資料庫的資訊安全維護

※本文摘錄自法務部調查局清流雙月刊 105 年 3 月號

◎魯明德(科技大學講師)

不管是政府機關的機密文件或商業機密資料，都像我們家中的貴重物品一樣，需要特別的保護，養成好的習慣及安全防護的基本概念，就能有效遏止有心人士的不良企圖。

VTech 在 2015 年 11 月發現駭客入侵了該站的資料庫，造成 485 萬名家長帳號及 636 萬兒童檔案受到影響，受影響的層面包括了美國、法國及英國等多個市場的 VTech 用戶。

無獨有偶的，Hello Kitty 的 Sanrio 公司的資料庫，在 2015 年 12 月也傳出遭到駭客入侵，報載有 330 萬用戶資料可能因此外洩，外洩的資料包括用戶的名稱、性別、國籍、電郵地址和加密的密碼。

科技新貴小潘看到這些報導，想到公司近年轉型進入電子商務的領域，這些年下來，公司的資料庫中也有不少的客戶資料，萬一也被入侵、被盜取，豈不就麻煩了！

於是，小潘趁著過年期間的聚會，趕快跟司馬特老師提起他擔心的這些問題，司馬特老師喝了口咖啡後，先問了小潘一個問題：「平時你們公司有沒有對網路採取什麼防護措施？」小潘就把公司現行的網路防護措施，簡單地對司馬特老師說了一下。

司馬特老師聽完小潘的敘述後指出，一般人在網路的基礎建設上，都會把資訊安全防護措施規劃進去，但是，這樣做只能治標不能治本，因為網路攻防是沒有終止的，這是一個矛與盾的戰爭，當使用者有了好的防護後，攻擊者不久就會有新的攻擊策略出來。在這個永無止境的戰爭中，要勝出

就不能只被動的防禦，應該要有更主動的作為。

小潘聽到這裏開始迷糊了，心想，老師的意思難道是要我們主動出擊嗎？那是要我們去當駭客嗎？司馬特顯然看穿了小潘的心思，喝了口咖啡後，笑著繼續說下去。

主動的作為並不是要我們去當駭客，駭客就像小草一樣，野火燒不盡、春風吹又生，是攻擊不完的。我們應該要做的是在系統建置之前，就先規劃好安全措施，除了包括前面所說的網路基礎建設的防護，還要從系統面去思考，該怎麼設計才不會讓駭客，一進到系統就如入無人之境。

就像我們家裏，為了不讓小偷進來，會裝鐵門、鐵窗一樣，但是，裝了鐵門、鐵窗以後，就保證不會有小偷進來嗎？也不盡然，所以，我們還會把家裏的貴重物品再收藏在隱密的地方，目的就是要讓小偷即使進來，也不會這麼快就找到了貴重物品。

我們的資源有限，在規劃系統資訊安全時，不能期望做到滴水不漏，但是，至少要做到駭客進來後，不是那麼容易就得手。也就是說，在資訊安全上，我們雖然做不到絕對安全，也要能做到相對安全。

小潘聽到這裏又迷糊了，什麼叫做絕對安全？什麼又是相對安全？司馬特老師再喝口咖啡後，順著剛剛的例子繼續說下去，絕對安全就是百分之百不會被入侵的防護作為，以家裏的保全來說，裝了鐵門、鐵窗後，如果小偷就進不來，那就是絕對的安全，但是，真的會有這樣的結果嗎？

我們裝的鐵窗可能被小偷剪斷、鐵門也可能被破壞，而遭到入侵，所以，我們除了第一線鐵門、鐵窗的防護之外，還要把貴重的財物收藏好，不能放在明顯的地方，讓小偷即

使突破第一道防線，也不能很快的得逞，如果花很多時間還找不到，為了自身的安全，他可能就會選擇撤退。

資訊安全的防護也是，既然不能百分之百的防止駭客入侵到我們的系統，就要想辦法築起第二道防線，不讓它一下就達到目的，資訊系統的第一道防線就是架在基礎建設上的防火牆、防毒軟體…等，這些設施就像我們家裏裝的鐵門、鐵窗一樣。

第二道防線就像我們要把家裏的貴重物品收藏好一樣，從系統面來看，我們在意的貴重物品就是資料庫內的資料，所以，我們在系統的設計階段，就要設法不要讓它曝露在外，設計思維就是不要讓駭客入侵後很快就拿到。

在系統設計時，可以採取 3-Tier 的設計，不要讓使用者一進入系統就有機會接觸到資料庫，把資料庫放到後方，透過 2 層的伺服器才能存取到，這樣的設計，讓駭客即使入侵到我們的系統，還不致於讓系統馬上受到損害。

當然，前提是資訊系統在基礎建設上，還是要有適當的防護作為，二者要一起作用，才能有效果，否則，就像把貴重物品放在客廳一樣，一旦鐵窗被剪斷，小偷一進來就可輕易拿走。

小潘聽到這裏，心中也開始盤算，上班之後應該要對公司的資訊系統做一個健康檢查，除了原有的防火牆之外，也要仔細的檢查一下系統架構，把有可能的漏洞趕快補強。

新春的第一次師生下午茶約會，就在濃郁的焦糖瑪琪朵香味中進入尾聲，小潘想到畢業 5 年，還能每個月跟老師一起討論問題、自我成長，感到很幸福，滿載收穫跟老師互道再見，明天又是充滿工作活力的一天。