Cloud Computing Security

Josua M Sinambela, M.Eng
CEH, CHFI, ECSA|LPT, ACE, CCNP, CCNA, CompTIA Security+
Computer Network & Security Consultant,
Digital Forensic Investigator
Website: http://rootbrain.com

STIKOM BALI,
4 Mei 2013

Outline

- Intro Cloud Computing
- Cloud Computing Security
- Demo
- Diskusi

Intro Cloud Computing

- Bagi sebagian kalangan IT Professional, istilah “Cloud Computing” merupakan “Hype”
- “Cloud Computing” merupakan tema atau topik yang sangat luas
- Kita tidak mungkin membahas seluruh isu isu keamanan “cloud computing” dalam 1 jam.
- Setiap orang dapat memiliki pengertian yang berbeda tentang Cloud Computing

Intro Cloud Computing

- Beberapa contoh yang disebut “Cloud Computing” antara lain:
  - Amazon Web Services : Cloud (EC2), Amazon Simple Storage Service (S3), dll)
  - Rackspace Cloud
  - Google’s App Engine
  - Windows’ Azure
  - Outsourced Campus Email (Google Edu atau Live.Edu)
  - Outsourced Spam Filtering (Postini or Ironport)
  - Penggunaan Teknologi Virtualisasi (Vmware/Xen/Proxmox) untuk hosting private server atau outsourced VPS
  - Internet /Web Based Application (SocialNetwork:Facebook/Twitter/G+, Storage:Dropbox, GoogleDrive, Live SkyDrive)
- Meskipun beberapa diantara teknologi diatas, ada yang sama sekali tidak menggunakan istilah “Cloud Computing” pada informasi layanan mereka

Berdasarkan Jenis “Cloud Computing”

Cloud Applications Software-as-a-Service	  
Cloud Software Development Platform-as-a-Service	  
Cloud-based Infrastructure Infrastructure-as-a-Service	      

