New Normal dan Entrepreneur bidang Keamanan Siber

Sugiyatno[1],
Universitas Bhayangkara Jakarta Raya, Jl. Perjuangan, Bekasi Utara, Kota Bekasi
sugiyatno@dsn.ubharajaya.ac.id

ABSTRAK

Krisis yang dihadapi para pelaku bisnis akibat pandemi Covid-19 saat ini adalah sesuatu yang luar biasa dan dialami oleh hampir semua perusahaan. Namun, harus disadari pandemi Covid-19 ini bukan kejadian terakhir yang akan men-*disrupsi* kehidupan. Ketika ada problem, di situ pasti ada peluang atau *opportunity*. Keadaaan ini berdampak pada kebutuhan akan konsultan IT yang semakin besar dari sebelumnya. Dengan menjadi konsultan IT/Enterpreneur IT, dapat membantu perusahaan mengevaluasi sistem keamanan dan menawarkan saran tentang bagaimana mereka dapat melindungi diri dari peretas dengan lebih baik. Selain itu, konsultan IT atau *cybersecurity* dapat membantu menyiapkan perangkat keras suatu perusahaan atau bisnis dan memecahkan masalah umum tentang teknologi dan keamanan siber. Menjadi konsultan IT/ Enterpreneur IT bidang *cybersecurity*, yaitu peluang bisnis di bidang ini masih terbuka lebar. Jika Anda memiliki *skill cybersecurity*, Anda juga bisa meningkatkan jenjang karier bisnis ke arah yang lebih menjanjikan, seperti *penetration tester, white hat hacker*, *computer forensic specialist*, dan masih banyak lagi.

Kata Kunci : Covid-19, *cybersecurity, white hat hacker*, *computer forensic specialist*

ABSTRACT

The crisis faced by business people due to the current Covid-19 pandemic is something extraordinary and experienced by almost all companies. However, it must be realized that the Covid-19 pandemic is not the last event that will disrupt life. When there is a problem, there must be an opportunity. This situation has an impact on the need for IT consultants which is greater than ever. Becoming an IT consultant/IT Entrepreneur can help companies evaluate security systems and offer advice on how they can better protect themselves from hackers. In addition, an IT or cybersecurity consultant can help set up a company or business hardware and solve common technology and cybersecurity issues. Become an IT consultant/IT entrepreneur in cybersecurity, that is, business opportunities in this field are still wide open. If you have cybersecurity skills, you can also advance your business career to a more promising direction, such as penetration tester, white hat hacker, computer forensic specialist, and many more.

Keywords: *Covid-19, cybersecurity*

Pendahuluan

Penjahat cyber tidak pernah memperhitungkan waktu saat akan bertindak. Ketika mereka mendeteksi kerentanan di sistem perusahaan sesegera mungkin mereka mengeksploitasinya. Oleh karea itu, perusahaan harus terus memperkuat pertahanan mereka untuk menjaga keamanan data perusahaan dan pelanggannya,

Beberapa tantangan perusahaan saat pandemi covid dan sistem kerja dengan model WFH (*Work From Home*) ini seperti ; menyediakan sistem yang beroperasi 24 kali 7 hari, bagaimana mendidik sumber daya manusia agar bekerja sesuai dengan standar keamanan, dan mengelola resiko yang dihadapi karena sistem yang sebelumnya *offlin*e menuju sistem online, perkembangan software tools keamanan dan peretas dalam skala besar dan komplek.

Dengan beberapa tantangan diatas, perusahaan perlu meningkatkan kualitas sistem yang telah diimplementasi dengan mengembangkan seperti; *Authentication Fast ID Online (FIDO), Bimetric, Face Recognition,* atau kerjasama dengan konsultan IT bidang security untuk menguji sistem secara berkala (*Pentesting*).

Aktivitas diatas dilakukan untuk mengatasi terjadinya kebocoran data (*data leakage*). Kebocoran data (data leakage) adalah suatu kondisi dimana data sensitif secara tidak sengaja terexpose atau terakses oleh pihak tidak sah. Ancaman ini dapat terjadi melalui situs website, email, hard drive, atau pun laptop.

