以最少的權限和應用程式控管來獲得安全和生產力

CYBERARK®

目錄

概述

依據設計，權限的授予經常是全有或全無的決定 — 亦即組織內的使用者通常擁有完全的"管理員"權限，不然就是完全沒有管理權限可言。因此，業務用戶和資訊管理員常常會擁有超過其所需的權限，因而形成經常被利用的廣大攻擊面。問題是，在移除管理員權限以降低風險的過程中，組織很可能會面對許多的挑戰。

這本電子書將探討這些挑戰，並針對開發平衡的分層式安全控管提出最好的實作方法。

挑戰一

功能強大的帳號群代表廣大的攻擊面

具本機管理員權限的帳號群代表廣大的攻擊面，因為這些帳號存在於運作環境中的每一個端點和伺服器上。而在這些相同的機器上擁有管理員權限的個別使用者帳號只會更加擴大攻擊面。

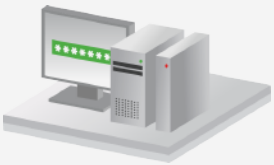
請試想具有管理員權限的使用者可能故意或不小心:

改變系統組態設定

- 安裝和啟用服務
- 關閉/解除安裝防毒軟體
- 使機器無法啟動
- 停止既存的服務 (例如防火牆)
- 以木馬程式置換作業系統或其它程式檔案

安裝惡意軟體

- 核心模式root kits
- 系統層次的鍵盤側錄器
- 惡意的ActiveX控制項
- 間諜軟體和廣告軟體
- 助長傳遞雜湊(Pass-the-Hash)攻擊的惡意軟體



存取和變更帳號

- 建立及修改使用者帳號
- 重新設定本機密碼
- 存取屬於其它使用者的資料

從安全的角度來看，擁有本機管理員權限的帳號經常是進階攻擊者的目標，因為這些帳號能夠提供進階的權限，且這些帳號若沒有受到適當的保護時便很容易被利用。

從業務活動的角度來看，擁有管理員權限但缺乏經驗的使用者經常會對機器造成意外損害，亦即資訊管理團隊必須持續花費許多時間和精力處理不小心所造成的損壞以及搶救突發事件。

挑戰二

要在安全性和生產力之間找到平衡是很困難的

取消業務用戶的管理員權限是最好的安全措施，但許多組織有正當的理由而對做出這項改變感到躊躇。業務用戶若沒有任何的管理員權限，就可能無法執行某些工作或使用某些其日常角色所需的應用程式。

例如，使用者可能因工作需要而必須要有權限來執行某個應用程式。或者，使用者可能會需要管理權限來安裝或更新經授權且受信任的應用程式。若完全取消業務用戶的管理權限，這些使用者會因為只是要執行每日例行工作而需要使用權限時，就得被迫請求服務支援。

這所導致的結果是:

挫折的使用者

沒有彈性的權限政策會讓業務運轉停滯。這無可避免地會導致使用者感到挫折，因為他們不再有權能夠執行必要的工作任務。

負擔過多的支援小組

當資訊政策阻礙了業務用戶日常必需執行的例行性工作時，使用者必須請求服務中心恢復其所需的權限許可。這樣會導致資訊管理成本的大幅提升，且會讓支援小組疲於奔命。

挑戰三

太少的權限會導致「權限蠕變」並增加風險

當組織選擇取消業務用戶的管理權限時，資訊小組就會不時地需要重新給予權限以便讓使用者可執行某些工作。例如，許多在企業資訊環境中以前就已存在的或自行開發的應用程式需要權限才可執行，許多商用現貨軟體(COTS)也有同樣的情況。為了讓業務用戶執行這些經授權且必需的應用程式，資訊小組就必須將本機管理員權限再次提供給這些使用者。

一旦權限被重新賦予就很少會有再收回的情形，如此經過一段時間後組織便會再次有許多使用者擁有本機管理員權限。這種「權限蠕變」會再次開啟與過多管理權限有關的安全漏洞，並使得這些相信自家有完善的保護機制的組織更容易遭受威脅。

