SailPoint

數據洩漏分析

今日我們所認知的企業資安景象已改變。企業的應用程式和數據不斷受到攻擊，洩漏事件不斷發生，而敏感性資訊也每天不斷地被發佈。數據洩漏變得愈來愈頻繁，範圍更廣，且更具毀滅性，其中程式原始碼、客戶和員工資料、以及其它敏感數據正不斷地被釋出。最讓企業對數據洩漏感到擔憂的不僅是它所造成的後果，更是一個常見的事實 – 這些數據洩漏有43%的比例是由內部人員所直接造成。

2015年在美國就發生了至少1400件可考證的數據遺失事件，釋放出超過1億6千9百萬筆的數據紀錄。而其中最大一件牽涉到8千萬筆紀錄被竊取，佔了總筆數將近一半的量。其它事件包括了美國國家人事管理局、摩根史坦利、和國稅局。所有這些高調的數據洩漏都是因為內部人員做了他們不該做的事情而造成，包括讀取網路釣魚電郵和使用脆弱密碼。

從過去吸取教訓

SailPoint技術暨資安長Darran Rolls所做的簡介

在80年代早期，當電腦尚未進入文化和媒體主流時；且在我適應這股潮流前，駭客這名詞尚未成為家喻戶曉的用語。那時候沒有技術長這樣的職稱，而我也尚未開始嘗試進入科技的世界，但我記得有那麼一個關鍵的時刻讓我決定踏入這領域。

那是一個電視節目Micro Live，讓我每周一大早起床觀看。節目中有一段插曲與資安世界息息相關，其中有個最早期的 "駭客事件" 就在這節目被現場轉播，但事件的發生不是因為駭客透過網路進入系統中破解程式碼或帳號密碼，而僅只是因人為錯誤所造成。

這節目主持人登入到一台遠端電腦作展示。此時，帳戶名稱毫無遮掩地顯示在螢幕上，像一面揮舞的旗幟般醒目，讓這節目變成惡作劇觀眾的目標。雖然他們做了該做的防範，在主持人鍵入密碼時將鍵盤隱藏。 然而，就在主持人嘗試登入的幾秒後，螢幕上卻顯示出駭客的訊息，破解成功。

是甚麼造成駭客破解呢?主持人在準備節目開播前以通訊線路問了導播並確認使用者密碼。他未料到的是控制室中有位工作人員無意間將通訊線路與後台線路搭接，而後台是要導引稍後在節目中的主題話語。這些駭客專家因此能夠獲得公開的使用者名稱和密碼，並干擾這節目的示範，都只是因為一個簡單的人為錯誤所造成。

這個故事告訴我們，現今組織中這類相同且單純的錯誤，已經造成一些我們所經歷過最大的數據洩漏事件，且其後果遠比當時更加嚴重。

常見的處理程序陷阱

如同我們領悟到如何從類似Micor Live節目的錯誤中保護我們自己，當有數據洩漏發生時，我們亦可藉由對過去違規事件的檢驗獲得對事件發生原因的洞察力，並找出組織內部安全處理程序失敗之處。這些處理程序中有五項與身份辨識息息相關，且每一項皆可延緩甚至防範數據洩漏。

- 不良的帳號管控：一旦駭客進入到企業的系統中，他們通常會建立自己的管理者帳號。 但若有適當的帳號管控機制，這種事情就不會發生。
- 脆弱密碼：或許駭客團隊被入侵最為人知的就是管理者密碼太脆弱[1]。脆弱的認證憑證通常是暴力攻擊的切入點。
- 孤立帳號：當員工離職或更換職務後，原本帳號應該被終止，但卻往往被留存且仍可使用。這樣就會造成巨大的安全縫隙，因為惡意的使用者獲得這些孤立帳號後，卻沒人會知道這些帳號已產生安全漏洞，因為無人使用這些帳號，自然就沒有偵測控制的可能。
- 脆弱的庫存檔案和目錄：一旦進入網路和檔案分享後，駭客就非常有可能嘗試將所有可存取的檔案資訊全部下載。
- 過度被授權的身份：雖然高階主管帳號是釣魚程式明顯的目標以獲得密碼憑證，但任何的使用者帳號對駭客而言皆是有價值的目標。

[1] *請上標Hacking 駭客團隊使用令人震驚的脆弱密碼*

被過度授權的身份會產生特別的威脅：看起來低風險的使用者也可能造成對系統和數據不適當的存取。若這樣的帳號被洩漏，且對其授權未有妥善的管理，駭客就可能得以存取敏感的資訊和系統。

數據洩漏分析觀察

確實有些資安問題需要解決，但問題還是存在：我們如何才能有更好的自我保護呢? 要了解這個問題，我們首先必須從過去集體的錯誤中學習，然後才能進入"野獸之腹"，從所學的教訓中，我們找出數據洩漏的四個一般性階段：偵察、滲透、竊取 和 滲出。

階段 1

偵察

數據洩漏的第一個階段是駭客對其目標的學習，並從中找到最好的攻擊方式。即使駭客開始迴避使用網路途徑和SQL注入作為其主要的滲透方式，這並不表示他們放棄這些途徑。作為啟始的戰術，駭客會先掃描目標企業所使用的外部可用資源。

