

**RSA[®]CONFERENCE
C H I N A 2012**

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑



业务及数据库安全风险分析

范渊

杭州安恒信息技术有限公司

专题会议主题：业务及数据库安全风险分析

专题会议分类：安全业务——中级



RSA CONFERENCE
C H I N A 2012

议题背景：

敏感数据泄露频繁爆发！

数据安全令人担忧！

——范渊

杭州安恒信息技术有限公司

专题会议主题：业务及数据库安全风险分析

专题会议分类：安全业务——中级



RSA CONFERENCE
C H I N A 2012

1、世界500强泄密事件

C114中国通信网: 门户(微博) - 论坛(微博) - 人才(微博) - 博客 - 商情 - 百科 - IDC产业联盟

C114 新闻 | 新闻 - 电信运营商 - 中

中移动吉祥号用户被

http://www.c114.net/2011/5/21...
● 主页 > 新闻 > 要闻 >

吉祥
祥手

中国移动“内

http://v

一桩“私家侦探”敲诈勒索案，而倒卖用客户个人信息，一条黑不足。

内虚增积分的同时，

时候，才发现了问题，

工，由于工作上需要处理

励长



2、互联网企业泄密事件

| 企业名称 | 泄露账号数量 | 泄露信息 |
|----------|-------------------------|--|
| CSDN | 6,428,632个帐号。 | 帐号、明文密码、电子邮件 |
| 多玩 | 8,305,005个帐号。 | 帐号、MD5加密密码、部分明文密码、电子邮件、多玩昵称 |
| 178.COM | 1,883,487个帐号，仍不断增加。 | 帐号、MD5加密密码、全部明文密码、电子邮件、178昵称(178账户通用NGA) |
| 天涯 | 9,695,513个帐号(预计超4千万数据)。 | 帐号、明文密码、电子邮件 |
| 人人网 | 4,768,600个帐号。 | 明文密码、电子邮件 |
| UUU9.COM | 7,513,773个帐号。 | 帐号、MD5加密密码、部分明文密码、电子邮件、U9昵称 |
| 网易土木在线 | 约4.3GB，137个文件。 | 帐号、邮箱、MD5密码、其他相关数据 |
| 梦幻西游 | 约1.4G(木马盗取)。 | 帐号、邮箱、明文密码、角色名称、所在服务器、最后登陆时间、最后登陆IP |
| 新浪微博 | 帐号数未知，疑似文件1个。 | 邮箱、明文密码 |
| 麒麟网 | 9,072,966个帐号。 | 帐户、明文密码 |
| 某婚恋网站 | 5,261,302个帐号。 | 帐户、明文密码 |