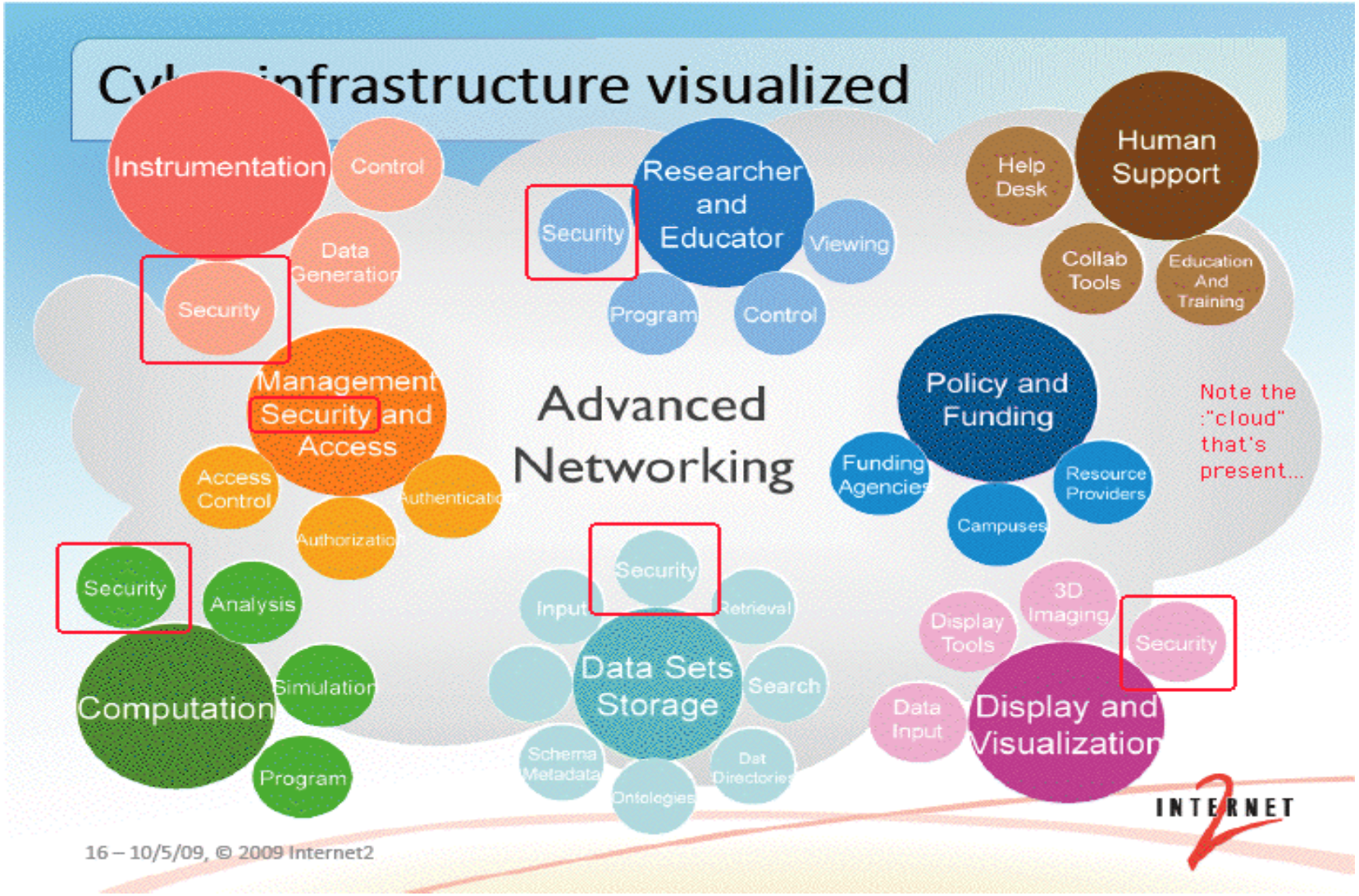
Pengertian Cloud Computing

- Pemahaman karakteristik Cloud Computing yang diterima secara umum (public cloud):
  - Memiliki biaya rendah atau bahkan Nol untuk Capex Awal (Capital Expenditure Costs)
  - Mengurangi secara drastis biaya dan tanggungjawab operasional ICT (Misalnya: jika Mesin atau HDD Server rusak, kita tidak perlu memperbaikinya)
  - Menawarkan elasticity dan scalability: Jika diawal kita hanya membutuhkan 1 Core CPU, kemudian tiba tiba membutuhkan 50 Core CPU karena kebutuhan komputasi yang meningkat, tidak masalah, dapat dengan mudah di berikan oleh provider , demikian juga jika kebutuhan resource tersebut ingin diturunkan, dapat dengan mudah disesuaikan dengan kebutuhan)

