RSA CONFERENCE
CHINA 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 CHINA 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

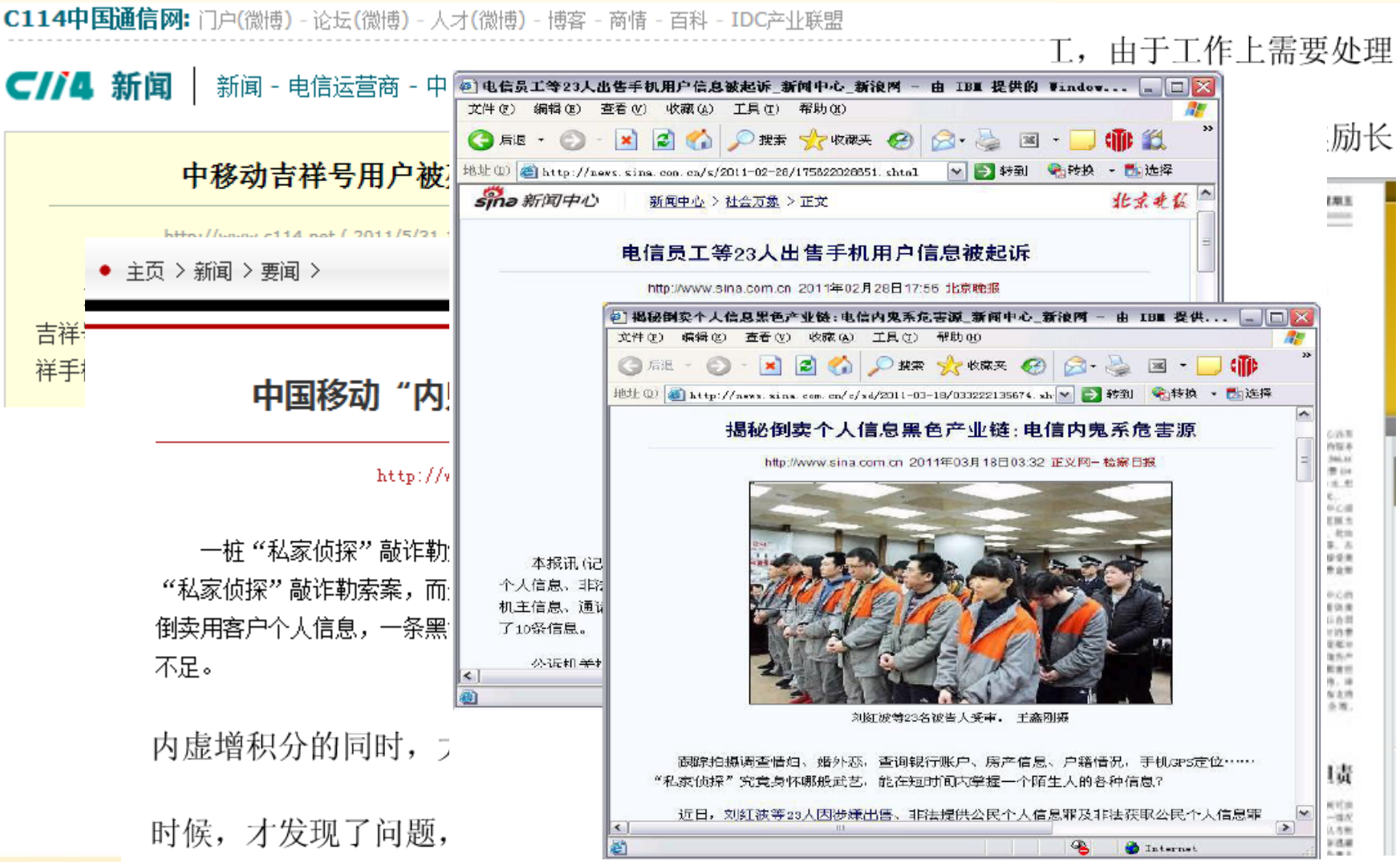
杭州安恒信息技术有限公司

RSA CONFERENCE CHINA 2012

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

1、世界500强泄密事件



2、互联网企业泄密事件

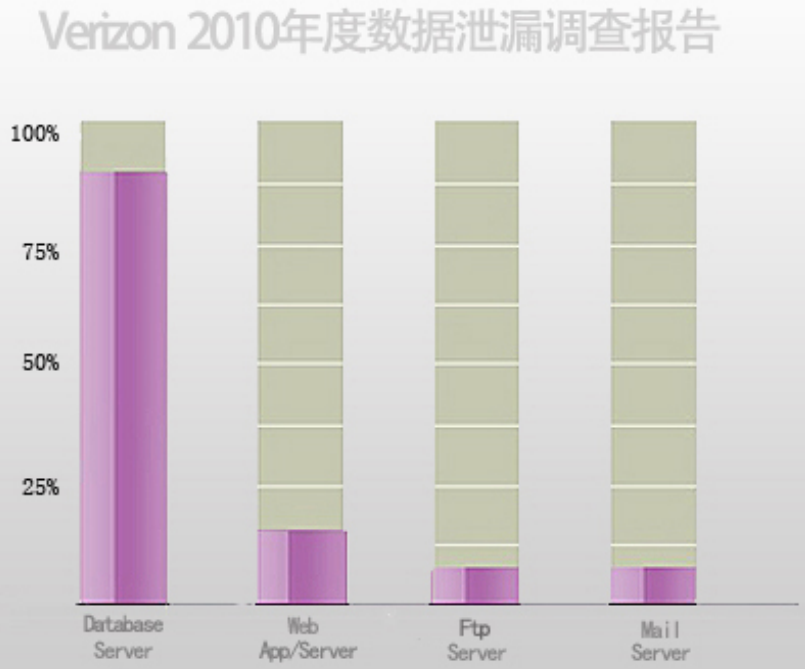
企业名称	泄露账号数量	泄露信息
CSDN	6,428,632个帐号。	帐号、明文密码、电子邮件
多玩	8,305,005个帐号。	帐号、MD5加密密码、部分明文密码、电子邮件、多玩昵称
178.COM	1,883,487个帐号，仍不断增加。	帐号、MD5加密密码、全部明文密码、电子邮件、178昵称(178账户通用NGA)
天涯	9,695,513个帐号(预计超4千万数据)。	帐号、明文密码、电子邮件
人人网	4,768,600个帐号。	明文密码、电子邮件
UUU9.COM	7,513,773个帐号。	帐号、MD5加密密码、部分明文密码、电子邮件、U9昵称
网易土木在线	约4.3GB ， 137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！