挑戰四

太多權限會增加來自內部人員和進階威脅的風險

限制業務用戶權限除了會抵銷生產力之外，許多組織對於限制IT管理員在Windows伺服器上的權限也是很躊躇的。理想的設定是系統管理員、應用程式擁有者和資料庫管理員在每一個伺服器上都各自有經過允許的存取範圍。但這樣的職責分割在實務上會有困難，且會導致IT管理員擁有比他們實際工作所需還要多出很多的權限。

分割IT管理員的職責時若沒有依據以角色為基準的授權政策，則會使得敏感系統容易被缺乏經驗的使用者損壞、被惡意的內部人員利用或者被進階攻擊者侵入並存取未經授權的特權帳戶。

新進而缺乏經驗的管理員可能會因執行錯誤的指令而不小心損壞系統

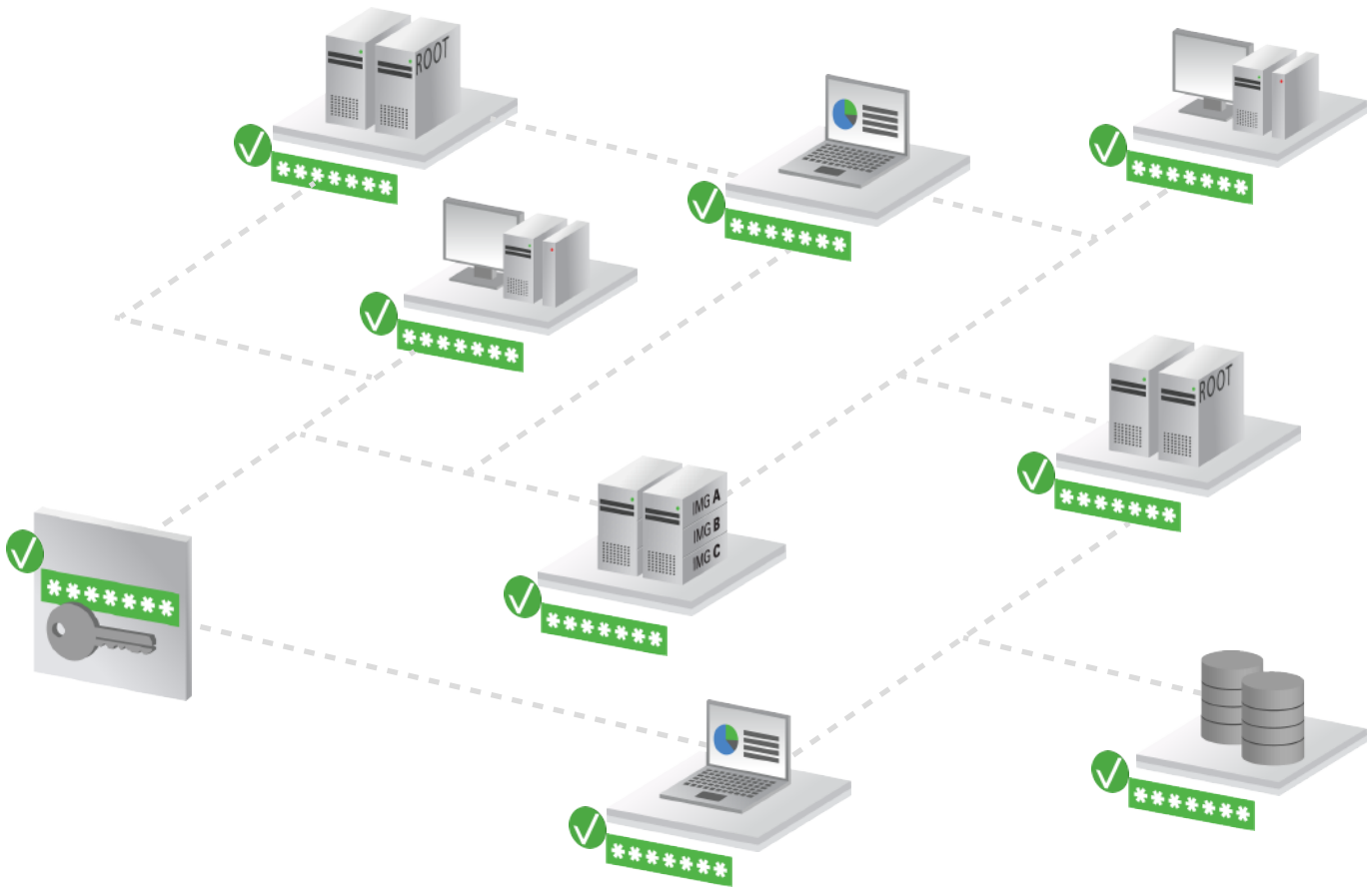
惡意的內部人士可能會使用他的權限刻意偷取資料或損壞系統

攻擊者可藉由侵入一個管理員帳號而獲得對機密系統的控制權

挑戰五

在每一台機器上，必定有一個「最高階管理員」帳號

就架構設計而言，每一個端點和伺服器都會有一個這樣的最高階管理員，這是一個第一階層或類似於第一階層的帳戶，其對本機擁有完整的管理控制權限。即使你已將管理員權限從個別使用者帳號中移除，這些功能強大的最高階管理員帳號仍然會繼續存在。這些最高階管理員帳號的密碼管理政策若不完善就可能會導致相同密碼跨越多個系統重複使用，如此便會讓攻擊者在侵入一台機器之後可以輕易平行移動到整個運作環境 - 提升權限、竊取資料並一路損毀系統。



挑戰六

儘管做了權限的限制，一些惡意軟體仍有辦法入侵

當限制權限的程度達到只有在絕對有需要的情況下才可獲得權限，可讓組織減少攻擊面並阻止惡意的應用程式嘗試利用權限安裝其他惡意軟體或損壞機器。但不是所有惡意的應用程式都需要權限才可執行，且當攻擊者有能力繞過防禦措施時，組織對於這類型惡意軟體的防護就會顯得更脆弱。

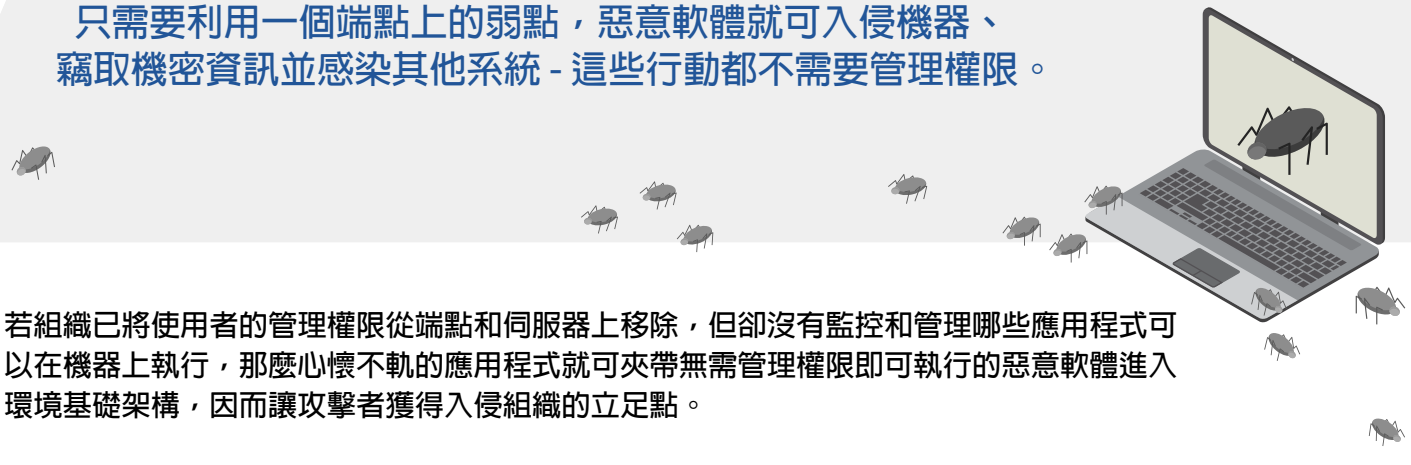
只要用10封電子郵件
基本上就有

90%

的機會使至少一人
變成罪犯的犧牲品

研究顯示大多數進階攻擊都始於寄給無權限業務用戶的網路釣魚電子郵件，且只需要10封電子郵件基本上就有90%的機會使至少一人變成罪犯的犧牲品。這些網路釣魚攻擊包括非常精密的惡意軟體。一旦進入組織網路，這些惡意軟體便可在無需使用任何管理權限的情況下入侵機器、竊取資料、獲取憑證或損毀系統。

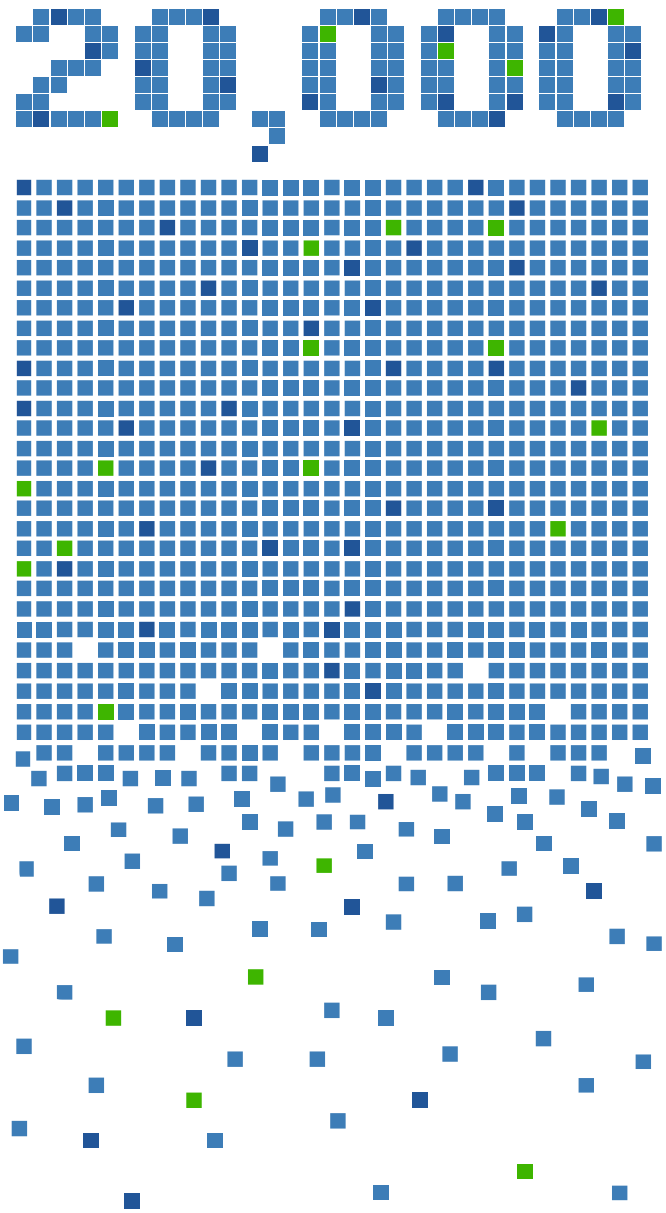
只需要利用一個端點上的弱點，惡意軟體就可入侵機器、
竊取機密資訊並感染其他系統 - 這些行動都不需要管理權限。



若組織已將使用者的管理權限從端點和伺服器上移除，但卻沒有監控和管理哪些應用程式可以在機器上執行，那麼心懷不軌的應用程式就可夾帶無需管理權限即可執行的惡意軟體進入環境基礎架構，因而讓攻擊者獲得入侵組織的立足點。

挑戰七

要確實追蹤到系統環境中有哪些應用程式是很困難的－而要能夠知道哪些是好的、哪些是壞的應用程式就更困難了



我們對員工端點的研究顯示在一個企業體中發現超過20,000個不同的應用程式是很平常的事情，亦即惡意的應用程式可以輕易地混在裡面，因為IT團隊不會有時間用人工去分析每一件事情。

以這樣的規模來看，要辨識出哪些應用程式是好的、壞的或未知的是令人怯步的任務，更不用說在成本上根本不可行。更糟的是，每檢查到一個明顯是業務用應用程式或明顯是惡意的應用程式，就會發現有更多不是那麼明顯的應用程式，管理員根本不會有時間去處理應用程式的分類。

開發分層式安全控管的七個建議

面對目前所描述到的這些挑戰，組織應尋求具彈性的工具以自動化管理本機管理員權限並控管端點及伺服器上的應用程式。這種最少權限和應用程式控管的獨特組合應該是平衡分層式安全措施的一部分，其可幫助組織減少攻擊面、抵禦已入侵的威脅並將潛在之進行中的攻擊警示給安全小組知道 — 這些行動都不需暫停使用者的生產力或讓IT安全小組疲於奔命。

要獲得安全與可使用性之間的平衡，組織應考慮
採用整合的權限管理和應用程式管控解決方案，包括讓安全小組能夠：

1. 以信任度為基礎，自動建立權限和應用程式控管政策。

自動定義甚麼樣的應用程式是被組織所信任的，辨識出這些應用程式中每一個所需的權限，並依據這些信任度建立政策以節省IT小組珍貴的時間和精力。

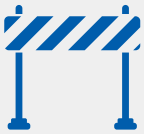
2. 依據其所需無縫提升業務用戶的權限。

從業務用戶移除管理員權限，但依據政策提供無縫的權限提升以保持使用者的生產力，而同時又不會增加攻擊面。

3. 針對Windows系統管理員實施縝密的最少權限政策。

縝密地控管哪些指令和工作任務是由哪一個IT管理者依據角色而允許執行，以便有效區隔職責並降低內部人員風險和進階威脅。

開發分層式安全控管的七個建議 (續)



4. 控管哪些應用程式可在IT環境中執行。

讓受信任的應用程式可無縫在環境中執行，並同時自動阻擋惡意應用程式且對於未知應用程式限制其權限。若有需要，可實施嚴格的白名單政策。

5. 保護「最高階管理員」帳戶憑證並將其保存於安全的中央管控區中。

控管對本機管理員和網域管理者帳戶的存取，因為這些帳戶可被用來獲取對Windows系統端點和伺服器的管理權限並進行存取。將這些憑證儲存於擁有強大的存取控制能力及完整的可審查能力之安全的中央管控區中。

6. 最高階管理員憑證每用過一次就輪動。

每次使用過後便立即輪動所有最高階管理員的密碼，將任何可能已被鍵盤側錄軟體捕捉的憑證作廢，並降低遭受傳遞雜湊(Pass-the-Hash)攻擊的風險。

7. 監控最高階管理員帳戶的使用情況以偵測異常狀況

監控與最高階管理員帳戶有關的所有活動以便快速偵測並警示可能準備進行攻擊的異常活動，且可讓安全小組人員獲得更全面性的審查線索。

結論

當今的企業環境不是黑與白那麼單純 — 而對安全防護工具也不該作如此簡單的思考。組織應學習如何找到安全和可用性之間的平衡以有效減少攻擊面，並同時保持使用者的生產力以及降低IT小組的工作量。

現在有一個可應對並解決這些問題的全面性解決方案。

CyberArk 的 Viewfinity 是 CyberArk 特權帳號安全解決方案的一部分。這是一個完整的解決方案，其設計用來主動保護企業核心資料並防止進階攻擊者利用管理權限獲得存取權限來竊取敏感資料並損毀重要系統。 該解決方案能藉由幫助組織減少駭客攻擊面，使組織可無痛地移除無需的本機管理員權限，防止惡意軟體進行攻擊，並強化授權帳號的安全。CyberArk特權帳號安全解決方案是設計用來主動保護、隔離、控制和持續監控在端點、伺服器、實體或虛擬機器、資料庫、應用程式、虛擬機器監視器、網路設備、安全裝置和其他物件上的授權帳戶。此解決方案的各項產品可單獨分開管理，或合併在一起做為一個緊密結合且全面的特權帳號安全解決方案。

欲知詳情，請上網瀏覽：www.cyberark.tw/viewfinity.

資料來源

1. Verizon. "2015 Data Breach Investigations Report." Page 13.
2. Viewfinity. "IT Security's 50 Shades of Grey Whitepaper." Page 2.