MODUL CLOUD COMPUTING DAN HL7 DALAM PELAYANAN KESEHATAN

SECURITY 2

PERTEMUAN 12 (ONLINE)

Disusun Oleh

Syefira Salsabila

National Institute of Standards and Technology (NIST) [6] mendefinisikan cloud computing sebagai model yang memungkinkan penggunaan *resource* bersama secara mudah, dimana – mana, dapat dikonfigurasi, dan on demand. NIST juga mengidentifikasi lima karakterisitk sehingga suatu layanan dapat dikatakan sebagai *cloud computing*, yaitu:

1. *On-demand self-service*. Pengguna dapat memesan dan mengelola layanan tanpa interaksi manusia dengan penyedia layanan, misalnya dengan menggunakan, sebuah portal web dan manajemen antarmuka. Pengadaan dan perlengkapan layanan serta sumber daya yang terkait terjadi secara otomatis pada penyedia.
2. *Broad network access*. Kemampuan yang tersedia melalui jaringan dan diakses melalui mekanisme standar, yang mengenalkan penggunaan berbagai platform (misalnya, telepon selular, laptop, dan PDA).
3. *Resource pooling*. Penyatuan sumberdaya komputasi yang dimiliki penyedia untuk melayani beberapa konsumen menggunakan model multipenyewa, dengan sumberdaya fisik dan virtual yang berbeda, ditetapkan secara dinamis dan ditugaskan sesuai dengan permintaan konsumen. Ada rasa kemandirian lokasi bahwa pelanggan umumnya tidak memiliki kontrol atau pengetahuan atas keberadaan lokasi sumberdaya yang disediakan, tetapi ada kemungkinan dapat menentukan lokasi di tingkat yang lebih tinggi (misalnya, negara, negara bagian, atau datacenter). Contoh sumberdaya termasuk penyimpanan, pemrosesan, memori, *bandwidth* jaringan, dan mesin virtual.

Semakin tinggi pohon maka semakin kencang pula angin yang menerpanya. Demikian pula yang terjadi pada metode penyimpanan cloud computing. Metode yang tengah naik daun untuk integrasi dan penyimpanan data ini kian menjadi perhatian para pengamat IT. Metode ini diperkirakan akan memiliki pengguna yang sangat luas, di masa yang akan datang, termasuk di Indonesia. Karenanya Cloud Computing harus benar-benar “dibedah” untuk mengetahui keuntungan dan kekurangan dalam implementasinya supaya dapat meminimalisir resiko yang mungkin akan muncul.

Di berbagai studi dan riset tentang pemanfaatan *cloud computing*, salah satu yang menjadi *concern* terbesar adalah terkait dengan faktor keamanan. Kita ketahui bersama, saat sebuah bisnis memilih untuk memanfaatkan layanan *cloud computing*, maka mereka bertaruh dengan sebuah kerpercayaan akan jaminan privasi dan keamanan data. Namun kini *cloud computing* sudah memiliki berbagai standar yang siap melindungi privasi dan keamanan data pengguna, yang juga menjadi jaminan rasa aman bagi pengguna.

Di Indonesia sendiri, layanan *cloud computing* yang umum digunakan ialah berkaitan dengan *cloud storage* dan *virtual machine*, untuk digunakan sebagai landasan sebuah aplikasi yang dijalankan secara online. Pemanfaatan tersebut juga sudah berkembang pesat, mulai digunakan sebagai *dedicated-hosting, hybrid solution* atau bahkan difungsikan sebagai *disaster recovery*. Untuk layanan SaaS (Software as a Services) sendiri, pengguna di Indonesia sudah sangat dimanjakan dengan berbagai produk vendor-vendor ternama dunia.Di tengah menggeliatnya pangsa pasar *cloud*

services, penting untuk dipahami oleh pengguna bisnis seputar langkah keamanan sebelum menentukan vendor *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).

Isu yang saat ini tengah beredar menyinggung mengenai keamanan dan privasi data pengguna. Keamanan yang dimaksud adalah keamanan data yang disimpan maupun beredar dalam cloud. Maraknya virus dan peretas data dalam jaringan internet menjadikan momok tersendiri bagi pengguna layanan, terutama perusahaan yang bergerak di bidang keuangan. Bagi setiap pengguna data tentunya merupakan hal yang penting dan sensitif. Karenanya hal ini menimbulkan kehawatiran pengguna yang kedua yaitu privasi. Setiap orang tentunya memiliki standar privasi yang berbeda, namun adanya penyimpanan data dalam bentuk digital membuat was-was dengan kemungkinan bahwa datanya dapat dengan mudah dilihat oleh orang lain.

Data yang disimpan dalam cloud sebenarnya jauh lebih aman daripada disimpan di dalam PC karena ada aturan yang mengharuskan setiap penyelenggara layanan cloud computing patuh terhadap regulasi dan aturan yang terkait. Salah satu aturan yang mengatur sitem keamanan untuk platform cloud adalah ISO 27002 (atau jika ada yang terbaru dapat ditambahkan), yang merupakan standar praktek keamanan informasi dan tingkat keamanan yang wajib dimiliki oleh penyedia jasa layanan cloud computing.

