Cloud Computing

Chapter 5 : Keamanan Cloud

STMIK WIDYA PRATAMA PEKALONGAN

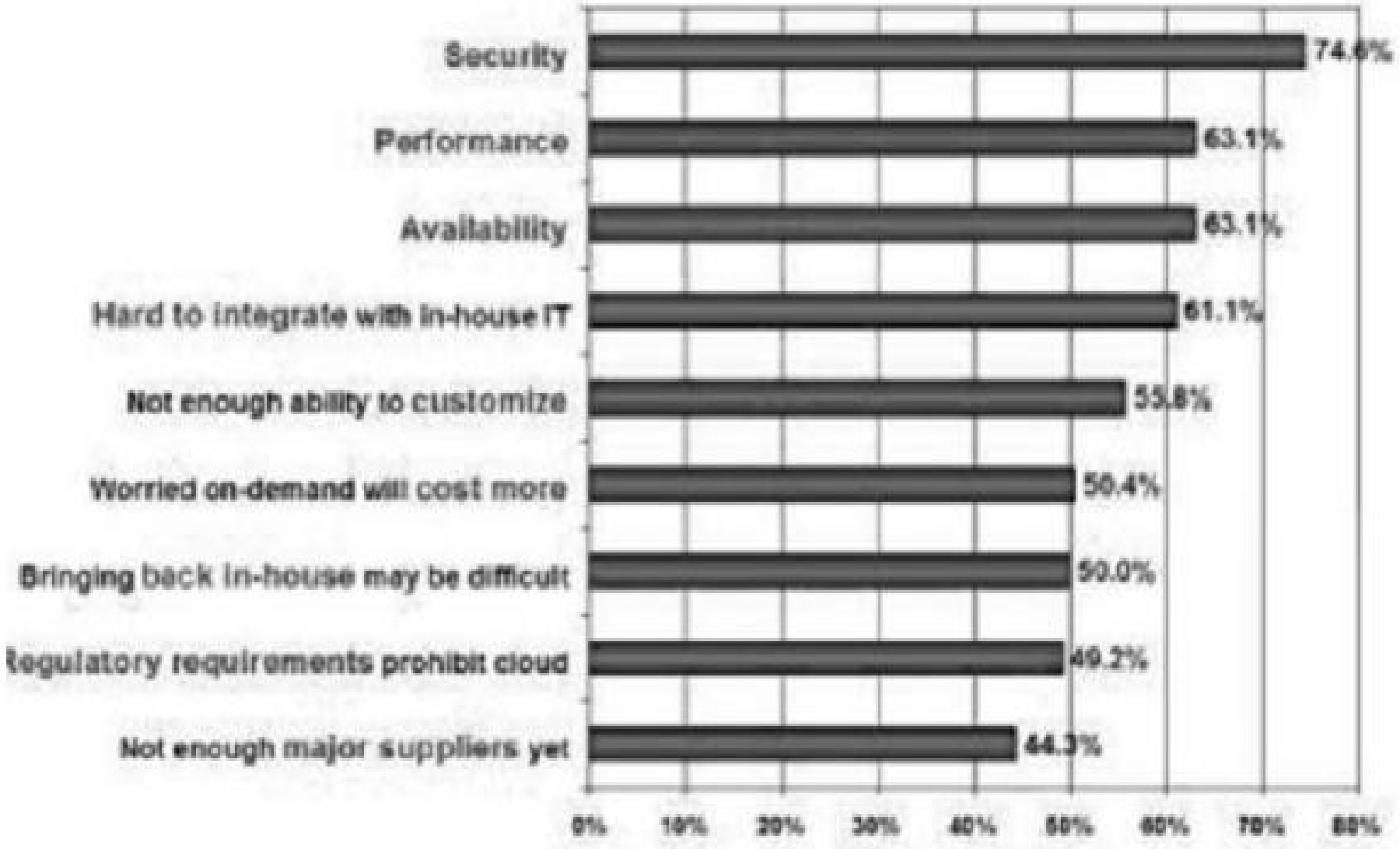
Pendahuluan

- Penyedia layanan Cloud harus terus belajar dan memastikan bahwa aplikasi dan data pelanggan mereka aman, jika mereka berharap untuk mempertahankan pelanggan dan daya saing.

- International Data Corporation (IDC) telah melakukan suvei kepada 244 CIO untuk mengukur pendapat mereka dalam menggunakan layanan teknologi awan.