数据泄密事件有何启发？

92%

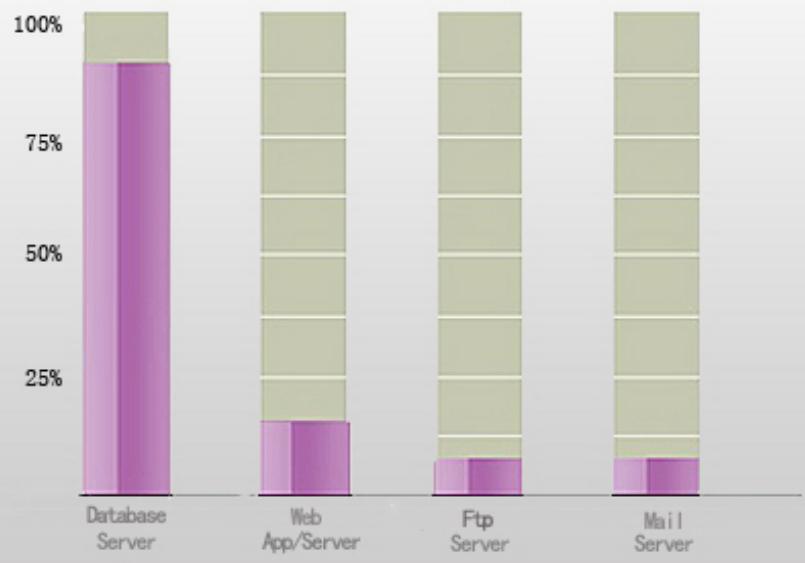
数据泄漏来源于



了解更多 →

来自verizon的数据支持！

Verizon 2010年度数据泄漏调查报告



专题会议主题：业务及数据库安全风险分析

专题会议分类：安全业务——中级

RSA CONFERENCE
C H I N A 2012

数据库面临安全风险TOP10

TOP 1.帐号授权不合理，越权操作严重

TOP 2.帐号复用与滥用

TOP 3.脆弱的web应用

TOP 4.数据库漏洞和配置不合理

TOP 5.身份验证措施薄弱

TOP 6.备份管理不足

TOP 7.审计措施不力

TOP 8.缺失有效加密措施

TOP 9.安全域规划不合理

TOP 10.服务器操作系统漏洞与配置不合理



——范渊

专题会议主题：业务及数据库安全风险分析

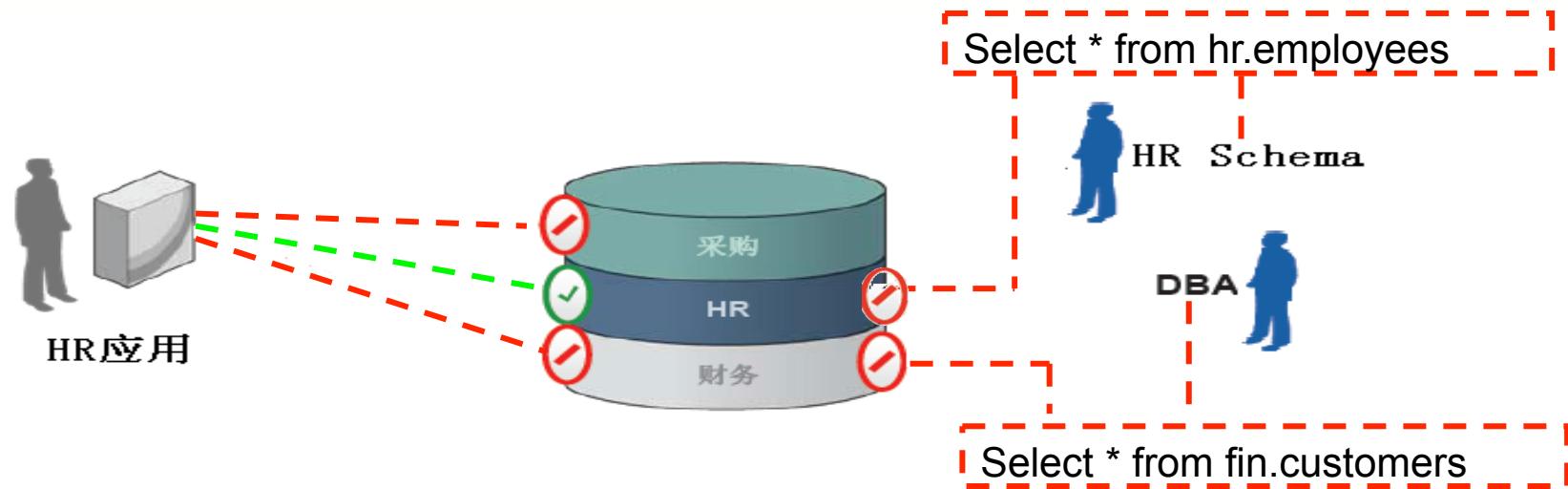
专题会议分类：安全业务——中级



RSA CONFERENCE
C H I N A 2012

威胁1：帐号授权不合理

- 内控规定DBA不允许访问业务数据，但我们没有办法控制
- 业务开发人员不应具备建表、查看业务数据权限；
- 最小权限原则由于其过于复杂无法实施。



威胁1：帐号授权不合理

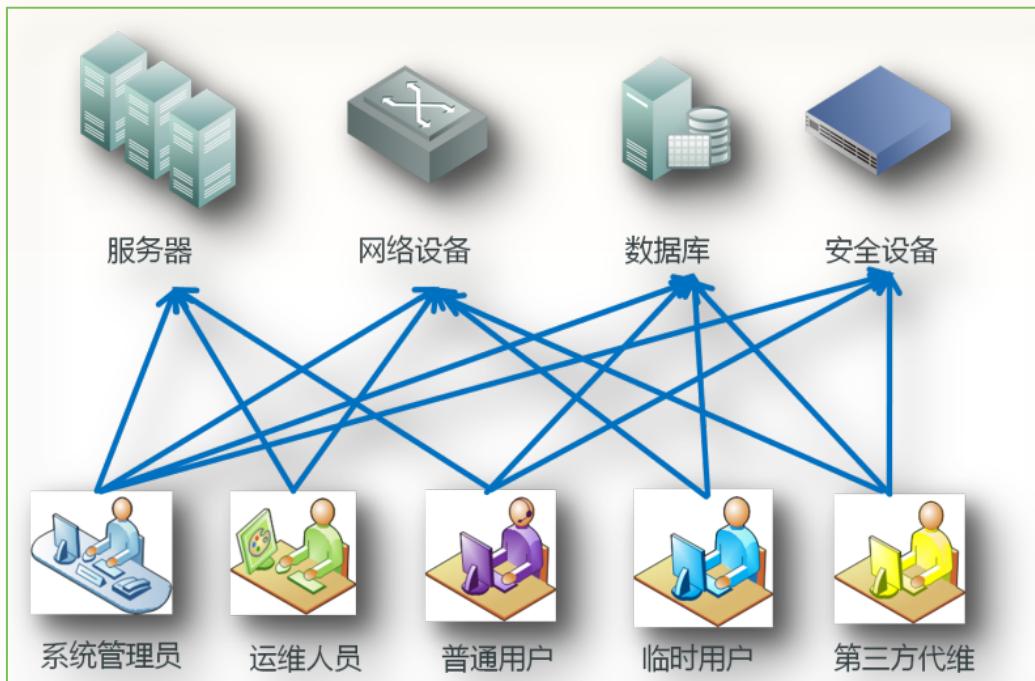


典型越权操作案例：

- 1、开标前30分钟，越权查看投标商报价；
- 2、通知合作投标商，以低于次低价几十元报价，协助其中标；

由于第三方人员权限过大导致的泄密事件数不胜数！

威胁2：帐号复用和帐号滥用

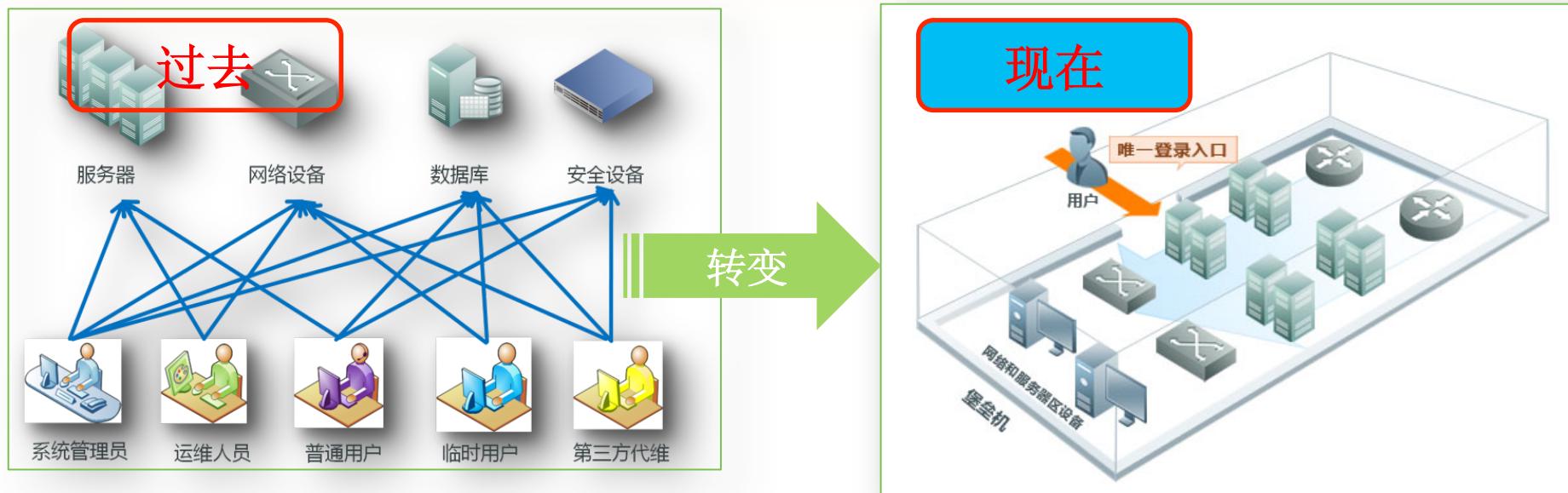