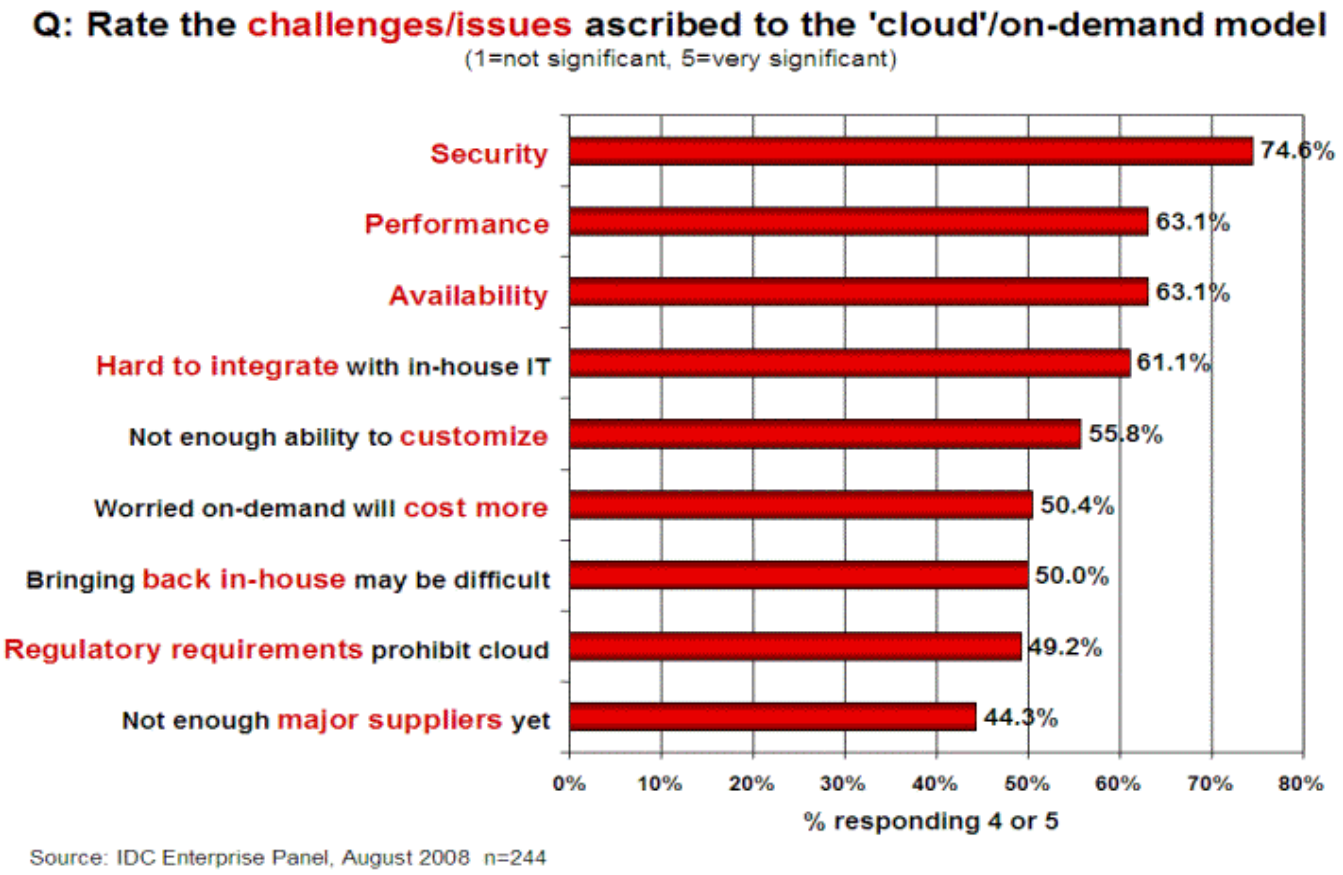
Pengertian Cloud Computing

- Karakteristik Private Cloud:
  - Capex awal akan cukup besar
  - Tanggung jawab dan biaya operasional mungkin masih tetap tinggi (Jika ada Hardware sptHDD yang rusak, tetap harus diperbaiki/diganti tim dari instansi kita sendiri)
  - Jika pada public cloud resource yang bisa digunakan dapat unlimited/sangat besar, tetapi pada private cloud pasti jauh lebih terbatas.

Perhatian Security pada Cloud



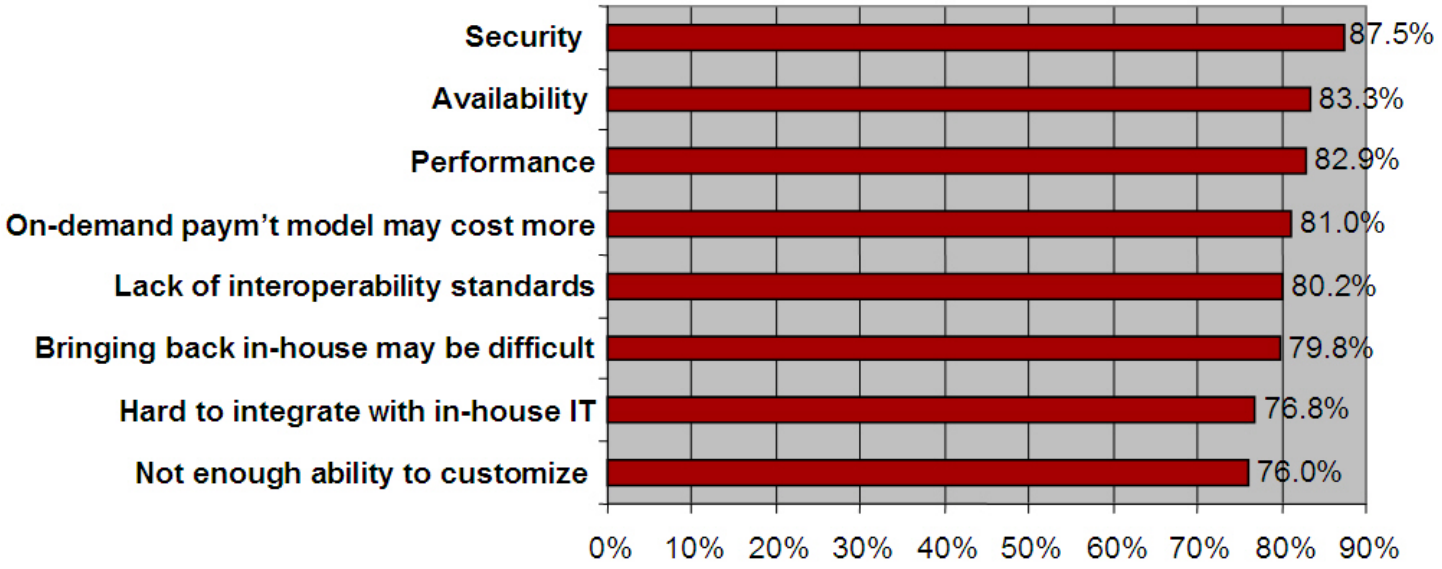
Survey Tantangan Cloud Computing



"The number one concern about cloud services is *security*."

