MODULPERKULIAHAN

Cloud Computing

Pertemuan 6
Model Keamanan Cloud

Abstract
Menjelaskan tentang model keamanan yang ada di Cloud Computing

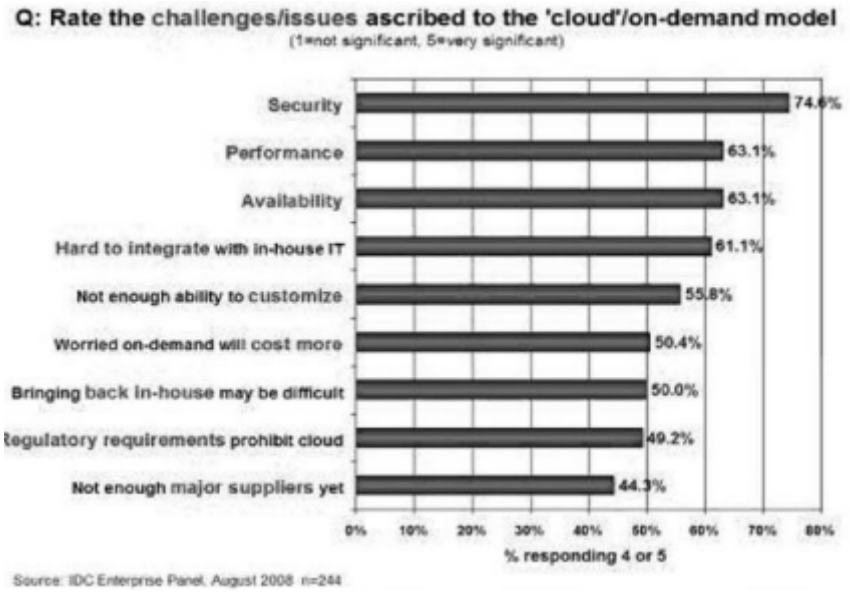
Kompetensi
Mampu memahami model keamanan yang ada di Cloud Computing

Pendahuluan

Komputasi awan telah didefinisikan sebagai penggunaan sekumpulan layanan terdistribusi, aplikasi, informasi dan prasarana terdiri dari kompute, jaringan, informasi dan sumber daya penyimpanan. Komponen-komponen ini dapat dengan cepat diatur, ditetapkan, diimplementasikan, dan dihentikan dengan menggunakan utilitas on - demand seperti model alokasi dan pemakaian.

Penyedia layanan awan memanfaatkan teknologi virtualisasi yang dikombinasikan dengan kemampuan layanan mandiri untuk menghitung sumber daya melalui Internet. Dalam lingkungan operator selular, mesin virtual dari beberapa organisasi harus terletak pada server fisik yang sama dalam rangka untuk memaksimalkan efisiensi virtualisasi.

Penyedia layanan Cloud harus belajar dari model penyedia layanan yang dikelola dan memastikan bahwa aplikasi dan data dari pelanggan mereka aman, jika mereka berharap untuk mempertahankan pelanggan dan daya saing. Saat ini, perusahaan mencari arah cakrawala/wawasan komputasi awan untuk memperluas infrastruktur lokal, tapi kebanyakan tidak mampu membayar resiko mengorbankan keamanan dari aplikasi dan data. Sebagai contoh, IDC baru-baru ini melakukan survei (lihat Gambar) dari 244 eksekutif IT/CIO dan rekan line - of -business (LOB) mereka, untuk mengukur pendapat mereka dan memahami perusahaan mereka dalam menggunakan layanan teknologi awan. Keamanan menduduki peringkat pertama sebagai tantangan dan masalah besar komputasi awan (Cloud Computing).



Gambar 1. Hasil survey tantangan keamanan IDC (International Data Corporation)

Sumber : IDC Enterprice Panel, August 2008

Terinspirasi oleh pergerakan industri IT menuju SaaS, di mana perangkat lunak tidak dibeli, tetapi menyewa layanan dari penyedia, IT-as-a-Service (ITaaS) sedang diusulkan untuk mengambil konsep ini lebih lanjut, untuk membawa hak model layanan untuk Infrastruktur TI anda. organisasi IT modern harus menjalankan dirinya sebagai operasi yang terpisah dan menjadi lebih strategis dalam pengambilan keputusan operasional.

Banyak organisasi dalam proses transformasi departemen IT mereka ke pusat biaya operasional mandiri, memperlakukan pengguna internal yang seolah - olah mereka adalah pelanggan.

