機關安全維護宣導-誰在看著你家客廳？

「物聯網」簡單來說，就是將日常生活物品嵌入感應器及晶片，使該等物品能透過網路被遠端操作或自行感知主動運作，以提供人類生活更多的便利性。

近年各類家電及交通工具等日常生活用品，總是愛冠個「智慧型」或「雲端化」，讓愛潮流的人們趨之若鶩。這些「智慧型」東西好不好用是一回事，然已讓以往只在個人電腦上才會發生的中毒、受駭事件，蔓延至各種家庭用品中。

「物聯網」有數不清的好處，但也潛在更大的負面風險，原因就是「物聯網」設備的「數量」及「種類」過多，這也是「物聯網」時代的資安問題遠大於 PC 時代的主因。

現將「物聯網」的資安問題分析如下：

一、資安攻防有個術語叫攻擊面，攻擊面越小的系統，其安全性越高；而「物聯網」的特色就是設備又多又雜，讓攻擊者在攻擊「物聯網」相關系統時擁有極大優勢，造成「物聯網」之資安風險難以克服。

二、資安領域有個「水桶理論」，即整個系統的安全性取決於最低安全程度的設備。「物聯網」的應用常常需結合數種設備：如手機遠端居家監控應用，需要結合監視器、監視設備主機、路由器、手機等等不同設備，任一環節有資安問題發生，就會導致整個監控系統曝露於風險之中。

三、「科技始終來自於人性」，Nokia 的一句帶著人文味道的廣告詞，同樣也適用於駭客犯罪，因為「漏洞始終來自於人性」，「物聯網」設備結合數種裝置，只要有任一裝置的使用者輕忽裝置安全措施的設定，就會讓駭客有機可乘。

這是個群眾極易被科技推動的時代，我們無法抗拒這波「物聯網」潮流的到來，只能去適應並找出生存法則與之共存。馬克．古德曼所著的「未來的犯罪」一書中即探討「物聯網」所帶來的各種未來犯罪型態。

以下引述該書所提供之口訣：「UPDATE」予進入「物聯網」時代的人們，明瞭如何簡單保護自己的方式。期盼各位在盡享「物聯網」時代便捷的同時，亦能充分保有自己的隱私及資料安全。

U：Update Frequently（經常更新），用來防止駭客用已知設備漏洞入侵。

P：Password（密碼），使用不易破解的密碼或二階段的保護措施。

D：Download（下載），只選擇官方下載站，避開盜版硬體或軟體。

A：Administrator（管理者權限），平時不使用管理者帳戶。

T：Turn Off（關機），不用時就關機。

E：Encrypt（加密），資料或裝置都要加密保護。

~~節錄自清流雙月刊~~

~~~政風室 關心您
~~~