

用Oracle9i保护你的电子商务

Oracle商业白皮书

2001年7月

用Oracle9i保护你的电子商务

执行概要

利用互联网从事商务活动的企业都面临着类似的选择 – 你如何能在利用互联网更开放更有效地从事商务活动的同时，仍然能安全地管理对你的至关重要的系统和数据的访问？由于互联网上存在的安全性漏洞，企业正面临着财务损失，失信于公众以及其他问题。而且，现在许多行业，如医疗保健，金融和电子商务正在强制性实施安全性规则和法律，以保护客户信息的隐私性。不遵守这些法规，如HIPAA和GLBA可能会导致高额的罚款，甚至监禁的处罚。毫无疑问，互联网安全性是各企业共同关心的问题，但他们究竟在这方面做了那些工作呢？

安全性是一个复杂的问题，但有许多企业并不清楚应从哪里开始？他们通常通过实施一些标准的安全性机制，如建立防火墙和加密网络等局部性措施来应付安全性问题。采取这样措施的企业目前就处在危险当中。

Oracle相信一个整体的安全性方案将会使由互联网安全性漏洞所带来的风险降低到最小。这就需要技术性解决方案和最优方法。令人惊讶不已的是，许多已知的安全性漏洞都可以经过一系列简单易行的最优方法得以防止。一个企业可以部署最安全的技术，但如果企业缺乏一套安全性制度，如强迫员工安全的管理密码，或委派专人跟踪缺陷，并迅速地将软件的补丁盘应用到系统等等，没有这种安全性举措，企业将始终处在危机之中。

整体的安全性方案可降低风险

作为电子商务本身，Oracle深刻理解潜伏在互联网周围的安全性问题的严重性，并且对保证关键系统和数据的安全需要什么也非常了解。Oracle在帮助客户部署安全的电子商务过程中所采取的一个途径就是，在我们的互联网基础性产品 – Oracle9i应用服务器和Oracle9i数据库中内置多层安全性。

Oracle已经与多家领先的安全性供应商，如Baltimore，Netegrity，Checkpoint以及其他企业等建立了合作伙伴关系，以保证他们的产品与Oracle环境良好的互换性。最后，Oracle安全性服务将通过安全性评定帮助客户，开发一套安全性策略，并通过对系统组件，如防火墙，非法入侵探知系统，电子邮件服务器以及Oracle9i等的安全配置，帮助客户设计和实施端到端的安全性。

安全性要求

为最大程度地降低风险，企业必须部署一些基本的安全性措施。应该注意，安全性不是一次性，易于识别的问题。它是一个必须利用审查，访问控制，新的抗攻击工具以及变更数据存储方式等方法进行持续性完善的过程。

- 超强认证
- 单一登录
- 精细的访问控制
- 密码系统
- 审核
- 防御侵害
- 安全性策略

Oracle为满足以上安全性需要所提供的整体安全性的具体体现是：

- Oracle9i - Oracle9i 数据库和 Oracle9i 应用服务器
- Oracle安全性服务

超强认证

通过互联网你可能看不到正在与谁做生意，所以在数字世界中存在着一种可以让系统识别身份的机制。用户名和密码的组合是一个系统认证和识别用户的最普遍或最基本的方式。一些企业认为，这种基础的，单向的认证方式并不十分安全，特别是当用户需要管理几个密码时更是如此。另一种方式，或者是认证的更安全的方式是所谓的超强认证。我们可以给出几个超强认证的例子，如X.509数字证书，证明卡和生物认证设备。Oracle9i支持基本认证和多种超强认证。

单一登录

管理多个账户以完成相关的工作任务将导致安全性的薄弱环节和高额的所有权成本。一般地，为完成每天的日常工作，一个员工要管理十四个密码或账户。为了应付“密码过多”的问题，员工可能会把密码抄写下来，或选择一个容易猜中的密码。人们经常忘记密码，并频繁地向帮助部门查询。系统管理员甚至面临者一个更大的问题。系统管理员需要花费大量的时间去管理分布于各种数据库，web服务器和网络上的这些账户。如果一个雇员离开了公司，而系统管理员没有注意删除所有的账户，一些老的账号可能就仍然处于激活状态。

这个问题的解决方案就是单一登录。单一登录可以使用户通过一个单一的登录过程就能访问所用被授权的应用。如果只管理一个密码或证明书，用户一般就不会把它记录下来，或选择一个不容易被猜中的密码。每个企业都应该有使雇员强制性选择安全密码的安全性策略。认证证书可以集中存储于一个LDAP目录，因此系统管理员可以在一个单独的地方管理这些账户。账户的集中化可以使系统管理员能更迅速地追加，删除和修正账户的工作。Oracle9i通过Oracle互联网目录LDAP集成提供了单一认证。Oracle9i也可以与其他第三方单一登录服务器的集成，如Kerberos 和 Netegrity。

精细的访问控制

互联网和在线服务目前已要求服务器能够实现精细的访问控制。如果您考虑数据库服务器将管理互联网上多团体用户的数据，数据库必须保证用户只能访问与它相关的数据，而不涉及其他的数据。例如，在线银行业务服务需要保证客户所访问的账户信息只能是他们自己的，而不能看到其他客户的信息。

