy Paper [Preprint].
- Dewanta, I.G.G.K., (2020). Jenis Serangan Siber yang Paling Sering Mengancam Pengguna Aplikasi pada Perangkat Mobile. URL <https://socs.binus.ac.id/2020/11/22/jenis-serangan-siber-yang-paling-sering-mengancam-pengguna-aplikasi-pada-perangkat-mobile/>
- Dinanda Diadeska Diara (2020) "Strategi Keamanan Siber Korea Selatan," *Jurnal Indonesia Sosial Sains*, 1(4). Available at: <https://doi.org/10.36418/jiss.v1i4.44>.
- Dutson, J., Allen, D., Eggett, D., & Seamons, K. (2019, June). Don't punish all of us: measuring user attitudes about two-factor authentication. In 2019 IEEE European symposium on security and privacy workshops (EuroS&PW) (pp. 119-128). IEEE. (Username dkk)
- Dwinanto, I. and Setiyani, H. (2021) 'IMPLEMENTASI KEAMANAN KOMPUTER PADA ASPEK CONFIDENTIALITY , INTEGRITY , AVAILABILITY (CIA) MENGGUNAKAN TOOLS LYNIS AUDIT SYSTEM', 8(1), pp. 35–46.
- ELSAM. (2015). *Privasi 101 Panduan Memahami Privasi dan Perlindungan Data*. Privacy International.
- Fauzan, R. (2018) "Karakteristik Model dan Analisa Peluang-Tantangan Industri 4.0," *Jurnal Teknik Informatika Politeknik Hasnur*, 4(1).
- Feradhita NKD (2022) Mengapa Indonesia Jadi Negara dengan Keamanan Siber Terburuk di Dunia? , [logique.co.id](https://www.logique.co.id). Available at: <https://www.logique.co.id/blog/2022/08/15/indonesia-jadi-negara-dengan-keamanan-siber-terburuk/> (Accessed: August 15, 2022).

- Gani, A. G. (2019) “Konfigurasi Sistem Keamanan Jaringan,” *JSI (Jurnal Sistem Informasi) Universitas Suryadarma*, 6(1), hal. 134–149.
- Garfinkel, S., Spafford, G. dan Schwartz, A. (2003) *Practical UNIX and Internet security*. “O’Reilly Media, Inc.”
- Geller, E. (2019, September). *How To Build Trust Through Privacy*. Forbes.
- Gold, S. (2004) ‘Threats looming beyond the perimeter’, *Information Security Technical Report*, 9(4), pp. 12–14. Available at: [https://doi.org/10.1016/S1363-4127\(04\)00047-0](https://doi.org/10.1016/S1363-4127(04)00047-0).
- Golose, Petrus.(2015) “Invasi Terorisme Ke Cyberspace,” Jakarta : YPIK
- Granthi, P.K., Bansode, S., (2017). *Android Security: A Survey of Security Issues And Defenses*. *International Research Journal of Engineering and Technology (IRJET)* e-I 4.
- Grimes, R. A. (2020) ‘Social Engineering Attacks’, *Hacking Multifactor Authentication*, 4(6), pp. 259–273. doi: 10.1002/9781119672357.ch12.
- Grimes, R. A. (2020) ‘Social Engineering Attacks’, *Hacking Multifactor Authentication*, 4(6), pp. 259–273. doi: 10.1002/9781119672357.ch12.
- Handrini Ardiyanti, (2014) “Cyber Security dan Tantangan Pengembangannya di Indonesia,” *Politica*, vol. 5, no. 1, Juni 2014.
- Hanifurohman, C., Hutagalung, D.D., (2020). *Analisis Statis Menggunakan Mobile Security Framework Untuk Pengujian Keamanan Aplikasi Mobile E-Commerce Berbasis Android*. SEBATIK. <https://doi.org/10.46984/sebatik.v24i1.920>
- Helios, (2022). *Mobile Device Management (MDM), Solusi Monitor dan Proteksi Perangkat Inventaris Perusahaan*. URL <https://www.helios.id/blog/detail/mobile-device-management-mdm-solusi-monitor-dan-proteksi-perangkat-inventaris-perusahaan>
- Hendropriyono, AM. (2009) “Terorisme:Fundamentalis, Kristen, Yahudi, Islam,” Jakarta : Kompas Media Nusantara.
- Herberger, C. (2018) *Worldwide Cybersecurity Laws, Regulations, Directives, Standards*, Radware Ltd. Available at: <https://blog.radware.com/security/2018/06/cybersecurity-laws-regulations-directives-standards/> (Accessed: August 16, 2022).