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

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

高

低

——范渊

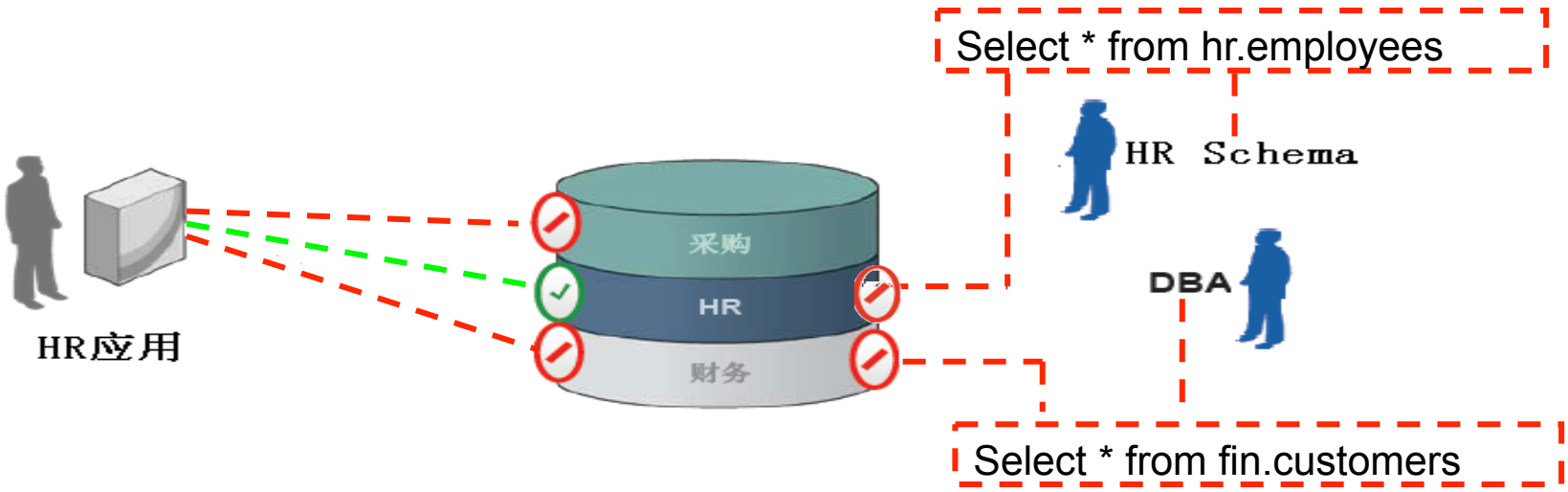
专题会议主题：业务及数据库安全风险分析

专题会议分类：安全业务——中级

RSA CONFERENCE CHINA 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

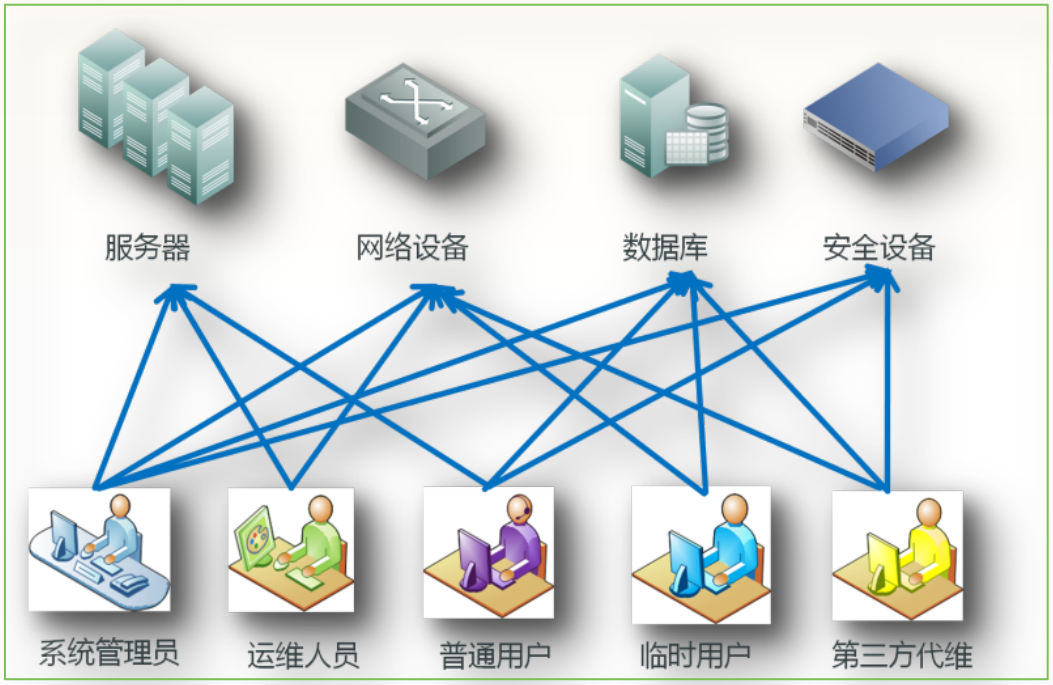
典型越权操作案例：

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；

