Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

Menggunakan Awan Dengan Selamat

Pengenalan

"Awan" membawa makna berbeza untuk setiap orang, tetapi selalunya memberi makna menggunakan penyedia perkhidmatan di internet untuk menguruskan sistem perkomputeran anda dan/atau maklumat anda. Salah satu kelebihan menggunakan Awan adalah anda boleh membuat sambungan dan penyegerakan maklumat anda pada peranti yang berbeza dimana-mana dalam dunia, dan anda boleh berkongsi maklumat anda dengan sesiapa yang anda mahukan. Kita gelarkan perkhidmatan ini Awan kerana selalunya anda tidak tahu dimana maklumat anda disimpan secara fizikal. Contoh-contoh perkomputeran Awan termasuklah mencipta dokumen menggunakan Google Docs, berkongsi fail menggunakan Dropbox, menyediakan pelayan anda sendiri di Amazon Cloud, menyimpan maklumat pelanggan di Salesforce atau pengarkiban muzik atau gambar-gambar anda di Apple iCloud. Perkhidmatan dalam talian ini menjadikan anda lebih produktif, tetapi ia juga datang dengan risikonya tersendiri. Dalam surat berita ini kami menerangkan bagaimana anda boleh menggunakan Awan sepenuhnya dengan selamat.

Editor Jemputan

Dave Shackleford (**@daveshackleford**) adalah seorang perunding profesional yang merupakan pemilik Voodoo Security dan pengarang kepada kursus-kursus SANS, termasuklah SANS Security 579: Virtualization and Private Cloud Security dan Security 524: Cloud Security Fundamentals.

Memilih Penyedia Perkhidmatan Awan

Awan bukanlah sesuatu yang baik mahupun jahat, ia merupakan satu alat untuk menyiapkan sesuatu perkara, dirumah dan juga ketika bekerja. Walaubagaimanapun, apabila anda menggunakan perkhidmatan ini anda memberikan maklumat peribadi anda kepada pihak ketiga dan anda harapkan mereka untuk menyimpannya dengan selamat dan tersedia. Oleh itu anda perlu memilih penyedia Awan anda dengan bijak. Untuk komputer pejabat atau maklumat berkaitan kerja semak dengan penyelia anda untuk memastikan samaada organisasi anda membenarkan perkhidmatan Awan. Jika anda dibenar menggunakan Awan, pastikan perkhidmatan Awan mana yang bole anda gunakan dan apakah polisi untuk menggunakannya. Jika anda bercadang untuk menggunakan perkhidmatan Awan untuk kegunaan persendirian, pertimbangkan perkara-perkara berikut.

1. **Sokongan**. Adakah mudah untuk mendapatkan bantuan atau mendapat jawapan dari soalan anda? Adakah terdapat alamat emel untuk anda hubungi, forum awam yang boleh anda ajukan soalan atau soalan pertanyaan kerap di dalam laman sesawang mereka.
2. **Tahap Kesukaran**. Adakah perkhidmatan tersebut mudah digunakan? Semakin kompleks perkhidmatan tersebut,

Menggunakan Awan Dengan Selamat

terdapat kemungkinan anda akan melakukan kesalahan dan mendedah atau kehilangan maklumat anda dengan tidak sengaja. Pilih penyedia Awan yang anda rasakan mudah untuk difahami, tatarajah dan gunakan.

3. **Keselamatan**. Apakah maklumat yang di kutip dari anda, jika ada? Bagaimana maklumat dari komputer anda disambungkan ke Awan dan bagaimana ianya disimpan – adakah ianya disulitkan dan betul siapa yang boleh menyahsulitkan maklumat tersebut?
4. **Syarat-syarat Perkhidmatan**. Ambil masa seketika untuk menyemak syarat-syarat perkhidmatan (selalunya ia mudah untuk difahami). Pastikan siapa yang boleh mencapai maklumat anda dan apakah hak undang-undang anda, dan juga sebarang tanggugjawab keselamatan yang ditanggung oleh penyedia dan yang anda perlukan.

