1. **Cloud Computing**

## **Definisi Cloud Computing**

Cloud computing mungkin masih samar terdengar bagi orang awam. Tetapi keberadaan cloud computing di era digital kini sebenarnya telah terasa di tengah masyarakat dalam kehidupan sehari hari seperti penggunaan email dan juga media sosial.

Secara umum, definisi cloud computing (komputasi awan) merupakan gabungan pemanfaatan teknologi komputer (komputasi) dalam suatu jaringan dengan pengembangan berbasis internet (awan) yang mempunyai fungsi untuk menjalankan program atau aplikasi melalui komputer – komputer yang terkoneksi pada waktu yang sama, tetapi tak semua yang terkonekasi melalui internet menggunakan cloud computing.

Cloud computing juga menjadikan internet sebagai pusat pengelolaan data dan aplikasi, di mana pengguna komputer diberikan hak akses (login). Penerapan komputasi awan saat ini sudah dilakukan oleh sejumlah perusahaan IT terkemuka di dunia. Sebut saja di antaranya adalah Google (google drive) dan IBM (blue cord initiative). Sedangkan di Indonesia, salah satu perusahaan yang sudah menerapkan komputasi awan adalah Telkom (Anggi, pusatteknologi.com).

## **Jenis Layanan Cloud Computing**

* + 1. **SaaS (*Software as a Service*)**

Sesuai namanya, layanan cloud computing jenis ini disediakan dalam bentuk software atau perangkat lunak. Contohnya adalah Google Docs dan Spreadsheet serta Adobe Creative Cloud. Pada praktiknya, Anda hanya menggunakan aplikasi-aplikasi tersebut tanpa perlu mengerti dimana (secara fisik) data disimpan atau bagaimana aplikasi dikelola. Hal-hal tersebut sudah termasuk dalam layanan yang diberikan oleh penyedia Software as a Service.

Melalui SaaS, Anda dapat mengakses software (aplikasi) dengan mudah tanpa perlu menediakan storage perangkat Anda khusus untuk menyimpan aplikasi tersebut. Penyedia layanan juga akan menjamin ketersediaan dan reliabilitas aplikasi miliknya. Dengan begitu, Anda bisa fokus dalam memaksimalkan penggunaan aplikasi tersebut.

* + 1. **PaaS (*Platform as a Service*)**

Layanan cloud jenis ini hadir dalam bentuk platform yang dapat Anda gunakan untuk membuat aplikasi. Jika dianalogikan, PaaS memungkinkan Anda untuk menyewa “rumah” dan berbagai “lingkungan”-nya (network, database engine, sistem operasi, framework aplikasi, dan sebagainya) untuk membantu berjalannya aplikasi yang Anda buat. Sebagai penyewa, Anda tak perlu memikirkan pemeliharaan rumah tersebut karena penyedia layanan Platform as a Service -lah yang akan melakukannya, sehingga Anda dapat fokus mengembangkan aplikasi yang Anda buat di “rumah” tersebut.

Contoh penyedia PaaS ini adalah IBM Bluemix. Pada layanan tersebut, Anda dapat membuat aplikasi sendiri dengan berbagai fitur yang telah tersedia. Idealnya, fitur utama dari PaaS adalah skalabilitas yang tinggi. Jadi, semakin banyak pengguna aplikasi Anda, penyedia PaaS akan secara otomatis membantu aplikasi Anda untuk dapat melayani jumlah pengguna tersebut.

* + 1. **IaaS (*Infrastructure as a Service*)**

Pada IaaS, penyedia layanan akan memberikan sumber daya infrastruktur komputasi (cloud computing) yang lengkap, mulai dari server, jaringan, storage, hingga ruang data center. Sederhananya, ketika menggunakan IaaS, Anda sebenarnya sedang menyewa komputer virtual yang masih kosong. Setelah disewa, Anda bisa menambahkan komponen komputasi seperti CPU, RAM, Storage, Public IP, dll untuk membangun komputer virtual yang sesuai dengan kebutuhan Anda.

