8步实现整体数据库安全

作者: Ron Ben Natan, 哲学博士,
IBM子公司Guardium CTO

计算机攻击、内部人员违法行为，以及各种监管要求，正促使组织寻求新的途径来保护其在商业数据库系统(比如Oracle、Microsoft SQL Server、IBM DB2和Sybase)中的企业和客户数据。本文探讨8项重要的最佳实践，提供一种整体方法来同时保护数据库和实现对关键法规(比如SOX、PCI-DSS、GLBA和数据保护法律)的遵从。

保护数据库并实现法规遵从

经济利益驱使下的攻击、内部人员的违法行为，以及各种法规要求正促使组织寻求新的途径来保护他们的企业和客户数据。

全球大部分敏感数据都存储在商业数据库中，比如Oracle、Microsoft SQL Server、IBM DB2和Sybase，这使数据库日渐成为最主要的犯罪目标。这也许可以解释为什么在2008年SQL注入攻击数量猛增了134%，从平均每天数千次增加到每天数十万次(根据IBM最新发布的报告[1])。

更严重的是，据Forrester [2]报告，60%的企业没有及时应用数据库安全性补丁，而据IBM分析，在2008年发现的所有Web应用漏洞中的74% (其中SQL注入漏洞占绝大多数)到2008年末还甚至还没有可用的补丁。

"您无法防御未知的攻击。您需要很好地安排您的敏感资产，无论是数据库实例还是数据库中的敏感数据。"

但是，在以前，绝大部分注意力都集中在保护网络边缘和客户端系统上(防火墙、IDS/IPS、反病毒软件等)我们现在正步入一个崭新的阶段，在这一阶段里，信息安全专业人员的使命是，确保企业数据库免遭破坏与未经授权的操作。

以下列出了8项重要的最佳实践，提供了一种整体方法来同时保护数据库和实现对关键法规(比如SOX、PCI DSS、GLBA和数据保护法律)的遵从。

1. 发现

您无法防御未知的攻击。您需要很好地安排您的敏感数据，无论是数据库实例还是数据库中的敏感数据。而且，您应该自动化发现流程，因为敏感数据的位置不断在变化，这源自于新的或修改的应用、合并和收购等因素。

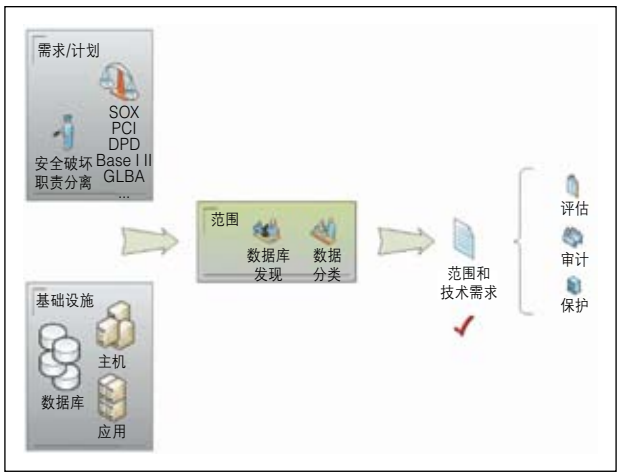

图1: 使用发现工具帮助自动实现。您需要规划数据库实例，以及您的敏感数据的存放位置。

有趣的是，一些发现工具还能够发现SQL注入攻击在您的数据库中放置的恶意软件。除了暴露机密信息，SQL注入漏洞还使攻击者能够在数据库中嵌入其他攻击代码，然后攻击访问网站的用户。

2.漏洞和配置评估

您需要评估数据库配置，确保它们不存在安全漏洞。这包括验证在操作系统上安装数据库的方式(比如检查数据库配置文件和可执行程序的文件权限)，以及验证数据库自身内部的配置选项(比如多少次登录失败之后锁定帐户，或者为关键表分配何种权限)。此外，您需要确认您没有运行带有已知漏洞的数据库版本。

1 "IBM Internet Security Systems X-Force? 2008 Trend & Risk Report"，IBM Global Technology Services，2009年1月。