数据库管理现状：
一个帐号多人使用；
多台设备共用密码；
应用系统帐号个人使用；

威胁2：帐号复用和帐号滥用——改进建议

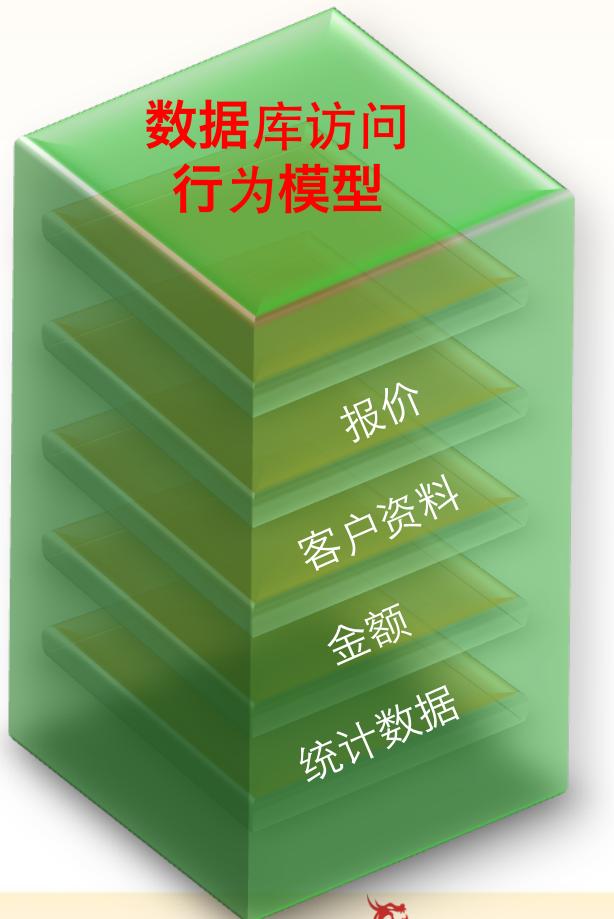
建立集中运维安全管理平台

- ✓ 逻辑上将人与目标设备分离，全局唯一身份标识，隐藏设备管理帐号密码；
- ✓ 转变传统IT安全运维的被动响应模式，建立面向用户的集中、主动的安全管控模式；



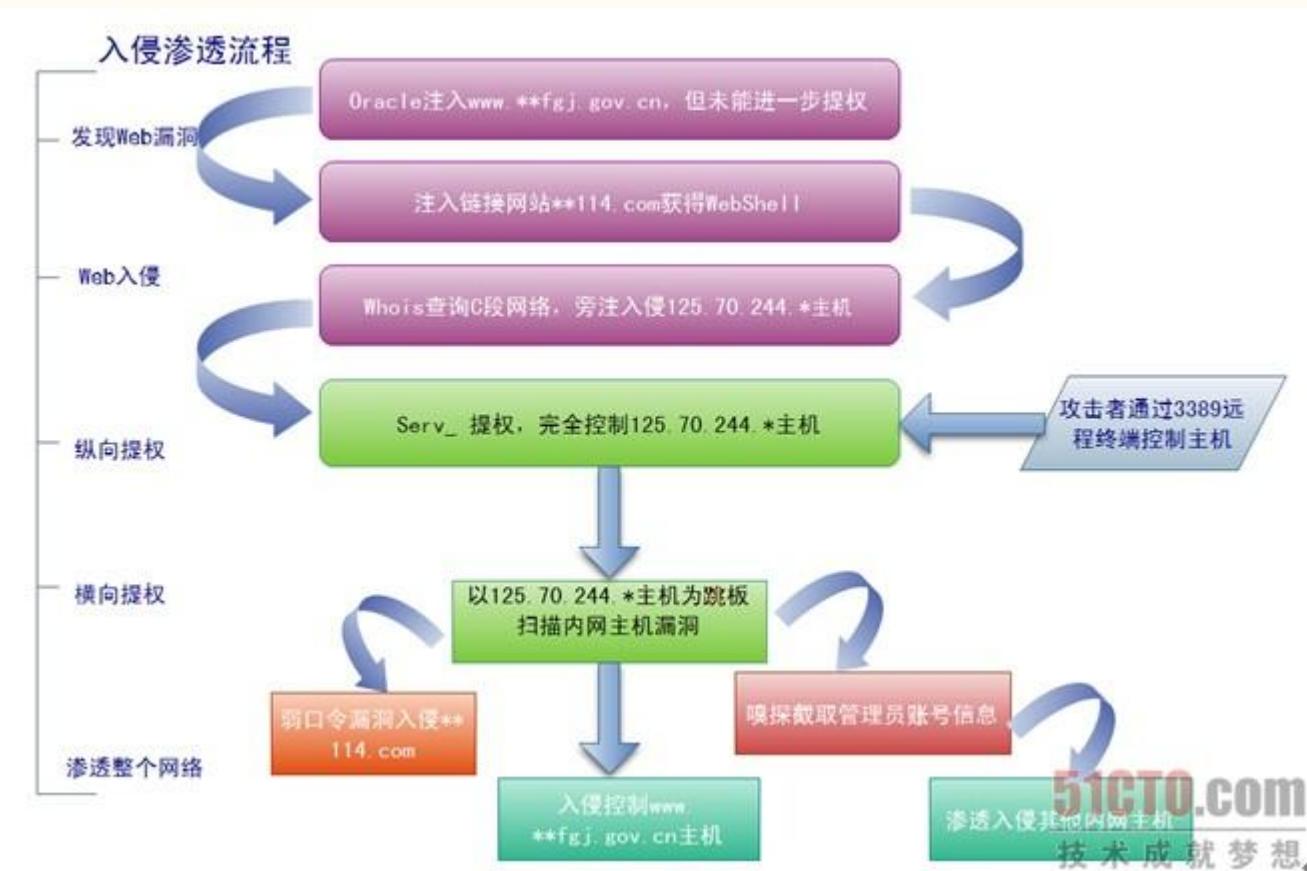
威胁2：帐号复用和帐号滥用——改进建议

持续监控审计构建数据库访问行为模型，梳理帐号权限！



威胁3：脆弱的web应用

- 85%以上的黑客攻击入口是脆弱的web系统



威胁3：脆弱的web应用——改进建议

- 建立有效的web防御体系（WAF和网页防篡改）

预警

短期间检测到大量攻击自动告警
安全态势跟踪

防护

已知的攻击、已知的漏洞
已知的正常访问方式

分析

应用程序：错误分析、延时分析、流量分析、用户群分析
安全分析：攻击态势、攻击目标分析、攻击源分析
安全分析：代码质量问题，编码规范问题

加固

已知应用漏洞加固
已知访问权限调整

威胁4：身份验证措施薄弱

| 弱口令 | |
|-------|--------------------------------------|
| 弱口令 | |
| 危险级别: | 紧急 |
| 类别: | 弱口令 |
| 描述: | 即容易破译的密码，像简单的数字组合如12345或者与帐号相同的数字组合成 |
| 改进建议: | 把口令改为不易猜解的强口令，强口令的基本要求包括足够的长度以及多种字符 |
| 影响平台: | oracle 8i,9i,10g,11g |
| 背景信息: | |

