OUCH! | 2016m. vasario mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Jūsų belaidis tinklas
- Jūsų įrenginiai

Jūsų namų tinklo apsauga

Apžvalga

Prieš keletą metų namų tinklai buvo gana paprasti, kadangi juos sudarė tik belaidžio ryšio prieigos taškas ir vienas ar du kompiuteriai, kuriais buvo naršoma po internetą, apsiperkama internetu ar žaidžiami žaidimai. Tačiau palaipsniui namų tinklai tapo ganėtinai sudėtingais. Dabar prie šių tinklų jungiame žymiai daugiau įrenginių, kuriuos naudojame ne vien tik naršymui po internetą ar naujienų skaitymui. Šiame naujienlaiškyje papasakosime, kaip sau ir savo šeimai galite sukurti saugų namų tinklą.

Kviestinė redaktorė

Cheryl Conley vadovauja „Lockheed Martin“ įmonės švietimo saugumo klausimais ir informuotumo komandai, vesdama The I Campaign™ kampaniją, kurioje dalyvauja daugiau nei 100 000 darbuotojų. Tai apima tiek darbą įmonės aljanse, tiek tikslinių grupių konsultavimą ir darbą pasaulinės sukčiavimo programos srityje. Cheryl veiklą galite sekti Twitter paskyroje įvedę **@conleychera**.

Jūsų belaidis tinklas

Beveik kiekvienuose namuose namų tinklas prasideda nuo belaidžio tinklo. Bevieliu būdu galite bet kurį iš savo įrenginių prijungti prie interneto, pradedant nešiojamaisiais ar planšetiniais kompiuteriais ir baigiant žaidimų pultais ar televizija. Dauguma namų tinklų yra valdomi naudojant interneto maršruto parinktuvą, t.y. interneto paslaugų tiekėjo jūsų namuose įdiegtą įrenginį, kuriuo jungiamasi prie interneto. Tačiau, kai kuriais atvejais, jūsų belaidis tinklas gali būti valdomas atskiros sistemos, vadinamos belaidžio ryšio prieigos tašku, kuris jungiasi prie jūsų interneto maršruto parinktuvo. Nepriklausomai nuo to, kokį belaidį tinklą naudojate, abu šie prietaisai veikia tokiu pat būdu – siųsdami belaidžio ryšio signalus. Įvairūs įrenginiai prie belaidžio jūsų namų tinklo jungiasi per šiuos signalus. Iš čia prie interneto gali jungtis ne tik šie įrenginiai bet ir kiti jūsų namų tinkle esantys įrenginiai. Tai reiškia, kad svarbiausias žingsnis, norint apsaugoti savo namus yra apsaugoti savo belaidį tinklą. Norėdami jį apsaugoti, turėtumėte atlikti toliau pateiktus veiksmus.

- Pakeiskite numatytą administratoriaus slaptažodį į savo interneto maršruto parinktuvo arba belaidžio ryšio prieigos taško, valdančio jūsų belaidį tinklą. Administratoriaus paskyra yra ta vieta, kurioje galite konfigūruoti savo belaidžio tinklo nustatymus. Problema yra ta, kad daugumoje interneto maršruto parinktuvų arba belaidžio ryšio prieigos taškų yra pristatomi su jau numatytu administratoriaus prisijungimo vardu ir slaptažodžiu, kuris yra gerai visiems žinomas ir dažnai skelbiamas internete. Todėl įsitikinkite, kad administratoriaus slaptažodį pasikeisite į patikimą ir unikalų, kurį žinosite tik jūs.

Jūsų namų tinklo apsauga

Siekdami apsaugoti savo namų tinklą įjunkite visų įrenginių naujinimus, apsaugokite juos slaptažodžiu.

