機關安全維護宣導-無煙硝的 5G 戰爭

美、澳、歐洲已有不少電信業者搶先推出 5G 服務，其餘各國將相繼在 2020 年走入 5G 時代。國際行動通訊組織定義出 5G 三大具體目標：一、增強型行動寬頻通訊--5G 技術進一步提升傳輸速率達到 10Gbps，有了高傳輸速率的 5G 便可以提供更多樣的行動應用。二、超可靠度和低延遲通訊--物聯網的情境下，智慧城市的交通控制樞紐、無人車駕駛以及遠端醫療等都不再是不可能。然而這類型的應用對於通訊的可靠度以及通訊間的回應時間都有高度且嚴格的需求，延遲時間依照標準需低於 1 毫秒。三、大規模機器型通訊--所想像到的物品都可連上網路，彼此之間傳遞訊息，新的 5G 規格必須能夠支援上述場景。平均而言，可能在每平方公里內將會有上百萬的裝置同時發送資料。

承襲前幾代的行動網路發展而來，5G 可能的資安威脅也繼承了原有架構可能遇到的資安問題。

一、行動雲端計算

5G 架構下的雲端計算可以分成用戶端及伺服器，用戶端最常遇到的資安風險就是潛藏手機中的惡意程式或間諜程式，透過使用者不經意的下載，植入到用戶端的裝置中，潛伏蒐集個人敏感資料或是破壞整體系統效能。另外由於網路傳輸的特性，使得 Wi-Fi 偵測、IP 位址欺騙及會話劫持（sessionhijacking）等仍是潛在的資安威脅。

二、軟體定義網路與網路功能虛擬化

軟體定義網路將原本部分屬於網路硬體的功能抽離出來，改由程式來控制，方便了網路管理者，同時也增加駭客攻擊的機會。由於軟體定義網路的控制器修改了原本資料傳輸的規則，因此屬於該

控制器發送出來的封包在網路中很容易被辨識出來，這也增加了該控制器被鎖定使用 DoS（Denial of Service）攻擊的可能性。網路功能虛擬化將分散的硬體裝置，以軟體的方式集中至一臺通用規格的硬體中，所以該臺通用規格硬體的使用者權限管理將成為最重要的議題，必須要嚴格地將所有使用者區分為一般使用者及系統管理者，兩者之間在伺服器中所能執行的功能及角色完全不同，系統管理者可以進行系統層面的參數修改，而一般使用者僅能使用系統管理者授權的權限進行操作。**在通用規格硬體中的帳號稽核若是沒有落實，不該擁有管理權限的使用者有可能惡意或不經意地調整了網路底層應有的行為，進而導致系統崩壞。**

最後，這兩者都大量仰賴軟體，然而如此龐雜的軟體工程，沒有人能完全保證軟體系統沒有任何錯誤（bug），一旦有了軟體錯誤，便為駭客提供了一扇入侵的門。細究上述所列舉的 5G 安全議題，其根本原因是無線通訊架構的先天性所造成。此外，亦有人為刻意附加惡意程式之風險，則基地臺可利用後門程式，監聽或轉送所有經過該基地臺的封包。在關注 5G 所帶來的便利性的同時，亦須重視資訊安全的面向，以免得了便利卻失了隱私。

~~節錄自清流雙月刊~~

~~~政風室 關心您
~~~