众多数据库帐号被破解！而且多个帐号使用同样密码！

| name | password | state |
|---------------------|---------------|------------------|
| _NEXT_USER | CHANGE_O***** | OPEN |
| XDBADMIN | WM*** | OPEN |
| XDB | CHANGE_O***** | EXPIRED & LOCKED |
| WM_ADMIN_ROLE | CHANGE_O***** | OPEN |
| WM\$SYS | CHANGE_O***** | EXPIRED & LOCKED |
| WKUSER | CHANGE_O***** | OPEN |
| WK\$SYS | CHANGE_O***** | EXPIRED & LOCKED |
| WKPROXY | CHANGE_O***** | EXPIRED & LOCKED |
| SH | CHANGE_O***** | OPEN |
| SELECT_CATALOG_ROLE | | |

威胁4：身份验证措施薄弱

1. 销售专业统方工具！
2. 可实现全国大部分HIS系统统方！
3. 方便易用，无需专业IT技能！



威胁4：身份验证措施薄弱

这就是为什么医院频繁出现泄密事件的主因之一！

宁波先进医院医生回扣单曝光 回扣占药价两成

2010-05-30 02:35:11 来源：京华时报（北京） 跟贴 2319 条 手机看新闻

核心提示：近日，一张用药清单曝光：“每开出一支通用名为氨曲南的药品，医生可拿到6.5元的回扣”。而惊现“回扣清单”的医院，是刚刚获得“2009年宁波市卫生作风建设先进单位”称号的宁波市第一医院。目前，医院已将库存品全部退回公司，并对当事医生进行诫勉谈话。



dǎo dí
导读

2010年10月26日，《新京报》接到匿名举报，指北京肿瘤医院两位医生收受医药代表回扣，随信附有视频光盘一张和相关文字材料。由此药品回扣再次走入普通大众的视野，也让早已见惯不惊的医界同行，不得不再一次深深体味医生的处境和中国医改的困境。请随我们走进本期的丁香观察……

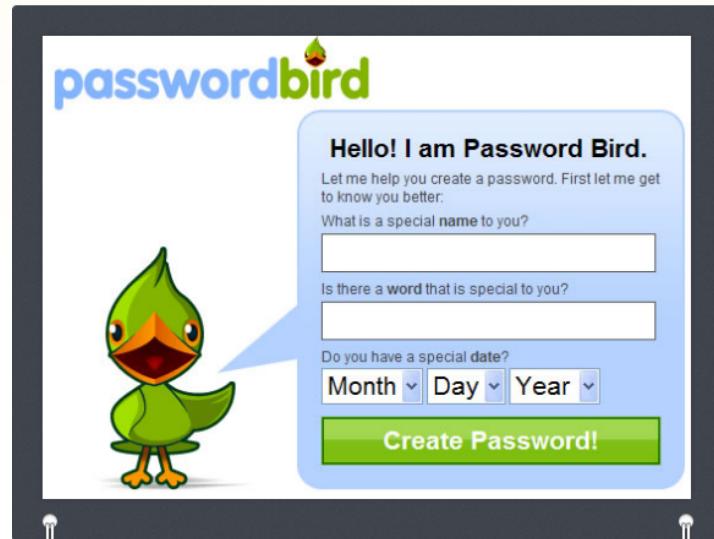
| 医生工号 | 医生姓名 | 门诊 | 001氨曲南0.5g/0.5g |
|----------------------------|------|--------|-----------------|
| 1701 | 张群峰 | 内科 | 16 816.4 |
| ✓3909 | 孙树琪 | 内科 | 43 1226.9 228.4 |
| ✓3907 | 史文鹏 | 内科 | 56 1638.8 754.1 |
| ✓1702 | 高军 | 内科急诊 | 33 1845.9 619.4 |
| ✓1702 | 廖丹江 | 内科急诊 | 34 2026.2 619.4 |
| 1712 | 王宇 | 内科急诊 | 21 1833.5 |
| 1703 | 赵晋海 | 内科急诊 | 44 1811.4 |
| ✓1702 | 陈以春 | 内科急诊 | 34 881.4 |
| 1707 | 孙伟 | 内科急诊 | 21 807.5 |
| 1741 | 朱静娟 | 内科急诊 | 31 1123.3 |
| ✓1209 | 丁香杰 | 内科门诊 | 42 1296.6 >75.4 |
| ✓4005 | 孙加坤 | 皮肤科 | 34 473.2 |
| 4409 | 章翠 | 皮肤科 | 24 713.6 |
| 1207 | 甘丁耀 | 眼科 | 31 1845.9 |
| 2716 | 张春行 | 外科急诊 | 34 217.6 |
| 2410 | 周晓冬 | 小外科 | 41 1335.3 |
| 2108 | 朱丽 | 普外科 | 21 275.3 |
| 2300 | 董立群 | 外科 | 16 516.8 |
| 总额: 001氨曲南0.5g/0.5g | | | |
| 医生工号 医生姓名 门诊 | | | |
| 3113 | 丁慧青 | 产科 | 14 462.2 |
| 3114 | 吴超杰 | 肝胆胰外科二 | 33 326.4 |
| ✓2115 | 薛晶 | 牙科综合科一 | 33 1152.1 154.4 |
| ✓2101 | 孙利娟 | 肝胆胰外科二 | 24 2446.4 279.4 |
| ✓2111 | 宋惠玲 | 肝胆胰外科二 | 31 2842.4 279.4 |
| 2254 | 林晓平 | 肝胆胰外科二 | 31 1822.8 |
| 2312 | 杨晓 | 肝胆胰外科二 | 21 3231.0 |
| ✓2111 | 吴夕 | 肝胆胰外科二 | 21 2520.5 61.4 |
| ✓2103 | 曹智 | 肝胆胰外科二 | 20 2879.7 206.4 |
| ✓2119 | 吴海燕 | 肝胆胰外科二 | 32 2371.4 61.4 |
| 3181 | 李永翠 | 肝胆胰外科二 | 24 1052.4 |
| ✓0706 | 姚益民 | 肝胆胰外科二 | 20 9899.4 179.4 |
| ✓2006 | 薛洪莉 | 肛肠外科 | 21 1261.5 239.4 |
| 3105 | 郭晓红 | 肛肠外科 | 13 2302.2 44.4 |

