金融機構DLP導入案例 預防資料外洩風險

撰文 | 叡揚資訊 資安事業處產品顧問　馬業強

一分鐘看問題

導入單位

國內某金融機構

導入範圍

網路端資料外洩防護（Data Loss Prevention；DLP）

評估重點

避免影響使用者作業及管控需求

導入產品

GTB DLP 資料外洩防護系統 - 網路端模組 Inspector

產生效益

- 落實金融機構個資法規範，建置系統保護機敏性資料，例：存款帳號、姓名、身分證字號等個資。
- 簡單易管理且自動化的個資防護系統，節省日常管理時間。
- 補強防火牆未能保護及防禦未知網站，達成互補作用。

為因應金融監督管理委員會對金融機構建議加強個資外洩保護，任何個資可能外洩的管道，都應進行合法的管控，因此該金融機構經過評估及效能考量導入資訊安全工具GTB DLP資料外洩防護系統，期望透過DLP達到資料外洩防護功能，同時保護企業員工上網行為，並且對企業防火牆未能自動或手動完整防禦之惡意網站及行為（如：於疑似惡意網站及不安全網站上傳資料），進行個資防護，透過GTB DLP協助解決困窘數年的資訊安全問題。

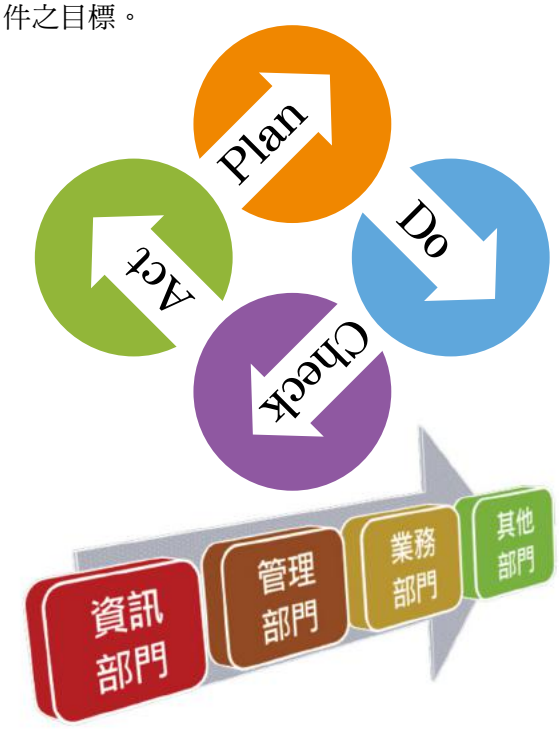
網路端DLP架設考量

建置資料外洩防護系統必須掃描網路端口上的所有協議，含HTTP、HTTPS、FTP及所有未知連接埠，並解析HTTPS加密連線封包及進行內容過濾分析，在評估期間閘道端設備擺放的位置，需持續討論及相對應的調整作業，該金融機構在初步評估後將閘道器放置網路出口端即可滿足個資防護要求。

在系統上線前進行功能再次確認及驗證機制，該金融機構在資訊部門的測試階段就高達數月之久，也證明金融業對資訊安全重視的程度，為避免影響使用者作業及管控需求，在資訊部門測試完成後，再將特定重要部門加入驗證工作，以確保系統能正常營運上線且不影響日常作業。

DLP導入的重點：採PDCA方式並與企業政策搭配

系統建置完成後，專案多數時間在進行政策制定標準、規劃、討論，其中政策制定需事先區分公務與非公務用途之網站，也同時要避免改變使用者行為或影響正常的公務作業。對於已討論完成且定案之政策，該金融機構採用PDCA原則分階段佈署至全行，也定期檢討政策並預計達成減少因惡意網站導致個資外洩事件之目標。

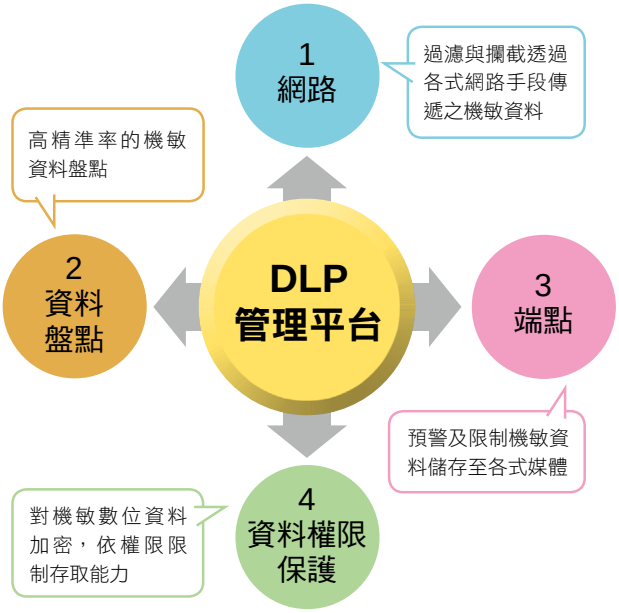


↑導入 DLP 將首先落實資訊部門，再依序推動到管理部門、業務部門和其他相關單位。

本專案DLP防護項目

- 傳送銀行帳號、授信帳號等超過特定筆數，將禁止傳送。
- 傳送身分證字號、公文資料、中文姓名、個資等超過特定筆數，將禁止傳送。
- 禁止傳送加密檔，如：RAR、ZIP、Office等資料格式。
- 禁止傳送資料格式為圖片等文件。

常見的資料外洩防護模組



↑ GTB 獨特高精準度「資料指紋」辨識技術，屬於內容感知型（Content-aware DLP），可有效降低誤判，提升各模組防護效益。

叡揚持續累積DLP 導入經驗 協助客戶鞏固資訊安全

叡揚自1987年成立以來，從系統軟體工具服務開始，長期協助國內金融業、電信醫療相關企業之Data Center提升效能及管理自動化近30年；多年前投入資訊安全領域，除整合自有軟體開發能量於軟體安全外，近年持續累積資料安全-資料外洩防護DLP解決方案建置經驗，協助客戶鞏固資訊安全。

Tips

GTB Technologies
Next Generation DLP

關於GTB Technologies

GTB Technologies為新世代資料外洩防禦DLP公司。GTB DLP結合精確性與執行速度，可防止發生在企業網路或端點，非法且令人困窘的敏感資料外洩。

更多客戶案例、資安資源 http://www.gss.com.tw/index.php/focus/security