

WEB应用安全和数据库安全的领航者！



数据安全的几道防线

杭州安恒信息技术有限公司
www.dbappsecurity.com.cn

目录

- 数据安全的现状
- 2011年发生的重大安全事件
- 数据安全面临的主要安全威胁
- 数据安全的几道防线



数据安全现状

- 概述
- 造成数据安全岌岌可危的原因
- 数据安全的现状



数据安全的现状

- 概述
- 往往一个大的事件会引起人们的警醒，甚至一定程度上会影响法律法规的制订和全员意识和手段的提高。
- 2011年之前，很多互联网企业、电子商务、电子政务等诸多在线业务系统没有过多地关注于数据安全这一块，自2011年底CSDN、天涯等网站发生用户信息泄露事件之后，各行各业开始注重关于数据库防泄露的探讨与分析，安全厂商也纷纷拿出了各自的防数据库信息泄露的解决方案。



数据安全的现状

- 2011年底，CSDN、天涯等网站发生用户信息泄露事件，被公开的疑似泄露数据库26个，涉及帐号、密码信息2.78亿条，严重威胁了互联网用户的合法权益和互联网安全。根据调查和研判发现，我国部分网站的用户信息仍采用明文的方式存储，相关漏洞修补不及时，安全防护水平较低。
- 这次被公布的账户信息不过是黑客产业链输出的已经失去价值的信息残渣；这背后可能存在修改核心数据库的记录、获取特定社会公众人物的重要信息、涉嫌大宗商业诈骗等违法行为等更为严重的不为人知的恶性安全事件。



数据安全的现状

- 造成数据安全岌岌可危的原因
- 数据库泄露事件仅仅是信息安全事件的一种表现形式而已。其主要引起原因如下：
 - 由于信息系统本身存在的安全漏洞及弱点，没有及时发现和修补，被恶意攻击者利用，从而获取后台数据库信息。如：恶意攻击者利用木马或僵尸等恶意程序感染用户信息系统，从而窃取用户信息。
 - 系统开发人员在系统交付之前留有后门，利用该后门进行后台数据窃取。
 - 第三方厂商员工或内部员工离职之后，没有及时的删除或禁用该员工的账号，导致该员工通过未删除账号进入后台数据库，窃取敏感数据。



数据安全的现状

- 数据安全的现状

- 木马和僵尸网络活动越发猖獗

- 2011年，CNCERT全年共发现近890万余个境内主机IP地址感染了木马或僵尸程序，较2010年大幅增加78.5%。其中，感染窃密类木马的境内主机IP地址为5.6万余个，国家、企业以及网民的信息安全面临严重威胁。

- 应用软件漏洞呈现迅猛增长趋势

- 2011年，CNVD共收集整理并公开发布信息安全漏洞5547个，较2010年大幅增加60.9%。其中，高危漏洞有2164个，较2010年增加约2.3倍。这为恶意攻击者窃取敏感信息创造了机会，带来了便利。



数据安全的现状

□ 内部安全管理机制的不健全、不完善

- 目前，据权威数据显示，所有发生的安全事件中，70%-80%的安全事件源自于内部。由于内部安全管理机制的不完善，如系统权限过大、误操作、越权操作等，导致内部重要信息泄露。



目录

- 数据安全的现状
- 2011年发生的重大安全事件
- 数据安全面临的主要安全威胁
- 数据安全的几道防线



2011年发生的重大安全事件

- 安全事件一
- 安全事件二
- 安全事件三
- 安全事件四
- 另外安全事件
- 重大安全事件发生后的效应



2011年发生的重大安全事件

- 安全事件一
- 国外安全公司HBGary Federal宣布打算披露关于离经叛道的Anonymous黑客组织的信息后不久，这家公司就遭到了Anonymous组织成员的攻击。Anonymous成员通过一个不堪一击的前端Web应用程序，攻入了HBGary的内容管理系统（CMS）数据库，窃取了大量登录信息。之后，他们利用这些登录信息，闯入了这家公司的多位主管的电子邮件、Twitter和LinkedIn帐户。他们还完全通过HBGary Federal的安全漏洞，进入HBGary的电子邮件目录，随后公开抛售邮件信息。
- 失窃/受影响的资产：60000封机密电子邮件、公司主管的社交媒体帐户和客户信息。