- Pakeiskite savo belaidžio tinklo numatytąjį pavadinimą (dar vadinamą trumpiniu SSID). Tai pavadinimas, kurį matys jūsų įrenginiai, ieškodami vietinio belaidžio tinklo. Sugalvokite savo tinklui unikalų pavadinimą, kurį būtų lengva atpažinti, tačiau įsitikinkite, kad jo pavadinimo nesudarys jūsų asmeninė informacija. Nelabai naudinga savo tinklą nustatyti kaip paslėptą (arba nesiunčiantį signalo), kadangi dauguma belaidžio tinklo ieškančių priemonių arba bet kuris patyręs nusikaltėlis gali lengvai paslėptus tinklus atrasti.
- Įsitikinkite, kad prie jūsų belaidžio tinklo galės prisijungti tik tie žmonės, kuriais jūs pasitikite ir kad tai bus šifruotas ryšys. Tai galite padaryti įjungdami patikimą apsaugą. Šiuo metu geriausias sprendimas yra naudoti apsaugos mechanizmą, kuris vadinasi WPA2. Įjungus jį, žmonių, norinčių prisijungti prie jūsų namų tinklo, bus prašoma įvesti slaptažodį, o jiems prisijungus visa jų internetinė veikla bus šifruojama. Įsitikinkite, kad nenaudojate tokių pasenusių ir nebegaliojančių apsaugos metodų, kaip WEP. Nenaudodami jokių saugumo priemonių, prieigą prie tinklo paliekate atvirą. Atvirais tinklais prie jūsų belaidžio tinklo gali jungtis bet kas be jokio tapatybės nustatymo.
- Įsitikinkite, kad žmonės, besijungiantys prie jūsų belaidžio tinklo naudoja patikimą slaptažodį ir kad jis nesutampa su administratoriaus slaptažodžiu. Prisiminkite, kad slaptažodį į visus savo įrenginius turėsite įvesti tik kartą, kadangi jie jį išsaugos ir prisimins.
- Dauguma belaidžių tinklų palaiko tai, kas yra vadinama svečių tinklu. Šis metodas ne tik leidžia lankytojams jungtis prie interneto, bet ir apsaugo jūsų namų tinklą, kadangi lankytojai negali prisijungti prie jokių kitų jūsų namų tinkle esančių įrenginių. Jei sukuriate svečių tinklą, įsitikinkite, kad yra įjungta WPA2 apsauga, o tinklas yra apsaugotas patikimu slaptažodžiu.
- Išjunkite belaidžio ryšio apsaugos nustatymą arba kitokį mechanizmą, leidžiantį naujam įrenginiui jungtis prie tinklo nežinant slaptažodžio ir konfigūracijos parinkčių.
- Jei sunku prisiminti visus šiuos skirtingus slaptažodžius, rekomenduojame naudoti slaptažodžių tvarkytuvę, kuri jums padės juos saugiai išsaugoti.

Jūsų namų tinklo apsauga

Nežinote kaip tai padaryti? Paklauskite to savo interneto paslaugų tiekėjo, patikrinkite kartu su interneto maršruto parinktuvu ar belaidžio ryšio prieigos tašku gautus dokumentus, arba apsilankykite atitinkamoje jų svetainėje.

Jūsų įrenginiai

Sekantis žingsnis yra sužinoti, kas yra prijungta prie jūsų namų tinklo ir įsitikinti, jog visi šie įrenginiai yra patikimi. Kai būdavo prijungti vos keli įrenginiai, tai padaryti buvo paprasta. Tačiau šiuolaikiniame pasaulyje, kuris yra „visada prisijungęs prie interneto“, prie jūsų namų tinklo gali jungtis beveik bet kas, įskaitant televizorius, žaidimo pultus, kūdikio stebėjimo kameras, garsiakalbius, termostato įrenginį ar net jūsų automobilį. Vienintelis paprastas būdas nustatyti, kas yra prijungta prie jūsų namų tinklo yra naudoti paprasčiausią tinklo skaitytuvą, pavyzdžiui, Fing. Šios kompiuteryje arba mobiliajame telefone įdiegiamos programos nuskenuoja jūsų belaidį tinklą ir praneša apie kiekvieną tinkle prijungtą įrenginį. Nustatę visus prie namų tinklo prijungtus įrenginius turite įsitikinti, kad visi jie yra patikimi. Geriausias būdas tai padaryti yra įsitikinti, kad jie turi naujausią operacinės sistemos/programinės aparatinės įrangos versiją. Kai tik įmanoma, įjunkite juose automatinį atnaujinimą. Jei kuriame nors iš jūsų įrenginių reikia nustatyti slaptažodį, visada naudokite unikalų ir patikimą slaptažodį. Galiausiai, apsilankykite savo interneto paslaugų tiekėjo svetainėje, kadangi jie gali siūlyti nemokamas priemones, padėsiančias jums apsaugoti savo namų tinklą.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę http://www.securingthehuman.org.

Šaltiniai

Slaptafrazės:	https://securingthehuman.sans.org/ouch/2015#april2015
Slaptažodžių tvarkytuvės:	https://securingthehuman.sans.org/ouch/2015#october2015
Jūsų naujos planšetės apsauga:	https://securingthehuman.sans.org/ouch/2016#january2016
Jūsų namų tinklo atvaizdavimas:	http://l.rud.is/home-network-mapping

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.