Awan boleh menjadikan maklumat anda lebih mudah dicapai dan menjadikan anda lebih produktif, tetapi berhati-hati bagaimana anda membuat capaian dan kongsi maklumat anda.

Melindungi Maklumat Anda

Setelah anda memilih pernyedia Awan, langkah seterusnya adalah memastikan anda menggunakan perkhidmatan Awan anda dengan betul. Bagaimana anda mencapai dan berkongsi maklumat selalunya memberi impak yang lebih besar terhadap keselamatan fail-fail anda dari perkara lain. Antara langkah-langkah yang boleh anda ambil termasuklah:

1. **Pengesahan**: Gunakan frasa laluan yang unik dan utuh sebagai pengesahan akaun Awan anda. Jika penyedia Awan anda menawarkan penentusah dua langkah kami merekomen anda membolehkannya. Ini merupakan langkah paling penting yang boleh anda ambil untuk melindungi akaun anda.
2. **Perkongsian Fail / Folder**: Perkongsian dengan Awan adalah sangat mudah, kadang-kala terlalu mudah. Dalam senario kes paling buruk, anda mungkin menyangkakan anda berkongsi fail tersebut dengan individu spesifik, tetapi dengan tidak sengaja anda mungkin kongsikan fail atau mungkin seluruh folder secara terbuka kepada seluruh internet. Cara terbaik untuk melindungi diri anda adalah dengan tidak berkongsi apa-apa fail dengan sesiapa secara lalai. Kemudian barulah anda benarkan orang-orang tertentu (atau kumpulan) capaian kepada kepada fail atau folder yang spesifik bila perlu. Apabila seseorang tidak perlu capaian kepada fail anda, singkirkan mereka. Penyedia Awan anda sepatutnya menyediakan cara mudah untuk menjejaki sesiapa yang mempunyai capaian kepada fail dan folder anda.
3. **Perkongsian Fail / Folder Menggunakan Pautan**: Salah satu sifat sesetengah perkhidmatan Awan adalah keupayaan untuk mencipta pautan sesawang yang membawa kepada fail atau folder anda. Sifat ini membolehkan anda untuk berkongsi fail dengan sesiapa anda mahu hanya dengan memberikan pautan sesawang. Sungguh pun begitu, pendekatan ini mempunyai ciri keselamatan yang rendah, sesiapa yang mempunyai pautan ini boleh mencapai kepada fail atau folder peribadi anda. Jika anda memberikan pautan tersebut kepada seseorang, beliau boleh berkongsi pautan

Menggunakan Awan Dengan Selamat

tersebut dengan orang lain atau ia boleh dijumpai di dalam enjin carian. Jika anda berkongsi maklumat menggunakan pautan, pastikan anda melumpuhkannya jika tidak diperlukan dengan menetapkan tarikh luput atau lindungi pautan tersebut dengan kata laluan.

4. **Tetapan**: Fahami tetapan keselamatan yang ditawarkan oleh penyedia Awan anda. Sebagai contoh, jika anda berkongsi satu folder dengan orang lain, bolehkah mereka berkongsi maklumat anda dengan orang lain tanpa pengetahuan anda? Pastikan juga terdapat cara untuk mengetahui siapa yang pernah melihat atau kongsi maklumat tersebut, dan bila mereka melihatnya. Bolehkah anda hadkan perkongsian tersebut kepada "baca sahaja" berbanding memberikan "baca+tulis" yang membenarkan orang untuk mengubah-suai fail tersebut?
5. **Antivirus**: Pastikan anda memasang perisian antivirus pada komputer anda dan juga komputer lain yang digunakan untuk berkongsi maklumat. Jika fail yang anda kongsi berjangkit, komputer lain yang mencapai fail yang sama berkemungkinan boleh berjangkit.

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 securingthehuman.sans.org/ouch/archives.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Sumber

Two-Step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

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