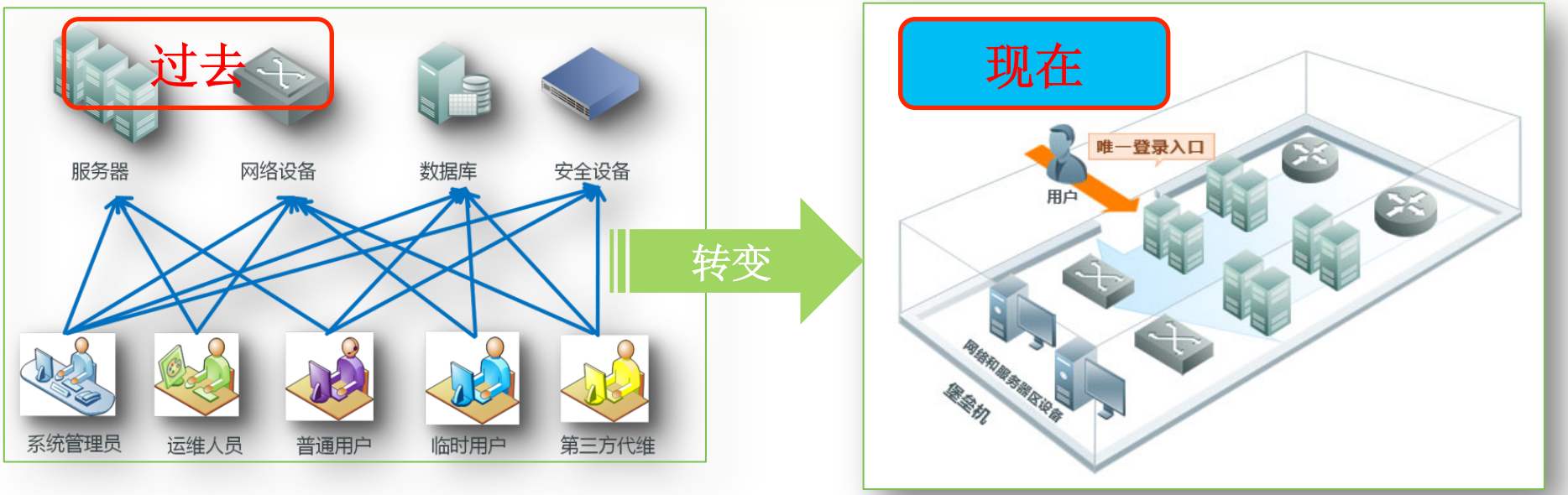
应用系统帐号个人使用；

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

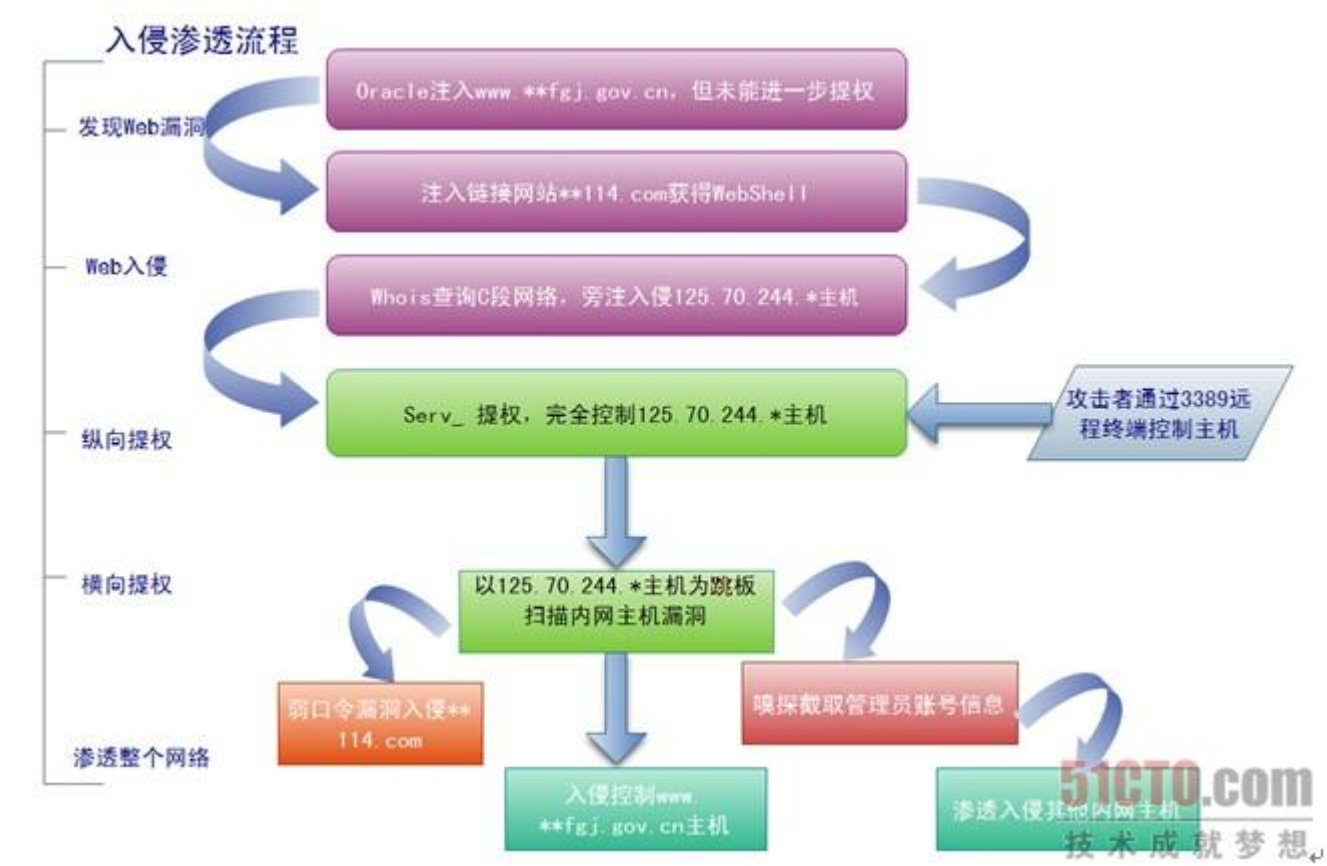
持续监控审计构建数据库访问行为模型，梳理帐号权限！

参数	内容
Who	JoJo、jamm
Where	192.168.1.1 192.168.8.8
What	price

How	工具	对象	when
select	PL/SQL	所有人报价信息	2012.5.18 14：30

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

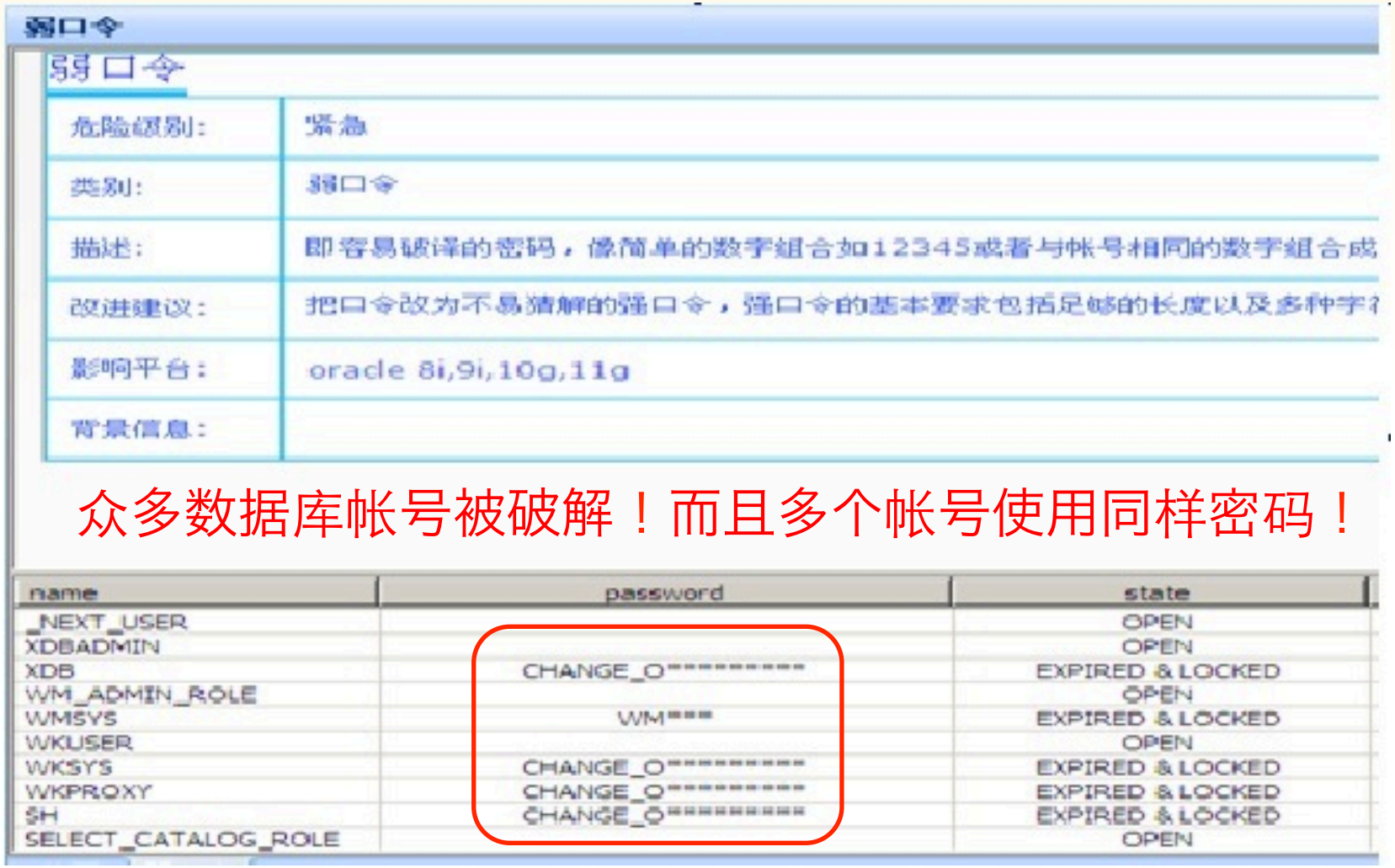


