第29卷 第2期 西 北 地 震 学 报 Vol. 29 No. 2
2007年6月 NORTHWESTERN SEISMOLOGICAL JOURNAL June, 2007

建立地震信息服务系统的网络安全管理体系的探索

郝 柽，梁子斌，李少华，郝 臻，张立红
（甘肃省地震局，甘肃 兰州 730000）

摘 要：以国际信息安全标准BS7799/ISO17799为信息安全管理体系的准则，根据《中国地震局信息安全等级保护建设方案》的相关要求和规定，通过分析信息网络的层次关系，在科学的安全框架之上，探讨建立以防火墙系统、VPN应用系统、网络反病毒软件，以及入侵检测系统(IDS)安全策略为核心的地震信息服务系统网络安全管理体系构。

关键词：地震信息服务系统；网络；安全；管理体系
中图分类号：TP393.09 **文献标识码**：A **文章编号**：1000－0844(2007)02－0165－05

Exploration for Establishing the Network Security Management of Earthquake Information Service System

HAO Cheng, LIANG Zi-bing, LI Shao-hua, HAO Zhen, ZHANG Li-hong
(*Earthquake Administration of Gansu Province, Lanzhou 730000, China*)

Abstract: Taking the international information security standard BS7799/ISO17799 as criterion of the information security management system, according to the related stipulations from China Earthquake Administration, through analyzing the level relationship of information network and based on the scientific security frame, a Earthquake Information Service System for the network security management is established, which mainly includes the fire wall system, the VPN application system, the anti-virus software for network and IDS.

Key words: Earthquake Information Service System; Network; Security; Management system

0 引言

“地震信息服务系统”是“中国数字地震观测网络”的基础支撑平台，它为数字地震观测网络项目中的其它业务系统(测震、前兆、应急、强震和活断层探测)提供基础的信息通信平台[1]。它的主要工作内容是为地震及相关行业提供数据、信息服务；为政府部门进行重要决策提供信息保障。随着网络技术的发展，网络应用的拓展，网络结构的多样化，网络拓扑结构的复杂化，对数字地震观测网络提出了更高的安全需求，特别是互联网上的不良信息、非法入侵、系统漏洞、病毒等又对地震信息服务系统产生了巨大的威胁，需要提供统一的安全访问策略、安全技术和安全管理[2]。所以网络安全管理体系建设在“中国数字地震观测网络”项目中地位重要，已经成为各级领导、网络管理员非常重视的问题。本文结合地震行业的特点和网络管理实践经验，在网络安全管理建设方面做一些粗浅的探讨。

1 地震信息服务系统的主要安全威胁

地震信息服务系统网络所面临的安全威胁主要指对网络中信息、设备的威胁，归结起来主要有三类：

(1) 人为的无意失误：如操作员安全配置不当造成安全漏洞，用户安全意识不强，用户口令选择不慎，将自己的帐号随意转借他人或与别人共享等。

(2) 人为的恶意攻击：这是计算机网络所面临的最大威胁，又可以分为以下两种：一种是主动攻

收稿日期：2006-08-17
中国地震局兰州地震研究所论著编号：LC20070006
作者简介：郝 柽(1971－)，男(汉族)，河北正定人，工程师，现主要从事地震信息网络维护工作.

击，以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，是在不影响网络正常工作的情况下进行截获、窃取、破译以获得重要机密信息。

(3) 网络软件的漏洞和“后门”：网络软件不可能是百分之百的无缺陷和无漏洞的，这些漏洞和缺陷恰恰是黑客进行攻击的首选目标。已发生的黑客攻入网络内部的事件大部分都是利用软件漏洞进行的。另外，软件的“后门”是软件公司的设计编程人员为了自便而设置的，一般不为外人所知，但一旦“后门”洞开，其造成的后果将不堪设想。

2 信息网络国际安全标准

目前国际上具有代表性的安全管理体系标准是BS7799，包括两部分：BS7799－1：1999《信息安全管理实施细则》；BS7799－2：2002《信息安全管理体系规范》。其中BS7799－1：1999被ISO(国际标准化组织)委员会评审、讨论通过，成为了信息安全领域的国际安全标准ISO/IEC17799：2000。ISO/IEC17799是基于最佳实践的成功的信息安全管理体系方法，为信息安全提供了一套全面综合的控制措施[3]。