Privasi data yang diinginkan oleh pengguna difasilitasi dengan adanya identifikasi digital. Karenanya pengguna dapat menentukan siapa yang berhak untuk melihat dan melakukan perubahan informasi yang ada dalam cloud. Dengan adanya identifikasi digital dan sistem keamanan cloud, pengguna tidak perlu lagi khawatir lagi mengenai keamanan dan privasi data.

Untuk mengatasi isu seperti ini dibutuhkan aksi dari kedua belah pihak, yaitu penyedia jasa cloud dan pengguna itu sendiri. Penyedia jasa cloud harus dapat memastikan bahwa data yang dipercayakan untuk beredar dalam cloud terjamin keamanan dan privasinya. Salah satunya dengan memberikan informasi yang memadai dan memberikan edukasi pada calon pengguna saat akan berlangganan. Kehawatiran ini dapat terjadi salah satunya akibat minimnya pengetahuan pengguna mengenai teknologi keamanan di internet. Karena itu pengguna harus mencoba untuk mempelajari lebih lanjut mengenai layanan yang akan digunakan, baik untuk pribadi maupun korporasi. Biasakan untuk melakukan cek dan ricek mengenai isu yang beredar mengenai layanan yang digunakan. Tanyakan kepada orang yang kompeten di bidang IT untuk menjelaskan dan berbagi mengenai kekhawatiran anda. Dan satu hal yang terpenting adalah, pengguna harus memilih layanan penyedia jasa cloud computing yang sudah terpercaya.

Agar data kita terjamin/aman di simpan di awan/Cloud. Berikut ini adalah pokok-pokok yang yang terkait keamanan data pada Cloud.

1. **Proteksi Data**

   Ketika kita sudah memutuskan untuk adopsi atau migrasi data ke Cloud, yang yang diperhatikan adalah bagaimana penyedia layanan Cloud memberikan proteksi terhadap data kita. Dengan metode apa mereka melakukan proteksi sehingga kita yakin data aman, selain itu lokasi penyimpanan data juga adalah pertimbangan penting dimana ini hubungannya dengan Data Center. Dipastikan data center yang mereka buat sudah tersertifikasi/teraudit, misalnya lokasi bebas gempa, standar sumber saya listrik 3 lapis dll.

2. **Security Control**

   Setelah data kita betul-betul terproteksi, selanjutnya adalah bagaimana keamanan dari akses terhadap data kita (role), bagaimana prosedurnya sehingga hanya orang-orang yang berhak saja yang bisa akses data kita. Disini teramsuk akses para pekerja/karyawan di penyedia layanan terhadap data kita.

3. **Compliance**
   Standar yang diterapkan pada penyedia layanan Cloud Computing, misalnya untuk keamanan data menggunakan ISO 27001, untuk penyediaan layanan memakai ITIL, COBIT, Cloud Security Alliance, termasuk regulasi internasioanl dan pemerintah. Sehingga jika ada pelanggaran akan mudah dalam penyelesaian
4. **Multi-tenancy**
   Salah satu sifat Cloud computing adalah resource sharing, nah bagaimana ketika ada penyewa lain terdapat melakukan kecurangan atau bocor, apa imbasnya terhadap data kita disana, ini harus dipertimbangkan. Karena secara fisikal, data kita bisa jadi ada dalam satu media fisik yang sama dengan yang lain.

5. **Security Governance**

   Ini lebih kepada policy governance dari penyedia layanan atau kita sebagai pemakai layanan, harus dijabarkan dan governance-nya paka apa harus didefinisikan disni.

Isu yang lagi hangat di Indonesia adalah setiap penyedia layanan elektronik luar harus mempunyai data center di Indonesia, ini adalah salah satu regulasi pemerintah terkait peraturan data center. Sama juga dengan kita ketika ingin memindahkan data ke Cloud, pastikan data kita ada dimana, karena setiap negara mempunyai tersendiri dan cara melakukan data dan data center-nya sendiri.

Resiko Cloud Computing

Meskipun beralih ke Cloud Computing menawarkan banyak solusi, tetapi Cloud Computing bukan tanpa resiko atau benar-benar aman. Sebuah pemahaman menyeluruh dan mitigasi risiko keamanan merupakan langkah penting menuju implementasi dan pemanfaatan Cloud Computing. Gambar diatas menyajikan daftar risiko yang teridentifikasi.

Dengan aplikasi dan data yang dikelola oleh penyedia layanan, data tidak lagi di bawah kendali manajemen dan rentan terhadap ancaman keamanan dan kerahasiaan data. Hosting aplikasi dan data dalam infrastruktur bersama yang dikelola penyedia layanan meningkatkan potensi akses yang tidak sah seperti privasi karyawan, identitas manajemen, otentikasi, integritas, ketersediaan data, enkripsi, keamanan jaringan dan keamanan fisik.

