BUKU

Keamanan SIBER

Esensi Keamanan Sistem Informasi

I Gede Putu Krisna Juliharta
Adrian
Ayu Pradnyandari Dananjaya Erawan

Keamanan siber merupakan salah satu aspek penting dalam dunia teknologi informasi. Maka dari itu, Buku Keamanan Siber: Esensi Keamanan Sistem Informasi membahas tentang pentingnya keamanan siber di era digital saat ini. Buku ini relevan dengan berbagai permasalahan atau studi kasus yang dihadapi karena menjelaskan berbagai aspek keamanan siber seperti:

1. Pengantar Keamanan Sistem Informasi
2. Keamanan Sistem Operasi
3. Keamanan Jaringan dan Koneksi
4. Arsitektur Keamanan Pada *Website*
5. Keamanan *Database*
6. Aspek Keamanan Penggunaan Email
7. *Malware Analysis* dan Proteksi
8. Digital Forensik
9. Penilaian Risiko dan Manajemen Keamanan
10. Keamanan Dari Segi Pengguna
11. Etika dan Hukum dalam Keamanan Siber

Buku ini menggunakan pendekatan dari berbagai *framework* keamanan yang ada sehingga sangat cocok bagi siapapun yang ingin mempelajari dan mengimplementasikannya termasuk dengan latar belakang yang beragam baik dari level mendasar hingga menengah.

BUKU

Keamanan SIBER

Esensi Keamanan Sistem Informasi

eureka media aksara
Anggota IKAPI
No. 225/JTE/2021

0858 5343 1992
eurekamediaaksara@gmail.com
Jl. Banjaran RT.20 RW.10
Bojongsari - Purbalingga 53362

ISBN 978-623-516-106-8
9 786235 161068

BUKU KEAMANAN SIBER

Esensi Keamanan Sistem Informasi

I Gede Putu Krisna Juliharta
Adrian
Ayu Pradnyandari Dananjaya Erawan

PENERBIT CV. EUREKA MEDIA AKSARA

BUKU KEAMANAN SIBER
Esensi Keamanan Sistem Informasi

Penulis : I Gede Putu Krisna Juliharta
Adrian
Ayu Pradnyandari Dananjaya Erawan

Desain Sampul : Eri Setiawan

Tata Letak : Nadhifa Khairusyifa

ISBN : 978-623-516-105-1

Diterbitkan oleh : **EUREKA MEDIA AKSARA, JULI 2024**
ANGGOTA IKAPI JAWA TENGAH
NO. 225/JTE/2021

Redaksi:
Jalan Banjaran, Desa Banjaran RT 20 RW 10 Kecamatan Bojongsari
Kabupaten Purbalingga Telp. 0858-5343-1992
Surel : eurekamediaaksara@gmail.com
Cetakan Pertama : 2024

KATA PENGANTAR

Puji dan syukur kami panjatkan kepada Tuhan Yang Maha Esa yang telah memberikan rahmat dan karunianya, sehingga penulis dapat menyelesaikan "Buku Keamanan Siber: Esensi Keamanan Sistem Informasi".

Keamanan siber merupakan salah satu aspek penting dalam dunia teknologi informasi. Serangan siber telah menjadi ancaman yang nyata bagi berbagai organisasi, baik pemerintah, swasta, maupun individu. Serangan siber dapat menyebabkan kerugian finansial yang signifikan, gangguan operasional, dan bahkan kerusakan reputasi.

Buku ajar ini disusun untuk memberikan pemahaman yang komprehensif tentang esensi keamanan sistem informasi. Buku ini membahas berbagai aspek keamanan siber, mulai dari konsep dasar, ancaman dan kerentanan, hingga praktik terbaik dalam mengamankan sistem informasi.

Buku ini ditujukan untuk berbagai pembaca, termasuk:

- Mahasiswa dan profesional keamanan siber
- Praktisi keamanan siber
- Pemilik bisnis dan manajer TI
- Siapapun yang tertarik untuk belajar lebih lanjut tentang keamanan siber

Akhir kata, semoga buku ini dapat bermanfaat bagi pembaca dalam memahami dan menerapkan keamanan siber untuk melindungi sistem informasi. Kami mengucapkan terima kasih kepada semua pihak yang telah membantu dalam penyusunan buku ini. Semoga buku ini dapat memberikan kontribusi positif bagi peningkatan keamanan siber di Indonesia.

Denpasar, 31 Januari 2024

Tim Penulis

PRAKATA

Dalam era digital yang terus berkembang, tantangan keamanan siber menjadi semakin mendesak di tengah dinamika sistem informasi modern. Buku ini yang berjudul, "Buku Keamanan Siber: Esensi Keamanan Sistem Informasi", hadir sebagai panduan komprehensif yang mengurai inti keamanan sistem informasi dalam lingkup yang semakin kompleks. Melalui pembahasan yang mendalam, buku ini bertujuan untuk memberikan pemahaman yang kokoh tentang prinsip-prinsip keamanan siber yang krusial dalam menjaga keutuhan, kerahasiaan, dan ketersediaan data di era digital ini. Dari konsep dasar hingga isu-isu terkini, buku ini menawarkan wawasan yang berharga bagi para profesional, akademisi, serta siapa pun yang tertarik memahami dan mengimplementasikan praktik keamanan siber yang efektif.

Ketika teknologi informasi menjadi tulang punggung masyarakat global, tantangan keamanan siber pun menjadi semakin mendesak. Perkembangan sistem informasi yang pesat membuka pintu bagi peluang inovasi, tetapi juga meningkatkan risiko terhadap serangan siber yang merugikan. Oleh karena itu, pemahaman yang mendalam tentang keamanan siber menjadi suatu keharusan bagi siapa pun yang terlibat dalam dunia teknologi informasi.

Dalam buku ini, pembaca akan dibimbing melalui perjalanan mendalam dalam pemahaman konsep keamanan siber, mulai dari pemahaman dasar hingga konsep-konsep yang lebih kompleks. Penyajian materi-materi yang relevan dan praktis, dilengkapi dengan studi kasus, tip, dan praktik terbaik yang akan membantu pembaca memperkuat sistem informasi mereka.

Buku ini tidak hanya ditujukan untuk para profesional keamanan siber, tetapi juga bermanfaat bagi mahasiswa, praktisi teknologi informasi, pengusaha, dan siapa pun yang tertarik memahami pentingnya keamanan siber dalam era digital ini. Harapan untuk buku ini adalah tidak hanya menjadi sumber pengetahuan, tetapi juga menjadi panduan yang menginspirasi

pembaca dalam melangkah menuju keamanan siber yang lebih kokoh dan terpercaya.

Ucapan terima kasih sebesar-besarnya kepada semua pihak, yang telah menyumbangkan pengetahuan dan pengalaman mereka dalam pembuatan buku ini, serta kepada pembaca yang telah memberikan dukungan dan kesempatan bagi kelahiran karya ini. Semoga buku ini dapat memberikan kontribusi positif dalam upaya memperkuat keamanan sistem informasi di berbagai sektor.

Denpasar, 31 Januari 2024

Tim Penulis

HALAMAN PERSEMBAHAN

Puji syukur kepada Tuhan Yang Maha Esa, karena atas berkat dan Karunia-Nya penulis dapat menyelesaikan buku keamanan siber dengan judul "Buku Keamanan Siber : Esensi Keamanan Siber". Penulis menyadari dalam penyusunan buku ini tidak akan selesai tanpa bantuan dari berbagai pihak. Karena itu pada kesempatan ini penulis mengucapkan terima kasih kepada:

1. Tuhan Yang Maha Esa yang telah memberikan kesempatan dan kelancaran dalam pembuatan buku ini hingga selesai,
2. Segenap Tim Penulis, yang telah bekerja keras, bahu membahu, dalam menuangkan ide, gagasan, dan pengetahuan mereka, sehingga buku ini dapat tercipta dengan baik.
3. Masing - masing keluarga penulis yang telah memberikan doa, motivasi, serta kasih sayang.
4. Teman - teman, sahabat, dan kenalan yang telah memberikan semangat, dorongan, serta masukan sehingga buku ini dapat diselesaikan.
5. Semua pihak yang tidak dapat disebutkan satu persatu yang telah berkontribusi baik langsung maupun tidak langsung sehingga buku ini dapat terselesaikan.

