落實沙賓法案

正視郵件稽核與備份

文／林裕洋

許多與案情相關的電子郵件，都被有心人事惡意刪除，以致於在案情追查的過程中，遇到極大阻礙。因此，美國證管會制訂了沙賓法案，郵件稽核與備份成為資訊部門必須正視的議題。

談到郵件稽核的議題，相信許多人對2001年由安隆有限公司(Enron)、世界通訊公司(Worldcom)等財務欺詐事件，所引爆的一連串惡意破產世界，應該都依然記憶猶新。

在該事件的調查過程中，美國證管會發現許多與案情相關的電子郵件，都被有心人事惡意刪除，以致於在案情追查的過程中，遇到極大阻礙。正因為如此，美國證管會制訂了沙賓法案，其中一部分條文是強迫上市公司必須針對與公司業務有相關的電子郵件，必須至少保存7年，導致郵件稽核與備份成為資訊部門必須正視的議題。

此外，隨著電子郵件已經成為洩漏公司機密的管道之一，無論是駭客的攻擊手法，或是有心人士惡意散播等等，以致於許多公司紛紛透過流程設計、行為監控、郵件稽核等，乃至於直接對機密資料加密如DLP（Data Loss Prevention，資料外洩防護）、DRM（Digital Rights Management，數位版權保護）等方式，來確保資料單全性。只不過在複雜的資料加密措施，仍然可能發生檔案外流之後會被破解的風險，所以若能夠在重要資料外洩之前便攔阻下來，自然可以避免對企業的營收或商譽造成傷害。

另一方面，從法律層面來看，以2012年10月份剛上路的個人資保護法為例，明確指出企業必須善盡保管人的責任，若發生機密資料外洩的狀況，最高將支付2億元的罰金，顯見郵件稽核是企業不可或缺的資安產品。

郵件稽核運作兩大原理

目前市面上常見的郵件稽核設備，通常是指一台1U高度的應用伺服器，本身並沒有發信或收信的功能，而是架設在郵件伺服器旁，針對郵件伺服器上的郵件進行檢查。當然，有些廠商也有提供可收、發郵件，並且具備防毒、防垃圾郵件、郵件稽核等功能的多功能郵件伺服器，強調能夠以單一台機器滿足企業用戶的需求。

其實郵件稽核的運作原理，就是讓資訊人員可用關鍵字查詢的方式，找出潛在的問題郵件，目前自訂查詢的範圍，則通常涵蓋寄件人信箱、郵件主旨、郵件內容、附件內容等等。

郵件稽核設備通常會提供事前稽核與事後審查兩種功能，若從防止機密資料外洩的角度來看，企業用戶應該要事前稽核的作法，也就是在郵件發送出去之前，先經過完整的比對與查詢之後，才允許郵件伺服器將資料送出。不過，此種作法在實務上執行時會遇到很大的困難，主要是郵件稽核設備必須逐一去拆解每封郵件，若郵件本身有夾寄檔案，還必須解開比對。在此種情形之下，若待處理郵件過多，輕則影響到業務上的延遲，重則會導致設備當機，以致於重要資料遺失的風險。

有鑑於此，許多廠商也推出事後稽核的功能，也就是讓郵件歸檔、備份與稽核三項功能同步進行。此種作法是在郵件伺服器在收、發信時，郵件稽核設備會同步抄錄一份資料，再依照管理者事先輸入的關鍵字，逐一去比對各種關鍵字與欄位，當有發生異常狀況時，便即刻發出警告信給管理員。

儘管從防止機密外洩的角度來看，企業用戶應該要選擇用事前後稽，才能達到採用該設備的目的，但事後審查卻具備有不會影響網路設定，工作流程不需要改變的優點，也能符合個資法的規範。因此，建議企業用戶不妨從分析工作流程著手，再評估企業能夠承受的風險，以及能夠負擔的預算，才能讓郵件稽核設備發揮最大的效益。

郵件稽核的關鍵

儘管駭客攻擊手法日益進步，對企業的攻擊行為也早就從破壞網頁，轉型為竊取機密資料。只不過根據國際電腦安全協會（ICSA Security Report）的統計資料指出，事實上有超過80% 的洩密事件來自企業內部，僅有20% 屬於來自外部的入侵攻擊，顯見員工有意或無意的洩漏資料，更是企業必須注意的重要事項。

目前市面上有提供郵件稽核的廠商不少，加上產品問世至今多年，所以多半都提供前、後稽核的功能，並且都支援市面上常見的電子郵件伺服器，如Exchange Server、Sendmail等等，大致上而言

功能並沒有差距太多。不過，郵件稽核設備的效能，除了取決於軟硬體設備之間的整合程度之外，引擎本身拆解郵件的速度與辨識能力，則會影響到郵件稽核的準確度查詢速度。其次，操作介面是否能夠符合企業用戶的需求，以及內建關鍵字詞的多寡，發現危險郵件後續處理方式，都是企業用戶可以考慮的重點。

Cellopoint Email UTM郵件安全與管理的整合式解決方案採行邏輯。

事前稽核功能相去不遠 差異程度取決於細膩度

目前各家廠商提供事前稽核功能的功能其實都差不多，除了最基本的寄、收件人、主旨、附件檔名等欄位之的必對之外，也都能夠深入郵件內容、附件內容等等，透過預設的關鍵字進行比對。尤其隨著個資法成為企業最在乎的議題之後，各家廠商似乎也都有志一同的提供身分證字號、電話、銀行帳號、信用卡號、地址等等資料的比對功能。若要挑出其中的差異，不妨從比對速度與添加、修改關鍵字的難度著手。

但要注意之處，各家郵件稽核設備能夠支援的附件格式不同，除了常見的doc、xls、PDF、txt等格式的檔案外，最好先詢問各部門慣用的檔案格式種類，除了公司允許的壓縮檔案外，是否還有其他特定格式的檔案，這些都是資訊人員在POC過程中，千萬不可忽視的重點。

另一項採購郵件稽核設備的重點，應該放在設備本身的稽核流程，能否與企業的資安流程結合，也就是在發現隱藏問題郵件時，能即時通知資訊部門與相關主管單位。

事後稽核功能差異大 需注重使用者查詢介面

在前面的文章曾經提過，事先稽核與事後稽核的目的不同，事後稽核比較偏向是將往來的郵件備份下來，並且做好歸檔的工作，除提供稽核單位透過關鍵字追查的功能之外，也是希望當用戶端電腦發生問題時，可以協助快速回覆資料。

若要從事後稽核的角度來篩選產品，要考慮的項目會相對更多些，除了先前提到的關鍵字搜尋、支援的檔案格式之外，防毒、防垃圾信功能也是需要考慮的重點。因為事後稽核會備份郵件伺服器上發出，以及收到的所有信件，而在郵件成為許多病毒的入侵工具，以及散播廣告的溫床時，若沒有透過防毒、防垃圾信功能的協助，不僅會將病毒備份下來，也會讓郵件備份所需的容量暴增。

另外，隨著愈來愈多企業用戶使用雲端服務，Google Apps的穩定性也廣被企業用戶所接受，但是目前有部分郵件稽核廠商的產品，並沒有支援網路郵件伺服器備份的功能，因此也是資訊人員不可忽視的重點。

至於郵件歸檔功能方面，考慮到多數企業會開放查詢的功能，讓員工可以依照工作上的需求，尋找過去的歷史郵件。因為該部分與流程設計有極大關係，所以建議資訊人員最好能夠邀請相關部門的同事一起參與測試，以確保導入過程能夠更為順利。