论信息系统的安全管理

【摘 要】在某公司集团级安全的信息系统项目中，本安全系统由安全机制、安全服务、安全技术三部分搭建而成，在实施中运用了项目管理的知识和技术，建立了一套满足用户需求、较为完善的安全系统，保障了用户信息系统的安全运行。

0 引言

某公司集团级安生的信息系统由安全机制、安全服务、安全技术三部分构成，工作分解结构 WBS[1]为：新的网络核心机房装修、数据备份机房装修、IT 设备支撑系统、UPS 系统、制冷系统、新风系统、消防系统、监控系统、数据备份机房、数据存储与备份系统、防火墙与入侵检测等子系统。该系统原来由于资金紧缺、网络结构简单、应用系统少等原因，在当时没有很完善的安全管理系统。但随着网络的不断的延伸，用户数量急骤上升，业务的不断扩展，如：资金系统、财务系统、通风系统、瓦斯系统、生产调度系统、电力调度系统等重要应用系统的运行，原来简单的安全管理已不能满足系统的安全需要，需要建立一套能满足用户需要的、较为完善且安全的系统。

1 某公司集团级安全的信息系统

为了提高某公司集团级信息系统的安全性，满足用户的更高水平要求，对信息系统进行了安全升级，并完善成安全的信息系统，具体做法如下：

1.1 安全机制

安全机制[2](security mechanism)是指设计用于检测、预防安全攻击或者恢复系统的机制；通过安装防火设施、防雷、视频监控、门禁、UPS、精密空调等附属设施，同时建立了异地备份机房，大大地保证了基础设施的实体安全。

a、基础设施实体安全。为了保障基础设施的实体安全，对机房进行了洁净机房装修，装修后面积约 140M2，分为三个功能区，从左到右分别为监控室、主机房和消防间。走廊东面设有安全门，南侧为开放办公区。核心机房全部采用整体落地玻璃间隔。主机房设有两个出入口，一个通向监控室，维护人员正常工作时使用；另一个面向走廊，当搬运大件设备或者紧急情况时启用。主机房东侧是消防间，面向走廊开门，用于存放消防钢瓶，同时也便于工作人员维护核心机房的空调室外机。

机房装修时，首先对窗户进行了双层玻璃的密封，地面铺设了防静电地板，安装了两台 APC FM40 精密空调机(带加温系统)，采用下送风上回风的气流循环方式，保证机房恒温恒湿的需要。安装了新风系统，完善了接地系统，保证了机房环境、温度、有效地防范了电磁、噪声、灰尘、静电等对设备的影响；场地安全方面在机房安全了视频监控系统、环境监测设备、七氟丙烷自动灭火系统，这些有效地保证了场地安全；设施安全方面，核心交换机由主备两台交换机进行冗余保护，通信线路实行双向环技术，这些措施保证了设备可靠性和通信线安全自愈能力；在动力系统安全中，电源系统采用了两路市电主备供电的方法，减少单路供电停的不安全因素，同时 UPS 采用了 APC 公司的 40k+10k 模块化设计的集成供电系统，保证机房 40K 千瓦的用电需求，现设备负荷率达 65%。并在电源端做了防雷装置，保证系统设备的正常供电或雷雨季节的安全运行。

灾难预防和恢复，为了提高容灾能力，建立了异地(因为条件限制实际是在不同的楼上)备份机房，其与主核心机房全是用光纤联接。

b、平台安全。为了保证本网络的平台安全，在内网与外网之间安全装了防火墙，在网络中还安装了安全入侵检测、脆弱性扫描，对系统内所的终端都安装卡巴斯基防毒软件；在 UNIX、WINDOWS、LINUX 系统上安装了操作系统漏洞检测与修复软件。总之通过这些工作基本上保证了平台安全。

c、数据安全。异主要采用异地数据容灾，为系统数据备份系统提供运行环境保障。同时也可作为网络核心机房的备份，并为非核心业务网络服务提供机房环境支持。数据备份机房建设充分利用了原核心机房撤出的基础设施和设备，并通过远程监控等手段实现与心网络核心机房的统一管理与维护。

