攝影／楊易達

「新世代數位治理公務資訊菁英講座」研討會記實

雲端時代的新資訊安全觀

從資安護理做好個資保護與資安

資訊社會會遭遇到很多種類型的攻擊手法，不論是被動、主動、實體臨近、內部人員或者分發攻擊，都可以導致各種重要資訊外洩。

這些工具除了常見的惡意軟體，例如後門和木馬程式入侵應用層，使用者模組和核心模組的Rootkit則攻擊作業系統的執行層，BIOS級惡意軟體則攻擊BIOS，CPU級惡意軟體則攻擊BIOS和CPU。目前除了BIOS和CPU的攻擊還是攻防實做階段外，其他的攻擊手法都已經是事實。

從安全違規的等級來看，從威脅、攻擊、破壞、滲透、破解到損失，安全違規等級越來越高，就像是一些支付卡公司，即使已經通過PCI DSS的標準，還是發生金融機構遭駭的資安事件。

根據Verizon Business在2009年資料外洩觀察報告發現，從入侵到破壞系統的時間，將近3成（27%）在1分鐘內就已經完成，超過2成（21%）則在1小時內完成，將近3成（29%）則在1天內完成，超過1週才完成系統入侵到破壞只有17%，超過1個月的只有6%，超過1年的則無。

攝影／楊易達

中華民國資訊安全學會
常務監事 樊國楨

從入侵到破壞將近6成所需要的時間都在1小時內，但從破壞到發現，1小時內被發現的只有不到1成（8%），1天內發現將近2成（16%），1周才發現的將近3成（25%），1個月才發現將近過半（49%），甚至還有1%是超過1年才發現系統已經遭到破壞，由此也可以證明，資訊系統有一種時間差產生的脆弱性風險。

而從該公司的研究中則發現，透過可以測錄封包的惡意軟體，資料外洩比數將近9成（89%），具有鍵盤測錄功能和間諜程式的惡意軟體，資料外洩筆數也超過8成（82%）其餘資料外洩筆數比例次高的則為後門程式（79%）和SQL Injection（79%），普遍將近8成資料外洩筆數。

因為不同的資訊系統會有不同的安全等級標準，若為普級，資訊系統的分級則應該做到安全內容自動化協定（SCAP）；資訊系統分級若為中級，除了SCAP的規定外，還需要符合可信賴網路接取（TNC）；資訊系統分級若為高級，除SCAP和TNC外，還需要做到可信賴平臺模組（TPM）和磁碟機加密。

系統的信任是基礎，若對照利害關係人的企業責任，根據馬斯洛（Maslow）需求框架來看，都有很好的對照。

從基礎的生理需求、安全需求、愛與歸屬需求、尊重需求和自我實現需求，對照企業四大責任，包括從基礎的經濟責任（股東、員工權益極大化）、法規責任（遵守法規的強制性要求）、倫理責任（公平、正義、不製造負外部性）及公益責任，都可以對照到ISO 26000提出的社會責任七原則：像是可歸責性（Accountability）、透明度（Transparency）、道德行為（Ethical Behavior）、尊重利害相關方、尊重法規、尊重國際行為標準和尊重人權。

上述行為準則與規範，都可以對照到ISO 26000提出社會責任的核心主題，包括：機構治理、人權、勞工實務、環境、公平運作實務。

網站安全三部曲 全面保障個資安全

Web仍是目前最顯著的攻擊管道，根據Websense Security在今年1月的調查，有58%的資料竊取攻擊是透過Web管道達成，其中，在35%的Web攻擊中，內含資料竊取的木馬程式。

若從幾個實際的案例來看，不論是智慧財產局二手教科書網站，資料外洩1.6萬筆，或者是美國電信服務商AT&T外洩11.4萬名iPad的用戶資料等，都可以看出網站已經成為重要的個資外洩管道。

根據新版個人資料保護法，因為強化企業以及公務機關的個資防護責任，所有經電腦處理和非經電腦處理的個人資料，當民眾要索賠時，不需要負起舉證的責任，非公務機關必須要證明「無故意或過失責任」才能免責，而公務機關責需要提出「無過失責任」才能免責。

若進一步從網站相關的個資循環來看，可以分成蒐集、處理、利用和傳輸等主要4個循環。網站的資料蒐集可以包括：取得個資的主要管道、必須揭露隱私規章；處理則包括：採取適當保護措施，避免個人資料被竊取、竄改或毀損；利用則包括：應使用於蒐集的特定目的內的使用，特定目的外的使用則需另外取得書面同意；傳輸則包括跨單位傳輸的同意與安全，以及跨國傳輸的規範。但是一般公務機關對於涉及個資的網站就應該做到安全檢測、安全防護和安全監控的責任，也必須做到善盡「保管」與「告知」之責。