Selain keamanan risiko, masalah lain termasuk SLA dan manajemen pihak ketiga (layanan penyedia), kualitas layanan, manajemen kontrol, beban kerja manajemen, kinerja, pengendalian perubahan, ketersediaan layanan, kurangnya monitoring dan manajemen peralatan, transparansi, kepatuhan terhadap hukum dan peraturan, portabilitas, kurangnya standar dan audit serta standard kelayakan Cloud Computing.

Berdasarkan wawancara tehadap responden mengenai penggunaan Cloud Computing, besarnya resiko keamanan dinilai mencapai 91,7 persen untuk pengimplementasian, perencanaan kelangsungan bisnis menjadi risiko kedua yang paling kritis, dengan nilai 66,7 persen. Standar, kebijakan dan kontrol untuk manajemen operasi, manajemen perubahan, pihak ketiga / layanan tingkat manajemen, interface management, dan peraturan perundang-undangan dinilai sebagai ‘agak penting ‘ untuk mitigasi risiko.

MITIGASI RISIKO KEAMANAN

Mitigasi risiko yang memadai merupakan strategi yang harus dikembangkan dan diikuti untuk memastikan risiko keamanan dan perlindungan data serta aplikasi pada cloud computing. Pengamanan yang tepat pada sistem dan perlindungan terhadap data bisnis yang berharga tetap menjadi tanggung jawab manajemen walaupun data dan sistem di-host di cloud dan dikelola oleh penyedia layanan.

a. **Data Security, Administration And Control**

   Keamanan data merupakan resiko penghalang terbesar untuk penerapan cloud computing. Beberapa bisnis masih enggan untuk pindah data dan aplikasi ke cloud, terutama data yang sangat penting untuk bisnis, karena risiko kebocoran data rahasia yang mengarah ke privasi (A1), kurangnya kontrol atas data dan aplikasi (A2), ketersediaan data pada layanan cloud (A3), risiko penurunan integritas data (A4), dan perlindungan yang tidak efektif dalam transmisi data, back-up karena enkripsi yang tidak memadai (A5). Keamanan data, administrasi, pengendalian risiko dan rekomendasi untuk mitigasi risiko.

b. **Logical Access**
   Risiko akses tidak sah ke data dan aplikasi di cloud dan rekomendasi untuk mitigasi resiko ini secara rinci dalam tabel III. Akses melalui jaringan publik dan host layanan berarti lebih meningkatan eksposur dan risiko. Keistimewaan hak akses (B1) harus diserahkan dengan hati-hati untuk pengguna yang berwenang saja, dan ditinjau secara berkala. Dibutuhkan teknik dan penggunaan tools keamanan untuk menjamin bahwa pengguna yang berwenang saja yang dapat mengakses data dan aplikasi(B2).

c. **Network Security**
   Risiko keamanan jaringan termasuk peningkatan risiko hacking dan intrusi (C1), perimeter kebijakan keamanan (C2) dan ancaman menggunakan perangkat mobile (C3).

d. **Physical Access**
   Dengan hilangnya perimeter pusat data fisik, penyerang bisa mendapatkan akses ke data dan aplikasi dari mana saja di jaringan (D1).

e. **Compliance**
   Walaupun sumberdaya berada pada penyedia layanan cloud computing, perusahaan tetap bertanggung jawab untuk memastikan keamanan dan integritas data mereka..

Berikut ini adalah lima langkah keamanan yang harus dilakukan sebelum bergabung dengan layanan cloud.

a. Memahami lingkup cloud

   Terdapat tiga segmen utama di setiap cloud deployment - yaitu cloud vendor, penyedia layanan jaringan dan dunia usaha. Menyadari bahwa cloud harus ditangani seperti perpanjangan pusat data dunia usaha, maka terdapat pertanyaan yang perlu dijawab, yaitu: apakah layanan dan kebijakan keamanan yang umum dapat diterapkan di ketiga segmen? Apa saja celah keamanannya?

Dalam pemilihan vendor, tanyakan kepada cloud vendor mengenai layanan keamanan yang disediakan dan vendor keamanan yang diajak bekerjasama. Cloud adalah lingkungan yang dinamis yang membutuhkan pemuktahiran yang teratur pada arsitektur keamanannya sehingga dapat mengikuti perkembangan ancaman terkini. Bagaimanakah cloud vendor dapat mengatasi ekploitasi keamanan baru serta memastikan kekokohan sistem keamanannya sepanjang tahun?

