OUCH! | 2016.gada februāris

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

Mājas tīkla drošība

Pārskats

Pirms vairākiem gadiem mājas tīkli bija samērā vienkārši, parasti nekas vairāk kā bezvadu piekļuves punkts un viens vai divi datori sērfošanai internetā, tiešsaistes darījumiem vai spēlēm. Tomēr mājas tīkli kļūst arvien sarežģītāki. Mēs pievienojam daudz vairāk ierīces tīklam un izmantojām tās arī citiem mērķiem, ne tikai tīmekļa pārlūkošanai vai mēdiju satura vērošanai. Šajā izdevumā mēs aprakstīsim, kā jūs varat izveidot Jums un jūsu ģimenei drošu mājas tīklu.

Viesredaktors

Cheryl Conley vada drošības izglītības un informēšanas komandu Lockheed Martin, izmantojot The I Campaign™ sasniedzot vairāk kā 100,000 darbiniekus. Tas ietver arī domubiedru grupas uzņēmumā, papildus globālai pret pikšķerēšanas programmai. Sekojiet Cheryl **@conleychera**.

Jūsu bezvadu tīkli

Vairums mājas tīklu sākas ar bezvadu tīklu (dažkārt saukts arī par Wi-Fi tīklu). Šis tīkls atļauj Jums bez vadiem savienot ar internetu Jūsu ierīces, sākot no portatīviem datoriem un planšetdatoriem beidzot ar spēļu konsolēm un televizoriem. Vairums mājas bezvadu tīklu kontrolē Jūsu Interneta maršrutētājs, kas ir iekārta, ko Jūsu Interneta pakalpojumu sniedzējs uzstāda Jūsu mājā, lai pieslēgtu Jūs Internetam. Atsevišķos gadījumos bezvadu tīklu var kontrolēt atsevišķa iekārta - bezvadu piekļuves punkts, kas ir savienots ar Interneta maršrutētāju. Neatkarīgi no tā kurš no variantiem tiek izmantots, tie abi darbojas pārraidot bezvadu signālus. Dažādās iekārtas Jūsu mājā pieslēdzas bezvadu tīklam, izmantojot šos signālus. Tālāk iekārtas var savienoties ar Internetu kā arī ar citām iekārtām Jūsu mājas tīklā. Tas nozīmē, ka, lai aizsargātu Jūsu māju bezvadu tīklam jābūt drošam. Mēs iesakām šādus pasākumus.

- Nomainiet noklusēto administratora paroli Jūsu interneta maršrutētājam vai bezvadu piekļuves punktam, atkarībā no tā, kas kontrolē Jūsu bezvadu tīklu. Administratora konts ir tas, kas ļauj Jums konfigurēt bezvadu tīkla iestatījumus. Daudzi maršrutētāji vai piekļuves punkti tiek piegādāti ar noklusēto administratora lietotājvārdu un paroli, kas ir labi zināmi un pieejami Internetā. Tādēļ nomainiet administratora paroli uz tādu, kas ir pietiekami droša, unikāla un zināma tikai Jums.

Mājas tīkla drošība

- Nomainiet noklusēto tīkla nosaukumu (dažkārt to sauc par SSID). Tas ir nosaukums, ko Jūsu iekārtas redz, kad tās meklē lokālo bezvadu tīklu. Iedodat savam tīklam unikālu nosaukumu, lai to Jūs varat viegli atšķirt, taču nerakstiet tur nekādu personīgo informāciju. Nav īpaši vērts konfigurēt Jūsu tīklu kā noslēptu (vai neraidošu) jo vairums bezvadu tīklu skenēšanas rīku vai prasmīgi uzbrucēji var viegli atklāt slēptus tīklus.
- Pārliecinieties, ka tikai cilvēki kam Jūsu uzticaties var pieslēgties un izmantot Jūsu bezvadu tīklu un ka šie savienojumi ir šifrēti. Iespējojat stingru drošības līmeni. Šobrīd labākā izvēle ir izmantot drošības mehānismu, ko sauc par WPA2. Izvēloties to, lai pieslēgtos tīklam ir nepieciešama parole un pēc pieslēgšanās savienojums ir šifrēts. Neizmantojat novecojušus risinājumus, piemēram, WEP un neatstājiet tīklu vispār bez drošības (atvērts tīkls). Atvērts tīkls ļauj ikvienam pieslēgties Jūsu bezvadu tīklam bez jebkādas autentifikācijas.

