

OUCH!

Dalam Edisi Ini...

- Sekilas
- Memilih Penyedia Layanan Cloud
- Pengamanan Data

Aman Menggunakan Cloud

Sekilas

“The Cloud” merupakan teknologi hebat yang mulai dipakai banyak orang dan organisasi. “Cloud” bisa memiliki banyak arti namun umumnya adalah penggunaan jasa layanan di Internet untuk menyimpan dan mengelola data untuk Anda. Manfaat penggunaan Cloud tidak terbatas pada kemudahan akses dan sinkronisasi data dari berbagai piranti dimana saja tapi juga dalam hal berbagi informasi ke orang lain. Alasan

kenapa dinamakan Cloud adalah karena tidak diketahuinya secara persis lokasi fisik dimana data disimpan. Beberapa contoh komputasi Cloud ialah pembuatan dokumen di Google Docs, berbagi file di Dropbox, pembuatan server pribadi di Amazon Cloud atau penyimpanan musik dan foto di iCloud Apple. Semua jasa layanan online ini berpotensi meningkatkan produktifitas namun juga memiliki resiko tersendiri. Dalam edisi ini akan dibahas bagaimana Cloud bisa dimanfaatkan dengan aman.

Editor Tamu

James dan Kelli Tarala ([@isaudit](#) / [@kellitarala](#)) adalah konsultan utama di Enclave Security serta perancang berbagai pelatihan di SANS, diantaranya adalah SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls dan MGT 415: A Practical Introduction to Risk Assessments.

Memilih Penyedia Layanan Cloud

Cloud adalah sebuah prasarana dalam mengerjakan sesuatu, baik di lingkungan kerja ataupun di rumah. Namun dalam penggunaan layanan ini, Anda menyerahkan penanganan data pribadi ke pihak lain dengan harapan data tersebut tetap aman dan siap digunakan, oleh sebab itu pemilihan penyedia layanan Cloud harus dilakukan dengan bijak. Untuk keperluan komputer atau informasi di dunia usaha/bisnis, tanyakan ke pihak manajemen apakah Cloud boleh digunakan. Jika diperbolehkan, tegaskan jasa layanan Cloud mana yang bisa dipakai serta bagaimana aturan penggunaannya. Bila mau menggunakan Cloud guna keperluan pribadi, pertimbangkan hal-hal dibawah ini:

1. **Layanan:** Mudahkan mendapatkan bantuan atau jawaban pertanyaan? Apakah tersedia nomer telpon layanan atau alamat surel yang bisa digunakan? Apakah ada pilihan lain, misalnya melalui forum publik atau daftar pertanyaan & jawaban (FAQ) di situs web?
2. **Kemudahan:** Gampangkah penggunaannya? Kian rumit layanannya, semakin besar kemungkinan terjadi kesalahan atau tanpa sengaja memaparkan atau menghilangkan informasi. Gunakan layanan Cloud yang mudah

Aman Menggunakan Cloud

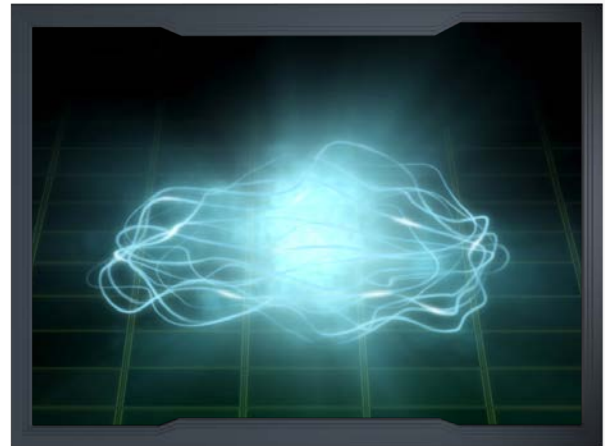
dimengerti, dipasang dan digunakan.

3. **Keamanan:** Bagaimana data dikirim dari komputer ke Cloud, apakah sambungan data terlindung dengan enkripsi? Bagaimana data Anda disimpan di Cloud, apakah dienkripsi? Jika dienkripsi, siapa yang berwenang membuka enkripsinya?
4. **Ketentuan Layanan:** Luangkan waktu untuk mempelajari Ketentuan Layanan (sering kali mudah dimengerti). Pastikan siapa yang bisa mengakses data dan juga apa saja hak hukum Anda.

