OUCH! | Agustus 2018

OUCH!

SANS SECURITY AWARENESS

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

Peralatan Rumah nan Cerdas

Apa itu Peralatan Rumah nan Cerdas

Dulu, hanya beberapa peralatan di rumah yang bisa terhubung ke internet seperti laptop, gawas/alkom atau peralatan game. Namun sekarang, semakin banyak peralatan tersambung ke jejaring internet, mulai dari bola lampu dan pengeras suara hingga TV, kunci pintu dan juga mobil. Dalam waktu tidak terlalu lama lagi, hampir semua peralatan di rumah bisa tersambung ke internet. Semua peralatan yang tersambung ini biasa dikenal sebagai Internet of Things (IoT) atau peralatan rumah nan cerdas. Walaupun semua peralatan ini membawa kemudahan, ada beberapa bahaya/resiko yang perlu diketahui.

Apa Masalahnya?

Semakin banyak peralatan tersambung ke jaringan di rumah, potensi terjadinya masalah akan meningkat. Peretas bisa memprogram peralatan Anda untuk menyerang peralatan lain, penjual bisa mengumpulkan banyak aktifitas perihal aktifitas Anda, atau peralatan jadi terinfeksi virus dan tidak bisa digunakan (terkunci). Banyak produsen peralatan ini tidak memiliki pengalaman keamanan siber dan malah melihat pengamanan sebagai faktor biaya. Oleh sebab itu, bisa jadi peralatan yang Anda beli memiliki sedikit atau bahkan tanpa fasilitas keamanan sama sekali. Misal, beberapa peralatan memiliki sandi awal yang mudah ditebak atau tidak memiliki fasilitas/cara untuk mengubahnya.

Bagaimana Melindungi Diri?

Jadi, apa yang bisa dilakukan? Tentu tujuannya adalah demi kebaikan dan keamanan peralatan yang terkoneksi. Berbagai peralatan ini memiliki banyak fitur untuk mempermudah aktifitas sehari-hari. Selain itu, seiring dengan berkembangnya teknologi, tidak ada pilihan untuk tidak menggunakan peralatan cerdas. Berikut adalah beberapa langkah perlindungan yang bisa dilakukan:

Sambung seperlunya saja: Paling bijak untuk tidak menyambung peralatan ke jaringan internet. Bila tidak diperlukan daring, jangan sambung ke jaringan nir kabel (Wi-Fi). Apakah benar sebuah pemanggang roti perlu terhubung ke internet?

Ketahui apa saja yang tersambung: Peralatan apa saja yang tersambung ke jejaring di rumah? Tidak ingat? Matikan jaringan nir kabel dan simak peralatan apa yang jadi tidak bekerja lagi. Itu mungkin tidak bisa mengungkap semuanya namun setidaknya memberikan gambaran peralatan apa saja yang tersambung (dan mungkin terlupakan).

Pastikan Pembaruan: Seperti halnya komputer dan gawas, penting untuk menjamin bahwa semua peralatan selalu diperbarui. Aktifkan opsi proses pembaruan otomatis bila ada.

Sandi: Ubah sandi di setiap peralatan dengan bai, benar sekaligus rahasia. Sebuah sandi mungkin hanya perlu diketik sekali saja. Tidak bisa mengingat semua frasa-sandi? Jangan kuatir, gunakan fasilitas pengelola sandi untuk menyimpannya.

Pilihan Privasi: Apabila sebuah peralatan memiliki fitur pengaturan privasi, batasi jumlah informasi yang bisa dikumpulkan & disebar. Bisa dengan cara mematikan fitur berbagi informasi.

Penjual: Beli peralatan dari perusahaan yang dikenal dan terpercaya. Temukan produk dengan fitur keamanan, seperti pengaturan pembaruan otomatis, pengubahan sandi awal dan pengaturan opsi privasi.

Selalu Mendengar: Bila sebuah peralatan sanggup menerima perintah lewat suara, maka alat tersebut selalu dalam kondisi siap dengar, peralatan tersebut bisa merekam obrolan rahasia. Pertimbangkan hal itu saat menentukan kapan dan dimana alat tersebut akan dioperasikan.

JejaringTamu: Pertimbangkan mengatur sambungan jaringan peralatan Anda ke dalam sebuah jaringan "Tamu/Guest" tersendiri, tidak digabung ke jejaring nir kabel untuk komputer dan gawas. Dengan cara ini bila peralatan terinfeksi, maka komputer dan gawas/alkom akan tetap aman.

Tidak ada alasan untuk gamang terhadap teknologi baru namun pahami resiko yang mungkin ada. Dengan memperhatikan beberapa langkah praktis diatas, niscaya bisa terbangun Smart Home (Rumah Cerdas) yang aman.

Versi Bahasa Indonesia

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

Editor Tamu

Robert M. Lee (@RobertMLee) adalah instruktur bersertifikat di SANS dan pemrakarasa modul FOR578 - Cyber Threat Intelligence and ICS515 - ICS Active Defense and Incident Response. Robert juga merupakan CEO dan pendiri perusahaan keamanan siber, Dragos.

Sumber Pustaka

Frasa-Sandi: https://www.sans.org/u/GEB

Pengelola Sandi: https://www.sans.org/u/GEG

Amankan Jejaring di Rumah Anda: https://www.sans.org/u/GEL

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, Cathy Click, Cheryl Conley | Diterjemahkan oleh: T. Gunawan*

BIPIMax