威胁3：脆弱的web应用——改进建议

- 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



威胁4：身份验证措施薄弱

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！

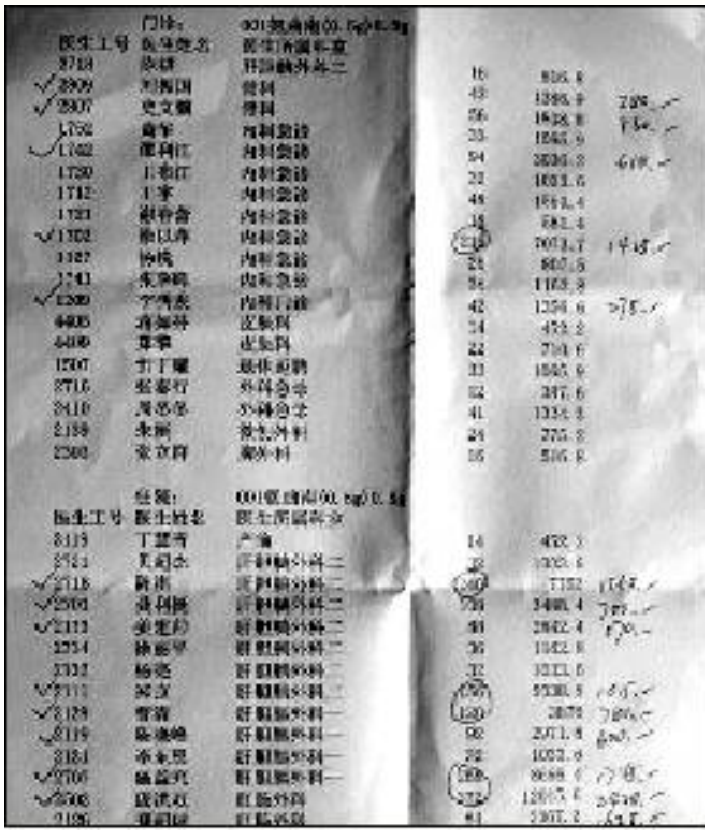
宁波先进医院医生回扣单曝光 回扣占药价两成

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年宁波市卫生行风建设先进单位”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 dú
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……



