ISACA 的四項 DLP 最佳實務

資料來源: 國際電腦稽核協會(ISACA)

翻譯整理: 叡揚資訊 資訊安全事業處

國際電腦稽核協會(ISACA)是一個具有 95,000 位IT專業人員的非營利性組織，最近發表了防資料外洩(DLP, Data Leak or Loss Prevention)最佳實務白皮書。

這份白皮書指出對於精通各式技巧的資料竊賊而言，DLP的發展仍未臻完善。實施DLP解決方案是一項複雜的工作事項，根據企業所使用的資產清冊上及資料型態作分析，需要長遠的籌劃活動包含政策制定、業務流程分析。藉由ISACA白皮書中，我們來看看實作DLP重要的最佳實務作法。

綱領 1：資料分級是實施DLP的基礎

企業通常不知道他們所處理資料的類型和存放位置，所以在採購DLP解決方案前，識別資料、機密分級、系統間及系統到人員間的資料流向就顯得很重要。瞭解企業資料生命週期（從搜集、處理、利用、儲存和銷毀），有助於揭示資料存放及傳遞路徑。

分級可包含客戶、員工、財務報表和智慧財產等類別，有良好的分級和主要儲存位置有益於DLP解決方案的評選和功能定位。

應收集資料流出口的相關資訊，因為並非所有業務流程有被文件化，也並非所有的資料流是排程後的結果，這些情況可由防火牆和路由器規則(日誌)得知。

綱領 2：建立政策為首要工作

一旦資料被定義和分級，政策應隨之建立或修訂，讓每個類別資料明確的依分級規範適當處理。在政策初始發展的階段，業務和技術人員就應該參與，並應採取以風險為基礎的方法。DLP實施計劃應包含有指標性(如：個資法明定的項目)的資料類型、違反政策、事件升級及例外情況的完整處理流程。每一項類型規則都確保具有適當的事件管理流程且實際運作，這一點也很重要。

綱領 3：DLP的實施

企業應審慎考慮實施DLP初期僅以監測模式即可，如此足以調校並推估對業務流程及企業文化的影響。一旦系

GSS Galaxy Software Services 叡揚資訊
台北總公司：10461 台北市中山區德惠街 9 號 5 樓 TEL：(02)2586-7890 FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3 TEL：(07)586-6195
海外據點：上海、北京、東京 www.gss.com.tw

統啟動(阻擋功能)時，管理階層會關切脫離管理的資料量、阻擋過當可能造成更嚴重的問題、或是阻礙核心業務的進行。DLP解決方案通常能提供許多有關資料盤點及傳輸路徑的有用資訊，但企業也因獲知龐大的機密資料軌跡和流失程度瞬間感到驚慌，因此可能導致躁進，試圖畢其功於一役，這會是另一個災難。

實施DLP的過程當中，規則是持續檢討改善的，企業應確保所有的資料保管人能忠於職守的回報DLP未能阻擋的檔案型式或傳遞方式。

綱領 4：瞭解DLP技術的侷限

DLP解決方案可以協助企業獲得機密資料的使用情況，但也應該要瞭解系統即有的限制（在實施之前）。例如，DLP解決方案只能支援事先解密的加密內容，如果使用者使用的加密金鑰未受DLP管理，這些檔案必然無法被DLP分析，另一個值得注意的地方是DLP解決方案目前也無法很有智慧的詮釋圖形檔。此外，現在手持裝置廣泛的使用，DLP解決方案尚無法輕易的監測和控制這些通訊管道。

GSS Galaxy Software Services 叡揚資訊
台北總公司：10461 台北市中山區德惠街 9 號 5 樓　TEL：(02)2586-7890　FAX：(02)2586-8787
高雄辦公室：80453 高雄市明華路 315 號 13 樓之 3　TEL：(07)586-6195
海外據點：上海、北京、東京　www.gss.com.tw