2011年发生的重大安全事件

• 安全事件二

- RSA的一名员工从垃圾邮箱文件夹收取了一封鱼叉式网络钓鱼的电子邮件，随后打开了里面含有的一个受感染的附件；结果，这起泄密事件背后的黑客潜入到了RSA网络内部很深的地方，找到了含有与RSA的SecurID认证令牌有关的敏感信息的数据库。虽然RSA从来没有证实到底丢失了什么信息，但是后来又传出消息，称一家使用SecurID的美国国防承包商遭到了黑客攻击，这证实了这个传闻：RSA攻击者已获得了至关重要的SecurID种子（SecurID seed）。
- 失窃/受影响的资产：关于RSA的SecurID认证令牌的专有信息。



2011年发生的重大安全事件

- 安全事件三

- 2011年4月攻击者闯入索尼公司三个不同的数据库--这些数据库含有敏感的客户信息，包括姓名、出生日期以及一部分索尼拥有的信用卡号码，这影响了PlayStation网络（PSN）、Qriocity音乐视频服务以及索尼在线娱乐公司的广大客户。到目前为止，索尼旗下大约九个服务网站因最初的泄密事件而被黑客攻破。
- 失窃的资产：超过1亿个客户帐户的详细资料和1200万个没有加密的信用卡号码。



2011年发生的重大安全事件

- 安全事件四

- 花旗集团是2011年受黑客之害的几家银行之一。花旗银行表示，被盗信息包括用户的名字、帐号密码及其他诸如邮箱地址等联系信息。然而，其他个人认证信息，如用户生日、社会安全号码、卡截止日期及CW代码并未被盗。
- 失窃/受影响的资产的资产：20万多个银行卡帐号被盗，对花旗银行2100万银行卡用户持有者中的1%的用户造成了影响。



2011年发生的重大安全事件

- 另外安全事件
- 陕西某运营商1400万手机用户信息被倒卖
- 医疗“统方”愈演愈烈，很多人为此付出终生代价
- 近期发生的“CSDN数据库泄露”事件
- 近期发生的“天涯4000万数据遭盗取”事件
- “3.15晚会”揭露用户信息被出售
-

晚会精彩看点回顾



招行工行泄露出售客户信息

胡斌，网名“夜光杯”，真实身份是招商银行信用卡中心风险管理部贷款审核员，向朱凯华出售个人银行信息300多份。



2011年发生的重大安全事件

- 重大安全事件发生后的效应
- 政府全面重视
- 金融行业如履薄冰
- 电信行业如履薄冰
- ○ ○ ○

下一个千万不要是我！



2011年发生的重大安全事件

通信产业网

www.ccidcom.com


首页 | 新闻专题 | 地方市场 | 产品库 | 案例库 | 报告库 | 访谈

全年定价240元，共49期，邮发代号：1-145 全国邮局均可订

欢迎订阅2012年中国通信第一

● 主页 > 新闻 > 要闻 >

工信部对六家网站试点网络安全防护

<http://www.ccidcom.com> 通信产业网 2012-01-12 13:49 官方微博  加关注

【通信产业网讯】为深入贯彻落实《通信网络安全防护管理办法》(工业和信息化部第11号令)，提高增值电信业务网络安全防护系统化、规范化、科学化水平，增强网站、域名等系统的防攻击、防入侵、防病毒能力，维护互联网用户的合法权益，保障互联网安全发展，工业和信息化部通信保障局2011年8月启动了增值电信业务和互联网域名服务网络安全防护试点工作。

试点以信息服务(含门户、搜索、微博、即时通讯、电子商务、移动信息服务等)、数据中心、域名解析服务等业务类型为重点，选取了百度、腾讯、新浪、淘宝、万网、空中网六家有代表性的增值电信业务企业和域名服务企业参加。试点企业要对本企业主要业务系统进行安全域划分，确定系统的安全保护等级，明确责任领导和责任部门。

在此基础上，参照通信网络安全防护有关标准，以保证用户数据信息安全、保证重要业务系统安全运行、维护公共网络环境为目标，综合运用安全评测、风险评估、应急管理、灾难备份等手段，排查隐患、控制风险，着重完善安全制度、落实安全责任、强化防护措施、



目录

- 数据安全的现状
- 2011年发生的重大安全事件
- 数据安全面临的主要安全威胁
- 数据安全的几道防线



数据安全面临的主要安全威胁

- 当前，数据安全面临的主要安全威胁如下：

- 外部系统安全
- 缺乏安全意识
- 内部越权行为
- 无法审计和追溯的风险



数据安全面临的主要安全威胁

□ 外部系统安全

- 由于数据库需要与外部系统进行交互，同时目前基于WEB的外部系统越来越多，而这些系统大多存在一些比较严重的安全漏洞，如：SQL注入、跨站脚本、目录遍历等。因此外部系统的安全（包括WEB应用系统）是数据安全的重要组成部分。