Dengan menggunakan layanan IaaS, Anda tak perlu membeli perangkat komputer fisik dan juga memikirkan pengelolaannya. Kabar baiknya lagi, IaaS memungkinkan Anda untuk melakukan konfigurasi komputer virtual tersebut secara mudah, cepat dan praktis. Misalnya, jika komputer virtual menampung data lebih dari kapasitas yang tersedia, Anda bisa menambahkan RAM atau storage dengan cepat.

## **Tipe-tipe Cloud Computing**

Ada empat macam atau tipe cloud yang berbeda yang dapat Anda pakai sebagai pengguna, sesuai dengan kebutuhan bisnis. Berikut ini !

1. **Private Cloud**

Private Cloud merupakan sumber daya cloud yang digunakan untuk satu organisasi tertentu saja (secara privat, tidak dibagi ke pengguna atau organisasi lain). Metode ini lebih banyak dipakai untuk interaksi seperti intra-bisnis, di mana sumber daya cloud dapat diatur, dimiliki, dan dioperasikan oleh organisasi satu yang sama.

1. **Community Cloud**

Community cloud mengacu pada penggunaan source untuk komunitas dan organisasi.

1. **Public Cloud**

Jenis cloud ini biasanya digunakan untuk interaksi tipe B2C (Business to Consumer). Public Cloud memakai sumber daya komputasi yang dimiliki, diatur dan dioperasikan oleh pemerintah.

1. **Hybrid Cloud**

Hybrid dapat digunakan untuk dua jenis interaksi – B2B (Business to Business) atau B2C (Business to Consumer). Jadi, sumber daya komputasi terikat bersama tetapi dengan cloud yang berbeda

## **Manfaat Cloud Computing**

### **Menghemat Biaya**

Hadirnya teknologi *Cloud Computing* akan memangkas biaya teknologi informasi. Hal ini karena perusahaan hanya perlu mengeluarkan biaya berlangganan tanpa perlu berinvestasi pada pembelian dan pemasangan alat. Selain itu, biaya pemeliharaan perangkat dan penggantian alat yang rusak juga dapat dihapus dari anggaran.

### **Fleksibilitas**

Manfaat berikutnya dari penggunaan *Cloud Computing* untuk bisnis adalah faktor fleksibilitas. Bahkan faktor ini dipercaya menjadi manfaat yang paling membuat pelaku bisnis mau memakai *Cloud Computing*.  Lantas mengapa dianggap fleksibel?

Hal ini lantaran *Cloud Computing* menawarkan akses ke dokumen dan data secara lebih mudah. Anda bisa mengakses atau berinteraksi dengan data tanpa dibatasi ruang dan waktu. Selagi memiliki akses internet, maka kapanpun dan dimanapun Anda seolah-olah bisa memiliki kantor virtual sendiri.

### **Lebih Efektif dan Efisien**

*Cloud Computing* memungkinkan adanya komunikasi dan interaksi dengan lebih mudah. Perangkat lunak ini menjadikan karyawan di sebuah perusahaan bisa berbagi dan mengerjakan data secara bersamaan. Bagi anda yang bekerja mobile atau sering bekerja di luar kantor, *Cloud Computing* juga tentu akan membuat pekerjaan lebih efektif dan efisien lantaran semua dokumen bisa ditransfer dengan cepat dan aman.

### **Meningkatkan Daya Saing**

Seperti yang sudah diungkap di awal, *Cloud Computing* adalah upaya perusahaan agar bisa bersaing dengan lingkungan global yang semakin ketat. Persaingan bisnis memaksa setiap bidang usaha untuk bisa menanggapi perubahan pasar yang dinamis. Melalui *Cloud Computing*, berbagai pekerjaan bisa berjalan lebih mudah karena sifatnya yang mudah disesuaikan dengan kebutuhan bisnis perusahaan atau kebutuhan pasar yang tengah menjadi tren.

