新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2007/11/26- 2007/12/2 第52期

郵件伺服器 / ML 系列報導

技術淺談與應用 - 如何提升垃圾郵件判斷率？

近年來由於網路資訊科技成長迅速，使得資訊傳播的速度透過網際網路而不斷成長，其中發展最為迅速但也最讓人們厭惡的，莫過於垃圾郵件了。以往，企業廣告都是透過電視、雜誌、報紙...傳播媒體或透過傳真...這些高成本方式來散播。相較於傳統的廣告手法，垃圾郵件藉網際網路之便，散發成本相當低廉，因此，中小企業族群特別喜愛此方式來廣告公司產品，但帶來的卻是垃圾郵件氾濫。

為了因應此問題，市面上有許多資安廠商相繼在其產品中內建垃圾郵件過濾機制；由於 Spammer（垃圾蟲）總是出奇不意，為了其利益經常更變垃圾郵件的發送方式，使的這些機制常常無法反映實際上的需求。

為此，新軟系統針對旗下郵件伺服器產品（ML 系列）、多功能 UTM 產品（MS 系列）的郵件安全系統，不斷更新、增加過濾機制來因應多變的垃圾郵件。在這些過濾機制中，目前以「灰名單」、「指紋辨識」、「垃圾郵件特徵」這三項功能為主要的垃圾郵件過濾機制：

利用「灰名單（Greylist Filtering）」機制先行排除絕大部分的垃圾郵件

現在流竄在網路之間的垃圾郵件，大多都是藉電子郵件發送軟體來大肆寄發垃圾郵件。這種垃圾郵件發送方式有一個特點－為了能在短時間內寄發大量的垃圾郵件，這種軟體通常只管寄送而不檢查信件是否發送成功。而且為了躲避垃圾郵件過濾，這些信件在寄送時通常使用隨機產生的「偽造寄件者帳號」來寄發垃圾郵件。針對這樣的寄送行為模式，本公司特別研發「灰名單」機制來防堵。

其實「灰名單」機制的運作原理十分簡單，但也十分管用。只要是「新寄件者」寄來的信件，其第一次 SMTP 連線「灰名單」機制將無條件中斷之，並將此寄件者帳號加入「灰名單資料庫」。往後如收到相同郵件帳號寄來的郵件，「灰名單」機制將不會阻擋而交由其他垃圾郵件過濾機制處理。

透過此種方式，企業將會大量減少收到“使用郵件發送軟體”寄發的垃圾郵件。至於其他透過正常郵件伺服器所傳送的垃圾信件則不屬於「灰名單」機制的防禦範疇，可以透過「指紋辨識」來阻攔。

通過「灰名單」的信件交由「指紋辨識（Fingerprint）」過濾

每一封信件經過「指紋辨識」的公式計算，可以換算出一組特別的識別碼；這識別碼就如同人類的指紋般擁有獨一無二之特徵。將信件的識別碼與網路上的「指紋資料庫」比對，如符合則可確定此信件為垃圾郵件。

上述之方法就是「指紋辨識」過濾機制的運作模式。至於「指紋資料庫」則是透過網路上成千成萬使用者申訴建構而成－當某一封信件被絕大部分的使用者申訴為垃圾郵件時，「指紋資料庫」便會加入該信件的辨識碼。藉由此方式不斷地更新「指紋資料庫」，以提供強大且有效率的垃圾郵件過濾。

透過「指紋辨識」雖然可以過濾絕大部分之垃圾郵件，但是也有其鞭長莫及的地方，那就是“最新之垃圾郵件”。要知道，「指紋資料庫」是由使用者申訴所建構而成。因此，如果您是第一批收到這封垃圾郵件的收件者（尚未有人申訴此信件），「指紋辨識」當然無法辨識成功。

「垃圾郵件特徵（Spam Signature）」過濾新式垃圾郵件

那這些“最新的垃圾郵件”要怎麼處理呢？為了讓郵件安全系統的垃圾郵件過濾功能可處理各種新型垃圾郵件，新軟系統特地加入了獨家的「垃圾郵件特徵」來過濾垃圾郵件。

每當有新型垃圾郵件出現時，新軟系統便會分析其各種特徵，並以「垃圾郵件特徵碼」方式，供新軟系統的「郵件伺服器」、「多功能 UTM」更新。藉此方式協助企業防護各種新式垃圾郵件。

	灰名單過濾	指紋辨識過濾	垃圾郵件特徵
優點	有效阻攔透過“郵件發送軟體”發送的大量垃圾郵件	幾乎不會將正常信件誤判為垃圾信件	可過濾新式垃圾郵件
無法辨識的垃圾郵件	透過“正常郵件伺服器”寄送的垃圾郵件	最新的垃圾郵件	–

