tenable Cloud Security

在 AWS 中落實最低特權

最低特權是雲端安全關鍵的一大步

在針對美國 300 位資安長進行的問卷調查當中，70% 以上的受訪者都指出最低特權是他們面臨的最嚴峻難題。

保障雲端身分和資料的安全極為困難，而且多數企業都搞不清楚狀況。而近期發生的資安事端顯示，與身分和憑證相關的風險不容輕忽。長期下來問題會變得越來越嚴重，因為企業在擴展雲端足跡的同時並沒有奠定能有效指派及管理權限的功能。因此，使用者和應用程式普遍都會累積遠超過技術及業務所需的權限，形成一個巨大的權限落差。

授權管理鬆懈可能會帶來毀滅性的後果。攻擊者可伺機使用權限過高的外洩憑證進行一些偷雞摸狗的勾當，像是在您的執行個體上竊取時間和 CPU 等資源來挖比特幣。但過高的特權也可能會讓威脅執行者得以竊取機密資料或刪除部分基礎架構。

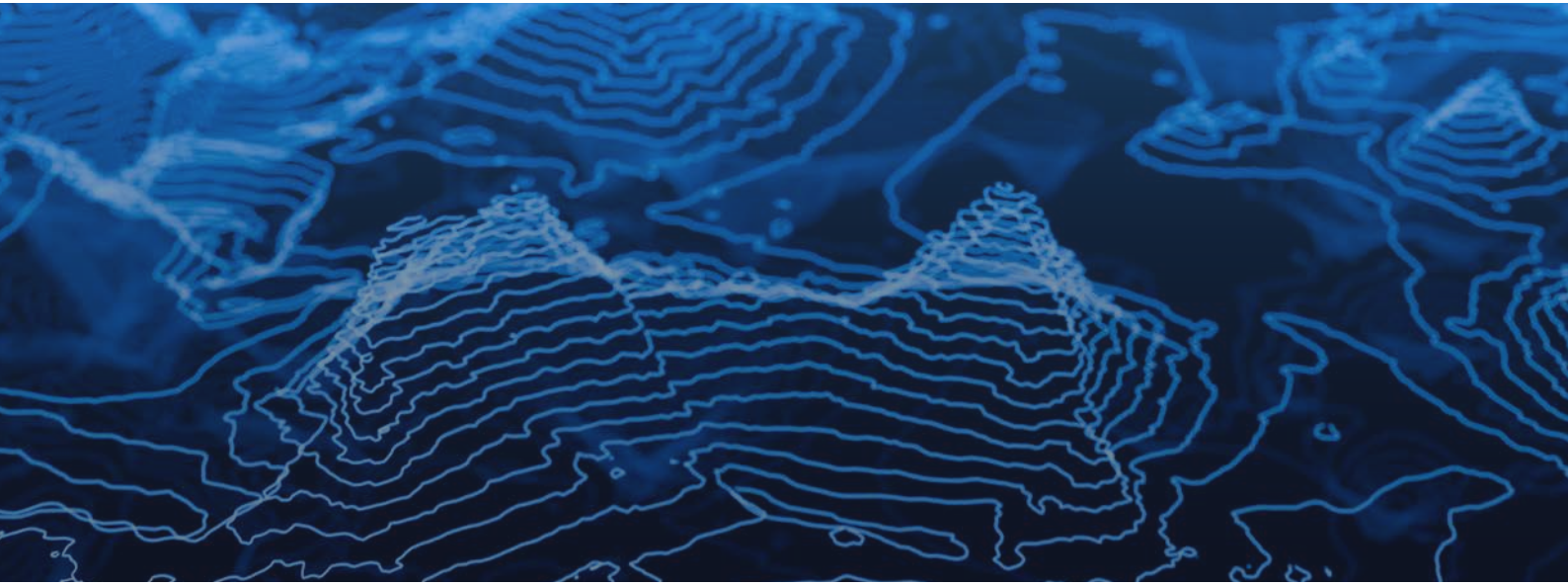
CAPITAL ONE 資料外洩：為採行雲端的企業敲響警鐘

近期討論最熱烈且震驚社會大眾的資料外洩案件之一，就是這起 1.06 億筆信用卡申請資料外洩的案件。

Capital One 資料外洩是因存取權限過高而引發風險的最佳例證。在我們繼續探討此事前，我們必須強調，我們極為推崇這家銀行。Capital One 是銀行業的開路先鋒，它率先採用了雲端運算，它的沿革史發生在大多數勇於試用新型技術的拓荒者們身上。