### **Mampu Mengontrol Dokumen dengan Aman**

Keamanan dokumen adalah hal penting bagi sebuah bisnis. Apalagi untuk perusahaan yang memiliki banyak mitra kerja, dokumen dalam jumlah besar tentu perlu pengontrolan yang lebih ketat. Jika dahulu karyawan harus mengirim file bolak-balik sebagai lampiran email kepada klien dan karyawan lain pada satu waktu, maka dengan *Cloud Computing* hal tersebut tidak perlu dilakukan lagi. Konten, format, dan judul dokumen menjadi lebih rapi tersusun dan lebih aman tersimpan.

Keamanan data pengguna *Cloud Computing* disimpan lewat server. Server ini disediakan oleh penyedia layanan *Cloud Computing* seperti jaminan *platform* teknologi, jaminan ISO, data pribadi, dan lain sebagainya.

### **Skala yang Mudah Disesuaikan**

Bisnis bersifat dinamis dan fluktuatif. Ada kalanya bisnis mengalami peningkatan permintaan namun ada kalanya juga mengalami penurunan. Oleh karena itu, *Cloud Computing* bisa menjadi alat untuk mengatasinya.

Perangkat lunak ini bisa beradaptasi dengan skalabilitas perusahaan. Jika kebutuhan meningkat, maka peningkatan kapasitas *cloud* bisa dilakukan tanpa harus membeli peralatan tambahan seperti *hardisk*. Begitu pun jika diperlukan penghematan, maka kapasitas *cloud* bisa dikurangi dengan mudah.

### **Minimalisasi Risiko**

Banyak hal yang bisa terjadi dari sebuah kegiatan bisnis. Perusahaan bisa saja mengalami kegagalan sistem, bencana, atau krisis lainnya. Namun, dengan menggunakan perangkat lunak *Cloud Computing*, maka perusahaan tidak perlu menghentikan bisnisnya selama memperbaiki sistem.

Teknologi *cloud* memungkinkan pengguna untuk menyimpan data secara terpusat di satu server berdasarkan layanan yang disediakan oleh penyedia layanan *Cloud Computing* tersebut. Semua kebutuhan juga saling terintegrasi sehingga risiko eror sebagian data bisa diminimalisir.

* 1. **Resiko Cloud Computing**

Sebagaimana yang dikatakan sebagai bisnis service, dengan teknologi cloud anda sebaiknya mengetahui dan memastikan apa yang anda bayar dan apa yang anda investasikan sepenuhnya memang untuk kebutuhan anda menggunakan service ini. Anda harus memperhatikan pada beberapa bagian yaitu:

* + 1. **Service level**

Cloud provider mungkin tidak akan konsisten dengan performance dari application atau transaksi. Hal ini mengharuskan anda untuk memahami service level yang anda dapatkan mengenai transaction response time, data protection dan kecepatan data recovery.

* + 1. **Privacy**

Karena orang lain / perusahaan lain juga melakukan hosting kemungkinan data anda akan keluar atau di baca dan dapat terjadi tampa sepengetahuan anda atau approve dari anda.

* + 1. **Compliance**

Anda juga harus memperhatikan regulasi dari bisnis yang anda miliki, dalam hal ini secara teoritis cloud service provider diharapkan dapat menyamakan level compliance untuk penyimpanan data didalam cloud, namun karena service ini masih sangat muda anda diharapkan untuk berhati hati dalam hal penyimpanan data.

* + 1. **Data ownership**

Apakah data anda masih menjadi milik anda begitu data tersebut tersimpan didalam cloud? mungkin pertanyaan ini sedikit aneh, namun anda perlu mengetahui seperti hal nya yang terjadi pada Facebook yang mencoba untuk merubah terms of use aggrement nya yang mempertanyakan hal ini.

