企业信息安全从内网安全抓起

王福生[1]，陈志[2]
([1]首钢信息部，北京 100041；[2]首钢自动化信息技术有限公司，北京 100041)

【摘 要】论文结合首钢网络安全建设的情况，阐述了首钢网络安全系统的整体结构。单一的防病毒软件、区域防御系统已经不能满足企业网络安全建设需要，通过在首钢内网的基础平台上建立从技术到管理的纵深防护安全体系建设，保证了首钢信息化业务系统的稳定运行。

【关键词】企业；信息化；网络安全
【中图分类号】TP393 【文献标识码】A 【文章编号】1009-8054(2009) 05-0064-03

Enterprise Information Security Based on Inside Network Security

WANG Fu-sheng[1], CHEN Zhi[2]
([1]Information Dept., ShouGang Group,Beijing 100041, China;
[2]Beijing Shougang Automation Information Technology CO., LTD, Beijing 100041, China)

【Abstract】In this paper, the whole structure of ShouGang network security is described in combination of its construction. Single anti-virvus software or local defence system could not satisfy the requirement by the construction of network security. The construction of network security, including technology of and management on the local network, could ensure the reliable operation.

【Keywords】enterprise; informatization; Network security

0 引言

国际标准化组织(ISO)将“计算机安全”定义为“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露”。由此可以证明，这种计算机安全不单单是网络安全，而是包括整个信息化体系的安全，最核心的是信息安全。内网安全则是大型企业工作的重点。

1 大型企业信息网络现状

大型企业的网络建设一般情况下是从基层建设开始，如首钢总公司就是在整合各个基层单位的局域网基础上，构成总公司级局域网并形成总公司级的应用系统。如ERP和OA的发展，就是在各个基层单位应用的基础上，利用SDH专线等技术手段将跨省市的外地子公司及下属工厂的局域网连接到一起，形成城域网，并建立统一的信息中心。这个城域网并没有打破各下属单位独立的应用系统和独立的网络架构，关键是这个网络是一个混合网，总公司级专用应用系统和企业员工访问互联网的公用应用系统都在一个网里，网络的结构有的是2层，有的3层，有的各重要应用系统间，以及较大的经专线连接的局域网间没有必要的防火墙等设置，网络没有统一的信息安全建设，应用效果大打折扣，只能各自依靠安全管理的规定来维持简单的信息安全。

1.1 网络自身的安全隐患

企业内部网络安全隐患除了网络协议及操作系统不完善外，更大的网络安全威胁来自于企业内部员工，其表现形式多种多样，但归纳起来，有以下几种类型。

(1) 用户操作失误。由于用户水平问题或培训不到位，记过一些误动作或习惯性动作，给内网安全带来影响。部分网管员水平不高，工作责任心差等都对内网构成威胁。

(2) 故意破坏。企业在日常经营生产过程中，势必要对

收稿日期：2008-10-16
作者简介：王福生，男，中共党员，副处长，高级工程师，1986年毕业于北京邮电大学，参加工作后长期在首钢从事电信、信息管理工作，曾主持首钢万门程控电话交换机的安装建设工程、主持参加首钢信息中心的建设、主持首钢网络信息安全体系的建设，现供职于首钢总公司信息部信息管理处。