- Hrestak, D., Picek, S., Rumenjak, Z., (2015). Improving the android smartphone security against various malware threats. IEEE. <https://doi.org/10.1109/MIPRO.2015.7160474>
- Huxham, H. (2006) Own view of Enterprise Information Security Architecure(EISA) Framework.
- Jackson, Robert & George Sorensen.(2005) “Pengantar Studi Hubungan Internasional,” Yogyakarta : Pustaka Pelajar.
- Jann Chambers (2021) The Latest Cybersecurity Statistics for 2022 | - UKWebHostReview, ukwebhostreview.com. Available at: <https://www.ukwebhostreview.com/cybersecurity-statistics/> (Accessed: August 15, 2022).
- Jhaveri, M. H. et al. (2017) ‘Abuse reporting and the fight against cybercrime’, ACM Computing Surveys, 49(4), pp. 1–27. doi: 10.1145/3003147.
- Jose, A., (2014). Tips Mengamankan Perangkat Mobile dari Peretas. Oketechno. URL <https://techno.okezone.com/read/2014/10/20/57/1054675/tips-mengamankan-perangkat-mobile-dari-peretas>
- Kaspersky, (2014). Kaspersky Lab and INTERPOL Report: Every Fifth Android User Faces Cyber-Attacks. URL https://www.kaspersky.com/about/press-releases/2014_kaspersky-lab--interpol-report-every-fifth-android-user-faces-cyber-attacks
- Kemp, S. (2021) Digital 2021: Indonesia. We Are Social.
- Kennedy, J.M.T. (2009) The Information Security Triad: CIA.
- Khasanah, S. N. (2016) “Keamanan Jaringan Dengan Packet Filtering Firewall (Studi Kasus: PT. Sukses Berkat Mandiri Jakarta),” Jurnal Khatulistiwa Informatika, 4(2).
- Lewis, J. A. (2002) ‘Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats’, Center for Strategic and International Studies, (December), pp. 1–12.
- Li, X. and Xue, Y. (2011) ‘A survey on web application security’, Nashville, TN USA. Citeseer, 25(5), pp. 1–14.
- Listiyani, D., (2017). Kurang Perlindungan, Hacker Incar Celah Keamanan Perangkat Mobile. I News. URL

<https://www.inews.id/amp/techno/internet/kurang-perlindungan-hacker-incar-celah-keamanan-perangkat-mobile>

- Listyorini, P. I. I. S. (2021) ‘Sistem Keamanan SIMRS di Rumah Sakit’, *Prosiding Seminar Informasi Kesehatan Nasional (SIKESNAS)*, pp. 234–240.
- Louis, B., & Samuel, W. (1890). The right of privacy. *Harvard Law Review*, 4(5), 193-220.
- M, L. (2022) Apa Itu Keamanan Siber: Cari Tahu Pengertian Dari Keamanan Siber, [id.bitdegree.org](https://id.bitdegree.org/tutorial/apa-itu-keamanan-siber/). Available at: <https://id.bitdegree.org/tutorial/apa-itu-keamanan-siber/> (Accessed: August 15, 2022).
- Matondang, N., Isnainiyah, I. N. and Muliawatic, A. (2018) ‘Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)’, *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 2(1), pp. 282–287. doi: 10.29207/resti.v2i1.96.
- Matt Ahlgreen (2022) Statistik, Tren & Fakta Keamanan Siber yang Penting untuk 2022, [websiterating.com](https://www.websiterating.com). Available at: <https://www.websiterating.com/id/research/cybersecurity-statistics-facts/> (Accessed: August 15, 2022).
- Muhammad, A., (2022). Inilah MDM Beserta Fungsinya di Dalam Bisnis. URL <https://cianjurtoday.com/mdm/>
- Munawar, Z. dan Putri, N. I. (2020) “Keamanan Jaringan Komputer Pada Era Big Data,” *J-SIKAI Jurnal Sistem Informasi Karya Anak Bangsa*, 2(01), hal. 14–20.
- Nasher, F. (2020) ‘Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (Lpse) Di Dinas Komunikasi Dan Informatika Kabupaten Cianjur Dengan Menggunakan Sni Iso/Iec 27001:2013’, *Media Jurnal Informatika*, 10(1), pp. 1–16. doi: 10.35194/mji.v10i1.465.
- National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST CSWP 04162018. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST CSWP 04162018. Available at: <https://doi.org/10.6028/NIST.CSWP.04162018>.