此階段亦是社群工程開始的時候。駭客會對每一個與該公司有連結的人 — 員工、客戶、廠商、夥伴等作深入觀察，並對能夠進入該公司系統的人送出大量的釣魚電郵。管理階層和其它具高價值目標會遭遇這些釣魚攻勢。

階段 2

滲透

企業擁有為數眾多的員工，且員工會出錯是不爭的事實，所以某個員工無意間按了一個不該按下的網路連結只是遲早的事情，而駭客就這樣進入了。例如，假設一個釣魚嘗試成功讓主管按下網路連結去下載一個惡意軟體到他的電腦中。只要這樣，區域的管理者帳號就會受到侵入，然後允許駭客存取企業中許多的資訊。一旦擁有區域管理者的存取權限，駭客就可測試該帳號在組織伺服器上的權限，並在網路上安裝竊取資訊的軟體，然後開始掃瞄系統上任何可能有價值的資訊。

階段 3

竊取

此階段，駭客已找到進入的途徑且正在尋找最好的方式以獲得對 "最肥美"資訊的完全存取。然後對管理性帳號發動暴力攻擊。此方法可擊破脆弱的密碼使駭客得以進入系統。例如，公司內部的入口網站就會被侵入。從那裏開使，入侵者可在網路上申請或建立新的管理者帳號，增加其檔案分享的權限，並進一步擴展深入組織的應用程式和數據。

階段 4

滲出

一旦所有需要下載資料的系統都被侵入後，駭客最後的階段就是下載一切所需的數據。這包括財務文件、客戶和員工資料、銷售數據、產品發展圖表、原始程式碼、以及其它各式各樣的資訊。在許多情況下，公司使用者身份的憑證認證加密資訊也被下載。SailPoint在2016作的市場脈動調查顯示65%的員工會在多個系統和應用程式重複使用相同密碼。駭客一旦完全掌握了認證資訊後，就可打開對其它公司的入侵大門，因而造成更多資訊的洩漏。

一旦企業察覺到被侵入且發現資訊被大量竊取時，這才是嚴重後果的開始。在許多情況下，這意味著客戶、夥伴和其它相關各方的抱怨所造成生意上的損失。對許多企業而言，駭客入侵代表著衝擊和違規罰款。畢竟被入侵會對被入侵者和其相關各方帶來許多的問題。

從身份存取管理(IAM)學到的教訓

當我們面對過去數據被入侵竊取且了解入侵在實務上如何發生的時候，我們就更能保護自己以及我們珍貴的數據。首先，要認知對企業系統的攻擊嘗試幾乎是不爭的事實，即使未必每次都滲透成功，且一年裡平均會有229天[2] 偵測到入侵。

在這7個月的時間裡，數不清的攻擊方式從企業外部和內部系統發動攻勢。若有一個強韌的身份治理程式，就可在入侵發生前有效降低風險，並可能在一旦入侵嘗試發動時減緩其進程。

建立良好的處理程序

從先前的例子可知，經常性的密碼重設和強韌密碼策略可減緩滲透和竊取階段的進程。我們觀察到在滲透階段駭客使用惡意軟體和區域管理者帳號成功入侵。若當時強制執行經常性的密碼重設，就不會發生入侵存取事件了。在竊取階段，脆弱的密碼是對公司內部入口網站不當授權存取的來源。當時若建置了強韌密碼政策，駭客要破解憑證就需要花更多的時間，企業就會有較多時間偵測到駭客入侵了。

偵測可疑的行為

良好身份治理解決方案的建立是要與其它系統整合，以便提供IT團隊企業系統和數據的整體圖像 — 無論是在那個節點上。

[2] 2016年數據洩漏成本研究：全球分析，Ponemon學院

藉由整合身份治理解決方案，你可與SIEM和數據存取治理方案整合，偵測即時的威脅。這樣的建置可幫助上述駭客滲透、竊取、滲出階段的偵測，揭發入侵並在任何資訊被竊取之前將之消滅。此外，這樣的系統協同作業可在駭客竊取階段偵測到流氓管理帳號的建立。

為入侵者設下陷阱

當駭客在計畫初期執行偵察以入侵你的組織前，他們對你系統的了解不如你IT人員知道的多。要有好的方法來分散駭客的注意力，讓你和你的團隊有較多的時間作偵測然後消滅任何的入侵，那麼就需要為駭客設下一個看似很有價值不能不竊取的假帳號和資訊"蜜罐"。

在建立了假的管理者帳號和其它具脆弱憑證的假帳號後，使用你的身份治理系統，在這些帳號被存取時，將旗幟高舉。這是個容易偵測捕捉駭客的方法。另一種戰術是將文件以重要名稱標示以誘使駭客認為這些文件含有敏感且具財務價值的資訊。如同你的整合系統可對假帳號的存取高舉旗幟，數據存取治理這部分也可在這些假帳號被存取時對適當之各方提出警訊，以降低風險。

結論

藉由以使用者為中心的途徑並將所有的系統 (身份治理、數據存取治理、網路安全、使用者行為分析等)，一起整合到IAM平台，IT人員就可檢視整個的安全生態系統。只有這些都做到了，屆時組織才能夠真正將其身份治理置於其安全的核心，降低入侵風險並保護企業成功所需的資訊。

WP1042-1610