一些员工的错误进行处理，造成某些员工对企业存有不满情绪或某些员工在利益驱使下受人雇佣进行故意破坏。

(3) 移动介质管理不到位。这是企业内网安全最难防范的一个威胁，如随意使用U盘、破盘等。

(4) 盗版软件泛滥，造成病毒传播。

(5) 管理不到位。各项规章制度形同虚设，如利用终端做游戏，账号及口令管理不严，用户权限分配不合理，服务端口过多过滥等等。

1.2 企业信息安全的主要风险

(1) 非授权访问接入。表现为冒用身份、越权访问，危害是对网络设备、资源的非法占用，影响正常用户使用，甚至破坏内部信息。

(2) 信息泄露。表现为企业内部信息丢失、泄漏，危害是通过隐蔽渠道长期窃取企业信息。

(3) 非法入侵信息系统完整性遭到破坏。表现为恶意删除和篡改信息，危害是干扰正常用户的使用。

(4) 拒绝服务。表现为病毒攻击瘫痪网络，危害是使用户得不到正常的服务。

(5) 攻击。表现为利用网络传播病毒、攻击、获利，危害最大，控制或瘫痪企业信息系统。

2 企业信息安全的内网安全建设

加强内网的安全管理与建设就是要增加各个终端系统的抵抗力，进而消除内网中的“病毒”。

2.1 网络结构的调整

大企业逐步形成的信息系统网络结构主要的特点是混网，最大的优点是节约投资，与分开建设一个上互联网为主的公共网和一套内部办公为主的专用网相比，节约投资50%以上。在现有网络结构的基础上，在不多花钱而改变重大网络结构的情况下，尽可能地降低网络结构造成的安全风险。首先，各个网络之间以SDH专线为大的边界，边界双向部署防火墙，以相对隔开网间的危险渗透；在网络内部实行安全区域管理，以减少同网段内危险的扩散；在条件允许的情况下，逐步将网络结构由2层交换改为3级交换，防止广播风暴的扩散转移。其次，整理不合理的互联网接入问题，每个以SDH为界的局域网网络只能设置一个互联网的出口，秘密信息禁止在企业专网及联网计算机上存放，企业内部处理重大保密信息的计算机要单独组网。

2.2 防病毒系统的建立

首钢总公司根据“总体规划、分析实施”的原则，在“统一标准、统一操作”的架构下兼顾并处理好基层单位的防病毒体系建设。根据企业本身网络拓扑结构和防病毒的要求，选择整个网络防病毒架构为分级管理、多重防护的管理架构(见图1)。

图1 分级管理、多重防护的防病毒管理架构

根据用户端使用人员的技术情况，对客户端的杀毒软件升级可以采取自动和手动相结合的办法，手动定时和自动定时、时时监控杀毒的不同策略；按照不同的分支机构的安全等级和网络级别设定独特的安全策略，便于网络管理员进行管理。同时，配置防病毒网关对病毒从互联网端口进行主动拦截，有效地防止病毒对网络的侵入。

2.3 员工上网行为的规范

我们统一制定的互联网访问策略，将用户和互联网内容分为几类：第一类，全网内的所有访问互联网的用户一律禁止访问的网站：国家明令禁止的反动等内容的网站，公认的病毒性网站，黑客类网站，规避管理的代理性网站，黄、赌、毒类网站；第二类，用户工作时间不得访问与工作无关的大量占用资源的视频类网站、占用带宽的大流量下载工具(如P2P)和网络游戏等网站；第三类，用户访问的内容：一般股票、游戏、体育则限时访问；第四类，与生产控制系统紧密相关联的用户不得访问互联网。这几类用户和访问内容策略要求各局域网和各厂矿遵守执行，分级管理员无法改变。各局域网和各厂矿我们分别设置管理员并给予一定的管理权限，如：在局域网内控制谁能访问互联网，谁能在什么时间访问什么样的网站内容，建立访问内容“白名单”，规定只能访问与工作相关的几个网站和内容。这些访问策略都由分级管理员根据自己网络的情况和工作性质灵活制定，正确处理好安全与易用性之间的矛盾。但有一点是肯定的，那就是收回权限比管理权限更重要，隔离比访问控制更安全。

2.4 落实制度防范的同时强化技术防范

目前，国家有明确的网络安全防范制度、保密制度，各个企业也会根据企业内部的特殊情况制定相应的网络安全制度，因此从制度上保证了企业网络的高安全度。但是，在制

度执行过程中，人为因素很大，所以制度防范是不可靠的。因此，在网络安全防范中要尽可能地减少人为因素，一个最佳的措施就是变制度防范为技术防范，技术防范是硬性的，是不以人的意志而转移的，是绝对可靠的。目前的企业内部网络安全防范策略中，缺乏有效的网络检测和控制功能，一方面导致了不能及时发现和解决网络安全事故，另一方面在网络安全事故发生后，由于没有可信的、完善的网络事件日志，要发现网络安全事故的责任人及了解网络安全事故的原因是非常困难的，因此，在网络安全防范策略中，做好网络安全防范的日志记录是非常有意义的。