* + 1. **Data Mobility**

Apakah anda dapat melakukan share data diantara cloud service? dan jika anda terminate cloud relationship bagaimana anda mendapatkan data anda kembali? Format apa yang akan digunakan ? atau dapatkah anda memastikan kopi dari data nya telah terhapus

## **Aspek Keamanan dalam Cloud Computing**

Di tengah menggeliatnya pangsa pasar cloud services, penting untuk dipahami oleh pengguna bisnis seputar langkah keamanan sebelum menentukan vendor cloud computing.

### **Memahami skema dalam lingkungan cloud computing**

Ketika sebuah bisnis telah menentukan vendor tertentu sebagai penyedia layanan cloud, maka ia telah menyerahkan kapabilitas perpanjangan pusat data kepada pihak terkait. Oleh karenanya penting untuk senantiasa memastikan apakah layanan dan kebijakan keamanan yang diterapkan cukup mumpuni sebagai tempat berlabuhnya data-data penting perusahaan?

Tak ada salahnya ketika hendak berlangganan layanan tertentu kita meminta segudang informasi seputar layanan keamanan yang disediakan provider tersebut. Dinamika teknologi yang selalu berubah membutuhkan sistem keamanan yang siap siaga untuk mencegah serangan cyber yang kian berkembang. Pahami betul tanggung jawab yang dapat diberikan oleh penyedia layanan, dan apa yang harus dilakukan pengguna sehingga keduanya dapat bersinergi dengan baik.

Umumnya saat berbicara tentang cloud, maka akan diharapkan pada sebuah skema virtualisasi. Lingkungan virtual memberikan tantangan tersendiri pada perlindungan data. Isu utama yang sering terjadi ialah pengelolaan keamanan dan trafik di ranah multi-tanency dan mesin virtual (beberapa layanan dengan spesifikasi rendah menggunakan server yang sama untuk beberapa pengguna).

### **Mendefinisikan peranan pengguna dengan baik**

Skema akses data granular, atau memberikan batasan sesuai dengan porsinya dapat menjadi pilihan. Terlebih layanan cloud kini mulai spesifik memberikan kinerja sesuai dengan kebutuhan sistem. Misalnya ada server khusus untuk basis data pelanggan, ada server yang mengoptimalkan kinerja sistem hingga backup.

Dengan adanya pembagian peran, dinilai akan mampu memberikan lapisan perlindungan tambahan. Mengingat saat ini modus penyerangan juga berusaha mencuri identitas login staf, terutama yang lengah dalam mengamankan akunnya.

### **Penggunaan enkripsi adalah harga mati**

Skema enkripsi biasanya juga sudah ditanamkan secara native bersama dengan layanan cloud yang dijajakan oleh vendor, umumnya SaaS. Pahami betul bagaimana sistem enkripsi bekerja melindungi data dan transmisi data.

Layanan cloud juga umumnya digunakan oleh banyak pihak di perusahaan, termasuk non-tech-savvyusers. Biasanya mereka mengakses layanan dari ponsel atau laptop pirbadi, yang tidak bisa selalu dipantau sisi keamanannya. Oleh karena perencanaan enkripsi menjadi hal yang cukup krusial.

Penerapan compliance seperti keamanan data menggunakan ISO 27001, untuk penyediaan layanan memakai ITIL, COBIT, Cloud Security Alliance dan sebagainya juga wajib menjadi perhatian.

Istilah Shadow IT beberapa waktu belakang juga santer dibicarakan, yakni tentang penggunaan layanan dan aplikasi cloud tanpa otorisasi. Padahal minimnya kontrol ini sebenarnya berisiko menghadirkan ancaman keamanan dan tantangan pengelolaan yang lebih berat.

## **Kelebihan dan Kekurangan Cloud Computing**

### **Kelebihan Cloud Computing**

* **Mudah Di Akses dimana saja**

Karena menggunakan cloud computing data kita tersimpan di dalam server di internet maka mudah bagi pengguna untuk mengakses data dimanapun dan kapanpun asal terhubung dengan internet.

* **Murah**

Penggunaan cloud computing sangat hemat biaya untuk alokasi perangkat keras. Cloud computing juga tidak memerlukan maintenance dan mengurangi pemakaian listrik.

