文章编号：1006-4354（2011）03-0045-03

陕西气象短信系统网络安全策略简析

杨承睿，张　宏，任　芳
（陕西省气象科技服务中心，西安　710014）

中图分类号：TP393.08　　文献标识码：B

目前陕西省气象部门广域网络已有相对完善的安全防御体系，硬件防火墙、漏洞扫描、防病毒等网关级别、网络边界方面的防御均已形成体系，重要的安全设施大多集中于专业级机房或网络入口处，在这些设备的严密监控下，来自网络外部的安全威胁大大减小。相反，网络内部计算机客户端缺乏必要的安全管理措施，安全威胁较大。未经授权的网络设备或用户可通过局域网的网络节点进入气象短信网络系统，形成极大的安全隐患。目前，网络系统本身的安全弱点是气象短信系统网络安全的主要隐患，而系统在使用和管理过程中的疏漏更增加了安全问题的严重程度。

1　气象短信系统网络结构

目前陕西气象部门的数据通讯网络主要是172.X.X.X网段，为了增加气象短信系统的网络安全管控能力，同时保证日常业务数据的正常使用，气象短信系统网络设计为192.X.X.X网段，两个网段的数据交互通过一个节点来实现（见图1）。有针对性的做好边际设备的安全管理工作，可有效提高气象短信系统的网络安全防护能力。

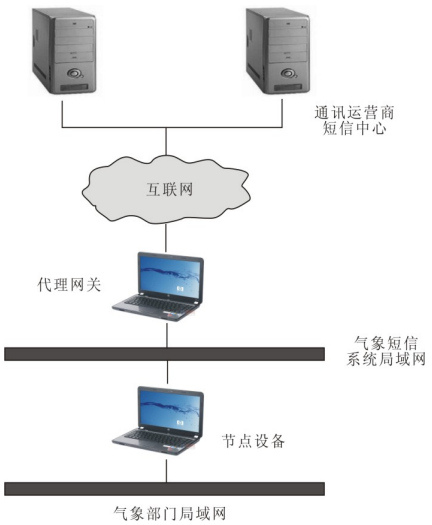

图1　陕西气象短信系统网络结构

2　影响气象短信系统网络安全的因素

气象短信系统的运行环境是基于windows操作系统，相对于unix系统来说，安全稳定性较弱。由于短信的数据交换必须通过互联网传输，因此，防范来自互联网上的恶意攻击，也是气象短信系统必须考虑的。

2.1　外部网络的不安全性

目前气象短信的传输协议是国内各大通信运营商以TCP/IP协议作为底层通信承载开发的各类点对点协议，由于TCP/IP协议在网络安全性方面的欠缺，加上TCP/IP协议的开放性，因此众多熟悉它的程序员（或黑客）可轻易地利用其安全缺陷来实施网络攻击。随着计算机网络技术的不断发展，计算机病毒和木马程序等来自外部的安全威胁，同样不可轻视。对于气象短信百万级的用户数据来说，木马程序等恶意代码带来的威胁甚至要大于普通病毒带来的威胁[1]。

2.2　内部网络的不安全性

气象短信系统的交换式局域网，采用的接入层设备是交换机，局域网的内部数据通过“端到

收稿日期：2010-08-30

作者简介：杨承睿（1978—），男，汉族，西安市人，硕士，工程师，从事气象科技服务。

端”方式传送交互，虽然减小了主机劫持、网络窃听等威胁的风险系数，但仍然可以采取 ARP 欺骗，甚至是采用交换机端口镜像的方式进行数据窃听[2]。这种来自于内部网络的不安全性也是无法回避的。

2.3 人为因素的不安全性

网络管理员或系统管理员对安全配置的不当操作也容易造成安全隐患。如将自己的用户名随意泄露或与他人共享，密码设置过于简单且没有定期修改等，都会对网络安全构成威胁。

3 气象短信系统网络安全策略

3.1 提高边际设备防护能力

网关是内外网数据交换的必经之路，也是内外网连接的咽喉。气象短信系统采用代理网关连接外部互联网与内部局域网，其优势是网络数据包的交换不在内外网络间直接进行，内部局域网系统必须通过代理网关才能访问互联网，同时它还能够阻止外部网络非法访问、入侵，方便管理员在边际设备这一环节进行有效的网络安全防护。

目前气象短信系统是通过路由器来实现代理网关功能。通过路由器来限定外部互联网指定 IP（通讯运营商短信中心）的访问，同时只开放业务必须的通讯端口访问权限。这样的网络结构能够有效提高内部网络的安全性，并通过 IP 地址的过滤规则将不安全服务的风险降低，使网络安全防护能力得到进一步加强。

3.2 提高恶意代码的防控能力

对于气象短信系统而言，来自内部 PC 机和服务器之间的入侵行为以及恶意代码造成的内外勾结的侵略行为，代理网关很难控制，因此针对内部网络系统的安全需求必须通过杀毒软件来实现。对病毒等恶意代码的防控工作要分防御和查杀两部分。而防止病毒等恶意代码的入侵比查杀更重要。

防控病毒的重点是对病毒行为的判断和控制病毒的传播，如何有效辨别病毒行为与正常程序行为是防控病毒成功与否的重要因素，因此必须将病毒防控体系建立在每一个 PC 或服务器上，统一安装网络版杀毒软件。管理员及时更新杀毒软件服务器端病毒库，对局域网内客户端病毒库统一升级，即可保障所有局域网内计算机的杀毒程序病毒库自动更新并保持最新版本，从而提高对局域网内 PC 和服务器同步查杀的工作效率。