Lai aizsargātu Jūsu mājas tīklu regulāri atjaunojiet programmnodrošinājumu un aizsargājiet savas iekārtas ar paroli.

- Pārliecinieties, ka parole, ko cilvēki izmanto, lai pieslēgtos Jūsu bezvadu tīklam ir atbilstoši droša un atšķirīga no administratora paroles. Atceraties, ka Jums visdrīzāk parole būs jāievada katrā ierīcē tikai vienu reizi, jo iekārtas var uzglabāt un atcerēties paroles.
- Daudzi bezvadu tīkli atbalsta tā saucamo viesa tīklu. Tas atļauj viesiem pieslēgties internetam, bet aizsargā Jūsu mājas tīklu, jo tie nevar pieslēgties citām iekārtām Jūsu mājas tīklā. Ja Jūs pievienojat viesu tīklu, iespējojiet WPA2 un izmantojat unikālu paroli šim tīklam.
- Izslēdziet WiFi aizsargāto konfigurāciju (WiFI protected setup) vai citus mehānismus, kas ļauj jaunai ierīcei pieslēgties tīklam nezinot paroli un konfigurāciju.
- Ja Jums ir grūti atcerēties paroles, izmantojat paroļu pārvaldnieku, lai tās droši saglabātu.

Neesat drošs, ka varēsiet šos pasākumus īstenot? Pajautājiet savam Interneta pakalpojumu sniedzējam, izskatiet maršrutētāja vai piekļuves punkta dokumentāciju, apmeklējat attiecīgās tīmekļa vietnes.

Mājas tīkla drošība

Jūsu iekārtas

Nākamais solis ir saprast, kas ir pieslēgts Jūsu mājas tīklam un pārliecināties, ka visas šīs iekārtas ir aizsargātas. Tas bija samērā vienkārši, kad bija pieslēgtas vien dažas iekārtas. Tomēr mūsdienu savienotajā pasaulē gandrīz jebkas var pieslēgties Jūsu tīklam - televizori, spēļu konsoles, zīdaiņu monitori, skaļruņi, termostati, iespējams pat Jūsu automašīna. Vienkāršs veids kā noteikt, kas ir pieslēdzies Jūsu tīklam ir izmantot vienkāršu tīkla skeneri, piemēram Fing. Šāda veida aplikācijas, ko Jūs varat instalēt uz datora vai mobilās iekārtas, skenē Jūsu tīklu un paziņo katru iekārtu, kas ir pieslēgta. Kad Jūs esat identificējis visas iekārtas Jūsu mājas tīklā, Jums jāpārliecinās, ka katra no šīm iekārtām ir aizsargāta. Labākais padoms ir vienmēr nodrošināt, ka to programmnodrošinājums ir atjaunots un tie izmanto jaunāko programmnodrošinājuma versiju. Kad vien iespējams izmantojat iespēju automātiski tās atjaunināt. Ja kādai no Jūsu iekārtām nepieciešama parole, izmantojiet unikālu, drošu parole. Visbeidzot apmeklējat Jūsu interneta pakalpojuma sniedzēja tīmekļa vietni, jo tas var sniegt padomus, vai piedāvāt risinājumus Jūsu mājas tīkla aizsardzībai.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni http://www.securingthehuman.org.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Paroles:	https://securingthehuman.sans.org/ouch/2015#april2015
Paroļu pārvaldnieks:	https://securingthehuman.sans.org/ouch/2015#october2015
Jūsu planšetdatora drošība:	https://securingthehuman.sans.org/ouch/2016#january2016
Jūsu mājas tīkla plānošana:	http://l.rud.is/home-network-mapping

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Tulkojums: Edgars Tauriņš