Penulis menyadari buku ini tidak luput dari berbagai kekurangan. Penulis mengharapkan saran dan kritik demi meningkatkan kualitas buku ini sehingga buku ini dapat memberikan manfaat bagi bidang pendidikan dan penerapannya di lapangan serta bisa dikembangkan lagi lebih lanjut ataupun sebagai bahan referensi.

"Knowledge is of no value unless you put it into practice." – Anton Chekhov

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1 PENGANTAR KEAMANAN SISTEM INFORMASI

A. Pendahuluan

Pemanfaatan internet telah menjadi suatu hal yang umum dalam berbagai aspek kehidupan saat ini, memberikan kontribusi signifikan dalam mempermudah aktivitas manusia sehari-hari. Internet sendiri sudah seperti bagian penting dalam kehidupan manusia yang gunanya untuk berkomunikasi, berbagi informasi serta mengakses berbagai layanan *online*. Internet terkoneksi dengan perangkat yang biasa digunakan oleh manusia seperti laptop, komputer, gadget, *smartwatch* dan lain sebagainya. Dan tentunya pada perangkat - perangkat tersebut terpasang berbagai macam aplikasi yang memudahkan manusia untuk beraktivitas seperti berkomunikasi, berbisnis, berbelanja, mendapatkan informasi, belajar, hiburan dan berbagai macam lainnya. Dengan menjadi tulang punggung bagi revolusi digital, internet telah mengubah cara manusia hidup, bekerja, berinteraksi, dan menjadi peluang tak terbatas serta tantangan yang baru pula dalam era informasi modern.

Tantangan penggunaan internet yang dihadapi di era modern ini semakin kompleks dengan munculnya berbagai jenis kejahatan yang terus berkembang. Kasus kejahatan penggunaan komputer atau internet dalam melakukan aktivitas kejahatan disebut juga kejahatan siber (*cybercrime*). Dikarenakan kecepatan dan skala pertumbuhan teknologi juga menyebabkan perkembangan kejahatan siber menjadi lebih banyak dan canggih. Banyak kasus yang menyerang sistem informasi seperti

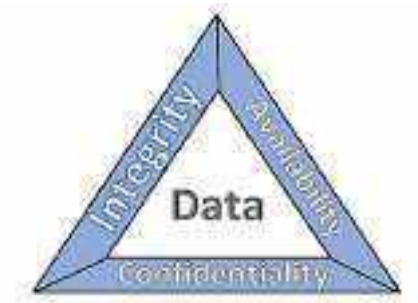
penipuan, peretasan (*hacking*), pencurian data, serangan yang mengganggu layanan sistem (*denial of service*) dan lain-lain. Didalam suatu organisasi atau lingkungan tertentu, Sistem Informasi terbentuk dari serangkaian elemen yang bekerja bersama dan saling mempengaruhi satu sama lain untuk pengumpulan, pemrosesan, penyimpanan dan distribusi informasi. Keamanan sistem informasi menjadi hal yang harus diperhatikan untuk menghindari segala macam kerugian atau hal-hal yang tidak diinginkan dari kejahatan siber.

B. Konsep Dasar Keamanan CIA Triad

Kerahasiaan (*Confidentiality*), Integritas (*Integrity*), dan Ketersediaan (*Availability*) atau disingkat CIA merupakan tiga komponen utama yang perlu diperhatikan dalam menjaga keamanan sistem dan informasi (Cawthra et al., 2020). Konsep keamanan CIA Triad adalah kerangka kerja dasar dalam keamanan informasi yang dibentuk guna melindungi data dan sistem informasi. Adapun CIA dijelaskan sebagai berikut :

1. Kerahasiaan (*Confidentiality*) adalah perlindungan informasi dari akses tidak sah, memastikan hanya pihak yang berwenang yang dapat mengaksesnya. Ini dilakukan melalui enkripsi data, pengaturan hak akses, dan penggunaan kata sandi yang kuat. Contohnya penggunaan enkripsi, membatasi kontrol akses, mengaktifkan autentikasi dua faktor dan lain-lain.
2. Integritas (*Integrity*) adalah keamanan yang memastikan bahwa data tidak dimodifikasi atau dimanipulasi selama penyimpanan, pengiriman, atau pemrosesan. Upaya keamanan integritas melibatkan penggunaan tanda tangan digital, *hash functions*, dan pengawasan untuk mendeteksi perubahan yang tidak sah dalam data.
3. Ketersediaan (*Availability*) mengacu pada kemampuan untuk memastikan bahwa sistem komputer, data, atau layanan selalu tersedia dan dapat diakses oleh pengguna yang berhak ketika diperlukan. Ini berarti menjaga agar sistem atau

layanan tetap berjalan dengan baik tanpa gangguan atau ketidaktersediaan.



Gambar 1. 1 CIA Triad
Sumber : National Institute of Standards and Technology (2020)

CIA Triad menciptakan kerangka kerja yang komprehensif untuk merancang strategi keamanan informasi, dengan tujuan mencapai keseimbangan antara melindungi kerahasiaan data, menjaga integritas data, dan memastikan ketersediaan sistem dan data, yang menjadi landasan dalam mengembangkan kebijakan keamanan, mengidentifikasi risiko keamanan, dan merancang kontrol keamanan yang sesuai untuk melindungi informasi berharga dalam banyak organisasi.

C. Pentingnya Keamanan Siber Dalam Dunia Teknologi Informasi

Kejahatan di internet dibutuhkan penangan khusus sehingga polisi saja tidaklah cukup melainkan dibutuhkan juga tenaga yang ahli di bidang IT atau lebih tepatnya di bidang keamanan siber (*cyber security*). Keamanan siber bukan lagi sekedar opsi, tetapi suatu kebutuhan yang mendesak dalam era teknologi modern demi menjaga data yang sensitif, mencegah gangguan sistem, dan melindungi reputasi organisasi. Cakupan keamanan siber yang harus dipertimbangkan tidaklah sekedar individu maupun organisasi, melainkan institusi, pemerintahan, atau bahkan negara.

1. Pengertian Cyber Security

Keamanan Siber, atau yang sering disebut juga sebagai *cyber security*, adalah bagian dari bidang teknologi informasi yang bertujuan untuk melindungi perangkat keras dan lunak (*hardware* dan *software*), jaringan, serta data dari akses yang tidak sah dan upaya pembobolan melalui internet oleh pihak yang tidak diinginkan seperti penjahat siber, teroris, atau peretas. Bidang keamanan siber mencakup beberapa area, termasuk keamanan jaringan (*network security*), komputasi awan (*cloud computing*), analisis keamanan (*security analysis*), basis data (*database*), dan lain-lain. Penggunaan komputer atau perangkat elektronik yang terhubung ke jaringan meningkatkan risiko terhadap serangan *cybercrime*.

Motivasi di balik *cybercrime* bervariasi dan tidak selalu dapat diketahui dengan pasti. Beberapa motif umum termasuk keuntungan finansial, uji coba pengetahuan dan keterampilan, motivasi pribadi seperti balas dendam atau reputasi, mendapatkan akses, dan lain-lain. Penting untuk dicatat bahwa tidak semua peretas memiliki niat jahat; beberapa memiliki motif yang lebih etis dan berperan dalam meningkatkan keamanan siber dengan menemukan dan memperbaiki kerentanan sistem.

