

OUCH!

DALAM ISU INI...

- Sandaran: Apa, Bila dan Bagaimana
- Pemulihan
- Perkara Utama

Sandaran & Pemulihan

Pengenalan

Sekiranya anda menggunakan komputer atau peranti mudah alih dalam jangkamasa yang lama, lambat-laun sesuatu akan terjadi dan akan menyebabkan anda kehilangan fail peribadi, dokume atau gambar. Sebagai contoh, anda mungkin dengan tidak sengaja terpadam fail yang salah, kerosakan kepada perkakasan, kehilangan peranti atau dijangkiti perisian hasad seperti perisian tebusan. Dalam keadaan seperti ini, sandaran adalah antara pilihan yang ada untuk membina semula kehidupan digital anda. Dalam surat berita ini, kami akan menerangkan apa itu sandaran, bagaimana cara membuat sandaran kepada data anda dan membangun strategi yang sesuai untuk anda.

Editor Jemputan

Keith Palmgren merupakan seorang profesional keselamatan siber dengan pengalaman lebih 30 tahun di dalam bidang keselamatan IT. Beliau merupakan seorang pengajar kanan SANS dan pengarang kursus SANS SEC301; 'Introduction to Information Security'. Keith mempunyai syarikat perunding keselamatan yang berjaya dan berada di Twitter: [@kpalmgren](https://twitter.com/kpalmgren)

Sandaran: Apa, Bila dan Bagaimana

Sandaran adalah salinan kepada maklumat yang disimpan di tempat selain komputer atau peranti mudah alih anda. Apabila kehilangan maklumat yang bernilai, anda boleh memulihkan maklumat tersebut dari sandaran. Malangnya, terlalu ramai orang gagal untuk melakukan sandaran secara kerap, walaupun ianya mudah dan murah. Langkah pertama adalah untuk membuat keputusan apa yang mahu anda sandarkan. Terdapat 2 pendekatan: (1) data khusus yang penting buat anda; atau (2) kesemuanya, termasuklah sistem operasi anda. Kebanyakan penyelesaian ditetapkan secara lalai untuk menggunakan pilihan pertama, ianya akan membuat sandaran kepada fail yang kerap digunakan. Selalunya hanya ini yang anda perlukan. Bagaimanapun, jika anda tidak pasti apa yang perlu disandarkan atau untuk lebih berjaga-jaga, pilih untuk sandarkan semuanya.

Kedua, anda perlu memilih kekerapan penyandaran data. Untuk komputer peribadi, program sedia terbina seperti Time Machine di Apple, atau program Backup and Restore pada Microsoft Window membolehkan anda membuat jadual sandaran automatik. Tetapan lazim termasuklah setiap jam, harian, mingguan dan sebagainya. Penyelesaian lain menawarkan perlindungan berpanjangan di mana fail yang telah diubahsuai akan disandarkan setiap kali anda menyimpan dokumen. Kami mengesyorkan sandaran harian sebagai minimum.

Akhir sekali, anda perlu memilih bagaimana cara untuk membuat sandaran. Terdapat dua cara untuk membuat sandaran kepada data anda: media fizikal atau storan awan. Setiap pendekatan mempunyai baik dan buruknya. Jika anda tidak pasti pendekatan mana yang perlu digunapakai, anda boleh menggunakan kedua-duanya pada masa yang sama. Media fizikal ada-

Sandaran & Pemulihan

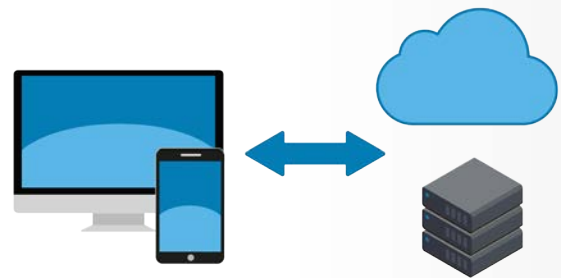
lah peranti yang anda kawal seperti pemacu USB luaran atau peranti rangkaian capaian Wi-Fi. Kelebihan menggunakan media fizikal sendiri adalah ia membenarkan anda membuat sandaran dan pemulihan data yang besar dengan cepat. Kekurangan menggunakan pendekatan tersebut adalah jika anda dijangkiti perisian hasad seperti perisian tebusan, terdapat kemungkinan ia akan tersebar ke sandaran anda. Begitu juga jika terdapat kecelakaan seperti kebakaran atau kecurian, anda bukan sahaja kehilangan komputer, malahan sandaran anda sekali. Oleh itu, jika menggunakan peranti luaran sebagai sandaran, anda perlu mempunyai perancangan untuk menyimpan salinan sandaran di luar kawasan di lokasi yang selamat. Pastikan sebarang sandaran yang anda simpan dilabel dengan betul.