数据安全面临的主要安全威胁

□ 缺乏安全意识

- 目前，很多企业的管理人员、系统维护人员缺乏安全意识。企业没有制定完善的操作规范、审计规范，企业高层对数据安全不够重视。系统管理人员为管理方便设置弱口令，或简化系统的安全构架导致黑客可很轻易的攻击内部系统获取各种敏感信息。



数据安全面临的主要安全威胁

□ 内部越权行为

- 由于对人员职责、流程、及日常操作的不规范，同时内部人员对了解程度，导致人员可进行本不能进行的一些行为，如：系统管理员通过系统上配置的数据库账户查看了关键数据库中的数据，甚至对部分数据进行了修改。这些行为如果没有一个很好的方式或机制进行约束和监控，数据很有可能通过内部人员进行泄露，并且很难察觉。



数据安全面临的主要安全威胁

□ 无法审计和追溯的风险

- 随着数据库信息价值以及可访问性提升，使得数据库面对来自内部和外部的安全风险大大增加，如违规越权操作、恶意入侵导致机密信息窃取泄漏，但事后却无法有效追溯和审计。同时审计数据库经常存在一些难度：
 - 制定了相应的数据安全管理制度，但没有相应的技术手段进行控制。数据库安装部署时，使用数据库厂商默认配置、缺省口令、默认权限等现象普遍存在。现有的数据库内部操作不明，无法通过外部的任何安全工具（比如：防火墙、IDS、IPS等）来阻止内部用户的恶意操作、滥用资源和泄露企业机密信息等行为。
 - 现有的依赖于数据库日志文件的审计方法，存在诸多的弊端,比如:数据库审计功能的开启会影响数据库本身的性能、数据库日志文件本身存在被篡改的风险，难于体现审计信息的真实性。



目录

- 数据安全的现状
- 2011年发生的重大安全事件
- 数据安全面临的主要安全威胁
- 数据安全的几道防线



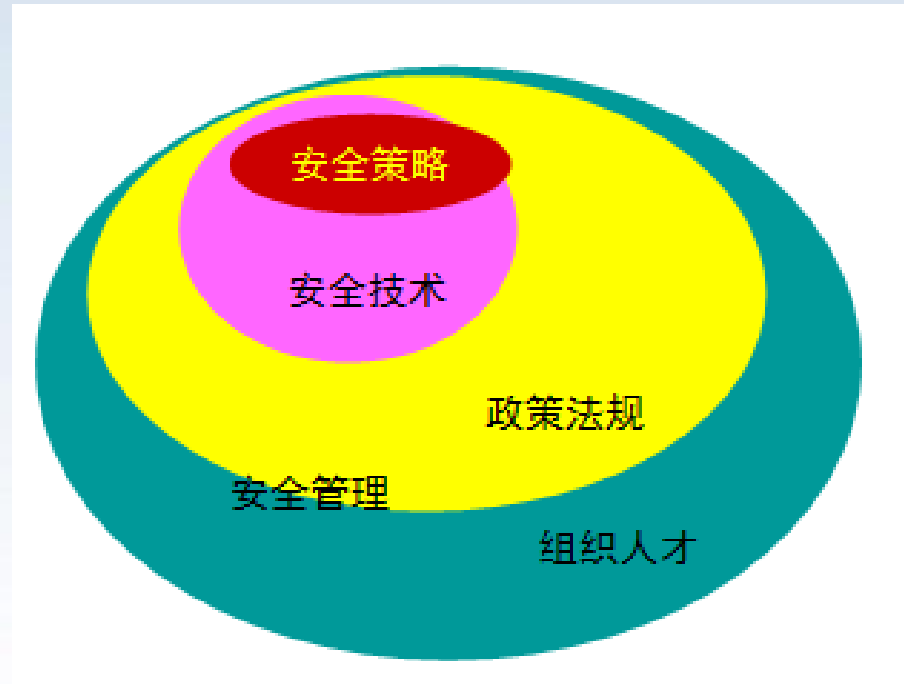
数据安全的几道防线

- 信息安全理念
- 信息安全防范体系介绍
- 保障数据安全的几道防线
- 最终实现事前防范、事中防御、事后审计



数据安全的几道防线

- 信息安全理念
- 信息安全三要素：
 - 安全策略
 - 安全技术
 - 安全管理



数据安全的几道防线

□ 安全策略

- 安全策略包括各种安全策略、法律法规、规章制度、技术标准、管理规范等，是整个信息安全建设的依据，其目的就是决定一个组织机构怎样来保护自己。

□ 安全技术

- 安全技术包含工具、产品和服务等，是实现信息安全的有力保证。一般来讲，信息系统的安全技术的核心本质是有效的风险识别和严格的访问控制，具体体现的产品一般有网络防火墙、入侵检测、应用防火墙、应用审计系统、弱点扫描工具等。