Berikut ini beberapa kasus

Tabel 1. Kasus kebocoran data

No	Tahun	Nama Institusi	Keterangan
1	2021	BPJS Kesehatan	Data yang diklaim milik 279 juta penduduk Indonesia bocor dan dijual di sebuah forum online bernama Raid Forums. Ratusan juta data tersebut dijual oleh seorang anggota forum dengan akun "Kotz".
2	Mei 2020	Tokopedia	Sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (dark web). Data pengguna Tokopedia yang dijual mencakup gender, lokasi, username, nama lengkap pengguna, alamat e-mail, nomor ponsel, dan password.
3	Mei 2020	Daftar Pemilih Tetap (DPT) Pemilu 2014	Jutaan data kependudukan milik warga Indonesia diduga bocor dan dibagikan lewat forum komunitas hacker. Data tersebut diklaim merupakan data Daftar Pemilih Tetap (DPT) Pemilu 2014. Temuan dugaan kebocoran data pemilih tetap KPU ini pertama kali diungkap oleh akun Twitter @underthebreach
4	Agustus 2020	KreditPlus	Kebocoran data pengguna KreditPlus dipaparkan dalam laporan dari firma keamanan siber asal Amerika Serikat, Cyble. Berdasarkan laporan tersebut, data pribadi milik sekitar 890.000 nasabah Kreditplus diduga bocor. Data ratusan ribu pengguna tersebut konon dijual di forum terbuka yang biasanya digunakan sebagai kanal untuk pertukaran database hasil peretasan, Raidforums. Adapun database ini menghimpun sejumlah data pribadi pengguna yang terbilang cukup sensitif, di antaranya seperti nama, alamat e-mail, kata sandi (password), alamat rumah, nomor telepon, data pekerjaan dan perusahaan, serta data kartu keluarga (KK)

5	September 2020	ShopBack	Kasus kebocoran data yang menimpa platform cashback rewards serta kurator e-commerce asal Singapura, ShopBack terjadi pada September 2020 lalu. Dalam keterangan resmi yang dibagikan ShopBack lewat e-mail kepada seluruh penggunanya, disebutkan bahwa ShopBack mengaku menemukan adanya akses ilegal ke sistem yang memuat data pengguna
6	November 2020	RedDoorz	Adanya 5,8 juta data pengguna RedDoorz yang dijual seharga 2.000 dollar AS atau sekitar Rp 28,2 juta rupiah pada November 2020 lalu. Data tersebut dijual di situs Raid Forum yang bisa diakses secara terbuka. Data pengguna RedDoorz yang bocor mencakup nama, e-mail, password bcrypt, foto profil, gender, hingga nomor ponsel.
7	November 2020	Cermati	sekitar 2,9 juta data pengguna platform fintech asal Indonesia, Cermati, dikabarkan diretas dan dijual secara bebas. Data tersebut kabarnya dijual melalui forum hacker bersama 34 juta data dari 17 perusahaan lain. Pendiri komunitas Ethical Hacker Indonesia, Teguh Aprianto mengatakan bahwa, 2,9 juta data pengguna Cermati yang dijual bebas mencakup nama lengkap, NIK, NPWP, alamat, nomor telepon, rekening, nama ibu kandung pengguna, hingga pekerjaan.

Pembahasan

Terjadinya kebocoran data dapat menimbulkan kerugian dan reputasi yang cukup besar. Oleh karena itu, setiap perusahaan memerlukan solusi keamanan data yang mumpuni dan berpengalaman. Hal ini bertujuan untuk memberikan solusi penerapan teknologi yang tepat dengan perkembangan korporasi. Apalagi ditambah lagi dengan tren *work from home* (WFH) membawa dinamika baru dalam melakukan pengamanan dan tuntutan produktivitas kerja.

Dalam artikel ini akan dibahas tahapan dalam implementasi manajemen framework keamanan siber yaitu: **sebelum (pencegahan), saat kejadian dan sesudah kejadian** insiden keamanan siber [1].

1. Pencegahan keamanan siber

Untuk mencegah terjadinya insiden keamanan siber perusahaan perlu langkah-langkah sebagai berikut :

a. Perusahaan harus membuat kebijakan keamanan

Membuat pedoman seperti menegakkan peraturan bahwa karyawan tidak boleh meninggalkan komputer dalam keadaan logged on/unlocked, tidak memberi tahu akun dengan rekan kerja yang lain.

b. **Mengontrol konten dalam email**

Dalam mengirim informasi dan dokumen rahasia melalui email, sering terjadi kebocoran data melalui email. Untuk meminimalisir, perusahaan dapat menggunakan email content filtering. Email filter akan melakukan proses penyaringan lalu lintas email baik itu pesan masuk atau pesan keluar. Filter akan memindai pesan dan mengklasifikasikan pesan ke dalam kategori seperti spam, virus, penipuan, dan lain-lain. Teknologi ini juga dapat memperingatkan administrator tentang ancaman orang internal dan memberi tahu jika ada pengguna yang mencoba mengirim info sensitif ke luar perusahaan.

