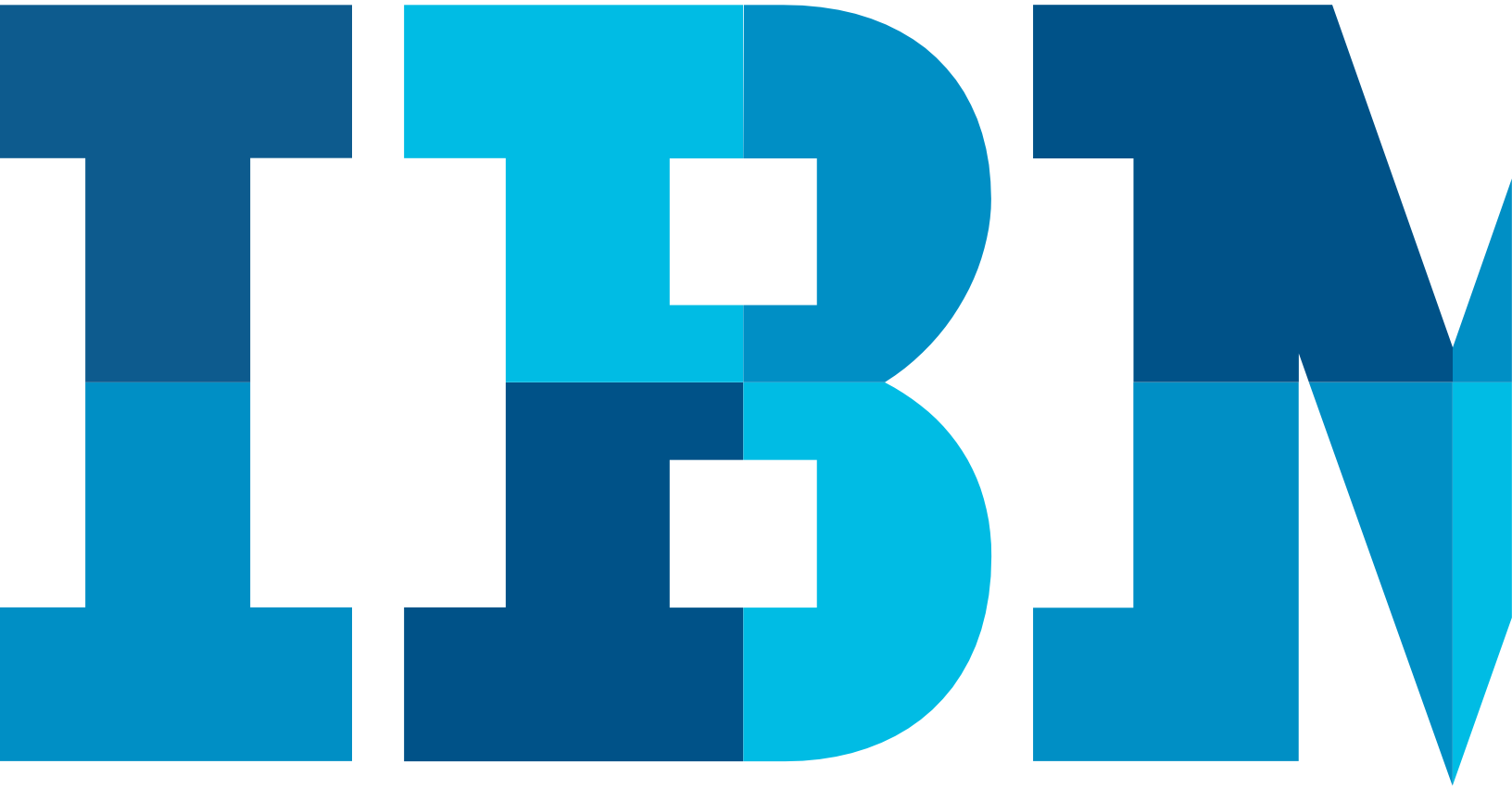
信息管理
白皮书

八步实现数据库整体安全

作者：Ron Ben Natan 博士，IBM 杰出工程师，集成数据管理首席技术官



IBM

网络攻击、内部员工渎职和监管要求违规都正促使组织寻求新途径保护其在商业数据库系统（如 Oracle、Microsoft SQL Server、IBM DB2 和 Sybase）中找到的企业和客户数据安全。 本文探讨了 8 种重要的最佳实践，旨在提供一套整体方法既保护数据库，又可实现 SOX、PCI-DSS、GLBA 及数据保护法律等关键法规的合规性。

