OUCH! | Ogos 2018

OUCH!

SANS SECURITY AWARENESS

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

Peranti Rumah Pintar

Apakah Peranti Rumah Pintar?

Secara tradisinya hanya beberapa peranti di rumah anda boleh dihubungkan kepada Internet seperti komputer riba, telefon pintar atau konsol permainan. Bagaimanapun, kini semakin banyak peranti terhubung kepada Internet, dari mentol lampu dan pembesar suara kepada TV, kuncipintu, malahan juga kereta. Pada masa akan datang, mungkin hampir kesemua peranti dalam rumah anda bersambung kepada Internet. Peranti bersambung ini selalunya dikenali dengan nama Internet of Things (IoT) atau peranti rumah pintar. Walaupun peranti bersambung ini memberikan banyak kemudahan, ia juga merbahaya.

Apakah Masalahnya?

Lebih banyak peranti yang terhubung dengan rangkaian rumah anda, lebih banyak masalah yang mungkin berlaku. Penggodam boleh memprogram peranti anda untuk menyerang, pembekal boleh mengumpul maklumat tentang aktiviti pengguna atau peranti boleh dijangkiti dan tidak dapat digunakan. Kebanyakan syarikat yang membina peranti ini tidak ada pengalaman dalam keselamatan siber dan menganggap keselamatan sebagai suatu kos tambahan. Justeru itu kebanyakan peranti yang anda beli mempunyai sedikit atau tiada fungsi keselamatan terbina. Sebagai contoh, sesetengah peranti mempunyai kata laluan lalai yang diketahui umum atau tidak boleh di kemaskini atau di konfigurasi.

Bagaimana Saya Boleh Lindungi Diri Sendiri

Jadi apa yang boleh anda lakukan? Kami mahukan andamenggunakan peranti bersambung dengan selamat dan terkawal. Peranti ini memberikan banyak kelebihan dengan memudahkan kehidupan harian. Sebagai tambahan, seiring dengan pembangunan teknologi anda mungkin tidak mempunyai pilihan selain menggunakan peranti pintar. Berikut adalah langkah yang boleh anda ambil untuk melindungi diri.

Berhubung Hanya Ketika Perlu: Cara paling mudah untuk melindungi sesuatu peranti adalah dengan tidak menyambungkannya kepada Internet. Jika anda tidak perlukannya untuk berada dalam talian, jangan sambungkannya kepada rangkaian wi-fi anda. Adakah anda benar-benar memerlukan pembakar roti untuk menghantar pemberitahuan kepada telefon anda?

Ketahui Apa Yang Telah Anda Sambungkan: Peranti apakah yang telah anda hubungkan pada rangkaian rumah anda? Tidak pasti atau tidak ingat? Padamkan rangkaian tanpa wayar dan lihat apa yang tidak lagi berfungsi. Ia mungkin tidak akan menunjukan kesemuanya tetapi anda akan terkejut dengan berapa banyak peranti yang anda lupa.

Kekal Kemaskini: Sama seperti komputer dan peranti mudah alih, ianya kritikal untuk mengekalkan semua peranti anda di kemaskini.

Kata Laluan: Tukar kata laluan peranti kepada ungkapan laluan kukuh dan unik yang hanya anda mengetahuinya. Anda mungkin hanya perlu memasukkannya hanya sekali. Tidak ingat kesemua ungkapan laluan anda? Jangan bimbang, begitu juga kami. Pertimbangkan untuk menggunakan pengurus kata laluan untuk menyimpannya dengan selamat.

Pilihan Privasi: Jika peranti boleh di konfigurasi untuk pilihan privasi, hadkan amaun maklumat yang dikumpul atau dikongsi. Salah satu cara adalah dengan melumpuhkan semua keupayaan untuk berkongsi maklumat.

Pembekal: Beli peranti dari syarikat yang anda tahu dan percaya. Cari produk yang menyokong keselamatan seperti membenarkan kemaskini automatik, menukar kata laluan lalai dan menukar tetapan privasi.

Sentiasa Mendengar: Jika sesuatu peranti boleh menerima arahan suara bermakna ia sentiasa mendengar. Sebagai contoh Alexa dan peranti Google Home boleh merakam perbualan sensitif. Pertimbangkan di mana anda letakkan peranti tersebut di dalam rumah dan semak pilihan privasi.

Rangkaian Tetamu: Pertimbangkan peranti pintar rumah anda disambungkan kepada rangkaian wi-fi tetamu dan tidak dihubungkan kepada rangkaian wi-fi utama yang digunakan oleh komputer dan peranti mudah alih. Dengan cara ini jika sebarang peranti pintar anda dijangkiti, komputer atau peranti mudah alih anda pada rangkaian utama kekal selamat.

Tiada sebab untuk takut dengan teknologi baru tetapi fahami risiko yang ada. Dengan mengambil langkah mudah ini anda boleh membantu untuk mencipta rumah pintar yang lebih selamat.

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/.

Editor Jemputan

Robert M. Lee *(@RobertMLee) adalah seorang pengajar bertauliah SANS dan pengarang untuk FOR578 - Cyber Threat Intelligence and ICS515 - ICS Active Defense and Incident Response. Robert juga adalah ketua pegawai eksekutif dan pengasas kepada Dragos, firma keselamatan siber industri.*

Sumber

Ungkapan Laluan:	https://www.sans.org/u/GEB
Pengurus Kata Laluan:	https://www.sans.org/u/GEG
Menjamin Rangkaian Rumah Anda:	https://www.sans.org/u/GEL