Transformasi ini tidak sepele dan biasanya melibatkan unsur-unsur manajemen proyek portofolio, alur kerja rekayasa ulang, dan perbaikan proses. Transformasi ini memerlukan waktu yang lama untuk diselesaikan. Banyak organisasi IT besar yang telah mengadopsi kerangka kerja Information Technology Infrastructure Library (ITIL) dengan maksud membantu melalui trasformasi ini.

Tantangan Keamanan Cloud

Meskipun virtualisasi dan komputasi awan dapat membantu perusahaan mencapai /melakukan sesuatu yang lebih dengan melanggar ikatan fisik antara infrastruktur IT dan penggunanya, ancaman keamanan yang tinggi harus diatasi dalam rangka untuk mendapatkan manfaat sepenuhnya dari paradigma komputasi baru. Hal ini terutama berlaku untuk penyedia SaaS.

Beberapa kekhawatiran keamanan adalah diskusi bernilai lebih. Sebagai contoh, di awan, Anda kehilangan kendali atas aset dalam beberapa hal, sehingga model keamanan Anda harus ditinjau kembali. Keamanan yang baik bagi perusahaan adalah yang menjadi mitra, departement yang dapat diandalkan atau dipercaya. Dapatkah Anda mempercayai data Anda ke penyedia layanan Anda? Dalam paragraf berikut, kita membahas beberapa isu yang harus Anda pertimbangkan sebelum menjawab pertanyaan.

Dengan model awan, Anda kehilangan kontrol atas keamanan fisik. Dalam awan umum, Anda berbagi sumber daya komputasi dengan perusahaan lain. Di luar perusahaan anda tidak memiliki pengetahuan atau kendali dimana sumber daya dijalankan. Mengekspos data anda dalam lingkungan bersama dengan perusahaan lain, menjadikan "alasan yang masuk akal" bagi pemerintah untuk menyita aset Anda karena perusahaan lain tersebut telah melanggar hukum. Hanya karena Anda berbagi lingkungan/tempat/ruangan di awan, dapat menempatkan data Anda pada resiko penyitaan/penyerangan.

Layanan Penyimpanan yang disediakan oleh satu vendor awan mungkin tidak kompatibel dengan layanan vendor lain namun disatu sisi anda harus memutuskan untuk berpindah dari satu ke yang lain, dalam rangka memenuhi kebutuhan perusahaan anda.

Jika informasi dienkripsi saat melewati awan (Cloud), siap yang mengontrol kunci enkripsi/dekripsi? Apakah pelanggan atau perusahaan Cloud? kebanyakan nasabah mungkin ingin data mereka dienkripsi dengan dua tipe control diatas (pengontrolan oleh pelanggan atau perusahaan Cloud) di internet menggunakan SSL (Secure Sockets Layer protocol). Mereka juga mungkin ingin data mereka terenkripsi ketika sedang beristirahat di pool penyimpanan perusahaan awan (Cloud). Pastikan anda sebagai pelanggan mengontrol kunci enkripsi/dekripsi, sama seperti ketika data masih tinggal di server anda sendiri.

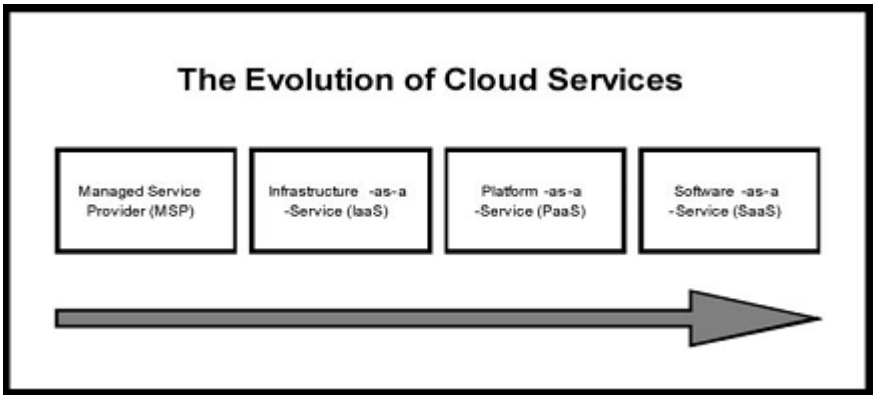
Integritas data artinya : memastikan bahwa data yang identik dijaga selama operasi apapun (seperti transfer, penyimpanan, atau pengambilan). Secara sederhana, integritas data adalah jaminan bahwa data konsisten dan benar. Memastikan keutuhan benar-benar dari data berarti bahwa perubahan hanya sebagai respons terhadap transaksi yang berwenang. Ini kedengarannya bagus, tetapi Anda harus ingat bahwa standar umum untuk memastikan integritas data belum ada. Menggunakan penawaran SaaS di awan berarti bahwa ada sedikit kebutuhan untuk pengembangan perangkat lunak. Jika Anda berencana untuk menggunakan kode yang dikembangkan secara internal di awan (Cloud), bahkan lebih penting untuk memiliki siklus pengembangan perangkat lunak yang aman secara formal. Penggunaan “teknologi mashup” yang belum matang (kombinasi layanan web), yang merupakan dasar aplikasi awan (Cloud), tanpa disadari akan menyebabkan kerentanan keamanan dalam aplikasi tersebut.

