◎資訊安全維護宣導

企業資訊系統分為系統與資料庫，設計時要把系統與資料庫分開，
以防駭客入侵系統後，資料庫內容也立刻被竊取。

－如何防止企業資料庫被駭－

報載某知名咖啡連鎖店的網站在今（2015）年５月 10 日遭到駭客攻擊，五千筆包含帳號、姓名、聯絡電話、生日、行動電話、行業、住址等會員資料，被公開在俄羅斯網路論壇。該公司也坦承被駭，但強調主要被駭的是電子報會員資料庫，曝光的個資不包含金融資料或身分證字號等較高機密性的訊息，消費者不必擔憂信用卡被盜刷。

從事網路工作的小潘看到這則新聞，想到網路安全對企業來說，會是未來一個很大的挑戰，而資訊安全又是一個矛與盾的戰爭，該如何做才能確保公司資料庫的安全呢？在這個月的師生下午茶約會中，小潘決定把這個問題弄清楚。

聽完小潘的問題，司馬特老師喝口咖啡後娓娓道來，根據趨勢科技所公布的 2015 年第一季資安報告顯示：臺灣名列最常遭受 PoS 系統（Point of Sales，銷售點系統）攻擊的第三名。而 2015 年駭客鎖定 PoS 系統取得信用卡資料的事件越來越多，在美國第一季就發生近一億筆醫療個資被駭客所竊。

現在行動商務蔚為風潮，每個行動裝置上都有數十個 APP，而駭客也把入侵管道放在 APP 上。目前已經有很多 App 只要靠近你的錢包，就能取得你的信用卡卡號。美國已下令在 2015 年 10 月前，磁條信用卡將全面轉換成晶片密碼信用卡，而歐洲也大多採用晶片密碼信用卡，再加上 PIN 碼的雙重認證，安全性就更高了。

在人手一機的時代中，行動裝置成了駭客的新目標，最常見的手法是，讓使用者看免費的影片或下載假的軟體，駭客在你未察覺的情況下取得你的電話簿及 E-mail 等。而且行動惡意威脅 App 數量急速竄升，在 2015 年第一季已正式突破 500 萬，而惡意廣告是行動裝置排名資安威脅的第一名。

根據趨勢科技的統計，截至今（2015）年３月份，Google Play 曾有超過二千個 App 可能含有惡意廣告程式，2015 年第一季全球總計有 800 萬用戶曾造訪惡意網站，臺灣是最常造訪惡意網站的第四名。

網路攻擊與防禦就像一場矛與盾的戰爭，攻防雙方不斷競逐，當防禦方的資安從業人員摸清楚持續的威脅與攻擊，掌握威脅殺傷鏈各個階段攻擊特徵之後，攻擊方又隨之展開新的變化以躲避偵查。

Websense 安全實驗室在 2015 的威脅報告中指出，從 2014 年到 2015 年的攻擊事件中，網路攻擊變得更有效率，使用既有的攻擊架構並置換攻擊工具包的惡意程式，就能發動新的攻擊，攻守雙方不斷在惡意程式的偵測與繞過技術中互有領先。

2015 年已是攻擊即服務的年代（Malware as a Service, MaaS），由於網路世界裡很容易找到可租或買的攻擊包，加上可以將一連串攻擊階段中的某些複雜部分轉包給高手，現在即使是入門的菜鳥攻擊者都可成功發動資料竊取攻擊。網路犯罪的技術門檻大幅下降，人人都可以是駭客。惡意程式作者只要在既有的攻擊手法中融入新的技術，便能成功繞過企業偵測，這讓攻擊者在發送惡意的電子郵件時，開始將舊手法融入新的繞過技術中。舊的攻擊手法又被重新使用在新的攻擊中，並透過電子郵件或網頁形式傳送，讓人防不勝防；Websense 偵測到的惡意郵件中，就有 28%是當下防毒軟體的特徵碼都無法辨識的。

小潘聽到這些駭人的數據後，開始擔心公司的資料庫安全問題。司馬特老師喝口咖啡繼續說，由於駭客的入侵技術日新月異、防不勝防，因此我們除了靠防火牆、防毒軟體做第一線的守護神外，也要在基礎建設上做防範。

資訊系統可分為系統與資料庫兩大部分，駭客癱瘓系統的目的是讓被駭的系統不能正常運作，影響使用人的操作，對企業造成的危害只在停止運作，還不會對資料造成大傷害；但若駭客入侵資料庫，對企業所造成的傷害就很大了，尤其是 B2C（Business to Consumer，企業對消費者經營模式）的業者，資料庫中存放的都是客戶的個人資料，一旦被入侵，甚至被非法竊取，造成的傷害就可能無可挽回。所以設計系統時，在基礎建設的規劃，就要把系統的程式跟資料庫分開，建構一個 2-tier（階層）甚至是 3-tier 架構，資料庫放在後層，不讓外部使用者透過瀏覽器就可以直接接觸，這樣做雖然尚不能?防止駭客的入侵，但至少可的提高資料庫的防護安全度。同時，在資料庫設計時，也可透過資料庫正規化，把資料庫切割，將客戶的資料放在不同的資料庫中，藉由關聯去連結，也可以防止駭客入侵後，馬上竊取所有資料。

聽完司馬特老師的詳細說明，小潘深深感受到資訊安全沒有百分之百的安全，道高一尺魔高一丈，安全絕不能輕忽，唯有不斷注意各種小細節，才能防止洩密事件發生。本月的師生下午茶就在細雨中進入尾聲。

（作者魯明德為科技大學資訊管理系講師）

台中榮民總醫院提醒您也關心您！