資訊管理
白皮書

以8步驟全方位保護資料庫

IBM子公司Guardium 技術長Ron Ben Natan 博士

電腦攻擊、內部人員違法行為，以及各種監管要求，正促使組織尋求新的途徑來保護商業資料庫系統（例如 Oracle、Microsoft SQL Server、IBM DB2 和 Sybase）中的企業和客戶資料。本文將探討8項重要的最佳實務，提供全面的方法來協助保護資料庫與遵循關鍵法規（例如 SOX、PCI-DSS、GLBA 和資料保護法）。

保護資料庫並實現法規遵循

經濟利益驅使下的攻擊、內部人員的違法行為，以及各種法規要求，正促使組織尋求新的途徑來保護企業和客戶資料。

全球大部分的機密資料都儲存在商業資料庫中，例如 Oracle、Microsoft SQL Server、IBM DB2、IBM Informix 和 Sybase，使得資料庫日漸成為最主要的犯罪目標。這或許可以解釋為什麼 SQL 的隱碼攻擊次數在 2008 年激增了134%，從平均每天數千次增加到數十萬次（根據 IBM 最新發佈的報告[1]）。

更嚴重的是，Forrester [2]指出 60% 的企業無法及時修補資料庫的安全性漏洞。根據 IBM 分析，2008 年發現的所有 Web 應用漏洞中，74%（其中 SQL 隱碼漏洞佔絕大多數）甚至到 2008 年年底還沒有可用的修補程式。

「您無法防範未知的攻擊。不論是資料庫實例或是資料庫中的機密資料，您都需要好好安排您的機密資產。」

過去絕大部分的注意力，都集中在保護網路周邊和用戶端系統（防火牆、IDS/IPS、防毒軟體等），而我們正步入嶄新的階段。今日資訊安全專業人員的使命，是確保企業資料庫免遭破壞與免於未經授權的操作。

下文列出8項重要的最佳實務，提供全方位的方法來協助保護資料庫與遵循關鍵法規（例如SOX、PCI DSS、GLBA和資料保護法）。

1. 發現

您無法防範未知的攻擊。不論是資料庫實例或是資料庫中的機密資料，您都需要好好安排您的機密資產。此外，您應該讓偵測流程能夠自動化，因為機密資料的位置會因為使用新應用或應用經過修改、併購等因素，不斷變化。

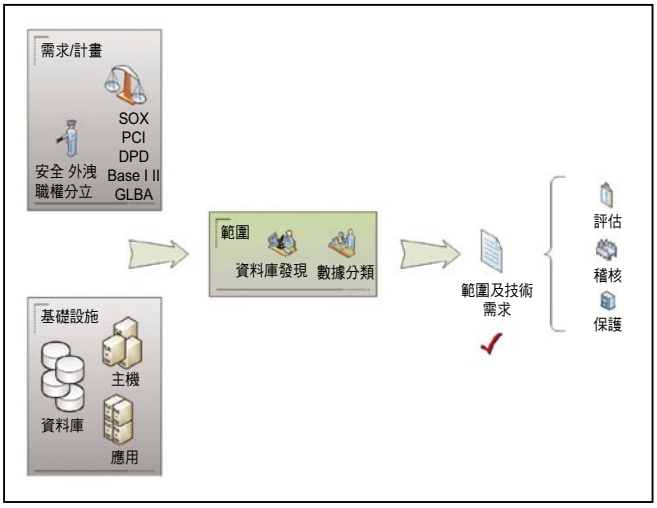

圖1：使用探索工具來完成工作。您需要規劃資料庫實例以及機密資料的存放位置。

值得注意的是，部分探索工具還能找出 SQL 隱碼攻擊在資料庫中放置的惡意軟體。除了洩漏機密資訊外，SQL 隱碼漏洞還使攻擊者能在資料庫中嵌入其他攻擊碼，然後攻擊存取網站的用戶。

2. 漏洞和配置評估

您需要評估資料庫配置，確保毫無安全漏洞。這項工作包括驗證作業系統安裝資料庫的方式（例如檢查資料庫配置檔和執行檔），以及驗證資料庫內部的配置選項（例如登錄失敗多少次後鎖定帳戶、為重要表單指定許可權）。此外，您需要確認您使用的資料庫版本沒有已知漏洞。