Di Indonesia, tindakan kejahatan siber ilegal diatur oleh Undang-undang Informasi dan Transaksi Elektronik (UU ITE). Undang-undang ini mencakup berbagai aspek kejahatan siber, keamanan siber, dan perlindungan data. Kehadiran regulasi seperti UU ITE diharapkan dapat memberikan deterensi bagi penjahat siber dengan membuat mereka berpikir dua kali sebelum melaksanakan aksinya.

2. Lingkup Cyber Security

Mempertahankan, mencegah dan memelihara agar terhindar dari kerugian merupakan tugas utama dari adanya *cyber security*. *Cyber security* ini memiliki berbagai cakupan tentang aspek – aspek saja yang termasuk kedalam keamanan yang harus dijaga, yang dijelaskan sebagai berikut :

a. Keamanan jaringan (*Network Security)* melibatkan serangkaian tindakan dan prosedur yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data yang berada dalam suatu jaringan komputer atau infrastruktur jaringan.
b. Keamanan perangkat lunak (*Software Security)* melindungi aplikasi dan sistem komputer dari ancaman dengan mengimplementasikan anti *virus* & anti *malware* serta melakukan patch management untuk memperbarui software dan sistem operasi dengan versi keamanan terbaru.
c. Keamanan data (*Data Security*) melibatkan perlindungan data sensitif dari akses tidak sah atau kebocoran. Contoh penerapan bidang keamanan data meliputi penggunaan enkripsi serta *backup* & *recovery*.
d. Keamanan Aplikasi (*Application Security*) bertujuan melindungi aplikasi perangkat lunak dari kerentanan yang dapat dimanfaatkan oleh peretas. Ini melibatkan pengujian keamanan aplikasi untuk mengidentifikasi dan mengatasi kerentanan seperti celah keamanan atau masalah autentikasi.
e. Keamanan Identitas dan Akses (*Identity* and *Access Management*) mengelola identitas pengguna dan kontrol akses mereka ke sistem dan data. Ini melibatkan sistem autentikasi yang kuat, otorisasi yang tepat, dan manajemen hak akses.
f. Keamanan Fisik (*Physical Security*), berkaitan dengan perlindungan terhadap akses fisik yang tidak sah atau tidak sah ke sumber daya, perangkat keras, infrastruktur, dan fasilitas penting lainnya.
g. Keamanan Sosial (*Social Engineering Security*) adalah keamanan yang berkaitan dengan taktik manipulasi mental yang digunakan oleh peretas untuk mendapatkan akses ke sistem. Ini melibatkan tipuan seperti *phishing*, *social engineering*, dan serangan manipulatif lainnya.

h. Keamanan Cloud (*Cloud Security*) melibatkan perlindungan data dan aplikasi yang disimpan di lingkungan cloud. Ini mencakup konfigurasi yang benar dari layanan *cloud*, manajemen *cloud*, dan kebijakan keamanan untuk melindungi sumber daya *cloud*.
i. Keamanan Internet of Things (IoT *Security*) adalah upaya untuk melindungi perangkat, jaringan, data, dan sistem dalam lingkungan *Internet of Things* (IoT) dari potensi ancaman, serangan, atau risiko yang dapat merusak integritas, kerahasiaan, dan ketersediaan informasi serta fungsionalitas perangkat IoT.

3. Mengapa Cyber Security Penting

Penyimpanan data dan informasi dalam media *online* atau secara *online* membuat *cyber security* sangat penting untuk berbagai aspek terutama aset digital dan kerahasiaan, pentingnya *cyber security* dijelaskan sebagai berikut :

a. *Cyber security* melindungi data pribadi, termasuk data medis, keuangan, identitas, dan informasi rahasia, baik untuk individu maupun organisasi.
b. Keamanan bisnis, untuk mendukung perkembangan bisnis dari segi keamanan dengan menjamin keamanan dari segi informasi bisnis, aset, dan data pegawai atau konsumen.
c. Keamanan nasional, data kependudukan dan catatan sipil negara tidak hanya disimpan di kantor, tapi juga secara online. Kehilangan keamanan data dapat berdampak buruk bagi negara, karena data yang bocor dapat menjadi resiko bagi penduduk.
d. Kepercayaan pengguna dan konsumen sangat penting bagi perusahaan, instansi, atau individu terkenal atau penting. Keamanan harus semakin baik untuk memberikan jaminan keamanan bagi pengguna layanan online atau penyimpanan informasi sensitif mereka.

e. Regulasi tentang keamanan data pengguna sudah tercantum dalam peraturan negara seperti UU Perlindungan Data Pribadi di Indonesia dan CCPA di California. Regulasi ini mewajibkan organisasi untuk menjaga data pribadi dan privasi konsumen serta menerapkan langkah-langkah keamanan yang baik.
f. Semakin baik keamanannya, semakin rendah risiko kriminalitas seperti peretasan atau kerugian. Bentuk kriminalitas bisa bervariasi dan tidak terduga. Jika data tidak aman atau bocor, dapat digunakan untuk penipuan atau transaksi ilegal di situs gelap.

4. Jenis-jenis Ancaman Siber

Ancaman yang dihadapi bervariasi dan menyesuaikan dengan tujuan dari peretas, kegiatan peretas ketika melakukan aksi dapat berupa berbagai bentuk ancaman seperti menyebarkan *virus*, *malware*, *hacking, denial of service* dan lain - lain (McGuire & Downling, 2013). Ancaman dapat sederhana atau kompleks, dengan sumber daya dari individu atau organisasi terorganisir. Ancaman bi CIA Triad sa bekerja secara simultan atau berurutan sesuai keinginan penyerang. Jenis ancaman siber meliputi :

a. *Virus* adalah *malware* (*malicious ware)* yang diciptakan untuk menginfeksi komputer tanpa izin pemiliknya, mengeksploitasi kerentanan sistem, atau mencuri data. *Virus* pertama, disebut "Creeper", muncul pada tahun 1971 dan menginfeksi sistem operasi TENEX, menampilkan pesan "I'M THE CREEPER CATCH ME IF YOU CAN". *Virus* telah berkembang menjadi lebih bervariasi dan berbahaya di era internet modern. Pada tahun 2003, *virus* telah menjadi ancaman serius bagi bisnis dan organisasi, mengganggu layanan ATM, menunda jadwal penerbangan, dan memengaruhi pusat layanan. (Balthrop et al., 2004).

Gambar 1. 2 *Virus Creeper*
Sumber : Podle Rose Barfield (2021)

b. *Worm* adalah jenis *malware* yang berbeda dari virus karena tidak memerlukan interaksi pengguna dan dapat menyebar melalui jaringan, sistem, atau perangkat. Pada tahun 1971, istilah "virus" belum tepat untuk menjelaskan "Creeper" karena karakteristiknya yang lebih mirip *worm*, yang dapat menggandakan diri tanpa inang melalui jaringan. Pada tahun 1988, Morris Worm, diciptakan oleh Robert Tappan Morris, menyebar dengan cepat melalui internet dan menginfeksi ribuan komputer. Morris Worm menyebabkan penurunan kinerja sistem dan meningkatkan kesadaran akan pentingnya keamanan sistem dan perlindungan terhadap serangan dan kerentanan.

Gambar 1. 3 *Morris Internet Worm*
Sumber : Ministry of Science and Education of the Republic of Azerbaijan Institute of Information Technology (2017)

c. *Trojan* adalah *malware* yang menyamar sebagai program atau *file* yang sah, tetapi sebenarnya memiliki tujuan jahat. Biasanya, *trojan* memiliki fungsi *remote control* yang memungkinkan penyerang mengendalikannya untuk mencuri data, merusak sistem, membuka pintu keamanan, dan mencuri kata sandi (Tasril et al., 2017). Nama "Trojan" diambil dari kisah perang Yunani karena sifatnya yang menyamar tetapi berbahaya. Pada tahun 2000-an, perkembangan *malware* ini pesat karena banyak bisnis yang menggunakan teknologi dan komputer. Zeus Trojan atau Zbot, misalnya, menyebabkan kerugian besar pada tahun 2009 dengan mencuri data perbankan seperti rekening bank online dan data kartu kredit di seluruh dunia.

