

Netöryggisáskoranir hlutaneta og leiðir til úrbóta

Hlutanet

Hlutanet (Internet of Things, IoT) færir fólki mikla möguleika þegar kemur að snjallvæðingu. Hinn almenni notandi ætti að geta nýtt þessa möguleika á öruggan hátt og með vissu um að fullnægjandi öryggi og persónuverndarráðstafanir séu fyrir hendi til að verja notkun þeirra á hlutanetinu (snjalltæki á netinu). Það er oft því miður ekki alveg þannig.

Öryggisvandamál hlutaneta

Fjöldmörg dæmi hafa komið upp sem snúa að því hversu auðvelt var að brjótast inn í t.d. barnasnjallúr, öryggismyndavélar á heimilum og ýmsan nettengdan snjallbúnað á heimilum. Hlutanetsbúnaður hefur þá verið tekinn yfir, eigendum til armæðu og í sumum tilfellum til tjóns.

Öryggisleiðbeiningar varðandi hlutanet á neytendamarkaði

Staðlaráð Íslands hefur þegar gefið út leiðbeiningar til að taka á þessum vanda, sjá ÍST WA 302:2021. Þær byggja á ETSI stöðlum og breskum leiðbeiningum. Þrjár megin leiðbeiningarnar eru:

1. Engin sjálfgefin aðgangsorð

Öll lykilorð fyrir hlutanetstæki eiga að vera einkvæm og ekki endursetjanleg í sjálfgefið lykilorð frá framleiðenda.

2. Innleiðing á upplýsingaskyldu vegna öryggisveikleika

Öll fyrirtæki sem selja nettengd tæki og þjónustu verða að bjóða upp á almennan aðgang, þar sem hægt er að senda inn upplýsingar um veikleika, þetta er gert til þess að fyrirtæki sem rannsaka öryggisveilur og aðrir geti upplýst um öryggisvandamál.

3. Halda hugbúnaði uppfærðum

Hugbúnaðareiningar í nettengdum tækjum eiga að vera uppfærðar á öruggan hátt. Upplýsa þarf opinberlega um uppfærslur á líftíma tækis

Netöryggismál hlutaneta innleidd með lögum og með merkingu á búnaði

Reynslan af slíkum leiðbeiningum erlendis hefur ekki verið talin nægjanleg góð, enda er fyrirtækjum í sjálfsveld sett að fara eftir þeim. Því hafa nokkur lönd ákveðið að setja lög um öryggi hlutaneta og samhliða búa til merkingar á hlutanetsbúnað til að gefa til kynna hversu öruggur búnaðurinn er. Unnið er að þessu víða um heim og er t.d. ESB að vinna að löggjöf, „EU Cyber Resilience Act“, sem nær líka til tölvu- og farsímabúnaðar. Reiknað er með að sú löggjöf verði kláruð 2025.

Vinna er einnig hafin við alþjóðlegan staðal á vegum staðlastofnanna ISO/IEC. Staðallinn ISO/IEC 27404, „Universal Cybersecurity Labelling Framework (UCLF) for consumer IoT“, mun skilgreina alþjóðlegt merkingarkerfi fyrir öruggan hlutanetsbúnað á neytendamarkaði. Merkingarnar hafa fjögur öryggisstig, þar sem stig 4 er öruggast. Búnaðurinn verður þá merktur á áberandi hátt með viðkomandi öryggisstigi. Þannig veit neytandi að hverju hann gengur.

Stuðningur við netöryggisstefnu stjórnvalda

Kynning á leiðbeiningum, ásamt öryggismerkingum á búnað, styður mjög vel við markmið ríkistjórnarinnar í netöryggismálum, eins og þau voru kynnt 1. nóvember síðastliðin. Þar helst að nefna lið 1.3. „Traust netöryggismenning og -vitund“ og undirliðinn „Almenningur styrktur í öruggri notkun netsins og vitundarvakning um mögulegar hættur sem þar leynast“.

Apríl 2023 – Þór Jes Þórisson

Vefráðstefna um öryggismál hlutaneta á neytendamarkaði

Háskóla-, iðnaðar- og nýsköpunarráðuneytið, Fjarskiptastofa og Staðlaráð standa að norrænni ráðstefnu um netöryggismál hlutaneta á neytendamarkaði þann 3. maí kl. 8:45-10:15. Flutt verða erindi frá breskum og finnskum aðilum sem eru framarlega í að innleiða netöryggismál hlutaneta á neytendamarkaði. Einnig verða pallborðsumræður um stöðuna á Norðurlöndum. Vefráðstefnan er öllum opin. Hægt er að skrá sig hér.