- Hasil survei menunjukkan bahwa keamanan menduduki peringkat pertama sebagai tantangan dan masalah besar komputasi awan

Pendahuluan



Tantangan Keamanan Cloud

- Penyedia layanan awan memanfaatkan teknologi virtualisasi yang dikombinasikan dengan kemampuan layanan mandiri untuk menghitung sumber daya melalui Internet.

- 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.

Tantangan Keamanan Cloud

Ada beberapa kekhawatiran terhadap layanan cloud, yaitu :

1. Kehilangan kontrol atas keamanan fisik karena Anda berbagi sumber daya komputasi dengan perusahaan lain
2. Layanan Penyimpanan yang disediakan oleh satu vendor awan mungkin tidak kompatibel dengan layanan vendor lain
3. Jika informasi dienkripsi saat melewati awan (Cloud), siapa yang mengontrol kunci enkripsi/dekripsi? Apakah pelanggan atau perusahaan Cloud?

Tantangan Keamanan Cloud

4. Integritas data artinya : memastikan bahwa data yang identik dijaga selama operasi apapun (seperti transfer, penyimpanan, atau pengambilan).

5. Kecepatan aplikasi yang akan berubah dalam awan akan mempengaruhi SDLC (software development life cycle) dan keamanan. Maksudnya proses upgrade layanan mungkin mengakibatkan tidak kompatibel dengan data lama.

Masalah keamanan data Cloud Computing

- Masalah keamanan dari Virtual machine
- Keberadaan super user
- Konsistensi data

Masalah keamanan dari Virtual machine

- Teknologi virtual mesin membawa keuntungan yang nyata, ini memungkinkan pengoperasian server tidak lagi bergantung pada perangkat fisik.

- 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.

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.

- Jika super user terhack, maka data disimpan dalam platform komputasi awan mungkin dicuri.

Konsistensi data

- Lingkungan Awan (Cloud) merupakan lingkungan yang dinamis, dimana data pengguna mentransmisikan data dari data center kepengguna.
- Konsistensi terhadap data harus dijaga untuk memastikan bahwa data yang diinput adalah data yang benar-benar dari pengguna layanan.
- Biasanya mennggunakan ekripsi data

Tantangan Keamanan Cloud

- Karena adanya beberapa kekhawatiran akan masalah keamanan cloud computing, maka Gartner (perusahaan analis dan konsultan teknologi) memberikan 7 daftar hal yang perlu diperhatikan sebelum memilih perusahaan cloud, yaitu:
  1. Hak istimewa dari pengguna akses
  2. Kepatuhan terhadap peraturan
  3. Lokasi data
  4. Pembagian / pemisahan data
  5. Pemulihanan / pembaruan
  6. Bantuan investigasi / bantuan penyelidikan
  7. Kelayakan/kelangsungan jangka panjang

Hak istimewa dari pengguna akses

- Siapa yang memiliki akses khusus untuk data, dan tentang pengangkatan dan pengelolaan administrator tersebut.
- Apakah anda diberikan hak akses root / super user terhadap data Anda atau tidak?

Kepatuhan terhadap peraturan

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

Lokasi data

- Apakah penyedia layanan dalam hal ini perusahaan Cloud Computing melakukan pengendalian terhadap lokasi data.
- Apakah data Anda berada ditempat yang aman, di negara sendiri atau di negara lain,dsb

Pembagian / pemisahan data

- Pastikan bahwa enkripsi tersedia di semua tahapan, dan bahwa skema enkripsi dirancang dan diuji oleh para profesional berpengalaman.
- Pastikan bahwa data Anda tidak dapat tersadap dengan mudah ketika terjadi proses input/output

Pemulihanan / pembaruan

- Cari tahu apa yang akan terjadi pada data sewaktu terjadi bencana / kerusakan.
- Apakah 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.

Bantuan investigasi / bantuan penyelidikan

- Apakah vendor memiliki kemampuan untuk menyelidiki setiap kegiatan yang tidak patut atau ilegal?

