Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU INI...

- Internet Benda(IoT)
- Isu-Isu IoT
- Melindungi Peranti-peranti IoT Anda

Internet Benda (IoT)

Apa itu Internet Benda(IoT)

Teknologi terdahulu adalah mudah, anda hanya perlu menghubungkan komputer dengan Internet dan menggunakannya untuk aktiviti harian anda. Kemudian teknologi bertambah maju dengan wujudnya peranti mudah alih dalam hidup kita seperti telefon pintar dan tablet. Kini alat-alat tersebut meletakkan kuasa komputer ke dalam poket anda. Walaupun jauh lebih mudah alih, peranti ini juga mempunyai cabaran-cabaran keselamatan mereka sendiri yang unik. Sekarang kemajuan teknikal yang lebih hebat adalah Internet Benda atau sering dipendekkan kepada IoT adalah tentang menyambungkan peranti harian kepada Internet, peranti dari loceng pintu, lampu, patung mainan dan termostat. Peranti-peranti yang bersambung ini boleh menjadikan kehidupan kita lebih mudah - sebagai contoh lampu anda diaktifkan secara automatik apabila telefon anda mengesan anda menghampiri rumah. Pasaran IoT berkembang pada kadar yang luar biasa apabila peranti-peranti baru dikeluarkan setiap minggu. Walau bagaimanapun, seperti peranti mudah alih, peranti IoT juga mempunyai isu-isu keselamatan mereka sendiri. Dalam surat berita ini, kami membantu anda memahami apa risiko dan apa yang anda boleh lakukan untuk melindungi peranti IoT anda, rumah anda, dan juga keluarga anda.

Editor Jemputan

James Lyne (**@jameslyne**) ialah ketua penyelidikan keselamatan global di firma keselamatan Sophos. Mengakui dirinya sebagai 'gek teragung', kepakaran teknikal beliau menjangkau pelbagai domain keselamatan. Beliau adalah pengajar yang bertauliah di institut SANS dan beliau juga merupakan penyampai maklumat utama di persidangan industri.

Isu-isu IoT

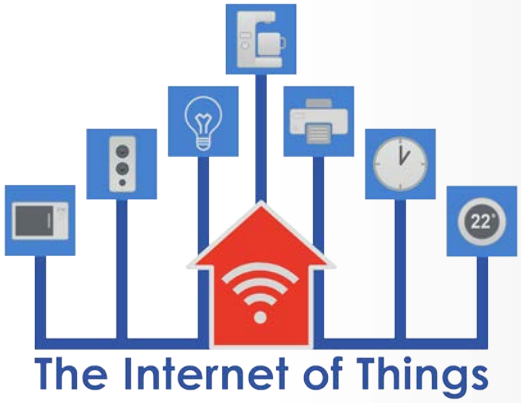
Kelebihan IoT adalah sebahagian besar alat-alat ini adalah ringkas. Contohnya, apabila anda menyambungkan plug mesin kopi anda, ia akan meminta untuk menyambung kepada rangkaian Wi-Fi rumah anda. Walaubagaimanapun semua kemudahan ini tidak percuma. Masalah terbesar dengan peranti IoT ialah banyak syarikat yang mengeluarkannya tidak mempunyai pengalaman dengan keselamatan, kepakaran mereka adalah pembuatan perkakas rumah sahaja. Atau mungkin mereka baru mencuba untuk mengeluarkan produk yang paling berkesan, paling cepat, seperti pada Kickstarter. Pertubuhan-pertubuhan ini mementingkan keuntungan, bukan keselamatan siber. Akibatnya, banyak peranti IoT yang dibeli hari ini hanya mempunyai sedikit atau tidak ada langsung keselamatan didalamnya. Sebagai contoh, ada yang mempunyai kata laluan lalai yang mudah diketahui, mungkin juga ada disiarkan di Internet, dan tidak boleh diubah. Selain itu, banyak daripada alat ini tidak mempunyai pilihan atau keupayaan untuk mengkonfigurasi, anda terjebak dengan apa sahaja yang telah dihantar. Lebih teruk lagi, banyak daripada alat ini boleh menjadi sukar untuk dikemas kini, malah mungkin tidak mempunyai keupayaan sama sekali. Akibatnya banyak peranti IoT yang anda gunakan boleh menjadi ketinggalan dengan cepat,

Internet Benda (IoT)

juga kelemahan yang diketahui dan tidak boleh diperbaiki, menjadikan anda kekal terdedah.

Melindungi Peranti-Peranti IoT anda

Apakah yang boleh anda lakukan? Sudah pastinya kami ingin anda untuk memanfaatkan sepenuhnya kelebihan menggunakan peranti IoT anda secara selamat dan efektif. Peranti-peranti ini boleh menyediakan ciri-ciri yang menarik yang boleh membuatkan hidup anda lebih mudah, menjimatkan wang dan meningkatkan keselamatan fizikal untuk rumah anda. Tambahan lagi, seiring dengan perkembangan teknologi anda tidak mempunyai pilihan melainkan membeli dan menggunakan peranti IoT. Berikut merupakan beberapa langkah yang boleh anda ambil untul melindungi peranti IoT dan diri anda.