簡而言之，部分問題根源出在一款容易受弱點影響的開放原始碼 Web 應用程式防火牆 (WAF)，Capital One 在營運時使用此防火牆且交由其雲端安全服務供應商 (CSP)(Amazon Web Services (AWS)) 代為管理。這個弱點讓攻擊者得以取得憑證，入侵 WAF 可存取之帳戶中的所有資源。

確實，AWS 的所有存取權都是透過一套憑證授予，而存取權全然取決於指定給實體的權限。以 Capital One 的案件為例，容易受弱點影響的 WAF 獲得的權限過高。更明確地說，它可以列出機密資料儲存貯體中的所有檔案並讀取所有檔案的內容。這些過高的權限可讓攻擊者入侵機密的 S3 儲存貯體。



落實最低特權的方式：理論與實踐

為了降低雲端遭到濫用的身分所引起的風險，企業都在設法強力執行最低特權原則。在理想情況下，每位使用者或每個應用程式的權限都應該侷限在確切的必要範圍內。

舉 AWS 為例，由於它是最廣為使用的雲端平台，而且也是當今最精細、最複雜的一款身分和存取管理 (IAM) 系統。AWS IAM 是一種功能強大的工具，可讓您安全地設定 AWS 雲端資源的存取權。IAM 具備 2,500 多個權限 (還在不斷增加)，可讓使用者精細地掌控可對某個 AWS 資源執行哪些動作。

理論上，要達到最低特權的第一步是定出能反映必要存取防護措施的原則。然後，您必須知道某個使用者或應用程式具備哪些權限，然後再與所有實際使用的權限進行對應。兩相對照之下，就可以看出落差在何處，還可以讓您決定哪些權限要保留，而哪些應該撤除。最終，那些過高的權限都會被移除或受到監控。

然而，在像 AWS IAM 這麼複雜的環境下，如果要確定每個應用程式確切所需的必要權限，需要的成本非常高昂，而且無法擴充規模。即使是像得知某位使用者被授予什麼權限這麼單純的任務，可能都非常困難。

可自動監控及減輕雲端身分風險並強制執行最低特權原則的解決方案已經問世。每個雲端安全利害關係人都應該將這樣的解決方案納入他們的策略和立即性的行動計畫當中。

關於 Tenable Cloud Security

Tenable Cloud Security 會找出雲端基礎架構的安全缺口、排定其優先順序並加以修復。它可以統一管理並自動盤點資產、深度分析風險、偵測執行階段威脅和合規性，讓利害關係人能充分發揮精準的視覺呈現、引導式修復建議與協同合作等功效。Tenable Cloud Security 是全方位的雲端原生應用程式保護平台 (CNAPP)，兼備雲端安全態勢管理 (CSPM)、雲端基礎架構與權限管理 (CIEM)、雲端工作負載保護 (CWPP)、Kubernetes 安全態勢管理 (KSPM) 以及基礎架構即程式碼 (IaC) 等安全工具。

關於 Tenable

Tenable® 是一家曝險管理公司。全球大約有 43,000 多家企業透過 Tenable 來瞭解並降低網路風險。身為 Nessus® 的創造者，Tenable 拓展了本身在弱點方面的專業知識，以提供全球第一個可在任何運算平台上查看和維護任何數位資產安全的平台。 在 Tenable 的客戶中，包含大約 60% 的財星 500 大企業、大約 40% 的全球 2,000 大企業以及大型政府機構。

如需深入瞭解，請前往 zh-tw.tenable.com

圖 1：
穩定的雲端身分監管解決方案有助於控制存取風險並主動強制執行最低特權原則

請與我們聯絡：

請傳送電子郵件至 sales@tenable.com 或前往 zh-tw.tenable.com/contact