傳統網路漏洞掃描程式的設計，並未納入相關考量，沒有嵌入資料庫結構和預期行為的知識，也不能執行 SQL 查詢（透過驗證的資料庫存取）來顯示資料庫配置資訊。

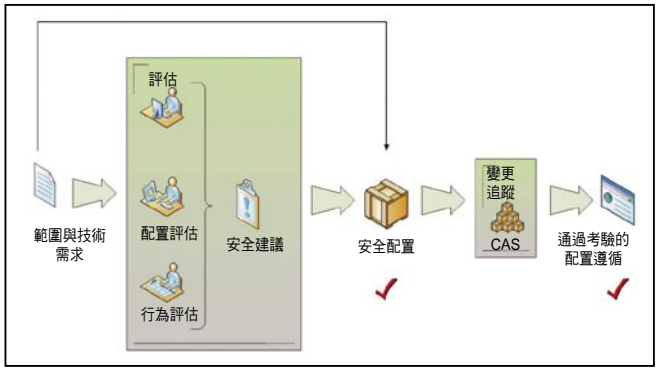

圖2：漏洞評估和變更追蹤範例。

3. 加強保護

執行漏洞評估通常可獲得具體的建議，也是加強資料庫保護的第一步。加強保護的其他要點還包括刪除所有不用的功能和選項。

4. 稽核變更

加強安全保護的配置後，必須持續追蹤，確認沒有偏離您的「黃金」（安全）配置。您可透過變更稽核工具來完成此一任務，比較配置的快照（作業系統和資料庫兩個級別），並在發生可能影響資料庫安全的變更時，立即發出警告。

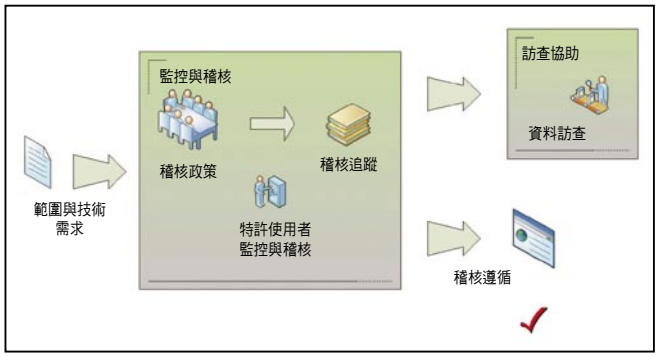

圖3：資料庫活動監控 (DAM) 和稽核範例。

5. 資料庫活動監控 (DAM)

即時監測資料庫活動是相當關鍵的步驟。透過立即發現入侵與濫用，可以減少資料外洩。例如，DAM 可以警告 SQL 隱碼攻擊的異常存取模式、財務資料的未授權更改、帳戶專用權的提升，以及透過 SQL 命令執行的配置變更。

監控專用權用戶也是 SOX 等資料隱私法和 PCI DSS 等資料隱私法的要求。偵測入侵也是要點，因為攻擊經常會讓攻擊者獲得特許使用者的存取許可權（例如透過您的業務應用憑證）。

DAM 也是漏洞評估的重要要素，可超越傳統的靜態評估，進行「行為漏洞」（例如多個用戶共用專用權憑證或資料庫登錄失敗次數過多）的動態評估。

「資料和用戶的建立方式各不相同。您必須對用戶進行身份驗證，確保每個用戶都肩負完整責任，並透過管理專用權來限制資料存取。」

最後，一些 DAM 技術提供了應用層監控，允許您檢測透過多級應用（例如 PeopleSoft、SAP 和 Oracle e-Business Suite）執行的詐欺行為，而不是透過直接連接資料庫執行的詐欺行為。

6. 稽核

凡可能影響安全防護、資料完整性或機密資料查看的所有資料庫活動，都應採取不可否認 (non-repudiable) 的安全稽核追蹤。除了遵循要求外，擁有精細稽核追蹤對於鑑識調查也很重要。

大部分組織目前都採用手動稽核的方式，利用傳統的本機資料庫日誌功能，但此類方法通常難以實施，因為執行起來很複雜，而且操作成本亦高。其他缺點尚包括較高的性能耗用、缺乏「職權分立」（DBA 可輕鬆篡改資料庫日誌的內容，進而影響不可否認性），且必需購買和管理大量的儲存容量，處理大量未經過濾的異動資訊。

