文章编号:1006-4354(2003)06-0039-02

地市级网络安全分析与防范措施

史海燕,李社宏,武广良,俱开省
(渭南市气象局,陕西渭南 714000)

中图分类号:TP393.08 文献标识码:B

1 网络常见安全漏洞及对策

1.1 操作系统和应用软件的缺省安装

操作系统和应用软件缺省安装,往往会造成系统庞大,速度慢。防范措施:卸载不必要的软件;关掉不必要的服务和端口;不要随意安装自己看不懂或不了解的软件,特别是非汉化软件。

1.2 没有备份或者备份不完整

数据没有进行有效的备份;根本没有备份或不去确认备份是否有效;备份数据被黑客破坏等。为了气象数据的完整性、正确性、有效性,最低要求一周做一次完整的备份,每天再做增量备份;至少一个月对备份介质做一次测试,以保证数据确实被正确的保存下来;重要气象资料数据每天都做完整的备份,必要时在不同地方做多次备份。

1.3 未保护的 Windows 网络共享

共享方便了气象资料、数据的使用,但同时又是危及网络安全的一个重要因素。网络共享数据时要注意:确保只共享所用目录;为增强安全性,只对特定 IP 共享;只允许特定用户共享文件夹。在网络共享问题上,建议采用 WIN2000,WIN2000 的安全性比 WIN98 高。

1.4 大量打开的服务端口

很多人认为端口扫描是黑客们才需要关心的问题,其实不然,端口扫描可以帮助了解系统。端口扫描时使用命令 Netstat 对本机连接速率、发送和接收字节数能够全面的了解。进行网络扫描采用 Nmap 命令,像 Windows 2K/XP 这样复杂的操作系统支持应用软件打开数百个端口与其他客户程序或服务器通信,端口扫描是检测服务器上运行的服务和应用、向 Interne 其他网络开放联系通道的一种办法。要确定所必须打开端口的最小集合,并且关闭其他端口;win2000 中,用 fport 程序确定在某个特定端口上侦听的进程。

2 常见病毒与防范措施

2.1 Code Red 红色代码

对WINXP、WIN2000操作系统,主要感染

收稿日期:2003-08-08

作者简介:史海燕 (1978-),女,陕西岐山人,主要从事网络工作。

```
        wFl.Close
    End If
End Sub
            创建 Ftp 命令文本文件
Sub CtreateFtpFile (fn, ofn, fSys)
  Set wFl = fSys.CreateTextFile (" csb.txt", True)
  wFl.WriteLine " open 172.23.64.18"
  wFl.WriteLine " dqt"
  wFl.WriteLine " cd /u/dbao"
  wFl.WriteLine " put " &.fn
  wFl.WriteLine " lcd /fb"
  wFl.WriteLine " get " &.fn
  wFl.WriteLine " get " &.ofn
  wFl.WriteLine " bye"
  wFl.Close
End Sub
```

文章编号：1006-4354 (2003) 06-0040-02

建（构）筑物防雷电装置的验收性检测

刘 波，杜建忠

（陕西省防雷中心，陕西西安 710014）

中图分类号：P429 文献标识码：B

1 查看设计图纸确定检测方案

首先查看电气设计说明书、防雷平面图和基础平面图等。通过查看图纸，帮助检测人员对建筑物的防雷系统建立切实可行的检测方案。高层建筑物的防雷电措施要求防直击雷、防侧击雷、防雷电电磁脉冲、防雷电感应，缺一不可。图纸设计环节有疏忽遗漏的，必须明确指出，特别警惕。

1.1 电气设计说明书中防雷部分的阅读

防雷部分是对图纸必要的文字性解释。通过阅读可帮助检测人员了解图中未注明内容。包括建筑物设计依据标准、防雷类别、接地阻值要求，对避雷引下线和接地极的要求，避雷接闪器选用

收稿日期：2003-07-18

作者简介：刘波 (1974-)，男，陕西丹凤人，助工，从事防雷电装置检测工作。

HTTP，传播速度极快，通过网络传播。防范措施：(1) 通知直接人，要求对自己的计算机杀毒，控制其传播。(2) 系统管理员应立即从网络断开，进行数据备份；停止 IIS 及相关服务，杀掉可疑进程；打补丁重新启动；重新检测，恢复网络连接。(3) 网络管理员要在路由器上，将内容进行过滤；检查防火墙的性能问题，有效性问题。

2.2 Nimda 病毒

影响 WIN98、WIN2000、WINXP 操作系统。通过 Email，文件共享、页面浏览进行传播。日常工作中群发电子邮件、扫描共享文件夹和扫描有漏洞的 IIS 都会感染生成病毒文件，影响网络安全。使用金山毒霸和 Norton 杀毒软件容易杀除。

2.3 Sircam 蠕虫病毒

主要危害群发邮件，选择随机文档附加在你的计算机的通讯簿的随机地址进行发送；删除硬盘文件，特别是删除机器使用“日/月/年”的日期格式；每一次启动都在硬盘上写数据，直到塞满硬盘；泄漏机密：随机将硬盘上的文件附加进邮件发送。删除步骤：清空回收站；在 DOS 模式下打开 Autoexec.bat 文件，如果有如下字段则删除“@win ecycledsirc32.exe”；更改注册表，将 gedit.exe 改名为 regedit.com。

3 提高网络安全性常用安全措施

3.1 计算机终端安装防火墙及其它反病毒软件

下载最新的病毒特征库，进行在线杀毒。如果用的是 Windows 系统，要到 Microsoft 公司的网站下载最新的 Service Packs

3.2 配置网络服务器

关掉不必要网络服务，配置防火墙、路由器，封锁不必要端口。

3.3 账号与口令设置

保证密码不易被人猜中：尽量采用 9 个字符以上，数字与字符相混的口令经常更改口令。

3.4 使用最新版的浏览器

浏览器往往存在安全漏洞，最新版 IE 比较安全。可以从 Microsoft 下载最新版的 IE。

3.5 做好记录

从事件中吸取教训。对每一次网络安全事件认真总结，并做好防范措施，避免类似事件再发生。

地市级网络连接省、县间网络的桥梁，它的安全程度直接影响到县—地—省之间气象数据能否正常传输，作好安全维护工作是不容忽视的。