2 "Market Overview: Database Security"，Forrester Research，2009年2月。

传统网络漏洞扫描程序并不是针对这一目的而设计的，因为它们没有嵌入关于数据库结构和预期行为的知识，它们也不能发起SQL查询(通过需要凭证的数据库访问)来揭示数据库配置信息。

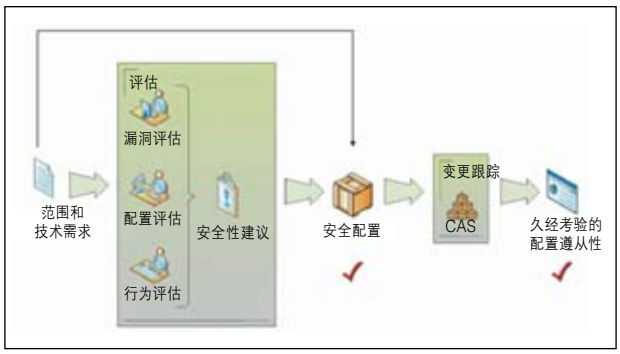

图2: 漏洞评估和变更跟踪用例。

3. 加强保护

通过漏洞评估，得到的通常是一些具体的建议。这是加强数据库保护的第一步。加强保护的其他要素还包括删除不使用的所有功能和选项。

4. 变更审计

一旦创建了加强了安全保护的配置，就必须持续跟踪它，确保您没有偏离您的“黄金”(安全)配置。可以通过变更审计工具来完成这一任务，这些工具能够比较配置的快照(在操作系统和数据库两个级别上)，并在发生可能影响数据库安全的变更时，立即发出警告。

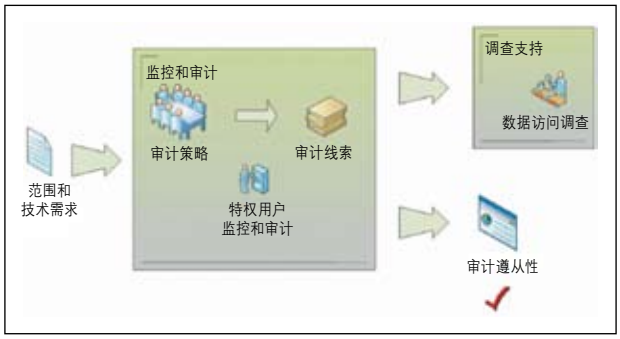

图3: 数据库活动监控(DAM)和审计用例。

5. 数据库活动监控(DAM)

对于通过及时检测入侵和误用来限制信息暴露，实时监控数据库活动非常重要。例如，DAM可以警告暗示着SQL注入攻击的异常访问模式、对财务数据的未授权更改、帐户特权提升，以及通过SQL命令执行的配置变更。

监控特权用户也是SOX等数据治理法规和PCI DSS等数据隐私法规的一项要求。检测入侵也很重要，因为攻击经常会让攻击者获得特权用户访问权限(比如通过由您的业务应用所有的凭证实现)。

DAM也是漏洞评估的一个重要要素，因为它支持您超越传统静态评估，以包括对“行为式漏洞”(比如多个用户共享特权凭证或者数据库登录失败次数过多)的动态评估。

“不是所有数据和所有用户都是使用同等的方式创建的。您必须对用户进行身份验证，确保每个用户拥有完整的责任，并通过管理特权来限制对数据的访问。”

最后，一些DAM技术提供了应用层监控，允许您检测通过多级应用(比如PeopleSoft、SAP和Oracle e-Business Suite)执行的欺诈行为，而不是通过直接连接数据库执行的欺诈行为。

6. 审计

必须为影响安全性状态、数据完整性或敏感数据查看的所有数据库活动生成和维护安全、防否认的审计线索。除了是一种重要的遵从性要求，拥有细粒度审计线索对于法庭调查也很重要。

幸运的是，现在有了一类新的DAM解决方案，以极低的性幸运的是，现在有了一类新的DAM解决方案，以极低的性能影响提供了细粒度、与DBMS独立的审计，同时通过自动化、集中的跨DBMS策略和审计存储库、过滤和压缩降低了操作成本。

大部分组织目前都采用手动审计形式，利用传统的本机数据库日志功能。但是，这些方法经常难以实施，因为它们实施起来很复杂，而且手动操作还具有很高的操作成本。其他缺点包括较高的性能开销、缺乏职责分离(因为DBA可以轻松地篡改数据库日志的内容，进而影响防否认性)，还需要购买和管理大量存储容量来处理大量未

经过滤的事物信息。

7.身份验证、访问控制和授权管理

不是所有数据和所有用户都是使用同等的方式创建的。您必须对用户进行身份验证，确保每个用户拥有完整的责任，并通过管理特权来限制对数据的访问。您还应该强制实施这些特权，即使是对于特权最高的数据库用户。您还需要定期审核授权报告(也称为“用户权利证明报告)，将其作为正式审计流程的一部分。

8. 加密

使用加密来以不可读的方式呈现敏感数据，这样攻击者就无法从数据库外部对数据进行未授权访问。这包括对传输中的数据进行加密，使攻击者无法在网络层窃听信息并在将数据发送到数据库客户端时访问数据，还包括对静止数据进行加密，使攻击者无法提取数据，即使能够访问媒体文件。

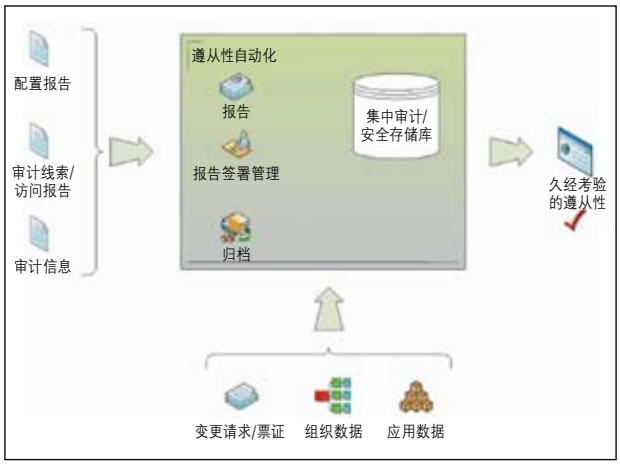

图4: 管理整个遵从性生命周期。

8步保障数据库安全

1. 发现

2. 漏洞和配置评估

3. 加强安全保护

4. 变更审计

5. 数据库活动监控(DAM)

6. 审计

7. 身份验证、访问控制和授权管理

8. 加密

关于作者

Dr. Ron Ben Natan拥有超过20年为Merrill Lynch、J.P. Morgan、Intel和AT&T Bell Laboratories等顶尖公司开发企业应用和安全技术的丰富经验。Ron还是Phillip Morris、Miller Beer、HSBC、HP、Applied Materials和瑞士武装部队在数据安全和分布式系统方面的顾问。

作为拥有计算机科学博士学位的IBM金牌顾问，Ron是分布式应用环境、应用安全和数据库安全方面的专家。他拥有12项专利并撰写了12部技术图书，包括Implementing Database Security and Auditing (Elsevier Digital Press) (这是该领域的一部标准著作)，以及于2009年出版的Ron的最新图书HOWTO Secure and Audit Oracle 10g and 11g (CRC Press)。

关于IBM子公司Guardium

Guardium是一家IBM子公司，致力于通过持续监控对高价值数据库的访问和变更来保护关键企业信息。Guardium可伸缩的平台通过针对异构基础设施的统一策略简化信息治理，同时通过自动化遵从性流程降低操作成本，支持企业安全地使用可信信息来推动更智慧的业务成果。

Guardium的企业平台现在已安装到全球超过450个数据中心中，包括5家全球顶级银行、6家顶级保险公司中的4家、3家顶级零售商中的2家、20家全球顶级电信公司、2家全球顶级饮料品牌、全球最著名的PC厂商、全球3大汽车制造商中的1家、全球3大航空公司中的1家，以及一家领先的商业智能软件提供商。Guardium是第一家通过可伸缩企业平台解决了核心数据安全问题的公司，既能够实时保护数据库，又能够自动化整个遵从性审计流程。

请回收利用

IMW14277-CAEN-00