表一 灰名單、指紋辨識、垃圾郵件特徵過濾機制的差異性

以其他垃圾郵件過濾方式輔助提升垃圾郵件判斷率

使用上述之三種方法層層過濾，可以協助企業濾除絕大部分的垃圾郵件。但是要知道，垃圾郵件過濾並不能像病毒掃描一樣可直接比對病毒碼（只要符合病毒碼的檔案就可判斷為有毒），而是採用比較模糊的方式來判斷－倘若信件符合垃圾郵件的其中一個特徵時，那它只是比較有可能是垃圾信件；藉由多重垃圾郵件過濾的比對來確認該信件是否為垃圾郵件。也就是這個原因，沒有任何的垃圾郵件過濾機制可達到百分之百準確。因此，假如一封來自於客戶之信件恰巧「長」的與垃圾郵件特徵相似，那它就很有可能被郵件安全系統判斷為垃圾郵件。

如要避免上述情形之發生，管理人員可以利用新軟郵件安全系統內建的其他機制來讓垃圾郵件辨識系統更加的完美：

設定「黑／白名單」（Whitelist / Blacklist）

為了避免將客戶信件誤判為垃圾郵件，而導致錯失商機，企業可將經常往來客戶、廠商的 E-Mail 帳號加入「白名單」中。至於那些不請自來的「電子報」則可以將它加入「黑名單」中，藉此方式解決大部分客戶信件遭誤判的問題。

設定「全體化規則」（Global Rule）

「全體化規則」與「黑 / 白名單」類似，但可設定的條件更加廣闊。企業可利用「全體化規則」來制定複雜的垃圾郵件過濾規則。

透過「辨識學習（Training）」提升貝氏過濾（Bayesian Filtering）辨識率

貝氏過濾是一種可“成長”的垃圾郵件過濾機制。藉由「辨識學習」的方式，使用者可將先前判斷錯誤的電子郵件交由「貝氏過濾資料庫」學習。透過學習，可大幅提升「貝氏過濾」的辨識率。

	全體化規則	黑 / 白名單	貝氏過濾
適用對象	需要複雜條件的郵件過濾規則	企業往來客戶、廠商、電子報..皆可設定之	無法找出“規則”之信件
優點	透過複數條件的交叉比對，可相當靈活運用	設定簡單	可成長，辨識率越用越高
缺點	設定複雜，非一般人員可輕鬆運用	運用靈活度較低	需要花費較長時間辨識學習

表二 全體化規則、黑 / 白名單、貝氏過濾功能之差異

文 黃贊中 isaac@nusoft.com.tw

市場行銷報導 - 完整的 Backup 機制，協助企業建構完整的電子郵件系統

電子郵件在企業 e 化的影響下，近年內已經取代了其他傳統溝通模式，成為企業對外主要之溝通管道；絕大部分的企業往來溝通、文件...皆會透過電子郵件來傳遞。倘若電子郵件發生了問題，將導致企業商機嚴重損害，因此最近企業電子郵件安全之相關議題日漸被廣為討論。在這些議題中除了「垃圾、病毒郵件氾濫問題」外，就屬如何「維持電子郵件系統的穩定運作」與「歸檔保存企業往來之電子郵件」最受到企業重視。

「維持電子郵件系統的穩定運作」是電子郵件系統安全之首要工作。當電子郵件系統出現問題，企業豈不是無法收送信件？所有企業往來之溝通將為此受阻。「歸檔保存企業往來之電子郵件」則可詳細記錄企業長久以來的對外溝通訊息，往後如有發生糾紛亦可以此為證。因此不僅是企業想要保存信件，外國政府甚至是立法強制要求部份產業保存往來之電子郵件（保存五至七年），以便日後存查。

為了協助企業架構完善的電子郵件系統，新軟系統在其所推出的郵件伺服器（ML 系列產品）中加入了各種電子郵件相關機制（雙掃毒引擎、多重垃圾郵件過濾機制、Push Mail...）當然也包含個完整的 Backup 機制－“即時硬體備援系統”、“電子郵件歸檔保存（Mail Archive）”、“遠端備份電子郵件（Remote Backup）”，來協助企業「維持電子郵件系統的穩定運作」與「歸檔保存企業往來之電子郵件」。

