浅谈我矿局域网网络安全控制及病毒防范

赵俊鹏

（山西兰花科技创业股份有限公司望云煤矿分公司）

摘　要：随着计算机技术、信息技术的高速发展，网络安全日益受到重视。本文根据单位局域网的实际情况，分析了网络运行中安全及管理方面存在的问题，并对局域网安全管理及防范进行了探讨。

关键词：局域网；安全控制；病毒防范

我矿局域网自 2004 年以来，网络与信息系统建设已逐步成形。保证网络信息安全以及网络硬件及软件系统的正常运转是基本前提，因此计算机网络和系统安全建设就显得尤为重要。

一　网络安全现状

我矿局域网通过防火墙和互联网相连，通过设置访问控制列表大大的减小外部的安全威胁。相反来自网络内部的计算机客户端的安全缺乏必要的管理措施，安全威胁较大。未经授权的网络设备或用户就可能通过局域网的网络设备自动进入网络，形成极大的安全隐患。

二　安全威胁分析

1、网络病毒的传播与感染

随着计算机网络的迅速发展和普及，各种计算机病毒也相继产生，其破坏性程度也不断增加，尤其是网络病毒破坏性就更强，一旦数据库服务器的硬盘感染病毒，就可能造成系统损坏、数据丢失，使网络服务器无法正常运行，应用程序和数据也无法正确使用，甚至导致整个局域网网络瘫痪，给矿上造成不可估量的损失。网络病毒普遍具有较强的再生机制，可以通过网络扩散与传染。一旦某个公用程序染了病毒，那么病毒将很快在整个网络上传播，感染其它的程序。

2、局域网用户安全意识不强

如今许多用户经常使用移动存储设备来进行数据的传递，经常将外来信息不经过必要的安全检查，就通过移动存储设备带入内部局域网，同时将内部信息带出局域网，这给木马、蠕虫等病毒的传播提供了方便，同时增加了信息泄密的可能性。另外一机两用甚至多用情况普遍，笔记本电脑在内外网之间平凡切换使用，还有一些用户将在 Internet 网上使用过的笔记本电脑在未经许可的情况下擅自接入内部局域网络使用，造成病毒的传染和信息的泄密。

3、系统数据的破坏

在网络系统中，有多种因素可能导致数据的破坏。首先是黑客侵入，黑客基于各种原因侵入网络，其中恶意侵入对网络的危害可能是多方面的。其中一种危害就是破坏数据，可能破坏服务器硬盘引导区数据、删除或覆盖原始数据库、破坏应用程序数据等。其次是病毒破坏，病毒可能攻击系统数据区，包括硬盘主引导扇区、Boot 扇区、FAT 表、文件目录等；病毒还可能攻击文件数据区，使文件数据被删除、改名、替换、丢失

部分程序代码、丢失数据文件；病毒还可能攻击 CMOS，破坏系统 CMOS 中的数据。

4、IP 地址冲突

局域网用户在同一个网段内，经常造成 IP 地址冲突，造成部分计算机无法上网。对于局域网来讲，此类 IP 地址冲突的问题会经常出现，用户规模越大，查找工作就越困难。

三　网络安全控制及防范

通过以上安全威胁分析我矿网络安全控制及病毒防范从以下几点抓起：

1、使用现有设备进行网络安全访问控制策略划分

（1）对全矿所有单位进行 VLAN 划分，使整个局域网成为好多个小虚拟局域网，这样一来增强了局域网的安全性。不同 VLAN 内的报文在传输时是相互隔离的，即一个 VLAN 内的用户不能和其它 VLAN 内的用户直接通信。

（2）采用硬件防火墙完成内外网隔离。限制网络互访，用来保护内部网络资源免遭非法使用者的侵入。

①利用 NAT（地址转换）使内部网络通过防火墙访问外部网络时，将产生一个映射记录。系统将外出的源地址和源端口映射为一个伪装的地址和端口，让这个伪装的地址和端口通过防火墙与外部网络连接，这样对外就隐藏了真实的内部网络地址。在外部网络通过防火墙访问内部网络时，它并不知道内部网络的连接情况，而只是通过一个开放的 IP 地址和端口来请求访问。

②IP/URL 过滤。一旦应用流量是明文格式，就必须检测 HTTP 请求的 URL 部分，寻找恶意攻击的迹象，这就需要一种方案不仅能检查 RUL，还能检查请求的其余部分。其实，如果把应用响应考虑进来，可以大大提高检测攻击的准确性。虽然 URL 过滤是一项重要的操作，可以阻止通常的脚本类型的攻击。

