OUCH! | 2016.gada Maijs

Ikmēneša biļetens par informācijas tehnoloģiju drošību datoru lietotājiem

OUCH!

ŠAJĀ NUMMURĀ …

Lietiskais internets (IoT)

Ko nozīmē lietiskais internets (IoT)

Pagātnē tehnoloģijas bija salīdzinoši vienkāršas, jūs pievienojāt datoru internetam un izmantojāt to savām ikdienas vajadzībām. Tad tehnoloģijas attīstījās, mūsu dzīvē ienākot mobilajām ierīcēm - viedtālruņiem un planšetdatoriem. Šīs ierīces piedāvā galda datora iespējas jūsu kabatā. Mobilajām ierīcēm nāk līdzi savādāki drošības apdraudējumi. Tagad nākamais attīstības posms ir Lietiskais internets. Lietiskais internets, ko bieži saīsina, izmantojot anglisko terminu Internet of Things jeb IoT, nozīmē ikdienas ierīču pieslēgšanu internetam - sākot ar durvju zvaniem un spuldzēm līdz rotaļlietām un termostatiem. Pieslēgtās ierīces var ļoti atvieglot dzīvi, piemēram, ieslēdzot gaismu istabā brīdī, kad Jūsu telefons saprot, ka Jūs tuvojaties mājām. IoT tirgus attīstās ļoti strauji un jaunas iekārtas parādās katru nedēļu. Tomēr, tieši tāpat kā ar mobilajām ierīcēm, IoT ierīces arī nes līdzi drošības apdraudējumus. Šajā rakstā mēs palīdzēsim Jums saprast šos riskus un palīdzēsim apzināties, ko Jūs varat darīt, lai padarītu Jūsu IoT ierīces drošākas, tādejādi aizsargājot Jūsu māju un galu gala Jūsu ģimeni.

Viesredaktors

James Lyne (**@jameslyne**) ir globālās drošības izpētes vadītājs drošības uzņēmumā Sophos. Viņa tehniskās zināšanas aptver dažādas drošības jomas. Viņš ir sertificēts pasniedzējs SANS institūtā un bieži uzstājas ar vadošajām prezentācijām industrijas konferencēs.

IoT problēmas

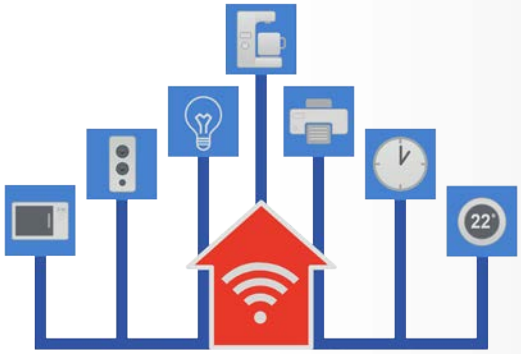
IoT stiprā puse ir tāda, ka vairums šo ierīču ir vienkāršas. Piemēram, Jūs vienkārši pievienojat savu kafijas automātu barošanas avotam un tas prasa, lai to pieslēdz Jūsu mājas bezvadu tīklam. Tomēr vienkāršība maksā. Lielākā problēma ar IoT ierīcēm ir tāda, ka daudziem ražotājiem nav pieredze ar drošības jautājumiem, viņu zināšanas aptver sadzīves iekārtu ražošanu. Vai arī ražotājs ir jauns uzņēmums, kas grib attīstīt produktu pēc iespējas efektīvāk un ātrāk, piemēram, izmantojot Kickstarter. Šādas organizācijas koncentrējas uz peļņu, nevis kiberdrošību. Tā rezultātā daudzās IoT iekārtās, ko var iegādāties šobrīd, par drošību ir padomāts visai maz. Piemēram, dažām ir tikai noklusētās paroles, kas ir labi zināmas, iespējams, pat publicētas internetā, un tās nav iespējams mainīt. Papildu daudzām ierīcēm nav iespējams veikt konfigurāciju,

Lietiskais internets (IoT)

un Jums jāsamierinās ar to, kas ir piegādāts. Vēl ļaunāk, daudzas ierīces nevar arī atjaunināt vai arī atjaunināšanas process ir ļoti sarežģīts. Tā rezultātā daudzas IoT ierīces ātri noveco, tām tiek atklātas ievainojamības un tās paliek pastāvīgi apdraudētas.