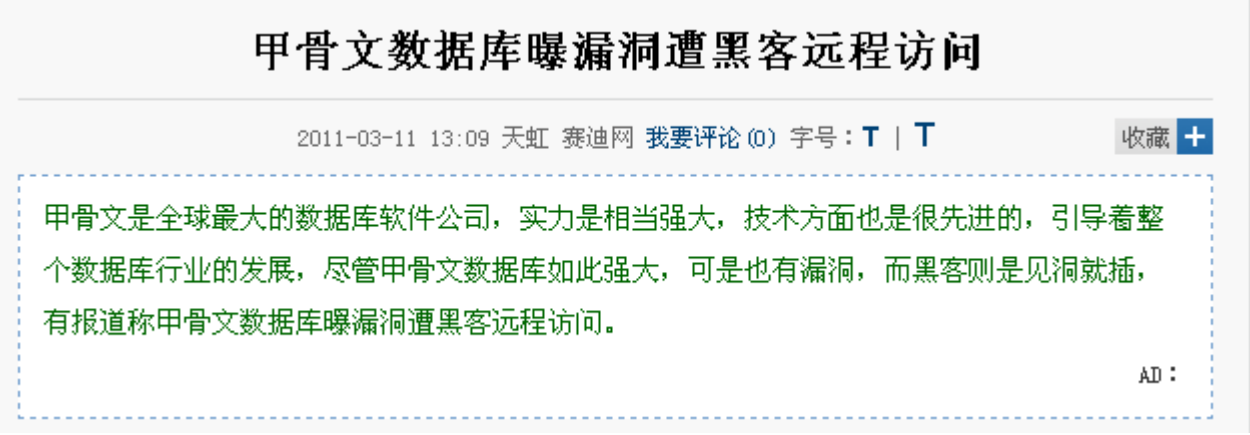
威胁4：身份验证措施薄弱——改进建议

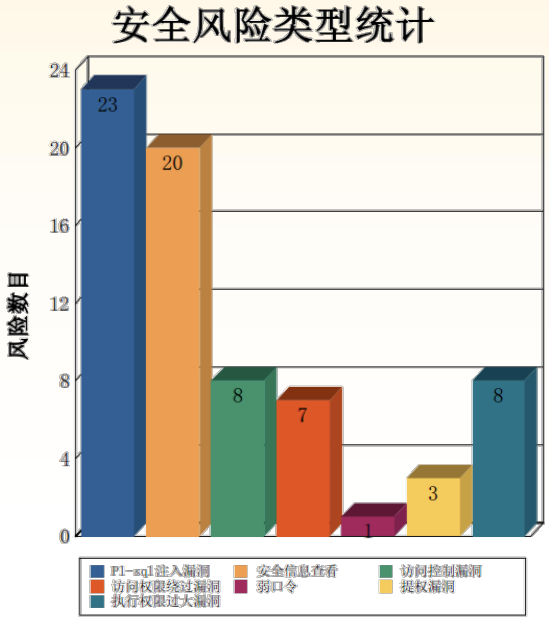
1、复杂的密码策略

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





- 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！

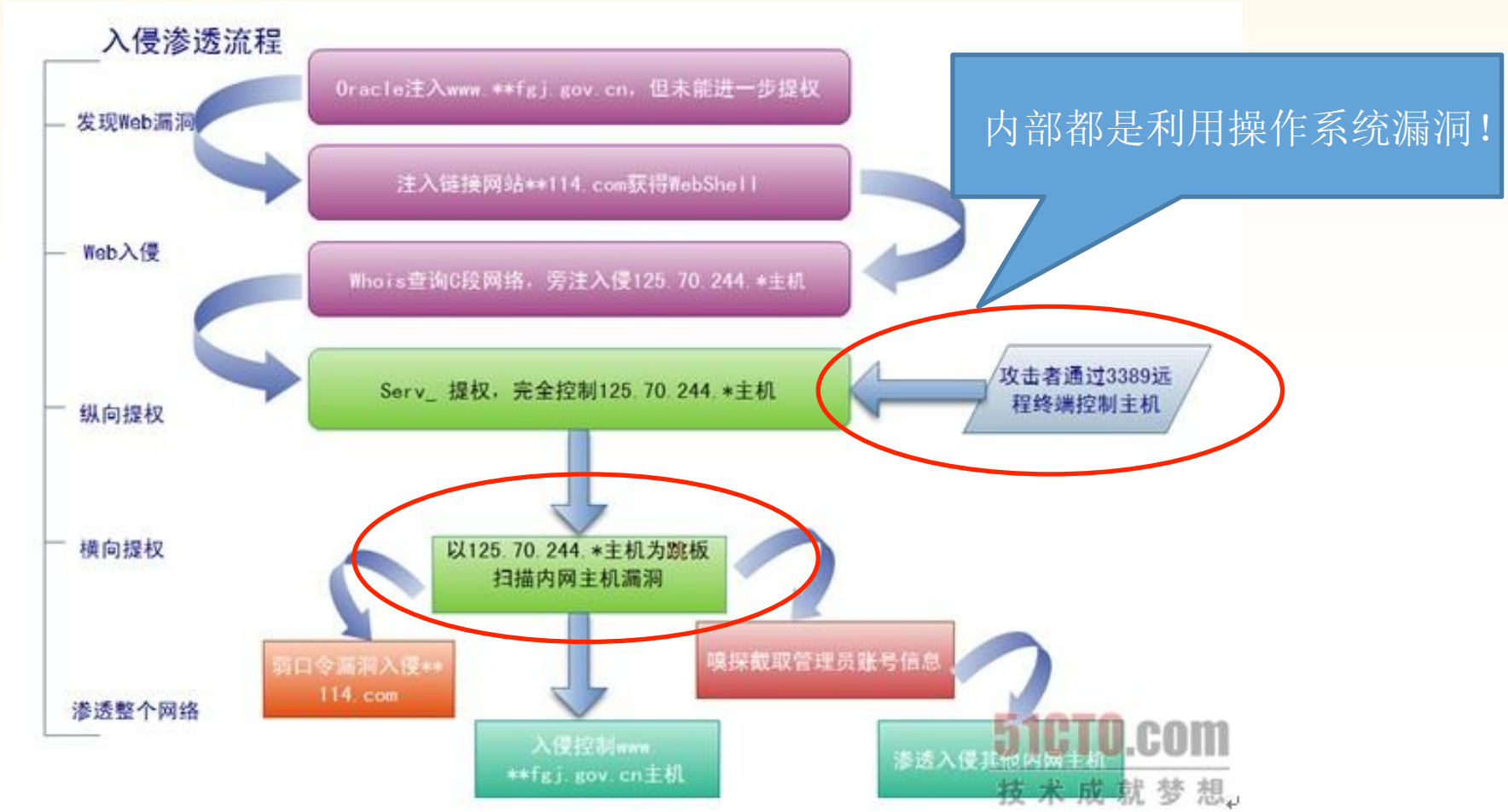
威胁5：数据库漏洞和配置不合理

- 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

RSA CONFERENCE CHINA 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

