文章编号:1674-6139(2010)11-0017-03

地市级环保数据网络的安全现状与对策

封龙,徐浙峰,丁长春

(淮安市环境监测中心站,江苏 淮安 223001)

摘 要:从地市级环保数据网络的安全现状展开调查,分析网络各个应用可能存在的安全漏洞和安全风险,并分析其解决方法,研究结果将对中国地市级进行环境信息系统的安全运行具有借鉴作用。

关键词:环境;信息系统;数据库;网络;安全

中图分类号:X32 **文献标识码**:A

Municipal Environmental Data Network Security and Countermeasures

Feng Long, Xu Zhefeng, Ding Changchun

(Environment Monitoring Central Station of Huai'an City, Huai'an 223001, China)

Abstract: Municipal environmental data network from the ground the security status of investigations into the various applications of the network potential security vulnerabilities and security risks and to analyze their solutions. The results will be in China to the municipal environmental information system for the safe running reference.

Key words: environment; information system; database; network; security

随着Intranet的广泛应用,内部网的安全问题也得到越来越多的关注,特别是网络病毒的泛滥、网络黑客的攻击、数据信息的泄密等,无不牵动着单位领导敏感的神经。地市级环境数据网络在全国环境信息网络中占有非常重要的地位,目前大部分的环境原始数据都产生和存储在地市级环保网络中,有些数据还涉及到国家机密,这些情况客观上要求对现有的网络和数据存储安全要有足够的重视,使之能安全、可靠、稳定、高效运行。

1 目前地市级环保数据网络的现状

目前中国环保网络自上而下分为:环保部、省环保厅、市环保局、县环保局四层网络结构,市级环保网络起着承上启下的关键作用,早在2000年前后,国家环境保护总局就非常重视市级信息网络的建设,先后对全国100多个地级市实施了"世行贷款"和"日援项目",项目的成功使市级在办公自动化和数据处理能力上得到了很大的提高。近期在省、市两级财政的支持下环保网络都得到了升级和改造,在网络建设上以TCP/IP协议为基础,星型网络拓扑结构,WEB为核心应用,构成统一和便利的信息数据处理平台。

2 环境数据的分类和存储

目前环境数据主要有:环境统计、排污申报、例行监测、污染源在线监测、污染源普查等数据,这些数据分别由环保局几个部门来收集录入和存储,最终存入数据中心的SQL SERVER服务器中,市局各处室通过内部局域网浏览实时和历史数据,这样实现了资源共享,提高了办公效率,随着用户的增长,数据量的增大,后台维护都集中在中心服务器上,这样加大了系统维护人员的工作量。

3 环境数据网络与数据面临的威胁

城市级环境信息网络发展很快,建成并使用的系统多,但出现的安全问题也多,运行过程中的问题更多,安全解决方案没有跟上;随着政务信息公开的力度越来越大,在公网和内网的应用越来越多,来自网络内外的威胁越来越频繁、越来越严重。主要有:

(1)系统安全漏洞。网络入侵大多利用了安全漏洞,包括安全管理的漏洞、操作系统的漏洞、数据库系统的漏洞、应用系统的漏洞、网络管理的漏洞。

(2)ARP攻击导致网络瘫痪[1]。ARP协议是

收稿日期:2010-06-08

作者简介:封龙(1977-),男,工程师,大学本科,从事环境信息管理工作。

"Address Resolution Protocol"(地址解析协议)的缩写,它是一个链路层的协议,工作在OSI模型的第二层,在本层和硬件接口间进行联系,同时对上层(网络层)提供服务。ARP病毒攻击造成网络严重拥堵,局域网内上网速度很慢,这种情况是有ARP请求广播风暴,当主机感染ARP病毒后,不断向局域网内几乎所有主机进行扫描,大量的ARP请求广播占用大量的网络资源造成网络的阻塞。

(3)数据泄露或丢失[2]。指原始数据在有意或无意中被泄露出去或丢失,它通常包括:恶意攻击而导致的信息在传输中丢失或泄露,环境信息网络没有和外网Internet物理隔离,来自Internet的攻击是主要的。这些威胁包括:网络报文嗅探、IP欺骗、数据包重发、拒绝服务攻击、远程暴力字典式破解、系统身份欺骗、通信窃听等,而互联网上有大量的"黑客"软件,不需要太高深的计算机知识就可以利用"黑客"软件进行攻击。

