Íslenskir staðlar

ÍST WA 302:2021

Gildistaka 07.06.2021

ICS: 35.240

Leiðbeiningar um öruggari notkun tækja á hlutanetinu (IoT)

Guidelines for cybersecurity of IoT on consumer market

Íslenskir staðlar

Staðfest af Staðlaráði Íslands

ÍST WA 302:2021

ÍST WA 302:2021

Formáli

Vinnustofa VS-2:2019 um IoT og öryggi var haldin af TN-IoT (tækninefnd FUT um hlutanet). Vinnustofan fól vinnuhóp að koma með drög að leiðbeiningum um öryggi IoT sem gefa átti út í vinnustofusamþykkt. TN-IoT skipaði vinnuhóp til að skrifa drög að leiðbeiningum sem yrði lokið við á nýrri vinnustofu. Vinnuhópinn skipuðu Þór Jes Þórisson (formaður), Valdimar Óskarsson, Sigurður Emil Pálsson og með þeim starfaði Guðmundur Valsson ritari FUT. Vinnustofan VS-2 hélt fund 26.5.2021 og þar voru leiðbeiningarnar yfirfarnar og samþykktar. Á vinnustofunni voru:

Nafn	**Aðili**
Guðmundur Valsson	Staðlaráð Íslands
Sigurður Emil Pálsson	Samgöngu- og sveitarstjórnarráðuneytið
Valdimar Óskarsson	Syndis
Þór Jes Þórisson	Fjarskiptaráðgjafi
Marcel Kyas	Háskólinn í Reykjavík

Leiðbeiningarnar í þessari vinnustofusamþykkt eru byggðar á skjölum sem yfirvöld í Bretlandi gáfu út í október 2018 vegna hlutanetsins (Internet of Things, IoT) til að auka öryggi IoT tækja á neytendamarkaði. (Code of Practice for consumer IoT security. Department for Digital, Culture, Media & Sport), vegna þess að verulegur hluti af tækjum á markaðinum í dag uppfyllir ekki lágmarks öryggiskröfur.

Bresk yfirvöld ákváðu í október 2020 að setja fyrstu þrjár reglurnar í lög, vegna þess að þó útbreiðsla leiðbeininganna hafi verið mikil, skorti enn nokkuð á að ástandið hefði lagast. Lagafrumvarpið er í samráðsferli, sem lýkur 6. september 2021.

Fjöldi alþjóðlegra stofnana og alþjóðlegra samstarfsverkefna eru að þróa öryggisráðleggingar og öryggisstaðla fyrir IoT. Þessar leiðbeiningar eru hannaðar til að vera viðbót og til stuðnings við alþjóðlegt samstarf og útgefna netöryggisstaðla.

Inngangur

Hlutanet (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 fullnægjandi öryggi og að persónuverndarráðstafanir séu fyrir hendi til að verja notkun þeirra á hlutanetinu (snjalltæki á Netinu). Því miður er það oft ekki raunin.

Fjölmörg dæmi hafa komið upp sem snéru að því hversu auðvelt var að brjótast inn í t.d. barnasnjallúr, öryggismyndavélar á heimilum og ýmsan nettengdan snjallbúnað á heimilum. Þrjár megin ástæður voru nefndar:

- Sjálfgefin notendanöfn og lykilorð, sem ekki er breytt þegar búnaðurinn er settur upp.
- Ekki hægt að tilkynna um veilur í öryggi og tryggja viðeigandi viðbrögð framleiðenda.
- Hugbúnaður í tækjum ekki uppfærður sjálfkrafa eða alls ekki uppfærður af framleiðenda.

Þessar leiðbeiningar eru hugsaðar fyrir framleiðendur búnaðar á IoT tækjum, þjónustuaðila á IoT þjónustu, framleiðendur á farsíma öppum sem styðja IoT tæki og seljendur á IoT búnaði.

Leiðbeiningarnar leggja fram hagnýt skref fyrir IoT framleiðendur og aðra hagsmunaðila í þessum geira til að bæta öryggi IoT tækja og tengda þjónustu sem ætluð eru neytendum. Innleiðing á þessum þrettán reglum mun bæta persónuvernd og öryggi neytenda, ásamt því að auðvelda þeim að nota tækin sín á öruggan hátt. Leiðbeiningarnar munu einnig draga úr hættunni á álagsárásum „Distributed Denial of Services (DDoS)“ sem geta átt sér upphaf í óöruggum IoT tækjum og þjónustu.

