電子郵件安全指引 - 電子郵件攻擊篇(上)

Openfind PM Team

近年來電子郵件已成為現代人最重要的溝通工具之一，因電子郵件在使用上簡單，而且傳遞快速，成本又相當的低廉，使得企業使用頻率大幅提升。但是隨之而來的電子郵件安全管理問題，例如社交工程、DDoS/DoS 阻絕服務或大量封包連線攻擊、垃圾郵件過濾、機敏郵件稽核...等，已引起各政府機關及企業的關切與重視。

然而完整的郵件安全規劃涵蓋的層面非常廣泛，包括郵件使用規範、郵件系統防護、系統維護、系統存取、系統驗證、郵件備份與稽核、緊急應變措施以及教育訓練等，欲完整瞭解上述的各個層面以及達到一定水準的郵件安全防護，並非是件容易的事情。

深耕郵件市場逾十二年的 Openfind，累積了豐富的實務經驗，並與各政府單位合作長達十年的豐富經歷與電子郵件領域深厚的技術背景，將針對上述多項郵件安全所需注意之處，集結成冊提供給企業做為最實用的一本工具書。此手冊彙整了研考會「電子郵件安全參考指引」的內容，並針對各項郵件安全的作業要點提出重點式的說明，希望透過此內容讓閱讀者對電子郵件安全有更進一步的瞭解。

本期電子報內容，我們將針對「電子郵件攻擊」為主題，再細分為幾個重點項目說明，如社交工程攻擊、Dos/DDos 攻擊垃圾郵件及退信攻擊等...並輔以 Mail2000 電子郵件系統、MailGates 郵件防護系統與 MailBase 郵件歸檔管理系統三項產品的功能作為範例參考，供讀者針對貴機關/公司現行郵件系統進行檢視與調整，希望透過這些介紹能夠讓讀者對於此部分有更深一層的認識。

電子郵件攻擊

隨著電子郵件使用的普及，越來越多人開始利用電子郵件進行不法的行為，輕則散發垃圾信件，重則竊取機密資料或是癱瘓他人郵件系統。本節將針對常見的電子郵件攻擊進行介紹，並在介紹的同時說明如何防備這些攻擊手法。

社交工程攻擊

社交工程（Social Engineering）指的是利用操縱人類心理弱點或是人際間的信任關係，竊取個人資料與公司機密的惡意陷阱。

常見的電子郵件社交工程手法，是透過聳動的郵件標題或假冒寄件人身分，來誘使收信人開啟郵件中的病毒檔案或是點擊惡意連結，若要避免組織受社交工程攻擊，除了針對員工進行教育訓練來提高資安意識外，透過優異的電子郵件系統主動進行社交工程防護，更能夠完善地保護組織資料。以下說明社交工程防護的作業重點：

- 教育訓練
  - 定期教育訓練

    定期對內部員工實施教育訓練，教導員工社交工程的攻擊手法、造成影響以及自我保護機制，例如不隨意的開啟連結、下載附檔以及寄送敏感資料等。
  - 社交工程演練

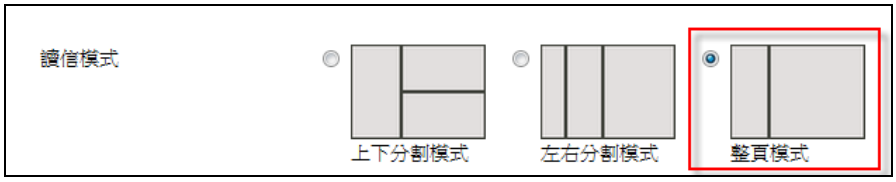
    定期透過社交工程演練來評估組織資安狀況，並設定評量指標，例如「郵件附檔開啟率」、「郵件點閱率」與「上次演練成績比提升」等，做為資安狀況的判斷標準。
- 郵件系統的安全設定

  社交工程雖是利用人類心理弱點做為攻擊手段，但仍可透過系統的設定來防範此類攻擊，例如直接關閉圖檔或是將信件類型轉為純文字檔，來避免使用者開啟信件中的惡意連結。以下利用 Mail2000 社交攻擊防護功能來做說明：

