OUCH! | September 2015

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Verifikasi Dua-Tahap

Sekilas

Proses pembuktian siapa Anda adalah langkah penting dalam pelindungan informasi. Otentifikasi yang baik bertujuan memastikan hanya Anda yang bisa mengakses informasi milik Anda seperti surel, foto ataupun akun bank. Ada tiga cara untuk memastikan siapa Anda; yaitu melalui sandi, barang pribadi misalnya Surat Ijin Mengemudi (SIM) dan diri Anda contohnya adalah sidik jari. Setiap metode ini memiliki keunggulan dan kelemahan. Cara paling umum dan dimengerti orang banyak adalah sandi. Dalam edisi ini, akan dipaparkan cara perlindungan diri dengan menggunakan metode verifikasi dua-tahap yang jauh lebih aman dari hanya sekedar sandi dan juga sangat mudah digunakan. Sebelum mengenal metode ini akan dibahas terlebih dahulu seputar sandi.

Editor Tamu

Keith Palmgren berpengalaman 30 tahun dibidang Keamanan Informasi. Beliau adalah instruktur bersertifikat di SANS Institute and pengarang SANS SEC301, kursus pengenalan Keamanan Informasi. Diwaktu senggang, Keith fokus pada kegiatan konsultasi dan penulisan. Keith bisa disimak di **@kpalmgren**.

Sandi

Sandi membuktikan siapa Anda berdasar sesuatu yang Anda tentukan. Bila sandi dibobol, biasanya akan menimbulkan banyak kerugian. Seandainya orang lain bisa menebak dan mendapatkan sandi tersebut, bisa saja orang itu berpura-pura menjadi Anda dan mengakses semua informasi yang terlindung oleh sandi tersebut. Atas dasar itulah diajarkan berbagai kiat mengamankan sandi, misalnya dengan penggunaan sandi yang kuat sehingga susah dibobol, menggunakan sandi berbeda untuk setiap akun dan tidak pernah berbagi sandi dengan siapapun. Meskipun wejangan itu benar namun keampuhan sandi sudah mulai luntur, sandi tidak lagi efektif dijaman modern ini. Teknologi terbaru memudahkan penyerang siber untuk membobol sandi. Yang diperlukan sekarang ini adalah solusi yang gampang digunakan tapi lebih aman dalam proses otentifikasi. Untungnya, kebutuhan itu bisa dipenuhi dengan metode verifikasi dua-tahap.

Verifikasi Dua-Tahap

Verifikasi dua-tahap (dikenal juga sebagai otentifikasi 2 faktor atau 2FA) menawarkan solusi lebih aman dibanding sekedar sandi. Cara ini membutuhkan tidak hanya satu tetapi dua cara dalam melakukan proses otentifikasi. Contohnya

Verifikasi Dua-Tahap

adalah kartu Anjungan Tunai Mandiri (ATM). Saat menarik uang dari mesin ATM, disini dipakai verifikasi dua-tahap. Untuk mengakses dana Anda, diperlukan dua hal yaitu Kartu ATM (yang Anda bawa) dan PIN (yang Anda ketahui). Seandainya kartu ATM itu hilang, uang masih tetap aman. Siapapun yang menemukan kartu tersebut tidak bisa akan menarik dana sebab tidak mengetahui PIN (kecuali Anda menuliskan PIN dibalik kartu tersebut). Hal yang sama juga berlaku bila Anda tahu PIN nya tapi tidak memiliki Kartu ATMnya. Diperlukan kartu ATM dan PIN untuk bisa membobol akun tersebut. Itulah sebabnya verifikasi dua-tahap lebih terpercaya karena menggunakan dua lapis pengaman.

Gunakan verifikasi dua-tahap bila memungkinkan, itu merupakan salah satu upaya terbaik untuk mengamankan informasi.

Menggunakan Verifikasi Dua-Tahap

Verifikasi dua-tahap harus diaktifkan disetiap akun. Untungnya, banyak layanan on-line menyediakan fasilitas ini. Salah satu pelopor penggunaan verifikasi dua-tahap adalah Google Akun Google acap menjadi sasaran utama upaya pembobolan karena memberikan banyak layanan bebas biaya kejutaan orang diseluruh dunia. Oleh sebab itu Google perlu menggunakan cara otentifikasi yang lebih aman sekaligus menjadi salah satu organisasi pertama yang meluncurkan fasilitas verifikasi dua-tahap diberbagai jasa layanan online. Bila Anda paham bagaimana cara kerja verifikasi dua-tahap Google maka mudah pula memahami penerapannya di Twitter,Facebook, Apple, Instagram dan jasa perbankan.

Pertama-tama, aktifkan verifikasi dua-tahap di akun Google kemudian daftarkan nomer ponsel. Selanjutnya, simak rincian cara kerja verifikasi dua-tahap berikut ini: lakukan login seperti biasa dengan menggunakan nama akun dan sandi. Ini adalah langkah pertama dari dua tahap. Google kemudian akan mengirim pesan singkat (SMS) berupa kode enam digit angka ke ponsel Anda. Seperti halnya sandi, deretan angka tersebut harus dimasukkan ke dalam situs web. Ini adalah bagian kedua dari dua tahap. Jadi untuk bisa berhasil login kesebuah akun, Anda harus menggunakan sandi yang benar dan dibutuhkan ponsel untuk menerima kode unik. Bahkan bila seseorang berhasil mendapatkan sandi Anda, mereka tidak akan bisa login ke akun Google Anda kecuali mereka memiliki ponsel Anda juga. Untuk memastikan akun Anda benar-benar aman, Google akan mengirimkan kode unik disetiap proses login.

Verifikasi Dua-Tahap

Ada cara lain untuk verifikasi dua-tahap di Google dan situs web lainnya. Alih-alih mengirimkan deretan kode unik melalui SMS, Anda bisa memasang aplikasi otentifikasi di alkom (alat komunikasi/smarphone). Aplikasi ini akan memunculkan kode unik setiap saat Anda berniat login. Keuntungan cara ini adalah tidak diperlukannya koneksi ke layanan jasa telepon untuk mendapatkan kode unik tersebut karena alkom akan menyiapkannya untuk Anda. Selain itu, karena kode unik itu dihasilkan oleh alkom dan tidak perlu dikirimkan ke Anda, otomatis informasi tersebut tidak bisa dicegat ditengah jalan oleh orang lain.

Ingat, verifikasi dua-tahap tidak otomatis langsung bisa digunakan, Anda harus mengaktifkannya terlebih dulu. Walaupun metode verifikasi dua-tahap terkesan merepotkan, disarankan untuk menggunakannya bilamana bisa, khususnya untuk layanan penting seperti surel, layanan perbankan online atau penyimpanan berkas secara online. Verifikasi dua-tahap memberikan perlindungan lebih baik dibanding sandi biasa.

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

Frasa Sandi:	http://www.securingthehuman.org/ouch/2015#april2015
Situs Pengguna Verifikasi Dua-Tahap:	https://twofactorauth.org
Stop|Think|Connect:	http://stopthinkconnect.org/2stepsahead
Verifikasi Dua-Tahap Google:	http://www.google.com/landing/2step/
SANS Security Tip of the Day:	http://www.sans.org/tip_of_the_day.php

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