Pengembangan alat pilihan Anda, harus memiliki model keamanan yang tertanam / melekat di dalamnya untuk membimbing pengembang dalam tahap pengembangan dan membatasi user dalam penggunaan data resmi mereka ketika sistem sedang digunakan di dalam produksi. Aplikasi Awan (Cloud) mengalami penambahan fitur yang konstan, dan pengguna harus terus up to date dengan perbaikan aplikasi untuk memastikan bahwa mereka dilindungi.

kecepatan aplikasi yang akan berubah dalam awan (Cloud) akan mempengaruhi SDLC (software development life cycle) dan keamanan. Sebagai contoh, Microsoft SDLC mengasumsikan bahwa misi penting perangkat lunak akan memiliki tiga sampai lima tahun periode dimana ia tidak akan berubah secara substansial, namun Awan (Cloud) mungkin memerlukan perubahan aplikasi setiap beberapa minggu sekali. lebih buruk lagi, SLDC yang aman tidak akan mampu memberi siklus keamanan yang terus menerus terjaga dengan perubahan yang terjadi begitu cepat. Ini berarti bahwa pengguna harus terus

- menerus upgrade, karena versi lama tidak dapat berfungsi, atau tidak dapat melindungi data.

Disini akan diambil contoh keamanan pada Layanan SaaS (Software as a Service).
Model Cloud computing masa depan kemungkinan besar akan menggabungkan penggunaan SaaS, utilitas komputasi, dan kolaborasi teknologi Web 2.0 untuk memanfaatkan Internet untuk memenuhi kebutuhan pelanggan mereka.
Model bisnis baru yang dikembangkan sebagai hasil dari peralihan ke Cloud Computing tidak hanya menciptakan teknologi baru dan proses operasional bisnis tetapi juga persyaratan keamanan baru dan tantangan yang baru. Sebagai langkah evolusi terbaru dalam model layan Cloud (seperti gambar di bawah ini), SaaS kemungkinan akan tetap menjadi model layanan awan yang dominan untuk masa yang akan datang dan sebagai tempat kebutuhan yang paling penting untuk praktik keamanan dan pengawasan.



Gambar 2. Evolusi Layanan Awan

Sumber : (herwin:2011)

Seperti halnya dengan penyedia layanan yang diatur, perusahaan atau pengguna akhir perlu kebijakan penelitian vendor pada keamanan data sebelum menggunakan jasa vendor untuk menghindari kehilangan atau tidak dapat mengakses data mereka.
Analis teknologi dan perusahaan konsultan Gartner mendaftar tujuh isu keamanan yang mana salah satu diantaranya harus dibahas dengan perusahaan Cloud Computing:

1. Hak istimewa dari pengguna akses.

   Menanyakan tentang siapa yang memiliki akses khusus untuk data, dan tentang pengangkatan dan pengelolaan administrator tersebut.

2. Peraturan kepatuhan.

   Pastikan bahwa vendor bersedia untuk menjalani audit eksternal dan / atau sertifikasi keamanan.

