OUCH! | Mei 2016

Buletin Bulanan Kesadaran Keamanan bagi Pengguna Komputer

OUCH!

Dalam Edisi Ini...

Jejaring Piranti Internet (JPI)

Mengenal Jejaring Piranti Internet (JPI)

Editor Tamu

James Lyne (@jameslyne) adalah pimpinan riset keamanan global di perusahaan Sophos. Pakar dibidang keamanan dunia komputer. Instruktur bersertifikat di SANS Institute dan sering menjadi pembicara utama diberbagai konperensi.

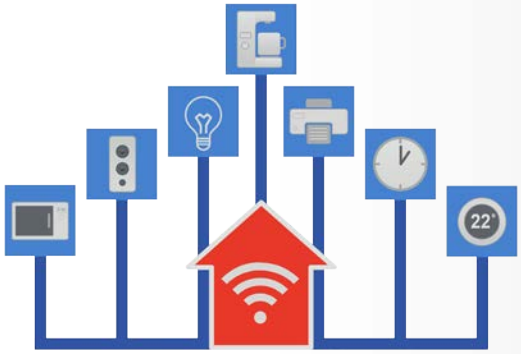
Dulu, bisa dibilang teknologi tergolong sederhana, lazimnya komputer dihubungkan ke internet dan dipakai untuk aktifitas harian. Perkembangan teknologi dan komunikasi meresap kedalam kehidupan manusia, hadirlah alkom (smartphone) dan tablet.Temuan ini mengemas kehebatan komputer dalam bentuk mungil. Karena mudah dibawa-bawa, sudah barang tentu perangkat ini memiliki tantangan keamanan tersendiri. Saat ini, perkembangan terbaru adalah Jejaring Piranti Internet (Internet of Things/IoT). Jejaring Piranti Internet (disingkat JPI) adalah upaya menyambung perangkat/peralatan rumah-tangga sehari-hari ke jaringan internet, bisa saja mulai dari bel pintu, lampu, boneka permainan hingga thermostat (pengatur suhu). Koneksi ini bisa membuat hidup lebih nyaman, contoh: lampu-lampu di rumah akan menyala saat telepon genggam mengetahui bahwa Anda sudah berada tidak jauh dari rumah. Pasar JPI berkembang pesat dengan hadirnya perangkat baru setiap minggu. Namun, seperti halnya alkom lainnya, perangkat JPI mempunyai sisi resiko keamanan tersendiri. Dalam edisi ini akan dibahas beberapa hal tersebut serta berbagai cara pengamanan perangkat JPI, rumah dan bahkan keluarga Anda.

Tantangan JPI

Kebanyakan perangkat JPI tergolong sederhana. Sebagai misal, mesin pembuat kopi hanya perlu disambung ke jaringan nir-kabel (wifi) di rumah. Tapi, kesederhanaan itu ternyata membawa resiko. Banyak produsen perangkat JPI tidak memiliki pengalaman dalam seluk beluk keamanan karena memang keahliannya hanya memproduksi peralatan rumah tangga saja. Mungkin juga karena perusahaan itu masih baru, jadi lebih banyak berfokus pada pengembangan produk yang efisien dalam waktu sesingkat mungkin. Pendek kata perhatian lebih ke profit dan bukan unsur keamanan siber. Hal ini menyebabkan perangkat JPI yang dijual hanya memiliki sedikit atau bahkan tanpa pengamanan siber sama sekali. Sebagai contoh, penggunaan sandi awal (default) yang mudah ditebak, malah mungkin juga diunggah ke internet serta ada juga yang tidak bisa diubah. Ada pula yang tidak memberikan pilihan untuk mengubah setup yang ada, jadi apa yang sudah ada tidak bisa diubah

Jejaring Piranti Internet (JPI)

sama sekali. Selain itu banyak peralatan yang tidak memiliki kemampuan, sulit atau tidak bisa diperbarui sama sekali. Semua hal itu membuat perangkat JPI mudah kadaluwarsa sekaligus rentan terhadap ancaman pembobolan/peretasan.



