Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

Internet of Things (IoT)

Mikä on Internet Of Things (IoT)

Ennen teknologia oli suhteellisen yksinkertaista, käyttäjä vaan yhdisti tietokoneensa verkkoon ja käytti laitetta päivittäisiin aktiviteetteihin. Teknologia on kuitenkin edennyt merkittävästi ja yksi suuri muutos on verkkoon liitettävät mobiililaitteet. Moni käyttäjä on vaihtanut tietokoneensa mobiililaitteisiin ja vaikka nämä laitteet voivat olla monessa asiassa vähintään yhtä tehokkaita kuin tietokoneet, näihin laitteisiin liittyy omia, ainutlaatuisia turvallisuushaasteita. Viime vuosien suurin harppaus on nimeltään Internet of Things (IoT). IoT:lla käsitetään erinäiset päivittäin käytettävät laitteet, jotka ovat yhteydessä verkkoon, mukaan lukien ovikellot, lamput, lelut ja termostaatit. Nämä laitteet tekevät päivittäisestä elämästämme helpompaa, esimerkiksi laittamalla valot tai lämmityksen päälle puolestasi automaattisesti kotiin saavuttuasi. IoT-markkina kasvaa merkittävää vauhtia ja uusia laitteita julkaistaan viikoittain. Aivan kuten mobiililaitteiden kanssa, myös IoT-laitteisiin sisältyy uusia turvallisuushaasteita ja tässä uutiskirjeessä autamme sinua ymmärtämään nämä haasteet ja kerromme miten voit suojata IoT-laitteesi, kotisi ja tämän myötä koko perheesi.

Vierastoimittaja

James Lyne (**@jameslyne**) vastaa globaalisti turvallisuuteen liittyvästä tutkimuksesta Sophos-nimisessä turvallisuusalan yrityksessä. Hänen tekninen osaamisensa ulottuu useisiin tietoturvan osa-alueisiin ja hän toimii sertifioituna kouluttajana SANS-instituutilla. James myös esiintyy usein alan konferensseissa.

IoT:n haasteet

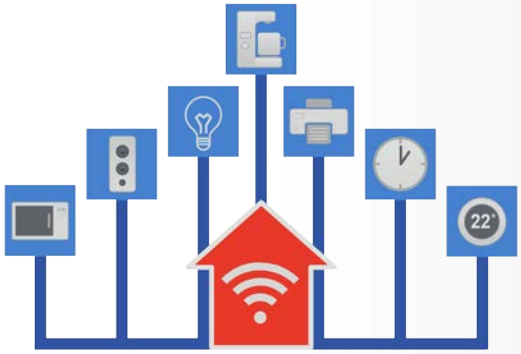
IoT-laitteiden suurin vahvuus on laitteiden yksinkertaisuus. Yksinkertaisimmillaan kytket kahvinkeittimesi virtapistokkeen kiinni ja laite pyytää lupaa liittyä kotiverkkoosi. Yksinkertaisuudella on kuitenkin hintansa ja suurin haaste IoT-laitteiden kanssa on se, että useimmilla laitevalmistajilla ei ole lainkaan kokemusta tietoturvasta vaan heidän osaamisesta liittyy pääasiassa laitteiden tekniseen kehittämiseen. Toisaalta valmistaja voi olla startup-tyyppinen pieni yritys, joka yrittää tuoda markkinoille laitteen mahdollisimman nopeasti, esimerkiksi joukkorahoitusta käyttäen. Nämä yritykset keskittyvät yleensä tulojen maksimointiin tietoturvan sijaan. Monissa laitteissa on käytössä esim. oletussalasana, jotka joissakin tapauksessa saattavat olla yleisessä tiedossa verkossa. Lisäksi monissa laitteissa ei edes ole mahdollisuutta muuttaa

Internet of Things (IoT)

turvallisuusominaisuuksia, vaan käyttäjä on pakotettu käyttämään laitteen määrittelemiä asetuksia. Laitteita on yleensä hankalaa tai joissakin tapauksissa mahdotonta päivittää. Näistä syistä, käyttämäsi IoT-laitteet sisältävät monia tunnettuja haavoittuvuuksia, joita ei pysty korjaamaan ja tämän vuoksi jättävät sinut alttiiksi uhille.