幸運的是，現在有了新的 DAM 解決方案，能夠在幾乎不影響性能的前提下，提供精細、獨立於 DBMS 的稽核，並可透過自動化、集中的跨 DBMS 策略和稽核儲存庫、過濾和壓縮，降低操作成本。

7. 身份驗證、存取控制和授權管理

資料和用戶的建立方式各不相同。您必須對用戶進行身份驗證，確保每個用戶肩負完整責任，並透過管理專用權來限制資料存取。您還應該強制實施專用權，即使是擁有最高專用權的資料庫用戶也是一樣，並且定期稽核授權報告（也稱為「用戶權利證明報告」），將其納入正式稽核流程。

8. 加密

使用加密並以不可讀的方式呈現機密資料，攻擊者就無法從資料庫外部對資料進行未授權存取。此步驟包括對傳輸中的資料進行加密，使攻擊者無法在網路層竊聽資訊，或在資料發送至資料庫用戶端時存取資料。此外還應對儲存的資料進行加密，讓攻擊者即使能夠存取媒體檔，也無法擷取資料。

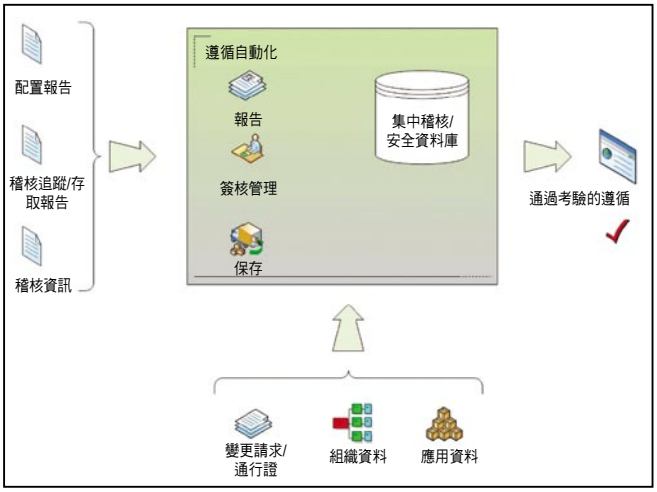

圖4：管理完整遵循週期。

以8步驟全方位保護資料庫

1. 發現
2. 漏洞和配置評估
3. 加強保護
4. 稽核變更
5. 資料庫活動監控（DAM）
6. 稽核
7. 身份驗證、存取控制和授權管理
8. 加密

關於作者

Dr. Ron Ben Natan 擁有超過 20年為 Merrill Lynch、J.P. Morgan、Intel 和 AT&T Bell Laboratories 等頂尖公司開發企業應用和安全技術的豐富經驗。Ron 亦為 Phillip Morris、Miller Beer、HSBC、HP、Applied Materials和瑞士武裝部隊的資料安全和分散式系統顧問。

身為擁有電腦科學博士學位的 IBM 金牌顧問，Ron 是分散式應用環境、應用安全和資料庫安全方面的專家，擁有12項專利，並撰寫了 12 本技術圖書，包括Implementing Database Security and Auditing（Elsevier Digital Press 出版，是該領域的標竿），以及2009年最新出版的 HOWTO Secure and Audit Oracle 10g and 11g (CRC Press)。

關於 IBM 子公司 Guardium

Guardium 是 IBM 子公司，致力於透過持續監控對高價值資料庫的存取和變更來保護關鍵企業資訊。Guardium 的可擴充平台可透過異質基礎設施的統一策略，簡化資訊治理，並透過自動化遵循流程來降低操作成本，協助企業以安全的方式使用可靠資訊，推動更智慧的業務成果。

目前全球超過 450 個資料中心都採用 Guardium 的企業平台，包括 5 家全球銀行龍頭、前 6 大保險公司中的 4 家、3 家頂級零售商中的 2 家、20 家全球頂尖電信公司、2 家全球頂級飲料品牌、全球最著名的 PC 廠商、全球 3 大汽車製造商中之一、一家全球前 3 大航空公司，以及一家商業智慧軟體供應龍頭。Guardium 是第一家透過可擴充企業平台解決核心資料安全問題的公司，既能即時保護資料庫，又能自動化完整的遵循稽核流程。

台灣國際商業機器股份有限公司
台北市松仁路7號3樓
市場行銷處：0800-016-888按1
技術諮詢熱線：0800-000-700