The Internet of Things

Ketahui semua perangkat JPI yang tersambung ke internet, batasi konektivitasnya, selalu perbarui dan gunakan sandi yang kokoh.

Perlindungan Perangkat JPI

Jadi, apa yang bisa dilakukan? Tentu saja dengan tujuan mendaya gunakan kemampuan piranti JPI secara aman dan efektif. Perangkat JPI menghadirkan kemudahan yang bermanfaat bagi kehidupan kita, menghemat biaya dan bisa jadi menambah keamanan seputar rumah Anda. Selain itu, dengan berkembangnya teknologi membuat Anda mau tidak mau membeli atau menggunakan perangkat JPI. Beberapa langkah di bawah ini bisa diterapkan untuk melindungi perangkat JPI dan juga Anda.

- **Sambung Yang Perlu Saja**: Cara termudah mengamankan perangkat JPI adalah dengan tidak menyambungnya ke jaringan Internet. Bila memang tidak diperlukan sambungan online, hindari sambungan ke jaringan Nir-kabel (Wi-Fi).
- **Jaringan Nir-Kabel Terpisah**: Bila perangkat JPI membutuhkan sambungan online, pertimbangkan untuk membuat jaringan nir-kabel terpisah. Banyak titik akses jaringan nir-kabel memiliki fasilitas untuk membuat jaringan tambahan, seperti jaringan untuk tamu (Guest). Pilihan lain adalah membeli perangkat titik akses nir-kabel khusus utk perangkat JPI. Jadi peralatan JPI akan berada dalam jaringan tersendiri, tidak bisa dimanfaatkan untuk menyerang atau menggangau peralatan lain yang tersambung ke jaringan utama di rumah (yang merupakan daya tarik utama kriminalis siber)
- **Upayakan melakukan Pembaruan**: seperti halnya PC atau perangkat genggam, upayakan perangkat JPI selalu diperbarui. Bila ada fasilitas pembaruan otomatis, aktifkan segera.
- **Sandi Kuat**: Lakukan perubahan sandi perangkat JPI agar bersifat unik dan menggunakan frasa-sandi yang kuat. Tidak ingat semua frasa-sandi? Jangan kuatir, banyak orang juga demikian. Pertimbangkan menggunakan Manager Sandi sebagai solusi.
- **Pilihan Privasi**: Bila ada fasilitas untuk mengatur tingkat privasi, batasi informas yang bisa diunggah. Salah satu pilihan adalah mematikan semua fasilitas berbagi informasi.

Jejaring Piranti Internet (JPI)

- **Ganti Peralatan**: dalam kondisi tertentu, mungkin Anda bermaksud mengganti sepenuhnya perangkat JPI bila ditemukan terlalu banyak kekurangan yang tidak bisa diperbaiki atau karena ada peralatan baru yang memiliki banyak fasilitas keamanan didalamnya.

Setiap perangkat memiliki keunikan tersendiri, ada baiknya memantau hal-hal yang sudah pernah dilakukan dan juga berbagai bahasan dalam hal pengamanannya. Pada dasarnya banyak perangkat JPI dirancang tanpa mempertimbangak unsur keamanan siber serta minim informasi keamanan. Sejalan dengan mulai tumbuhnya kesadaran akan keamanan siber, diharapkan dimasa depan, produsen JPI meningkatkan segi keamanan produk serta memberikan informasi lebih lengkap dalam hal perlindungan dan pembaruannya.

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:	https://securingthehuman.sans.org/ouch/2015#april2015
Pengelola Sandi:	https://securingthehuman.sans.org/ouch/2015#october2015
Mengamankan Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Mengamankan Jaringan di Rumah:	https://securingthehuman.sans.org/ouch/2016#february2016

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