避免特權濫用！

利用 CA 特權管理提升安全保護、稽核輕鬆過關

文章來源 | CA Technologies　　文章整理 | 叡揚資訊 資安事業處

近年來，IT 系統受攻擊與資料遭盜用的頻率與衝擊程度可說是日漸加劇，但令人驚訝的是，大多數的攻擊是來自內部人員。產業統計數據顯示，在企業內部具有管理員或特權存取權的 IT 破壞者，為多數資訊安全漏洞的元兇。美國企業平均每年因資安漏洞而付出的代價就高達 5,400 萬美金（(Ponemon Institute.2013 年「資料外洩代價的研究」(Cost of Data Breach Study)）。

如何找出易遭濫用特權的狀況

企業易遭特權濫用的常見徵兆包括以下 4 點：

① **孤立帳戶：**已離開公司的有效使用者帳戶，常被心懷不軌的管理員拿來再利用

② **權限爬升：**使用者升職後獲得更多權限，導致使用者擁有的權限超過實際所需

③ **稽核包袱：**驗證使用者權限的過程為人工進行，使得存取權限無法全程受到嚴密監控

④ **能見度不足：**不只造成難以判斷使用者擁有的存取權類型，也造成無法知道使用該存取權的時間、地點和方式

為何需要CA特權管理（Privileged Identity Governance）？

身份與存取管理功能是CA特權管理（Privileged Identity Governance）的首要元件，提供強大的身份分析資料與彈性的工作流程，能夠協助企業：

- 利用分析資料評估、稽核和清理過度存取權
- 自動驗證使用者、角色和資源的授權，並修正授權
- 建立集中管理的權責區分原則
- 透過全方位儀表板與報告監控存取權

特權身份管理功能是CA特權管理的次要元件，利用自動化特權控制功能，讓企業實施在管理階段所開發的原則，能夠協助企業：

- 利用細微調整的存取控制，保護共享帳戶的密碼，並採用最低特權存取權
    - 依存取模式和組織特性，發現並建議可能的角色
        - 探索背後的企業架構，將成千上萬個存取權變成上百個角色
        - 隨著企業的發展調整模型

最後，是 CA特權管理解決方案的使用者活動報告元件，可提升使用者活動對企業來說的能見度 （例如：誰使用哪些資源、時間、地點和方式等），其範例報告包括以下 5 點：

① **原則管理：**檢視原則部署的狀態及與標準原則的差異

② **授權：**檢視使用者與群組在系統資源上授權（例如：查看誰對系統具有root 存取權）

③ **使用者管理：**檢視不常用的帳戶、使用者、群組成員資格和管理帳戶，並管理 SoD

④ **密碼管理：**檢視密碼已存留時間和密碼原則合規等資訊

⑤ **特權使用者存取：**檢視所有特權使用者的活動，包括登入、登出、工作流程核准和其他動作

↑ CA Privileged Identity Manager 除了能在作業系統層級限制存取，還能限制對個別應用程式的存取。

關於 CA Technologies 提供的解決方案

CA Technologies 的特權管理（Privileged Identity Governance）解決方案，係結合了CA Privileged Identity Manager和CA Identity Management & Governance等兩大領導業界之身份管理產品而來。

CA Identity Management & Governance可將身份與存取管理程序自動化，提供不間斷的身份控制，以友善的企業使用者角色為基礎，向使用者呈現對其有意義的資訊。此外，進行諸如授權認證之類的程序時，也會檢查安全性原則，並向企業經理人點出潛在的存取違規或授權違規。

CA Privileged Identity Manager是一項可擴充的解決方案，功能包括：從中央管理主控台，跨伺服器、應用程式與裝置進行特權使用者密碼管理、細微調整存取控制、使用者活動報告和UNIX 驗證。