Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

Daiktų internetas

Kas yra daiktų internetas (angl. Internet of Things)?

Praeityje technologijos buvo gana paprastos – tereikėdavo kompiuterį prijungti prie interneto ir naudoti jį kasdieninėje veikloje. Tuomet technologijos tapo pažangesnės ir mūsų gyvenimuose pasirodė tokie nešiojamieji įrenginiai kaip išmanieji telefonai ar planšetiniai kompiuteriai. Dabar šie įrenginiai ne tik pasižymi stalinių kompiuterių galia, bet ir telpa į mažiausias kišenes. Tapę mobilesniais, šie įrenginiai taip pat susidūrė su unikaliais saugumo iššūkiais. Šiuo metu naujausias ir didžiausias technikos pasiekimas yra daiktų internetas. Daiktų internetas, dažnai trupinamas DI, yra susijęs su kasdieninių įrenginių jungimu prie interneto, pradedant durų skambučiais ir lemputėmis, baigiant žaislinėmis lėlėmis ir termostatais. Prijungti prie interneto, šie daiktai gali žymiai palengvinti mūsų gyvenimus, pavyzdžiui, kambariuose automatiškai įsijungs šviesa, jūsų telefonui nustačius, kad esate arti namų. Daiktų interneto rinka kuriasi nepaprastu greičiu, kas savaitę rinkoje pasirodant vis naujesniems prietaisams. Tačiau kaip ir mobilieji įrenginiai, su daiktų internetu susieti prietaisai turi savų apsaugos problemų. Šiame naujienlaiškyje paaiškinsime, kokie tai pavojai ir ko galite imtis, siekdami apsaugoti su daiktų internetu susietus savo prietaisus, namus ir galiausiai savo šeimos narius.

Kviestinė redaktorė

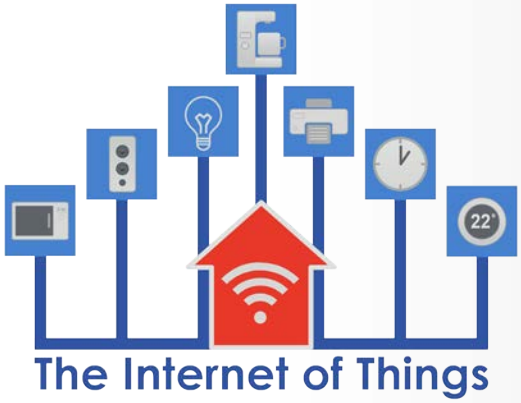
James Lyne (**@jameslyne**) yra apsaugos firmos „Sophos“ pasaulinis saugumo tyrimų vadovas. Jis atvirai prisipažįsta esantis „dideliu moksliuku“, o jo techninė patirtis apima daugybę saugumo sričių. James yra sertifikuotas dėstytojas „SANS“ institute ir dažnas pramoninių konferencijų vedėjas.

Daiktų interneto problemos

Daiktų interneto pranašumas yra tas, kad daugelį šių prietaisų yra gana paprasta naudoti. Pavyzdžiui, įjungus kavos aparatą, jis paprašo leisti prisijungti prie jūsų namų belaidžio tinklo. Tačiau visas tas paprastumas turi savo kainą. Didžiausia prietaisų, susietų su daiktų internetu, problema yra ta, kad dauguma juos gaminančių įmonių neturi jokios patirties saugumo srityje, nes jų pagrindinė kvalifikacija yra gaminti buitinius prietaisus. O galbūt tai tiesiog naujokai, bandantys sukurti kuo efektyvesnį produktą per kuo trumpesnį laiką, pavyzdžiui, naudodamiesi finansavimo internetu platforma „Kickstarter“. Šios organizacijos labiau orientuojasi į pelną, o ne į kibernetinį saugumą. Todėl daugumoje šiais laikais įsigytų prietaisų, susijusių su daiktų internetu, yra įdiegta tik menka apsauga arba jos nėra išvis. Pavyzdžiui, kai kuriuose prietaisuose yra numatyti gerai žinomi slaptažodžiai, kurie galbūt netgi yra paskelbti internete ir negali būti

Daiktų internetas

keičiami. Be to, daugumoje šių prietaisų nėra parinkties arba galimybės juos konfigūruoti, todėl naudojatės tuo, kas jums yra pristatoma. Dar blogiau yra tai, kad daugelį šių prietaisų gali būti sudėtinga atnaujinti, o galbūt to padaryti net neįmanoma. Todėl dauguma jūsų naudojamų prietaisų, susijusių su daiktų internetu, gali greitai pasenti ir likti su nepataisomais pažeidimais, dėl kurių visad jausite pavojų.