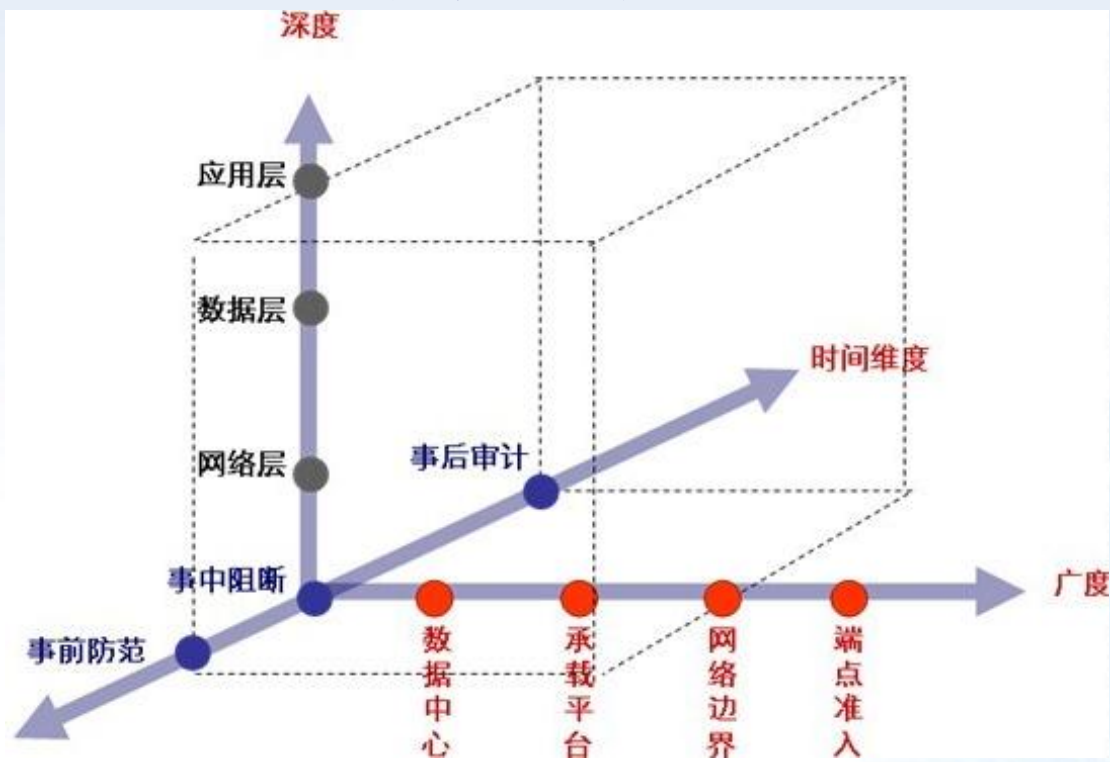
□ 安全管理

- 安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。安全管理主要是人员、组织和流程的管理，是实现信息安全的落实手段。



数据安全的几道防线

- 信息安全防范体系介绍
- 从防御时间、防御广度、防御深度三个维度进行综合考虑，信息安全防范体系架构图如下：



数据安全的几道防线

- 保障数据安全的几道防线
- 针对目前数据安全面临的严峻安全现状，结合信息安全理念和信息安全防范体系，如何实现数据的相对安全性，具体我们要做好以下几道防线：
- 防线一：进行信息资产分析、风险分析和评估以及需求分析
- 防线二：制定安全策略
- 防线三：建立有效的安全管理机制
- 防线四：安全防护系统建设
- 防线五：实施维护
- 防线六：监督核实



数据安全的几道防线

- 防线一：进行信息资产分析、风险分析和评估以及需求分析。
- 通过分析人员、安全评估人员对信息资产分析、风险分析和评估以及需求分析，从而充分了解目前的网络现状和安全现状，以及相应的安全需求。



数据安全的几道防线

- 防线二：制定安全策略
- 根据安全需求分析结果制定适合用户信息系统的准确的安全策略，安全策略是整个信息安全的指导方针。



数据安全的几道防线

- 防线三：建立有效的安全管理机制
- 通过建立有效的安全管理机制，从而实现信息安全流程化、制度化、规范化的管理。
- 建立有效的安全管理机制，主要包括以下内容：
 - 建立专门的WEB 应用安全管理机构
 - 建立有效的安全操作管理制度
 - 建立有效的网络安全管理制度
 - 建立有效的安全管理制度
 - 建立有效的病毒防范管理制度
 -