* **Hemat**

Kelebihan lain dari cloud computing, dengan adanya sistem komputasi awan memungkinkan perusahaan atau instansi untuk mengurangi infrastruktur komputer yang memerlukan biaya pengadaan dan perawatan cukup besar.

* **Fleksibel**

Ketika data yang kita punya terlalu besar maka ia otomatis menambah kapasitas hanya dalam hitungan menit dengan melakukan self-provisioning. Sehingga tidak perlu melakukan penambahan jumlah komputer.

* **Ketersediaan Data**

Sistem yang digunakan cloud computing sudah didesain high availability, sistem tersebut sudah berada pada data center yang sudah menjamin ketersediaan listrik, pendingin, dan lainnya yang sudah menjadi fasilitas pendukung selama 24 jam.

* **Skalabilitas**

Penggunaan layanan cloud yang menyediakan dan menawarkan penyimpanan sesuai dengan permintaan pengguna, jadi di sini pengguna dapat dengan mudah melakukan manajemen data baik untuk mengurangi atau mereproduksi data yang akan disimpan di server cloud.

* **Aman**

Jadi tidak perlu ragu lagi untuk menggunakan cloud computing karena sudah pasti aman dan terjamin asalkan mencari partner yang memang sudah mempunyai mempunyai sertifikat atau terstandarisasi ISO untuk menjamin keamananya.

### **Kekurangan Cloud Computing**

* **Bergantung Pada Koneksi Internet**

Internet merupakan satu-satunya jalan menuju cloud computing. Ketika tidak ada koneksi internet di tempat Anda, atau jalur internet menuju cloud provider sedang bermasalah, secara otomatis akses ke mesin cloud computing Anda akan terputus.

Nah dari sinilah hambatan terbesar yang tengah terjadi di Indonesia, karena belum semua seluruh wilayah telah terjangkau oleh akses internet.

* **Harus Cari Vendor Yang Sudah Standarisasi untuk Menjamin Keamanan**

Dengan menggunakan sistem komputasi awan berarti Anda mempercayakan sepenuhnya atas keamanan dan kerahasiaan data-data kepada cloud provider. Untuk itu anda harus mencari partner cloud computing yang sudah mempunyai sertifikat atau terstandarisasi ISO untuk menjamin keamananya.

## **Shadow IT**

* + 1. **Definisi Shadow IT**

Shadow IT atau dalam bahasa Indonesia adalah penerapan bayangan IT, merupakan aplikasi atau perangkat lunak yang dipergunakan oleh para pegawai perusahaan tanpa mendapatkan persetujuan atau berkonsultasi terlebih dahulu dengan Departemen IT di perusahaan tersebut. Sebagian besar pegawai tidak mengetahui apa resiko Shadow IT untuk perusahaan, sehingga mereka bebas mendownload berbagai macam aplikasi dari internet. Kegiatan tersebut ternyata bisa mengancam keamanan perusahaan. Privacy perusahaan bisa terancam dan Departemen IT pun memperoleh tantangan baru karena Shadow IT.

Berdasarkan survey yang dilakukan pada tahun 2015 oleh Aliansi Keamanan Cloud, ternyata hanya sekitar 8% saja perusahaan yang paham mengenai Shadow IT dan efeknya bagi keamanan perusahaan. Maka tak mengherankan jika banyak kasus mengenai pencurian data perusahaan. Selain itu efek lain dari Shadow IT adalah terjadinya pelanggaran kepatuhan dalam perusahaan.