保护数据库并实现合规性

经济动机攻击、内部员工渎职和监管要求违规都会促使组织寻求新途径保护其企业和客户数据安全。

绝大部分全球敏感数据均存储在商业数据库系统（如 Oracle、Microsoft SQL Server、IBM DB2 和 Sybase）中，促使数据库成为犯罪分子越来越受青睐的攻击目标。 这或许恰好可以解释为什么 SQL 注入攻击在 2008 年突然蹿升至 134%，IBM[1] 最近公布的调查报告发现，其数量已从平均每天几千次上升为每天数十万次。

更加糟糕的是，Forrester[2] 报告称有 60% 的企业在应用数据库安全修补程序方面滞后，同时据 IBM 调查发现，在 2008 年公开的所有 Web 应用程序漏洞（主要是 SQL 注入漏洞）有 74% 的漏洞直到 2008 年底仍未开发可用修补程序。

“您不可能保护自己不了解的内容。您需要有效地划定敏感资产范围，包括数据库实例和数据库内的敏感数据。”

从前一直专注于保护外围网络和客户端系统（防火墙、IDS/IPS、病毒防护等）安全，而现在我们正在步入一个崭新的阶段，如今由信息安全专业人员专项负责确保企业数据库安全，使其免受违规和未授权更改的侵扰。

以下是 8 种重要的最佳做法，旨在提供一套整体方法既保护数据库，又可实现 SOX、PCI DSS、GLBA 及数据保护法律等关键法规的合规性：

1. 发现。

您不可能保护自己不了解的内容。 您需要有效地划定敏感资产范围，包括数据库实例和数据库内的敏感数据。此外，您还应当自动执行发现流程，这是因为新应用程序或修改应用程序、兼并和收购等情况都会导致敏感数据的位置不断发生变化

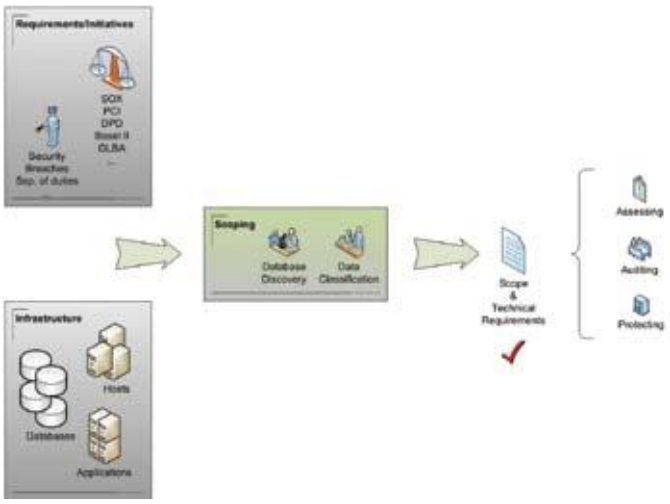


图 1： 使用发现工具启动实现过程。 您需要绘制数据库实例地图，并确定敏感数据的所在位置。

1 “IBM Internet Security Systems X-Force® 2008 趋势与风险报告，”IBM 全球技术服务部，2009 年 1 月。
2 “市场概述： 数据库安全，”Forrester Research，2009 年 2 月。

有趣的是，某些发现工具还能够找出由 SQL 注入攻击进入数据库内的恶意软件。 除泄露机密信息外，SQL 注入漏洞还会协助攻击者将其他攻击嵌入数据库内部，以便随后用于攻击网站访客。

2. 漏洞和配置评估。

您需要评估数据库配置，以确保数据库不存在安全漏洞。 这项评估包括验证操作系统上安装数据库的方式（例如，检查数据库配置文件和可执行文件的文件特权），以及数据库本身的配置选项（如经过多少次登录失败后锁定帐户，或向判定表分配哪些特权）。 此外，您还需要确认并未运行带有已知漏洞的数据库版本。

传统的网络漏洞扫描程序无法实现这一功能，因为其中并未嵌入有关数据库结构和预期行为的知识，也不能（通过对数据库进行有效访问）发起 SQL 查询，以便显示数据库配置信息。