- NIST (2012) Information Security. NIST Special Publication 800-30. U.S. Department of Commerce, p. 95.
- Nita Azhar (2021) Serangan Cyber Security Indonesia Tahun 2020 VS 2021 , ids.ac.id. Available at: <https://ids.ac.id/serangan-cyber-security-indonesia-tahun-2020-vs-2021/> (Accessed: August 15, 2022).
- Nurul, S., Anggrainy, S. and Aprelyani, S. (2022) ‘Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi , Teknologi Informasi Dan Network (Literature Review Sim)’, Jurnal Ekonomi Manajemen Sistem Informasi (Jemsi), 3(5), pp. 564–573.
- Odishvili, N. (2021) The Fundamentals of Cyber Law in the International and National Spheres - Cyber Insights, Cyber Insights Magazine. Available at: <https://www.cyber-insights.org/the-fundamentals-of-cyber-law-in-the-international-and-national-spheres/> (Accessed: August 16, 2022).
- Pan, Y. et al. (2019) ‘Detecting web attacks with end-to-end deep learning’, Journal of Internet Services and Applications. Journal of Internet Services and Applications, 10(1)..
- Pitchan, M.A. and Omar, S.Z. (2019) “Cyber security policy: Review on netizen awareness and laws,” Jurnal Komunikasi: Malaysian Journal of Communication, 35(1). Available at: <https://doi.org/10.17576/JKMJC-2019-3501-08>.
- Prakasa, J. E. W. (2020) ‘Peningkatan Keamanan Sistem Informasi Melalui Klasifikasi Serangan Terhadap Sistem Informasi’, Jurnal Ilmiah Teknologi Informasi Asia, 14(2), p. 75. doi: 10.32815/jitika.v14i2.452.
- Pranggono, B. and Arabo, A. (2021) ‘ COVID -19 pandemic cybersecurity issues ’, Internet Technology Letters, 4(2), pp. 4–9. doi: 10.1002/itl2.247.
- Rahmawati, C. (2019) “Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0,” in Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO AAU).
- Ramadhani, A. (2018) ‘Keamanan Informasi’, Nusantara - Journal of Information and Library Studies, 1(1), p. 39. doi: 10.30999/n-jils.v1i1.249.
- Randall, A. (2011) Risk and Precaution. 1st edn. Cambridge University Press. Available at: <https://doi.org/10.1017/CBO9780511974557>.

- Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level-a literature review. *Vilakshan-XIMB Journal of Management*.
- Rivera, R. et al. (2022) 'An Analysis of Cyber Espionage Process', *Smart Innovation, Systems and Technologies*, 255(February), pp. 3–14. doi: 10.1007/978-981-16-4884-7_1.
- Rohmansyah, R.R., Nurwasito, H., (2018). Pengembangan Aplikasi Mobile untuk Sistem Keamanan Kantor Menggunakan NFC (Near Field Communication) dan Wi-Fi (Studi Kasus : PT. Rahmi Ida Nusantara) 2, 81–90.
- Ross, R., McEvelley, M. and Oren, J.C. (2018) *Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1*. NIST SP 800-160v1. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST SP 800-160v1. Available at: <https://doi.org/10.6028/NIST.SP.800-160v1>.
- Sahri, I.K. (2018) "ICT dan Perubahan Budaya di Indonesia: Kajian atas Penggunaan ICT Kecenderungan Perubahan Budaya Masyarakat Indonesia," *TARBAWI*, 6(2). Available at: <https://doi.org/10.36781/tarbawi.v6i1.2967>.
- Sepis, Y.T. (2022) 'ANALISA KEAMANAN SISTEM INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 DENGAN DOMAIN DSS05 DAN APO13 DI PT XYZ', *TeIKa*, 12(01), pp. 35–42. Available at: <https://doi.org/10.36342/teika.v12i01.2821>.
- Siburian, H., Moeldoko, H., Latif, A. A. (2020) "Data and Cyber Security Technology, Use Case and Governance," Bandung: Perkumpulan Basis Data Indonesia.
- Sihotang, J.I. (2021) *Sistem Informasi Akuntansi dan Bisnis*. Yayasan Kita Menulis.
- 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*. Yogyakarta: Andi Publisher.
- Sofyan Tsauri (2014) *Manajemen Kinerja*. STAIN Jember Press.