要建立网络用户的信息数据库，对访问重点检测数据的用户、访问地点、访问时间有详细记录。建立内部网络主机登录日志，对登录主机的用户、登录时间、退出时间等有详细记录 对发现可疑操作如多次尝试用户名和密码的行为，要及时报警并采取必要的安全措施如关机等，并形成日志记录。对主机访问移动存储介质的操作以及各种在线设备进行监测和控制，如禁用或开启软驱、光驱、USB端口等，并在关机时检测这些解释是否取出驱动器，防止将移动存储介质丢失。要对每次所发生的事件进行记录，并对设备的更改自动形成日志。除了对非授权存取、外联、接入有必要的技术检测手段外，还要及时响应，并形成日志记录。管理员通过对日志的审计，可以发现一些可疑的信息，进行重点跟踪监测。

2.5 灾备建设不容忽视

我们加强了内网安全的建设与管理，但是，一旦出现问题，如何尽快恢复正常工作，将因灾难造成的损失降低到最小程度，也是内网安全建设必须要考虑的问题。

首先要按照《信息安全风险评估指南》的要求，正确进行风险分析，并根据可能造成的业务影响以及灾难恢复目标，设计多种恢复预案，其中之一就考虑了存储系统型异地灾备。这种方式的优点是将数据与运行分开，对主机系统的运行资源影响比较小。另外，由于运行机制大多是利用镜像来复制数据，并借助高速缓冲存储器加速I/O存取，两端的数据差异时间点比较小，加上存储系统本身具有一定的容错能力，使之具有一定运行性能和可靠性。当然，各个单位的情况不一样，所以应当选择自己最适合的灾备方式。

3 企业信息安全的内网管理

内网安全重在防范，在落实大型企业信息安全的内网管理工作中，应该充分分析企业内部网络安全的威胁因素，做到最大限度地保证网络安全，做到重点数据重点防范，重点任务重点监测，将管理监测和控制有机地结合起来，变被动防范为主动防范，根据企业的特殊性质制定出科学、具体有效的安全防范策略。

3.1 信息安全制度建设

从信息安全管理制度的制定和落实抓企业内网的安全管理工作。大型企业内部和各局域网管理单位制定“企业专网信息安全管理办法”，建立以主管领导为组长的信息安全领导小组，设置专职信息安全管理员，明确各应用系统主管部门、各系统的使用单位、信息系统运行维护单位的具体职责和管理上的要求。每季度进行一次信息安全管理的情况(包括安全系统的设备运行数据、安全管理动态)分析并通报全网各个单位和计算机终端用户，要求各个局域网每半年进行一次网络系统的信息安全检查，每年总公司组织一次全网的信息安全检查工作，并通报全公司。信息安全领导小组组织对全年信息安全的情况进行分析，解决信息安全存在的问题，提出下一年度信息安全工作的重点工作。

统一的内网安全策略包括：防病毒策略、员工上网行为管理策略、员工终端计算机管理策略、应用系统认证与权限管理策略。

3.2 对各应用系统的用户的管理

对于应用系统的数据丢失、破坏,甚至攻击，往往是来自系统内部的攻击和终端设备的不安全因素造成的，有的是有意，更多的是无意，我们的管理就是要将这些有意、无意的不安全行为减少到最小。对各应用系统的用户认证与权限控制的管理，首先是对各应用系统的系统管理员、权限管理员、有重要权限用户的身份认证，利用PKI技术采用双因子认证方式，增加这类用户的认证可靠性；要求每个月各系统的管理员权限及密码变换一次，一般用户及权限密码一个季度变换一次，而且密码的长度不得少于8位数且必须数字与字母同用，每次更改密码必须有5位数不相同，不及时变更者将不能再使用，每次进入系统只能试用密码3次，每次限定30秒，否则不能使用；对用户的权限做到最小化，够用就行，每3个月对各用户系统的管理员、用户的用户名及权限进行整理和清理，及时清除那些权限不对、用户调动不用的用户，保证用户和系统的一致性。

3.3 内网客户终端管理

“企业内网管理系统”既是一套软件，更是一套管理系统。在对内网终端设备的管理上借助这套系统，起到终端设备“身份认证”和“安全认证”的功能，达到了内网安全管理的目的。

(1) 设备接入管理。要求每台接入企业网的终端设备(包括台式机、笔记本、服务器等)都必须安装统一的防病毒客户端软件，并且要保证版本和病毒代码随时升级到最新版本，

(下转第69页)

