企業郵件安全策略，轉向多雲、混合雲智慧資安服務

文/網擎資訊 資安服務總監 張世鋒

企業對雲端的接受度越來越高，但將郵件管理完全轉成雲端代管來提供服務，對多數企業而言，仍是需要妥善評估的重點，但不論使用雲端郵件代管服務或自建郵件系統的企業，皆可透過雲端資安服務 (Security as Service) 來優化與升級郵件安全，相對資安自建系統 (On-Premise) 有哪些效益與優點？不妨我們從觀察現有企業郵件安全作法，進而了解雲端資安能協助企業解決哪些問題。

從資安趨勢，觀察郵件安全新需求

今年初國際研究暨顧問機構紛紛提出 2019 年的科技發展重點，包含 Gartner 科技策略趨勢(註 1)報告指出，對個人、企業組織和政府而言，將更重視數位倫理和隱私 (Digital ethics and privacy) 的問題。藉由規劃資安法規來保護機敏資訊，從臉書發生「劍橋分析竊取 8700 萬份用戶個資(註 2)」、「Gmail 讓第三方軟體開發商檢閱數百萬用戶的收信內容的事件(註 3)」以及歐盟推動 GDPR 的法規來觀察，對歐美企業而言首重法規遵循來有效控制內部威脅的發生，不論多大規模的企業，都必須優先符合資安相關法規。

[國際相關法規發展趨勢觀察]

[資料來源:行政院資安處(註 2)◎網擎資訊整理]

觀察日本 IPA 情報推進處理機構(註 4)所發佈的 2017-2018 日本信息安全 10 大威脅資料顯示，前三大威脅來自於「持續性威脅攻擊、勒索軟體損害、企業電子郵件詐騙」 等外部威脅，由於日本企業文化重視員工忠誠度與教育訓練，因此商務溝通行為相對公私分明，優先遵循公司的資安政策，因此內部威脅的風險

程度沒有外部威脅來的高。

而台灣企業文化相對多元,不僅有超過千人以上的跨國企業規模也有中大跟中小企業，但相對美日企業規模 (註 5) 仍有基礎建設與資安管理上的差異，從 iThome 的媒體資料調查 (註 6) 顯示企業資安事件的威脅來源,最多仍是來自來外部攻擊的資安威脅事件佔最多，而歸咎於內部員工造成的資安威脅，對企業而言也是一大隱憂，嚴重程度甚至超越釣魚郵件、惡意程式與勒索軟體。但調查資料也顯示台灣企業缺乏資安人才，雖然投資重點仍在資訊安全，但需求會以必要性支出的成本為優先考慮，需兼具安全與彈性政策的考量。

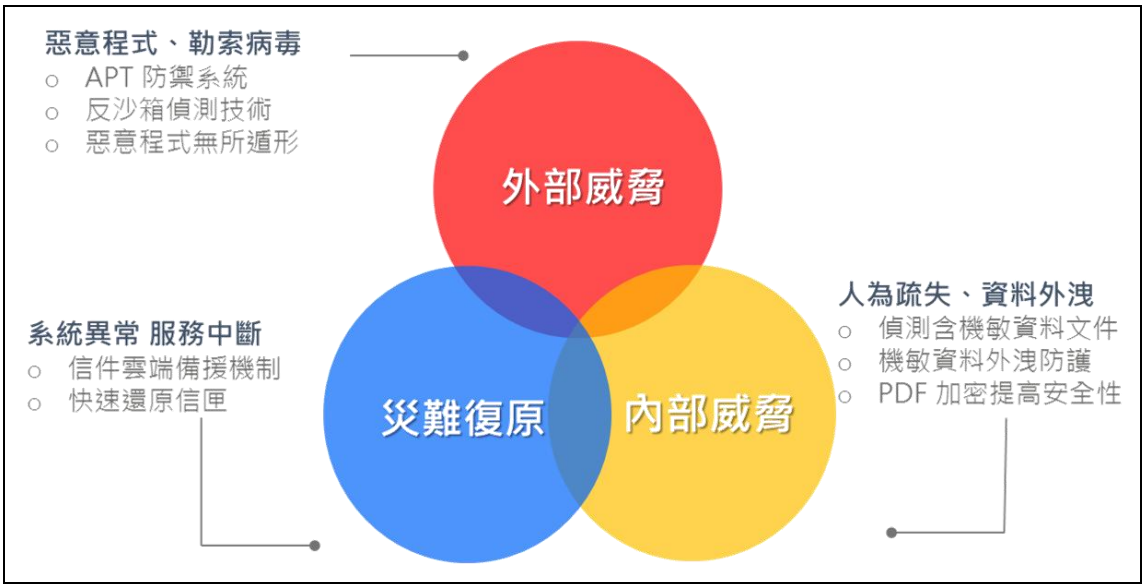
郵件安全面臨縱深防禦的新挑戰

郵件安全縱深防禦不外乎從外部威脅、內部威脅、災難復原三個面向，外部威脅而言，主要的議題來自新型態的垃圾信 (Spam) 與持續性的威脅攻擊 (APT)，過去透過病毒與垃圾信樣本更新可以阻擋絕大多數的垃圾信,但新型態的垃圾信不僅採用合法的發送機制與更新型的惡意病毒,例如偽造系統通知信讓一般防垃圾信閘道器 (Anti-Spam Gateway) 產生漏判。而更進一步則使用合法的寄件人與接近企業內部文化的用詞，將惡意連結或程式埋伏在附檔，避開防垃圾信系統的檢查，待使用者開啟檔案後才進行觸發，目的來騙取使用者帳密資料，進而偽冒使用者進行詐騙。