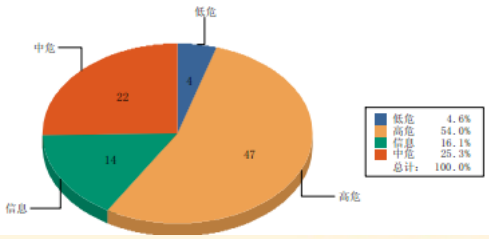
扫描主机信息：

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



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

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

凤凰科技讯 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

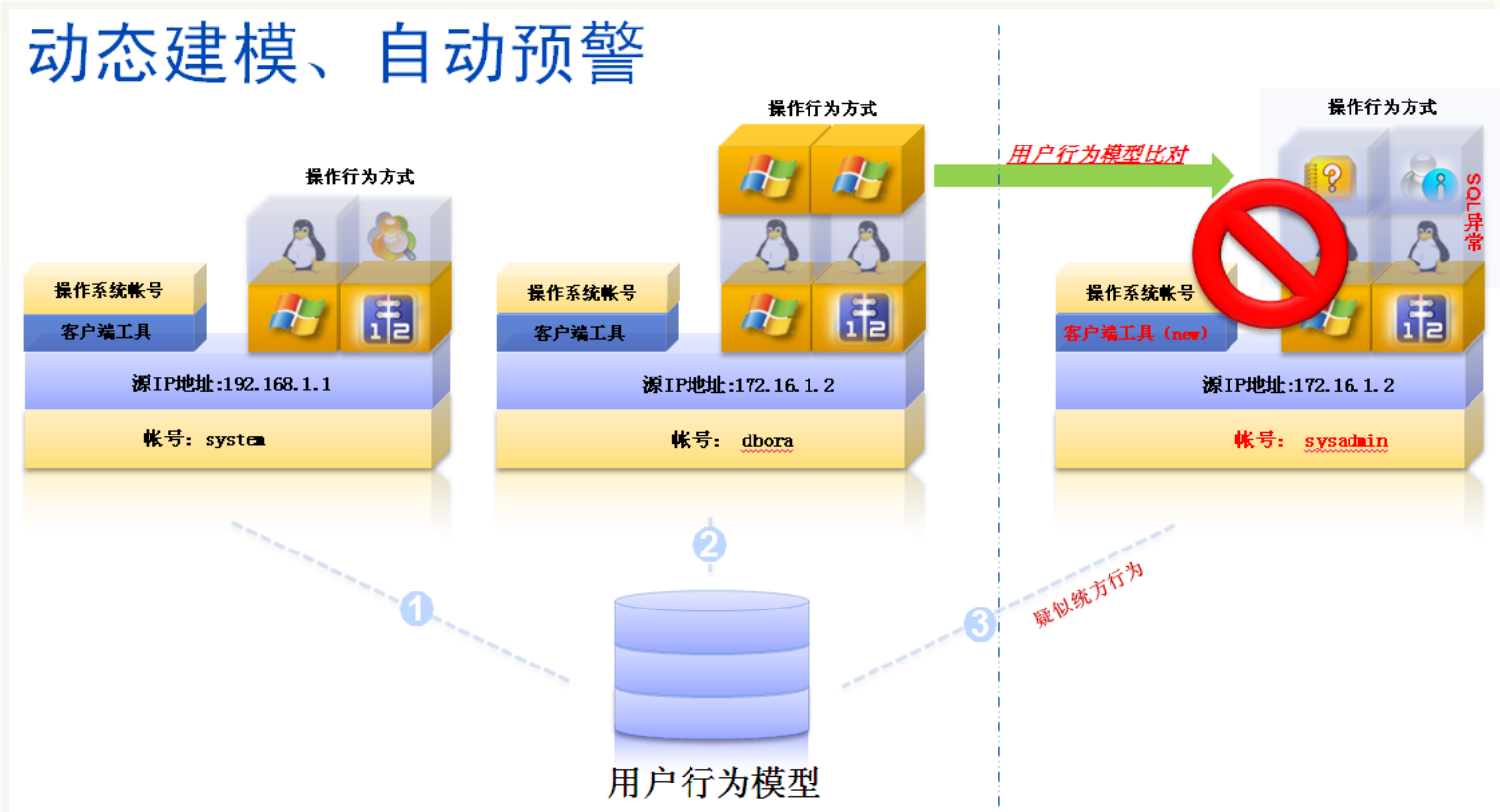
无审计	审计有缺陷	缺乏审计分析
大部分企业都还没有任何审计措施，特别是核心数据库系统.	部分企业开启了数据库自身审计，但是其详细度、可信度不足.	审计设备成为摆设也是很普遍的问题，有不重视、也有审计设备分析不足等原因.

