資訊系統外包的安全管理

◎魯明德

在新的全國戶政系統上線後,由於系統測試不完全而影響作業的速度，造成媒體與民眾一片撻伐;旋即又有議員爆料,該系統得標商為節省人力，將部分系統包給大陸的軟體公司撰寫程式，因而產生水土不服，且易形成資訊安全的漏洞。

科技新貴小潘在看到這則報導後，想起公司很多系統的開發，也都是委外作業，會不會因而造成資安問題？如果為了安全的考量，全部收回自行開發，人力又無法負荷，有沒有辦法兩全其美呢？一連串的問題，小潘在這個月的師生下午茶約會中，提出跟司馬特老師討論。

司馬特老師喝口咖啡緩緩道來。專業分工是產業發展的趨勢，軟體的委外開發，其實也是代工的一環，像微軟的作業系統開發，也是外包給印度的公司撰寫程式，難道使用者會擔心 windows 拿到臺灣會水土不服嗎？會讓公司洩密嗎？資訊系統的安全應該在一開始規劃時，就要從軟體開發及基礎建設上加以考慮。首先要考慮的是整個系統要委外開發，還是只有程式撰寫的部分要委外，這二者的資安風險並不相同。如果要把整個系統委外開發，公司就是系統的使用者，他要提出系統的需求，讓資訊廠商依需求去開發系統。如果只是把程式撰寫的部分委外，公司就要自行做好需求調查、系統分析與設計、測試驗收計畫等，委外的廠商只負責依規格寫程式，不用管系統規劃是否正確。

小潘聽到這裡豁然開朗，企業的資訊系統開發，如果採取整個系統委外的策略，就要在系統的需求規格中，完整要求各項資訊安全作為。如果只把程式的部分委外，因為廠商不清楚撰寫的程式在系統中的位置，而且未來還要跟其他程式整合測試，洩密的機率相對較低。

司馬特老師又丟出另一個問題：資料庫的資料安全要如何確保呢？小潘受到老師的鼓勵,接著回答:資料庫的資料安全可以分為二個階段考慮，在系統開發初期及單元測試階段，可以用虛擬資料做測試，因為資料非真實資料，因此沒有資料安全的問題。在系統整合測試階段，因為使用實際資料上線測試時，應該有嚴格的資訊安全規範，而且業主要有承辦人員在場參與測試,一方面查看系統符不符合規範,另一方面做資訊安全的監控。凡是涉及資料庫的資料，委外廠商都只能在指定的場所存取不能帶走，並做人員隨身物品的管制，以免資料外洩。

小潘又想到另一個問題：一套系統這麼龐大，開發的程式又這麼多，怎麼知道有沒有被人寫入後門程式？系統在測試時都沒有問題，如果在執

行期間發生問題怎麼辦？司馬特老師答道：前面所談的都是在系統開發階段要如何防止資料洩漏，當然我們沒有辦法用逐行檢視程式的方式，來確保系統中有無後門程式，所以另一個防止洩密的方法，就是從基礎建設上著手。稍具規模的企業，工廠、辦公室可能都不會集中在一處，所以資訊系統建置後，勢必要靠網路連結，面臨的挑戰並非只有軟體開發，硬體的規劃與建置，也是影響系統良窳的重要因素。

如果系統間的連結是透過網際網路，被入侵或者後門程式洩密的風險自然很高，這種設計應盡量避免。企業如果有足夠的資源，最安全的方式是跟電信業者租用專線，做為資料傳輸的管道，因為只有一家公司在使用，沒有對外的連結點，即使系統被植入後門程式，也沒有出口可以把資料送出，像全國戶政這麼重要的系統，就可以採用這種方式。

由於大部分的公司沒有足夠的資源可以拉專線，也有很多公司的據點遍布全世界各地，無法逐一拉專線，為確保資料的安全，可以把重要的資料集中管理，做好系統的存取管理，防止資料不正常存取，並要求使用者透過虛擬私有網路（VPN）登入，以確保資料的安全。

這次的師生下午茶約會已進入尾聲。小潘心想：原來資訊系統的安全，應該是「軟硬兼施」才對，不能只考慮軟體而已，硬體的防護也是很重要的一環；在軟體的委外開發上，不同的委外策略應有不同的安全議題。以後面臨這些問題時，更應面面俱到，才能確保系統的安全。

（文摘自法務部調查局清流月刊 103 年 4 月號）

嘉義區監理所 關心您