③TCP/IP 终止。应用层攻击涉及多种数据包，并且常常涉及不同的数据流。流量分析系统要发挥功效，就必须在用户与应用保持互动的整个会

话期间，能够检测数据包和请求，以寻找攻击行为。至少，这需要能够终止传输层协议，并且在整个数据流而不是仅仅在单个数据包中寻找恶

意模式。系统中存着一些访问网络的木马、病毒等 IP 地址，检查访问的 IP 地址或者端口是否合法，有效的 TCP/IP 终止，并有效地扼杀木马等。

④访问网络进程跟踪。访问网络进程跟踪。这是防火墙技术的最基本部分，判断进程访问网络的合法性，进行有效拦截。这项功能通常借助于

TDI 层的网络数据拦截，得到操作网络数据报的进程的详细信息加以实现。

（3）启动 IP 地址绑定，采用上网计算机 IP 地址与 MCA 地址唯一对应，给每个单位发放 IP 地址表，对所用交换机空闲端口进行关闭。这样一来有

效防止 IP 地址引起的网络中断和移动计算机随意上内部局域网络造成病毒传播和数据泄密。

（4）网络服务器的系统安全和物理安全措施

防火墙做为网络的第一道防线并不能完全保护内部网络，必须结合其他措施才能提高系统的安全水平。在防火墙之后是基于网络服务器的系统安全和物理安全措施。按照级别从低到高，

分别是主机系统的物理安全、操作系统的内核安全、系统服务安全、应用服务安全和文件系统安全；同时主机安全检查和漏洞修补以及系统备份安全作为辅助安全措施。这些构成整个网络系统的第二道安全防线，主要防范部分突破防火墙以及从内部发起的攻击。系统备份是网络系统的最后防线，用来遭受攻击之后进行系统恢复。在防火墙和主机安全措施之后，是全局性的由系统安全审计、入侵检测和应急处理机构成的整体安全检查和反应措施。它从网络系统中的防火墙、网络主机甚至直接从网络链路层上提取网络状态信息，作为输入提供给入侵检测子系统。入侵检测子系统根据一定的规则判断是否有入侵事件发生，如果有入侵发生，则启动应急处理措施，并产生警告信息。而且，系统的安全审计还可以作为以后对攻击行为和后果进行处理。是对系统安全策略进行改进的信息来源。

2、病毒防治

相对于单机病毒的防护来说，网络病毒的防治具有更大的难度，网络病毒防治应与网络管理紧密结合。网络病毒的防治最大的特点在于网络的管理功能，如果没有管理功能，很难完成网络防病毒的任务。只有管理与防范相结合，才能保证系统正常运行。计算机病毒的预防在于完善操作系统和应用软件的安全机制。

（1）增加安全意识

首先是杜绝病毒，主观能动性起到很重要的作用。病毒的蔓延，经常是由于电脑操作人员对病毒的传播方式不够了解，病毒传播的渠道有很多种，可通过网络、物理介质等。其次是查杀病毒，要知道病毒到底是什么，它的危害是怎么样的，知道了病毒危害性，提高了安全意识，病毒防治的任务就已经成功了一半。再次是平时要从加强安全意识着手，对日常工作中有可能隐藏的病毒增加警觉性，如安装网络版杀毒软件，定时更新病毒定义，对来历不明的文件运行前进行查杀，每周定期查杀一次病毒，减少共享文件夹的数量，文件共享的时候尽量控制权限和增加密码等，都可以很好地防止病毒在网络中的传播。

（2）小心邮件

随着网络的普及，电子信箱成了工作中不可缺少的一种媒介。它在方便快捷地提高人们工作效率的同时，也无意之中成为了病毒传染的帮凶。

有数据显示，如今有超过 90%的病毒通过邮件进行传播。尽管这些病毒的传播原理很简单，但这决非仅仅是技术问题，还应该要求用户随时小心警惕，不要打开有怀疑的邮件。

（3）小心使用移动存储设备。在使用移动存储设备之前进行病毒的扫描和查杀，也可把病毒拒绝在外。

总之，网络安全控制与病毒防范是不可分开的，是一项长期而艰巨的任务。我们必须综合考虑安全因素，制定合理的目标、技术方案等，来把握好局域网网络安全的大门。