2.3 需要的工作

从上可知，本体系主要基于现有的安防部署进行升级、整合，以最小代价获取最大效益。必要的工作有4部分：

——新的智能化应急系统开发、部署及与现有110应急中心的整合。

——现有警用对讲设备的改装、更新。

——现有的安防设备(监控摄像头及其他等)的改装、升级。

——手机紧急模块的开发及整合。

3 本系统的工作模式及社会意义

3.1 工作模式

一但本系统得以部署，可能的工作模式如下：公民在购买包含紧急报警模块的设备时(基本上为手机等便携常用设备)可申请开通此模块，模块ID数据与个人身份证捆绑。部署于大街小巷的新安防设备形成强大的布控网，每个设备都是一台定位仪，监控着固定的区域，记录着管区内的治安状况。智能化应急中心全时开放，只接受处理两类信号以确保信道通畅：一是定时更新各监控点区内巡警数据，以备紧急通知之需，二是接受、处理紧急状况下来自各个设备的紧急信号。公民的报警模块常态为关闭，而巡警的接受模块全时开放。一但某个呼救信号触发安防系统，流程则如上节所述。

3.2 社会影响及意义

本系统沿袭现有设备及触发模式，在经济及习惯方面几乎无差别，因此可预见的社会接受度高[5]。本系统首创的吓阻模式用声光效益对犯罪行为进行威慑阻止，在一定程度上有扰民的副作用，但精神上却能给公民一定的安全感。本系统的及时取证模式能极大降低犯罪调查的取证成本，大大加强法律制裁的力度及广度，凸显公平效应。本系统的智能处理模式能很好地降低人力成本，减少人为误差，能更快、更准确地对犯罪事件做出反应。本系统的隐蔽性报警方式，可鼓励心有余而力不足的目击者对受害者伸出援手，是社会团结、和谐的有力推动。

参考文献

[1] 刘生荣. 论危害社会治安犯罪的惩治与预防[J]. 中国法学，2001，04(03) 21.

[2] 袁翀. 关于社会治安综合治理的几点思考[J]. 兰州学刊，2002，02(05) 35.

[3] 李建强，李建明. 论建立社会治安防控体系[J]. 铁道警官高等专科学校学报，2003，03(03) 16.

[4] 陈波，江为强. PKI/CA技术的起源、现状和前景综述[J]. 西南科技大学学报(自然科学版)，2003，06(04) 23.

[5] 邹立晔. 统一的公共警报系统[J]. 国际地震动态，2005，04(08) 43.

(上接第66页)

规定客户端系统必处于时时监控和活动状态，每日必须手动或自动查杀病毒一次，否则不能接入网内。

(2) 移动存贮设备管理(包括U盘、硬盘、光驱等)。对重要的生产岗位的终端设备阻止其移动存贮设备的使用；对高权限重要信息的终端设备要求移动设备加密使用。有效地防止了通过移动存贮设备携带病毒和外泄企业秘密的行为。

(3) Websense系统的建立。根据防病毒系统的报告分析发现用户感染病毒多数来源于互联网，所以建设了完善的用户互联网访问管理系统，针对每一个员工、每一个职能部门进行有效的Web访问行为的管理。通过浏览内容的过滤执行总公司互联网访问政策，从而保证员工合理使用公司的网络资源；降低随意的Web访问带来的法律责任风险；封锁间谍软件、恶意传播代码(MMC)和其他基于Web的威胁；管理实时信箱的发送、P2P共享、流媒体和其他高宽带的应用，从而减小互联网病毒感染企业专网终端主机，节约Internet带宽和网络设备包转发资源。针对非80端口的网络流量，Websense系统采用了独立部署方式，利用网络监听原理实现了数据包的分析和策略执行。

4 结语

内网管理和建设对网络信息安全十分重要，它有效地保证了企业信息系统的正常运行。信息安全是一个动态的，因此安全管理也必定是一个动态的管理过程，我们要随着信息系统应用的进一步扩大和安全管理的需要，加大对企业内网安全建设的投入，增加企业内网安全管理的力量，随时满足安全动态管理的需要。

参考文献

[1] 网管员必备宝典—网络安全[M]. 王文寿，王珂，编著. 北京：清华大学出版社，2007，09，26.

[2] 网络管理员手册[M]. 梅刚，孙斌，刘晓霞，编著. 北京：国防工业出版社，2007，02，14.