SANS SECURITY AWARENESS

Buletin Bulanan Keamanan Komputer

Apakah Saya Diretas?

Sekilas

Seaman-amannya (sistem komputer) Anda, seperti halnya mengemudi kendaraan, suatu saat bisa saja terjadi hal-hal yang tidak diinginkan. Dibawah ini dibahas beberapa indikasi adanya peretasan dan bagaimana penanganannya. Semakin cepat hal itu diketahui, semakin besar potensi pemulihannya.

Indikasi Adanya Peretasan

Gejala umum adanya peretasan sebuah komputer atau akun adalah sbb:

- **Program Anti-virus menampilkan peringatan bahwa sistem terinfeksi/tertular virus. Pastikan pesan itu berasal dari program anti-virus, bukan pop-up windows dari situs web yang mencoba mengelabui Anda untuk menelpon atau menginstal sesuatu. Masih ragu? Akses program anti-virus Anda.**
- **Muncul peringatan bahwa komputer Anda terenkripsi dan harus membayar tebusan untuk mendapatkan kembali semua berkas/file.**
- **Browser Anda menampilkan beragam situs web yang tidak biasa.**
- **Aplikasi komputer sering terhenti (crash), muncul icon aplikasi tidak dikenal atau munculnya pop up windows aneh.**
- **Sandi tidak bisa dipakai lagi walaupun Anda yakin itu sandi yang benar.**
- **Teman atau rekan kerja bertanya kenapa Anda mengirimkan surel spam.**
- **Muncul tagihan ke kartu kredit atau penarikan tunai tanpa pernah Anda lakukan.**

Cara Bertindak

Bila Anda merasa/curiga terjadi peretasan, lebih cepat bertindak akan lebih baik. Jika peretasan berhubungan dengan tugas/urusan kantor, laporkan segera. Untuk lingkup pribadi, beberapa langkah ini bisa dilakukan:

- **Ganti Sandi:** Ini tidak hanya untuk komputer dan gawai namun juga akun daring. Jangan menggunakan komputer yang diretas guna mengganti sandi, gunakan komputer lain yang lebih aman. Bila Anda memiliki banyak akun, pritoritaskan yang paling penting dulu.

Finansial: Bila ada persoalan di kartu kredit atau akun finansial lain, segera hubungi bank atau perusahaan kartu kredit. Gunakan sambungan telepon terpercaya, biasanya tercantum di bagian belakang kartu kredit atau situs web.

Anti-virus: Bila perangkat lunak Anti-virus mengeluarkan pesan bahwa ada berkas terinfeksi, ikuti langkah-langkah penanganannya. Biasanya perangkat lunak memiliki tautan (link) untuk bisa mengenal dan mempelajari infeksi virus tertentu.

Instalasi Ulang: Bila gagal dalam upaya pemulihan komputer yang terinfeksi atau ingin 100% yakin sistem sepenuhnya aman, lakukan instalasi ulang sistem operasi. Jangan gunakan cadangan (backup) karena mungkin saja memiliki kelemahan sistem yang dimanipulasi peretas. Cadangan hanya boleh digunakan untuk mendapatkan kembali berkas pribadi. Bila Anda tidak merasa nyaman melakukan proses instalasi, gunakan bantaun/jasa pihak lain. Selain itu, bila sistem komputer Anda sudah tua, mungkin lebih mudah dan murah beli baru. Akhirnya, setelah proses instalasi ulang berhasil, atau membeli komputer baru, pastikan semua perangkat lunak terperbarui dan bila memungkinkan aktifkan fasilitas update otomatis.

Pencadangan (backup): Langkah paling penting dalam proteksi, lakukan pencadangan secara berkala. Semakin sering tentu semakin baik. Beberapa solusi pencadangan otomatis akan melakukan proses pencadangan berkas rutin harian atau bahkan setiap jam. Apapun pilihan metode pencadangan, jangan lupa memastikan bahwa berkas cadangan bisa diunduh-ulang. Terkadang dalam situasi tertentu, cadangan merupakan satu-satunya pilihan untuk memulihkan kondisi setelah terjadi peretasan.

Penegak Hukum: Bila Anda merasa terancam, jangan ragu untuk lapor ke pihak berwenang. Di Indonesia bisa menghubungi Badan Siber dan Sandi Negara di https://bssn.go.id/

Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

Editor Tamu

Dr. Johaness Ullrich *(@johullrich) adalah dekan riset di SANS Technology Institute, direktur SANS Internet Storm Center dan SANS Fellow. Pencipta jejaring DShield collaborative sensor dan pengasuh rubrik harian Internet Storm Center's podcast.*

Sumber Pustaka

Pencadangan: https://www.sans.org/u/JGP
Frasa Sandi: https://www.sans.org/u/JGU
Password Managers: https://www.sans.org/u/JGZ
Apa Itu Malware: https://www.sans.org/u/JH4