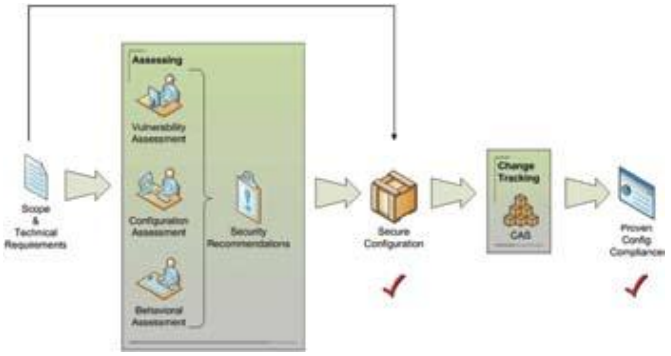


图2： 漏洞评估和更改跟踪用例。

3. 强化。

漏洞评估结果往往是一系列特定建议。 这是强化数据库的首要步骤。 其他强化因素还包括删除不使用的所有功能和选项。

4. 更改审计。

一旦您创建了强化配置，就必须持续跟踪，以确保不会偏离您的“黄金”（安全）配置轨道。 您可以使用更改审计工具实现这一目标，（在操作系统级别和数据库级别）比较各配置快照，同时每当做出可能会影响数据库安全的更改时立即向您发出警报。

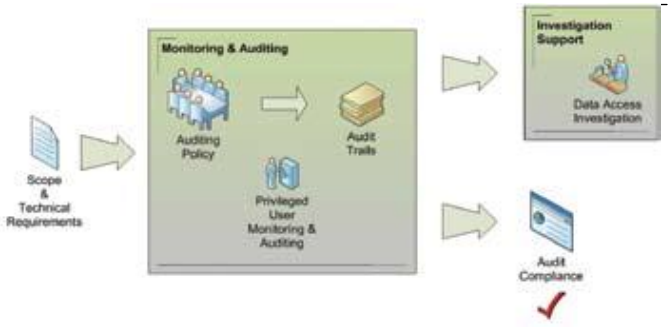


图3： 数据库活动监控 (DAM) 和审计用例。

5. 数据库活动监控 (DAM)。

实时监控数据库活动是有效避免受到攻击的关键所在，通过立即检测入侵和误用来实现。 例如，DAM 能够在出现异常访问模式时发出警报，从而指示 SQL 注入攻击、财务数据未授权更改、帐户特权提升以及通过 SQL 命令执行的配置更改。

监控特权用户也是数据治理法规的一项必备要求，如 SOX 和 PCI DSS 等数据隐私法规。 这对于检测入侵同样非常重要，因为攻击经常会为攻击者获取特权用户访问权限（如通过您的业务应用程序所拥有的凭证）。

DAM 也是漏洞评估的一项基本要素，因为它可让您超越传统的静态评估纳入“行为漏洞”动态评估，如多用户共享特权凭据或数据库登录失败次数过多。

“并非所有数据和所有用户创建时都均等。 您必须验证用户身份，确保对每位用户全权负责，并管理特权限制数据访问。”

最后，某些 DAM 技术会提供应用程序层监控，让您通过多层应用程序（如 PeopleSoft、SAP 和 Oracle e-Business Suite）而不是直接连接数据库检测欺诈行为。

6. 审计。

必须进行必需的安全审计跟踪，并且保持对影响安全状态、数据库完整性或敏感数据查看的所有数据库活动进行这种层次的跟踪。 除遵循主要合规要求外，具体审计跟踪对于取证调查同样至关重要。

绝大多数组织目前均采用利用传统本地数据库记录功能的某种形式的手工审计技术。 但是，用户往往发现这些方法存在不足，即由于手动工作导致复杂度大增及高昂的运营成本。其他缺陷包括运营费用高昂、缺乏职责分工（这是因为 DBA 能够轻易篡改数据库日志内容，进而影响不可否认性），同时需要购买和管理大存储容量，以便处理大量未经筛选的事务信息。

幸运的是，现已提供一系列新型的 DAM 解决方案，在最大限度地降低性能影响的情况下提供独立于 DBMS 的具体审计，同时通过自动化集中式跨 DBMS 策略和审计知识库、过滤和压缩降低运营成本。

7. 身份验证、访问控制和授权管理。

并非所有数据的性质都相同，也并非所有用户的权限均等。您必须验证用户身份，确保对每位用户全权负责，并管理特权限制数据访问。 同时，您应当强制执行这些特权，即使对享有最高特权的数据库用户也是如此。 您还需要将权利报告（也称作用户权利证明报告）作为正式审计过程的一个环节进行定期审查。