Penyelesaian awan adalah perkhidmatan dalam talian yang menyimpan fail anda di internet. Selalunya anda akan memasang satu aplikasi di dalam komputer anda. Aplikasi tersebut kemudiannya membuat sandaran fail-fail secara automatik sama ada mengikut jadual atau apabila anda mengubahsuainya. Kelebihan menggunakan awan adalah ianya mudah, sandaran dibuat hampir secara automatik dan selalunya capaian kepada fail anda boleh dibuat dari mana sahaja. Dengan itu memandangkan maklumat anda terdapat di awan, kecelakaan yang berlaku di rumah seperti kebakaran atau kecurian tidak akan menjejaskan sandaran tersebut. Keburukannya pula adalah untuk membuat sandaran dan pemulihan data yang besar akan mengambil masa yang sangat lama. Selain itu, keselamatan dan privasi adalah penting. Adakah perkhidmatan sandaran menawarkan kawalan keselamatan yang kukuh seperti penyulitan data dan pengesahan yang kukuh?

Akhir sekali jangan lupakan peranti mudah alih anda. Dengan peranti mudah alih kebanyakan maklumat anda seperti emel, kalendar, peristiwa dan kenalan telah berada di awan. Bagaimanapun, tetapan aplikasi peranti mudah alih, gambar terbaharu, dan pilihan sistem mungkin tidak disimpan di awan. Dengan membuat sandaran kepada peranti mudah alih, bukan sahaja anda menyimpan maklumat ini, tetapi ia juga memudahkan pemindahan maklumat apabila anda menaiktaraf kepada peranti baru. iPhone/iPad boleh membuat sandaran secara automatik kepada Apple iCloud. Android atau peranti mudah alih yang lain bergantung kepada pengeluar dan penyedia perkhidmatan. Dalam kes-kes tertentu, anda mungkin perlu membeli aplikasi mudah alih yang dibangunkan khas untuk sandaran.

Pemulihan

Membuat sandaran kepada maklumat anda hanyalah sebahagian dari kerja yang perlu dibuat kerana anda harus memastikan yang anda boleh memulihkannya semula. Semak secara berkala jika sandaran tersebut boleh digunakan dengan mendapatkan satu fail dan mengesahkan maklumatnya. Selain itu, pastikan sandaran penuh telah dilakukan sebelum



Sandaran yang automatik dan boleh dipercayai selalunya adalah benteng terakhir untuk melindungi maklumat anda.

Sandaran & Pemulihan

perubahan besar (seperti berpindah kepada komputer atau peranti mudah alih yang baru) atau proses baikpulih (seperti menukar cakera keras) dan pastikan ianya boleh dipulihkan.

Perkara Utama

- Tidak kira penyelesaian mana yang anda gunakan untuk membuat sandaran kepada maklumat, pastikan anda melakukan sandaran automatik dan semak secara berkala.
- Apabila membina semula sistem dari sandaran, pastikan anda melaksanakan semula tampalan keselamatan dan kemas kini sebelum menggunakannya semula.
- Sandaran yang telah lapuk dan tidak diperlukan lagi adalah liabiliti, musnahkan sebelum ianya dicapai oleh individu yang tidak dibenarkan.
- Jika menggunakan penyelesaian awan, selidiki polisi dan reputasi penyedia tersebut dan pastikan mereka memenuhi keperluan anda. Sebagai contoh, adakah mereka menyulitkan maklumat? Siapa yang mempunyai capaian kepada sandaran anda? Adakah mereka menyokong pengesahan kukuh seperti pengesahan dua langkah?

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://snc.skmm.gov.my/>.

Sumber

Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Two-step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Cloud Security:	https://securingthehuman.sans.org/ouch/2016#november2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

OUCH! diterbitkan oleh program SANS "Securing The Human" dan diedarkan di bawah lesen [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Kebenaran diberikan untuk mengedarkan surat berita ini atau menggunakannya dalam mana mana program kesedaran selagi tiada perubahan dibuat kepada kandungan asal.

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