3.3 优化网络系统管理措施

为了保证气象短信系统安全，在建立完善的网络安全技术防护体系的基础上，还需建立完善的日常安全管理措施。

3.3.1 建立数据存储机制 为保证气象短信系统数据安全，采用 Raid5 存储技术。它是一种存储性能、数据安全和存储成本兼顾的存储解决方案。Raid5 不对存储数据进行备份，而是把数据和相对应的奇偶校验信息存储到组成 Raid5 的各个磁盘，且奇偶校验信息和相对应的数据分别存储于不同的磁盘。当 Raid5 的一个磁盘数据发生损坏后，利用剩下的数据和相应的奇偶校验信息恢复被损坏的数据。

3.3.2 限制登录用户权限 所有用户初始权限最高为 power user，尽可能限制登录用户的数量、权限，遵循“用户权限最小化”的网络配置原则，让系统登录用户处于随时可控状态，并停止 Guest 系统账户。

3.3.3 定期监测修复系统漏洞 操作系统总是存在各种漏洞，软件漏洞包括 IE 漏洞、办公软件漏洞、数据库漏洞等，硬件漏洞包括防火墙漏洞和路由器漏洞等。而这些漏洞是安全防护工作最薄弱的环节。网络管理员要定期检查系统和软件补丁，并及时修复，防止因系统漏洞造成的安全隐患。

3.3.4 设置复杂的系统密码并定期更换 网络管理员必须定期修改密码，包括网络系统密码、操作系统密码等。密码过于简单，甚至是空密码的计算机通常是网络中最脆弱的部分，应当使用多种复杂的字符串组合设置密码，以防止账户密码被轻易破解。

3.3.5 关闭非业务需要的端口、服务 关闭如 Remote Registry 服务、Computer Browser 服务、Indexing Service 服务等非业务需要的后台服务，这些都是病毒恶意代码甚至攻击者常用的“通道”。同时只开放业务需要的通讯端口，如 80、21、25、110 等，关闭其它端口。

文章编号：1006-4354（2011）03-0047-02

自动观测方式下的几种常见错情及处理方法

孟　茹[1]，李爱华[2]，田耀齐[3]

（1. 汉台区气象局，陕西汉中　723000；2. 西乡县气象局，陕西西乡　723500；
3. 汉中市气象局，陕西汉中　723500）

中图分类号：P412.1　　文献标识码：B

自实现气象要素的自动观测以来，观测方式的改变使测报错情的类型与以往有较大区别。

1　编报错误

1.1　重要天气报中的 GGggW$_0$ 组出错

（1）1RRRR 组

陕西省规定，凡日降水量（20—20 时，北京时）≥0.0 mm 时，基本站（基准站）在次日 08 时需编发 1RRRR 重要天气报，故在 GGggW$_0$ 组中 W$_0$ 应为 1，但在 OSSMO 软件中，常常自动编发为 0。08 时观测员在编发完天气报后，再编发重要报，未注意 W$_0$ 的正误，致使发报错。

处理方法　人工干预将 W$_0$ 修改为 1。

（2）95VVV、957WW 组

由于启动重要天气报后，读入窗口的初始时间取自计算机系统时间，一些观测员常忘记修改为重要天气出现时间而导致 GGggW$_0$ 中的 GGgg 编发错误。特别是 95VVV、957WW 所报的视程障碍现象由前一日持续到本日 20 时后的，或白天守班台站视程障碍现象由夜间持续到 08 时后的 GGgg（夜间未发报），应编发为 2001 或 0801，

收稿日期：2010-12-08

作者简介：孟茹（1971—），女，陕西汉中人，大气探测工程师，从事地面气象观测工作。

3.3.6　谨慎使用移动存储设备　针对移动存储设备的使用，必须在确保安全的前提下进行。做好移动存储设备使用前的安全扫描和病毒查杀，也能减小病毒、木马等恶意代码的危害性。

3.3.7　提高系统属性安全控制　严格控制系统属性权限，比如：限制关键目录和文件的删除权限；严格控制具有修改、查看、删除权限的登录用户；限制对系统关键的 dll 文件、注册表信息、执行文件、隐含文件、共享文件的属性修改等。

3.4　完善管理机制

当气象短信系统网络受到攻击或威胁时，没有健全的网络安全管理制度，会失去气象短信信息安全的可控性；当安全事故发生后，没有相应的应急预案，就无法追踪攻击来源及依据，在第一时间恢复系统正常运行。因此，建立和完善气象短信系统安全管理制度和应急方案，使气象短信系统网络安全工作有据可循。同时还应建立常态化安全培训机制，不断提高管理员的安全责任意识和技术水平，组织操作人员系统学习网络安全知识，提高操作人员的技术水平，尽量避免因操作人员的误操作导致安全责任事故的发生。

4　结语

目前，陕西气象短信用户已超过百万，保证气象短信业务系统的安全稳定运行显得愈加重要。随着网络应用的不断发展，计算机病毒形式及传播途径日趋多样化，网络安全问题日益复杂化。只有将技术把关、完善设备、严格制度、规范操作等紧密配合，形成多层次、立体化的防护体系，才能确保气象短信业务系统的安全性和稳定性。

参考文献：

[1]　Wikipedia. Phishing［EB/OL］. http：//en. wikipedia. org/wiki/Phishing，2009-09-18.

[2]　张基温. 信息安全实验与实践教程［M］. 北京：清华大学出版社，2005：187-188.