Cari tahu mengenai batas-batas dalam model keamanan bersama yang datang dengan layanan cloud. Pahami jangkauan tanggung jawab penyedia cloud – serta tanggung jawab Anda. Pada beberapa layanan cloud, seperti IaaS, tanggung jawab untuk mengamankan aplikasi dan data yang berada di cloud berada di tangan dunia usaha. Oleh sebab itu, penting untuk mengetahui apa saja perangkat keamanan dan apa saja yang ditawarkan/disediakan oleh vendor penyedia cloud kepada dunia usaha guna mempersiapkan cloud.

b. Aplikasi baru, pertahanan baru

Siap untuk memindahkan aplikasi ke cloud? Sebelumnya, pertimbangkan untuk menambahkan pertahanan baru ke langkah-langkah keamanan yang telah Anda bangun di sekeliling proses otentifikasi dan log-in aplikasi Anda. Untuk memperkokoh akses ke aplikasi cloud Anda, anda sebaiknya memiliki skema akses data granular. Anda dapat melakukannya dengan membatasi hak akses sesuai dengan peran, jawabatan di perusahaan dan proyek. Hal ini akan memberikan lapisan perlindungan tambahan ketika penyerang berusaha mencuri identitas login staf Anda.

Pembajakan akun mungkin terkesan biasa saja saat ini, namun pelanggaran model lama ini tetap dinilai sebagai ancaman utama bagi pengguna cloud. Untuk memperkokoh proses login Anda, pertimbangkan untuk menerapkan otentifikasi dua faktor, pemeriksaan postur dan penggunaan kata sandi yang hanya dapat digunakan satu kali saja. Salah satu tip yang berguna adalah membuat persyaratan untuk mengubar user ID pada login awal.

c. Menggunakan enkripsi

Enkripsi data adalah sekutu keamanan terbesar Anda di cloud, dan hal ini harus digunakan setiap kali melakukan transfer file dan email. Meskipun hal ini tidak akan mencegah upaya perentasan atau pencurian data, hal ini dapat melindungi bisnis Anda dan menyelamatkan organisasi dari denda peraturan ketika terjadi perentasan.

Tanyakann pada vendor cloud Anda mengenai skema enkripsi data mereka. Cari tahu bagaimana skema tersebut akan mengenkripsi data yang tidak aktif, tidak sedang digunakan, dan sedang dipindahkan. Untuk memahami data apa saja yang sebaiknya dienkripsi, maka akan bermanfaat untuk mengetahui

dimanakah data tersebut berada – apakah di server cloud vendor Anda, di server perusahaan pihak ketiga, laptop karyawan, PC kantor atau di USB.

d. Pergulatan dengan dunia virtual

Berpindah ke cloud memampukan bisnis untuk menuai manfaat dari virtualisasi, tetapi lingkungan virtualisasi dapat menghadirkan tantangan dalam perlindungan data. Isu utama terkait dengan pengelolaan keamanan dan traffic di ranah multi-tenancy dan mesin virtual.

Perangkat kemananan fisik bisanya tidak dirancang untuk mengatasi data yang berada di cloud. Ini sebabnya mengapa perangkat keamanan virtual dibutuhkan – untuk mengamankan traffic yang mengalir dari mesin virtual ke mesin virtual. Perangkat seperti ini dibangun untuk mengatasi kompleksitas dalam menjalankan berbagai aplikasi secara simultan, atau multi-tenancy.

Oleh sebab itu, perangkat ini memungkinkan bisnis untuk mengerahkan kontrol keamanan yang baik terhadap data yang dimiliki di cloud. Tanyakan kepada penyedia cloud mengenai cara mereka mengamankan lingkungan virtual mereka dan cari tahu mengenai perangkat keamanan vitual yang digunakan. Jika Anda sedang membangun cloud pribadi atau hybrid, pertimbangkan untuk menggunakan produk keamanan virtual yang berfokus pada kontrol granular.

e. Jangan menutup mata terhadap shadow IT

Terdapat banyak anekdot dan laporan di luar sana yang menunjukkan bagaimana penggunaan layanan aplikasi dan cloud tanpa otorisasi, atau shadow IT, semakin meningkat di dunia bisnis. Sifat yang tidak terkontrol ini menghadirkan ancaman keamanan dan tantangan pengelolaan.

Aplikasi cloud baru Anda akan terancam karena hal ini. Pertimbangkan skenario sederhana ini dimana karyawan Anda menggunakan smartphones mereka untuk membuka file di perangkat mereka. Kemungkinan telefon tersebut akan menyalin file tersebut, yang dapat dikirimkan ke tujuan penyimpanan online yang tidak disetujui saat telefon melakukan proses backup otomatis secara teratur. Data perusahaan Anda yang aman baru saja dipindahkan ke lokasi yang tidak aman

Mencegah akses ke shadow IT kecil kemungkinannya dapat menghentikan pertumbuhannya di organisasi apapun. Pemberian pemahaman kepada pengguna dan penggunaan teknologi untuk mengatasi isu tersebut akan menjadi cara yang lebih efektif. Enkripsi, alat monitoring jaringan dan pengelolaan keamanan dapat membantu melindungi aplikasi cloud pertama Anda dari risiko shadow IT.