Frank Gens, IDC, Senior VP & Chief Analyst

Key Challenges/Issues to the Cloud/On-demand Model



Source: Source: IDC eXchange, "New IDC IT Cloud Services Survey: Top Benefits and Challenges," (http://blogs.idc.com/ie/?p=730) December 2009

Cloud Computing Security

- Secara umum “Cloud Computing Security” tidak berbeda dengan IT/Network Security secara umum yang mungkin sudah biasa didiskusikan.
- Semua jenis ancaman atau serangan yang ditemukan pada sistem “tradisional/konvensional”, masih tetap menjadi ancaman pada Cloud Computing. Misalnya Web Security Vulnerabilities yang disebut pada OWASP mulai SQL injection, cross site scripting (XSS), cross site request forgeries (CSRF), dll. Atau bahkan ancaman teknik lain mulai penyadapan, scanning, remote exploit, bruteforce dll juga masih bisa terjadi. Ancaman keamanan fisik juga masih tetap sama, karena bisa saja diakses oleh pihak pihak yang tidak terotorisasi, hanya saja mungkin sudah menjadi tanggung jawab provider untuk bagian pengamanan fisik tersebut.

Cloud Computing Security

- Pada Prinsip IT Security, terdapat 3 yang menjadi objectives dasar yakni “C” “I” “A”
  - Confidentiality
  - Integrity
  - Availability
- Kesimpulan dari merangkum berbagai kasus di media akhir akhir ini, tantangan paling besar pada cloud computing saat ini adalah “Availability”
- Padahal hampir setiap provider Cloud memberikan jaminan “Availability” yang tinggi pada clientnya

Friction > Cobblers

Cloudflare reveals details of 'world's biggest' cyber attack

Open DNS recursors are a problem

By **Egan Orion**

Thu Mar 28 2013, 10:26

INTERNE
Cloudflare
about the
Spamhaus
nearly to

In a post
Cloudflare
events wh
Spamhaus
an attack against its spam blocking service that alle
gangs" in Eastern Europe and Russia at the behest
Cyberbunker.

Cloud Computing di Indonesia Rentan Serangan DDoS

Achmad Rouzni Noor II - detikinet

Senin, 12/03/2012 15:39 WIB

Ilustrasi (Ist.)

Jakarta - Salah satu tantangan dalam menjalankan cloud computing di Indonesia adalah menjaga keamanan data pelanggan. Terlebih, Indonesia ada di posisi nomor dua untuk negara yang sering diserang Distributed Denial of Service (DDoS).

Tak pelak, cloud yang sedang merangkak tumbuh perlu perlindungan keamanan yang maksimal. Apalagi, cloud diyakini bakal menjadi primadona di semua sektor, mulai dari enterprise hingga kalangan usaha kecil dan menengah (UKM).

Bagi perusahaan jasa keamanan internet, kondisi ini justru jadi peluang emas. Itu sebabnya, perusahaan CQ Cloud yang didirikan di Korea Selatan dengan basis operasi di Amerika Serikat, tak ragu-ragu menjejakkan kakinya di Indonesia.

"Kami baru saja mendirikan CQ Cloud Indonesia beberapa minggu lalu," ungkap CEO CQ Cloud, Heon Soo Rhee di Jakarta, Senin (12/3/2012).

Amazon cloud down; Reddit, Github, other major sites affected

Summary: *Major sites are experiencing trouble as Amazon's infrastructure fails on the East Coast. Reddit, Github, Airbnb, and others are suffering as a offline.*

By Zack Whittaker for Between the Lines | Octobe

Follow @zackwhittaker

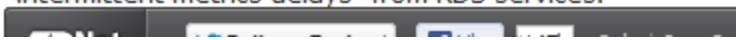
Another day, another Amazon outage, it seems, taking do getting worse, according to the cloud provider's status pa

The retail turned cloud giant is suffering with issues on the Amazon's North Virginia data center, after the firm's cloud

The firm's EC2 operations appear to be the main source of status page. Dubbed "performance issues," Amazon has y this article was written, the troubles appear to have sprea

At first the Elastic Compute Cloud crumbled and the Relati then spread through the data center to hit ElastiCache se

At 4:00 p.m. PT, when this article was last updated, only A running. Amazon CloudWatch was also operating normally "intermittent metrics delays" from RDS services.