BS7799/ISO17799标准共分两部分，内容涉及信息安全技术、管理和法律问题。第一部分是信息安全管理实践指南，提供了一些如何做或者好做法的指导，单位确保信息安全需要采取的措施、建议和推荐做法；第二部分是信息安全管理体系规范，提供了建立有效信息安全管理体系框架的建议，信息安全管理体系的开发和实施细则。信息安全管理体系可以根据单位的需求有所发展变化。BS7799/ISO17799标准中提及10个信息安全领域36个控制目标和127个控制点(2005年最新ISO17799涉及11个信息安全领域39个控制目标133个控制点)，标准中列出的最佳实践控制项是企业有效管理信息安全的基础，依据BS7799/ISO17799的实施原则，企业可以检测、分析和降低信息安全风险[4]。

2004年我国发布《计算机信息系统安全保护等级划分准则》，也是参考了国际标准BS7799/ISO17799信息技术安全性评估准则，该准则是以对信息安全分等级、按标准进行建设、管理和监督为核心，将信息系统安全分为相应的五个安全保护等级[5]。

3 地震信息服务系统网络安全管理体系

网络安全体系的核心目标是实现对网络系统和应用操作过程的有效控制和管理，通过实施一整套适当的控制措施实现信息安全。控制措施包括策略、实践、步骤、组织结构和软件功能。

信息安全具有以下特征：(a)保密性：确保只有经过授权的人才能访问信息；(b)完整性：保护信息和信息的处理方法准确而完整；(c)可用性：确保经过授权的用户在需要时可以访问信息并使用相关信息资产。

安全管理必须架构在科学的安全体系和安全框架之上，因为安全框架是安全方案设计和分析的基础。为了系统、科学地分析网络安全系统涉及的各种安全问题，网络安全技术专家提出了三维安全体系结构，并在其基础上抽象地总结了能够指导安全系统总体设计的三维安全体系(图1)，它反映了信息系统安全需求和体系结构的共性。

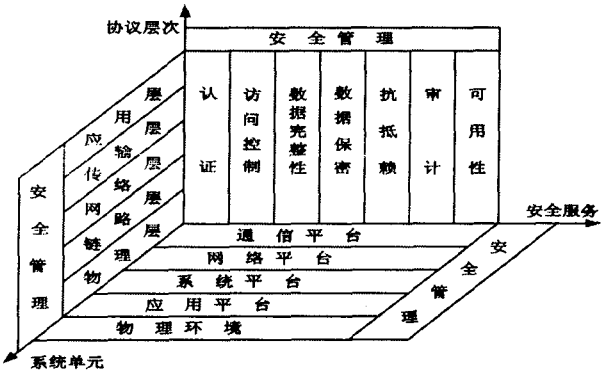

图1 网络安全框架示意图

Fig. 1 Sketch of security frame in network security.

地震信息服务系统网络安全体系是根据《中国地震局信息安全等级保护建设方案》的要求，参照国际信息安全管理标准BS7799/ISO17799，综合考虑可实施性、可管理性、可扩展性、综合完备性、系统均衡性等方面，同时考虑所保护资源的价值，实现所需费用，可用资金的限制，对用户可能造成的消极影响，安全方案的可扩充性以及维护费用等因素，主要采用的安全管理是：

(1) 身份认证：用于确认所声明的身份的有效性；

(2) 访问控制：防止非授权使用资源或以非授权的方式使用资源；

(3) 数据保密：数据存储和传输时加密，防止数据窃取、窃听；

(4) 数据完整：防止数据篡改；

(5) 不可抵赖：取两种形式的一种，用于防止发

送者企图否认曾经发送过数据或其内容和用以防止接收者对所收到数据或内容的抗否认;

(6) 审计管理:设置审计记录措施,分析审计记录;