c. ***Endpoint protection***
Endpoint protection merupakan cara mengamankan *endpoint* pengguna atau *end user devices* seperti dekstop, laptop, perangkat mobile, dan lain-lain agar terlindungi dari eksploitasi tidak sah yang dilakukan oleh penjahat cyber. Untuk memproteksi endpoint dapat menggunakan software seperti *McAfee Endpoint Security, Sophos Endpoint Protection*, dan lain-ain. Sistem perlindungan *endpoint* tersebut dikembangkan untuk mendeteksi, menganalisis, memblokir, dan menahan serangan cyber. Peretas selalu ingin memiliki cara baru untuk mengakses sistem, mencuri informasi, serta memanipulasi karyawan agar mereka memberikan informasi sensitif, sehingga kita membutuhkan *endpoint protection*. Selain menggunakan endpoint protection software, juga menggunakan kata sandi yang kuat serta menggunakan *screen lock*.

d. **Menguji keamanan data**
Data leakage (kebocoran data) sering terjadi karena kelalaian user atau karena adanya kerentanan keamanan pada sistem yang digunakan. Untuk menghindari bocornya data dengan memastikan sistem yang digunakan memiliki keamanan yang baik dengan melakukan penetration testing secara rutin. Dengan penetration testing, kerentanan keamanan dapat segera ditemukan dan diperbaiki sehingga data dapat terlindungi. Kebocoran data merupakan musibah bagi bisnis dan merugikan serta membawa dampak buruk bagi citra perusahaan secara keseluruhan, terlebih jika ada data pengguna.
Contoh cara cegah kebocoran data pribadi.

1. Kurangi jumlah data yang kita bagi
   Ketika baru memasang aplikasi, yang meminta izin mengakses data dan layanan; seperti kamera, album **foto**, lokasi, dan kontak, ada tiga hal yang mesti kita pastikan, yakni:
   a. Apakah aplikasi itu perlu akses ke data agar berfungsi dengan baik?
   b. Apakah aplikasi itu hanya perlu akses untuk sementara atau selamanya?
   c. Apakah kita percaya kepada perusahaan aplikasi?

2. Blokir pelacakan aplikasi
   Aplikasi yang terus-menerus mengakses informasi dari perangkat, berupa model ponsel dan sistem operasinya; lalu membagikan data itu ke pihak ketiga. Sehingga, penjual mendapat informasi itu bisa menargetkan iklan di berbagai aplikasi. Untuk memblokir pengambilan data tak terlihat itu, gunakan pemblokir pelacak seperti Fyde, Privacy Pro, dan Disconnect Premium; tersedia di iOS dan Android.

3. Cari informasi soal aplikasi sebelum memasang
   Jika merupakan aplikasi gratis yang mengandalkan iklan, umumnya data pengguna termasuk dalam transaksi maka, aplikasi telah memiliki data Anda secara utuh, dan telah mereka jual ke banyak lain dan akan sulit untuk mengendalikannya kembali.

Selain beberapa metode diatas, untuk perusahaan yang menangani jutaan data pengguna dan teknologi besar perlu menyiapkan Langkah-langkah sebagai berikut :

a. Membuat tim Pusat Operasi Keamanan (SOC) di perusahaan untuk memantau ancaman terbaru, mengikuti perkembangan alat, teknik, dan taktik baru yang sedang berkembang yang digunakan oleh aktor ancaman dan pelaku kejahatan siber;
b. Untuk mendeteksi level endpoint, investigasi, dan remediasi insiden tepat waktu, dan menerapkan solusi EDR (*Endpoint Detection and Response*);
c. Menerapkan solusi keamanan tingkat perusahaan untuk mendeteksi ancaman tingkat lanjut di tingkat jaringan pada tahap awal.

Untuk mengantisipasi dan kesiapan tim di berbagai level memerlukan kegiatan diantaranya

a. Membuat rancangan penanggulangan serangan hacking dan semacamnya
b. Membuat simulasi atau skenario kejadian agar rencana tersebut bisa dibuktikan
c. Menguji dan memastikan rencana respons terhadap kejadian-kejadian yang bersifat merugikan
d. Melakukan *review* dan menindaklanjuti laporan keamanan di periode-periode sebelumnya.

e. Melihat pola serangan, melakukan tindakan antisipasi, mendokumentasikan jenis serangan, sumber dan apa target untuk memetakan mana sistem yang rentan dan mana yang harus diprioritaskan.
f. Mengembangkan petunjuk langkah demi langkah untuk menangani setiap insiden, karena dapat terjadi dengan berbagai cara.
g. Menyiapkan asuransi untuk aset-aset digital yang ada.