IoT iekārtu aizsardzība

Tātad, ko Jūs varat darīt? Mēs noteikti gribam izmantot IoT iespējas droši un efektīvi. Šīs ierīces var nodrošināt brīnišķīgas lietas, kas atvieglo Jūsu dzīvi, ietaupa naudu un, iespējams, uzlabo fizisko mājas drošību. Papildu tam, attīstoties tehnoloģijām, Jums iespējams vairs nebūs izvēles - būs jāizmanto vai jāiegādājas IoT ierīces. Šeit ir daži ieteikumi, kā aizsargāt Jūs un Jūsu IoT ierīces.



Ziniet, kādas IoT iekārtas esat pieslēguši savam tīklam, pēc iespējas tās izolējiet, atjauniniet un aizsargājiet ar drošām parolēm.

- **Pievienojiet tikai to, kas Jums nepieciešams**: Vienkāršākais veids, kā aizsargāt IoT ierīci, ir nepieslēgt to internetam. Ja Jums nav nepieciešams, ka ierīce atrodas tiešsaistē, nepieslēdziet to Jūsu wi-Fi tīklam.
- **Atsevišķs Wi-Fi tīkls**: Ja Jums ir nepieciešams ierīci pieslēgt tīklam, apsveriet iespēju izveidot atsevišķu Wi-Fi tīklu tikai IoT ierīcēm. Daudziem Wi-Fi piekļuves punktiem ir iespēja izveidot papildu tīklus, piemēram, Viesu tīklu. Cita iespēja ir iegādāties piekļuves punktu tikai šīm ierīcēm. Tas nodrošina, ka IoT ierīces atrodas izolētā tīklā, kur nevar tikt izmantotas, lai nodarītu kaitējumu Jūsu datoram vai mobilajām ierīcēm, kas pieslēgtas Jūsu mājas pamata tīklam (kas tomēr ļaundariem interesē vairāk).
- **Atjauniniet, kad iespējams**: Tieši tāpat kā datoru un mobilās ierīces arī IoT ierīces atjauniniet, kad vien tas ir iespējams. Ja ierīcei ir automātiska atjaunināšanas iespēja, iespējojiet to.
- **Drošas paroles**: Nomainiet visas paroles Jūsu ierīcēs uz unikālām, drošām parolēm, kas zināmas tikai Jums. Neuztraucieties par to, ka nevarēsiet visas paroles atcerēties. Izmantojiet paroļu pārvaldnieku to drošai uzglabāšanai.
- **Privātuma iespējas**: Ja Jūsu IoT ierīce atļauj Jums konfigurēt privātuma iestatījumus, ierobežojiet informāciju, ko tā izplata. Viena iespēja ir atslēgt visas informācijas nosūtīšanas iespējas.

Lietiskais internets (IoT)

- **Apsveriet nomaiņu**: Kādā brīdī Jums, iespējams, būs jānomaina IoT ierīce, kad iepriekšējā parādīsies pārāk daudz drošības ievainojamību, kas nevar tikt novērstas, vai ir parādījušās jaunākas ierīces ar daudz lielākām drošības iespējām.

.

Nav vienota risinājuma visām ierīcēm, tādēļ ir vērts izskatīt piemērus un publikācijas, kas apraksta, kā uzlabot tieši konkrētās IoT ierīces drošību. Diemžēl vairums IoT ierīču nav izstrādātas, ņemot vērā drošības prasības, un ražotāji bieži nepiedāvā nekādu drošības informāciju. Tomēr zināšanas par kiberdrošību palielinās, tādēļ ceram, ka aizvien vairāk IoT ierīču ražotāju iebūvēs drošību savās iekārtās un nodrošinās vairāk informācijas par to, kā šīs ierīces aizsargāt un atjaunināt.

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 pārvaldnieki:	https://securingthehuman.sans.org/ouch/2015#october2015
Jūsu jaunā planšetdatora drošība:	https://securingthehuman.sans.org/ouch/2016#january2016
Mājas tīkla drošība:	https://securingthehuman.sans.org/ouch/2016#february2016

License

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