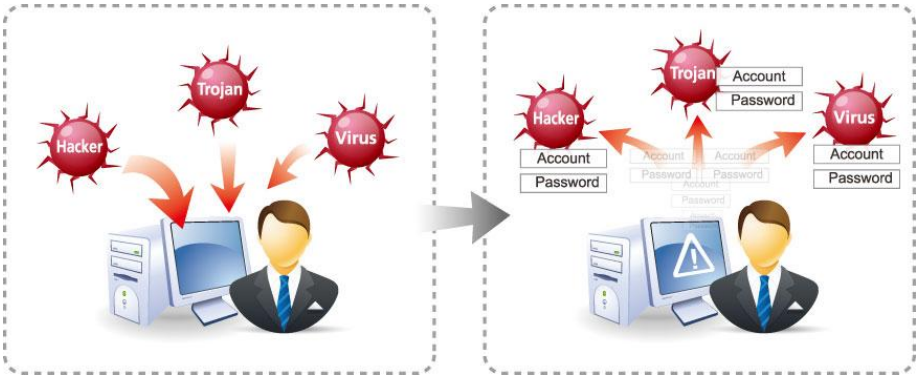
# 杜絕機密外洩，從建立可信任的郵件安全環境開始

**網路上的風險**

近期 Google 退出中國的事件鬧的沸沸揚揚，依 Google 的說法其原因是中國針對網路進行了監控及審查。另外從去年多個網路服務、購物平台爆發洩漏個資 8 千多筆、知名主機代管商洩漏客戶資料超過 4 千筆的事件來看，突顯了資訊透過網路傳送的不安全性，除了內容遭竊取外，透過電子郵件社交工程（Email Social Engineering）的駭客攻擊模式也層出不窮。讓收件者誤觸「網路釣魚」、「木馬程式」、「殭屍病毒」等，這類的變種病毒會在登入系統時盜取帳號及密碼，根據資安人雜誌（2010.03）的公佈，每天平均超過 300 個變種殭屍病毒新樣本的產生，對企業而言，要具備可防禦不斷更新的垃圾郵件攻擊的能力，是資安人員首要面對的問題。




企業間經常透過電子郵件做為溝通的重要工具，但是若沒有一套完整的保護機制，只要有心人透過一些封包擷取工具，就算沒有高超的駭客技術也能輕易取得電子郵件的內容。因為郵件都是以類似明信片的方式在遞送，所以遞送的過程中可以說是沒有任何隱私可言，雖然郵件簽章加密（Email Signature Encryption）的技術已經推行多年，但因為憑證的導入成本較高，而且若想寄出加密的信件，也不是自己單方面能完成，還必須先取得收件人的電子簽章。因此，在憑證使用並不普及的現況下，簽章加密並不是方便的保護機制。除了簽章加密的方式外，其實還可以透過其他的方式來保護郵件遞送時不被有心人士擷取資訊。Openfind 針對上述的郵件問題，特別在產品中規劃了多項的安全性功能，可以讓寄件人能安心寄信，管理者能方便管理。

**安全的網路傳輸**

透過網路遞送資訊時最基本要注意的就是避免透過明碼方式遞送資訊，Openfind Mail2000 可以支援 HTTP、SMTP、POP3 與 IMAP4 透過 TLS/SSL 的加密傳輸協定來進行資料傳遞，由於傳遞的資料是經過加密的，就算拿到資料也無法識別內容，這樣無論透過 Web Mail 或 Outlook 之類的電子郵件工具進行信件收發，都不用擔心傳遞的資訊被有心人所擷取。但上述的機制只解決從用戶端到 Mail Server 的資料傳遞安全，而郵件主機間的溝通是透過 SMTP 通訊協定，雖然也可支援加密傳輸，但是加密必須是雙方配合才能達成的，而實際上沒法要求收件人的郵件主機也一定要開啟加密傳輸的功能，因此郵件的遞送還是得透過明碼的 SMTP 方式來進行。

為了強化加密傳輸的完整性，Openfind MailGates 提供了隨選加密的機制，透過標準的 ZIP 壓縮加密方式，不但可以縮小郵件大小，更重要的是還可以將信件內容及附檔進行加密，如此即使透過標準 SMTP 方式遞送郵件，也可以確保郵件到收件人開啟時都是處於加密的狀態。而密碼則可由寄件人與收件人先行約定，或是由 MailGates 自行亂數產生給寄件人，再由寄件人通知對方即可。MailGates 隨選加密技術是以低成本但可簡易應用的方式來達到類似簽章加密效果。