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



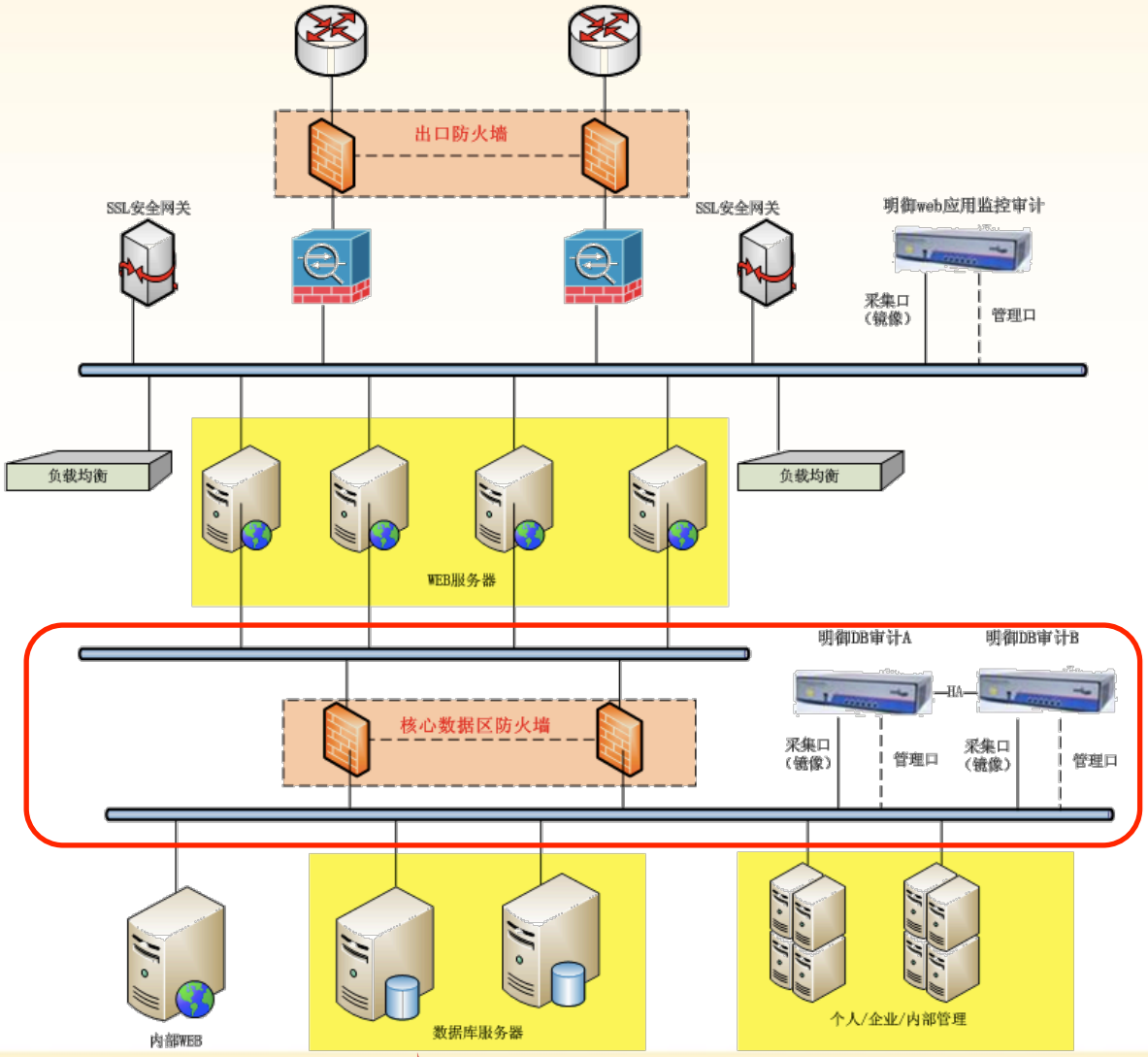
威胁8：审计措施不力——改进建议

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