(7) 可用性、可靠性:在系统降级或受到破坏时能使系统继续完成其功能,使得在不利的条件下尽可能少地受到侵害者的破坏。

BS7799/ISO17799 是安全管理体系实施的准则,构建一个信息安全管理体系,需要重点考虑以下 10 个步骤:

(1) 安全方针—表明对信息安全体系的支援和承诺;

(2) 安全组织——个已建立的管理架构,用于单位内部信息安全的管理和控制,以及执行现有的信息安全规定;

(3) 资产的分类和控制—确保对单位各项资产的安全进行有效保护;

(4) 人员安全—明确所有单位人员在安全方面的职责和任务;

(5) 环境安全—对单位内部人员提出简单明确的安全要求;

(6) 沟通和运行管理—完善单位内外的联系,以利于信息安全管理体系的顺利运行;

(7) 存取控制—加强网络管理,确保具有许可资格的人员才能进入并使用网络信息;

(8) 开发和维护—确保单位相关资料的控制和加密;

(9)持续的管理—制定和维护单位紧急应变计划,保护关键业务活动免受重大灾难的影响;

(10) 符合法规—符合信息安全法律或规定的相关要求。

4　地震信息服务系网络安全技术措施

信息网络安全管理体系必须实现从 Internet 进入内部资源网络的数据被有效检查和过滤,所有对内部资源网络的访问可以被有效控制,移动用户从 Internet 进入内部网络进行业务操作的通信和通过广域网进入内部网的用户通信必须加密,所有网络访问行为能够被记录和审计,非法访问被预警和阻拦,应用系统平台及数据可以被有效备份以抗击灾难风险,用户的身份的真实性认证等几方面的目标。

地震信息服务系统网络安全体系是行业网络中各类安全系统硬件、软件及其配套网络安全管理策略和措施的总和。网络安全体系与网络管理平台具有良好的接口[1]。

地震信息服务系统网络安全体系中包括以下常规技术工作:

(a) 安全设备管理。分级对全网的安全设备进行设置和配置,对网络中所有的安全产品,如防火墙、VPN、防病毒、入侵检测(网络、主机)、漏洞扫描等产品实现统一管理、统一监控。

(b) 安全信息管理。管理来自于全网各个安全设备的信息,对网络中的安全设备、操作系统及应用系统的日志信息收集汇总,实现对这些信息的查询和统计。并通过对这些集中的信息的进一步分析,可以得出更深层次的安全分析结果。

(c) 安全事件管理。监视潜在安全隐患,事件触发相应的安全事件应对预案,即管理、保护及自动分发全局性的安全策略,包括对安全设备、操作系统及应用系统的安全策略的管理。

构筑网络安全系统的最终目的是对网络资源或者说是保护对象实施最有效的安全保护。从网络的系统和应用平台对网络协议层次的依赖关系不难看出,只有对网络协议结构层次的所有层实施相应有效的技术措施,才能实现对网络资源的安全保护。针对地震信息服务系统网络的结构和应用要求,为了达到保护网络资源的目的,设立了相应的安全措施,见表 1。

表 1　地震信息服务系统的安全措施

	物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
认证			*	*		*	*
访问控制			*	*		*	*
数据保密	*	*	*	*		*	*
数据完整性			*	*		*	
不可抵赖性						*	
审计			*	*	*		*
可用性	*	*	*	*			

注 * 表示需要实施

作为全方位的、整体的网络安全管理体系也是分层次的,不同层次反映了不同的安全问题。根据地震信息网络的应用情况和网络的结构,我们将安全防范体系的层次划分为物理层安全、系统层安全、网络层安全、应用层安全和安全管理[6]。

(1) 物理环境的安全性(信息网络运行的物理环境)

该层次的安全包括通信线路的安全、物理设备的安全、机房的安全等,主要体现在通信线路的可靠性(线路备份、网管软件、传输介质)、软硬件设备安全性(替换设备、拆卸设备、增加设备)、设备的备份、防灾害能力、防干扰能力、设备的运行环境(温度、湿

