OUCH! | November 2016

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Aman Menggunakan Cloud

Sekilas

"The Cloud" bisa memiliki beragam arti bagi setiap orang, namun umumnya merujuk pada penggunaan layananan di internet untuk menyimpan dan mengelola sistem komputer dan/atau data bagi penggunanya. Cloud menghadirkan kemudahan akses dan sinkronisasi data dari berbagai piranti dimanapun berada, sekaligus memudahkan berbagi informasi dengan siapapun yang diinginkan. Model layanan ini dinamakan "The Cloud" (Cloud) lantaran pengguna tidak tahu persis dimana data tersebut sebenarnya disimpan. Banyak contoh penggunaan Cloud, seperti pada saat olah dokumen di Google Docs, berbagi berkas di Dropbox, membuat server sendiri di Amazon Cloud, menyimpan data pelanggan di Salesforce atau menyimpan berkas musik dan gambar di Apple iCloud. Layanan online ini bisa menambah produktifitas namun perhatikan juga resikonya. Buletin edisi kali ini akan membahas bagaimana memaksimalkan penggunaan Cloud secara aman.

Editor Tamu

Dave Shackleford (**@daveshackleford**) adalah konsultan profesional pemilik Voodoo Security serta perancang beberapa program pelatihan SANS, seperti SANS Security 579: Virtualization dan Private Cloud Security and Security 524: Cloud Security Fundamentals.

Menentukan Penyedia Jasa

Cloud secara umum hanya merupakan sebuah alat bantu untuk mengerjakan sesuatu, di tempat kerja atau di rumah. Ingat, dengan menggunakan jasa layanan ini, Anda mempercayakan data pribadi ke pihak lain dan berharap agar disimpan dengan aman dan dalam kondisi siap pakai. Jadi, pilihlah penyedia jasa layanan Cloud dengan bijak. Untuk kebutuhan bisnis/kantor atau informasi yang berhubungan dengan pekerjaan, pastikan ke pihak managemen apakah penggunakan jasa Cloud diperbolehkan. Bila boleh, pastikan layanan Cloud mana yang bisa dipakai dan juga aturan apa saja yang wajib dipatuhi dalam penggunaannya. Untuk keperluan pribadi, pertimbangkan hal-hal sbb:

1. **Layanan**: Seberapa mudah mendapatkan bantuan atau jawaban atas sebuah pertanyaan? Apakah ada alamat surel yang bisa dihubungi, forum publik untuk mengunggah pertanyaan atau FAQ di situs webnya?
2. **Kemudahan**: Seberapa mudah penggunaannya? Semakin ruwet layanannya, semakin mungkin terjadi kesalahan dan secara tidak sengaja mengungkap atau kehilangan informasi. Pilih jasa layanan Cloud yang mudah dipahami, dipasang dan digunakan.

Aman Menggunakan Cloud

3. **Keamanan**: Data pribadi apa saja yang dibutuhkan? Bagaimana cara pengiriman data dari komputer ke Cloud dan bagaimana cara penyimpanannya di Cloud, apakah dienkripsi? Siapa saja yang bisa melakukan dekripsi data tersebut?
4. **Ketentuan Layanan**: Luangkan waktu untuk membaca Syarat dan Ketentuan Layanan (Term of Service) yang sering kali cukup mudah dimengerti. Pastikan siapa yang bisa mengakses data serta apa saja hak Anda, sekaligus kewajiban pengamanan yang harus dilakukan penyedia layanan atau wajib Anda lakukan.

Cloud menjadikan informasi lebih gampang diakses sekaligus meningkatkan produktifitas namun jangan sembrono dalam menyimpan dan berbagi informasi.

Mengamankan Data Anda

Setelah menentukan penyedia jasa layanan Cloud, langkah selanjutnya adalah memastikan bahwa layanan tersebut digunakan dengan benar. Cara akses dan berbagi data seringkali lebih berpengaruh terhadap keamanan berkas (file) dibanding aspek lainnya. Simak beberapa langkah penting dibawah ini:

1. **Otentifikasi**: Pilih frasa sandi yang baik (kuat) untuk otentifikasi akun Cloud. Jika penyedia layanan Cloud menyediakan proses verifikasi dua tahap, gunakan fasilitas itu. Ini merupakan salah satu langkah terpenting untuk perlindungan akun Anda.
2. **Berbagi Berkas/Folder**: Cloud mempermudah proses berbagi, malahan terkadang menjadi terlalu gampang. Dalam situasi tertentu, mungkin saja berkas yang seharus nya hanya diketahui beberapa orang saja namun secara tidak sengaja terpapar secara menyeluruh kesemua orang di jaringan internet. Cara terbaik menghindari hal ini adalah tidak secara otomatis memperbolehkan siapapun mengakses berkas Anda. Lakukan pemberian akses berkas atau folder ke orang lain (atau grup) secara selektif atau sesuai kebutuhan saja. Bila seseorang tidak lagi membutuhkan akses ke berkas tertentu, cabut/hapus saja hak aksesnya. Penyedia jasa layanan Cloud pasti menyediakan cara untuk melacak siapa saja yang memiliki akses ke berkas dan folder Anda.
3. **Berbagi Berkas/Folder Melalui Tautan (link)**: Satu fitur layanan Cloud adalah kemampuan membuat tautan (link) web yang menunjuk ke lokasi berkas atau folder. Ini tentu memudahkan Anda berbagi berkas pihak lain, cukup dengan hanya memberikan tautan itu. Ternyata, cara itu kurang aman, lantaran siapa saja yang tahu tautan itu akan bisa mengakses berkas atau folder Anda. Jika tautan itu dikirimkan ke orang lain, bisa saja lalu disebarkan ke pihak

Aman Menggunakan Cloud

lain atau malah muncul di salah satu mesin pencari (search engine). Bila Anda berbagi data dengan menggunakan tautan, jangan pernah lupa untuk menon-aktifkan tautan tersebut jika sudah tidak diperlukan lagi dengan mengatur masa berlakunya (expired date) atau gunakan sandi (password) sebagai perlindungan tambahan.

4. **Pengaturan**: Pahamilah pengaturan keamanan yang ditawarkan penyedia layanan Cloud. Sebagai contoh: pada saat berbagi folder dengan orang lain, bisakah orang itu menyebarkan data Anda ke orang lain tanpa sepengetahuan Anda? Bila memungkinkan, lacak siapa dan kapan orang lain mengakses berkas/folder Anda. Bisakah akses dibatasi menjadi "read only" (baca saja) sebagai ganti "read+write" (baca+tulis) yang artinya orang lain bisa mengubah berkas?
5. **Antivirus**: Pastikan program antivirus terbaru terpasang disetiap komputer Anda dan komputer lain yang digunakan untuk berbagi data. Jika sebuah berkas berbagi pakai (shared file) tertular virus, komputer lain yang mengakses berkas tersebut juga bisa tertular.

Selanjutnya

Untuk berlangganan buletin bulanan OUCH! Kesadaran Keamanan, mengakses arsip buletin OUCH! dan mengetahui lebih banyak solusi kesadaran keamanan SANS, silakan kunjungi securingthehuman.sans.org/ouch/archives.

Versi Bahasa Indonesia

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

Sumber Pustaka

Verifikasi Dua Tahap:	https://securingthehuman.sans.org/ouch/2015#september2015
Frasa Sandi:	https://securingthehuman.sans.org/ouch/2015#april2015
Manager Sandi:	https://securingthehuman.sans.org/ouch/2015#october2015
Mengenal Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

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