IoT-laitteiden turvaaminen

Mitä käyttäjä voi itse asialle tehdä? Toki haluamme että saat IoT-laitteistasi kaiken hyödyn irti tietoturvallisesti ja tehokkaasti. Nämä laitteet tarjoavat useita ominaisuuksia, jotka tekevät elämästä helpompaa, säästävät rahaa ja joissakin tapauksissa jopa tehostavat kotisi turvallisuutta. Voi olla, että teknologian vielä kehityttyä ei ole mahdollista edes käyttää muunlaisia laitteita. Alla on lueteltu asioita, joita voit tehdä itsesi ja laitteidesi suojaamiseksi.



Tiedä mitä IoT-laitteita olet kytkenyt verkkoosi, eristä ne aina kun mahdollista, pidä ne päivitettyinä ja suojaa ne laadukkailla salasanoilla.

- **Liitä vain laitteita mitä tarvitset**: Yksinkertaisin tapa IoT-laitteiden suojaamiseen on olla yhdistämättä niitä verkkoon. Jos laitteen ei ole välttämätöntä olla yhteydessä verkkoon, älä yhdistä sitä.
- **Erillinen verkko**: Jos IoT-laitteesi pitää olla verkossa, harkitse erillisen verkon luomista näitä laitteita varten. Monissa reitittimissä on mahdollisuus luoda monia eri verkkoja, esim. vierasverkko. Toinen vaihtoehto on ostaa erillinen reititin vain IoT-laitteita varten. Näillä keinoilla saat pidettyä IoT-laitteesi eristettynä ja näitä ei pysty käyttämään haitantekoon varsinaisessa verkossasi (joka yleensä kiinnostaa rikollisia enemmän).
- **Päivitä aina kun mahdollista**: Aivan kuten tietokoneet ja mobiililaitteet, päivitä IoT-laitteesi aina kun niihin on saatavilla päivityksiä. Jos IoT-laitteesi mahdollistaa automaattiset päivitykset, kytke ne päälle.
- **Vahvat salasanat**: Vaihda IoT-laitteidesi salasanat vahvoiksi, ainutlaatuisiksi salasanoiksi, jotka vain sinä tiedät. Onko sinulla vaikeuksia muistaa salasanojasi? Älä huoli, sama ongelma on monilla muillakin. Harkitse salasanahallintasovelluksen käyttöönottoa, tämä tekee salasanojen hallinnasta mutkatonta.
- **Yksityisyysasetukset**: Jos IoT-laitteesi mahdollistaa yksityisyysasetusten muuttamisen, rajoita laitteiden verkkoon jakaman tiedon määrää. Paras vaihtoehto on yksinkertaisesti kieltää kaikki tiedon jakaminen.

Internet of Things (IoT)

- **Harkitse laitteen vaihtamista**: Jos jossakin vaiheessa vaikuttaa siltä, että laitteessa on monia haavoittuvuuksia joita ei pysty paikkaamaan, tai saatavilla on uudempia laitteita joissa tietoturva on otettu huomioon paremmin, harkitse laitteiden vaihtamista.

Ei ole yhtä valmista muottia jokaiselle laitteelle, parasta on perehtyä jokaisen laitteen parhaisiin käytäntöihin tai dokumentaatioon liittyen kyseisen laitteen suojaamiseen. Valitettavasti suurin osa IoT-laitteista on kehitetty ilman tietoturvanäkökulmaa ja tämän vuoksi monet valmistajat eivät tarjoa mitään tietoa tietoturvaan liittyen. Kuitenkin kun tietoisuus asiasta kasvaa, toivomme että monet IoT-toimittajat rakentavat laitteisiin enemmän tietoturvaominaisuuksia ja lisäävät tietoa laitteiden suojaamisesta.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa http://www.securingthehuman.org.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava IT-johtaja. Kirill turvaa tällä hetkellä Elisa Appelsiinin liiketoimintaa vastaamalla niin yrityksen omasta kuin asiakkaiden tietoturvasta.

Lähteet

Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2015#april2015
Salasananhallintasovellukset:	https://securingthehuman.sans.org/ouch/2015#october2015
Uuden tablet-laitteesei suojaaminen:	https://securingthehuman.sans.org/ouch/2016#january2016
Kotiverkkosi suojaaminen:	https://securingthehuman.sans.org/ouch/2016#february2016

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy