優先保護特權的五大原因

引言

特權存取是取得企業最寶貴資產的門戶，而且在幾乎所有重大資安事件中都扮演著核心角色。若企業希望緩解當前的進階攻擊造成的風險，企業必須制定管理及監視特權存取的策略，同時偵測威脅且採取動作。

您的應用程式堆疊及基礎架構可能相當複雜，因而難以確定哪些資產屬於最敏感的資產。供應商會努力不懈與您接觸，以引起您的關注，因而佔用您的時間。鑒於這兩點現實情況，確定後續實施哪個資安專案變得越來越困難。考慮如何決定優先順序時，回過頭來想一想自己的業務目標會有好處，但這時應採取略有不同的觀點：試想一下，如果您是外部攻擊者或惡意內部人員，希望竊取敏感性資料，執行勒索軟體或利用您的基礎架構進行非法挖礦，您會尋找什麼樣的目標？

Forrester 估計，80% 的安全性漏洞涉及特權帳號（憑證）或密碼。[1]幾乎每一起嚴重攻擊往往都會利用特權，原因顯而易見：攻擊者需要特權帳號、憑證或密碼及秘密資訊來獲取權限或工具，以便冒充內部人員且存取特權資訊或資產。攻擊者需要執行特權存取才能存取網路基礎架構且竊取資料。但是，如果沒有特權存取權，攻擊者將受到嚴格限制。

嚴酷的現實是，沒有任何企業能夠全面保護所有應用程式及基礎架構的安全，不論資料中心是在本地、在雲端還是混合維運。我們不可能防範攻擊者可能採用的各種攻擊方法；攻擊者將會入侵，這是他們的目的所在。當前，市面上沒有任何一種解決方案能夠防止每一種進階網路攻擊。儘管如此，當務之急是優先保護最關鍵的項目 — 特權存取，這需要成為每一家企業的核心策略。理由如下：

目錄

[1] The Forrester Wave™：特權身份管理，2016 年第 3 季度，Andras Cser，2016 年 7 月 8 日

「特權存取安全是保護第0層資產的強大工具。」

1. 特權是取得最關鍵資產的路徑

眾所周知，如果攻擊者獲得網域控制站的存取權，攻擊者基本上就擁有整個企業的全部存取權，且可以不受限制地破壞您的網路。鮮為人知但變得越來越普遍的是：在攻擊者設法入侵您的每一個基礎架構元件，以便在不被發現的情況下進行偵察時，雲端控制台或協作工具（如 K8S、Docker Swarm）等新型系統也成為攻擊者的主要目標。獲得這種等級存取權（無論是網域控制站還是雲端控制台）的任何人（或某個事物）可存取網路上任何位置處的任何伺服器、控制器、端點或資料。不僅如此，攻擊者還可以執行任何命令，或下載/安裝所需的任何項目。這時，攻擊者基本上就可完全控制您的整個網域。

特權存取安全是保護第 0 層資產的強大工具，在公司採用 DevOps 方法及思維時尤其如此，然後，就可以引入其它工具來支援數位轉型達成的敏捷性。這其中的每一個工具都需要人來執行某種等級的特權管理任務，因此應像其它第 0 層及可創造收入的資產一樣受到保護。在將安全性擴展到這些平台時，應小心避免造成額外限制，防止影響維運速度或對本地使用者體驗造成重大轉變。如果不落實適當的控制及特權，網域控制站將易於受到攻擊。如前所述，相比於針對網域控制站的攻擊，沒有任何其它威脅會造成企業正常維運的更大影響。

2. 人類總是存在弱點

採取阻力最小的方案是人的本性，因此，許多時候，人往往是攻擊向量中的薄弱環節。由於各種各樣的原因，走捷徑都會伴隨著危險。跳過某些步驟，避開某些流程時，隨後往往會鑄成大錯。而且，在日常例行工作中，內部人員可能會建立連接系統的捷徑，這會建立不受監視的路徑，使得內部或外部人員可以存取他們不應存取的內容。駭客也是人，也會尋找最輕鬆的入侵方式，駭客可以追蹤留下的蛛絲馬跡，直到取得能夠以各種方式加以利用的項目。

外部攻擊者會找出擁有特權的使用者，以便偽裝成特權內部人員或直接存取敏感資訊，而內部使用者會有意或無意地存取他們不應存取的資訊，顯而易見，要防止人類自身犯錯，制訂特權存取計畫至關重要。特權是一種控制措施，可確保針對敏感應用程式及基礎架構，相關人員只具有完成其工作所需的存取權，而沒有更多特權。特權控制措施還可確保在某環境中展開的活動不是出於惡意，或者對於確實出於惡意的活動，資安維運團隊會迅速做出回應以採取必要行動。

人類始終會尋找便捷的逃離（或入侵）路徑

3. 不是只有相關人員才擁有特權

需要特權存取以執行例行或重要任務的機器及應用程式的數量遠大於人員的數量。根據一般經驗，企業中特權帳號的數量是人員數量的 3-5 倍，內嵌特權使用者的數量甚至更大。通常情況下，監視、追蹤甚至是確定這些內嵌實體往往會面臨更大困難。

當前部署的 CMDB、企業票證、弱點掃描器等「傳統」商用應用程式都需要存取網路的不同部分來完成其任務。但是，由於需要存取整個網域，這些（及其它許多）應用程式基本上有權存取您的整個環境，因而需要受到保護。攻擊者除了攻擊更加傳統的舊型第 0 層應用程式以外，還會攻擊高可見性/高價值目標，如協作平台（例如 Puppet 及Ansible）及自動化伺服器（例如 Jenkins）。另外，隨著機器人流程自動化（RPA）的出現，軟體機器人將取代人類操作員來執行重複性任務（無論是否採用 DevOps），寫死的憑證或密碼及秘密資訊變得幾乎無處不在。

制訂特權策略將有助於您的企業監視各個特權層次所處的位置，且偵測出現的異常活動。

4. 所有員工工作站上都存在特權

企業首次考慮如何保護其環境時，通常會著眼於伺服器、資料庫、交換機、路由器及防火牆等設備。但是，請記住，依據預設值，每一台工作站都包含特權。記住，是每一台。所有工作站都具有內建管理者帳號，可供內部IT使用者用於修復本地出現的問題。但是，這會造成巨大的安全性漏洞，因為這些管理者帳號經由共用帳號來設立，而可能很難監控這些共用帳號，並且這些帳號還具有不必要的存取權。同樣的道理，許多時候，使用者被授予本地管理者的預設存取權，這會顯著放大攻擊承受面，但幾乎不會帶來經營效益。

被授予不必要的存取權時，終端使用者就可以自由執行一些操作，如安裝潛在危險的應用程式及軟體。駭客可利用這些存在風險的系統，首先入侵，然後在工作站間橫向移動，直到駭客獲得尋找的目標。制訂計畫來保護環境的安全時，必須採取步驟優先保護特權，且取消工作站上的本地管理權限。如果不採取此步驟，就可以更輕鬆地在您的網路中橫向移動，查明每名使用者的行為及活動將會更加困難。

請記住，在預設組態，每台工作站都包含特權。

5. 通過稽核及滿足合規要求都與特權有關

從某種程度上說，通過稽核是每家企業的日常工作。此外，由於越來越多的法律法規要求企業保護自身及客戶資料的安全，因此，至關重要的是，企業必須確定安全工具且制定計劃來幫助滿足要求。許多時候，稽核人員需要收集詳盡的日誌、記錄及證據，證明企業正在保護其最敏感性資料的安全；同時，由於會面臨罰款及未來的限制等嚴厲懲罰，對任何企業而言，滿足合規要求都是一項長期的工作。企業需要全力以赴地保護其特權資料，無論是客戶相關資料、個人健康資訊、財務信用卡資訊，還是其它資料。

藉由保護特權作為企業的核心策略，您就可以自動收集且記錄與關鍵IT基礎架構及/或敏感資訊有關活動。優先保護特權將提供企業的精細可見性，有助於深入瞭解最關鍵資產的情況。而且，雖然能夠監視及偵測您環境中的可疑事件非常重要，但如果不重點關注那些會給企業帶來最大風險的事件，就無法向稽核人員及監管機構證實，您即符合要求，又能夠處理危險活動。

> 「每家企業都需要滿足稽核及合規要求：利用特權存取安全可簡化此程序。」

一直以來，特權存取控制都是一項至關重要的舉措，可有助於降低高階攻擊造成的風險。實際上，特權存取控制是 CIS 基本控制措施中的五大措施之一。

據Gartner調查，特權帳號管理是 CISO 2018 年關注的首要資安專案。[2]特權存取安全不僅可降低風險，而且有助於保護企業的安全，提高維運及生產效率，整個企業皆可獲益。

雖然特權存取一直是多名專家確認的首要資安控制措施，但一些企業認為實施特權存取安全專案過於複雜並且/或會耗用大量資源，因此仍猶豫不決，止步不前。在某些情況下，如企業試圖在短時間內完成太多工作時，情況確實是如此。因此，我們始終建議您循序漸進，在啟動任何安全專案之前先制訂明確但數量有限的目標：設定目標，完成目標，然後重複這個程序。

需要再三強調的是，您安全堆疊中的任何一個部分都無法全面保護企業，阻止當前無休無止的各類網路攻擊。但是，優先保護特權存取，您可圍繞最敏感的資產實施強大的控制措施。

CyberArk 是特權存取安全領域排名首位的全球解決方案提供商，公司負責確保企業最關鍵基礎架構、資料及資產的安全，無論位於本地、雲端還是 DevOps 環境中。眾多全球知名機構（包括一半以上的財富 100 大企業）都依賴 CyberArk 公司來防範外部攻擊者及心懷不滿的內部人員。

瞭解詳情

請瀏覽 cyberark.com 瞭解詳情。

[2] Gartner, Smarter with Gartner，Gartner 2018 年十大資安專案 ，2018 年 6 月 6 日