度、烟尘)等。要可靠设计不间断电源(ups)保障,提供一定的冗余,保证网络供电系统的安全。防止非法进入计算机房和各种偷窃、破坏活动的发生。

(2) 操作系统的安全性(信息网络的操作系统平台)

该层次的安全问题来自网络内使用的操作系统的安全,如 Windows2000,Windows 2003,Solaris,Linux 等。主要表现在三方面:一是操作系统本身的缺陷带来的不安全因素,主要包括身份认证、访问控制、审核、系统漏洞等;二是对操作系统的安全配置问题;三是病毒对操作系统的威胁。

(3) 网络的安全性(信息网络的通信平台)

该层次的安全问题主要体现在网络方面的安全性,包括网络层身份认证、网络资源的访问控制、数据传输的保密与完整性、远程接入的安全、域名系统的安全、路由系统的安全、入侵检测的手段、虚拟专用网(VPN)应用等。

(4) 应用的安全性(信息网络各种应用的开发、运行平台)

该层次的安全问题主要由提供服务所采用的应用软件和数据的安全性产生,包括应用程序的加固,如 Web 服务、电子邮件系统、DNS、FTP 服务等。数据库系统主要包括 Oracle,MS SQL 数据库。需要对这些系统进行安全漏洞的扫描和实时入侵的检测。

(5) 管理的安全性(信息网络运行的管理制度和人员管理)

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。管理的制度化极大程度地影响着整个网络的安全,严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其它层次的安全漏洞。

5 地震信息服务系统网络安全策略

根据《中国地震局信息安全等级保护建设方案》的相关要求和规定,地震信息服务系统安全策略是信息系统具体的安全实施的依据和基础,是单位所有安全行为的准则[2],它主要包括四个方面:防火墙、VPN、反病毒软件,以及入侵检测系统(IDS)。防火墙可以检测数据包并试图阻止有问题的数据包;VPN 则是在两个不安全的计算机间建立起一个受保护的专用通道;反病毒软件提供了实时监控、全面查杀、病毒隔离、邮件防护等多种功能;入侵检测系统是一种网络安全系统,当有恶意用户试图通过 Internet 进入网络甚至计算机系统时,IDS 能够检测出来并进行报警,通知网络该采取措施进行响应。

(1) 防火墙安全策略

网络层安全系统通过防火墙系统实现访问控制、网络信息检查、通信加密、非法入侵检测和拦截,异常情况告警和审计几大功能目标[7]。在 Internet 和地震行业网的进出口,防火墙系统通过有效的策略选择可以阻断有害的网络数据和被禁止的数据源进入单位内部网络。从互联网入口进入信息网内部的用户,可以被防火墙有效地进行类别划分,即区分为通过互联网进入内部网的单位移动用户或外部的公共访问者。对于要求进入信息网内部网的访问者进行用户的授权认证,拦截没有用户权限的访问者试图进入内部网,同时可以实现按照单位资源被访问权限划分的访问路由控制。对于内部或外部的本单位用户而言,防火墙系统可以实现单位各类资源的应用系统在逻辑上进行子网系统的划分,即在技术上提供可以独立选择安全策略的虚拟系统划分。

防火墙的安全策略主要包括:利用防火墙将内部网络、Internet 外部网络、DMZ 服务区、安全监控与备份中心进行有效隔离,避免与外部网络直接通信;防火墙建立网络各终端和服务器的安全保护措施,保证系统安全;配置防火墙对来自外网的服务请求进行控制,使非法访问在到达主机前被拒绝;利用防火墙使用 IP 与 MAC 地址绑定功能,加强终端用户的访问认证,同时在不影响用户正常访问的基础上将用户的访问权限控制在最低限度内;利用防火墙全面监视对服务器的访问,及时发现和阻止非法操作;利用防火墙及服务器上的审计记录,形成一个完善的审计体系,建立第二条防线;根据需要设置流量控制规则,实现网络流量控制,并设置基于时间段的访问控制。