安恒信息

DB APP
Security

威胁4：身份验证措施薄弱——改进建议

1、复杂的密码策略



2、双因子认证



- 利用扫描软件定期评估数据库密码健壮性！
- 通过审计监督“密码修改”也非常有必要！
- 隐藏设备的密码也很重要！

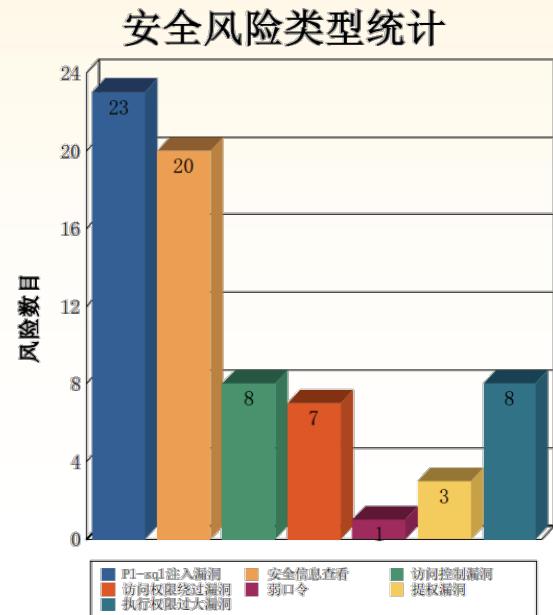
威胁5：数据库漏洞和配置不合理

甲骨文数据库曝漏洞遭黑客远程访问

2011-03-11 13:09 天虹 赛迪网 我要评论(0) 字号:T | T 收藏 +

甲骨文是全球最大的数据库软件公司，实力是相当强大，技术方面也是很先进的，引导着整个数据库行业的发展，尽管甲骨文数据库如此强大，可是也有漏洞，而黑客则是见洞就插，有报道称甲骨文数据库曝漏洞遭黑客远程访问。

AD:



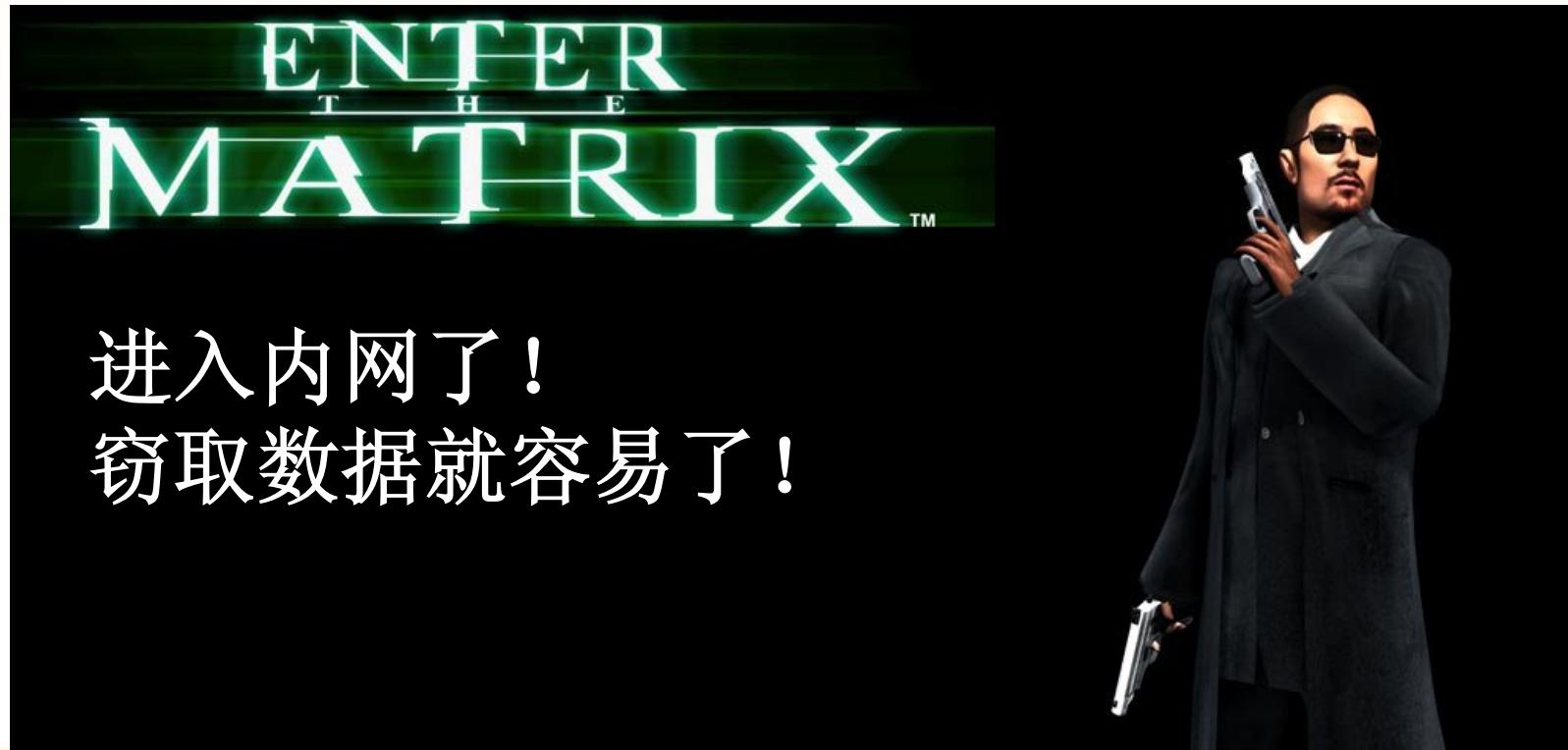
- 数据库的漏洞并不少见，但了解度比系统漏洞要低很多！
- 当然更重要的是数据库配置不合理！