Tahu peranti IoT apa yang telah disambungkan ke rangkaian anda, mengasingkan mereka apabila perlu, sentiasa mengemaskini dan melindungi mereka dengan frasa laluan yang kukuh.

- **Menyambung hanya bila perlu**: Cara paling mudah untuk memastikan peranti IoT anda selamat ialah dengan tidak menyambungkan peranti tersebut kepada internet. Jika anda tidak memerlukan peranti anda dalam berkeadaan atas talian, jangan sambungkan ianya kepada rangkaian Wi-Fi anda.
- **Asingkan rangkaian Wi-Fi**: Jika anda perlu untuk menggunakan peranti IoT anda dalam keadaan di atas talian, pertimbangkan untuk mewujudkan rangkaian asing Wi-Fi hanya untuk peranti-peranti tersebut. Banyak pusat akses Wi-Fi yang mempunyai keupayaan untuk mewujudkan rangkaian tambahan seperti rangakaian tetamu. Pilihan lain pula ialah dengan membeli pusat akses Wi-Fi tambahan hanya untuk peranti-peranti IoT. Ini boleh memastikan peranti-peranti IoT anda berada dalam rangkaian terasing supaya mereka tidak boleh digunakan untuk merosak atau menyerang mana-mana computer atau peranti mudah alih yang disambungkan ke rangkaian utama atau rumah (yang masih menjadi tarikan utama kepada jenayah siber).
- **Kemaskini jika boleh**: Sama seperti komputer peribadi dan peranti mudah alih anda, pastikan peranti-peranti IoT anda sentiasa dikemas kini. Jika peranti IoT anda mempunyai pilihan untuk mengemas kini secara automatik, sila aktifkannya.
- **Kata laluan yang kuat**: Ubah mana-mana kata laluan peranti IoT anda kepada unik, frasa laluan yang kuat yang hanya anda tahu. Tidak dapat mengingati semua frasa laluan anda? Jangan bimbang, kami juga begitu. Pertimbangkan untuk menggunakan pengurus kata laluan untuk menyimpan semua kata laluan secara selamat.
- **Pilihan privasi**: Jika peranti IoT anda membenarkan anda untuk menetapkan pilihan privasi, hadkan jumlah informasi yang boleh dikongsi. Salah satu pilihan adalah untuk mematikan segala keupayaan perkongsian maklumat yang ada.

Internet Benda (IoT)

- **Pertimbangkan penggantian**: Hingga satu ketika anda mungkin ingin untuk menukar atau menggantikan peranti IoT anda apabila peranti IoT sedia ada mempunyai terlalu banyak kelemahan yang tidak boleh dibaiki ataupun terdapat peranti-peranti yang baru yang mempunyai lebih banyak fungsi keselamatan yang dibina ke dalam peranti tersebut.

Tidak ada satu saiz yang muat untuk setiap peranti, jadi adalah berbaloi untuk menyemak amalan terbaik dan apa-apa penerbitan mengenai bagaimana untuk menyelamatkan mereka. Malangnya kebanyakan peranti IoT tidak dibuat dengan mementingkan keselamatan siber, jadi banyak pengeluar tidak memberikan maklumat keselamatan yang mencukupi. Tetapi apabila kesedaran tentang keselamatan siber telah tersebar, kami berharap untuk melihat lebih banyak vendor IoT mementingkan keselamatan dalam peranti mereka dan memberikan maklumat lanjut mengenai cara untuk melindungi dan mengemaskinikannya.

Mari Belajar Lebih Lanjut!

Langganilah surat berita bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer OUCH!, akseslah arkib OUCH!, dan belajar lebih lanjut mengenai penyelesaian kesedaran keselamatan SANS dengan melayari laman sesawang kami di http://www.securingthehuman.org.

Penterjemahan oleh SNSC.

Pusat Keselamatan Rangkaian SKMM (SKMM Network Security Centre- SNSC) beroperasi di bawah Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM) dengan matlamat menjamin keselamatan maklumat, kebolehpercayaan dan keutuhan rangkaian di Malaysia. Laman Web: http://snsc.skmm.gov.my/.

Sumber

Frasa laluan:	https://securingthehuman.sans.org/ouch/2015#april2015
Pengurus kata laluan:	https://securingthehuman.sans.org/ouch/2015#october2015
Menjamin Keselamatan Tablet Baru Anda:	https://securingthehuman.sans.org/ouch/2016#january2016
Menjamin Rangkaian Rumah Anda:	https://securingthehuman.sans.org/ouch/2016#february2016

Editor: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Translated by: Muhamad Hashimi, Rahayu Aziz, and Sheikh Ahmad Raffie