(4)SQL Server漏洞[3]。SQL Server和其他大型网络数据库一样,都属于"端口"型数据库,这意味着居心不良的人可以使用分析工具试图连接到数据库上,尝试绕过服务器系统的安全机制,从而得以进入系统,破坏和窃取机密的数据资料,严重情况下会危及整个系统的安全。对于许多需要远程访问敏感数据的单位而言,将大大增加数据保护的风险。数据库安全性问题一直是围绕着数据库管理员的难题,数据库数据的丢失以及数据库被非法用户的侵入使得数据库管理员身心疲惫不堪。

(5)传播病毒。病毒随着互联网的发展而快速发展,计算机病毒的传播速度越来越快,影响范围越来越大,危害的对象不仅仅局限于个人计算机,还威胁到服务器和主干网络。目前环境信息网络安全受到最常见的威胁来自计算机病毒和木马程序,环境信息网中已经发现网络病毒对数据服务器的破坏、病毒引起的网速变慢、数据消失、系统无法正常响应等情况。现在很多地级市因为资金原因,内网和外网没有做到物理隔离,办公内网与公网混合使用,任意在互联网上下载不安全的控件和程序,通过网络传播计算机病毒,其破坏性大大高于单机系统,而且用户很难防范。

(6)网络配置不合理。因为经费等原因,市级信息网络不能完全按照《环境信息网络建设规范》(HJ 460-2009)标准来进行建设,网络中没有配置防火墙、入侵检测和磁盘阵列等安全设备,无事故应急替换设备,一旦有突发事故必将造成数据丢失。

4 环境数据网络安全对策[1]

国家环保部已经发布了六条信息管理标准,其中囊括了环境数据库设计与运行管理规范、环境信息网络建设规范、网络管理规范,它是对信息资源的合理使用、管理规则的正确描述,是整个信息网络和数据安全建设的基础和依据。结合各地的实际情况,总结了如下的一些方法与对策:

(1)物理层控制。物理层的安全设计应从三个方面考虑:环境安全、设备安全、线路安全。采取的措施包括:机房屏蔽,电源接地,布线隐蔽。另外,根据各地保密局委有关文件规定,凡是计算机同时具有内网和外网的应用需求的,必须采取内网外网安全隔离技术,保密办公内网采用屏蔽双绞线和屏蔽模块等保密设备,在计算机终端安装隔离卡、双硬盘结构,使内网与外网之间从根本上实现物理隔离,防止涉密信息通过外网泄漏。

(2)数据链路层控制。主要是利用VLAN技术将内部网络分成若干个安全级别不同的子网,从而实现内部一个网段与另一个网段的逻辑隔离。因此对于地市级环保网络,可以划分为机关、监测、监理三个子网,有效防止某一网段的安全问题向整个网络传播,可限制局部网络安全问题对全网造成大范围影响。

(3)访问数据权限的控制。访问权限控制是指对主体访问客体的权限或能力的限制,包括出入控制和存取控制。它是在身份识别的基础上,根据身份对提出的资源访问请求加以控制。常用的做法是把数据分为几个等级,不同的部门给与相应的权限,读取的数据的内容,防止窃取原始数据。

(4)病毒防护控制。对病毒防护更广泛的定义是防范恶意代码,包括木马、逻辑炸弹和其他未经授权的软件,保护的范围包括网关、服务器、工作站等。对防病毒产品的病毒库和杀毒引擎要及时更新,这样才能保证对新的病毒和一些未知病毒的查杀能力。

(5)设置防火墙、入侵检测等网络安全设备。防火墙在作为一个或一组在不同策略的网络或安全域之间实施访问控制,构建了一道安全屏障,它可以有选择的拒绝非法端口,允许合法的TCP/IP数据流通过,以保证内部网的数据和资源不会流向非法地点。通常使用包过滤、应用级网关、代理技术等安全控制手段实现其安全防护功能。入侵检测设备分为主机型入侵检测系统和网络型入侵检测系统,具有数据探测、入侵分析、入侵响应、管理控制、检测结果处理。安全审计网络脆弱性扫描系统是网络安全防

御中的一项重要技术，对采用的安全策略和规章制度进行评审，发现不合理的地方，擦用模拟攻击的形式对目标可能存在的已知网络脆弱性进行逐项检查，确定存在的安全隐患和风险级别。

