美國國家標準與技術研究院公布物聯網設備核心網路安全基礎指南草案

美國國家標準與技術研究院（National Institute of Standards and Technology, NIST）於2019年8月1 日公布「安全物聯網設備之核心網路安全特徵基準（Core Cybersecurity Feature Baseline for Securable IoT Devices）」指南草案，提出供製造商參考之物聯網設備網路安全基本要素，該指南草案中提出幾項重要核心要素如下：

1. 設備辨識：物聯網設備必須有可供辨識之相關途徑，例如產品序號或是當連接網路時有具獨特性之網路位址。
2. 設備配置：獲得授權之使用者應可改變設備的軟體以及韌體（firmware）之配置，例如許多物聯網設備具有可改變其功能或是管理安全特性之途徑。
3. 資料保護：物聯網設備如何保障其所儲存以及傳送之資料不被未經授權者使用，應清楚可被知悉，例如有些設備利用加密來隱蔽其儲存之資料。
4. 合理近用之介面：設備應限制近用途徑，例如物聯網設備以及其支持之軟體應蒐集並認證嘗試近用其設備的使用者資訊，例如透過使用者名稱與密碼等。
5. 軟體與韌體更新：設備之軟體應可透過安全且可被調整之機制進行更新，例如有些物聯網設備可自動的自其製造商取得更新資訊，並且幾乎不需要使用者特別之動作。
6. 網路安全事件紀錄：物聯網設備應可記錄網路安全事件並且應使這些紀錄讓所有人或製造商可取得，這些紀錄可幫助使用者與開發者辨識設備之弱點以近一步修復。

本文為「經濟部產業技術司科技專案成果」

相關連結

- Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers
- 美國參議院提出「2019年物聯網網路安全促進法」草案

你可能會想參加

柯亦儒
組長 編譯整理

上稿時間： 2019年09月

進階閱讀： 美國參議院提出「2019年物聯網網路安全促進法」草案https://stli.iii.org.tw/article-detail.aspx?tp=5&i=1&d=8234&no=57

文章標籤

推薦文章