Cloud services coming under increasing DDoS attack

News James Stirling, January 29, 2013

New report sheds light on cyber criminals targeting cloud-based infrastructure

Cloud services and data centres are coming under increasing attacks from hackers and defending such infrastructure against the bad guys remains an uphill struggle.

DDoS threats are changing from clumsy battering rams into sophisticated, long-lived, multi-vector attacks, according to the eighth Worldwide Infrastructure Security Report by IT security firm Arbor Networks.

Nearly half of research respondents experienced DDoS attacks targeted at their data centres during the survey period.What's more, some 94 per cent of these respondents reported seeing DDoS attacks regularly.

As more companies move their services to the cloud, they now have to be wary of the shared risks and the potential for collateral damage, according to Arbor

Ancaman Keamanan dari Cloud Computing

- “Cloud Computing” membawa ancaman baru untuk Keamanan
- Pada sistem keamanan sistem server konvensional (tradisional), umumnya yang dijaga adalah agar penyerang tidak dapat masuk ke dalam sistem
- Untuk itu penyerang (attacker) harus mampu menyusup dengan berbagai serangan pada otentikasi atau otorisasi/access control, atau mendapatkan secara ilegal account user lain.
- Sedang pada “Cloud Computing”, attacker yang dapat bertindak sebagai pelanggan yang juga memiliki hak atau akses ke mesin yang sama dengan target.

Ancaman Keamanan dari Cloud Computing

- Tantangan untuk attacker:
  - Bagaimana mengetahui dimana lokasi mesin target (Cloud server mana)
  - Bagaimana cara agar attacker dapat hosting di mesin yang sama.
  - Bagaimana mendapatkan informasi informasi penting lainnya mengenai target
  - Exploitasi target

Ancaman pada Cloud Computing

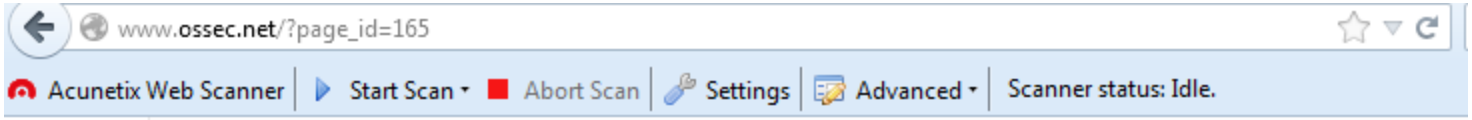
- Permasalahan Confidentiality
- Perilaku/attitude yang tidak baik dari pihak Provider
- Memahami resiko yang ada pada setiap industri yang mempraktekkan sistem oursourcing
- Provider dan Instrastrukturnya membutuhkan kepercayaan

Beberapa jenis serangan dan ancaman baru

- Ancaman-ancaman baru bertambah dari yaitu dari sesama pelanggan
- Server Virtualisasi pelanggan dan attacker dapat ditempatkan pada fisik mesin yang sama
- Serangan kolaborasi (DoS)
- Pemetaan internal cloud infrastructure
- Mengidentifikasi lokasi target Server Virtual target
- Cross-VM side-channel attacks
- Menggali informasi dari target pada mesin yang sama

HIDS (Host Intrusion Detection System)

- Meski infrastruktur Server menggunakan Cloud provider, bukan berarti kita menjadi tidak aware dalam keamanan sistem.
- Sebaiknya tetap memasang lapisan lapisan keamanan seperti Host IDS
- OpenSource HIDS seperti OSSEC (Ossec.net) mendukung aplikasi Cloud seperti Vmware ESX.



OSSEC Features

OSSEC is a full platform to monitor and control your systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring and SIM/SIEM together in a simple, powerful and open source solution. It is also backed and fully supported by Trend Micro.

Key Benefits

Compliance Requirements

OSSEC helps customers meet specific compliance requirements such as PCI, HIPAA etc. It lets customers detect and alert on unauthorized file system modifications and malicious behavior embedded in the log files of COTS products as well as custom applications. For PCI, it covers the sections of file integrity monitoring (PCI 11.5, 10.5), log inspection and monitoring (section 10) and policy enforcement/checking.

Multi platform

OSSEC lets customers implement a comprehensive host based intrusion detection system with fine grained application/server specific policies across multiple platforms such as Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac and Vmware ESX.

Real-time and Configurable Alerts

Demo