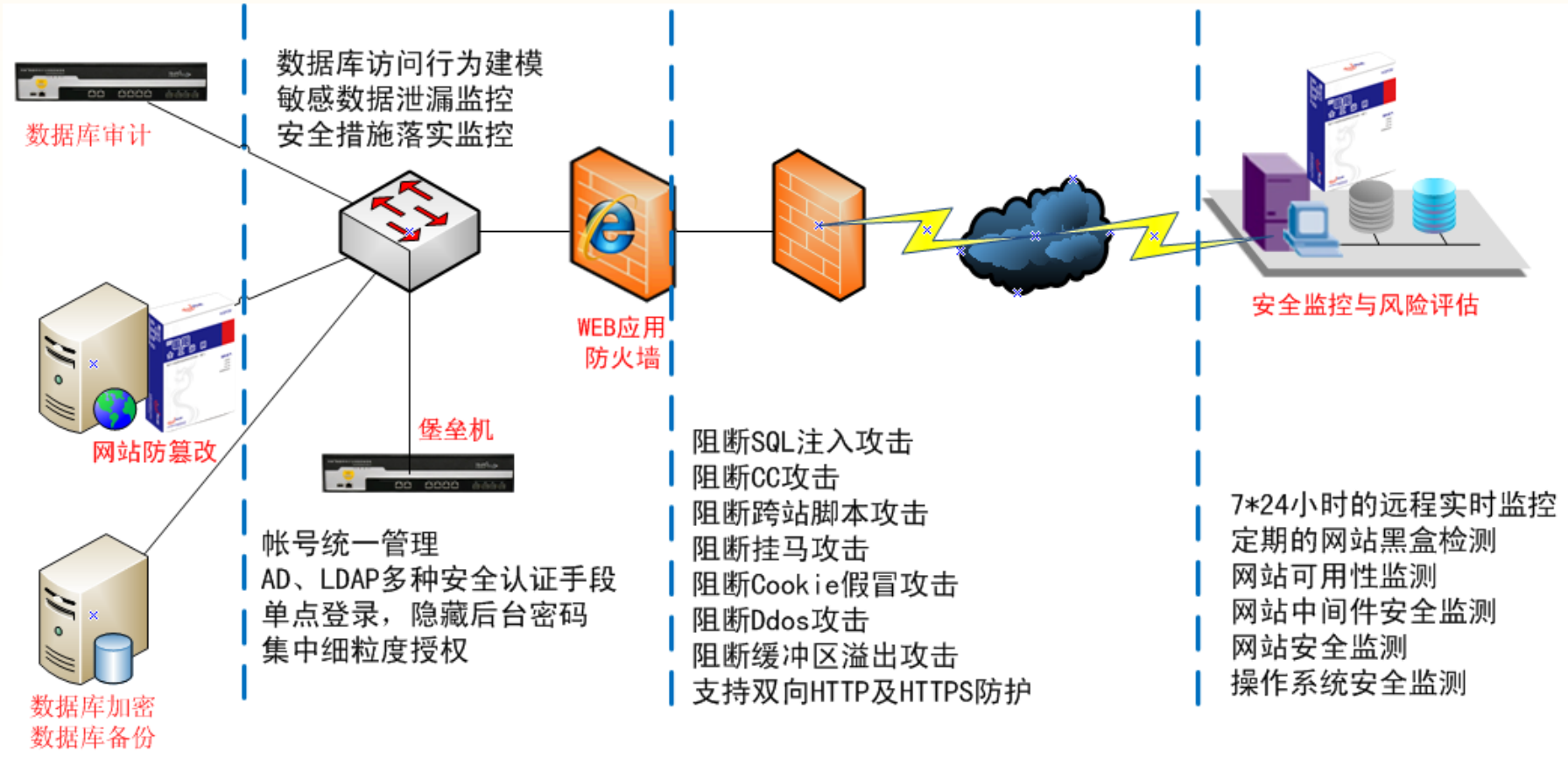
数据库自身管理配置问题

- 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
CHINA 2012