3. Lokasi data. Apakah penyedia layanan dalam hal ini perusahaan Cloud Computing melakukan pengendalian terhadap lokasi data.
4. Pembagian / pemisahan data.
   Pastikan bahwa enkripsi tersedia di semua tahapan, dan bahwa skema enkripsi dirancang dan diuji oleh para profesional berpengalaman.
5. Pemulihanan / pembaruan.
   Cari tahu apa yang akan terjadi pada data sewaktu terjadi bencana / kerusakan. Mereka menawarkan pemulihan lengkap? Jika demikian, berapa lama waktu yang dibutuhkan untuk pemulihan tersebut sehingga pengguna layanan dapat menerima / mengambil data mereka sesuai kebutuhan denganm cepat dan tepat.
6. Bantuan investigasi / bantuan penyelidikan.
   Apakah vendor memiliki kemampuan untuk menyelidiki setiap kegiatan yang tidak patut atau ilegal?
7. Kelayakan/kelangsungan jangka panjang.
   Apa yang akan terjadi pada data jika perusahaan yang bersangkutan (vendor) keluar/berhenti dari bisnis? Bagaimana data yang dikembalikan, dan dalam format apa?

Menentukan jaminan keamanan data untuk jaman sekarang (hari-hari ini) begitu sulit, sehingga fungsi keamanan data menjadi begitu penting dibandingkan masa lalu. Taktik yang tidak terhandle oleh Gartner adalah meng-enkripsi data diri anda. Jika Anda mengenkripsi data menggunakan algoritma yang terpercaya, maka terlepas dari keamanan penyedia layanan dan kebijakan enkripsi, data hanya akan dapat diakses dengan kunci dekripsi. Tentu saja, ini mengarah ke tindak lanjut pada masalah: Bagaimana Anda mengelola kunci pribadi dalam infrastruktur komputasi pay-on-demand?

Masalah keamanan data Cloud Computing.

a. Masalah keamanan dari Virtual machine.
   Apakah Blue Cloud IBM atau Windows Azure di Microsoft, teknologi mesin virtual dianggap sebagai platform komputasi awan dari komponen fundamental, perbedaan antara Blue Cloud dan Windows Azure adalah bahwa virtual mesin berjalan pada sistem operasi Linux atau sistem operasi Microsoft Windows. Teknologi virtual mesin membawa keuntungan yang nyata, ini memungkinkan pengoperasian server tidak lagi bergantung pada perangkat fisik. Tapi pada server virtual. Pada mesin virtual, perubahan yang fisik terjadi atau migrasi tidak mempengaruhi layanan yang diberikan oleh penyedia layanan.

jika pengguna membutuhkan jasa lebih, penyedia dapat memenuhi kebutuhan pengguna tanpa harus memperhatikan perangkat keras fisik.

Namun, server virtual dari kelompok server logis membawa banyak masalah keamanan. Pengamanan terhadap pusat data tradisional diukur pada platform perangkat keras, sementara Cloud Computing mungkin merupakan server dari beberapa server virtual, server virtual mungkin milik kelompok server yang berbeda logis, server virtual, sehingga ada kemungkinan saling menyerang, yang membawa server virtual pada banyak ancaman keamanan.

Virtual mesin membentang pada tepi Cloud yang membuat hilangnya batas jaringan sehingga mempengaruhi hampir semua aspek keamanan, isolasi fisik tradisional dan infrastruktur keamanan berbasis hardware tidak dapat menghentikan lingkungan komputer Cloud yang saling menyerang antara virtual mesin.

b. Keberadaan super user.

Untuk perusahaan yang menyediakan layanan komputasi awan (Cloud Computing), mereka memiliki hak untuk melaksanakan pengelolaan dan pemeliharaan data, adanya superuser sangat bermanfaat untuk menyederhanakan fungsi manajemen data, tetapi merupakan ancaman serius bagi pengguna pribadi. Dalam era privasi pribadi, data pribadi harus benar benar dilindungi, dan fakta membuktikan bahwa platform Cloud Computing memberikan layanan pribadi dalam kerahasiannya. Bukan hanya pengguna individu tetapi juga organisasi memiliki potensi ancaman serupa, misalnya pengguna korporat dan rahasia dagang disimpan dalam platform komputasi awan mungkin dicuri. Oleh karena itu penggunaan hak super user harus dikendalikan di awan (Cloud).

c. Konsistensi data.

Lingkungan Awan (Cloud) merupakan lingkungan yang dinamis, dimana data pengguna mentransmisikan data dari data center kepengguna. Untuk sistem, data pengguna berubah sepanjang waktu. Membaca dan menulis data berkaitan dengan identitas otentikasi pengguna dan hal perijinan. Dalam sebuah mesin virtual, mungkin ada data pengguna yang berbeda yang harus wajib dikelola. Model kontrol akses tradisional dibangun di “tepi” komputer, sehingga sangat lemah untuk mengendalikan pembaca dan penulis di antar komputer yang terdistribusi.

