文章编号：1005-8451（2008）10-0053-02

铁路信息系统的安全隐患及其防范

李 旭
（大秦铁路股份有限公司 大同车务段，大同 037005）

摘 要：针对铁路管理信息系统存在的安全隐患，结合日常工作的经验心得，给出各种隐患的解决方法或相应防范措施。

关键词：安全；隐患；信息系统；管理；防范
中图分类号：TP39 文献标识码：A

Security hidden dangers and preventive measures in Railway Management Information System

LI Xu
(Datong Train Operation Depot of Daqin Railway CO.,LTD, Datong 037005, China)

Abstract: Facing with the security hidden dangers in Railway Management Information System, it was given the experience of day-to-day work experience, the solution and the corresponding preventive measures on hidden dangers

Key words: security; hidden danger; Information System; management; preventive measure

随着铁路信息系统建设和应用的不断发展，铁路企业对管理信息系统的依赖程度越来越高。我们在享受它所带来的高效和快捷的同时，又面临着系统的各种安全威胁。因此必须重视铁路信息系统安全，找到隐患的踪迹，把隐患消灭于无形，才能够让铁路信息系统更好地为铁路运输生产服务。

1 找出隐患所在

1.1 在管理上存在的安全隐患

很多人的安全意识淡薄，从管理上带来的安全威胁是安全隐患中最常见也是最可怕的一种：责权不明、管理混乱，使得一些员工或者管理员随便让一些非本地员工甚至外来人员进入机房重地，或者员工有意无意泄露他们知道的一些重要信息，而管理上却没有相应制度来约束；由于内部人员的违规操作等，当网络出现攻击行为或网络受到其他一些安全威胁时，无法进行实时的检测、监控、报告与预警。由于不重视数据备份，使数据丢失或遭受破坏。

1.2 存在于网络中的安全隐患

铁路管理信息系统依赖于网络的运行，因此有网络攻击。网络攻击主要有截获信息、更改报文流、拒绝报文服务、伪造连接初始化和恶意程序等攻击。其中恶意程序对网络安全威胁较大的有：计算机病毒、计算机蠕虫、特洛伊木马和逻辑炸弹等。网络的连接使得离职员工和其他有恶意的人有可能和系统连接，利用网络攻击手段对系统进行攻击从而造成不可忽略的损失；由于要信息共享、数据传输，所以那些恶意程序就会通过网络通信功能从一个地方传播到另一个地方进行攻击、破坏，从而给系统造成各种故障甚至瘫痪。

1.3 还有来自服务器和数据库的安全隐患

目前铁路管理信息系统所使用的服务器、操作系统、数据库系统等核心软硬件有些是国外公司研制的，存在着的不安全因素；用户帐号和权限设置随意或经过若干次改动后造成用户权限和用户级别混乱配合，数据库安全保护功能较弱或没有安全机制和安全策略，都可能造成对系统的破坏；操作系统或其他软件中存在的一些缺陷也带来了安全隐患。各种外在因素如自然灾害、电源的不稳定、设备的老化等，还有人为破坏、内部人员的恶意窃取、本地用户的误操作等，这些也都会直接威胁到系统的安全。

2 防患于未然

2.1 加强管理，提高安全意识

收稿日期：2008-07-02
作者简介：李 旭，助理工程师。

针对铁路管理信息系统的脆弱性，应该切实加强安全管理。要加强物理安全，保护管理信息系统服务器及铁路管理信息系统运行所依赖的计算机网络中的设备如路由器、工作站、交换机和打印机等硬件实体和通信线路免受自然灾害、人为破坏和搭线窃听攻击。

建立和实施严密的安全制度也是实现系统安全的基础。良好的系统管理有助于增强系统的安全性，要建立完备的安全管理制度、安全保护制度和安全教育制度，妥善保管备份磁盘和文档资料，防止非法人员进入机房进行偷窃和破坏活动等。

