OUCH! | Januari 2014

Surat Berita Bulanan berkenaan Kesedaran Keselamatan Untuk Pengguna Komputer

OUCH!

DALAM ISU KALI INI...

Mengukuhkan Rangkaian Rumah Anda

Pengenalan

Beberapa tahun lalu rangkaian di rumah begitu mudah, ia hanya terdiri daripada akses tanpa wayar dan satu atau dua komputer untuk melayari internet atau permainan video dalam talian. Walaubagaimanapun, rangkaian di rumah kini telah menjadi kompleks. Kita bukan sahaja menghubungkan peranti kepada rangkaian rumah tetapi lebih daripada itu. Dalam isu ini kita akan melihat beberapa langkah mudah untuk mewujudkan rangkaian rumah yang selamat.

Editor Jemputan

Kevin Johnson adalah CEO di Secure Ideas, menguruskan **MySecurityScanner.com** dan merupakan pengajar kanan di SANS Institute. Anda boleh mendapatkan maklumat lanjut di **www.secureideas.com**.

Rangkaian Tanpa Wayar Anda

Hampir kesemua rangkaian di rumah bermula dengan rangkaian tanpa wayar (sering kali dipanggil rangkaian Wi-Fi). Ini memungkinkan anda untuk menghubungkan semua peranti ke internet, dari komputer riba dan tablet kepada konsol permainan dan televisyen, tanpa wayar. Rangkaian tanpa wayar anda perlu mempunyai sesuatu yang dipanggil access point tanpa wayar untuk berfungsi. Ini adalah peranti fizikal yang menghubungkan router internet (atau yang tersedia dalam router) dan menghantar isyarat tanpa wayar kepada peranti anda. Apabila peranti anda berhubung dengan access point, ia kemudian boleh menghubungi peranti lain dalam rangkaian rumah anda dan juga internet. Access point tanpa wayar adalah bahagian yang terpenting dalam rangkaian rumah dan kami mencadangkan langkah-langkah berikut untuk menjamin keselamatannya.

- Bagi kebanyakan access point tanpa wayar, log masuk dan kata laluan pentadbir diketahui umum dan dipaparkan. Oleh itu, pastikan log masuk dan kata laluan anda ditukar kepada sesuatu yang hanya anda tahu. Pastikan ianya unik dan tidak digunakan untuk akaun lain.
- Tetapan seterusnya adalah nama rangkaian tanpa wayar anda (kadangkala dipanggil SSID). Ini adalah nama yang akan dipaparkan pada peranti anda semasa ia mencari rangkaian tanpa wayar berdekatan. Berikan nama rangkaian yang unik supaya ianya mudah untuk anda kenali, tetapi pastikan ianya tidak mengandungi maklumat peribadi. Langkah ini tidak memberi sebarang kesan jika anda menetapkannya sebagai rangkaian tersembunyi (atau non-broadcast). Kebanyakan alatan pengimbas tanpa wayar atau penyerang yang pakar boleh mengenal pasti maklumat rangkaian tersebut dengan mudah.
- Langkah seterusnya ialah memastikan hanya orang yang anda kenali dan percaya sahaja boleh berhubung dengan rangkaian tanpa wayar anda. Pastikan tiada jiran atau orang yang tidak dikenali

Mengukuhkan Rangkaian Rumah Anda

membuat sambungan atau memantau rangkaian anda. Anda boleh menangani risiko ini dengan mudah dengan cara mengukuhkan keselamatan access point tanpa wayar anda. Pilihan terbaik buat masa ini adalah dengan menggunakan mekanisme keselamatan WPA2. Dengannya anda memerlukan kata laluan untuk menyambungkan rangkaian rumah anda, dan setelah ianya disahkan, sambungan tersebut dienkripsi. Elakkan cara lama seperti WEP atau tidak menggunakannya langsung (rangkaian terbuka). Rangkaian terbuka membenarkan sesiapa sahaja menyambung kepada rangkaian tanpa wayar anda tanpa pengesahan.

Untuk menjamin keselamatan rangkaian rumah anda pastikan anda mempunyai rangkaian tanpa wayar yang selamat, anda menggunakan OpenDNS atau perkhidmatan yang serupa, dan kesemua peranti yang berada di dalam rangkaian rumah anda dikemas kini dan terkini.

- Pastikan kata laluan yang akan digunakan oleh pengguna untuk membuat sambungan kepada rangkaian anda kukuh dan tidak mudah untuk diteka serta berbeza daripada kata laluan pentadbir. Anda mungkin perlu memasukkan kata laluan hanya sekali untuk setiap peranti kerana kata laluan tersebut akan disimpan dan diingati.
- Kebanyakan access point tanpa wayar mempunyai pilihan rangkaian tetamu. Rangkaian Tetamu membenarkan pelawat untuk membuat sambungan kepada access point tanpa wayar dan akses kepada internet, tetapi tidak kepada sebarang peranti di dalam rangkaian rumah anda. Jika anda mempunyai Rangkaian Tetamu, pastikan anda membolehkan WPA2 dan kata laluan lain untuk menggunakan rangkaian tersebut.
- Jika sukar untuk anda mengingati kata laluan yang berbeza, gunakan pengurus kata laluan untuk menyimpannya dengan selamat.

OpenDNS

Apabila rangkaian tanpa wayar anda telah dikonfigurasi, kami mencadangkan anda menetapkan rangkaian rumah anda menggunakan OpenDNS sebagai pelayan DNS (atau perkhidmatan yang sama seperti Norton ConnectSafe for Home). Apabila anda menaip nama ke dalam pelayar anda, DNS adalah cara pelayar anda tahu ke pelayar mana ia perlu disambung di internet. Perkhidmatan OpenDNS mengenal pasti laman sesawang yang dijangkiti dan menghentikan mana-mana peranti yang bersambung ke rangkaian tanpa wayar rumah anda daripada melayari laman yang dijangkiti secara tidak sengaja. Sebagai tambahan, perkhidmatan seperti ini memberikan anda kelebihan untuk menapis dan menyekat laman sesawang yang menjelikkan. Apa yang menjadikan cara ini lebih efektif adalah anda tidak perlu memasang sebarang perisian di dalam peranti anda, anda hanya perlu menukar tetapan pada access point tanpa wayar anda.

Mengukuhkan Rangkaian Rumah Anda

Peranti Anda

Langkah seterusnya adalah untuk mengetahui peranti yang bersambung kepada rangkaian rumah anda dan memastikan ianya selamat. Sebelum ini ianya mudah kerana anda mempunyai beberapa peranti yang bersambung kepada rangkaian anda. Namun sekarang hampir kesemuanya berhubung dengan rangkaian rumah anda termasuk TV, konsol permainan video, alat pengawasan bayi, pembesar suara, termometer rumah dan mungkin juga kereta anda. Apabila anda telah mengenal pasti kesemua peranti di dalam rangkaian rumah anda, anda mungkin akan terkejut dengan bilangannya. Cara terbaik untuk menjamin keselamatan semua peranti ini adalah dengan memastikan ianya menggunakan sistem operasi yang terkini. Pastikan anda membolehkan kemas kini secara automatik sekiranya ada. Jika tidak, lakukan semakan sebulan sekali, jika perlu. Sebagai tambahan, pastikan anda melawat laman sesawang penyedia rangkaian anda, kerana mereka mungkin menyediakan aplikasi percuma bagi membantu meningkatkan keselamatan rangkaian rumah anda.

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

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Network Security Scanner:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Password Managers:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

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