OUCH! | April 2016

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

- **Sekilas**
- **Tanda-Tanda Diretas**
- **Tindakan**

Atasi Peretasan

Sekilas

Kami tahu Anda berupaya mengamankan komputer dan alkom (mobile device/alat komunikasi) serta melakukan beragam tindakan untuk itu. Namun, apapun usaha Anda, cepat atau lambat mungkin saja tetap akan terjadi peretasan atau pembobolan. Buletin ini akan membahas cara mengetahui adanya peretasan di komputer atau alkom sekaligus tindakan apa yang bisa dilakukan. Yang jelas, semakin cepat ditemukan kejanggalan serta sigap bertindak, Anda bisa mengurangi dampak negatif yang mungkin timbul.

Editor Tamu

Samantha Davison (**@sam_e_davison**) adalah manager Security Awareness and Education Program di Uber untuk karyawan yang tersebar di 350 kota diseluruh dunia.

Tanda-Tanda Diretas

Terkadang tidak mudah menentukan terjadinya peretasan. Namun, peretas biasanya meninggalkan beberapa tanda yang disebut juga sebagai indikator. Bila Anda menemukan beberapa hal dibawah ini maka tidak menutup kemungkinan telah terjadi peretasan.

- Program anti-virus menampilkan pemberitahuan bahwa sistem terinfeksi virus, khususnya bila muncul pesan yang menyatakan bahwa berkas (file) yang terinfeksi tidak bisa dihapus atau dikarantina.
- Browser tiba-tiba berubah atau menampilkan situs web yang tidak pernah diinginkan.
- Muncul beberapa akun baru walaupun Anda tidak pernah menciptakan akun itu atau muncul program baru yang tidak pernah ada sebelumnya.
- Komputer atau aplikasi sering gagal-fungsi (crashing), tiba-tiba muncul icon aplikasi baru.
- Sebuah aplikasi meminta otorisasi untuk melakukan perubahan sistem, walaupun Anda tidak memasang atau memperbarui aplikasi.
- Sandi tidak bisa digunakan untuk login ke sistem atau akun online, meskipun Anda yakin itu sandi yang benar.
- Teman/rekan mengatakan bahwa mereka menerima surel yang tidak pernah Anda kirim (spam).

© SANS Institute 2016

Atasi Peretasan

- Alkom memunculkan tagihan SMS Premium
- Alkom tiba-tiba menggunakan banyak data dan juga boros penggunaan batere.

Cepat atau lambat, komputer Anda mungkin diretas, sedini mungkin lakukan deteksi dan tindakan.

Tindakan

Bila Anda yakin telah terjadi peretasan, lebih cepat bertindak akan lebih baik. Bila Anda menggunakan komputer milik organisasi/perusahaan untuk keperluan kerja, jangan berupaya memperbaiki komputer tersebut secara mandiri. Hal ini bisa memperumit keadaan sekaligus merusak bukti-bukti yang bisa dipakai dalam proses penelusuran dan penyelidikan. Sebagai gantinya, laporkan secepatnya kepihak managemen melalui help desk, team keamanan atau atasan Anda. Jika pelaporan tersebut tidak bisa dilakukan atau mungkin ada hambatan lain, putuskan sambungan jaringan komputer dan biarkan komputer tersebut dalam kondisi “sleep”, “suspend” atau “airplane”. Bahkan jika Anda masih ragu apakah benar terjadi peretasan, melakukan pelaporan adalah hal terbaik. Bila komputer atau peralatan adalah milik pribadi, beberapa langkah dibawah ini bisa dilakukan:

- **Ubah Sandi**: Tidak hanya di perangkat komputer dan alkom namun juga semua akun. Pastikan tidak menggunakan komputer yang diretas untuk mengubah sandi. Gunakan komputer atau peralatan lain untuk itu.
- **Anti-virus**. Saat program anti-virus menemukan berkas yang tertular virus, ada beberapa pilihan tindakan. Bisa saja berkas akan dikarantina, dibersihkan dari virus atau dihapus/dibuang. Kebanyakan program anti-virus memiliki pranala (link) informasi seluk beluk virus untuk dipelajari. Bila ragu, lakukan karantina berkas yang tertular atau jika hal itu tidak bisa dilakukan, hapus saja berkas tersebut.
- **Bangun-Ulang**. Bila infeksi tidak bisa diatasi atau ingin yakin sistem sudah pulih sepenuhnya, pilihan paling aman adalah melakukan bangun-ulang. Untuk komputer, ikuti instruksi produsennya. Dalam banyak kasus, biasanya tersedia sebuah program aplikasi khusus untuk instal sistem operasi. Seandainya fasilitas ini tidak ada/ hilang, rusak atau terinfeksi; hubungi produsen untuk mendapatkan petunjuk atau kunjungi situs webnya. Jangan membangun-ulang sistem operasi dari backup karena mungkin saja memiliki titik lemah yang bisa dimanfaatkan oleh peretas. Backup hanya boleh digunakan untuk mendapatkan kembali data saja. Untuk alkom, ikuti petunjuk

© SANS Institute 2016

Atasi Peretasan

dari produsen peralatan atau penyedia jasa yang tersedia di situs web. Kebanyakan, cukup dengan hanya mengembalikan kondisi alkom seperti kondisi baru/awal. Bila Anda merasa tidak yakin dalam melakukan bangun-ulang, gunakan jasa profesional. Pertimbangkan juga untuk membeli peralatan baru bila peralatan yang dipakai sudah tua. Bila komputer atau alkom sudah dibangun-ulang, atau diganti baru, pastikan semua sistem terperbarui, terkini dan sebisa mungkin aktifkan fasilitas pembaruan otomatis.

- **Backup**. Langkah terpenting untuk perlindungan adalah dengan melakukan backup secara rutin. Semakin sering dilakukan, akan semakin bagus. Beberapa aplikasi akan melakukan backup otomatis pada setiap berkas baru atau perubahan secara rutin setiap jam. Apapun pilihan solusi backup periodik yang dipakai, pastikan proses pembacaan berkas dari backup bisa dilakukan. Terkadang mendapatkan kembali data dari backup adalah cara satu-satunya setelah diretas.
- **Langkah Hukum**: bila Anda merasa terancam, laporkan kejadian tersebut ke pihak yang berwajib.

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

Backup:	https://securingthehuman.sans.org/ouch/2015#august2015
Frasa Sandi:	https://securingthehuman.sans.org/ouch/2015#april2015
Mengenal Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Mengamankan Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

OUCH! diterbitkan oleh SANS “Securing The Human” dan didistribusikan sesuai lisensi Creative Commons BY-NC-ND 4.0. Anda diperkenankan menyebarkan buletin ini atau menggunakannya di dalam program pembelajaran sejauh tidak melakukan pengubahan isi buletin. Untuk keperluan alih bahasa atau informasi lainnya, silakan menghubungi ouch@securingthehuman.org.

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