智慧家庭裝置

智慧家庭裝置是什麼?

過去家中會使用到網路連線的裝置並不多,不外乎筆記型電腦、智慧型手機或是遊戲主機;然而,現在有許多裝置和網路連線,從家裡的燈泡、電視音響、門鎖,甚至是車子。在可預見的將來,家中的任何裝置都能透過網路聯結在一起。這些裝置通常稱為物聯網裝置或是智慧家庭裝置。雖然這些設備能使生活變得更加便利,卻可能潛藏不少的風險。

有什麼樣的問題?

家中可以連線到網路的設備越多就越有可能發生問題。駭客可以控制您的設備去攻擊其他人的設備、廠商能夠藉由物聯網設備收集大量資訊、或是裝置感染了惡意程而無法使用。由於大部份生產這些裝置的公司沒有網路安全的經驗,且認為增加網路安全相關功能會提高生產成本。因此,市面上販售的大部分產品只有設置少量或是根本沒有安全性功能。例如,部分裝置有預設的出廠密碼,但這組密碼可能早已眾所皆知,或是無法加以更改。

如何保護自己?

是否有自我保護的方法呢?我們衷心地希望大家使用物聯網裝置時,是安全無虞的。物聯網裝置提供絕佳的功能設計,讓我們的生活能夠更加便利。此外,隨著科技的演進,我們日後可能除了使用智慧型裝置外別無其他選擇。以下提供一些大家可以用來保護自己的有效方法。

僅將必要的裝置連上網路: 想要安全使用物聯網裝置最簡單的方式就是儘可能不要使用網路連線。如果設備根本沒有必要連線到網路,那麼請不要將它連線到您的Wi-Fi網路。試想一下,烤麵包機發出的通知訊息真的有必要寄送到您的手機嗎?

清查有哪些物聯網裝置: 您知道自己家中到底有哪些設備連上網路嗎?是否無法確定或是早已不記得了?那麼建議您可先關掉家裡的無線網路,看看有哪些裝置因此無法使用。也許無法找出所有裝置,但您會對有多少設備被遺忘感到驚訝。

保持軟體在最新狀態: 如同電腦或是行動裝置，請務必將家中物聯網設備的軟體維持在最新的狀態。如果您的裝置有自動更新功能，我們也建議將其啟用。

密碼: 請為家中裝置設定特殊、具有高強度且只有自己知道的密碼。您很可能僅需要輸入一次密碼。記不得多組密碼該怎麼辦？別擔心，一般人也記不住，此時可以考慮使用密碼管理器來安全地儲存這些密碼。

隱私權設定選項: 如果家中裝置能設定隱私權設定選項，請限制裝置收集或是分享的資訊。直接關閉資訊分享功能也是選項之一。

廠商: 建議跟熟悉或信任的廠商購買裝置。選擇支援安全性設定的產品，像是允許您啟用自動更新、修改預設密碼及設定隱私權設定選項的裝置。

保持監聽: 如果裝置可以接受您的語音指令，那它將持續聆聽您的聲音。例如，您的Alexa和Google Home裝置可以記錄私密的對話。請仔細考慮您放置裝置的位置並確認隱私權設定選項。

訪客網路: 考慮將您的智慧家庭裝置連線到獨立的「訪客Wi-Fi」網路上，而不是您的電腦和行動裝置所使用的主要Wi-Fi網路。這樣一來，就算任何智慧家庭裝置遭到感染，主網路上的電腦和行動裝置仍然可以保持安全。

不需要害怕新的科技，但是要了解他們可能帶來的風險。透過以上這些簡單的方式，您能夠建立一個更安全的智慧家庭環境。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站http://www.tsc-tech.com/或臉書@tsctech了解更多訊息。

客座編輯

Robert M. Lee (@RobertMLee) 是SANS認證講師，以及FOR578－網路威脅情報、ICS515－ICS主動防禦和資安事件應變的作者。Robert同時也是工業網路安全公司Dragos的執行長和創辦人。

資源

密碼短語: https://www.sans.org/u/GEB
密碼管理器: https://www.sans.org/u/GEG
保護您的家庭網路: https://www.sans.org/u/GEL