威胁5：数据库漏洞和配置不合理

- 数据库常见配置不合理性说明：
- 数据库版本信息泄漏；
- 数据库默认帐号密码没有修改；
- 密码规范没有启用（密码生存周期、长度、锁定策略等）
- 无关帐号、过期帐号未锁定、删除；
- 公共权限（public）用户组授权不合理；
- 访问权限绕过漏洞；

威胁6：数据库服务器操作系统漏洞

- 操作系统漏洞大家都最熟悉不过了！但由于数据库的特殊性，其漏洞往往没有进行任何的修补！



威胁6：数据库服务器操作系统漏洞



威胁6：数据库服务器操作系统漏洞

——改进建议

RSACONFERENCE
C H I N A 2012

- 1、定期开展操作系统漏洞和数据库漏洞扫描
- 2、开展专业安全评估和风险加固服务



任务详细报告

数据库地址:

172.16.254.129

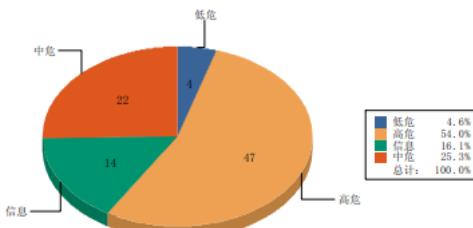
扫描主机信息:

被检测数据库所在主机信息，如下表所示：

| | |
|---------|------------------------|
| 数据库名 | : 172.16.254.129:1521 |
| 安全风险总数 | : 87 |
| 数据库安全值 | : 30 |
| 开始扫描 | : 2011-6-10 12:40:05 |
| 结束扫描 | : 2011-6-10 12:40:18 |
| 扫描用时 | : .00分13.00秒 |
| 服务器信息 | : 172.16.254.129/snake |
| 协议 | : |
| 端口 | : 1521 |
| 成功检测策略数 | : 386 |
| 安全策略总数 | : 386 |

按风险危害等级统计图表:

对于172.16.254.129 / snake / 2011-06-10 12:40:05



安恒信息

DB APP  security

23

RSA信息安全大会2012

威胁7：备份管理不足

备份措施不足

- 1、缺少安全有效的备份措施：还有大部分企业采用简单复制文件进行备份
- 2、备份数据未进行加密：对于包含用户资料等敏感信息的数据未加密

- 1、备份数据存放位置不对：比如备份文件存放在本机或者web服务器，备份介质丢失
- 2、备份系统管理不善：备份任务计划是否执行成功？非法备份经常发生？
- 3、备份数据的有效性未经检验：从未进行备份数据恢复演练

备份管理不善

威胁7：备份管理不足

雅虎回应“备份是企业自己问题”

雅虎日本系统出故障：近5700家企业数据丢失

2012年06月26日 20:26

来源：凤凰科技 作者：若水

0人参与 0条评论 转发 字号:T | T

凤凰网讯 北京时间6月26日消息，据国外媒体EconomicTimes网站报道，**雅虎**日本今天声称，上周，由位于大阪的旗下一家子公司Firstserver运营的一个出租服务器发生系统故障，导致5698家企业数据丢失，数据当中包括这些公司的网站信息内容。

Firstserver在其网站发布信息称，“非常抱歉，我们已确信这些数据无法恢复”。Firstserver还称，目前其无法重装系统，公司计划将对客户进行补偿。

威胁7：备份管理不足——改进建议



威胁8：审计措施不力



| | | |
|---|--|---|
| <h3>无审计</h3> <p>大部分企业都还没有任何审计措施，特别是核心数据库系统。</p> | <h3>审计有缺陷</h3> <p>部分企业开启了数据库自身审计，但是其详细度、可信度不足。</p> | <h3>缺乏审计分析</h3> <p>审计设备成为摆设也是很普遍的问题，有不重视、也有审计设备分析不足等原因。</p> |
|---|--|---|