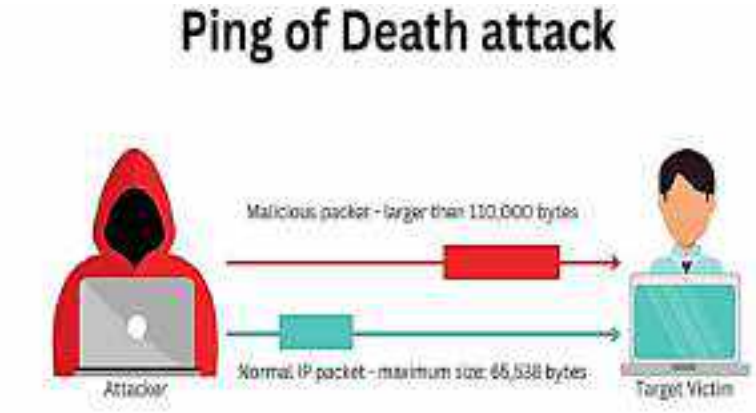
Gambar 1. 4 *Zeus Trojan*
Sumber : forum null-byte.wonderhowto (2015)

d. *Spyware* adalah perangkat lunak berbahaya yang bertujuan memata-matai atau mengawasi aktivitas pengguna di komputer maupun perangkat *mobile*. Tingkatannya dapat bervariasi, mulai dari yang berguna hingga yang berbahaya, seperti penggunaan *cookies* untuk menyimpan riwayat atau pencurian data privasi (Ames, 2004). Pada tahun 2000-an, *spyware* mulai muncul dan awalnya dikategorikan sebagai *adware* atau *trackware*

karena melacak perilaku *online* pengguna. Namun, pada tahun 2001, *spyware* yang sebenarnya muncul, sebagai bentuk aplikasi untuk membantu orang tua melindungi anak-anak di internet, tetapi sebenarnya mengumpulkan data pribadi pengguna. Contohnya adalah kasus Superfish pada tahun 2010, *malware* yang terpasang pada laptop Lenovo untuk menyisipkan iklan dalam penelusuran web. Selain itu, Superfish juga menimbulkan kelemahan SSL yang mengakibatkan kerentanan pada serangan komputer pengguna.

Gambar 1. 5 Superfish Spyware
Sumber : Stelian Pilici (2014)

e. DoS (*Denial of Service*) dan DDoS (*Distributed Denial of Service*) adalah serangan yang bertujuan mengganggu kinerja suatu sistem, baik dari segi layanan maupun sumber daya, sehingga tidak dapat bekerja sebagaimana mestinya. Perbedaannya terletak pada cara penyerangan, di mana DoS menggunakan satu komputer atau perangkat, sedangkan DDoS menggunakan banyak perangkat yang terorganisir. DoS ada sejak tahun 1990-an, dan hingga tahun 2000-an, muncul serangan DoS yang lebih merugikan seperti *Ping of Death*.



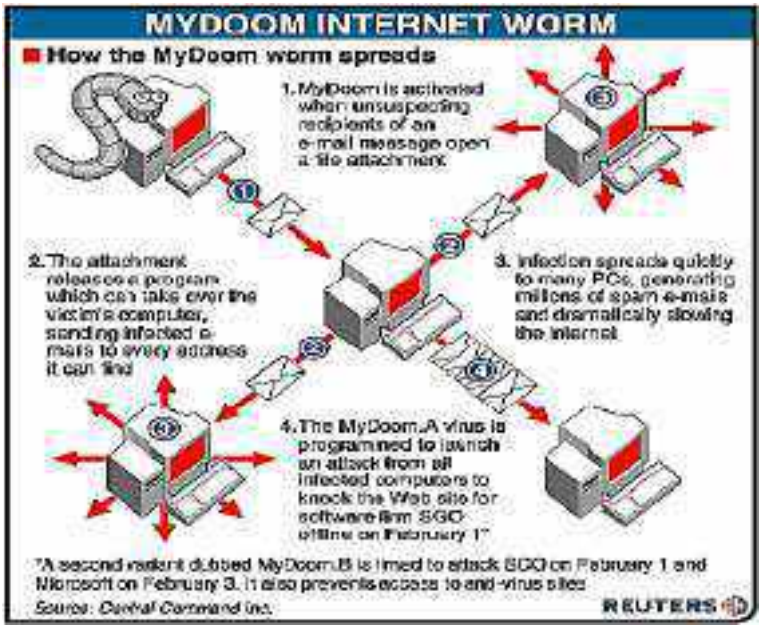
Gambar 1. 6 *Ping of Death*
Sumber : Vasilena Markova (2023)

f. *Spam* adalah pesan atau komunikasi tidak diharapkan yang terutama terkirim melalui email atau perangkat untuk berkomunikasi, yang mengandung iklan, tautan yang berbahaya, atau pesan promosi. Awalnya muncul pada tahun 1990-an, *spam* berisi berbagai penipuan seperti "Make money fast". Saat ini, *spam* telah berkembang melalui *platform* seperti Facebook, Instagram, Whatsapp dll. Meskipun ada perlindungan hukum, kesadaran pengguna tetap penting untuk menghindari masalah yang tidak diinginkan.

Gambar 1. 7 Contoh *Spam*
Sumber : Natalie Polly (2023)

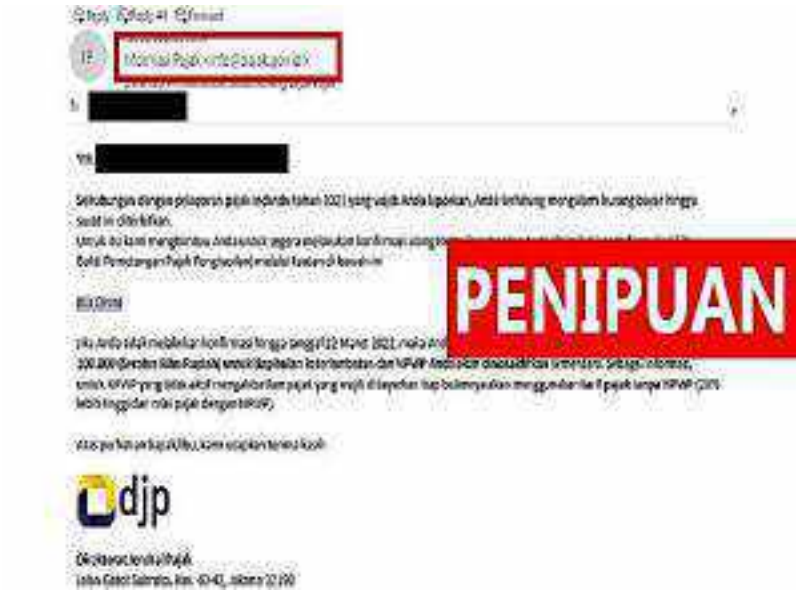
g. *Botnets*, atau jaringan bot, adalah jaringan komputer yang terdiri dari sejumlah besar perangkat yang dikendalikan oleh penyerang atau pembuat *botnets*. *Botnets* dapat digunakan untuk menjalankan aksi penyerangan melalui program atau perintah yang telah dibuat, menggunakan *Internet Relay Chat* (IRC) atau melalui server HTTP. Meskipun sejarah *botnets* kurang pasti, perkiraan munculnya pada tahun 2000-an seiring dengan

perkembangan DDoS. Contoh penggunaan *botnets* adalah kasus Mydoom pada tahun 2004 yang menyebar melalui email dan internet, digunakan untuk mengirim spam dan melancarkan serangan DDoS.