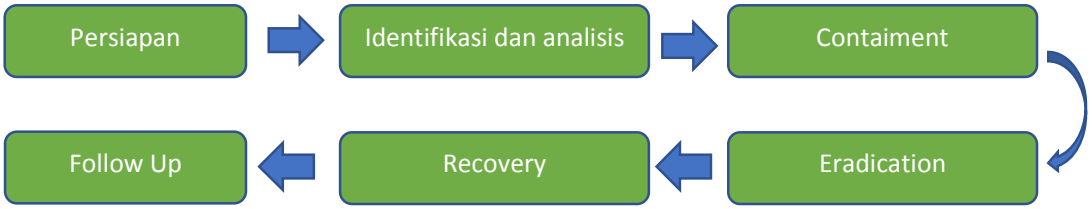
2. Penanganan ketika terjadi insiden

Ketika sistem monitoring bekerja dan menemukan kejadianya yang diluar kebiasaan (kondisi normal) maka perlu melakukan h al-hal sebagai berikut:

a. Melindungi aplikasi dan data penting.
b. Menemukan dengan cepat perubahan konfigurasi file sistem menggunakan pengujian otomatis dan verifikasi data cadangan untuk membantu respons cepat dan mengurangi waktu *downtime.*
c. Mengamankan jaringan, sistem, dan aplikasi secara efektif.
d. Dokumentasikan lain terkait insiden
e. Membuat pedoman tertulis untuk memprioritaskan insiden seperti dampak fungsional dari insiden (dampak negative), dampak informasi dari insiden (misalnya, efek pada kerahasiaan, integritas dan ketersediaan informasi organisasi) dan pemulihan dari insiden (waktu dan jenis sumber daya yang harus digunakan)

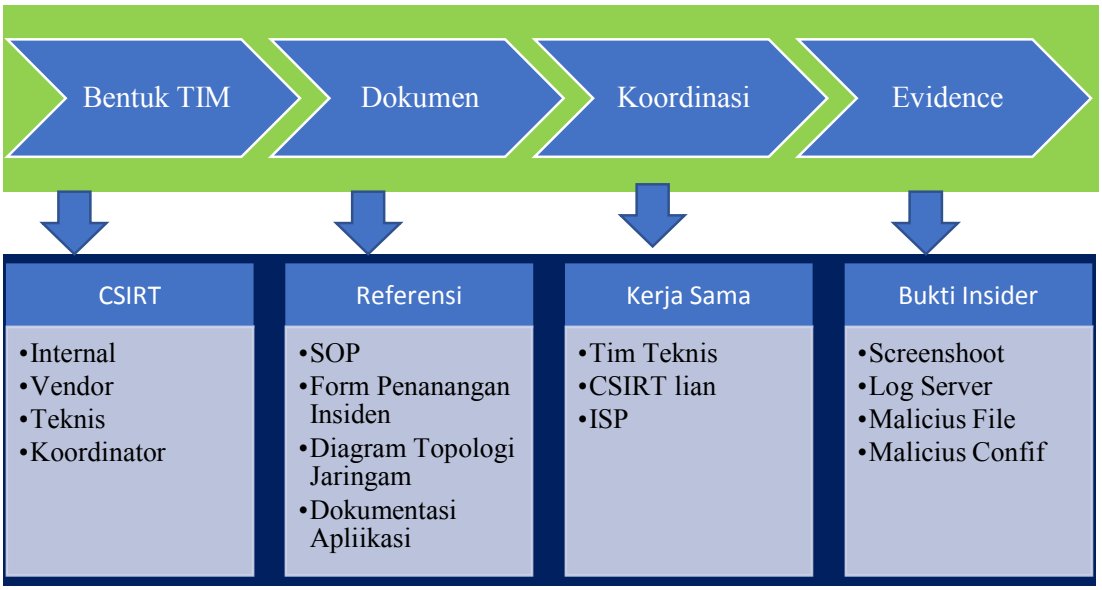
3. Penanganan setelah kejadian insiden

Berikut ini tahapan dalam penanganan insiden :



Gambar 2. Tahapan penanganan Insiden

Tahap persiapan dalam penanganan insiden



Gambar 3. Tahapan persiapan penanganan insiden

Tahap Identifikasi dan Analisis dengan Langkah-langkah

a. Periksa perubahan pada file statis, kapan berubah?
b. Periksa semua link web
c. Periksa semua log
   - Access log apache server (usr/local/apache/logs/access.log)
   - Error log apache server (usr/local/apache/logs/error.log)