数据安全的几道防线

- 防线四：安全防护系统建设
- 通过第三方安全产品、安全技术、安全服务相结合，建设安全防护系统，从而实现数据安全保护。
- ❑ 网络防火墙及VPN：用于实现安全域的划分和网络访问控制；
- ❑ 入侵防御系统（IPS）：用于实现检测和防御那些被明确判断为攻击行为（对网络、数据造成危害的恶意行为）。
- ❑ WEB应用防火墙：用于网站应用层的安全防护；
- ❑ 安全审计系统：设置有效的安全审计系统，对来自重要服务器内外部的操作进行安全审计，实现事后有效追溯和审计；
- ❑ 安全扫描工具：用于扫描发现系统可能存在的安全漏洞及弱点；
- ❑ 风险评估：用于对主机、网络等整个系统进行风险评估识别脆弱性；
- ❑ 安全加固：针对评估结果进行加固，提高系统的安全防护能力；
- ❑ 应急响应：针对WEB应用系统可能出现的安全事件，快速有效响应；
- ❑ 安全培训：增加信息系统相关人员的安全意识。



数据安全的几道防线

- 防线五：实施维护
- 成立专门负责实施维护信息系统部门，不同系统成立不同的实施维护小组，来实施维护相应的信息系统，从而实现安全防护系统的正常稳定运行。



数据安全的几道防线

- 防线六：监督核实
- 成立监督核实安全管理制度、安全防护措施具体落实的监督部门，通过专门的监督人员来核查其落实情况，对于没有落实或违反制度人员进行相应的处罚，从而实现保障安全管理制度、安全防护措施的具体落实。



数据安全的几道防线

- 最终实现

- 事前防范

- 事前针对本信息系统进行深入的风险评估工作，涉入网络层、应用层、主机操作系统等技术层面，还有对安全管理制度、安全策略进行评估。在安全评估的基础上定制新的安全策略。做好安全防范工作、充分准备安全预案一方面降低业务系统自身暴露的安全问题，另一方面积极加固系统的防御能力，尽可能的降低遭受攻击而带来的损失。

- 事中防御

- 合理部署网络层、应用层安全产品如抗DDOS、网络防火墙、IPS、WEB应用防火墙等，严格按照风险评估的结论实施安全策略，并动态的调整安全策略实现动态最佳安全平衡，当攻击事件发生时能很好的起到预计的防御能力，同时能够快速有效的进行应急响应。

- 事后审计

- 做好安全防范、安全防御的同时做好安全审计工作，实现针对可疑行为发生时可实时告警和记录，实现安全事件事后有效追溯和审计。



WEB应用安全和数据库安全的领航者！



Thank You !

杭州安恒信息技术有限公司
www.dbappsecurity.com.cn

数据安全的几道防线

- WEB应用防火墙功能：
- 提供对SQL Injection、XSS等WEB攻击的监测和阻断；
- 提供WEB加速功能；
- 支持HTTP/HTTPS模式；
- 提供对攻击和扫描的阻断模式；
- 提供对攻击和扫描的告警模式；
- 提供By-Pass模式提供网页防篡改功能。



数据安全的几道防线

- 安全审计系统功能：
- 安全审计系统应记录重要服务器相关的安全事件，包括重要用户行为和重要系统功能的执行等；
- 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；
- 安全审计记录应受到保护避免受到未预期的删除、修改或覆盖等。



数据安全的几道防线

- 风险评估指安全专家通过安全扫描工具，包括主机、操作系统、网络设备、数据库系统、应用系统等方面的安全扫描工具，结合人工渗透技术，以及自身安全经验和知识，验证并分析，发现系统可能存在的安全漏洞及弱点，提出针对评估结果的安全加固措施或安全解决方案。



数据安全的几道防线

- 应急响应指对国内外或当前系统内发生的有关计算机安全的事件，进行实时响应与分析，提出解决方案和应急对策，来保证计算机信息系统和网络免遭破坏。应急响应六个阶段：



响应前的
准备工作

- ① 工作流程
- ② 报警方法
- ③ 备份体系
- ④ 安全培训

识别和发现
各种安全的

紧急事件

- ① 检测设备
- ② 报警 Agent

把事件影响
降到最小

- ① 阻断
- ② 缓解
- ③ 封堵
- ④ 隔离

真正解
决问题

如：清楚病毒、
修补漏洞

数据和系统
被破坏情况
下，进行恢
复

回顾并整合
安全事件的
相关信息

