Keskeiset tietoturvahuomiot kodin IoT-laitteissa

Ari Pönkkä / Voimaseniorit

10.02.2026

Johdanto

- Kodin perinteiset IT-laitteet, kuten tietokoneet ja älypuhelimet, ovat yleensä varsin hyvin suojattuja – niissä on palomuurit, virustorjunta ja säännölliset päivitykset. Mutta entä kodin IoT-laitteet?
- Kodin IoT-laitteet (esim. valvontakamerat, älytelkkarit, hälyttimet) voivat tehdä arjesta sujuvampaa, mutta ne tuovat myös uusia riskejä
- Älykkäät laitteet kotona – mutta kuinka estää niitä olemasta liian älykkäitä?
- Turvallinen älykoti: Pidä kotisi älykkäänä, hakkerit ulkona.
- Älykoti on fiksu vasta, kun se on turvallinen.

Kodin yleisimmät IoT-laiteet

🎧 **Viihde ja media**

- **Äly-TV:t** (Netflix/YouTube-sovelluksilla, usein mikrofoni ja kamera)
- **Älykaiuttimet** (Amazon Echo, Google Home, Apple HomePod)

🏠 **Kodinkoneet**

- **Älyjääkaapit** (näyttö, kamera sisällä, sovellusohjaus)
- **Älypesukoneet ja kuivausrummut** (sovellusohjattavia ohjelmia)
- **Robotti-imurit** (Roomba, Roborock, Dreame jne., usein kartoituksella ja etäkäytöllä)
- **Kahvikoneet ja muut pienkoneet** (verkkoon yhdistettäviä malleja alkaa tulla lisää)

Kodin yleisimmät IoT-laiteet

🔒 **Turvallisuus**

- **Valvontakamerat** (sisä- ja ulkokamerat, ovikellokamerat kuten Ring, Arlo)
- **Älylukot** (koodilla, sormenjäljellä tai sovelluksella avattavat)
- **Hälytysjärjestelmät** (liiketunnistimet, vuotovahdit, savuilmaisimet verkossa)

🌡️ **Kotiympäristö ja energia**

- **Älytermostaatit** (esim. Google Nest, Netatmo)
- **Älypistorasiat ja älyvalokatkaisijat**
- **Älyvalot ja -lamput** (Philips Hue, IKEA Trådfri, Xiaomi jne.)
- **Ilmanlaadun, kosteuden ja lämpötilan mittarit**

Kodin yleisimmät IoT-laiteet

🚙 Liikkuminen ja muut

- **Sähköautojen latauslaitteet** (usein app-ohjattavia ja verkossa)
- **Älykellot ja aktiivisuusrannekkeet** (vaikka ne onkin "puettavaa IoT:ta", moni laskee ne samaan kategoriaan kodin IoT:n kanssa, koska ne yhdistyvät muihin laitteisiin).
- **Kotona asumisen teknologiat ikäihmisille** (mm. Sote uudistuksen myötä tuleva etähoito kotihoidossa)

Keskeiset tietoturvahuomiot kodin IoT-laitteissa

- **Mahdolliset IOT-laitteiden riskit**
  - Tunkeutuminen verkkoon älylaitteen kautta
  - Tietojen vuotaminen pilvipalveluun
  - Haittaohjelmat tai salakuuntelu
  - Matkapuhelimien hakkerointi
  - Yhteys pankkitietoihin tai muihin laitteisiin
  - Poistettavien / palautettavien laitteiden sisältämä data

Keskeiset tietoturvahuomiot kodin IoT-laitteissa

- Päivitä laitteet säännöllisesti
  - Tarkista, että laite saa valmistajalta tietoturvapäivityksiä.
  - Asenna ohjelmistopäivitykset heti kun niitä on saatavilla.
- Vaihda oletussalasanat
  - Monet IoT-laitteet toimitetaan oletustunnuksilla, jotka ovat hyökkääjien tiedossa.
  - Käytä pitkiä, uniikkeja salasanoja. (Pari vinkkiä: Älä aina aloita isolla kirjaimella, älä laita erikoismerkkejä viimeiseksi)
- Lataa sovellukset vain virallisista kaupoista
  - Käytä App Storea tai Google Playta. Älä asenna tuntemattomista lähteistä.
- Poistettavat- / palautettavat laitteet
  - Palauta laite aina tehdasasetuksiin ennen palautusta (Saattaa sisältää luottokortti tietoja esim. Netflix)

Keskeiset tietoturvahuomiot kodin IoT-laitteissa

- Rajoita sovellusoikeuksia
  - Jos laite toimii mobiilisovelluksella, tarkista sen pyytämät oikeudet.
  - Äly-TV tai kaiutin ei tarvitse pääsyä kaikkeen puhelimesi sisältöön.
- Minimoi tarpeettomat laitteet
  - Jokainen uusi IoT-laite on uusi hyökkäyspinta.
  - Vältä "turhaa älykkyyttä" esim. jääkaapissa, jos et oikeasti tarvitse sitä.
- Käytä vahvaa Wi-Fi-salausta (WPA3 tai vähintään WPA2-AES)
  - Älä käytä avoimia tai vanhentuneita suojaustapoja (WEP, WPA-TKIP).
- Erota IoT-laitteet omalle verkolleen
  - Luo kotiverkkoon erillinen vierailija (guest)- tai IoT-verkko, jolloin esim. äly-TV ei pääse samoihin laitteisiin, joilla hoidat pankkiasioita.