- swarnavo09 (2022) Elements of Cybersecurity - GeeksforGeeks, geeksforgeeks.org. Available at: <https://www.geeksforgeeks.org/elements-of-cybersecurity/> (Accessed: August 15, 2022).
- Tashiha (2017) Keamanan Jaringan Internet dan Firewall – Ditjen Aptika. Tersedia pada: <https://aptika.kominfo.go.id/2017/06/keamanan-jaringan-internet-dan-firewall/> (Diakses: 22 Agustus 2022).
- Tatte, G., Bamnote, G.R., (2013). Mobile Device Management: A Functional Overview. *International Journal of Computer Science and Applications* 6, 319–323.
- Thielman, S. (2016). Apple v the FBI: what's the beef, how did we get here and what's at stake?. *The Guardian News*.
- Thornton, Rod. (2007) “Asymmetric Warfare,” UK : Polity Press.
- Threestayanti, L., (2020). 10 Tips Agar Perangkat Mobile Aman Digunakan oleh Karyawan. *Info Komputer*. URL <https://infokomputer.grid.id/read/122229770/10-tips-agar-perangkat-mobile-aman-digunakan-oleh-karyawan?page=all>
- Triyadi (2019) Apa itu Firewall? Pengertian, Fungsi dan Cara Kerja. Tersedia pada: <https://www.rumahweb.com/journal/apa-itu-firewall/> (Diakses: 22 Agustus 2022).
- Valeur, F., Mutz, D. and Vigna, G. (2005) ‘A learning-based approach to the detection of SQL attacks’, *Lecture Notes in Computer Science*, 3548(Detection of Intrusions and Malware, and Vulnerability Assessment: Second International Conference, DIMVA 2005. Proceedings), pp. 123–140..
- Varga, G. (2022) Global Cybercrime Report: Which Countries Are Most at Risk? 2022 - SEON, seon.io. Available at: <https://seon.io/resources/global-cybercrime-report/> (Accessed: August 16, 2022).
- Vinayakumar, R. et al. (2019) *Cybersecurity and Secure Information Systems*, Springer Nature Switzerland AG 2019. Springer International Publishing.
- Von Solms, R. and Van Niekerk, J. (2013) ‘From information security to cyber security’, *computers & security*. Elsevier, 38, pp. 97–102.

- Wang, Y., Alshboul, Y., (2015). Mobile Security Testing Approaches and Challenges. <https://doi.org/10.1109/MOBISECSERV.2015.7072880>
- Wang, Y., Streff, K., Raman, S., (2012). Smartphone Security Challenges. *IEEE* 45. <https://doi.org/10.1109/MC.2012.288>
- Wangen, G. (2015) 'The role of malware in reported cyber espionage: A review of the impact and mechanism', *Information (Switzerland)*, 6(2), pp. 183–211. doi: 10.3390/info6020183.
- Wangen, G. (2015) 'The role of malware in reported cyber espionage: A review of the impact and mechanism', *Information (Switzerland)*, 6(2), pp. 183–211. doi: 10.3390/info6020183.
- Widyawinata, R. (2021). 9 Rekomendasi Tools Terbaik untuk Security Analyst. Retrieved from https://glints.com/id/lowongan/tools-security-analyst/#.YudQ_3ZBxPY

Biodata Penulis



Yose Indarta S.Pd., SH., M.Pd., MH., MM., M.Sos saat ini menjabat sebagai Perwira Polisi di kantor pusat Kepolisian Negara Republik Indonesia, Jakarta. Beliau lahir di Padang, Sumatera Barat, Indonesia pada tanggal 11 Juni 1984. Lulus dari Universitas Negeri Padang dengan gelar Sarjana Teknik Elektro pada tahun 2007. Dan pada tahun 2009 beliau meraih gelar Magister Pendidikan Vokasi di Universitas Negeri Padang. Beliau juga merupakan lulusan Sarjana Hukum dan Magister Hukum dari Universitas Bhayangkara Jakarta Raya pada tahun 2016.

Kemudian melanjutkan studi Magister Manajemen pada tahun 2021 di STIE Mahardika, Surabaya, Jawa Timur. Pada tahun 2022 juga mendapatkan gelar Magister Intelligent Strategic Study dari STIN, Jakarta. Saat ini merupakan kandidat Doktor di bidang Teknologi dan Pendidikan Vokasi. Aktif sebagai Dosen di organisasinya dan memiliki ketertarikan pada teknologi pendidikan, sumber daya pendidikan terbuka, pembelajaran digital, lingkungan pembelajaran virtual dan TVET.



Fadhli Ranuharja, Lahir pada tahun 1989 tanggal 10 bulan Agustus, kelahiran Minang pernah belajar di Jawa. Menamatkan bangku kuliah 2014 S1 Pend Teknik Informatika dengan mengangkat skripsi berupa tugas akhir mengenai perancangan web dinamis menggunakan bahasa Pemrograman Java (JSP). Memahami beberapa bahasa pemrograman, Java Script dalam mengembangkan website. Menjadi seorang konsultan IT dalam perancangan database hingga tamat. Mengambil studi S2 Pend Teknologi Kejuruan di Universitas Negeri Padang dan wisuda pada tahun 2016. Di samping menjadi Illustration Artist dari 2018 sampai

sekarang menjadi Junior Web Developer trainer dan dosen jurusan Elektro Universitas Negeri Padang.



komputasi pervasife.

Ilham Firman Ashari lahir di Batusangkar, . Ia tercatat saat ini sebagai dosen aktif di Program Studi Teknik Informatika Institut Teknologi Sumatera. Sebagai dosen, ilham aktif untuk melakukan penelitian di bidang keamanan informasi, IoT, dan kecerdasan buatan. Ilham adalah lulusan dari Institut Teknologi Bandung tahun 2018 dan bergabung menjadi dosen tahun 2019. Saat ini menjabat sebagai ketua kelompok keilmuan bidang keamanan siber dan



Mobile, Konsep analisa E-Bisnis dan E-commerce, serta Nilai dan Resiko TI. Penulis juga telah memperoleh beberapa sertifikasi berstandar Internasional, serta menghasilkan beberapa karya ilmiah baik secara nasional maupun internasional.

Jay Doan Sihotang, MT. Lahir di Tangerang pada tanggal 17 Juli 1991. Penulis menyelesaikan pendidikan Sarjana Teknologi dari Universitas Advent Indonesia pada tahun 2013. Dan penulis menyelesaikan pendidikan Magister Teknologi dari Institut Teknologi Bandung pada tahun 2016. Saat ini penulis berstatus sebagai Dosen Tetap pada prodi Sistem Informasi di Fakultas Teknologi Informasi Universitas Advent Indonesia. Penulis memiliki bidang peminatan ajar dan penelitian: Jaringan dan Kualitas Layanan Multimedia, Pemrograman



Dr. Janner Simarmata, S.T., M.Kom., C.SP., C.BMC., C.DMP., C.PI., C.PKIR., C.SF., C.PDM., C.SEM., C.COM., C.SI., C.SY., C.STMI INT'L., CBPA., C.WI. 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.



Muhammad Habib Algifari, S.Kom., M.T.I. Lulus S1 di Program Sarjana Ilmu Komputer Universitas Lampung tahun 2014. Lulus S2 di Program Magister Teknologi Informasi Universitas Indonesia tahun 2017. Saat ini adalah dosen tetap Program Studi Teknik Informatika Institut Teknologi Sumatera. Mata kuliah yang diampu diantaranya: Sistem Informasi, Pemrograman Web dan Pengembangan Aplikasi Mobile. Adapun karir profesional yang

pernah dijalani dimulai pada Januari tahun 2014 sampai Agustus tahun 2020 sebagai praktisi pengembang perangkat lunak pada perusahaan-perusahaan swasta di Jakarta. Pengalaman dalam mengembangkan perangkat lunak diantaranya pernah membuat dan mengembangkan sistem B2B dan B2C pada beberapa sektor industri seperti: Airlines, F&B, dan Transportasi Online.