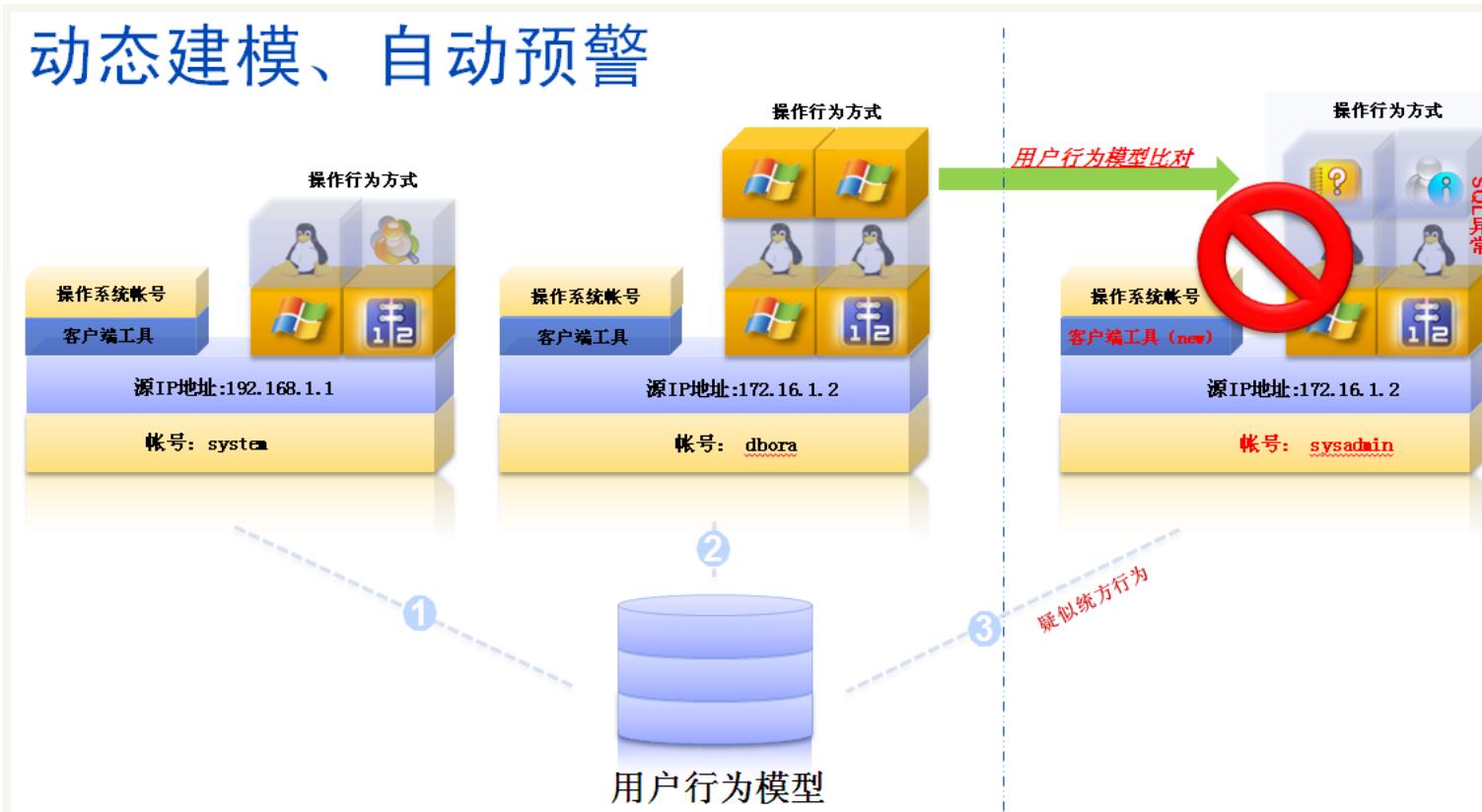
威胁8：审计措施不力——改进建议

- 首先需要有审计，包括数据库审计、web审计、运维审计，综合日志审计等；
- 审计设备的选择尤为重要
 - 厂家实力：能否提供整体审计解决方案
 - 关联分析能力：不同日志、不同设备是否能够关联
 - 规则分析能力：是否支持细粒度分析？是否有默认规则库？
 - 性能：数据库、web日志量非常大，性能要求高
 - 分析报表：报表是否有价值，是否丰富多样

威胁8：审计措施不力——改进建议

- 智能学习建模，自动形成规则

动态建模、自动预警



威胁8：审计措施不力——改进建议

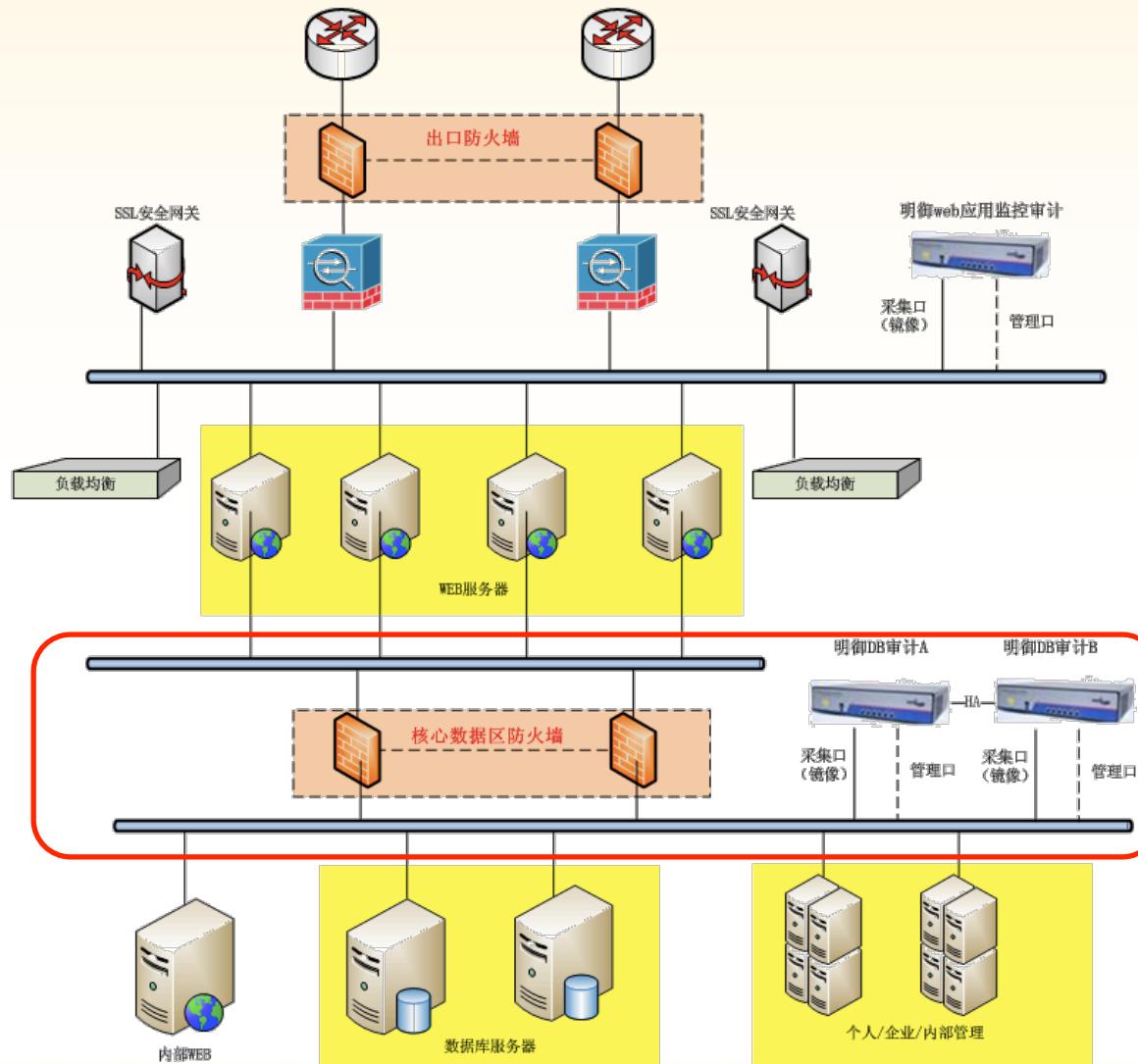
一个非常有意思的
敏感数据保护案例！



威胁9：安全域规划不合理

- DB服务器直接暴露在internet
- DB服务器没有单独的安全域
 - 很多单位都配置了服务器区防火墙，但是数据库服务器和web、ftp等服务器都在一个区域，区域内部并没有任何访问控制手段，一旦其他服务器被入侵当作跳板机，入侵数据库就非常容易了。

