OUCH! | 2018 m. rugpjūčio mėn.

SANS SECURITY AWARENESS

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

Išmanieji namų įrenginiai

Kas yra išmanieji namų įrenginiai?

Įprastai prie interneto būtų galima prijungti vos keletą jūsų namuose esančių įrenginių, pavyzdžiui, nešiojamąjį kompiuterį, išmanųjį telefoną arba žaidimų konsolę. Kaip bebūtų, šiandien prie interneto yra jungiama vis daugiau įrenginių, pradedant elektros lemputėmis ar garsiakalbiais ir baigiant durų ar net nuosavo automobilio užraktais. Greitai prie interneto galės būti prijungtas beveik kiekvienas jūsų namuose esantis įrenginys. Šie, prie interneto jungiami, įrenginiai yra dažnai vadinami „daiktų internetu“ (angl. Internet of Things, IoT) arba „išmaniaisiais namų įrenginiais“. Nors jie yra labai patogūs, tačiau jie gali būti ir pavojingi.

Kokia yra problema?

Kuo daugiau įrenginių yra prijungta prie jūsų namų interneto, tuo didesnė tikimybė, kad kažkas negero gali nutikti. Programišiai gali užprogramuoti, kad jūsų įrenginiai atakuotų kitus įrenginius, pardavėjai gali rinkti daug informacijos apie jūsų veiklą, o jūsų įrenginiai gali būti ne tik užkrėsti virusais, bet jūs galite netekti ir galimybės prie jų prisijungti. Dauguma šiuos įrenginius gaminančių įmonių neturi jokios patirties, susijusios su kibernetiniu saugumu, o patį saugumą vertina kaip papildomas sąnaudas. Todėl dauguma jūsų įsigytų įrenginių neturi jokių arba turi mažai saugumo galimybių. Pavyzdžiui, kai kuriuose įrenginiuose yra naudojami numatytieji slaptažodžiai, kuriuos gali žinoti bet kas ir kurių negalima atnaujinti arba pakeisti.

Kaip galiu apsisaugoti?

Taigi, ką galite padaryti? Mes neabejotinai norime, kad prie interneto jungiamais įrenginiais naudotumėtės saugiai ir užtikrintai. Šie įrenginiai gali pasižymėti nuostabiomis, gyvenimą palengvinančiomis, funkcijomis. Be to, tobulėjant technologijoms gali nelikti nieko kito, kaip tik naudoti išmaniuosius įrenginius. Štai keli pagrindiniai veiksmai, kurių galite imtis, siekdami apsisaugoti:

Prie interneto junkite tik tada, kai reikia. Paprasčiausias būdas apsaugoti įrenginį, yra nejungti jo prie interneto. Jei jūsų įrenginiui nereikia interneto, tada nejunkite jo prie savo belaidžio tinklo. Ar jums išties reikia, kad duonos skrudintuvas siųstų pranešimus į jūsų mobilųjį telefoną?

Žinokite, ką esate prijungę prie interneto. Kokius įrenginius esate prijungę prie savo namų tinklo? Nežinote? O galbūt neatsimenate? Išjunkite savo belaidį tinklą ir patikrinkite, kuris iš jų nebeveikia. Galbūt nenustatysite visų įrenginių, tačiau nustebsite, kiek daug įrenginių tiesiog pamiršote.

Pastoviai atnaujinkite programinę įrangą. Kaip kompiuterį ar kitus mobiliuosius įrenginius, taip ir visus kitus įrenginius reikia atnaujinti. Jei jūsų įrenginys turi automatinio atnaujinimo parinktį, įjunkite ją.

Slaptažodžiai. Pakeiskite esamus savo įrenginių slaptažodžius unikalesnėmis ir patikimesnėmis slaptafrazėmis, kurias žinotumėte tik jūs. Greičiausiai jas turėsite įvesti tik kartą. Sudėtinga prisiminti visas slaptafrazes? Nesijaudinkite, mums taip pat. Apsvarstykite galimybę naudoti slaptažodžių tvarkyklę, kurioje jie visi būtų patikimai saugomi.

Privatumo parinktys. Jei įrenginyje įmanoma nustatyti privatumo parinktis, apribokite informacijos kiekį, kurį jis renka arba kuriuo dalinasi. Vienas iš sprendimų būtų paprasčiausiai atjungti bet kokios informacijos dalinimosi funkcijas.

Pardavėjas. Pirkite įrenginius tik iš žinomos ir patikimos įmonės. Ieškokite saugumu pasižyminčių produktų, pavyzdžiui, leidžiančių įjungti automatinį atnaujinimą, pakeisti numatytąjį slaptažodį ir privatumo nustatymus.

Nuolatinis klausymasis. Jei įrenginys reaguoja į balso komandas, tuomet jis pastoviai jūsų klausosi. Pavyzdžiui, jūsų „Alexa“ ir „Google Home“ įrenginiai gali įrašinėti konfidencialius pokalbius. Atsižvelkite į tai prieš nuspręsdami, kur namuose laikysite padėtus įrenginius ir peržiūrėkite jų privatumo parinktis.

Svečių tinklas. Apsvarstykite galimybę savo išmaniuosius namų įrenginius jungti prie atskiro „svečių“, o ne pagrindinio belaidžio tinklo, prie kurio jungiate savo kompiuterius ir kitus mobiliuosius įrenginius. Tokiu būdu, virusais užkrėtus bet kokį išmanųjį įrenginį, jūsų kompiuteriai ir kiti mobilieji įrenginiai, prijungti prie pagrindinio tinklo, liks saugūs.

Neverta bijoti naujų technologijų, tačiau verta suprasti jų keliamą riziką. Atlikę šiuos kelis paprastus veiksmus, padėsite kurti žymiai saugesnius išmaniuosius namus.

Kviestinė redaktorė

Robert M. Lee *(@RobertMLee) yra atestuotas dėstytojas SANS institute ir kursų FOR578 „Kibernetinių grėsmių žvalgyba“ bei ICS515 „Pramonės kontrolės sistemų (ICS) aktyvi gynyba ir reagavimas į incidentus“ autorius. Robert'as taip pat yra pramoninio kibernetinio saugumo firmos „Dragos“ generalinis direktorius ir įkūrėjas.*

Šaltiniai

Slaptafrazės:	https://www.sans.org/u/GEB
Slaptažodžių tvarkyklės:	https://www.sans.org/u/GEG
Jūsų namų tinklo apsauga:	https://www.sans.org/u/GEL