(2) 虚拟专用网(VPN)安全访问控制策略

VPN 应用是为网络通信提供有效的信息加密手段[7]。在 VPN 应用中,应采用三倍 DES 的加密技术,这是目前可以获得的最先进和实用的网络通信加密技术手段。网络的 VPN 应用范围包括移动用户的客户机到单位网络 Internet 出入口的防火墙、各区域中心的广域网出入口防火墙到国家中心广域网出入口防火墙。

VPN 系统安全策略的设定:控制用户访问,对于来自各个省级内部网的具有固定(静态)IP 地址的访问可基于 IP 地址和使用的服务进行控制;而对

于拨号用户或具有动态IP地址的用户,可采用网关中的用户身份认证系统功能,通过识别用户的身份来控制用户的访问请求。对系统内的合法用户,可以限制对内部重要服务如中心数据库等的使用,仅开放允许访问的内部资源的使用权,只允许浏览授权的信息或传送文件;控制内部网用户出访;识别系统各种中心内的主机IP地址的合法性,防止内部主机IP地址的滥用;对所有访问控制过程进行记录。

(3) 防病毒策略

所有联网计算机都应统一安装网络杀毒软件,非联网计算机也应安装杀毒软件并经常更新病毒库。计算机之间进行文件拷贝或邮件收发之前都应进行检查病毒工作。已确认感染病毒的计算机应及时拔掉网线,在未经管理员处理之前不能与其他计算机进行网络连接和文件传输。每周定期进行病毒扫描及清理。定期对网络系统中各个工作站计算机进行病毒监测和清理,并进行详细记录。严禁使用来历不明的软件,对于来历不明的、可能引起计算机病毒的软件应使用杀毒软件查毒、杀毒。应根据权威网站(http://www.antivirus－china.org.cn)公布的流行性或重大恶性病毒及时下载系统补丁和杀毒工具,采取相关措施,防范于未然。

(4) 入侵检测系统(IDS) 策略

IDS能够帮助网络系统快速发现攻击的发生,它扩展了系统管理员的安全管理能力(包括安全审计、监视、进攻识别和响应),提高了信息安全基础结构的完整性[8]。

IDS的主要策略是:对网络边界点的数据进行检测,防止黑客的入侵;对服务器的数据流量进行检测,防止入侵者的蓄意破坏和篡改;监视内部用户和系统的运行状况,查找非法用户和合法用户的越权操作;对用户的非正常活动进行统计分析,发现入侵行为的规律;实时对检测到的入侵行为进行报警、阻断,能够与防火墙/系统联动;对关键正常事件及异常行为记录日志,进行审计跟踪管理。完成对以下的攻击识别:网络信息收集、网络服务缺陷攻击、Dos&Ddos攻击、缓冲区溢出攻击、Web攻击、后门攻击等。要经常保持安全补丁保持自动更新,根据网上公布的系统漏洞信息随时更新,并关闭不必要的服务和端口[8]。

6　结束语

地震信息服务系统的网络安全体系应该是一个动态的、立体的、全面的体系,是以整体策略为核心,以技术为根本,以管理为基础。它必须建立在技术、组织和制度这三个基础之上,是一个集管理、法规、技术综合作用为一体的、长期的、复杂的系统工程。

感谢台网中心李卫东先生对此文的帮助。

[参考文献]

[1] 李卫东,等.中国地震信息服务系统技术规程[M].北京:地震出版社,2005.

[2] 国际标准.BS 7799－2:2002.信息安全管理规范[S/OL].[s.n.],[2005].http:www.isra.infosec.org.cn/pgbz/infosec-mangage/200604/1166.html.

[3] 国际标准.,ISO/IEC 17799:2000.信息安全管理规范[S/OL].[s.n.],[2005].http:searchwhatis.techtarget.com.cn/searchwhatis/362/1948362.shtml.

[4] 中华人民共和国国家标准.GB17859-1999.计算机信息系统安全保护等级划分准则[S].北京:中国标准出版社,2000.

[5] 毛汗书.网络技术基础[M].北京:人民邮电出版社,2000.

[6] Cisco system.思科网络技术学院教程[M].北京:人民邮电出版社,2002.

[7] 何艳辉.网管员必读——网络管理[M].北京:电子工业出版社,2005.