Muhammad Takdir Muslihi lahir di Ujung Pandang, pada 17 Desember 1989. Ia tercatat sebagai lulusan Universitas Hasanuddin Fakultas Teknik Program Studi Teknik Informatika. Saat bertugas sebagai dosen di Akademi Komunitas Industri Manufaktur Bantaeng, Kementerian Perindustrian.



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, technopreneurship dan pendidikan.



A. Aviv Mahmudi, lahir di Rembang, Jawa Tengah, pada tanggal 16 Agustus 1977, anak pertama dari pasangan Mustofa (alm) dan Fai-zah. Penulis adalah Dosen Tetap pada Universitas YPPI Rembang (perubahan bentuk dari STIE YPPI Rembang). Selain itu juga pernah menjabat sebagai Ketua Badan Penjaminan Mutu periode 2013 s.d 2017, Plt/Pembantu Ketua I periode 2020 s.d 2022 pada Sekolah Tinggi Ilmu Ekonomi YPPI Rembang, serta menjabat Wakil Rektor I pada Universitas YPPI Rembang periode 2022-2026. Pen-didikan formalnya dimulai dari SD Nawawiyah Tasikagung Rem-bang, SMP Negeri 1 Rembang, dan SMA Negeri 3 Rembang, dan melanjutkan studi strata satu pada program studi Sistem Informasi, STMIK AKI Pati lulus tahun 2009, serta melanjutkan studi pada Magister Sistem Informasi Universitas Diponegoro Semarang lulus tahun 2014.

Sambil menekuni profesi sebagai dosen, suami dari Layyinatul Wardah yang telah dikaruniai 2 orang putra bernama Hazel Althaf Zulhilmi dan Zafran Kafie El Azzam, banyak melakukan berbagai kegiatan antara lain melaksanakan penelitian dan pengabdian kepada masyakat yang bermuara kepemilikan Ciptaan-HaKI, melakukan kajian akademis, pembicara/narasumber, fasilitator pelatihan di bidang pengembangan Usaha Kecil Menengah berbasis Teknologi Informasi. Selain aktif menulis artikel di berbagai jurnal ilmiah/prosiding

nasional dan internasional, juga aktif sebagai editor, reviewer maupun mitra bestari pada berbagai jurnal penelitian maupun jurnal pengabdian kepada masyarakat.

Penulis juga aktif pada dunia pergerakan dan organisasi. Pada dunia pergerakan, penulis aktif pada IKA-Pergerakan Mahasiswa Islam Indonesia (PMII). Sementara pengalaman organisasi penulis dapatkan menjadi anggota APTIKOM, Sekretaris Lembaga Perekonomian Nahdlatul Ulama Kabupaten Rembang, Anggota Dewan Dakwah Majelis Ulama Indonesia Kabupaten Rembang, Majelis Wakil Cabang NU, Kecamatan Rembang, Pengurus Karang Taruna Kabupaten Rembang, dan pengurus Gabungan Suporter Rembang (Ganster).



Aslam Fatkhudin, S.Kom. M.Kom. kelahiran Pekalongan, 16 Mei 1982 ini merupakan lulusan Program Studi Sarjana Teknik Informatika Universitas Abadi Karya Indonesia (UNAKI) Semarang tahun 2003, melanjutkan pendidikan Pasca Sarjananya di Program Studi Magister Sistem Informasi Universitas Diponegoro (MSI UNDIP) lulus tahun 2014. Saat ini sebagai dosen tetap pada Program Studi Sarjana Informatika yang juga menjabat sebagai Wakil Rektor III Bidang Kemahasiswaan Universitas Muhammadiyah Pekajangan Pekalongan. Sebagai Dosen, beberapa jurnal ilmiah sudah beliau hasilkan, termasuk menjadi narasumber dalam berbagai seminar atau workshop seputar Teknologi Informasi maupun Sistem Informasi.



dunia robotik dan android studio saat ini.

