內部管理的盲點 – 特權帳號】

資料來源：CyberArk　資料整理：叡揚資訊資訊安全事業處

挑戰

特權帳號可存取企業重要系統和敏感的商業資訊，所以特權帳號的不當使用可能會對企業生計造成致命衝擊。為了保護企業的核心利益，企業組織應該對特權帳號的活動採取「零信賴」方針。

「零信賴」方針包括企業組織的主動監控和側錄所有特權帳號連線 (privileged session) 活動，以避免不懷好意的內部人員、缺乏經驗的第三方使用者或外部網路駭客損壞企業重要系統，或存取未經授權的敏感資訊。企業組織也應隔離特權帳號連線，以避免惡意軟體 (malware) 從脆弱的使用者端擴散到企業重要系統之中。若缺乏主動管理特權帳號連線的妥善方法 (包含密碼和 SSH 金鑰啟用程序和管理)，企業組織恐陸續面連一連串無可勝數的風險。

放任特權連線的相關風險包括

重要系統的故意及意外損壞

企業組織會讓企業內部人員和第三方使用者，透過特權存取以執行日常工作、維護和管理 IT 基礎架構。為了避免這些使用者意外或故意不當使用特權帳號，資安團隊必須監控所有特權帳號連線的活動，確保授權使用者僅執行授權的活動。企業組織也應考慮使用特權帳號單次登入的功能，以確保安全憑證或密碼不會外流到終端使用者或其終端裝置中，進而避免憑證或密碼遭到中途攔截，導致企業重要目標系統出現未授權和未監控的存取

惡意軟體滲入重要系統

惡意軟體可輕易透過網路連結攻擊脆弱的終端使用者裝置。為了避免惡意軟體滲透到企業的重要系統中，企業組織應當機立斷隔離特權帳號連線，將脆弱的終端使用者裝置與高價值的企業重要目標系統完整的分離。

管理費用高昂，徒增資料外洩風險

若無法提供方便的搜尋、鎖定以及檢視可疑的特權帳號活動之方法，電腦鑑識分析就會變得非常窒礙難行而且曠日費時。當資安小組傾全力忙於整理紀錄的同時，網路駭客正好整以暇的提升攻擊技術。緩慢冗長的手動操作程序，不僅導致高額的管理費用支出，而且還可能助長資料外洩風險。

失敗的法規稽核和鉅額罰款

許多法規都闡明，企業組織必須針對儲存有敏感與受法規保障資料 (regulated data) 的系統，進行系統存取的追蹤與監控。不合宜的存取監控恐導致企業無法通過稽核，因此遭受刑罰以及鉅額罰款。

管理效益：隔離、監管並控制特權帳號連線，以減少資 安威脅面、快速偵測並回應可疑的網路活動，以及展現法規遵循的能力。

解決方案

CyberArk 的特權帳號連線管理 (PSM，Privileged Session Manager) 專門用來作為企業重要系統的中央存取管控點，由此隔離、監管並控制特權帳號連線的所有活動。 解決方案以維護資安為一切重心，其規模足以符合大型企業的需求，同時仍保有個別使用者的方便性。

功能與效益

CyberArk PSM 可以讓企業達成以下目標：

隔離企業重要系統

CyberArk PSM 可讓企業組織即時監管所有的特權帳號連線活動，讓資安團隊能迅速偵測特權帳號的不正常使用。此解決方案會持續監控側錄的所有的鍵盤輸入及指令，並建立詳細稽核紀錄與影像資料，資安與稽核小組可藉此進行事後檢討與查驗。CyberArk PSM 與許多平台系統整合，包括 Windows 作業系統、Unix/Linux 作業系統、資料庫、大型主機系統、網路裝置、虛擬架構系統等等，所以企業組織可以在整個網路中，監控與側錄目標系統的特權帳號連線狀況。

迅速對應資安威脅

工作階段的稽核紀錄與影像資料，會被安全保存在防竄改的數位金庫內，防止惡意使用者竄改其活動紀錄。在調查與稽核階段，調查人員可以輕鬆搜尋這些紀錄與綠影，確定可擬狀況的起始時間、被使用過的帳號，以及惡意使用者的後續

動作。當系統即時偵測到可疑的工作階段與活動，資安團隊可以遠端鎖定並終止該工作階段，防止潛在攻擊發生。

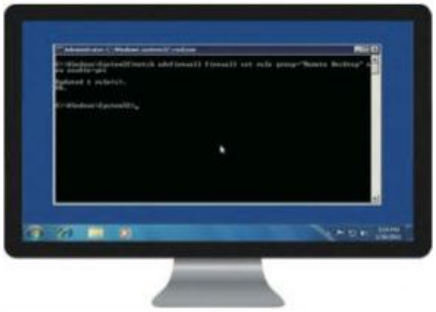
控管第三方的特權帳號使用情形

諸如協力供應商、顧問和稽核人員等第三方使用者，通常都不會直接建立與企業組織的資安信任關係，而且他們多半透過未受管理的終端系統，存取企業的重要系統，因而提高資安風險。為了降低這類風險，CyberArk PSM 隔離第三方工作階段的功能，讓特權帳號可以單次登入，並且監管與側錄所有第三方工作者階段的活動，快速找出未經核准且可能造成破壞的活動。而且不須向使用者或是其中端裝置暴露目標系統的安全憑證。

防止直接存取重要系統

CyberArk PSM 可以設定只有存取端點才可以進入重要系統，使用者必須先在 CyberArk PSM 系統完成身分任，才能直接連到目標系統。因為控與側錄的動作是在代理服務 (Proxy) 上進行，而不是直接在目標系統上執行運作，即使技藝超群的專業使用者，也無法在自己的終端系統上直停止這些監控功能。此外，節由整合 CyberArk 的企業密碼金庫，或是 CyberArk SSH 金鑰管理員等系統，企業就可以提供特權存取的功能，而且不需向使用者或是其終端裝置暴露目標系統的安全憑證。

具備安全的特權存取能力，同時兼顧使用者經驗



只要完成 CyberArk 解決方案的身分認證，使用者就可以直接迅速的存取目標系統，CyberArk 也保留了 Unix/Linux 的使用者經驗，讓使用者直接透過 CyberArk 針對目標系統下達 Unix/Linux 內建指令。額外的 Active Directory(AD) 橋接功能。可以透過 CyberArk 平台開啟 AD 身分認證功能，同時保存 Unix 使用者帳號的權限。

展現法規遵循能力

CyberArk PSM 協助企業組織達成業界法規要求，能夠強制主動監控系統，並且側錄特權帳號連線的公活動功能。只接受唯讀存取的稽核紀錄與影像資料，可以提供給稽核員，作為企業遵循相關法規的稽核資料與證明。

全面的特權帳號安全性解決方案

透過隔離、監控和控制特權帳號連線的所有活動，企業可以降低資安攻擊面，快速偵測與處理有問題的特權帳號，同時證明企業符合業界規範。CyberArk PSM 緊密結合 CyberArk 特權帳號安全性解決方案，讓企業組織得以在共同的網路基礎架構下，透過單一管理介面，對特權帳號的憑證 (包含密碼與 SSH 金鑰) 採取安全的防護措施，並且偵測其異常使用狀況。

更多最新資安電子報：請瀏覽 http://www.gss.com.tw/index.php/focus/security