Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

- Pengenalan
- Memilih Pembekal Awan
- Melindungi Maklumat Anda

Menggunakan “Awan” (Cloud) dengan Selamat

Pengenalan

Awan adalah teknologi terkini yang semakin banyak digunakan oleh organisasi dan orang perseorangan. Perkataan Awan boleh membawa erti yang berbeza kepada orang yang berbeza, tetapi secara umumnya ia bermaksud menggunakan pembekal perkhidmatan di internet untuk menyimpan dan menguruskan maklumat anda. Kelebihan menggunakan Awan bukan sahaja memudahkan capaian dan menyelaras maklumat daripada beberapa jenis peranti dari mana juga di dunia, tetapi anda juga boleh berkongsi maklumat dengan sesiapa sahaja. Perkhidmatan ini dipanggil Awan kerana anda tidak tahu di mana maklumat anda disimpan secara fizikal. Contoh pengkomputeran Awan termasuklah menulis dokumen di Google Docs, berkongsi fail menggunakan Dropbox, mewujudkan pelayan anda sendiri di Amazon Cloud, atau menyimpan muzik atau gambar anda di Apple iCloud. Perkhidmatan dalam talian ini mempunyai potensi untuk menjadikan anda lebih produktif, walaubagaimanapun, ia juga mempunyai risiko tersendiri. Dalam surat berita ini kami akan membincangkan bagaimana anda boleh memanfaatkan Awan dengan selamat.

Editor Jemputan

James dan Kelli Tarala (**@isaudit**/**@kellitarala**) merupakan dua perunding utama di Enclave Security yang telah banyak mengarang kursus latihan SANS, termasuklah SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls dan MGT 415: A Practical Introduction to Risk Assessments.

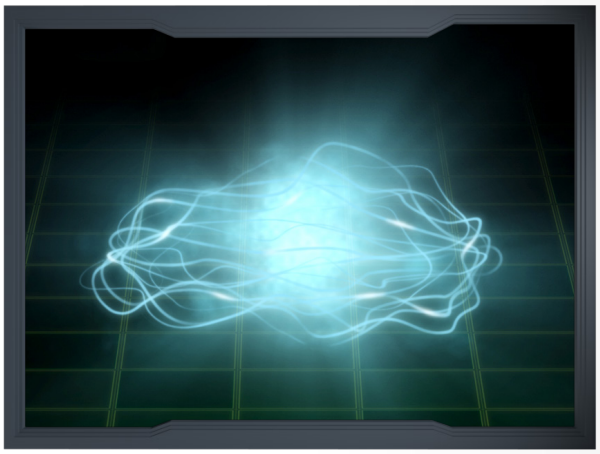
Memilih Pembekal Awan

Awan tidak boleh dikatakan baik mahupun buruk kerana ia adalah salah satu alat yang digunakan untuk menyiapkan sesuatu kerja, sama ada di rumah atau di tempat kerja. Walaubagaimanapun, apabila anda menggunakan perkhidmatan ini, anda juga menyerahkan maklumat peribadi anda kepada orang asing dan anda mengharapkan mereka untuk menyimpan maklumat tersebut dengan selamat dan tersedia. Untuk komputer pejabat atau maklumat berkaitan kerja, rujuk dengan penyelia anda sama ada anda boleh menggunakan perkhidmatan Awan. Jika anda dibenarkan menggunakan Awan, pastikan anda mengesahkan perkhidmatan Awan mana yang anda boleh gunakan dan polisi untuk menggunakannya. Jika anda mempertimbangkan perkhidmatan Awan untuk kegunaan peribadi, sila pertimbangkan yang berikut.

1. **Sokongan**. Adakah mudah untuk mendapatkan bantuan atau mendapatkan jawapan untuk soalan anda? Adakah ianya mempunyai nombor telefon atau alamat e-mel untuk dihubungi? Adakah terdapat pilihan lain untuk sokongan, seperti forum terbuka atau soalan-soalan lazim di laman sesawang mereka?

Menggunakan "Awan" (Cloud) dengan Selamat

2. **Memudahkan**. Adakah ianya mudah digunakan? Semakin kompleks perkhidmatan tersebut, semakin besar kemungkinan anda akan membuat kesilapan dan mendedahkan maklumat anda dengan tidak sengaja. Gunakan pembekal yang mudah difahami, ditala dan digunakan.
3. **Keselamatan**. Bagaimanakah maklumat anda disalurkan dari komputer ke awan, adakah ia selamat dengan penyulitan? Bagaimana maklumat anda disimpan di dalam Awan, adakah ia disulitkan, dan jika ya, siapakah yang boleh menyahsulit maklumat anda?
4. **Terma-terma Perkhidmatan**. Luangkan masa untuk menyemak terma-terma perkhidmatan (ia selalunya mudah untuk difahami). Sahkan siapa yang boleh mengakses maklumat anda dan apakah hak perundangan anda.