威胁9：安全域规划不合理——改进建议



将数据库服务器建立专用防火墙，严格控制访问源以及可访问端口。
(交换机ACL控制也可)

威胁10：缺失有效加密措施

| 企业名称 | 泄露账号数量 | 泄露信息 |
|----------|-------------------------|--|
| CSDN | 6,428,632个帐号。 | 帐号、明文密码、电子邮件 |
| 多玩 | 8,305,005个帐号。 | 帐号、MD5加密密码、部分明文密码、电子邮件、多玩昵称 |
| 178.COM | 1,883,487个帐号，仍不断增加。 | 帐号、MD5加密密码、全部明文密码、电子邮件、178昵称(178账户通用NGA) |
| 天涯 | 9,695,513个帐号(预计超4千万数据)。 | 帐号、明文密码、电子邮件 |
| 人人网 | 4,768,600个帐号。 | 明文密码、电子邮件 |
| UUU9.COM | 7,513,773个帐号。 | 帐号、MD5加密密码、部分明文密码、电子邮件、U9昵称 |
| 网易土木在线 | 约4.3GB，137个文件。 | 帐号、邮箱、MD5密码、其他相关数据 |
| 梦幻西游 | 约1.4G(木马盗取)。 | 帐号、邮箱、明文密码、角色名称、所在服务器、最后登陆时间、最后登陆IP |
| 新浪微博 | 帐号数未知，疑似文件1个。 | 邮箱、明文密码 |
| 麒麟网 | 9,072,966个帐号。 | 帐户、明文密码 |
| 某婚恋网站 | 5,261,302个帐号。 | 帐户、明文密码 |

关键字段都是明文信息！
造成重大损失的主因！

威胁10：缺失有效加密措施

- **库外加密**：对数据库文件进行加密，它把数据库作为一个文件，把每一个数据块当作文件的一个记录进行加密，文件系统与数据库管理系统交换的就是块号。
- **库内加密**：对数据库中的数据进行加密，库内加密按加密的方式，可以进行记录加密，也可以进行字段加密，还可以对数据元素进行加密。

TOP10安全风险分类

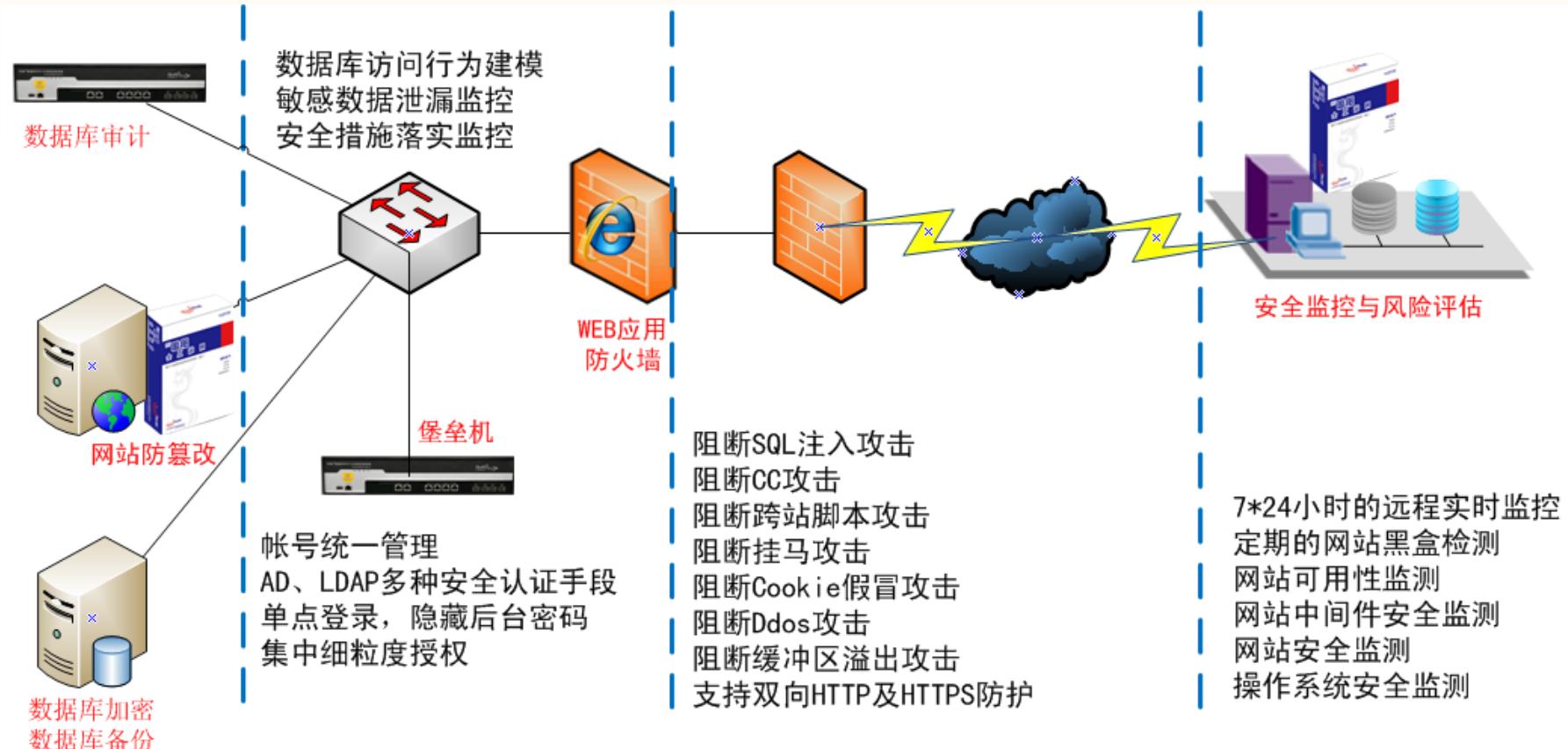
数据库自身管理配置问题

- TOP 1.帐号授权不合理, 越权操作严重
- TOP 2.帐号复用与滥用
- TOP 4.数据库漏洞和配置不合理
- TOP 5.身份验证措施薄弱

周边环境与其他保障措施

- TOP 3.脆弱的web应用
- TOP 6.备份管理不足
- TOP 7.审计措施不力
- TOP 8.缺失有效加密措施
- TOP 9.安全域规划不合理
- TOP 10.服务器操作系统漏洞与配置不合理

建议总结——构建纵深防御体系



谢谢



RSA CONFERENCE
C H I N A 2012