Reglurnar ná yfir það sem almennt eru taldar vera góðar venjur í IoT öryggi. Áherslan er á niðurstöðuna, frekar en ákveðna forskrift, það gefur fyrirtækjum sveigjanleika til nýsköpunar og innleiðingar á öryggislausnum sem eru viðeigandi fyrir þeirra vörur.

Þessar starfsreglur eru ekki einhlýt lausn til að leysa allar öryggisáskoranir. Aðeins með því að leggja áherslu á öryggishugsjón og öruggt vöruþróunarferli geta fyrirtæki skapað öruggt IoT umhverfi. Vörur og þjónusta ættu að vera hönnuð með öryggi í huga, frá vöruþróun til enda líftíma þeirra.

Leiðbeiningarnar eru samtals 13, fyrstu þrjár eru mikilvægastar vegna þess að til skemmri tíma munu þær auka öryggið mest. Þessar reglur eru í stuttu máli: Að nota ekki sjálfgefin leyniorð, að geta tilkynnt um öryggisveilur og fengið viðbrögð frá framleiðendum ásamt sjálfvirkum öryggisuppfærslum.

ÍST WA 302:2021

Leiðbeiningar um öruggari notkun tækja á hlutanetinu (IoT)

1. Engin sjálfgefin notendanöfn og lykilorð. Öll lykilorð fyrir IoT tæki eiga að vera einkvæm og ekki endursetjanleg í sjálfgefið lykilorð frá framleiðenda. Mörg IoT tæki eru seld með almennum sjálfgefnum notendanöfnum og lykilorðum (eins og „admin, admin “) sem neytandanum er ætlað að breyta eftir kaup. Þessa leið verður að hætta að nota. Brýnt er að koma í veg fyrir notkun sjálfgefinna aðgangsgilda, því öruggast er að notandinn tilgreini aðgangsgildin sjálfur. Aðstoða ber notanda til að finna bestu aðferðafræði við lykilorð og aðrar aðferðir við auðkenningu, sjá t.d. ráð á netoryggi.is.

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. Upplýsingum um veikleika á að bregðast við tímanlega.

3. Halda hugbúnaði uppfærðum. Hugbúnaðareiningar í Nettengdum tækjum eiga að vera uppfærðar á öruggan hátt. Uppfærslur eiga að vera tímanlegar og eiga ekki að hafa áhrif á virkni tækisins. Upplýsa þarf opinberlega um uppfærslur á líftíma tækis, sérstaklega þarf að taka fram lágmarkstíma sem viðkomandi tæki mun fá uppfærslur og ástæðu fyrir takmörkun á stuðningstíma tækisins. Þörfina fyrir hverri uppfærslu þarf að útskýra fyrir neytendanum og uppfærsluna á að vera auðvelt að framkvæma.

4. Örugg geymsla á skilríkjum og viðkvæmum gögnum. Öll skilríki eiga að vera geymd á öruggan hátt bæði í tækinu og viðeigandi þjónustu. Harðkóðuð skilríki í hugbúnaði tækis eru ekki ásættanleg, enda hægt að komast að slíkum skilríkjum á tiltölulega einfaldan hátt.

5. Öruggt fjarskiptasamband. Viðkæm öryggisgögn, þ.m.t. fjarstýring og fjarstjórnun, eiga að vera dulkóðuð eins og viðeigandi er m.v. möguleika tækninnar í hverju tæki og notkun tækisins.

6. Lágmarka árásarmöguleika. Öll tæki og öll þjónusta eiga aðeins að bjóða minnsta mögulega aðgang, þ.e. ónotuð port eiga að vera lokuð, vélbúnaður á ekki að hafa ónauðsynlega aðgangsmöguleika, þjónusta á ekki að vera aðgengileg ef hún er ekki í noktun og hugbúnaður á að vera afmarkaður við að veita aðeins þá þjónustu sem nauðsynleg er.