Perkhidmatan Awan memudahkan maklumat anda diakses dan boleh membantu anda menjadi lebih produktif, tetapi hati-hati bagaimana anda menyimpan dan berkongsi maklumat anda.

Melindungi Maklumat Anda

Setelah anda memilih perkhidmatan Awan, langkah seterusnya adalah memastikan perkhidmatan Awan tersebut digunakan dengan betul. Cara anda mencapai dan berkongsi maklumat mempunyai kesan yang besar kepada keselamatan fail anda berbanding perkara lain. Antara langkah utama yang boleh anda ambil adalah:

1. **Pengesahan**: Gunakan frasa laluan yang kukuh dan unik sebagai pengesahan akaun Awan anda. Jika pembekal Awan anda mempunyai pengesahan dua-langkah kami mencadangkan supaya anda mengaktifkannya.
2. **Berkongsi Fail/Folder**: Awan memudahkan perkongsian, kadang kala terlalu mudah. Dalam senario terburuk, anda mungkin dengan tidak sengaja menjadikan fail atau keseluruhan folder anda boleh dibuka oleh semua dalam internet. Cara terbaik untuk melindungi diri adalah langsung tidak berkongsi fail. Hanya benarkan orang tertentu sahaja (atau sekumpulan orang) boleh mengakses fail atau folder yang tertentu apabila perlu sahaja. Apabila mereka tidak lagi memerlukan akses tersebut, keluarkan mereka. Pembekal Awan anda perlu menyediakan cara yang mudah untuk anda menjejak siapa yang mempunyai akses kepada fail dan folder anda.
3. **Berkongsi Fail/Folder Menggunakan Pautan**: Salah satu fungsi yang biasa terdapat pada perkhidmatan Awan adalah keupayaan untuk mencipta pautan laman sesawang yang akan menghala ke fail dan folder anda. Fungsi ini membolehkan anda berkongsi fail dengan sesiapa yang anda mahu dengan hanya memberikan pautan tersebut. Walaubagaimanapun, cara ini mempunyai ciri keselamatan yang rendah, sesiapa yang mempunyai pautan tersebut boleh mengakses fail dan folder peribadi anda. Jika anda menghantar pautan tersebut kepada seseo-

Menggunakan “Awan” (Cloud) dengan Selamat

rang, beliau boleh berkongsi pautan tersebut dengan individu lain atau pautan anda boleh tersenarai dalam enjin carian. Jika anda berkongsi maklumat menggunakan pautan, pastikan anda mematikan pautan tersebut setelah tidak lagi digunakan atau jika boleh, lindungi pautan tersebut dengan menggunakan kata laluan.

4. **Tetapan**: Fahamkan tetapan keselamatan yang ditawarkan oleh pembekal Awan anda. Sebagai contoh, jika anda berkongsi folder dengan orang lain, bolehkah mereka berkongsi maklumat anda dengan orang lain tanpa pengetahuan anda?
5. **Antivirus**: Pastikan perisian antivirus yang terkini dipasangkan pada komputer anda dan mana-mana komputer yang digunakan untuk berkongsi maklumat anda. Jika fail yang anda kongsi dijangkiti virus, komputer lain yang mengakses kepada fail tersebut akan turut dijangkiti.
6. **Sandaran**: Walaupun pembekal Awan anda membuat sandaran maklumat, pertimbangkan untuk membuat sandaran sendiri. Ini bukan sahaja dapat melindungi maklumat anda jika pembekal Awan anda gulung tikar, terpaksa ditutup atau tidak dapat diakses untuk sebarang alasan, tetapi ia lebih mudah untuk memulihkan semula maklumat dalam kuantiti yang banyak dari sandaran tempatan dari memuat turun dari Awan. Pastikan juga berapa kerap pembekal anda membuat sandaran, adakah mereka membenarkan anda memulihkan fail versi yang sebelumnya, dan berapa lama mereka menyimpan sandaran anda?

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di http://www.securingthehuman.org.

Sumber

Strong Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Backups:	http://www.securingthehuman.org/ouch/2013#september2013
Security Terms:	http://www.securingthehuman.org/resources/security-terms

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie