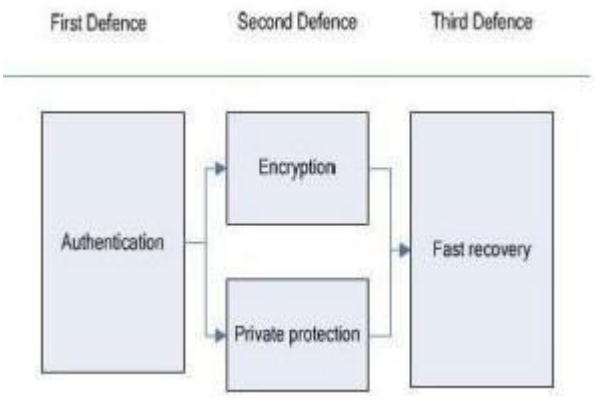
Hal ini jelas bahwa kontrol akses tradisional, jelas sangat tidak cocok untuk lingkungan komputasi awan. Dalam lingkungan komputasi awan, mekanisme kontrol akses tradisional memiliki kekurangan serius.

Prinsip Keamanan Data.

Semua teknik keamanan data dibangun pada kerahasiaan, integritas dan ketersediaan dari tiga prinsip dasar. Kerahasiaan mengacu pada apa yang disebut dengan data aktual atau informasi yang tersembunyi, terutama pada daerah yang sensitive, kerahasian data berada pada persyaratan yang lebih ketat. Untuk komputasi awan, data disimpan di "pusat data", keamanan dan kerahasiaan data pengguna, merupakan hal yang penting.

Model keamanan data.

Berikut gambar model keamanan data pada Cloud Computing.



Gambar 3. model keamanan data

Sumber : (herwin:2011)

Model struktur yang digunakan adalah system pertahanan tiga tingkat. di mana setiap tingkat melakukan tugas masing-masing untuk memastikan keamanan data dari lapisan awan (cloud).

Lapisan pertama : bertanggung jawab untuk otentikasi pengguna, pengguna sertifikat digital yang diterbitkan oleh yang sesuai/berwenang, mengatur hak akses pengguna.

Lapisan kedua : bertanggung jawab untuk enkripsi data pengguna, dan melindungi privasi dari pengguna melalui cara tertentu;

Lapisan ketiga : Data pengguna untuk pemulihan sistem yang cepat, perlindungan sistem lapisan terakhir dari data pengguna.

Kesimpulan:

Sebagai pengembangan komputasi awan, masalah keamanan telah menjadi prioritas utama.Akhirnya kami menyimpulkan teknologi komputasi awan ini sangat tepat untuk menjaga keamanan data.

Daftar Pustaka

1. Anggeriana Herwin, Cloud Computing, 2011
2. Berkah I Santoso, Perkembangan Virtualisas, 2012
3. Berkah I Santoso, Cloud Computing dan Strategi TI Modern, 2012
4. Berkah I Santoso, Mobile Backend as a Services, 2012
5. Demystifying the Cloud An introduction to Cloud Janakiram MSV Cloud Computing Strategist www.janakiramm.net| mail@janakiramm.net
6. Llorente, I. M. (July 2008). Towards a new model for the infrastructure grid. *Panel From Grids to Cloud Services in the International Advanced Research Workshop on High Performance Computing and Grids, Cetraro, Italy*.
7. http://id.wikipedia.org/wiki/Komputasi_awan
8. http://infreemation.net
9. http://docs.google.com
10. http://www.biznetnetworks.com/En/?menu=cloudhosting
11. http://detik.com
12. http://www.salesforce.com
13. http://www.amazon.com
14. http://www.okezone.com
15. http://www.kompas.com
16. http://www.insw.go.id/
17. http://www.windowsazure.com/en-us/
18. http://www.chip.co.id
19. http://www.cloudindonesia.or.id
20. http://eliyaningsih.wordpress.com/2020/09/11/praktek-aplikasi-membuat-layanan-cloud-storage-sendiri-dengan-owncloud/
21. http://id.wikipedia.org/wiki/OwnCloud
22. http://owncloud.org/
23. www.youtube.com

24. http://www.hightech-highway.com
25. http://basingna.wordpress.com
26. http://kompas.com
27. http://techno.okezone.com