SANS SECURITY AWARENESS

OUCH!

Buletin Bulanan Keamanan Komputer

Ya, Anda Adalah Sasaran

Sekilas

Banyak orang keliru berpikir bahwa mereka bukan sasaran serangan siber: mereka, sistemnya atau akunya tidak bernilai apapun. Ini adalah pendapat keliru. Bila Anda pengguna teknologi, di kantor atau rumah, percayalah, Anda adalah berharga bagi peretas. Tapi, jangan kuatir. Anda mempunyai sistem pertahanan terbaik melawan serangan siber, yaitu Anda sendiri.

Kenapa Anda Menjadi Sasaran

Sekarang ini banyak jenis penyerang siber di dunia internet dan mereka memiliki beragam motivasi. Tapi, kenapa mereka mau menyerang Anda? Karena dengan melakukan peretasan, mereka bisa mencapai tujuannya. Di bawah ini ada dua contoh serangan siber dan alasan kenapa mereka menjadikan Anda sebagai target.

⚠ **Kriminalis Siber:** Orang-orang ini bertujuan mencari uang sebanyak mungkin. Internet adalah hal penting bagi mereka karena siapa saja diseluruh dunia bisa menjadi target dengan mudahnya. Mereka memiliki banyak cara untuk mendapatkan uang dari Anda. Bisa saja dengan mencuri uang dari akun bank atau dana pensiun, membuat kartu kredit atas nama Anda dan mengirimkan tagihan ke Anda, menggunakan komputer Anda untuk meretas komputer lain, atau meretas akun sosial media & game lalu menjualnya ke orang lain. Masih banyak hal-hal lain yang bisa dijadikan peluang usaha oleh penjahat siber. Ribuan orang seperti itu setiap hari bermaksud meretas sebanyak mungkin akun termasuk akun Anda.

☆ **Penyerang Terfokus:** Ini adalah penyerang siber terlatih, terkadang bekerja untuk badan pemerintah, sindikat kriminal atau pesaing. Anda beranggapan pekerjaan yang Anda lakukan tidak menarik perhatian, namun perlu diketahui:

- Informasi yang Anda tangani di tempat kerja memiliki nilai besar bagi perusahaan atau pemerintah lain.

- **Penyerang terfokus bisa saja menyasar Anda bukan untuk meretas, tapi menjadikan Anda sebagai perantara untuk meretas rekan kerja lain.**
- **Anda dijadikan sasaran sebagai jalan pintas menyerang rekanan lainnya.**

Ada Anti-Virus, Mestinya Aman

Ok, bila memang menjadi target, bukankah memasang anti-virus dan firewall di komputer sudah cukup? Ternyata tidak. Banyak orang beranggapan, menggunakan aplikasi keamanan akan menyelesaikan masalah, kenyataannya tidak demikian. Penyerang siber semakin mahir, pintar dan banyak akal dalam menerobos teknologi pengamanan. Contoh: mereka bisa menciptakan malware kelas kakap tanpa bisa dikenali anti-virus. Bisa menembus filter surel dalam serangan phishing khusus atau menelpon guna memperdaya Anda seputar kartu kredit, uang atau sandi. Teknologi memang berperan penting dalam perlindungan namun pada akhirnya, Anda sendiri merupakan proteksi terbaik.

Jangan kuatir, menjadi aman sesungguhnya tidak susah, hanya perlu akal sehat dan perilaku sederhana sebagai tameng terbaik. Bila Anda menerima surel atau telepon yang bersifat mendesak, aneh atau mencurigakan, itu bisa jadi adalah sebuah serangan. Pastikan komputer dan peralatan lain selalu terperbarui dengan mengaktifkan pembaruan otomatis. Juga, gunakan sandi yang kuat dan unik disetiap akun. Sikap waspada adalah pertahanan terbaik. Masih bingung mau mulai dari mana? Pertimbangkan berlangganan buletin OUCH! di sans.org/ouch.

Versi Bahasa Indonesia

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

Editor Tamu

Matt Bromiley *(@mbromileyDFIR) adalah ahli keamanan dan forensik digital dengan pengalaman lebih dari delapan tahun dan bekerja sama dengan banyak organisasi diseluruh dunia. Matt juga instruktur Digital Forensic dan Incident Response, staff pengajar modul SANS FOR508 dan FOR572.*

Sumber Pustaka

Stop Malware: https://www.sans.org/u/L1J
Rekayasa Sosial: https://www.sans.org/u/L1O
Phone Call Scams: https://www.sans.org/u/L1T
Frasa Sandi: https://www.sans.org/u/L1Y
Poster - You Are a Target: https://www.sans.org/u/L23

OUCH! diterbitkan oleh SANS "Security Awareness" 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 www.sans.org/security-awareness/ouch-newsletter. Dewan Redaksi: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Diterjemahkan oleh: T. Gunawan