微型企業的資安策略

科技大學教師　魯明德

資通訊技術的快速發達，為企業經營帶來了前所未見的便利，相對的，也帶來了資訊安全上額外的風險，近期加密勒索軟體橫行、身分剽竊、資安攻擊組織化等趨勢，大至政府機關小至個人無一能倖免於難，加上行動裝置普及的推波助瀾，讓企業的資訊安全更形艱鉅。

由於資通訊載具的普及，使用者的年齡有普遍下滑的趨勢，企業所面對的駭客危機不再是成年人所為，報載 1 名 10 歲的芬蘭駭客，成功找到臉書(Facebook)的資訊安全漏洞，幸好他只是做善意提醒，沒有從事什麼進一步的行為，否則恐怕上億使用者都可能遭到損害。

科技新貴小潘看到這則新聞，思索著如果像臉書這麼有頭有臉的大公司，都會面臨到駭客的攻擊，那麼全台灣超過 250 萬家的微型企業，他們的資源如此不足，面臨到駭客攻擊，豈不是更加危險？

在端午節的師生下午茶約會中，小潘就提出了這個問題，司馬特老師邊喝著咖啡邊說，微軟在 2015 曾經針對旗

下 5 萬名國內客戶做測試，樣本含蓋了銀行、保險、運輸、傳產 、高科技、製造業和公部門等，進行近 18 萬次的測試，彙整不同測試結果並交叉分析後發現：有高潛在風險、易遭鎖定攻擊之帳號佔 47%、使用者行為具高風險者佔 38%、違反郵件安全規範而導致系統遭感染佔 32%、密碼帳號權限遭破解並盜用佔 29%、設備遭植入殭屍網路佔 9%。

小潘在聽完司馬特老師的說明後，更加深了他原來的擔憂，如果連這麼大的公司，都無法阻擋駭客的攻擊，那些小公司豈不更是要自求多福了？司馬特老師喝口咖啡繼續說，資訊安全的問題，應該在於人及管理上，如果大家都不在意、沒有警覺性，管理上也沒有作為，那麼，很快就會淪陷。

駭客攻擊手法今昔

隨著時代的改變，駭客的行為模式也在改變中，以前常見的駭客攻擊手法是，入侵電腦、竊取重要資料後，便發出勒索信要求支付贖金，否則便公開資料或是威脅要把資料提供給競爭對手，這時候，企業雖然要持續與駭客周旋，但仍能維持正常運作。

但是，現在的狀況不一樣了，駭客攻擊的手法逐漸演變成以勒索軟體為主，利用客製化手法設計惡意電子郵件，當使用者打開了郵件中的惡意連結或執行附加檔案，就會自動下載勒索軟體至電腦中，這個勒索軟體不僅會把電腦中的重要文件加密，還有可能切斷鍵盤、滑鼠與電腦間的連結，導致企業日常工作無法維持正常運作，直到交付贖金為止，甚至於交了贖金也可能無法恢復原狀。

微型企業因為資源有限，資訊系統規模小，不容易花大錢建立防護系統，可以思考的方向有二，如果是以電子商務為主的企業，除非本身就對資訊安全很熟悉，可以駕輕就熟的處理任何事件，否則可以把網站委由專業的業者負責，架設在安全性高的 ISP 提供的空間中，減少自己處理不熟悉問題的風險。

其次，如果企業的資訊系統只是做內部管理之用，初期在自己無法當控全局的情況下，可以把電腦與外部網路做實體隔離，這雖然是最笨的方法，但卻也是在沒有辦法下的好辦法，存放重要資料的電腦，不僅要定期做備份，還要跟外部網路徹底隔離，讓駭客無法入侵，以減少被攻擊的風險。

強化資安管理作為

當然，在管理上是不可或缺的，企業的資訊安全考慮的構面不外乎是：人員、環境、設備及資料，在人員安全上，要防止人為的疏忽、濫用或誤用資訊及設備，在環境安全上，要做到防止環境的問題所造成資訊及設備的傷害，在實體設備安全上，要能防止設備因不當的安裝、設定及使用，造成的資訊安全事件，最後，在資料安全上，應防止資料遭未經授權之存取及誤用，並保護資料的完整性及可用性。

要達到以上目標，就要從人員教育訓練、制度與作業流程的規劃及施行，資訊技術及工具的使用等三方面來著手。員工是企業在資安防護上的第一線，由於他們的疏忽，可能會造成惡意軟體感染與意外資料外洩的風險。很多公司都忽視了這個防線，欲提升人員的資訊安全意識，唯有透過不斷的資訊安全教育訓練，才能灌輸員工正確的觀念，讓資訊安全的觀念深植人心。

制度就像企業的骨架，用來撐起企業的整個經營管理，一套完善的資訊安全管理制度，雖然無法完全避免危安事件的發生，但卻可以降低及避免許多不必要的資訊安全風險和傷害，而這些可以降低的風險通常才是造成企業傷害的主因。

企業好不容易建立了良好的管理制度，但要去落實執行卻常常會有心有餘而力不足之憾，原因在於某些制度的落實，可能非常耗時費力，久而久之就疲乏了，這時可以去搭配一些有效率的工具來協助解決問題。

小潘聽到這裏，心想自己在大公司有錢、有人，要推動資訊安全的工作都很費力，微型企業要錢沒錢、要人沒人，何況資訊安全對企業而言又不是現階段最重要的議題，要推動就更加困難了，如何協助微型企業做好資訊安全，也許是下一個重要的議題！在師生下午茶約會結束離開時，小潘心中默默許下願望，有朝一日應該要投入協助微型企業做好資訊安全管理的工作。