即時硬體備援系統（Real Time HA）

硬體備援（HA，High Availability，高可用性）最主要的功能就是「以防萬一」之用，避免因設備硬體故障，導致相關工作頓時停擺。部份廠商將此功能導入其推出的郵件伺服器中，以確保電子郵件系統在突發狀況發生時仍能運作正常。可惜的是，硬體備援功能導入郵件伺服器的用意雖然是好，但是這些廠商往往忽略到“即時資料同步”的重要性。

在郵件伺服器之硬體備援功能中，所需要同步的資料包括「設定資料」、「使用者帳號 / 密碼」與「郵件」，其中以「郵件」資料最需要即時同步。可以想想看，在兩次資料同步之間隔期間，如郵件伺服器發生問題而必須切換至備份主機時，那些尚未資料同步的郵件會到哪裡去了呢？當然是從此消失了。假如這些信件中剛好有客戶的訂單，那後果不堪設想！因此，新軟系統特別推出了全新的硬體備援概念－「即時硬體備援」。

顧名思義，「即時硬體備援」就是隨時隨地同步雙方所有之資料；日常運行的郵件伺服器所收到之信件，備援主機一樣也會同時間收到，完全沒有時間差的問題。因此在郵件伺服器發生問題時，電子郵件系統仍能正常運作，企業也不用再擔心信件遺失問題。

	具有備援功能的郵件伺服器	新軟郵件伺服器
採用備援方式	一般硬體備援	即時硬體備援
每次資料同步間隔時間	1 小時 ～ 1 天	無間隔
優缺點	在資料同步間隔期間所收到的信件，如遇硬體備援切換時會遺失	不會有信件遺失之問題

表一 一般硬體備援 與 即時硬體備援 之差異

至於「歸檔保存企業往來之電子郵件」方面，新軟系統也提出了兩種功能供企業使用：

電子郵件歸檔保存（Mail Archive）

一般來說企業假如要保存往來之電子郵件，除了以手動方式備份外，就只有建構「郵件備份伺服器」方能達到備份郵件之目的。手動方式備份信件麻煩無比，雖然可以依使用者的需求僅備份需要之信件，但亦也有可能因人為之疏忽而導致有部份重要信件遺漏備份。「郵件備份伺服器」則簡單多了，一切都交由「郵件備份伺服器」自動處理，完全沒有手動備份的麻煩。但是，企業需要額外增加電子郵件系統的建構成本，而且絕大部分的「郵件備份伺服器」並沒有篩選機制，因此正常郵件、垃圾郵件、病毒郵件...全部備份，真正有用的信件少之又少。

新軟系統為了協助企業節省備份郵件之成本，在其推出的郵件伺服器中加入了「郵件歸檔」功能。「郵件歸檔」可自動將企業往來信件歸檔存查，完全不需使用者手動備份或是額外添購「郵件備份伺服器」。除此之外，「郵件歸檔」功能亦可依照管理人員所設定之條件規則選擇所需要的信件備份，讓企業能更靈活備份其電子郵件。

	手動郵件備份	一般郵件伺服器 + 郵件備份伺服器	新軟郵件伺服器
建構經費	無	高	低
建構方式	無	麻煩	無
備份方式	非常麻煩	簡單	簡單
所備份的信件	正常信件	正常信件 + 垃圾信件 + 病毒信件	正常信件
條件式備份	需人工自行判斷	有	有

表二 各種信件備份方法之差異

遠端備份電子郵件（Remote Backup）

先前有提到過，已有政府立法要求企業電子郵件需要備份個五至七年。但是，新軟郵件伺服器內建的硬碟只有 250G（NUS-M2500）啊！明顯不夠用怎麼辦呢？其實，新軟郵件伺服器還內建了「遠端備份」功能，可以把「郵件歸檔」的信件備份至遠端設備。與其它郵件備份伺服器不同的是，新軟郵件伺服器的「遠端備份」功能並非採用燒錄 CD / DVD 方式備份信件，而是使用備份至 NAS、File Server、擁有網路芳鄰的電腦...的方式。

使用這種方式遠端備份信件的好處可多了。除了備份空間大（今年初已有廠商推出 1 TB的硬碟）、全自動備份、使用磁碟陣列確保資料不損毀...外，在資料讀取查閱上也有著隨時隨地、方便、快速...的特性。

	光碟備份	NAS 備份
可用空間大小	DVD 4.7 GB	1 TB 硬碟今年已上市
自動 / 手動備份	手動	自動
信件保存期限	2~5年（光碟保存期限）	利用磁碟陣列不怕信件遺失
信件瀏覽 / 查閱	需有光碟方能查閱，且要每片光碟瀏覽才可找到資料	任何時間、地點

表三 光碟與 NAS 備份方法之差異

文 程智偉 rayearth@nusoft.com.tw