Cara Menjaga Keamanan Sistem IT

Teknologi terus maju dan berkembang seiring dengan berjalannya waktu. Dengan berkembangnya teknologi tersebut, banyak keuntungan yang didapatkan oleh manusia. Seperti, dapat membantu mempercepat pekerjaan manusia, meningkatkan kualitas dan kuantitas layanan, mempermudah proses transaksi keuangan, dan lainnya. Tidak hanya dilihat dari segi keuntungannya saja, namun segi keamanan teknologi itu sendiri juga harus diperhatikan. Untuk mendukung hal tersebut, Anda harus mengetahui 10 cara agar Keamanan sistem IT Anda terjaga, sebagai berikut ini:

1. ***Protect with passwords***

   Banyak serangan cyber yang berhasil meretas karena kata sandi (*password*) yang lemah. Semua akses ke jaringan maupun data, sangat sensitif dan harus dijaga dengan nama pengguna dan kata kunci yang unik. Sandi yang kuat berisi angka, huruf dan simbol. Disarankan untuk setiap pengguna menggunakan kata sandi yang unik.

2. ***Design safe systems***

   Batasi akses ke infrastruktur teknologi Anda untuk mencegah mudahnya peretas dan pencuri merusak sistem Anda. Hilangkan akses yang tidak perlu ke hardware maupun software Anda, dan batasi hak akses pengguna hanya untuk peralatan dan program yang dibutuhkan saja. Bila memungkinkan, gunakan juga alamat email, login, server dan nama domain yang unik bagi setiap pengguna, kelompok kerja maupun departemen.

3. ***Conduct screening and background checks***

   Melakukan skrining dan pemeriksaan latar belakang pada karyawan perlu dilakukan. Sama halnya dengan meneliti kredibilitas mereka juga. Pada periode percobaan awal, akses terhadap data sensitif atau jaringan yang mencurigakan yang dilakukan oleh karyawan Anda harus dilarang dan juga dibatasi, agar sistem IT Anda menjadi aman.

4. ***Provide basic training***

   Pelanggaran keamanan yang tak terhitung jumlahnya kerap terjadi sebagai akibat kesalahan dan kecerobohan manusia. Anda dapat membantu dengan membangun budaya perusahaan yang menekankan pada keamanan komputer melalui program pelatihan yang memperingatkan berapa besarnya risiko pada penggunaan kata sandi, jaringan, program dan perangkat yang ceroboh.

5. ***Avoid unknown email attachements***

Jangan pernah mengklik lampiran email yang tidak dikenal, yang kemungkinan bisa berisi virus komputer. Sebelum membukanya, hubungi pengirim untuk mengkonfirmasi isi pesan. Jika Anda tidak mengenal pengirim tersebut, baiknya Anda menghapus pesan, memblokir akun pengirim yang tidak dikenal, dan memperingatkan orang lain untuk melakukan hal yang sama.

6. ***Hang up and call back***

   Jika Anda menerima panggilan dari orang yang tidak dikenal yang tiba-tiba ingin memberikan hadiah dan berpura-pura hadiah itu diberikan oleh perwakilan dari bank atau mitra lainnya, segera akhiri panggilan yang tidak dikenal tersebut. Kemudian hubungi kontak langsung ke organisasi tersebut, atau salah satu nomor call centernya untuk mengkonfirmasi bahwa panggilan yang Anda terima tersebut sah/tidak.

7. ***Think before clicking***

   Untuk menghindari penipuan yang terjadi melalui email yang meminta informasi nama pengguna, kata sandi atau informasi pribadi, Anda harus mempertimbangkannya kembali agar Anda tidak terdorong ke sebuah situs web palsu yang mendorong calon korban untuk memasukkan data mereka sendiri.

8. ***Use a virus scanner, and keep all software up-to-date***

   Baik Anda bekerja di rumah atau di jaringan kantor, disarankan untuk menginstal antivirus pada PC Anda. Banyak penyedia jaringan sekarang menawarkan aplikasi antivirus secara gratis. Di samping itu, menjaga perangkat lunak agar terus *up-to-date* juga mampu mencegah virus masuk dan membuat keamanan sistem IT Anda terjaga.

9. ***Keep sensitive data out of the cloud***

   Cloud computing menawarkan banyak manfaat dan penghematan biaya kepada bisnis Anda. Namun layanan semacam itu juga dapat menimbulkan ancaman tambahan karena data ditempatkan di server jarak jauh yang dioperasikan oleh pihak ketiga yang mungkin memiliki masalah keamanan tersendiri.

10. ***Stay paranoid***

    Rusak atau robek semua hal termasuk dokumen dengan nama perusahaan, alamat dan informasi lainnya, termasuk logo vendor dan bank yang sedang ingin berurusan dengan Anda. Jangan pernah meninggalkan laporan yang bersifat penting dan sensitif di meja Anda. Ubah juga kata sandi secara teratur dan sering, terutama jika Anda membaginya dengan rekan kerja Anda. Hal ini sangat penting Anda lakukan, untuk membuat keamanan sistem IT Anda terjaga.