Zelvi Gustiana lahir di salah satu daerah kecil di Sumatera Barat yaitu Sungai Rumbai, pada 16 Agustus 1994. Ia tercatat sebagai lulusan Magister Komputer di Universitas Putra Indonesia "YPTK" Padang. Wanita pecinta kopi ini sedang mendedikasikan dirinya di dunia pendidikan dengan menjadi dosen disalah satu Universitas di Sumatera Utara. Dia juga sedang belajar menulis dengan baik dan ingin menjadi seseorang yang layak untuk membaga ilmu yang ia miliki. Dia juga tertarik dengan



Associate Data Scientist dari BNSP. Selain mengajar penulis juga aktif sebagai programmer lepas pada pembuatan aplikasi website maupun android. Penulis dapat dihubungi pada alamat email edy.subowo@gmail.com.

Edy Subowo lahir di Pekalongan, pada 24 April 1988. Ia tercatat sebagai lulusan Teknik Fisika Universitas Gadjah Mada dan Magister Sistem Informasi Universitas Diponegoro. Laki – laki yang kerap disapa Bowo ini saat ini bekerja menjadi dosen S1-Informatika Fakultas Teknik dan Ilmu Komputer Universitas Muhammadiyah Pekajangan Pekalongan. Penulis beberapa kali mengisi webinar nasional mengenai keamanan siber. Selain itu, penulis juga menyukai bidang Data Science dengan sertifikat



Mohamad Idris, S.Si., M.Sc., lahir di Denpasar pada tanggal 10 Oktober 1986. Pada Tahun 2011 meraih gelar Strata I Program Studi Matematika dari Universitas Udayana (UNUD). Berhasil meraih gelar Strata II Program Studi Matematika dari Universitas Gadjah Mada (UGM) pada tahun 2017. Profesi beliau saat ini adalah Dosen Pegawai Negeri Sipil (PNS) Program Studi Teknik Informatika di Institut Teknologi Sumatera (ITERA). Aktif di berbagai kegiatan akademis dan non akademis baik di ITERA maupun Provinsi Lampung. Menikah pada tahun

2020 dengan Linda Septiani, S.Si., M.Sc. serta dikaruniai satu orang putra pada tahun 2021 bernama Fatih Hamizan Idris. Sejak tahun 2021 melanjutkan studi Strata III di Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung (STEI-ITB).

KEAMANAN SIBER TANTANGAN DI ERA REVOLUSI INDUSTRI 4.0

Teknologi informasi dan komunikasi saat ini digunakan di banyak bidang kehidupan, termasuk sosial, ekonomi, hukum, organisasi, kesehatan, pendidikan, budaya, pemerintah, keamanan, dan pertahanan. Hal ini menjadikan keamanan siber telah mendapat perhatian utama bagi semua negara di dunia. Tingkat bahaya dan ancaman penyalahgunaan teknologi informasi dan komunikasi semakin meningkat dan menjadi lebih rumit karena berbanding lurus dengan tingginya tingkat penggunaan teknologi tersebut.

Semoga memberikan sumbangsih keilmuan dan menambah wawasan bagi semua pihak terutama para akademisi, praktisi, dan pihak-pihak yang tertarik terutama dalam bidang keamanan siber.

Secara lengkap buku ini membahas:

- Bab 1 Keamanan Siber
- Bab 2 Hukum dan Regulasi Siber
- Bab 3 Ancaman Keamanan Siber
- Bab 4 Arsitektur Keamanan Siber
- Bab 5 Keamanan Jaringan
- Bab 6 Keamanan Aplikasi
- Bab 7 Keamanan Privasi
- Bab 8 Keamanan Web
- Bab 9 Keamanan Mobile
- Bab 10 Keamanan Sistem Informasi
- Bab 11 Keamanan Perangkat Keras
- Bab 12 Siber Terorisme
- Bab 13 Spionase Siber
- Bab 14 Pencegahan Kejahatan Siber



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

KOMPUTER- Referensi

ISBN 978-623-342-595-7



9 786233 425957