Mail2000 - 社交工程防護

(1) 調整讀信模式為「整頁模式」

讀信模式設為整頁模式，此模式可確保進入郵件列表時，所有未讀取信件都呈現未開啟的狀態，避免因預設開啟而誤觸病毒信件。



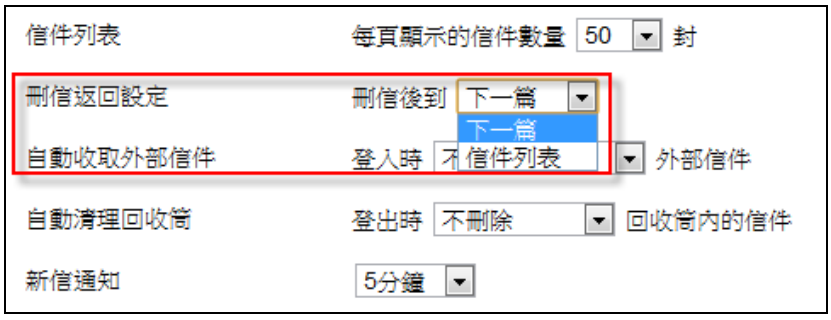
整頁模式設定

「上下分割模式」、「左右分割模式」的讀信方式下，使用者在進入信件匣時，系統會自動開啟最新的信件（如下圖紅框處），這樣很有可能會直接誤觸病毒信件，故在資安考量下，使用者應將讀信模式設定為「整頁模式」，確保進入信件匣時，信件都呈現未開啟的狀態，降低開啟病毒信件的風險。

整頁模式範例

(2) 「刪信後到信件列表」:

Mail2000 可讓使用者針對刪信後的動作進行設定，可設定為「刪信後到信件列表」，避免刪信後因為自動開啟下一封郵件，而誤觸病毒信件。



刪信返回設定

(3) 去除 JavaScript：

許多惡意信件是透過收件人開啟信件時，自動執行信件內嵌的惡意 JavaScript 語法來對收件人進行攻擊，Mail2000 可設定強制去除信件中的 JavaScript 語法。

(4) 封鎖外部圖檔：

信件中的外部圖檔會要求郵件伺服器向外部下載圖檔，這樣可能會觸發惡意連結或是受到 XSS（跨網站攻擊程式）攻擊，Mail2000 可設定強制封鎖外部圖片，使用者在確認寄件者為可靠寄件者後再行開啟圖片。

(5) 預設讀信方式設定為「純文字」

將信件內容轉為純文字，讓惡意連結直接失效。(此功能可透過管理者從管理介面強制開啟。)

安全性設定

預設讀信方式

垃圾信件

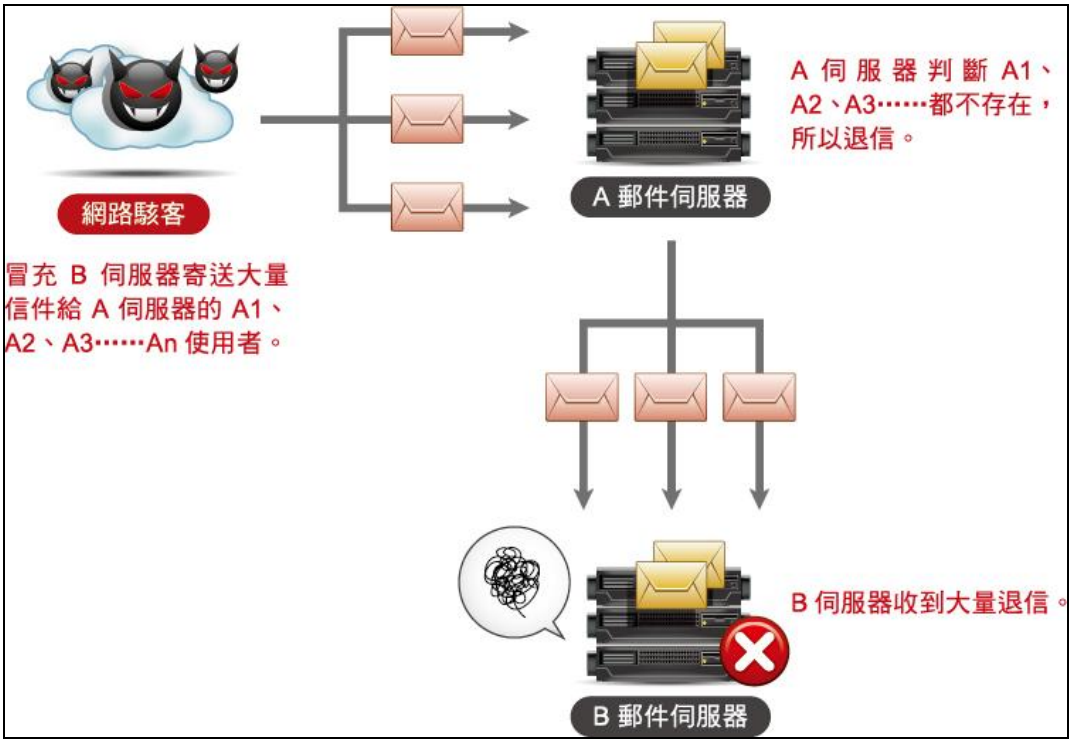
垃圾郵件（Spam）指的是未經收信者同意而大量寄發的電子郵件。這一類的垃圾郵件，通常會隱藏寄件人，甚至偽造寄件人、發信日期、IP、原始發信記錄..等，垃圾信件的內容以色情、發財等具引誘性的廣告居多。由於垃圾郵件通常是大量寄發，不但對收件人造成困擾，也會對 ISP 或公司郵件主機造成流量的負擔與經濟上的損失。