能够控制对敏感信息的访问对需要满足隐私性需求的应用也由帮助。例如，医疗应用软件必须保证医生只能看到他们自己病人的记录。

因为数据库在传统上是在表的级别上分配权限，而不会控制在单独的记录或更低的级别，附加的应用代码可能被要求取得更精细的访问控制。传统方法的问题是如果用户利用应用之外的方式，如特别的查询工具等访问数据库，就可以绕过安全性设置。而且，维护复杂的访问控制代码会导致高额的开发和管理成本。

Oracle9i数据库的标签安全性组件是一个精细访问控制或行级别安全性的无限的解决方案。建立在Oracle虚拟个人数据库的工具包基础上的Oracle标签安全性向数据行中追加了一个特别的标记（标签），可以达到行级别的安全性。例如，在线服务可以使用一个订阅标签，它可以将存储于相同数据库服务器中的各企业的数据更安全有效的分离开。

密码系统

通过互联网从事商务活动需要通过网络传输信息。任何人，不论是黑客，解密高手还是不诚实的雇员，都可以下载一个信息包的嗅探器，当信用卡等这类敏感信息在网络中传输时，利用嗅探器可以捕获它们。不会好意的用户也可以利用一些途径获得对存储于服务器中的数据非法访问。为了防止对数据的非法访问，可以采用密码系统，利用信息的不规则性保护数据。它涉及数学的计算方法和钥匙键。公共钥匙键的基础结构是最普遍采用的方法。它为加密，数据整合，数字认证和数字签字提供了技术。

当数据在网络中的所有层，包括用户层，中间层和数据库层传输时，Oracle9i提供了网络中端到端的加密。Oracle9i应用服务器提供了网络中用户层和中间层的加密。Oracle9i数据库的高级安全性组件提供了网络中中间层和数据库层的加密。为了强化性能，Oracle通过Oracle与RSA的BSAFE库的集成，支持BHAPI的接口。Oracle9i也对存储于Oracle9i数据库内部的数据提供加密。对于非常敏感信息如信用卡号的加密，如果有对数据非法访问的企图或摆脱数据库控制的企图，如通过操作系统，可在数据库中追加一个额外的保护层。

审核

审核是普遍使用的最有效的安全性机制，它可以保证系统的合法用户能完成他们应该从事的工作，同时又限制他们对权限的滥用。通过审核，企业可以跟踪用户的活动，从而发现安全性的漏洞。而且，用户如果知道他们正受到跟踪，他们也不愿意滥用他们的权限。因为传统的审核将产生大量的数据，因此也很难发现有用的信息，Oracle9i引进了精细的审核。利用精细的扩展审核，安全性漏洞将会非常容易被发现。例如，如果建立了一个审核策略用于重复性筛选信用卡号，就会自动生成一个警告，警告系统管理员可能的入侵。系统管理员可根据这些警告做出响应，如终止非法数据库的对话。

防御侵害

具有防御侵害的IT基础结构可以保证数据和服务随时随地的有效性。一个IT基础结构由许多方面组成，每一次向系统中追加新的用户，新的软件，或新的硬件都会潜在地生成一个安全性漏洞。为了将风险降低到最小程度，企业需要购买的基础结构产品应该是安全和集成的，可经常性的扫描安全性漏洞并能捕捉到入侵，可以立即对安全性漏洞做出反应，如果受到了损失，也要把它降低到最小。

利用**Oracle9i**，为部署电子商务应用，只需要两个集成的基础结构产品，即**Oracle9i**数据库和**Oracle9i**应用服务器。需要安装和维护的集成产品越少，薄弱环节就越少。而且，**Oracle9i**在互联网基础结构的所有层提供了多层安全性普及，因此对一个机制的挖掘危及道关键数据的安全。而且，**Oracle**的产品已经经历了独立的评定机关完成的全面测试，包括安全性保证的公用基准和**FIPS-140**。从十三个安全性评估获得的“认可图章”使得**Oracle9i**不再容易受到攻击。

在**Oracle**的环境之外，使入侵可以降低到最小程度的方式包括经常性的侵入力测试，网络中的入侵监测和安全的路由器和防火墙配置等。**Oracle9i**还可以与**ISS**，**Cisco**，和**Checkpoint**等供应商的网络安全性产品相集成。**Oracle**安全性服务有助于配置网络安全性，因此所有的系统组件都可以安全可靠地在一起工作。

安全性策略

安全性策略定义了一个企业将如何保护她自己。它涉及评定企业中哪些信息是有价值的，决定谁将使用它们以及如何保证它们的安全。它驱动安全性需求，决定需要什么技术，并定义使整体的风险降低到最小程度的最佳方法和程序。**Oracle**安全性服务将能够在开发企业安全性策略方面提供帮助。

结论

利用**Oracle**，许多薄弱环节可以克服，通过互联网从事商务活动的风险可以降低到最小程度。利用**Oracle9i**和**Oracle**安全性服务，**Oracle**已经在本行业推广了建立最安全数据库的专门技术，以便于在本行业中建立最安全的互联网基础结构。与信息安全性的领先者**Oracle**在一起，您完全可以信赖您的商务关键数据。



用Oracle9i保护你的电子商务
商务白皮书
2001年7月
作者: Mona Patel
Oracle 公司
全球总部
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

全球咨询:
电话: +1.650.506.7000
传真: +1.650.506.7200
www.oracle.com

Oracle是Oracle公司的注册商标。本文所提到各种产品和服务的名称可能是Oracle公司的商标。本文所涉及的所有其它的产品和服务名称可能分别是它们所有者的商标。

Copyright © 2001 Oracle Corporation
All rights reserved.