Kelayakan/kelangsungan jangka panjang

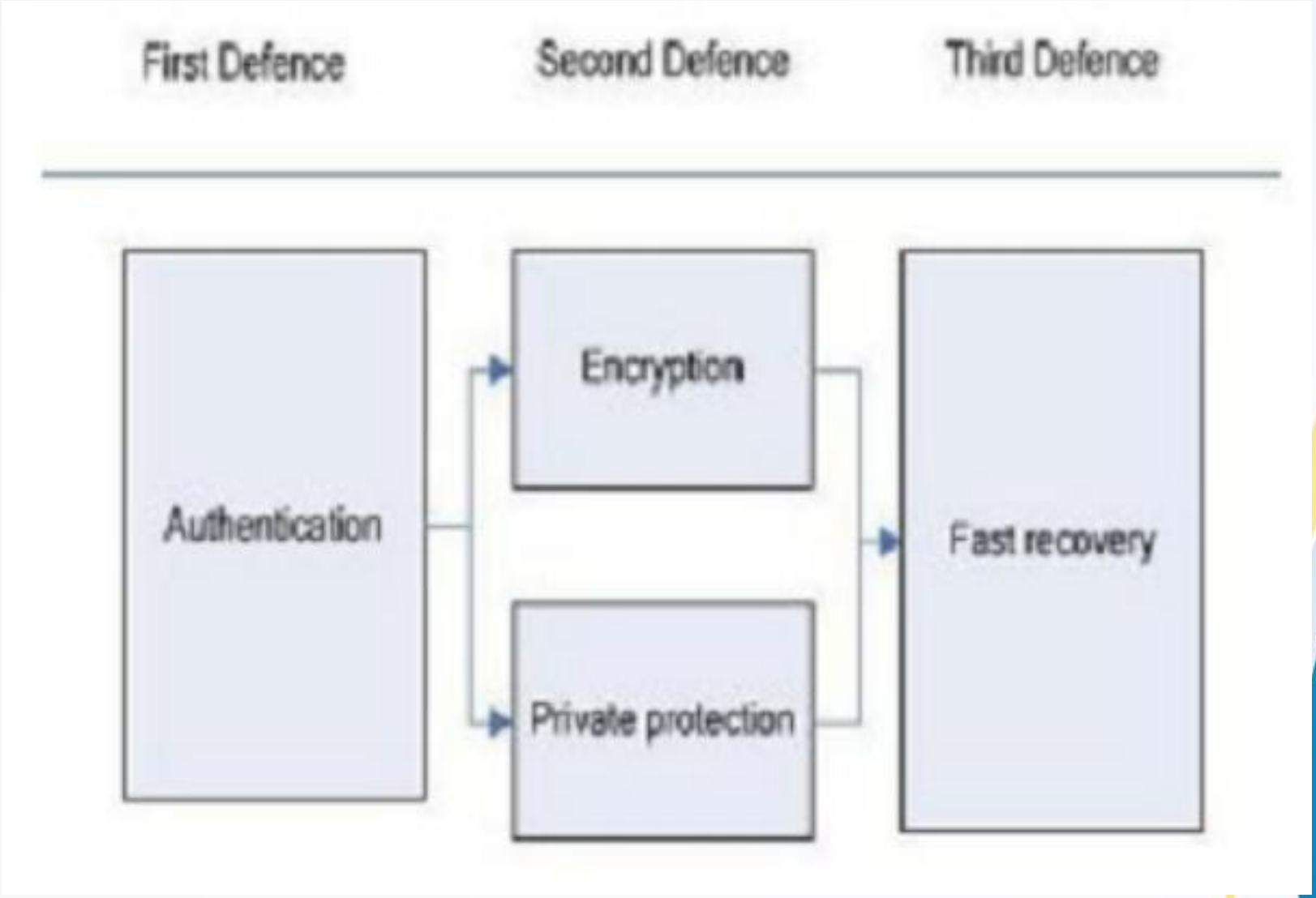
- Apa yang akan terjadi pada data jika perusahaan yang bersangkutan (vendor) keluar/berhenti dari bisnis? Bagaimana data yang dikembalikan, dan dalam format apa?

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



Model Keamanan Data

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

First Defence (Lapisan 1)

- Bertanggung jawab untuk otentikasi pengguna, pengguna sertifikat digital yang diterbitkan oleh yang sesuai/berwenang, mengatur hak akses pengguna.

Second Defence (Lapisan 2)

- Bertanggung jawab untuk enkripsi data pengguna, dan melindungi privasi dari pengguna melalui cara tertentu.
- Cara enkripsi yang paling umum dipakai adalah dengan menerapkan SSL (Secure Sockets Layer) protocol

Third Defence (Lapisan 3)

- Untuk pemulihan sistem yang cepat, perlindungan sistem lapisan terakhir dari data pengguna.