(6) SQL SERVER 的安全策略[2]。保护 SQL 和网络连接，在实例属性中的 TCP/IP 协议的属性的默认端口 1433 更改为其他端口，同时对路由器或防火墙上进行相应的设置，屏蔽 1433 端口；使用安全帐号策略，对 sa 这个超级用户进行最强的保护，最好不要在数据库应用中直接使用 sa 帐号；正确分配使用权限，很多主机使用数据库知识来查询、修改等简单功能的，可以根据实际需要赋予仅仅能满足应用要求和需要的权限；我们可以把权限分配给角色而不是直接把它们分配给全局组，这种能力使得我们能够轻松地在安全策略中使用 SQL Server 验证的登录。

5 结语

本文通过对地级市环境数据网络现状分析，提出了环境数据网络安全的解决方法，可以有效地提高安全策略的合理性，以及做出响应的及时性，从而有效地提高网络系统的安全性和稳定性。总的来说，应该在不断采用新的安全技术的基础上，加强系统人员和使用人员的管理和培训，强化各项规章制度，加强人员安全意识，从而建立起一套适合环境数据网络的安全体系。环境数据网络系统是一个融合环境数据和计算机网络技术于一体的复合体，其安全建设要求统一规划、长远考虑、保证技术的先进性和可扩展性。在技术上要求适应数据的增长变化，不仅包括物理安全、系统安全、网络安全、应用安全等多方面内容，需要诸如防火墙、防病毒产品、身份认证等多种安全设备、安全技术作为保障手段。

参考文献：

[1](美)海吉(Bhai Ji, Y.)著，罗进文等译. 网络安全技术与解决方案[M]. 北京：人民邮电出版社，2009(3).

[2]王达编著. 网管员必读——网络安全(第2版)[M]. 北京：电子工业出版社，2007(6).

[3]韩朝军，等. 编著，SQL Server 管理与开发技术大全[M]. 北京：人民邮电出版社，2007(4).

(上接第11页)

表9 C-P层次的总排序结果

层次C / 层次B	C_1 0.36	C_2 0.18	C_3 0.148 5	C_4 0.148 5	C_5 0.109	C_6 0.054	总排序权值
P_1	0.125	0.065	0.505	0.06	0.056	0.100	0.152
P_2	0.273	0.307	0.112	0.299	0.285	0.300	0.262
P_3	0.219	0.192	0.135	0.442	0.173	0.300	0.234
P_4	0.384	0.436	0.248	0.199	0.486	0.300	0.352

根据总排序结果可知(见表9)，分选工艺流程方案4(P_4)最优，即根据淮安市生活垃圾特点设计的分选工艺为最优分选工艺。

3 结论

(1)人工手选 + 卫生填埋的方案权值最小，说明现阶段淮安市城市垃圾的产量大，虽然人工分选效果比较好，但分选效率低，已经满足不了现阶段垃圾处理的要求。

(2)根据淮安市生活垃圾性质制定的分选方案的权值最大，说明不同地区的垃圾分选工艺不同，根据该地区实际状况及垃圾特性制定的分选方案才是最适合的方案。P_2 的城市生活垃圾简易分选法具有广泛的适用性，而不具备针对性，P_3 适合南方潮湿地区分选工艺只具有针对性，但不是针对淮安市的状况，所以这两种分选工艺虽然也是比较好的方案但不能成为淮安市生活垃圾处理的最优方案，权值次于 P_4。

(3)由于城市生活垃圾的复杂性，任何一种单一的分选技术都是无法将其中的物质完全分离出来，所以需要将各种分选技术加以综合，组成一定的工艺流程，才能达到良好的分选效果。

参考文献：

[1]庞建峰，赵洪飞. 淮安市生活垃圾的处理现状控制对策[J]. 能源与环境，2008，1：107－108.

[2]周翠红，路迈西，吴文伟，等. 北京市城市生活垃圾产量预测[J]. 中国矿业大学学报，2003，32(02)：169－173.

[3]赵全升，李悦，谢新民等. 环境系统分析原理[M]. 北京：地质出版社，2005.

[4]张禄文，孙可伟. 城市垃圾资源化分选工艺[J]. 中国资源综合利用，2003，9：10－12.

[5]王晋，李定龙，张凤娥. 城市生活垃圾处理模式选择判断方法研究. 江苏工业学院学报，2006，18(2)：15－18.

[6]吴克，俞志敏，金杰，等. 合肥城市生活垃圾处理方案选择探讨[J]. 合肥学院学报(自然科学版)，2008，18(03)：56－60.