* + 1. **Resiko Keamanan**

Shadow IT jelas-jelas bisa membahayakan perusahaan dan bisnis. Perusahaan seakan tidak dapat mengontrol secara penuh mengenai keamanan datanya. Arus data mengalir tanpa terkendali melalui aplikasi, umumnya melalui Dropbox dan Google Document. Bagaimana Shadow IT bisa mengancam keamanan data perusahaan? Inilah gambaran yang terjadi; Beberapa pegawai perusahaan memiliki aplikasi atau cloud di smartphone mereka tanpa persetujuan tim IT perusahaan. Ketika mereka membuka file tertentu, terdapat kemungkinan bahwa smartphone akan mengcopy file perusahaan dan mengirimkannya ke tempat penyimpanan online yang tidak aman. Ini bisa terjadi saat smartphone melakukan backup data reguler secara otomatis.

* + 1. **Mengatasi Shadow IT**

Shadow IT tidak boleh diabaikan, karena efeknya bisa merugikan perusahaan. Bagaimana cara untuk mencegah resiko Shadow IT untuk perusahaan? Mencegah akses Shadow IT akan membuat tugas Departemen IT menjadi lebih berat. Secara teknis, pencegahan bisa dilakukan dengan enkripsi atau dengan alat monitoring jaringan serta pengelolaan keamanan. Setelah itu lakukan sosialisasi mengenai Shadow IT pada seluruh pegawai perusahaan. Departemen IT memberikan penjelasan secara rinci mengenai definisi Shadow IT serta dampak buruknya bagi [perusahaan](http://robicomp.com/pengertian-bisnis-continuity-planning-dan-perannya-di-perusahaan.html).

Selanjutnya Departemen IT harus memiliki peraturan yang ketat mengenai pelanggaran Shadow IT di perusahaan. Aplikasi apa saja yang diperbolehkan atau dilarang dalam lingkup pekerjaan. Itulah yang harus dilakukan agar resiko Shadow IT untuk perusahaan tidak terjadi di perusahaan Anda.

# Downloading 3rd party applications

## **Definisi Aplikasi Pihak Ketiga**

Aplikasi pihak ketiga adalah aplikasi yang dibuat oleh pengembang yang bukan produsen perangkat tempat aplikasi dijalankan atau pemilik situs web yang menawarkannya. Aplikasi pihak ketiga dapat disambut atau dilarang oleh perangkat atau kepemilikan situs web.

Misalnya, aplikasi web browser Safari yang hadir di iPhone kita adalah aplikasi asli buatan Apple, tetapi App Store berisi aplikasi peramban web lain yang disetujui Apple untuk digunakan di iPhone tetapi tidak berkembang. Aplikasi tersebut adalah aplikasi pihak ketiga. Facebook mengizinkan beberapa aplikasi yang tidak berkembang berfungsi di situs media sosialnya. Mereka adalah aplikasi pihak ketiga.

## **Jenis-jenis Aplikasi Pihak Ketiga**

Ada beberapa situasi yang berbeda di mana kita dapat menemukan istilah “aplikasi pihak ketiga.”

* Aplikasi yang dibuat untuk toko aplikasi resmi oleh vendor selain Google (Google Play Store) atau Apple (App Store Apple) dan yang mengikuti kriteria pengembangan yang diperlukan oleh app store tersebut adalah aplikasi pihak ketiga. Aplikasi yang disetujui oleh pengembang untuk layanan seperti Facebook atau Snapchat dianggap sebagai aplikasi pihak ketiga. Jika Facebook atau Snapchat mengembangkan aplikasi, maka itu adalah aplikasi asli.
* Aplikasi yang ditawarkan melalui toko aplikasi atau situs web pihak ketiga tidak resmi yang dibuat oleh pihak yang tidak berafiliasi dengan perangkat atau sistem operasi juga merupakan aplikasi pihak ketiga. Semua aplikasi yang disediakan di toko-toko ini adalah aplikasi pihak ketiga. Gunakan hati-hati saat mengunduh aplikasi dari sumber apapun, terutama toko atau situs web aplikasi tidak resmi, untuk menghindari perangkat lunak perusak.
* Aplikasi yang terhubung dengan layanan lain (atau aplikasinya) untuk menyediakan fitur yang disempurnakan atau mengakses informasi profil adalah aplikasi pihak ketiga. Contohnya adalah Quizzstar, aplikasi kuis pihak ketiga yang memerlukan izin untuk mengakses bagian tertentu dari profil Facebook kita. Jenis aplikasi pihak ketiga ini tidak diunduh, tetapi diberikan akses ke informasi yang berpotensi sensitif melalui koneksi ke layanan atau aplikasi lain.

