成 功 案 例

北京尚良风信信息技术有限公司

2011 年 5 月

目 录

一． 北京移动业务系统数据安全尚良风信项目介绍

1.1. 应用背景

随着北京移动业务支撑系统和支撑网络的不断完善，移动业务服务器群及数据大量集中，全公司办公网和业务网完成 IP 网络互联，这样对安全的压力明显加大，信息安全成为业务支撑系统安全运行的首要问题。目前已完成的安全建设有：实施了内外网隔离、统一安全网关、网络入侵检测、内网核心系统的防火墙保护、远程办公用户安全接入公司内网等网络安全建设，以及重要主机访问控制、日志审计、防病毒等操作系统安全建设，同时在网络和操作系统的安全实施中，适时作网络和系统的安全漏洞扫描，及时发现并修补了系统漏洞，使得计费业务中心的信息安全水平得到了很大的提高，能够防范和检测绝大部分病毒、扫描、黑客入侵等攻击。

目前在北京移动中所作的安全措施主要是针对网络和操作系统层面，而应用层面的安全，尤其是对于内部管理员、操作员、开发厂商的权限控制和审计并没有做专门的解决，是北京移动公司现在最大的薄弱环节。为了有效地解决应用层面中对数据访问的控制和相关操作的审计问题，需要对应用操作中各种内部有关人员对应用系统和数据库系统的操作，实施统一的访问控制和操作审计，建立统一的应用系统运维安全管理平台，保证移动公司数据库中敏感数据的安全，实现北京移动公司业务支撑系统和支撑网络全方位的安全。

从 2004 年 11 月份开始，风信子系统在北京移动计费中心正式上线，目的是要解决对业务支撑系统（包括 BOSS 等系统）中重要资源访问的身份认证、访问授权和行为审计问题。

1.2. 达到的效果

风信子系统部署后，来自移动公司计费业务中心的管理员、维护员、开发厂商人员和要访问业务支撑系统内受保护的重要资源，除了应用系统本身具有的“口令/用户名”机制和防火墙系统外，必须由风信子系统进行统一授权。对应

个人不同的身份，风信子系统赋予其访问不同应用主机和不同应用服务的权限。这样，就将用户的内部网络访问权限集中并统一管理起来。同时，风信子系统还对相关人员的操作行为进行完全审计。这样，通过风信子系统的管理，所有人员的操作行为历历在目，这对有违法企图和经常随意操作的人员有了很强的震慑力，从而增强了业务支撑系统的安全性和可管理性。

由于风信子系统采用旁路接入技术，服务器端不需要安装任何软件，跨平台效果好，并且可以进行集中统一的管理，因此，对整个业务支撑系统没有影响。

1.3. 风信子系统的升级及服务

风信子系统在北京移动 BOSS 的应用，经历了“应用－需求更新－开发－应用”不断升级的过程。随着风信子系统使用的不断深入，新的功能需求也不断出现。我们与北京移动方面共同配合，及时的完成了北京移动对风信子系统所要求的新增功点，使风信子系统保护 BOSS 系统的安全运营。由于风信子系统的优异表现和全方位的售后服务，在 2005 年 7 月份完成了风信子系统的二期扩容，确保了新建的 BOSS 系统灾备中心的安全运营。

1.4. 系统扩展计划

目前，由于风信子系统的优异表现和全方位的售后服务，以及随之带来的良好效果，北京移动已经实施部署第三期、第四期风信子系统。

1.5. 总结

由于风信子系统采用旁路接入技术，不需要在服务器端安装任何软件或插件，客户端也与应用软件无关，因此不会对业务系统和网络运行造成影响。根据风信子系统在实际使用中的情况分析，该系统在移动 BOSS 中将起到非常重要的安全保障作用，同时，又是一套很好的跨平台的、绿色的安全管理系统。

二． 中国电信网络安全管理平台 2010 年扩容工程（动态密码系统）

2.1. 应用背景

为了提高中国电信网络安全管理能力，实现中国电信网络集中化、体系化、层次化的安全管理，中国电信集团已经针对 ChinaNet 在集团公司（北京）和江苏两地完成了网络安全管理平台（SOC）的试点建设。SOC 平台能够在全局层面实现 IP 网安全策略的统一，对全局资源进行统一调度，协同对各种网络安全问题进行有效的防范和处理，同时实现对 C 网分组域和部分 C 网业务平台的安全管理，有利于中国电信 IP 网网络的健康、稳定、安全运营。在目前试点 SOC 平台顺利开展工作、中国电信 IP 网的网络安全管理水平有了长足进步的同时，网络安全技术的发展对网络安全管理平台的功能提出了新的需求。

SOC 平台管理全网 2000 多台路由器、多个业务平台、多个网管系统，对这些系统的帐号管理比较分散，帐号和口令分配、回收、增加、删除等操作较为混乱，带来不少安全隐患，而且对于外来人员的帐号口令也缺乏有效的管理。因此需要对 SOC 平台升级集中的用户认证、口令管理功能，采用动态密码技术，加强密码管理的安全性。同时根据工信部要求，需要具备较强的审计功能，以便事后追溯。

2.2. 达到的效果

根据原系统访问控制授权方式，采用 SPAN 到业务核心交换机，对登录用户作相应的用户登录身份确认，通过在系统中设置保护网段、TCP 端口，保证合法用户只能在合法的网段才能通过认证，登录系统。达到用户的实体级授权控制。账号管理模块统一了业务系统的实体内角色权限管理，4A 账号管理员根据被分配管理的资源与用户，在账号管理平台中为用户分配访问资源的角色，依据用户账号绑定关系，达到了自然人的实体内授权。