Peraturan di Indonesia

Berdasakan definisi yang pada awal tulisan, dapat dilihat bahwa *cloud computing* dapat digunakan oleh pribadi, kelompok, perusahaan, maupun pemerintahan. Pengguna memiliki kebebasan terhadap layanan *cloud computing* yang dipakainya. Namun, kebebasan tersebut perlu dibatasi terutama hal-hal yang berkaitan dengan keamanan negara atau data-data rahasia. Oleh karena itu, perlu aturan yang membatasi penggunaan *cloud computing*.

Indonesia merupakan negara hukum, setiap tindakan kejahatan ada UU yang mengaturnya, salah satunya di dunia cyber. Beberapa peraturan berikut yang sesuai dengan kejahatan yang dilakukan di atas dan dapat menjerat pelaku peretasan adalah sebagai berikut:

Undang-undang yang mengatur mengenai peretasan

UU nomor 11 tahun 2008 tentang informasi dan transaksi elektronik dan UU no 19 tahun 2016 tentang perubahan UU No 11 tahun 2008.

1. pasal 30 ayat (1,2, dan 3) yaitu :

   (1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun.

   (2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.

   (3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apapun dengan melanggar, menerobos, melampaui atau menjebol sistem pengamanan.

   Maka berdasarkan pasal 30 (1) UU-11-2008 tindak pidana apabila memenuhi unsur sebagaimana maksud dalam pasal 30 ayat (1) adalah dengan ancaman pidana maksimum 6 tahun denda maksimum Rp. 400.000.000 Pasal 46 [1] .

   Maka berdasarkan pasal 30 (2) UU-11-2008 tindak pidana apabila memenuhi unsur sebagaimana maksud dalam pasal 30 ayat (2) adalah dengan ancaman pidana maksimum 7 tahun denda maksimum Rp. 600.000.000 Pasal 46 [2] .

   Maka berdasarkan pasal 30 (3) UU-11-2008 tindak pidana apabila memenuhi unsur sebagaimana maksud dalam pasal 30 ayat (3) adalah dengan ancaman pidana maksimum 8 tahun denda maksimum Rp. 800.000.000 Pasal 46 [3] .

2. **Pasal 31 Ayat (1, dan 2) yaitu :**

(1) Setiap orang dengan sengaja dan atau tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas informasi elektronik dan/atau dokumen elektronik dalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi informasi elektronik atau dokumen elektronik yang tidak bersifat publik dari, ke, dan didalam suatu komputer dan/atau sistem elektronik tertentu milik orang lain, baik yang tidak menyebabkan adanya perubahan, dan/atau penghentian informasi elektronik dan/atau dokumen elektronik yang sedang ditransmisikan.

Maka berdasarkan pasal 31 (1) dan (2) UU-11-2008 tindak pidana apabila memenuhi unsur sebagaimana maksud dalam pasal 31 ayat (1) dan (2) adalah dengan ancaman pidana maksimum 10 tahun denda maksimum Rp. 800.000.000 Pasal 47 .

3. **Pasal 32 Ayat 1 yaitu :**

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu informasi elektronik dan atau dokumen elektronik milik orang lain atau milik publik. Perbuatan tersangka yang melakukan tindak pidana cracking melalui botnet telah memenuhi unsur subjektif

Pasal 32 ayat (1) dan pasal 32, maka berdasarkan Pasal 48 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik : Setiap orang yang memenuhi unsur sebagai mana dimaksud dalam Pasal 32 ayat (1) dipidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp. 2.000.000.000,00 (dua miliar rupiah).

4. **Pasal 33 :**

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya sistem elektronik dan atau mengakibatkan sistem elektronik menjadi tidak bekerja sebagaimana mestinya.

Berdasarkan Pasal 49 UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, setiap orang yang sebagaimana dimaksud dalam Pasal 33, dipidana dengan penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp. 10.000.000.000,00 (sepuluh miliar rupiah).