因此，第一步就是實施網站安全檢測。一般網站常見的功能元件包括登入頁面、全文檢索、資料庫系統、訊息交流和討論區、參加抽獎、報名活動、課程、網頁問卷、資料轉送和檔案下載等功能，但這些功能元件中，則有包括常見的跨站攻擊（XSS）、隱碼攻擊（SQL Injection）、資源嵌入、檔案匯入、明文密碼及不當錯誤資訊揭露等資安弱點。在OWASP頒布的10大網站資安弱點中，隱碼攻擊則從2007年的第二名躍升為2010年的第一名，顯見此類惡意攻擊的嚴重。

攝影／楊易達

達友科技資安顧問
林皇興

常見的檢測方式包括動態的黑箱測試，靜態的白箱測試、源碼檢測及靜態檢測。但這沒有絕對的解決方案，通常是相互搭配而成。第二步則是做好網站安全防護，搭配Web AP防火牆進行保護；第三步則是做好網站安全監控。以此三個資安防護方式針對個資蒐集、處理、利用做到縱深防禦策略。

從個資法風暴談訊息保全

現行電腦所導致的犯罪事件詐騙手法日新月異，常出事的單位不在管轄範圍內，不僅無法獲得機關組織的重視成為治理的議題，資料外洩犯罪事件的起訴成功率不高，上述因素都成為修訂現行個資法的重要原因之一。

個資法修改最主要的目的就是尊重人格權，除了擴大保護客體，納入人工資料；刪除行業別限制，普遍適用每一種行業；新增行為規範，要求資料蒐集必須書面同意，也增加許多告知義務；此外，強化政府行政監督檢查的能力，賦予中央目的事業主管機關以及地方政府都有強制檢查的能力；促進民眾參與，加入團體訴訟的制度；也調整責任內涵，包括刑罰以及加重負責人監督責任。

個資法強調個人資訊揭露的自主權，為組織帶來最大的風險除了2～50萬元的行政罰鍰與處分，單一案件5百元～2萬元的民事賠償，以及團體訴訟2億元的求償金額外，還有2年以下有期徒刑、拘役後併科20萬元以下罰金，意圖營利者，加重其刑到5年以下，或併科100萬元以下罰金。


攝影／楊易達

網擎資訊產品經理 廖享進

也因為個人資料外洩為組織帶來極大的風險，組織進行訊息傳遞和保存的過程中，一定要能夠符合風險規避的原則。目前，企業幾個重要的資料外洩管道包括：網頁、網站、資料庫和電子郵件，透過符合個資法規範的Web和Email Assurance主動式偵測解決方案，提供郵件安全和郵件外洩防護，提供完善的郵件備份管理系統，和郵件稽核管理、隨選加密按郵件記錄追蹤功能，並且能做到主動檢測外部文件、資料庫是否有洩至，當組織原有系統毀損時，也提供有使用才付費的雲端郵件緊急備援機制，僅需要透過更動DNS設備就可以啟動相關的備援機制。

如何做好雲端應用程式安全

傳統網路服務如何做到，要能在對的時間點，快速的將所需要的應用程式服務，即時傳遞到對的人身上，並確保中間的安全並節省成本，是一件難度很高的事情。不過，當所有的應用程式都變成雲端服務的同時，所有服務都是動態提供，除符合法規遵循外，資源運用除了整合實體還有虛擬，還能跨平臺或跨多個IDC甚至是不同的公有雲或私有雲。


攝影／楊易達

F5臺灣區技術經理 林志斌

這樣的雲端服務可以將應用程式和資訊，透過專屬全球應用遞送控制平臺，遞送到相關雲端服務的企業，藉此達到可用性、HA、異地備援、網路優化、資訊安全、整合、可視性等優點。

企業虛擬化到雲端成熟模型大致可分成分離、合併、整合、叢集、自動化和自主性五個階段。分離階段是測試與開發環境各自獨立；合併階段則是做到後端伺服器的整合；整合階段則達到容量隨需的境界；自動化階段則做到資料中心的自我管理；最後的自主性階段，則是達到企業雲端服務可隨需求自行開關取用，上述各階段端視企業現階段處於何處，就知道已經到達何種類型的雲端服務模型。

BIG-IP則可以做到滿足應用程式安全，並符合法規規範，達到具有強大防護且不中斷合法流量的防護境界。對此，也同樣可以改善網路語音的使用者溝通經驗，減少影音不同步的現象，關鍵在於，可以透過QoS頻寬流量調整的功能，讓網路語音以及重要的應用程式優先，其餘網路應用的流量則列為次要。透過這樣的優先次序調整，可以做到確保網路影音的安全與效率。

內外網都需做好資安協同防禦

現在的網路問題已經不是單純的內外網單點防禦問題，而是未來企業或組織越來越需要整體內部網路與系統的協同防禦機制。新一代安全威脅的挑戰在於，傳統的威脅依舊存在，透過內部網路的攻擊來源不斷，以及假冒、利用合法使用者不斷，才造成有超過85％的安全威脅來自企業內部。


