文／郭尊華

資訊保安已超逾網路範疇

使用防火牆及防病毒軟體就足以保護公司數據安全，似乎只是不久以前的事。按照現今的標準，以往的網路保安威脅傳播緩慢，且容易預知，只需於網路邊界採取阻擋措施，即可將負面影響降至最低。

如今情況卻不再如此簡單。在現今的商業環境中，資訊於員工、合作夥伴及客戶之間不斷流動，其中只有少數用戶是處於企業網路的控制範圍內。每個端點均是網路罪犯截取重要及敏感資訊的潛在點，而隨著網路罪行日益嚴重，許多人透過竊取敏感資訊以換取經濟利益。

在此同時，除了企業本身的內部網路保安政策外，業界及政府法規亦敦促企業確保網上商業通訊及交易受到保障，以及維護資訊安全可用。

顯然，網路已不再是隔絕外界威脅的邊界，因此，資訊保護不再只是保護網路，而是隨時隨地保護資訊。

無論數據遠或近，保安亦不容忽視

在這數位時代，商業數據在網路保安狀況各異的機構及個人之間川流不息。無論是製造新產品、交付貨物及服務，或業績報告，機構均倚賴彼此間的互動聯繫開展業務。

例如，銷售人員會透過飯店網路連接至公司網路；訪客透過公司網路或無線網路上網；員工透過家居網路存取公司資訊、檢閱電郵，或由遠端資訊站下載附件；客戶透過家居網路或無線網路，進行網上商業交易。

合作夥伴的情況又如何？一般金融企業擁有數千名合作夥伴的「信賴」，並以每年新增 50 ～ 200 名的速度成長。對網上零售商而言，情況更為複雜，需與各方保持網際往來，其中涉及合作夥伴、聯繫機構、附屬機構及其相關的合作夥伴等。

處身這些連繫中的重要資訊極為脆弱。因此，保護資訊不僅須在網路內部進行，以消除駭客、網上竊賊及間諜程式的風險，亦須於整個業務的銜接範圍採取必要措施，包括透過保護、配置、使用及端點管理加強終端網路保安，亦即是端點保安。當然，簡單的人為錯誤亦會使機構面臨危機，甚至殃及客戶、合作夥伴及員工。

企業及個人的生活、工作、娛樂，更是息息相關，資訊的保護與風險，往往只差咫尺，潛在風險卻可能影響深遠。

今非昔比

以往的網路保安威脅顯而易見，如今卻往往經過精心設計低調行事。因為按現今價格，成功安裝廣告及間諜程式，於視窗上顯示一次，均有 5 ～ 20 美元的回報。

這僅是冰山一角。研究人員發現，傀儡網路（bot networks）的「租金」高達每小時 3000 美金，而

個人資料如身份證號碼則售價為 50 美元。以往的威脅多為無的放矢，任何人都可能遇上；如今的威脅卻有清晰的目標及針對的地域。網路罪犯正以此為生財工具，透過不著痕跡及精密的模組式惡意程式代碼等犯罪程式，從事盜竊、勒詐及詐騙等勾當。

保存、管理及保護數據的工作已由過往的具挑戰性，演變至今異常複雜及困難，同時又極為關鍵的情況。資訊保護重要性已超逾網路保安範疇，必須隨時隨地保護資訊。

畢竟，數據的損失，亦即是業務的損失。

隨時隨地保護數據

為降低資訊風險，機構必須確保資訊的存放點，即其管理範圍內外的所有端點均備有安全措施。由於端點保安管理在機構行政控制範圍內，因此可採用固定式的代為管理採取適當應對措施。由於這些端點往往擁有廣泛存取及儲存權限，因此針對端點應採取更健全及堅固的保安措施，絕不可掉以輕心。

防病毒軟體、個人防火牆及入侵偵查保護均有效保護受控終端。現在防病毒工具已被普遍使用，最有效的保護措施包括不規則或探索式威脅偵查技術及防間諜程式功能。

儘管個人防火牆（或主機防火牆）的效果只侷限於網路層面，有一定限制，但亦是一種被普遍採用的應對措施。個人防火牆主要利用規則允許的協議及連接，通常無法阻止應用軟體層面的攻擊。不過，個人防火牆仍是受控端點保安的重要組成部分，因為其只會允許規則許可的網路傳輸。

入侵偵查保護可為受控端點提供另一層網路保安防護。主機入侵偵查保護可阻止針對系統及對應用程式的不明攻擊，補防病毒軟體之不足。網路入侵偵查保護工具可使系統免受蠕蟲等網路威脅侵害。部分網路入侵偵查保護解決方案倚賴簽名，因此能保護系統免受已知攻擊的侵襲；而其他解決方案則針對更先進的機制，如簽名式漏洞及協議異常偵測，以阻止未知的威脅。

常見的保安技術還包括應用程式控制、主機整合檢測、修補程式管理、緩衝溢出保護以及加密技術。應用程式控制可找出個人防火牆技術的漏洞，並進一步確定控制網路流量。主機整合檢測可評估多種網路保安系統，確保終端有能力防禦各種潛在的威脅。

修補程式管理可確定並根除軟體代碼缺陷，緩衝溢出保護可監控端點，並找出所有企圖利用緩衝溢出攻擊的已知及未知威脅。最後，在手提電腦等端點被竊或遺失的情況下，檔案及磁碟加密可防止資訊洩漏。

這些技術固然均相當重要，但仍要正確安裝、開啟、設置並根據連接公司系統時的情況做及時更新，才有價值。網路連接控制技術可確保連接公司系統的電腦，均已妥善安裝所有最新並可正常運作的保安裝置，提供接觸敏感數據的安全環境，以符合公司制度的要求。這對受控系統（公司手提電腦、桌上電腦、流動設備）及未受控系統（訪客電腦、員工電腦及資訊站）均十分重要。

為降低資訊外洩風險，保護未受控終端亦十分重要。然而，由於這些設備不在機構的控制範圍，需要不會在特定數據交流外強制執行變動或限制的「隨需」保護。

針對該情況，機構可利用隨需技術，包括主機整合檢測、暫緩清除、惡意程式代碼保護、防火牆以及虛擬安全空間。隨需主機整合檢測及隨需防火牆與代理程式提供相近的保護，待交易完成後隨需暫緩清除，可清除瀏覽器的殘餘數據及應用程式的暫存。

隨需惡意程式代碼保護利用行為分析技術，可確定未受控端點上可能存有的鍵盤記錄器及其他惡意程式代碼。此外，隨需保安虛擬空間技術，可製造加密的工作空間，防止因未受控端點而造成資料外洩。

當然，倘若沒有端點使用者的配合，網路資訊保安解決方案不可能取得成果。公司及員工的網路保安意識和責任，已被視為網路資訊保安策略中不可或缺的一環，只要公司認真確立要求，並採用自動化以簡化執行，效果將顯著增強。

單憑防火牆或防病毒軟體便已足夠的時代已走入歷史，然而，只要機構的資訊保安意識不再侷限於網路，配合眾多工具，仍可隨時隨地保護資訊。只要公司及員工配合執行最佳網路保安措施，機構完全能夠借助網路保安科技，不但保障自己控制的系統，同時亦保障重要合作夥伴、員工及客戶設備的安全。

郭尊華小檔案
香港玉山科技協會　理事
Symantec 大中華地區總裁

有關香港玉山科技協會的資料或入會詳情，請與本會秘書處聯絡（電話：+852-2758-6276 / 電郵：secretariat@montejadehongkong.com），或瀏覽本會網址 www.montejadehongkong.com。