Gambar 1. 8 Mekanisme Mydoom Internet worm
Sumber : chinadaily (2004)

h. *Phishing* adalah jenis kejahatan siber yang bertujuan mendapatkan keuntungan dengan cara menipu, seperti mendapatkan nomor kartu kredit, identitas korban, atau kata sandi. Penyerang menggunakan berbagai cara, seperti menyamar sebagai pihak terpercaya, teman, atau memberikan penawaran menarik. *Phishing* telah ada sejak munculnya internet, dan penyebarannya semakin canggih menyebabkan banyak korban. Kesadaran pengguna untuk berhati-hati terhadap pesan dan situs web yang terlihat terpercaya menjadi upaya mitigasi yang efektif dalam menghadapi *phishing*. Contohnya adalah pesan dari gambar dibawah alamat website yang benar adalah *pajak.go.id* bukan *pajak.gov.id*.



Gambar 1. 9 Contoh *Phising*
Sumber : Redaksi DDTCNews (2023)

i. *Crypto Jacking* adalah praktik menggunakan komputasi milik korban untuk menambang *cryptocurrency* bagi penyerang. Penyerang menggunakan skrip pemrograman atau *malware* untuk menginfeksi perangkat target, yang kemudian mulai menambang *cryptocurrency* tanpa sepengetahuan atau izin pemiliknya ketika perangkat mengakses situs yang telah terinfeksi. Pada tahun 2017, situs web torrent terkenal "The Pirate Bay" diketahui melakukan *crypto jacking* pada komputer pengunjungnya tanpa izin, yang menuai kontroversi dan memicu penghapusan *script* tersebut setelah kontroversi tersebut mencuat.

Gambar 1. 10 Situs The Pirate Bay
Sumber : Andy Peterson (2021)

j. *SQL injection* adalah serangan di mana input data pengguna disisipkan ke dalam *SQL query* yang telah dimodifikasi oleh penyerang, yang kemudian dieksekusi oleh sistem sebagai kode SQL. Serangan ini dapat mengakibatkan modifikasi, penghapusan, atau kerusakan data dalam database. Input data yang berpotensi disisipkan dapat berupa formulir, URL, atau input lainnya. Pada awal perkembangan aplikasi web pada tahun 2000-an, serangan *SQL injection* menjadi umum karena adanya celah keamanan yang belum tertutup. Salah satu contoh kasus terkenal adalah serangan *SQL injection* pada Sony Pictures pada tahun 2014, yang menyebabkan kebocoran data sensitif seperti email pegawai dan informasi pengguna. Insiden ini merusak reputasi Sony Pictures karena kegagalan mereka dalam menjaga keamanan data pengguna dan karyawan.

Gambar 1. 11 SQL injection pada Sony Pictures pada Tahun 2014

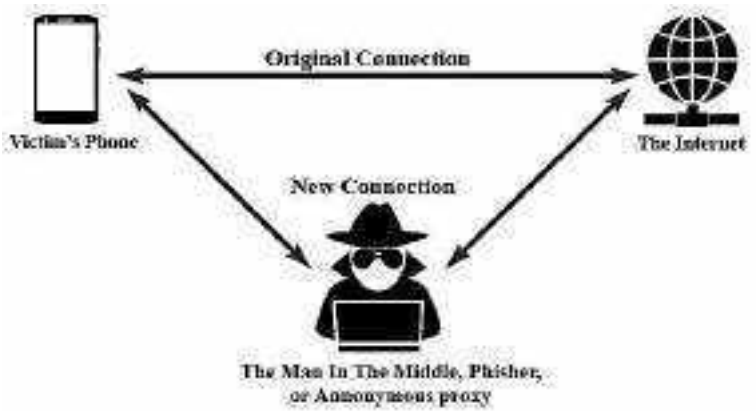
Sumber : Dancho Danchev (2008)

k. *Ransomware* adalah jenis *malware* yang dirancang untuk mengunci atau mengenkripsi data pada komputer atau perangkat korban, kemudian meminta tebusan agar korban dapat mendapatkan kembali akses ke data mereka. Penyerang biasanya meminta pembayaran tebusan dalam bentuk *cryptocurrency* seperti Bitcoin, dan mengancam untuk menghapus data yang terenkripsi jika tebusan tidak dibayar. Ransomware pertama kali dikenal sebagai "PC Cyborg" pada tahun 1989, yang mengenkripsi file pada sistem korban dan meminta pembayaran sebesar $189. Salah satu insiden *ransomware* yang paling terkenal adalah CryptoLocker pada tahun 2013, yang menggunakan enkripsi RSA yang kuat dan menyebar melalui lampiran email, meminta tebusan dalam bentuk Bitcoin.

Gambar 1. 12 Tampilan terkena CryptoLocker
Sumber : William Baptist (2023)

l. *Man in the Middle* (MITM) adalah serangan siber di mana penyerang mencoba untuk mencuri atau memanipulasi komunikasi antara dua pihak tanpa sepengetahuan mereka. Serangan ini dapat terjadi dalam berbagai situasi,

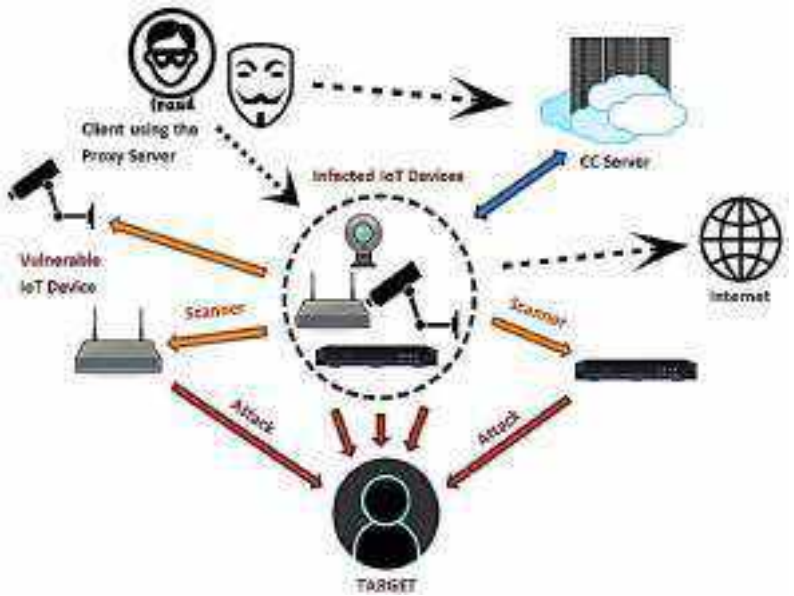
seperti ketika pengguna mengakses situs tanpa protokol HTTPS, menggunakan jaringan Wi-Fi publik, atau melakukan panggilan telepon. MITM sudah ada sejak lama, mulai dari penyadapan langsung hingga penggunaan jaringan untuk mengakses informasi rahasia. Saat ini, serangan MITM telah berkembang menjadi lebih canggih dan mengikuti perkembangan teknologi. Contoh serangan MITM yang terkenal adalah *SSL strip attack*, di mana peretas memanfaatkan permintaan pengguna ke server dengan menyusup di tengah-tengah sebelum mencapai tujuan akhirnya.