內部威脅主要來自人為疏忽，包含誤寄附檔造成機敏資料外流，例如某公司將求職者的個資,不小心夾帶在其他信件回覆或者未將重要的技術文件或營業機密以明文方式寄送，甚至寄到私人的免費信箱 ; 其次是系統錯誤或設計不當，例如某壽險公司辦理保戶通知信函寄發作業時,因系統管理中心修改電腦程式的覆核作業與公司所訂內部規範不符，導致電腦系統執行錯誤程式，使部分保戶保單資料不當郵寄予第三人。誤寄或未經檢查而寄出的資料產生的危害，對企業而言都是控制的風險

災難復原重點在服務不中斷（High Availability, HA）與資料備份還原 (Backup & Recovery) 機制建立。從以前不久發生的台積電病毒事件的案例，就包含了人為疏失、病毒攻擊，以及確保營運不中斷的問題。企業要落實災難復原的關鍵在於成本的投資，以成本規畫而言，基本為雙主機 (Active-Active/Active-Standby)運作，其次加入資料備份與長期儲存空間的估算，最後是異地機房的評估，成本也相對最高。

[郵件安全縱深防禦]



[整理@網擎資訊]

隨著威脅持續更新，企業自主建構資安縱深防禦將面臨以下挑戰

1. 新型態的攻擊威脅需敏捷回應
2. 落實事前預防減少災害成本擴大
3. 資安設備汰換與升級成本提高

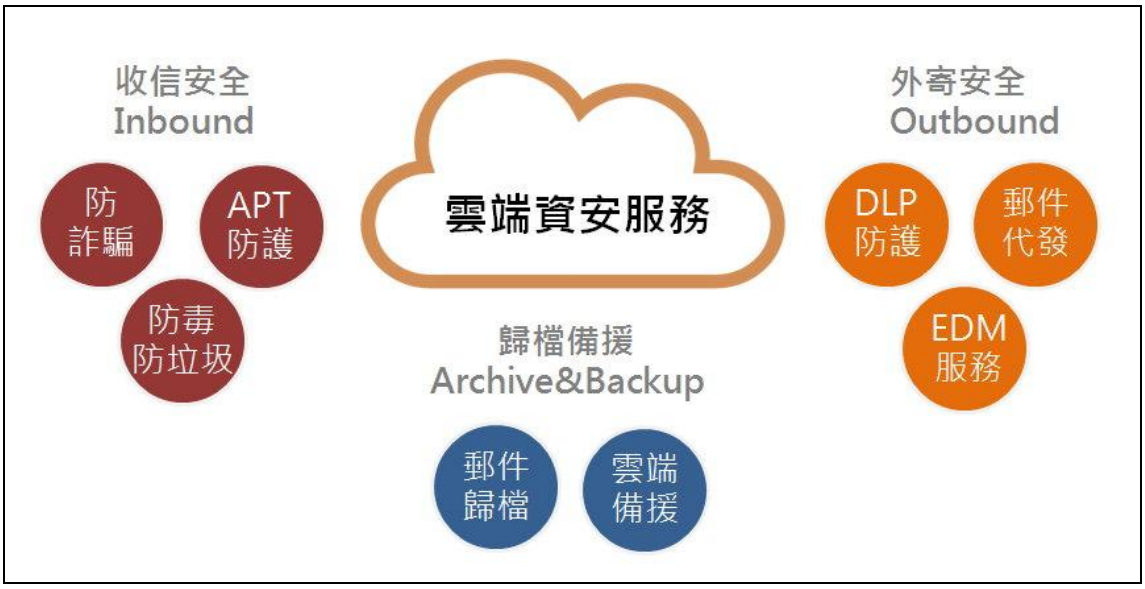
過去企業強化資安作法，以資安威脅角度出發評估企業需要的資安系統之後，開始進行專案導入，流程上要讓一套資安系統得以運作，企業要先採購必要的硬體、儲存設備並安裝系統軟體，其次整合網路跟郵件路由，最後設定優化校調設定監控。當有多資安需求時同時進行時，IT 人員就需要把不同品牌的資安系統，整合設定跟政策一致性，但不同資安領域有不同的知識基礎，經驗或技術到位的 IT 人員還能夠駕馭，反之就會是一件難度高的任務。

上述從風險分析、採購導入來解決資安需求的做法，難以在更短時間內針對不同威脅提供快速回應，加上企業資安維運，面臨設備老舊汰換問題，以及需要版本升級與模組採購取得新的資安功能，對企業而言皆是高成本的負擔。