IoT-laitteet omalle verkolle

- Miksi verkon erottaminen on tärkeää
  - Kuvitellaan, että joku murtautuisi sisään kodin Wi-Fi-verkkoon älypölynimurin kautta. Pääsisikö hän silloin myös käsiksi tietokoneeseen, jossa on pankkitunnukset? — Mahdollista, jos kaikki ovat samassa verkossa.
  - IoT-laitteet (älylamput, kaiuttimet, kamerat jne.) eivät ole yhtä turvallisia kuin tietokoneet.
  - Jos joku pääsee yhteen niistä käsiksi, hän ei pääse muihin laitteisiin, jos ne ovat eri verkossa.

IoT-laitteet omalle verkolle

🥉 Guest-verkko

Useimmissa operaattoreiden toimittamissa reitittimissä on:

- “**Vierailijaverkko**” tai “**Guest WiFi**”
- Sille oma nimi (SSID), esim. “Koti-Guest”
- Asetus: **Ei pääsyä pääverkkoon**

🥈 Eri verkko taajuuden mukaan

Useimmissa reitittimissä on erilliset verkot:

- 2.4 GHz (IoT-laitteille, koska monet käyttävät vain tätä)
- 5 GHz (tietokoneille ja puhelimille)

🥇 VLAN tai erillinen IoT-reititin

Teknologiaorientoituneille:

- Reitittimessä voi tehdä **virtuaalisia verkkoja (VLAN)** tai käyttää **erillistä reititintä IoT-laitteille**.

Keskeiset tietoturvahuomiot kodin IoT-laitteissa

- Sammuta tarpeettomat toiminnot
  - Poista käytöstä etäkäyttö, Bluetooth tai mikrofonit, mikäli niitä ei tarvita. (Esim. Valvontakameroissa voi mikrofonin käyttö olla tarpeellista)
- Suojaudu reitittimen asetuksilla
  - Varmista, että Wi-Fi-verkossa on vahva WPA3 (tai vähintään WPA2) -salaus.
  - Päivitä reitittimen ohjelmisto.
  - Älä jätä reititintä oletustunnuksille.
- Suosi tunnettuja brändejä
  - Suosi laitteita valmistajilta, jotka tarjoavat päivityksiä usean vuoden ajan.
  - Tuntemattomat merkit voivat jäädä ilman tietoturvapäivityksiä.

Keskeiset tietoturvahuomiot kodin IoT-laitteissa

- Kerätyn datan hallinta
  - Tutki, mitä tietoja laite kerää (esim. TV:n katseluhistoria, jääkaapin ostosdata).
  - Rajoita tietojen jakamista asetuksista, jos mahdollista.
- Käytön seuranta
  - Tarkkaile, jos laite toimii oudosti (lähettää paljon dataa, kuumenee, toimii hitaasti).
  - Tarvittaessa käynnistä uudelleen tai palautus tehdasasetuksiin.

Kyberturvallisuusasetus (Cyber Resilience Act)

- **Kyberturvallisuusasetus (Cyber Resilience Act)**, edellyttää, että IoT-laitteiden valmistajien on täytettävä tietyt kyberturvallisuusvaatimukset, kuten suojaus haavoittuvuuksilta, tietoturvapäivitykset ja tiedonhallintakäytännöt, ennen kuin he voivat myydä tuotteitaan EU:n markkinoilla. Asetus pyrkii parantamaan kuluttajien ja yritysten digitaalista turvallisuutta vähentämällä kyberuhkia ja lisäämällä luottamusta IoT-laitteisiin.
- Kyberturvallisuusasetus astui voimaan vuonna 2025 ja sen säännökset tulevat asteittain käyttöön seuraavien kahden vuoden aikana.

EU Datasäädös

- Datasäädöksen tarkoituksena on antaa käyttäjille – sekä kuluttajille että yrityksille – paremmat mahdollisuudet hallita verkkoon liitettyjen laitteidensa, kuten autojen, älytelevisioiden ja teollisuuskoneiden, tuottamaa dataa. Se luo perustan oikeudenmukaiselle, innovatiiviselle ja kilpailukykyiselle eurooppalaiselle datataloudelle
- Datasäädöksellä ei muuteta nykyisiä dataan pääsyä koskevia velvoitteita, mutta tulevan lainsäädännön olisi oltava sen periaatteiden mukaista.
- Astunut voimaan 11.01.2024
- Aletaan soveltaa 12.09.2025

Yhteenveto:

- Tärkeimmät kohdat ovat
  - Päivitykset
  - Vahvat salasanat
  - Verkon eriyttäminen
  - Turhien toimintojen poistaminen
  - Sovellukset vain virallisista kaupoista
  - Palauta laite aina tehdasasetuksiin ennen kierrätystä