Gambar 1. 13 Cara kerja man in the middle SSLstrip attack
Sumber : Milad et al (2018)

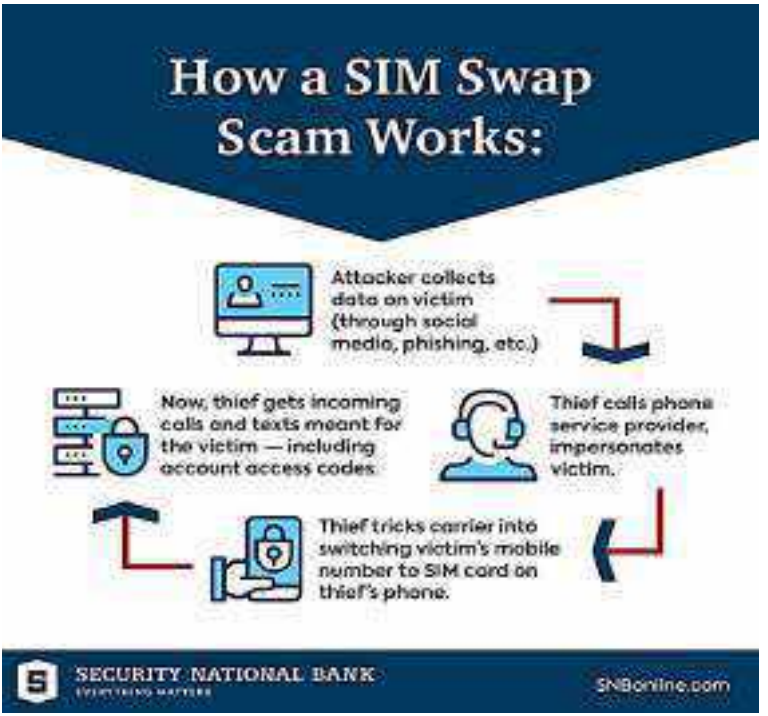
m. Eksploitasi IoT (*Internet of Things*) adalah pengeksplorasi kerentanan pada perangkat IoT untuk mengakses, mengendalikan, atau melakukan tindakan jahat. Meskipun alat-alat IoT membantu kehidupan sehari-hari, mereka juga rentan terhadap serangan. Penyerang dapat menembus keamanan perangkat dan masuk ke jaringan, seperti kasus peretasan CCTV yang memantau aktivitas. Contoh terkenal eksploitasi IoT adalah Mirai-based bot, di mana penyerang menggunakan malware Mirai untuk meretas perangkat IoT seperti kamera keamanan dan

router, lalu menggunakannya untuk melakukan serangan DDoS.



Gambar 1. 14 Mekanisme *Mirai-based Bot*
Sumber : Do Son (2018)

n. *Social Engineering* adalah teknik manipulasi yang digunakan untuk memanipulasi individu atau entitas agar mengungkapkan informasi rahasia, melakukan tindakan tertentu, atau memberikan akses yang tidak sah. Penyerang dapat memanfaatkan informasi ini untuk kepentingan pribadi, seperti menjual data di pasar gelap atau *dark web*. Salah satu contoh praktik ini adalah sim *swapping*, di mana penyerang menggunakan teknik ini untuk mengalihkan nomor ponsel korban ke kartu SIM yang mereka kendalikan, dengan tujuan mengakses akun online yang terkait dengan nomor ponsel tersebut.

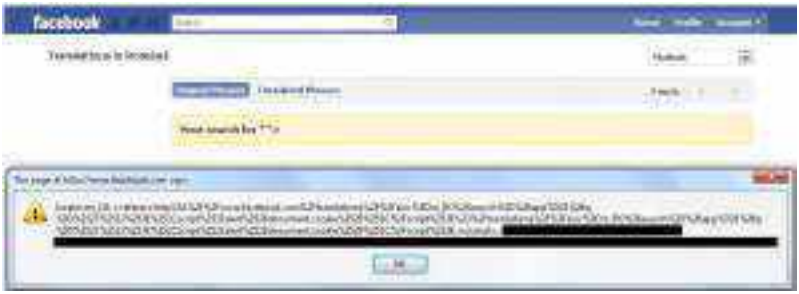


Gambar 1. 15 Cara kerja SIM swapping
Sumber : Security National Bank (2021)

o. *Adware* (*Advertising-supported software*) adalah *software* yang menampilkan iklan kepada pengguna dengan tujuan memperoleh profit bagi penciptanya. Meskipun tidak semua *adware* berbahaya, beberapa dirancang dengan iklan yang mengganggu dan berpotensi membahayakan pengguna. Contoh kasus Vonteera adware pada tahun 2016 menunjukkan penggunaan *adware* yang merugikan, karena menampilkan iklan secara berlebihan dalam setiap aktivitas *online* pengguna dan dapat menyisipkan *malware* yang berisiko bagi pengguna.

Gambar 1. 16 Pendeteksian malware Vonteera
Sumber : Pieter Arntz (2015)

p. *Cross Site Scripting* (XSS) adalah kerentanan keamanan pada perangkat lunak dan aplikasi *web* yang memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman web. Serangan XSS terjadi ketika aplikasi web tidak menyaring input pengguna dengan benar, sehingga skrip tersebut dieksekusi oleh peramban pengguna. Tujuan dari serangan XSS bervariasi, tetapi dapat mencakup pencurian data pengguna, pemalsuan identitas, dan kejahatan lainnya. Kasus XSS pada Facebook merupakan salah satu contoh serangan XSS terbesar, di mana skrip tersebut disisipkan pada bagian login dan komentar di postingan pengguna.



Gambar 1. 17 Deteksi kerentanan XSS Facebook
Sumber : Neal Poole (2011)

q. *Password Cracking* adalah upaya untuk mengungkap atau mendekripsi kata sandi yang telah dienkripsi atau di-*hash*. Ini merupakan aktivitas yang sering dilakukan oleh penyerang yang mencoba mendapatkan akses ilegal ke akun, sistem, atau data yang dilindungi oleh kata sandi. Dengan berhasil mendapatkan kata sandi, penyerang dapat menggunakan identitas tersebut untuk mencapai keuntungan yang diinginkan. Contohnya adalah kasus pencurian data pengguna Adobe pada tahun 2013, di mana kata sandi yang di-*hash* dan data sensitif lainnya dicuri oleh penyerang, meningkatkan risiko akses ilegal ke akun dan sistem yang terpengaruh.

Gambar 1. 18 Kerentanan panjang *password*
Sumber : Hive Systems (2023)

r. *Cross-Site Request Forgery* (CSRF) adalah serangan keamanan web di mana penyerang memanipulasi pengguna agar melakukan tindakan yang tidak disengaja pada situs web atau aplikasi web yang telah mereka autentikasi. Serangan ini terjadi ketika pengguna yang terpengaruh secara tidak sadar mengirim permintaan HTTP palsu, yang dieksekusi di dalam sesi otentikasi yang valid. Penyerang memanfaatkan ini untuk mengubah data, mengganti kata sandi, atau bahkan melakukan transaksi finansial atas nama pengguna yang terpengaruh tanpa izin mereka.

Gambar 1. 19 Cara kerja sederhana CSRF
Sumber : Islem Othmani (2024)

s. Serangan fisik dan bencana, melibatkan segala tindakan fisik yang dapat mengakibatkan kerugian pada sisi teknologi seperti pencurian, banjir, kebakaran, perusakan secara sengaja, dan hal-hal fisik lainnya. Hal ini membuat selain keamanan dalam layanan, keamanan di dunia nyata perlu diperhatikan.

5. Kasus kejahatan siber terkenal

Keamanan siber tidak bisa diperkirakan saat terjadinya namun harus selalu siap akan segala macam ancaman dengan melakukan berbagai pencegahan merupakan hal yang masuk akal. Dengan meningkatnya ketergantungan pengguna terhadap teknologi, penjahat siber semakin canggih dan berani dalam melancarkan serangan terhadap individu, organisasi atau bahkan pemerintah. Tidak semua hal akan berjalan baik-baik saja seperti kasus - kasus cyber crime yang pernah terjadi berikut :

a. WannaCry *Ransomware Cyber Attack* pada tahun 2017

Kasus kejahatan Siber paling terkenal dan merugikan pada tahun 2017 adalah WannaCry. Ini menyebar melalui eksploitasi *vulnerabilities* pada sistem operasi Windows yang masih versi lama, menggunakan kerentanan bernama "EternalBlue" yang awalnya dibuat oleh NSA dan bocor oleh kelompok peretas bernama Shadow Brokers. WannaCry mengenkripsi data pengguna, meminta tebusan dalam bentuk kripto untuk mengembalikan akses. Kasus ini mempengaruhi jaringan

dan sistem komputer global, termasuk di Indonesia, menyerang rumah sakit, lembaga pemerintahan, perusahaan, dan individu. Beberapa rumah sakit di Inggris bahkan harus menunda operasi karena data terenkripsi. Microsoft merilis pembaruan keamanan darurat untuk sistem operasi Windows yang rentan sebagai respons atas serangan ini.

Gambar 1. 20 Tampilan Ketika Terkena WannaCry
Sumber : Lely Maulida (2017)

b. Bocornya data *e-commerce* terkemuka di Indonesia dan dijual ke situs gelap.

Pada tahun 2019, terjadi peretasan pada sebuah *e-commerce* terkemuka di Indonesia, dimana sebanyak 91 juta data dilaporkan bocor karena peretas dengan nama akun "whysodank." Peretas ini bekerja sama dengan teman-temannya karena mengalami kesulitan dalam memecahkan enkripsi data. Pada bulan Maret 2020, peretas memutuskan untuk menjual data pengguna tersebut, yang mencakup nama, password yang masih

terenkripsi, email, nomor telepon, dan lain-lain, ke situs gelap (*dark web*) yang bernama Empire Market. Mereka mengklaim berhasil menjual 91 juta data akun pengguna seharga US$5.000 atau sekitar 75 juta rupiah. Meskipun pihak *e-commerce* mengklaim bahwa tidak ada informasi sensitif seperti riwayat pembayaran, kartu kredit, atau rekening yang dibocorkan, serta *password* yang dicuri masih terenkripsi, mereka tetap menghimbau semua pengguna untuk mengganti kata sandi mereka dan menggunakan fitur kode OTP (*one-time password*).

Gambar 1. 21 Akun hacker yang Meretas dan Menjual Data Milik Salah Satu E-Commerce
Sumber : CNN Indonesia (2020)

c. RockYou2021 dan kebocoran 8,4 miliar kata sandi

RockYou2021 merupakan sebuah kasus bocornya data yang melibatkan lebih dari 8.4 miliar kata sandi pada bulan Juni 2021. Insiden ini disebabkan oleh sejumlah kompilasi insiden yang akhirnya berujung pada kebocoran kata sandi tersebut. Salah satu faktor utama adalah pelanggaran data terdahulu (*data breach*), dimana kata sandi tersebut awalnya telah bocor dari layanan online atau perusahaan yang mengalami pelanggaran data sebelumnya. Lemahnya kata sandi dan metode

enkripsi yang sederhana juga memudahkan peretas untuk membocorkan kata sandi tersebut. Kejadian ini membuka kemungkinan bagi pihak jahat untuk meretas atau mengambil alih akun pengguna untuk kegiatan seperti pencurian data, pencurian identitas, dan pemerasan.

Setelah insiden ini, layanan online dan perusahaan menjadi lebih berhati-hati dalam mengamankan kata sandi pengguna dan menerapkan verifikasi dua faktor (2FA) atau autentikasi ganda untuk meningkatkan keamanan akun. Pengguna juga diingatkan untuk secara rutin memeriksa keamanan kata sandi mereka dan mengambil langkah-langkah keamanan yang diperlukan guna melindungi akun mereka.

Gambar 1. 22 Meledaknya Kasus RockYou2021 di Internet
Sumber : Josh Frank (2021)

d. Kejahatan Bjorka pada tahun 2022

Bjorka, peretas dengan profil penyanyi, melakukan serangkaian aksi peretasan terhadap data perusahaan dan pemerintah Indonesia pada 2022. Dengan motif kepentingan pribadi dan 'keadilan', ia mengklaim

bertanggung jawab atas serangkaian insiden peretasan, termasuk data sensitif seperti data pelanggan provider internet terbesar, data registrasi SIM Card, data KPU (Komisi Pemilihan Umum), dan dokumen rahasia negara. Bjorka tidak hanya menjual data tersebut di situs gelap, media sosial, dan aplikasi *chatting*, tetapi juga melakukan *doxing* dengan menyebarkan informasi pribadi pihak lain. Meskipun belum tertangkap, aktivitasnya telah berhenti.

Gambar 1. 23 Salah Satu Akun Media Sosial Bjorka
Sumber : Faiz Iqbal Maulid (2022)

D. Framework dalam Mengatur, Mengelola, Menjaga dan Memelihara Keamanan Sistem Informasi

Dalam menjaga keamanan sistem informasi, dunia berlomba-lomba dalam menciptakan regulasi dan kerangka kerja (*framework*) yang baik dengan tujuan mengidentifikasi, mengelola, dan mengurangi risiko yang terkait dengan kerentanan dan ancaman terhadap informasi penting organisasi. Kerangka kerja manajemen keamanan informasi adalah seperangkat prinsip, proses, pedoman dan praktik yang dapat digunakan oleh organisasi untuk merencanakan, mengimplementasi, mengoperasikan, mengawasi dan memperbaiki sistem dengan tujuan melindungi keamanan informasi mereka. ISO/IEC 27001, NIST Cybersecurity Framework, COBIT, OWASP dan ITIL merupakan sedikit dari

banyaknya kerangka kerja mengenai manajemen keamanan sistem informasi. Berikut perbandingannya :

1. ISO/IEC 27001 (*International Organization for Standardization / International Electrotechnical Commision*). ISO / IEC 27001 adalah standar yang diakui secara internasional yang mengatur dan menjelaskan bagaimana untuk mengelola keamanan sistem informasi dalam suatu organisasi (Kurii & Opirskyy, 2013). *Framework* ini dapat diimplementasikan pada berbagai jenis organisasi baik *profit, non-profit, private*, besar, kecil atau milik negara. Dari segi kompleksitas, dapat dikatakan relatif tergantung dari pedoman mana yang ingin di ikuti, dengan lebih menekan pada pendekatan berbasis risiko dalam mengelola keamanannya. Keunggulan dari *framework* ini terdapat pada informasi keamanan standar yang menjelaskan bagaimana mengimplementasikan *Information Security Management System* (ISMS)
2. NIST 800-53 (*National Institute for Standards and Technology*) *Cybersecurity Framework*. NIST Cybersecurity Framework adalah kerangka kerja yang berisi mengenai kontrol keamanan dan privasi untuk perlindungan sistem informasi dan organisasi guna melindungi pengoperasian dan aset-aset organisasi dengan tujuan mengelola risiko dengan efisien. Diciptakan terutama untuk membantu lembaga federal Amerika Serikat, dan berkembang untuk segala macam sistem informasi yang membutuhkan baik untuk organisasi, personal maupun pemerintahan. Keunggulan dari NIST yaitu sebagai pedoman opsional, bahan praktik terbaik, dan standar untuk menerapkan serta meningkatkan program keamanan siber.
3. COBIT (*Control Objectives for Information and Related Technology*). COBIT adalah kerangka kerja tata kelola teknologi informasi (TI) yang digunakan untuk membantu organisasi mencapai tujuan bisnisnya melalui penggunaan TI. COBIT menyediakan kerangka kerja yang komprehensif untuk mengelola TI, termasuk proses, struktur, dan orang. Ditujukan untuk semua organisasi yang menggunakan TI,

baik itu organisasi bisnis, organisasi pemerintah, atau organisasi nirlaba. COBIT dapat digunakan oleh organisasi dari berbagai ukuran dan industri. Kelebihannya terdapat pada tata kelola TI yang komprehensif, fleksibel, dan teruji. COBIT dapat membantu organisasi meningkatkan efisiensi dan efektivitas penggunaan TI, mengurangi risiko TI, meningkatkan kepatuhan terhadap peraturan, dan meningkatkan nilai bisnis dari TI.

4. OWASP 2021 (*Open Web Application Security Project*). OWASP bukanlah sepenuhnya *framework* melainkan nama perusahaan nirlaba yang berfokus untuk meningkatkan keamanan aplikasi *web* dengan pendekatan mulai dari proyek, penelitian, alat-alat dan sumber daya lainnya yang dapat membantu pengembangan dan keamanan terutama dalam keamanan aplikasi *web*. OWASP ditujukan untuk organisasi, pemerintah, individu, *developers* dan lain - lain selama menggunakan aplikasi *web*. Kelebihannya yaitu sangat mutakhir untuk keamanan dan pengembangan *web* karena membantu dari segi pengetahuan, proyek, *tools*, dan komunitas.
5. ITIL (*Information Technology Infrastructure Library*). Merupakan *framework* manajemen layanan TI (*IT service management*) yang digunakan untuk membantu organisasi mengelola dan memberikan layanan TI yang berkualitas tinggi. ITIL menyediakan kumpulan praktik terbaik yang dapat disesuaikan untuk memenuhi kebutuhan organisasi yang berbeda. Sasaran dari ITIL tertuju untuk semua organisasi yang menggunakan TI, baik itu organisasi bisnis, organisasi pemerintah, atau organisasi nirlaba. ITIL dapat digunakan oleh organisasi dari berbagai ukuran dan industri. ITIL memiliki tingkat kompleksitas yang bervariasi. ITIL dapat digunakan dalam bentuk yang sederhana atau dapat disesuaikan untuk memenuhi kebutuhan organisasi yang lebih kompleks. ITIL dapat membantu organisasi meningkatkan efisiensi, efektivitas, kepuasan pelanggan, dan nilai bisnis dari TI.

Pilihan antara *frameworks* yang digunakan tergantung pada kebutuhan dan tujuan organisasi. Secara lebih rinci informasi mengenai *frameworks* diatas dapat dilihat pada bagian Penilaian Risiko dan Manajemen Keamanan dan Keamanan aplikasi web. Banyak organisasi memilih untuk menggabungkan elemen-elemen dari kedua kerangka kerja ini untuk mencapai tingkat keamanan informasi yang optimal sesuai dengan konteks dan lingkungan mereka. Berikut tabel yang menjelaskan kapan *framework* tersebut bagus atau tepat digunakan :

Tabel 1. 1 Perbandingan Kapan penggunaan frameworks

Framework	**Fokus**	**Tujuan**	**Kapan digunakan**
ISO 270001	Keamanan informasi	Manajemen resiko	Organisasi dari semua ukuran dan industri yang ingin memenuhi persyaratan keamanan informasi yang ditetapkan oleh standar ISO 27001
NIST	Keamanan siber	Peningkatan keamanan siber	Organisasi dari semua ukuran dan industri yang ingin meningkatkan keamanan siber mereka
COBIT	Tata kelola TI	Manajemen TI yang efektif dan efisien	Organisasi dari semua ukuran dan industri yang ingin mengelola TI

Framework	Fokus	Tujuan	Kapan digunakan
			mereka secara efektif dan efisien
OWASP 10	Keamanan aplikasi web	Peningkatan keamanan aplikasi web	Organisasi yang mengembangkan atau menggunakan aplikasi web
ITIL	Manajemen layanan TI	Manajemen dan pemberian layanan TI yang berkualitas tinggi	Organisasi dari semua ukuran dan industri yang ingin mengelola dan memberikan layanan TI yang berkualitas tinggi

E. Peran dan Tanggung Jawab Seorang Cyber Security

Seorang *cyber security* adalah seorang profesional keamanan siber yang memiliki tanggung jawab untuk melindungi sistem komputer, jaringan, dan data dari ancaman siber. Dengan bantuan *cyber security*, organisasi biasanya mengembangkan kebijakan dan prosedur keamanan yang mengatur bagaimana informasi sensitif harus ditangani, disimpan, dan dibagikan. Selain itu, pelatihan keamanan siber diberikan juga kepada karyawan untuk meningkatkan pemahaman mereka tentang pentingnya kerahasiaan dan tindakan yang harus diambil untuk melindunginya. Tiga hal yang dapat dilakukan untuk membantu menjaga keamanan selain dari pihak *cyber security* yaitu pendidikan, pelatihan dan kesadaran (*security education, training and awareness* atau disingkat SETA) terhadap karyawan pada suatu organisasi (Amin et al., 2014).

1. Pendidikan. Pendidikan keamanan memberikan pengetahuan tentang konsep dasar, teknik serangan, dan strategi pertahanan siber melalui pelatihan formal, kursus, dan sertifikasi kepada personel organisasi.
2. Pelatihan. Pelatihan keamanan melibatkan latihan praktis untuk membantu personel menghadapi ancaman keamanan siber sehari-hari.
3. Kesadaran. Kesadaran keamanan melibatkan sosialisasi, pelatihan umum, dan informasi yang menyeluruh tentang ancaman keamanan siber, bertujuan untuk meningkatkan kesadaran personel dan peran mereka dalam melindungi organisasi.

Ada berbagai macam ahli keamanan siber (*specialist cyber security*) yang menekuni dan profesional terhadap bidang yang mereka pilih terkait keamanan siber. Berikut beberapa jenis ahli keamanan siber :

1. *Machine Learning Engineer*, ahli keamanan yang bertugas mendesain, membuat dan mengimplementasikan algoritma-algoritma kecerdasan buatan untuk membantu dalam melindungi dan menjaga keamanan.
2. *Security Analyst*, profesional yang bertugas untuk memantau keamanan perusahaan atau organisasi dan potensi pelanggarannya.
3. *Digital Forensic Expert*, bertugas untuk menyelidiki insiden keamanan siber dan mengumpulkan bukti-bukti elektronik untuk membantu menemukan pelaku kejahatan serta menciptakan laporan yang dapat dipakai dalam persidangan.
4. *Network Security Analyst*, ahli keamanan siber yang bertugas untuk monitoring, menjaga, dan melindungi keamanan dari sisi jaringan.
5. *Security System Administrator*, merupakan ahli yang bertanggung jawab dalam memastikan keamanan perangkat lunak dan keras yang digunakan.
6. *Application Security Development*, bertugas dalam memastikan perangkat lunak yang dikembangkan memiliki keamanan yang baik.

7. *Information Security Manager*, merupakan pemimpin keamanan suatu organisasi yang mengelola dan mengatur keamanan informasi, termasuk kebijakan prosedur dan kepatuhan hukum.
8. *Cloud Security Specialist*, ahli yang berfokus pada keamanan data dan aplikasi yang ada pada lingkungan cloud computing.
9. IoT (*Internet of Things*) *Security Specialist*, ahli yang bertugas untuk melindungi perangkat IoT baik seperti kamera keamanan, perangkat smart home dan lain-lain.
10. *Security Consultant*, merupakan penasihat keamanan untuk membantu organisasi meningkatkan keamanannya.
11. *Social Engineering Security Specialist*, ahli yang bertugas mulai dari melindungi, menjaga hingga memberikan pengetahuan kepada organisasi mengenai serangan social engineering agar tidak terserang atau tertipu.

Sebagai seorang profesional *cyber security*, peran dan tanggung jawab meliputi identifikasi risiko keamanan, merancang strategi perlindungan, merespons cepat terhadap ancaman, menjaga integritas data, meningkatkan kesadaran keamanan, dan memastikan kolaborasi untuk menghadapi risiko *cyber* secara efektif, mirip dengan respons terhadap bencana untuk mencegah kerugian lebih lanjut.