7. Tryggja heilleika hugbúnaðar. Hugbúnaður í IoT tækjum á að vera sannreyndur með því að nota örugga uppkeyrslu (e. secure boot) á tæki. Ef óleyfileg breyting finnst, þá á tækið að láta neytandann/kerfisstjórann vita og ekki tengja tækið við Netið, nema til að láta vita um mögulega öryggisveilu.

8. Tryggja að persónulegar upplýsingar séu varðar. Þar sem tækið eða þjónusta tengd tækinu vinnur með persónugreinanlega gögn, ber þeim að fara eftir persónuverndarlögum (sbr. GDPR). Framleiðendur og þjónustuveitendur á IoT þjónustunni eiga að upplýsa neytandann á skýran hátt um hvernig gögnin eru notuð, af hverjum og í hvaða tilgangi.

9. Kerfið hafi seiglu þegar útföll eru á netsambandi og rafmagni. IoT tæki eru sífellt að verða mikilvægari og því nauðsynlegt að þau virki áfram þótt netsamband rofni og að þau komi aftur upp í eðlilegu ástandi þegar netspenna kemur aftur inn eftir útfall.

10. Fylgjast með gögnum til og frá IoT tækinu. Ef gögnum er safnað frá tækinu og IoT þjónustunni, eins og notkunargögn og mæligögn, þá þarf að hafa eftirlit með sambandinu til að fylgjast með mögulegum öryggisógnum.

11. Auðvelda neytendum að eyða persónuupplýsingum. Tækin og þjónustan á að vera uppsett á þann hátt að auðvelt er að eyða persónulegum upplýsingum þegar neytandinn hættir að nota tækið og þjónustuna.

12. Uppsetning og viðhald á tækjum einfalt. Uppsetning og viðhald á IoT tækjum ætti að innfela eins fá skref og mögulegt er og fylgja bestu öryggisvenjum í notkun.

13. **Sannreyna innslegin gögn.** Innslátt á gögnum þarf að sannreyna þetta gildir um notendaskil, forritunarskil (API) og á milli hlutanetsþjónustu og hlutanetstækja.

Ritaskrá

[1] Code of Practice for consumer IoT security. Department for Digital, Culture, Media & Sport, October 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

Staðlaráð Íslands er vettvangur hagsmunaaðila til að vinna að stöðlun og notkun staðla á Íslandi. Ráðið starfar á grundvelli laga um stöðlun.

Staðlaráð stendur fyrir námskeiðum og veitir ráðgjöf, upplýsingar og þjónustu um hvaðeina er lýtur að stöðlum og stöðlun. Jafnframt sér Staðlaráð um sölu staðla frá fjölmörgum staðlastofnunum.

Staðlaráð er fulltrúi Íslands í alþjóðlegu staðlasamtökunum ISO og IEC og evrópsku staðlasamtökunum CEN og CENELEC og ETSI og þátttakandi í norrænu stöðlunarsamstarfi INSTA.

Helstu verkefni eru:

- Umsjón með staðlagerð á Íslandi.
- Að aðhæfa og staðfesta þá staðla sem skylt er vegna aðildar Staðlaráðs að erlendum staðlasamtökum.
- Að greiða fyrir því að íslenskum stöðlum verði beitt í opinberri stjórnsýslu og hjá einkaaðilum.
- Að starfrækja miðstöð stöðlunarstarfs á Íslandi sem þjónustar stofnanir, fyrirtæki, einstaklinga og samtök sem vilja nýta sér staðla.

Staðlaráð Íslands tekur ekki efnislega afstöðu til staðla og ákveður ekki hvað skuli staðlað. Ákvarðanir um það eru teknar af þeim sem eiga hagsmuna að gæta og þeir greiða fyrir verkefnin.

Á vegum Staðlaráðs starfa fjögur fagstaðlaráð:

Byggingarstaðlaráð (BSTR)
Fagstaðlaráð í fiskimálum (FIF)
Fagstaðlaráð í upplýsingatækni (FUT)
Rafstaðlaráð (RST)

Á vegum Staðlaráðs starfa einnig fagstjórnir í gæðamálum og í véltækni.

Það er einfalt og fyrirhafnarlítið að panta og finna staðla á netinu

www.stadlar.is

Íslenskir staðlar

Þórunnartúni 2 105 Reykjavík Sími: 520 7150 stadlar@stadlar.is www.stadlar.is