Pengamanan Data

Setelah menentukan jasa layanan Cloud, langkah berikutnya adalah memastikan bahwa layanan Cloud digunakan dengan benar. Cara akses dan berbagi data seringkali lebih menentukan pengamanan berkas (file) dibanding aspek lainnya. Beberapa langkah penting untuk diperhatikan:

1. **Otentikasi:** Gunakan sandi yang baik (kuat) untuk otentikasi akun Cloud. Jika penyedia layanan Cloud menyediakan proses verifikasi dua langkah, gunakan fasilitas itu.
2. **Berbagi Berkas / Folder:** Cloud memudahkan proses berbagi, terkadang terlalu mudah malah. Dalam kenyataan, bisa saja beberapa berkas atau bahkan seluruh folder terpapar secara terbuka ke internet. Cara terbaik agar hal ini tidak terjadi adalah secara otomatis tidak berbagi berkas apapun pada saat awal, selanjutnya akses hanya diberikan ke orang tertentu (atau sekelompok orang) ke berkas atau folder sesuai kebutuhan. Bila seseorang tidak lagi memerlukan akses kesuatu berkas, hentikan aksesnya. Penyedia layanan Cloud wajib menyediakan cara mudah untuk melacak siapa saja yang memiliki akses ke berkas dan folder Anda.
3. **Berbagi berkas / Folder melalui Tautan (links):** Satu fitur layanan Cloud adalah kemampuan membuat tautan (link) web yang menunjuk ke lokasi berkas atau folder. Hal ini memudahkan Anda berbagi berkas kesiapa saja, cukup dengan hanya memberikan tautan itu. Cara itu ternyata kurang aman, siapa saja yang tahu tautan itu akan bisa mengakses berkas atau folder Anda. Jika tautan itu dikirimkan ke seseorang, bisa saja lalu disebarluaskan ke orang lain atau malah muncul di salah satu mesin pencari (search engine). Bila Anda berbagi data dengan menggunakan tautan, pastikan menon-aktifkan tautan tersebut jika sudah tidak diperlukan lagi atau gunakan sandi (password) sebagai perlindungan tambahan.
4. **Pengaturan:** Pahami pengaturan keamanan yang ditawarkan penyedia layanan Cloud. Sebagai contoh:



Cloud bisa menjadikan informasi lebih mudah diakses serta menambah produktifitas namun waspadalah dalam hal menyimpan dan berbagi informasi.

Aman Menggunakan Cloud

pada saat berbagi folder dengan orang lain, bisakah orang tersebut membagi data Anda ke orang lain tanpa sepengetahuan Anda?

5. **Antivirus:** Pastikan program antivirus terbaru terpasang disetiap komputer Anda dan komputer lain yang dipakai untuk berbagi data. Jika sebuah berkas yang sedang dipakai untuk berbagi tertular virus, komputer lain yang mengakses berkas tersebut juga bisa tertular.
6. **Backup:** Meskipun penyedia layanan Cloud melakukan backup data, pertimbangkan untuk secara berkala melakukan backup sendiri. Hal ini tidak hanya memberikan perlindungan jika penyedia layanan Cloud tiba-tiba bangkrut, berhenti operasi atau alasan lain yang menyebabkan gagal akses, namun akan lebih mudah mendapatkan data dalam jumlah besar dari backup lokal dibandingkan dari Cloud. Selain itu, pastikan seberapa sering proses backup dilakukan, apakah mungkin mendapatkan kembali versi lama sebuah berkas dan berapa lama data backup tersebut disimpan.

Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi <http://www.securingthehuman.org>.

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: <http://www.bipimax.net>

Sumber Pustaka

- Sandi yang Baik: <http://www.securingthehuman.org/ouch/2013#may2013>
- Pengaturan Sandi: <http://www.securingthehuman.org/ouch/2013#october2013>
- Backup: <http://www.securingthehuman.org/ouch/2013#september2013>
- Istilah Keamanan: <http://www.securingthehuman.org/resources/security-terms>

OUCH! diterbitkan oleh SANS "Securing The Human" dan didistribusikan sesuai lisensi [Creative Commons BY-NC-ND 4.0](http://creativecommons.org/licenses/by-nc-nd/4.0/). Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan perubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi ouch@securingthehuman.org.

Dewan Redaksi: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Diterjemahkan oleh: T. Gunawan



securingthehuman.org/blog



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/@securethehuman)



[securingthehuman.org/gplus](https://plus.google.com/securingthehuman.org)