制定备了份策略：每周联机热备，结合每月定时脱

机冷备，每日晚做完全逻辑备份，同时在平时持续备份archivelog：每周六晚 10 点，做一次完全联机热备；每日晚 10 点，做一次增量备份；每周三晚 10 点，做一次差分备份；每日每隔 2 小时往磁带备一次新产生的archivelog，这个备份做 2 份。

d、运行安全。为了保证运行安全，对运行中存的各种风险进行分析、评估、排序，并对不同风险制定了《信息系统安全应急预案》，在预案中明确了安全求援的机构、指挥长，阐明应急等级和启动应急预案的流程，使设备在运行中如果出事故时，在应急预案的指导下使故障能速迅得到恢复，保证了系统运行安全。

e、管理安全。在安全上专家认为是“三份技术、七份靠管理”所以我组项目相关干系人，通头脑风暴法、专家咨询等手段，结合相关标准建立健全了：《人员安全管理》、《培训管理》、《应用系统管理》、《软件管理》、《设备管理》、《文档管理》、《数据管理》、《操作管理》、《运行管理》、《机房管理》等各项管理制度，为安全管理打下坚实的制度基础。

f、授权和审计安全。为了保证系统安全，采取发对用户认证系统，完善了网络内部活动的监控、统计和分析，提高了对空发事件的事后分析能力，为系统安全运行提供了依据。

1.2 安全服务

为了保证安全服务，安装了身份认证系统，认证系统中的端点准入防御[3](EAD，Endpoint Admission Defense)功能从网络端点接入控制入手，加强网络终端的主动防御能力，控制病毒、蠕虫的蔓延。EAD 通过安全客户端、安全策略服务器、接入设备以及防病毒软件的联动，可以将不符合安全要求的终端限制在“隔离区”内，防止“危险”终端对网络安全的损害，避免“易感”终端受病毒、蠕虫的攻击。

认证服务器是整个系统的核心部分，控制所有远程用户对网络和应用系统的访问，提供全面的认证、授权和审计服务。用户在登录系统时，通过安全加密通道与远程身份认证服务器通讯，由认证服务器完成对用户身份的认证，并得到当前用户的身份以及系统的授权信息。

本系统还可以支持多种登录方式的灵活定制，可以满足不同情况的需要，及对用户的管理，支持人员账户的查询，修改，删除，及对用户账号的停用和对用户权限的限制，支持对第三方 CA，及一次性口令的认证登录和管理员的登录。这样避免非授人员对系统的访问，提高了系统的安全性。

1.3 安全技术

1)访问控制，访问控制主要通过防火墙设备来实现。通过防火墙访问控制措施，保障防火墙服务器区或内网资源的安全性。限制非授权用户对重要资源的访问能力，同时允许授权开放的资源供外网用户提供访问，最大限度避免将系统漏洞暴露于外部而带来的网络安全威胁。本项目使用的是包过滤(Packet filtering)型防为墙，包过滤型防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址，目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。包过滤方式是一种通用、廉价和有效的安全手段；适用于所有网络服务；包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。

2)VPN 技术，由于建设方的应系统如：资金系统、财务系统、通风系统、瓦斯系统、生产调度系统、电力调度系统等都跨越不同城市，所以本系统利用 VPN 技术来解决这些专网的安全，VPN 的核心是采用隧道技术，将企业专用网的数据加密封装后，透过虚拟的公网隧道进行传输，从而防止敏感数据的被窃取。企业通过公网建立 VPN，就如同通过自己的专用网建立内部网一样，享有较高的安全性、优先性、可靠性和可管理性，而其建立周期、投入资金和维护费用却大大降低。从而保证了其安全。

2 结束语

在安全的信息系统项目的实施中，经过项目组人员一致努力，为用户建立了一套较为完善的信息安全系统，满足了用户需求，得到了用户的好评，同时也积累了实施集团级的安全系统的经验并锻炼了队伍，近而使认识安全是一种意识，而不是某种的技术就能实现真正的安全。除缺乏必要的安全产品和技术引起的不安全因素外，更多的不安全因素来自于管理上的漏洞，要想保证网络的安全，在做好边界防护的同时，更要做好内部网络的管理。安全是永恒的话题，怎样在安全机制、安全服务、安全技术三维空间中，合理运用各类设备各技术、建立满足用户需求的安全策略，还有待于去研究、探索、实践、总结和提高。