攝影／楊易達

凹凸網路科技 資深業務經理 單益智

凹凸網路智慧型的流量管理設計，除了具備精確的識別技術（IPR）以分流標籤技術外，也必須支援多閘道極多ISP路由的流量管理能力，透過獨立流量管理模組、獨立流量策略並具備排程功能，基於應用的第三層流量管理，做到頻寬與配額管理，支持頻寬限制、頻寬靜態保證、頻寬動態保證，以期能貼近用戶的流量管理需求，並可結合DDoS模組，限制P2P功能，做到即時流量統計和排行。

若以目前流量管理的處理過程，首先要先進行流量安全過濾，再來要進行流量識別、流量分類，才做到流量管理和報表統計。因為採用這樣的智慧型三層流量管理，以路由或NAT方式放置在網路出口，則可以達到防火牆、流量管理、多ISP路由管理、多WAN負載平衡、伺服器負載平衡、DDoS防護及HA（高可用性）。透過提供獨立的Anti-DDoS模組，針對ISO七層網路協定，提供七層防禦機制，包括：協議異常檢測、來源異常檢測、黑白名單、兩級統計異常限制、訪問控制、特徵式的異常檢測與流量管理，達到保護伺服器、降低頻寬耗盡風險及降低對伺服器的資源損耗；也可以確保設備本身遇到DDoS攻擊時不癱瘓，能為後端伺服器提供防護。

用直接連網加快雲端服務導入

當上網需求增加時，包括傳統的應用程式、Web應用程式、精簡型電腦、影音、虛擬化，甚至是雲端服務或者是SaaS（軟體即服務）等，其中，雲端服務則是未來發展趨勢。

根據調查，資安問題是最大的挑戰（53％），其次為效能（33％）和控制性（31％）等，也有部分企業擔心一旦採用雲端服務，就會被部分廠商限制或鎖定（30％）。

但時至今日，企業總部的對外連網，還可以使用各種雲端服務外，企業內部除了內網，還可以使用私有雲等各種網路服務。

但到了雲端服務的時代，面對同樣的網路威脅，Blue Coat透過SaaS、網路安全閘道器（SWG）和Proxy Client，加上16個威脅偵測引擎，便可以提供低成本、簡化、高效率和安全的雲端資安解決方案。


攝影／楊易達

Blue Coat大中華區市場營銷經理 申強

當每個地方都有使用者、資料和應用程式存在時，為什麼網路流量都必須流回企業總部才能控管呢？透過直接連網（Direct To Internet）服務則可以加速企業導入相關的雲端服務，時間上只需要3個月到半年的時間，可以節省至少80％內網的網路成本。

甚至有企業評估，每年可以節省30萬美元以上的IT支出。面對雲端企業時代的來臨，每個地方都可以連網，爆量的網路資訊，有超過3分之1的員工可以進行遠端工作，且網路就如同一個資料中心一般，Blue Coat提供的雲端資安解決方案，增加3倍～25倍的企業產能，降低多餘的授權費用並整合更多的資安需求。

用即時內容分析保護雲端安全

根據調查，2010年的資安挑戰就是網頁威脅，隨著各種服務Web化，92％的新興威脅來自網頁；從2008年至今，惡意程式威脅則已經成長671％；84％的網頁惡意程式來自合法網站。


攝影／楊易達

M86 Security大中華區業務總監 林鴻源

而從Web 2.0的規模來看，目前針對未知攻擊的病毒攔截率只有40％，也有52％的惡意程式在24小時內會自動刪除，全球平均每天都有10億封含混合式威脅的電子郵件。這也證明黑色產業鏈已經成形。

Web 2.0資安威脅日新月異，69％的資安弱點是Active X，11％是Java，Quicktime也有10％，其餘資安弱點包括Flash（4％）、Acrobat（4％）。

不論哪一種解決方式，目前，唯一能夠刪除零時差攻擊的方式是「即時」和「動態」。因為這種攻擊能夠了解行為偵測和廠商服務，得提供即時性動態偵測，行為偵測和啟發式偵探技術。當測試環境擁有3萬個以上惡意程式的網站，傳統的網頁過濾只有3.8％有效；整合三種主要防毒產品，只有39％有效，能做到即時內容虛擬分析技術，就可以達到100％有效。

M86 Security推出整合式威脅管理閘道器，可以做到即時防惡意程式，動態Web 2.0控制，動態網頁自動修復，URL過濾，應用程式控管、安全網頁快取（Secure Web Caching），由HTTP、HTTPS和FTP進出流量全管，SSL加密通道的疏漏，整合卡巴斯基或Sophos的防毒功能。但要真正做到解決第一代零時差Web 2.0修復版的產品才行。