Žinokite, kokius daiktų interneto įrenginius esate prijungę prie savo tinklo, izoliuokite juos, kai tik galite, diekite naujausius atnaujinimus ir naudokite sudėtingus slaptažodžius.

Daiktų internetą naudojančių prietaisų apsauga

Ko galite imtis? Mes tikrai norime, kad mėgautumėtės prietaisų, susijusių su daiktų internetu, teikiamais privalumais saugiai ir veiksmingai. Šie prietaisai gali turėti nepaprastų, gyvenimą palengvinančių, savybių, padėti taupyti pinigus ir, tikėtina, pagerinti fizinę jūsų namų apsaugą. Be to, technologijoms tobulėjant, gali nebelikti jokio kito pasirinkimo kaip tik įsigyti arba naudoti prietaisus, susijusius su daiktų internetu. Žemiau pateikiame keletą veiksmų, kurių galite imtis, norėdami apsaugoti tiek save, tiek su daiktų internetu susijusius prietaisus.

- **Prie interneto junkite tik tai, ko jums reikia**. Paprasčiausias būdas apsaugoti su daiktų internetu susijusį prietaisą yra nejungti jo prie interneto. Jei nebūtina, kad prietaisas veiktų internetu, tiesiog nejunkite jo prie savo belaidžio tinklo.
- **Atskiras belaidis tinklas**. Jei visgi reikia, kad prietaisai veiktų internetu, apsvarstykite galimybę jiems sukurti atskirą belaidį tinklą. Daugumoje belaidžio tinklo prieigos taškų galima sukurti tokius papildomus tinklus kaip, pavyzdžiui, svečių tinklą. Kitas variantas yra įsigyti papildomą belaidžio tinklo prieigos tašką, skirtą daiktams, susijusiems su daiktų internetu. Taip tokie prietaisai lieka veikti visiškai atskirame tinkle. Jais negalima pasinaudoti, siekiant pažeisti arba įsilaužti į kurį nors kompiuterį ar mobiliuosius įrenginius, prijungtus prie jūsų pagrindinio namų tinklo (kuris lieka pagrindiniu kibernetinių nusikaltėlių traukos objektu).
- **Atnaujinkite, jei tik įmanoma**. Atnaujinti prietaisus, susijusius su daiktų internetu, reikia lygiai taip pat kaip ir kompiuterį arba mobiliuosius įrenginius. Jei jūsų prietaisas, susijęs su daiktų internetu, turi parinktį, leidžiančią jo sistemą atnaujinti automatiškai, įjunkite ją.

Daiktų internetas

- **Patikimi slaptažodžiai**. Pakeiskite bet kokius slaptažodžius, esančius prietaisuose, susijusiuose su daiktų internetu, į unikalias ir patikimas slaptafrazes, kurias žinotumėte tik jūs. Negalite prisiminti visų savo slaptafrazių? Nesijaudinkite, nes to padaryti negalime ir mes. Apsvarstykite galimybę naudoti slaptažodžių tvarkytuvę, kur galėtumėte juos visus saugiai laikyti.
- **Privatumo parinktys**. Jei jūsų prietaise, susijusiame su daiktų internetu, galima konfigūruoti privatumo parinktis, tuomet apribokite informacijos kiekį, kuriuo jis gali dalintis. Vienas iš sprendimų yra paprasčiausiai išjungti bet kokias galimybes dalintis informacija.
- **Apsvarstykite galimybę prietaisą pakeisti**. Tam tikru momentu, kai pastebėsite, kad turimas prietaisas, susijęs su daiktų internetu, yra pernelyg pažeidžiamas ir to pataisyti neįmanoma, arba atsiradus naujesniems ir saugesniems prietaisams, galite norėti savo turimą prietaisą pakeisti.

Nėra vieno varianto, kuris tiktų kiekvienam prietaisui, taigi verta pasidomėti geriausiais praktikos pavyzdžiais ir bet kokiais leidiniais, aprašančiais, kaip tuos prietaisus galima apsaugoti. Deja, dauguma prietaisų, susijusių su daiktų internetu, nebuvo kuriami galvojant apie kibernetinį saugumą, taigi dauguma gamintojų nepateikia daug su saugumu susijusios informacijos. Visgi, didėjant suvokimui apie kibernetinį saugumą, tikimės išvysti vis daugiau šių prietaisų pardavėjų, įdiegiančių saugumo sistemas ir suteikiančių daugiau informacijos apie tai, kaip galima juos apsaugoti bei atnaujinti.

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 apsauga:	https://securingthehuman.sans.org/ouch/2016#february2016

Licencija

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