Isu dan Risiko Privasi Data

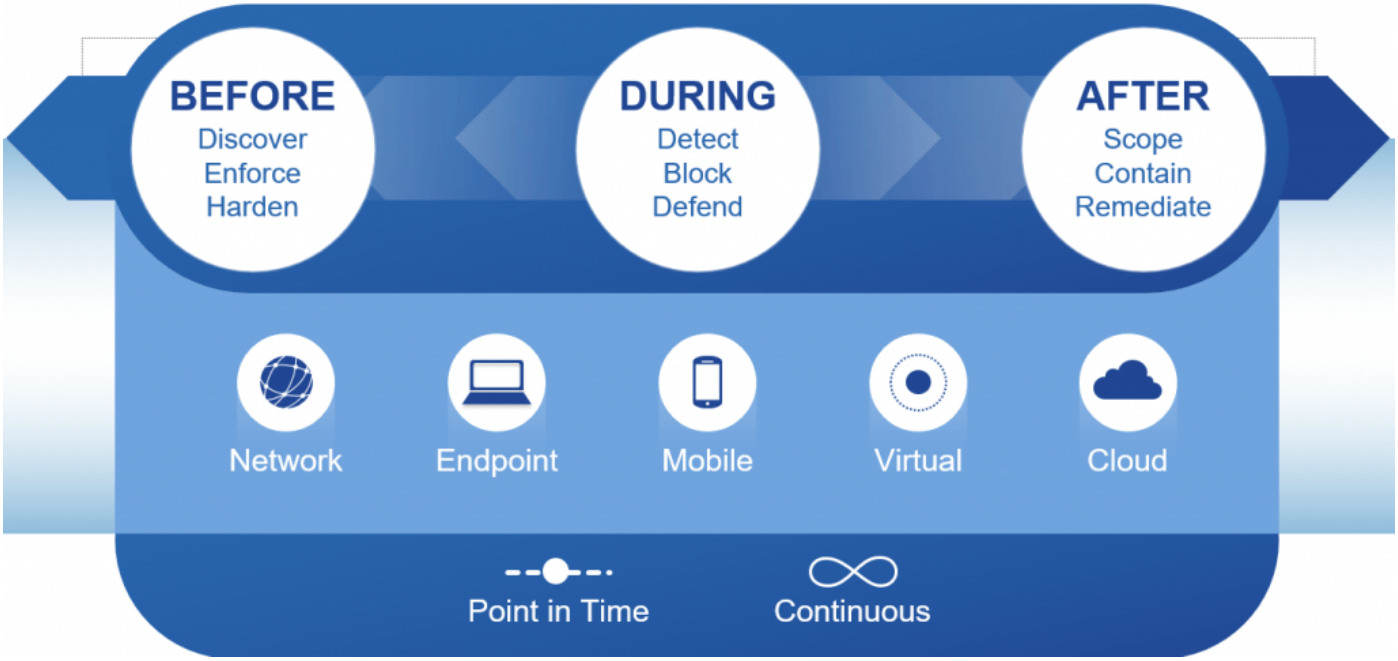
Infrastruktur *cloud computing* yang memungkinkan akses dan penggunaan secara bersama menimbulkan masalah privasi data, termasuk konsekuesi hukum akibat adanya penyimpangan penggunaan terhadap informasi rahasia suatu bisnis. Dengan menyediakan penyimpanan data secara bersama, meningkatkan kerentanan data sedang diakses atau disalin oleh orang yang tidak berhak. Ancaman privasi data dapat berasal dari pihak internal (penyedia layanan, pengguna dalam perusahaan), dan kebocoran data bisa terjadi karena kegagalan hak akses keamanan di beberapa domain.

Konsep privasi sangat berbeda dalam konteks negara, budaya atau yurisdiksi. Definisi yang diadopsi oleh Organisasi Kerjasama Ekonomi dan Pembangunan (OECD), privasi adalah informasi yang berkaitan dengan individu yang diidentifikasi (subjek data). D. Chen dan H. Zhao secara umum mengidentifikasi isu privasi ke dalam *data life cycle* yang terdiri dari pengumpulan, penggunaan, pengungkapan, penyimpanan, dan penghancuran data pribadi.

Isu privasi dari sudut pandang yang berbeda. Mereka melihat isu privasi ini dari dua sisi yaitu sisi pengguna cloud dan penyedia layanan cloud itu sendiri atau yang lebih dikenal dengan *cloud service provider*. Masing-masing sudut pandang tersebut memiliki fokus yang berbeda dalam melihat keamanan privasi data tersebut. Dari sudut pandang pengguna layanan cloud itu sendiri harus mempertimbangkan beberapa hal penting seperti : kontrol terhadap sistem dan data, menciptakan fasilitas untuk penggunaan banyak identitas dan membatasi informasi identitas serta autentifikasi untuk transaksi tingkat tinggi atau yang dianggap penting. Semua hal tersebut yang harus dijamin bagi seorang individu agar privasi informasi yang disampaikan kepada cloud provider dapat dipastikan aman.

Sedangkan bagi *cloud service provider* itu sendiri, beberapa hal yang harus diperhatikan diantaranya menyediakan fasilitas untuk mengelola data pribadi pengguna, enkripsi untuk setiap data yang menyimpan informasi pribadi pengguna, pengolahan dan penyimpanan data, mengendalikan pengidentifikasi unik, mengelola eksplisit persyaratan privasi dan keamanan antara penyedia layanan awan. Menurut G. Zhang dan Y. Yang, isu privasi dalam CSP terdapat di dalam semua level *cloud environment* yang terdiri dari *cloud service application level, application platform level, cloud management platform level, physical computing, VM management platform level*, dan *storage and network level*.