## **Bagaimana Aplikasi Asli Berbeda dari Aplikasi Pihak Ketiga**

Saat membahas aplikasi pihak ketiga, istilah aplikasi asli dapat muncul. Aplikasi asli adalah aplikasi yang dibuat dan didistribusikan oleh produsen perangkat atau pembuat perangkat lunak. Beberapa contoh aplikasi asli untuk iPhone adalah iTunes, Message, dan iBooks.

Apa yang membuat aplikasi ini asli adalah bahwa aplikasi dibuat oleh pabrikan untuk perangkat pabrikan itu, sering kali menggunakan kode sumber proprietary. Misalnya, ketika Apple membuat aplikasi untuk perangkat Apple – seperti iPhone – ini disebut sebagai aplikasi asli. Untuk perangkat Android, karena Google adalah pencipta sistem operasi seluler Android, contoh aplikasi asli termasuk versi seluler dari salah satu aplikasi Google, seperti Gmail, Google Drive, dan Google Chrome.

Hanya karena aplikasi adalah aplikasi asli untuk satu jenis perangkat, itu tidak berarti tidak ada versi aplikasi yang tersedia untuk jenis perangkat lain. Misalnya, sebagian besar aplikasi Google memiliki versi yang berfungsi di iPhone dan iPad yang ditawarkan melalui App Store Apple. Itu dianggap aplikasi pihak ketiga di perangkat iOS.

## **Kenapa Beberapa Layanan Mencekal Aplikasi Pihak Ketiga**

Beberapa layanan atau aplikasi melarang penggunaan aplikasi pihak ketiga untuk alasan keamanan. Setiap kali aplikasi pihak ketiga mengakses profil atau informasi lain dari akun kita, ini menghadirkan risiko keamanan. Informasi tentang akun atau profil kita dapat digunakan untuk meretas atau menggandakan akun kita. Dalam kasus anak di bawah umur, itu dapat mengekspos foto dan detail tentang remaja dan anak-anak kepada orang yang berpotensi membahayakan.

Dalam contoh kuis Facebook, sampai kita masuk ke pengaturan akun Facebook dan mengubah izin aplikasi, aplikasi kuis tersebut dapat mengakses detail profil yang kita berikan izin untuk mengaksesnya, lama setelah kita berhenti menggunakan aplikasi. Ini dapat terus mengumpulkan dan menyimpan detail dari profil kita – detail yang mungkin merupakan risiko keamanan untuk akun Facebook kita.

Agar jelas, menggunakan aplikasi pihak ketiga tidak ilegal. Namun, jika persyaratan penggunaan untuk layanan atau aplikasi menyatakan bahwa aplikasi pihak ketiga tidak diizinkan, mencoba menggunakan salah satu untuk terhubung ke layanan tersebut dapat menyebabkan akun kita dikunci atau dinonaktifkan.

## **Siapa yang Menggunakan Aplikasi Pihak Ketiga**

Tau nggak sih kita juga merupakan pengguna aplikasi pihak ketiga, Ini karena banyak aplikasi pihak ketiga yang sangat berguna. Aplikasi pihak ketiga adalah aplikasi yang membantu mengelola beberapa akun media sosial pada saat yang sama, seperti Hootsuite atau Buffer. Kita mungkin mengelola rekening bank di perangkat seluler, menghitung kalori, atau mengaktifkan kamera keamanan rumah melalui aplikasi pihak ketiga.

Buka layar menu aplikasi di smartphone dan gulir melalui aplikasi yang kita unduh. Apakah memiliki game, media sosial, atau aplikasi belanja? Kemungkinannya baik mereka adalah aplikasi pihak ketiga.