2.2 构造服务器、数据库的安全策略

对于服务器操作系统，如Windows Server系列，系统管理员可以通过用户帐号设置3种安全规则，即帐号规则、用户权限规则和审核规则。对于基于B/S的网络管理信息系统，除了利用Windows的安全特性之外，还可以利用IIS的许多工具来确保站点安全；此外，还要定期更换用户密码、定期删除过期数据和清理日志文件等。对于服务器的硬件系统，定期做好除尘工作。还可以增加备用电源、UPS（不间断电源）来保护服务器硬件设备，减小停电或电压不够稳定给服务器硬件带来的损害；

对于数据库，以SQL Server数据库为例，构造安全策略的第1步是确定SQL Server用哪种方式验证用户。如果服务器可以访问域控制器，应该使用Windows验证，它的最大好处是很容易通过Enterprise Manager实现，缺点则在于SQL Server验证的登录只对特定的服务器有效；构造安全策略的第2步是确定用户应该属于什么组。通常，每一个组织或应用程序的用户都可以按照他们对数据的特定访问要求分成许多类别。控制数据访问权限最简单的方法是，对于每一组用户，分别创建满足该组用户权限要求的、域内全局有效的组。我们既可以为每一个应用分别创建组，也可以创建适用于整个企业的、涵盖广泛用户类别的组。除了面向特定应用程序的组之外，还需要几个基本组，基本组的成员负责管理服务器；实施安全策略的最后一个步骤是创建用户定义的数据库角色，然后分配权限。完成这个步骤最简单的方法是创建一些名字与全局组名字配套的角色。

2.3 重视数据备份，维护数据的完整和准确

数据备份的方法主要可以分为硬件级、软件级和人工级3类。

硬件级的备份是指用多余的硬件来保证系统的连续运行，比如增加备用服务器、硬盘双工、双机容错等。但这种方式无法防止逻辑上的错误，如人为误操作、病毒、数据错误等；

软件级的备份是指将系统数据保存到其他介质上，当系统出错时可以将系统恢复到备份时的状态。由于这种备份是由软件来完成的，所以称为软件备份。用这种方法进行备份和恢复数据都要花费一定的时间，但可以完全防止逻辑错误。因为备份介质和计算机系统是分开的，错误不会复写到介质上。这意味着，只要保存时间足够长的历史数据，就能够恢复正确的数据；

理想备份系统是软件备份和手工方式相结合。如果系统出错，备份之前的数据用软件方法恢复，备份之后的数据用手工方式恢复。如果在备份系统的基础上再加上硬件容错系统，会更加安全可靠。

2.4 安装防火墙

防火墙是由软件、硬件构成的系统，用来在两个网络之间实施接入控制策略。需要注意的是这个接入控制策略是由使用防火墙的单位自行制订的。这种安全策略应当最适合本单位的需要。

防火墙的功能有两个：阻止和允许。“阻止”就是阻止某种类型的通信量通过防火墙（从外部网络到内部网络，或反过来）。“允许”的功能与“阻止”恰好相反。在大多数情况下防火墙的功能是“阻止”。

此外，铁路信息管理员要具备较高的个人素质、较强的安全意识和较为娴熟的管理技术。平时还要注重经验的积累，如果把本单位信息系统所受威胁、采取的相应措施悉心收集，并简明地列出，无疑就是一份具有使用价值的安全维护手册。一些重要设备的备用也是必要的。

3 结束语

铁路网络管理信息系统的安全是动态的，在新的隐患不断出现时，没有一劳永逸的应对策略。因此，只有把安全管理制度与安全管理技术手段结合起来，不断进行研究、探索和实践，动态地构筑完善的安全体系，系统的安全性才有保障。

参考文献：

[1] 谢希仁. 计算机网络[M]. 北京：电子工业出版社，2003.

[2] 雷震甲. 网络工程师[M]. 北京：清华大学出版社，2006.