

企業首選！給您最安心的雲端智慧辦公室解決方案



（ 群環科技 雲端事業部產品經理 邱怡蓁 ）

群環科技於去（2018）年成立 Best Cloud 品牌與平台，目前有 10 位雲端服務顧問與 12 位專業技術人員共同為企業提供全方位雲端服務，包含智慧辦公室的 Office 365、MailCloud；資安的 Microsoft 365、OSecure；備份的 Azure Backup、Veritas、Barracuda，IaaS/PaaS 等雲端基礎建設方面則有 Microsoft Azure、IBM Cloud 以及騰訊雲，並且也提供遷移、維運等技術服務。



在多项雲端服務中企業最頻繁與普遍運用為 Office 365，Office 365 包含原有微軟 Office 功能，如 Word、Excel，以及由 Outlook、Exchange Online 構成的商務級電子郵件，也包含 OneDrive 雲端儲存與檔案共享、線上會議的 Teams、小組協同工作的 SharePoint 等。

而諸多線上服務中最需要關注的是電子郵件，群環科技雲端事業部產品經理邱怡蓁以近期受高度關注的電視劇《我們與惡的距離》為例，該劇引發眾人討論與省思「事物的一體兩面」，而電子郵件同樣有一體兩面，郵件收發既是企業運作最便利的工具，對駭客而言也是傳送惡意軟體的便利工具，根據調查「91%的駭客攻擊利用電子郵件作為切入點」。言下之意企業一方面享受便利，另一方面也必須重視自郵件管道進入的資安威脅。

在郵件威脅中有兩種較常見的手法，一是釣魚郵件，郵件假裝成知名網站要求你上網更新帳號密碼，借此取得你的帳密。另一是商務電子郵件詐騙（BEC），駭客鎖定一潛在攻擊對象而後側面分析其相關資訊，而後偽造出高度逼真的高層信件要求收件者匯款。

面對不斷翻新的郵件威脅企業不能只有一層郵件防範機制，且根據一份對 295 名資訊技術專業人員的調查，85% 受訪者表示惡意信件可以繞過郵件安全機制順利進去個員的收件匣。

對於郵件威脅邱怡蓁也舉實例，有人假冒廣達電腦對 Facebook、Google 發出請款信件，信中聲稱尚有積欠款項未支付並要求匯款，如此騙得 37 億台幣。另外一家位於台中的肉品貿易公司亦因駭客假冒供應商要求更改匯款帳號而被詐騙 540 萬台幣。

類似案例層出不窮，我國於 2015 年至 2018 年間有近 200 家企業被詐騙近 2 億元，且持續增加中。

釣魚與詐騙郵件屢屢得逞除了收件者輕忽外企業主抱持僥倖心態亦為因素，Office 365 內建的郵件防護仍有不足。國外報告顯示 Office 365 內建的郵件防護功能僅能攔截 75% 垃圾郵件，以及 2018 年國際防護軟體商在 Office 365 內建防護基礎上進行深度偵測，共偵測出 890 萬次高風險威脅，其中包含約 10 萬 BEC 詐騙嘗試、100 萬次惡意程式，以及 770 萬次釣魚嘗試，此均顯示內建基礎防護的薄弱性。

對於如何加強郵件安全邱怡蓁首先建議啟動多因素驗證機制，其二為運用 MailGates 增加防護層、提升威脅攔截率並減少惡意郵件誤判率。



MailGates 也具備 BEC 防護功能，透過語意偵測、行為分析、自定政策等判斷郵件而後決議退信或留置。另也提供 APT 沙箱防護的進階方案，於沙箱環境中執行可疑檔案與連結並觀察其行為以研判是否帶有惡意。最後期望企業均能享有郵件原有的便利並避開風險威脅。