**防範惡意程式**

郵件傳輸的安全性可以靠加密技術來保護，但是收到的郵件中若有包含惡意程式要如何防範呢？Mail2000 可以讓使用者透過封鎖圖片、去除 Javascript 及強制純文字轉換的方式來阻擋社交工程的攻擊或惡意程式的入侵。此外許多郵件系統都是與作業系統整合，信箱的登入直接使用網域的帳號密碼或是作業系統本身的帳號密碼。而現在上網的方式很多，若是在網咖或其他公共網路上進行信件收發時剛好被有心人側錄了帳號密碼，駭客透過帳號登入作業系統或進行其他動作，這可能會對公司系統及網路環境造成嚴重影響。因此 Openfind Mail2000 上的信箱

並不使用系統上的帳號權限，而是自行建立虛擬帳號，萬一帳號密碼被竊取，最多的影響也只是個人郵件的部份，對主機或網域並不會產生安全上的漏洞。

Mail2000 可以支援各種安全性的機制來保護密碼不被擷取，包含密碼複雜度的設定可以規範使用者不能設定過於簡單的密碼，Web Mail 登入可要求輸入驗證碼阻擋機器人式的字典攻擊，還有提供虛擬鍵盤可以防止木馬程式側錄鍵盤輸入，甚至也能設定成一次性密碼來確保使用者身分的正確性。這些安全機制都可更加保障系統運作的安全。

等級低：標準虛擬鍵盤

等級中：重新亂數排列

等級高：按鍵支援遮罩防護

**防患於未然，避免機密外洩**

企業提供員工郵件信箱主要是讓員工可以方便與外部聯繫，但企業內有許多機密資訊可能會因為員工的不當行為而經由電子郵件對外洩漏。MailGates 可以提供管理者即時發現資訊不當外洩的機制，並且不會影響到一般信件對外的正常溝通，因此除了郵件傳送接收需要能有安全的保護外，企業也有必要制定郵件遞送的政策，將違反郵件政策的信件進行攔截並依管理需要進行刪除、放行、退回、轉寄等稽核動作。郵件的即時過濾雖然可以攔截明顯違反企業政策的信件，但是有時政策制定沒法面面俱到，或是遇到員工有心規避，還是可能讓不該外流的資訊出去，這時企業採取的手段就是進行完整的郵件歸檔保存，日後當有需要進行證據調閱時，還能有機會事後找出資訊外洩的原因。

**分權分責做好管理**

許多公司為了要保存與客戶往來的紀錄或為了符合法規要求，會針對郵件進行歸檔備份的規劃。而大部分企業把電子郵件的管理交由資訊部門的同仁來進行，但是卻沒有對資訊人員做權限的控管，如此資訊部門的同仁可能可以輕易看到他人信件的內容，這樣不但沒有達到資訊管理的目的，反而增加了資料外洩的風險。


Openfind 針對企業郵件的需求提供了完整的稽核管理機制，在 Mail2000 的管理者權限上是沒有辦法直接開啟使用者的信件來閱讀的。MailGates 的主要功能是進行郵件過濾，除了垃圾信和違反郵件政策的信件外，一般信件都無須保留在系統上，此做法可避免系統管理者有機會去檢視一般正常往來的信件，只讓管理者專心處理問題信件即可。MailBase 則是能將完整郵件進行歸檔保存，但是操作上必須搭配完整的權限控管機制來區分系統管理權及信件調閱權，系統管理者只能進行系統管理的工作，內容稽核人員才有查詢他人信件的權限，若有需要還可以做到查詢信件時一定要經過他人授權才可進行的雙重認證機制，並且所有的信件查詢及調閱的動作都會被完整的記錄下來，這樣郵件備份資料就可以在有管理的機制下被保存，如此才能在適當的時機提供給企業最有利的利用。

**系統與制度並重**

郵件安全光是依靠系統是絕對不夠的，資料安全最大的問題通常都是出在人的身上，因此要做好郵件安全的管理，除了建置完善的郵件系統外，還要制定出良好的管理規範讓郵件系統的使用者及管理者都能在標準的規範下安全的使用郵件系統。