資安結合 AI 在雲端，內外威脅敏捷回應

企業可以選擇最新結合人工智慧技術的雲端郵件安全服務來解決上述提到的問題，雲端郵件安全服務共有收信安全(Inbound Secure)、寄信安全(Outbound Secure)、備份歸檔(Acrhive&Backup) 等三個領域。

[雲端資安服務發展領域]



[整理@Openfnd]

收信安全(Inbound Secure) 領域，雲端整合多品牌核心提供最新的安全防護，從企業需要的郵件安全需求為前提，提供防毒(Anti-Virus)、防垃圾信(Anti-Spam)過濾、零時差行為分析(Zero-Hour)、內容安全(Content Filtering)、APT 防禦、防勒索詐騙服務等機制，結合人工智慧分析，應用在 Email 數據分析包含從寄件人來源、網址解析到內文語意解析，用在詐騙信件或惡意信件威脅程度分析，主動學習提高攔截率。雲端定期提供功能更新、一致性的整合設定與進階分析報表。管理者不用再擔心過去採購閘道式設備衍生的大版本升級、新功能模組加購授權問題。

寄信安全(Outbound Secure) 領域，雲端提供防資料外洩 (DLP) 功能，內建多種彈性稽核檢查功能，符合各種外寄情境，降低外洩的機率。相較於傳統政策設定，利用人工智慧主動解析郵件行為，例如分析往來名單主動加入合法收寄件人，或根據內文敏感程度，主動提供攔截規則的建議。提供外寄代管與大量外寄服務，協助企業用戶解決外寄障礙提高郵件送達率。

歸檔備援(Archive&Backup) 領域，雲端歸檔方案提供去重複與壓縮的功能，妥善平衡企業自行歸檔的儲存成本，並可納入企業郵件生命週期管理的方案選擇，

結合人工智慧與大數據分析，主動提供歷史郵件的分析報告；雲端備援結合主動偵測可協助企業郵件服務異常時，即時提供收信與發信的服務，維持服務不中斷，讓企業落實高可用性。

無需更換郵件品牌，雲端快速提昇資安等級

企業導入雲端資安服務，不限於使用何種郵件品牌，從自建郵件系統 (On-Premise) 到雲端信箱服務 (SaaS)，皆可搭配雲端資安服務強化郵件安全。

自建郵件系統的企業用戶，例如 Microsoft Exchange 或其他符合標準 SMTP 通訊協定的郵件主機，可透過雲加端的混合雲模式使用資安服務，用戶將 DNS-MX 設定指向雲端後，由雲端協助過濾所有外部信件後，再轉送回本地的郵件主機，不影響本地郵件主機與使用者收發設定，而且所有外部信件衍生的連線與頻寬成本都由雲端統一處理。外部信件可由本地端主機導向雲端提供防機敏資料外洩檢查與加密寄送服務。

使用雲端信箱的企業用戶，例如 Office365、Gmail、MailCloud 或其他品牌雲端信箱服務，皆能透過雲對雲的整合模式使用資安服務。雲端資安服務針對不同雲端品牌提供完整的郵件安全、稽核與歸檔備援服務。

隨選即用是雲端服務的優點，對用戶而言只要選擇需要的服務，僅需處理政策設定問題。不用管理多系統安裝佈署、版本更新、設備老舊汰換跟網路品質的定期檢整，同時雲端提供 7*24 小時維運服務，企業資訊人力也能夠專注於資安政策規劃，減少維運成本的浪費。

建議企業用戶重新檢視現有的防垃圾信 (Anti-Spam Gateway) 過濾設備功能是否完整，選擇加購雲端防詐騙勒索服務或置換雲端郵件過濾服務，尤其是新型態的垃圾信或詐騙信件層出不窮，單靠單台防垃圾閘道器或資安設備，已不足以應付持續增加的資安威脅。面對郵件安全，皆可評估將資安交給值得信任的專業雲端資安服務來處理，透過雲端服務的安全性、即時性與功能更新的特性，持續強化縱深防禦，優化企業資安防護能力。

本文章參考資料

註 1. Gartner(2019) Top 10 Strategic Technology Trends for 2019。網址:https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/。

註 2.行政院(2017)資通安全管理法與發展藍圖。網址:

https://s.itho.me/egov/2017/A-1320.pdf。國際趨勢觀察 P.11。

註 3.風傳媒(2018) 劍橋分析」恐竊取 8700 萬份用戶個資！臉書坦承管理漏洞，加強保護個資、阻擋第三方程式。網址:https://www.storm.mg/article/420842。

註 4.東森新聞(2018) Gmail 有後門漏洞？第三方廠商可看光你的信件。網址:https://fnc.ebc.net.tw/FncNews/Content/43423。

註 5. IPA(2018)情報處理推進機構 2018 十大資安威脅。網址:https://www.ipa.go.jp/security/vuln/10threats2018.html

註 6.台灣綜合研究院(2019)各國中小企業定義。網址:http://www.tri.org.tw/ceo/ 。

註 7. iThome(2018)台灣企業資安數據調查。網址:https://www.ithome.com.tw/article/122185