系统采用旁路部署，负载均衡的服务器部署方式，成熟可靠且容灾响应迅速。

通过对设备账号的统一认证、授权、审计管理，有效控制受保护网络设备资源的安全访问。动态密码方式的账号认证具有高安全性和易用性的特点，使所有层面的用户都易于接受。集中管理的账号和授权，配置简单灵活，粒度细，修改方便。所有操作的可审计记录可供事后安全检查，符合塞班斯法案要求。

2.3. 系统定制、升级及服务

风信子系统在中国电信集团公司的应用，同样经历了“应用－需求更新－开发－应用”的升级过程。我们与电信方面共同配合，整理出新增功能，制定开发进度表。根据用户的需求，专门安排工程师为该系统进行服务工作，包括：

- 用户使用反馈收集；
- 问题整理及完善进度；
- 用户方提出地新增功能及进度表；
- 厂商提出的新的安全功能建议；
- 协助电信方面处理安全事故；
- 定期检查风信子系统工作状况；
- 紧急上门服务。

2.4. 总结

风信子统一认证系统，在中国电信集团公司部署了相应的安全监控系统，以实现统一管理、身份认证，从而统一系统管理员、开发厂商对后台业务网络系统的动态密码认证接口，控制其访问权限并进行对应的审计工作。通过部署风信子统一认证系统，搭建起统一的安全管理技术和平台和全网统一身份认证系统的框架，制止内部合法用户的违法操作，实现对登录应用系统的过程进行审计的要求，并及时响应非法操作。

三. 北京市烟草公司网络安全监控与管理系统项目

3.1. 概述

北京烟草在互联网接口处已采用防火墙设备保障内部网络安全，再增加VPN系统，通过互联网使专卖点客户端和移动客户端与北京烟草网络连接成封闭的烟草虚拟广域网络；原互联网的防火墙成为唯一的互联网出口；在内部，布署风信子系统，使拥有 USB 令牌的用户根据配置的相应权限，访问内部网络中的服务器所开通的服务，并且记录访问人员的相关操作，以方便事后分析，和为出问题时提供依据；VPN 和风信子系统相集合，使外部人员通过唯一路径访问与其权限一致的内部服务器，并记录其操作内容。

3.2. 达到的效果

风信子安全管理系统会对我们内部管理员、操作员、用户访问教务系统有详细的记录，提供基于 IP 数据报和用户名的日志审计，并提供强大的日志搜索查询功能，一旦出现安全事故，可通过查询日志审计，找到事故原因和责任人。

系统实现了强身份认证、访问控制和安全审计，当系统出现重大安全问题、系统敏感信息泄漏时，可以提供相关的操作记录信息，便于追查原因，可以把事故责任落实到人，充分的保证系统敏感数据的安全性。

系统可以实现对用户在访问过程中全程实时监控，发现有违法操作立即断开网络阻断非正常操作，有效的避免了黑客的恶意攻击和不法分子非法牟利行为。

3.3. 总结

通过风信子安全管理系统的部署，实现了对北京烟草内部系统的安全控制和审计，切实有效的保障系统敏感数据的安全，使我们企业信息化系统得到了很好的保护，弥补了防火墙及其它安全设备的不足，在根本上提高对最终用户的服务水平，增强系统的稳定性和数据防篡改实现公平、公正。

四． 其它成功案例

序号	合作用户	项目内容
1	国家审计署	异地非现场联网审计安全保障项目
2	国家某机密部委	内部办公网非机密信息桌面保护及认证系统
3	外交部	因公护照签发系统
4	公安部	交通管理网安全解决方案 （一期：覆盖全国 40 个中心城市 二期：覆盖全国 400 多个大中城市）
5	黑龙江省公安厅	一期：省公安厅内部办公网络完全项目 二期：公安信息网络安全系统集成
6	云南省公安厅	综合业务网（覆盖全省 20 多个市级公安局）
7	成都市公安局	综合业务网（覆盖全市 7 区 12 县分局科所队）
8	深圳市劳动局	网络信息安全服务项目
9	上海工商行政管理局	企业数据库共享系统
10	国家邮政总局	邮政综合计算机网络电子汇兑系统 （覆盖全国 2479 个市县邮政网点）
11	上海市农业银行	备份拨号线路安全系统
12	上海市工商银行	电话银行安全系统
13	河北省石家庄农信社	支付网络安全平台项目
14	中国农业银行	金融数据联网审计 内部办公数据安全控制系统
15	四川联通	网管与网络安全系统项目
16	贵州联通	网络安全审计与控制系统项目
17	中国移动通信集团四川有限公司	天府储值卡安全认证系统
18	中国移动通信集团河北有限公司	计费营帐系统安全项目
19	中国移动通信集团山东有限公司	BOSS 系统主机数据库审计行为系统项目

20	中国移动通信集团山西有限公司	IT-NMS 二期扩容工程
21	中国移动通信集团上海有限公司	BOSS 系统安全审计项目
22	中国移动通信集团海南有限公司	信息安全二期工程项目
23	中国移动通信集团西藏有限公司	信息审计管理系统项目
24	中国移动通信集团江西有限公司	业务支持网安全审计系统建设项目
25	黑龙江移动通信公司	移动储值卡安全认证系统
26	北京市烟草公司	网络安全项目
27	新疆烟草	网络安全项目
28	吉林省朝鲜延吉自治州林业局	网络应用系统安全防护项目
29	黑龙江省国电总公司	国电总公司办公网络整体安全一期实施
30	重庆力帆集团	远程 OA 安全接入系统
31	中信国安信息产业股份有限公司	远程 OA 安全接入系统
32	神华集团有限责任公司	远程 OA 安全接入系统
33	重庆长安集团	计算机桌面安全系统项目