8. 加密。

使用加密技术呈现无法读取的敏感数据，以确保攻击者无法对数据库外的数据进行未授权访问。 这包括传输数据加密和静态数据加密，前者确保攻击者无法在网络层进行窃听以及在向数据库客户端发送数据时访问数据，后者确保攻击者即使有权访问媒体文件也无法提取数据。

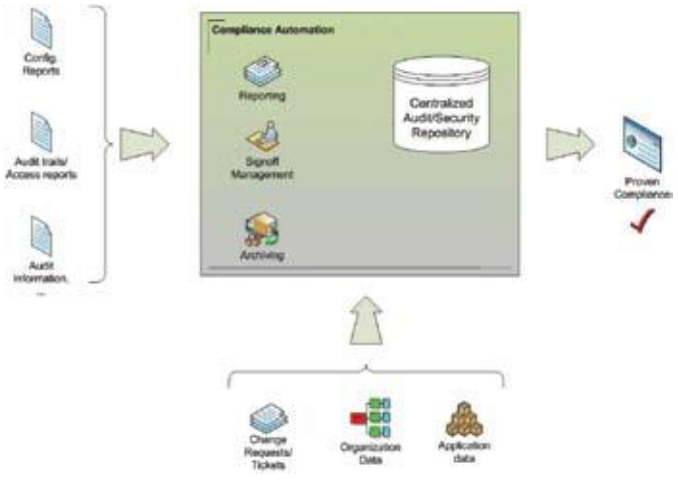


图 4： 管理整个合规生命周期。

八步实现数据库安全

1. 发现
2. 漏洞和配置评估
3. 强化
4. 更改审计
5. 数据库活动监控 (DAM)
6. 审计
7. 身份验证、访问控制和授权
8. 加密

关于作者

Ron Ben Natan 博士曾就职于 Merrill Lynch、J.P. Morgan、Intel 和 AT&T Bell Laboratories 等多家享有声誉的知名公司，拥有超过 20 年的企业应用程序和安全技术开发经验。 Ron 还曾担任 Phillip Morris、Miller Beer、HSBC、HP、Applied Materials 和 Swiss Armed Forces 的数据安全和分布式系统顾问。

作为 IBM 的金牌顾问，拥有计算机科学博士学位，Ron 在分布式应用程序环境、应用程序安全和数据库安全领域是当之无愧的专家。 迄今为止他已获得 12 项专利，并撰写了 12 本技术书籍，包括《*Implementing Database Security and Auditing*》（Elsevier Digital 出版社出版），即该领域的标准范本，以及 2009 年出版的 Ron 的最新著作《*HOWTO Secure and Audit Oracle 10g and 11g*》（CRC 出版社出版）。

关于 IBM InfoSphere Guardium

InfoSphere Guardium 是采用最为广泛的数据中心信息泄露预防解决方案，从而确保企业数据的完整性。 全球各地有超过 400 位企业客户安装了该解决方案，其中包括全球五大银行、六大保险公司的其中四家、多家顶级政府机构、三大零售商的其中两家、二十大世界顶级电信运营商、两大全球知名的饮料品牌、最知名的 PC 品牌、三大汽车制造商、三大航空航天公司以及一家主要商业智能软件供应商。 InfoSphere Guardium 是弥补核心数据安全空白的首要解决方案，通过提供跨 DBMS 的可扩展性企业平台实时保护数据库并自动完成整个合规审计流程。

Guardium 是 IBM InfoSphere 的一个组成部分，是一种定义、集成、保护和管理跨系统受信任信息的集成式平台。InfoSphere 平台可提供所有受信任信息功能构建基础构建块，包括数据集成、数据仓库、主数据管理和信息治理，所有这一切均围绕共享元数据和模型这一核心进行集成。 该产品组合为模块化组合，因而您可以随时随地开始构建，并可混合 InfoSphere 软件构建块并将其与其他厂商提供的组件进行匹配，或选择将多个构建块部署在一起以提高速度及提升价值。InfoSphere 平台可为信息密集型项目提供企业级基础，同时提供简化各种艰巨挑战所需的性能、可扩展性、可靠性和速度提升，更加迅速地为您的企业提供受信任信息。

IBM Corporation
Route 100
Somers，NY 10589

在美国印刷
2010 年 5 月

InfoSphere®
软件

IMW14277-CAEN-01