   Log merupakan sebuah dokumentasi dari seluruh kegiatan yang dilakukan oleh Server, aplikasi ataupun perangkat keamanan yang digunakan dalam sebuah sistem, diantaranya;
   a. **Sumber Serangan**; alamat IP Penyerang terdokumentasi secara otomatis oleh sistem Log.
   b. **Malicious**; dapat mengetahui layanan/file malicio us yang diupload ke server
   c. **Exploit;** teknik hacking yang dilakukan.

Tahap Containment

a. Melakukan back up data (forensik dan pengumpulan bukti)
b. mengidentifikasi semua service dan koneksi
c. mengidentifikasi cara penyerang masuk system pertama kali
d. memeriksa kode-kode berbahaya dalam system (trojan, backdoor)
e. menginventarisir kerentanan
   - Kode sql
   - Komponen yang memiliki akses write
   - Respon web saat url salah

Tahap Penghapusan Konten (Eradication)

a. Hapus malicious content (termasuk konten deface)
b. Hapus aplikasi mencurigakan
   - Jalankan service yang diperlukan saja
c. Patching keamanan aplikasi web
d. Periksa dan hapus backdoor
e. Lakukan vulnerability assessment

Tahap Pemulihan *(Recovery)*

Mengembalikan ke keadaan semula

Tahap Tindak Lanjut *(Follow Up)*

a. Lesson learned
b. Laporan Akhir
c. Bukti Arsip dan Dokumentasi
d. Menutup proses penanganan insiden

4. Penerapan Control dan Monitoring

Framework, Kontrol dan Monitoring perlu diterapkan pada Process, People & Technology untuk mengamankan data.

Gambar 4. Penerapan Kontrol dan Monitoring

Gambar 5. Manajemen Layanan Security

Studi Kasus

Pentest Report PT X
Target : https://pt.id/

Vulnerability :

A. Missing Security Header Protection (Low)

1. Tidak di terapkannya Security Header Protection akan berpotensi menyebabkan beberapa celah vulnerability seperti Clickjacking, XSS, dll.
2. List Security Header untuk di pasang seperti :
   - HTTP Strict Transport Security (HSTS)
   - Public Key Pinning Extension for HTTP (HPKP)
   - X-Frame-Options
   - X-XSS-Protection
   - X-Content-Type-Options
   - Content-Security-Policy
   - X-Permitted-Cross-Domain-Policies
   - Referrer-Policy
   - Expect-CT
   - Feature-Policy
3. Beberapa sudah terpasang karena default dari cloudflare
4. Reference : https://owasp.org/www-project-secure-headers/
5. Remediation :

- Terapkan security header protection

B. Information Disclosure Through DS Store File (Medium)

1. Terdapat _DS_File yang dimana menyimpan cache list file pada folder dimana DS File tersebut berada, file ini bisa di manfaatkan attacker untuk melakukan mapping directory dan file pada folder tersebut, contoh :
   - https://www.ptx.id/assets/_DS_Store
   - https://www.ptx.id/assets/css/_DS_Store

C. Information Disclosure Through Public Repository (High)

1. Terdapapat beberapa repository yang isinya source code dari web PTX seperti :
   - https://github.com/xxx/web-id
   - https://github.com/xxxx/ptx
   - https://github.com/yyyy/ptx
2. Dimana jika developer menyimpan informasi penting pada repo tersebut akan sangat berbahaya karena dapat di lihat oleh public

Kesimpulan

Sistem layanan yang 24 x 7, memerlukan monitoring sistem keamanan yang sama 24 x 7, jika terjadi kebocoran data, maka sangat merugikan secara material maupun reputasi perusahaan. Penerapan sistem keamanan wajib diterapkan dalam perusahaan dan dipahami oleh seluruh sumber daya manusia yang ada dilingkungan perusahaan. Kesempatan ini menjadi peluang dan membuka kesempatan menjadi konsultan IT/ Enterpreneur IT bidang *cybersecurity*, yaitu masih terbuka lebar. Dengan memiliki *skill cybersecurity*, Anda juga bisa meningkatkan jenjang karier bisnis ke arah yang lebih menjanjikan, seperti *penetration tester, white hat hacker*, *computer forensic specialist*, dan masih banyak lagi.

Daftar Pustaka

[1] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," NiST, US, 2018.