垃圾信件的過濾方式主要可透過信件發送行為分析、黑名單資料庫、SPF 防偽技術、網路認證金鑰（DomainKeys）、關鍵字過濾、貝氏過濾法（Bayesian filtering)

等，這些過濾技術的介紹請參考章節＜電子郵件過濾機制＞

退信攻擊

郵件伺服器在進行收信時，會在 SMTP （請見章節＜SMTP 協定＞）的階段檢查收件者是否存在，若是收件人不存在就會自動將該信件送回給寄件者，而駭客就是利用此退信功能，攻擊郵件伺服器。首先駭客會先確定要攻擊的帳號，然後假冒這些帳號，大量寄信給其它收件端伺服器中不存在的帳號，因為這些帳號都不存在，便會引起大量的退信湧進被攻擊的帳號，不但增加郵件系統的負擔，也容易使該公司名列垃圾郵件的黑名單。



退信攻擊模式

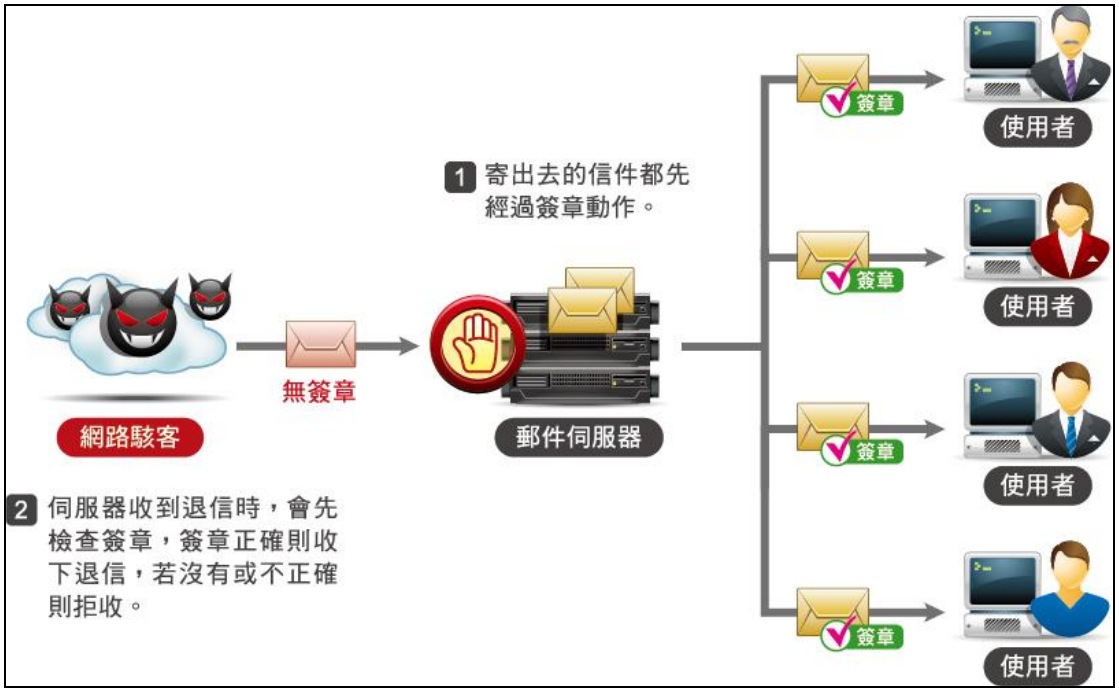
MaiGates - 防退信攻擊機制

MailGates 採用了退信地址驗證 （BATV, Bounce Address Tag Validation）的技術，在透過 SMTP 協定寄送郵件時就簽署簽章，所以系統收到退信時，就可透過簽章的驗證辨別此信件是一般正常的退信或是寄件人遭冒用的退信。

防退信攻擊功能設定

退信地址驗證（Bounce Address Tag Validation）機制運作流程如下圖所示。

1. 信件寄出給他人時，都會將該進行簽章的動作。
2. 系統收到退信時，就會先檢查信件是否有該簽章，若有則將該退信收下，若無則拒絕收取該信件。



退信驗證機制

由於電子郵件攻擊種類眾多，下期的電子郵件攻擊主題，我們還會針對 Dos/DDos、郵件炸彈攻擊及字典檔發送攻擊做更詳盡的解說，敬請期待。