資訊擁有者、使用者與雲端平臺管理員都應了解網路攻擊的趨勢，只有掌握最新的雲端威脅，才能確保資訊服務的安全。

認識雲端服務與安全

◎李柏毅

雲端服務是一個大家目前耳熟能詳的網路名詞。這一朵原本只存在網路拓樸圖上的雲，隨著資訊科技的不斷進步與革新，已經慢慢地擴大到我們每一個人的日常生活中了。

雲端服務（Cloud Service）是一項結合雲端運算（Cloud Computing）、雲端儲存（Cloud Storage）、網路連線與管理的新時代網際網路服務。國際研究暨顧問機構 Gartner 對雲端服務的註解為：雲端服務是大量且具有可擴充性的資訊資源，透過網路以服務的方式提供給使用者存取。舉凡影音娛樂、文書處理、收發電子郵件、訊息交換、瀏覽網頁等日常的網路行為，以至於醫療機構為居家照護患者所提供的遠端醫療服務、教育機構的遠距教學平臺等公共服務，都在雲端服務的範疇之中。

美國國家技術標準局提出雲端服務應具備的五種性質：

一、隨需自助服務：在使用者需要雲端服務時，可在不透過其他系統維運人員的協助之下，於任何時候自行存取所需要的服務內容。如此一來，雲端服務就能協助企業或組織提升服務效率，增加使用者的滿意度，同時也可以降低互動時間以及服務成本。

二、網路服務連線：由於網際網路技術的進步和無線網路建設的普及，雲端服務已能讓使用者在地球上任何一個角落，透過網路通訊標準進行服務存取。

三、資源共享：透過虛擬化及其他綠能科技的協助，雲端服務可同時將運算和儲存資源分享給許多使用者，如此一來，即可大量減少硬體閒置資源的浪費，也可透過專業化的集中管理，降低服務成本。

四、彈性部署：可彈性化部署的伺服器群以及網路儲存設備提供了雲端服務高度的服務彈性化，使用者可以依據自己的需求，進行服務的增加、刪除。

五、量化服務：雲端服務可以根據資源的使用，進行量化指標的監控，包含 CPU 數目、記憶體使用量、儲存空間的使用量、網路頻寬的使用量等；這樣的特色有助於幫助管理員監控服務的即時狀態，也能針對各種服務的使用狀況進行資源最佳化的分配。

當雲端服務越來越普及時，其所衍生的資安問題將會是下一波被大家重視的課題。謹就雲端安全聯盟（Cloud Security Alliance）提出的七大雲端威脅分述如下：

一、雲端運算的濫用：資訊的進步除了提供使用者更便利的生活，同時也會造成新的資安問題。近年來越來越多的網路犯罪者已開始透過雲端服務來進行不法行為。例如利用殭屍網路（Botnet）作為訊息交換的中繼站，建構在雲端服務商所提供的系統平臺上，藉由正常雲端服務的網路流量，隱藏殭屍電腦的通訊行為，並躲過偵查。此外，雲端運算也已被利用來提供密碼破解的服務，只要有心人士取得系統的帳號密碼資料檔案，並將其中的 MD5 雜湊值（Hash value）取出，透過現成的雲端服務，即可分析出該雜湊值所代表的可能密碼組合，進而取得系統內部的任何帳號密碼。

二、不安全的通訊介面或是應用程式：使用者使用特定的通訊介面與應用程式存取雲端服務，因此，當通訊介面或是應用程式發生安全漏洞時，都會影響服務存取的安全，造成資料在未經授權的狀況下，遭到第三人存取或是修改。

三、內鬼難防：當所有的資訊服務都移轉到雲端空間時，管理的責任同時也部分移轉到雲端服務供應商身上。因此，若雲端服務供應商內部存有居心不良的使用者，便可能對存放在雲端服務平臺的資訊造成危害。這方面的風險，是使用者無法預測與轉嫁的。

四、資源共享造成的潛在問題：資源共享雖可節省閒置資源的浪費，達到節能省碳的目的，但同時也衍生資料保密的問題。雲端服務使用虛擬化的技術，將實體的資訊資源同時分配給多位使用者存取，雖然每一位使用者都是使用獨立的運算空間，但若其實體隔離機制出現漏洞，有心人士確實可以藉此影響其他雲端服務，甚至讀取其記憶體或是儲存空間的資料。

五、檔案遺失或資料外洩：雲端服務供應商在資料保全上所提供的安全防護機制，也必須要能確保使用者的資料不會受到未經授權的存取；若發生資料毀損的狀況時，雲端服務供應商也必須要有完善的資料備援機制，才能降低資料遺失的風險。

六、帳號或服務挾持：雲端服務的認證機制主要係透過網際網路的方式，藉由輸入帳號密碼來進行身分確認。一旦使用者帳號遭到竊取或是資訊傳輸的過程，連線遭到中間人攻擊重設，都會導致第三者取代原使用者而取得該系統的完整控制權。由於使用者無法透過重設實體系統（本機終端機登入或是切斷網路連線）來進行緊急應變，所以一旦帳號密碼外洩或是服務被挾持了，其損害程度及影響範圍可說是無法評估。

七、未知風險：雲端服務隨著資訊科技的進步，也在不斷地改變其服務型態，所以未知的困難以及可預見的資安問題將會越來越多。

雲端服務改變了以往資訊服務的面貌。透過網路，使用者可以隨心所欲地使用雲端資源，組織單位也可以透過雲端服務，降低服務建置與管理成本。但隨著服務型態改變所衍生的資安問題，並不會同時全部移轉到雲端服務提供者身上，凡是資訊擁有者、使用者與雲端平臺管理員都必須了解網路攻擊的趨勢，掌握最新的雲端威脅，才能確保資訊服務的安全。