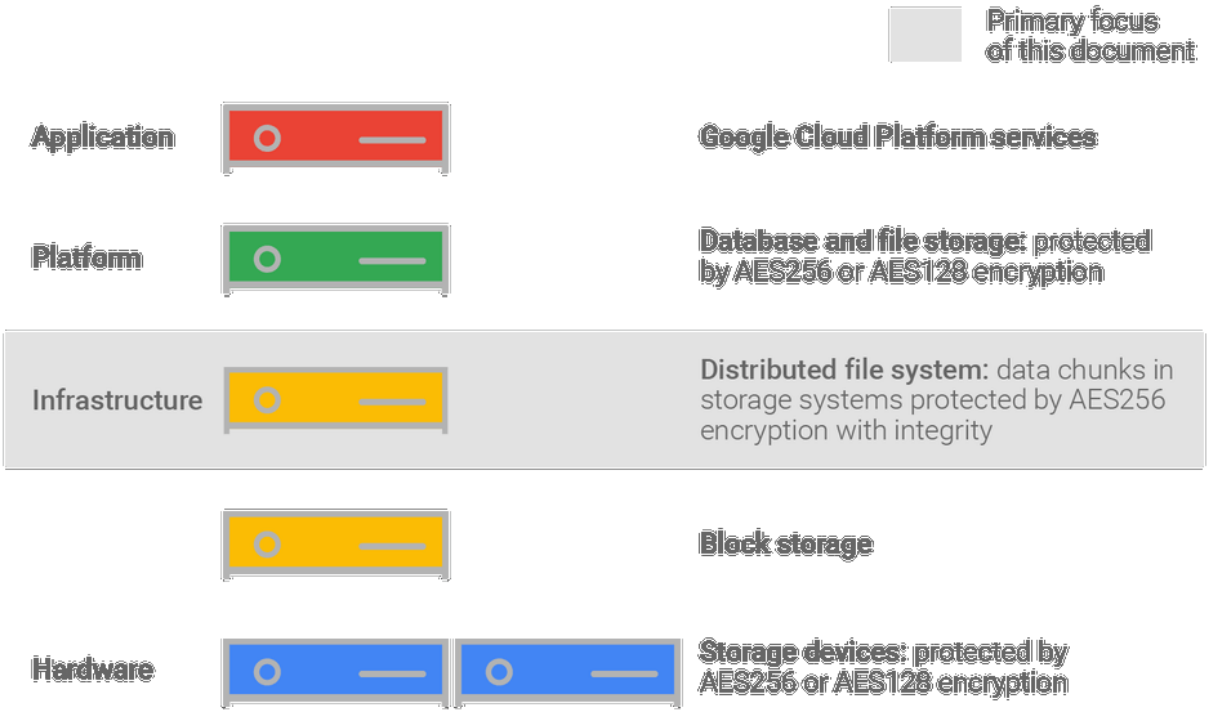
Implementasi Sistem Keamanan Pada Cloud Computing



Cisco AMP endpoints dan Cisco Umbrella merupakan paket duo yang bekerja dengan baik dalam mendeteksi, melindungi, mengontrol, hingga mencegah kejahatan kriminal yang dapat merusak sistem keamanan data di perusahaan.

Proteksi Ganda juga dibenamkan Google di G Suite

Setali tiga uang dengan Cisco, Google sebagai perusahaan yang juga telah menggunakan *cloud* tidak main-main dalam memberikan keamanan bagi penggunanya. Salah satu *software* yang berbasis 100% cloud, G Suite, sangat mengedepankan keamanan pengguna terutama dari segi penyimpanan data. Cara G Suite melakukan penyimpanan data tidak dilakukan di satu tempat. Data yang sudah Anda percayakan pada Google, tersimpan di pusat data Google yang tersebar di banyak negara. Jadi, jika Anda berlokasi di Indonesia, bisa saja data Anda berada di Singapura, Jepang, ataupun Hongkong. Hal ini juga untuk menjamin jika salah satu pusat data mengalami gangguan, data Anda masih tetap bisa didapatkan di lokasi lain.



Cara Google melindungi data Anda selain melalui pusat data yang tersebar di banyak negara juga melalui Google Cloud Security and Compliance. Serupa dengan Cisco Protect, Google Cloud Security and Compliance bertugas untuk melakukan *screening* situs dan mencegah malware mengacak-acak data Anda.

DAFTAR PUSTAKA

P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” National Institute of Standards and Technology, Information Technology Laboratory2009.

Presiden RI, “Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi danTransaksi Layanan Elektronik,” no. 1, pp. 1–29, 2008.

P. R. INDONESIA, “UU RI No.25/2009 Tentang Pelayanan Publik,” pp. 1–44, 2009.

P. R. INDONESIA, “Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 Tentang Pelayanan Publik,” pp. 1–26, 2012.

Security European Union Agency for Network and Information, “Cloud standards and security,” no. August, pp. 1–23, 2014.