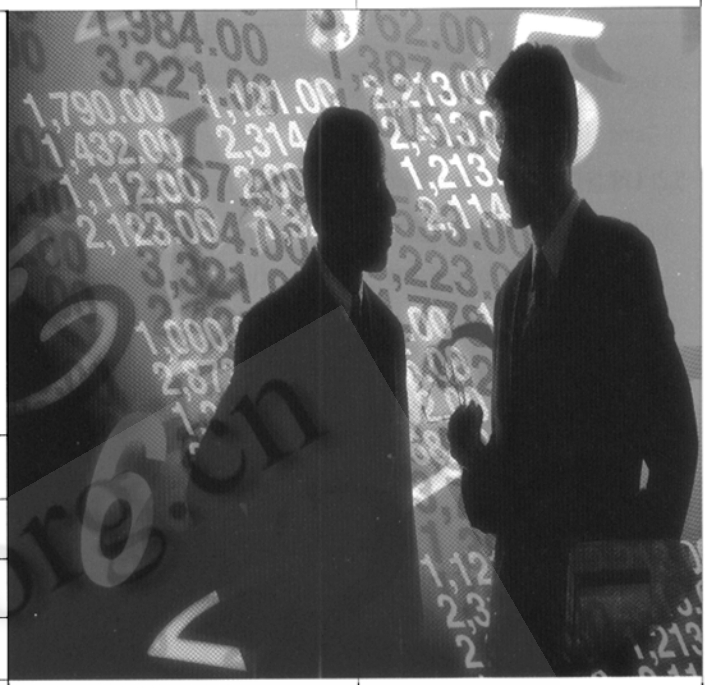
石长铁路办公管理信息系统安全体系的探讨与实践



金 路 张 欣 (石长铁路有限责任公司电子计算信息中心 410000)

摘要: 首先对计算机系统的网络安全进行分析，然后结合石长铁路办公网的实际对铁路办公管理系统的安全问题进行了探讨，并提出了现阶段的解决措施。

关键词: 系统安全 解决办法

1 引言

随着计算机技术的不断发展，计算机的网络安全越来越引起人们的高度重视，防范安全漏洞、隐患和非法入侵，保证计算机系统安全是我们的重要任务之一。本文结合石长铁路办公系统现状，从风险分析、安全策略、安全防范等方面展开讨论，以求建立起有效的计算机系统的安全体系，将风险减少到最低。

2 风险分析

办公管理信息系统风险主要来自：

- 外部或内部的非法入侵和攻击。
- 计算机病毒导致重要数据丢失或系统瘫痪。
- 网络的复杂性、系统的多样性可能导致整个网络出现安全漏洞隐患。
- 网络操作系统、网络协议安全、数据库系统安全的脆弱性。
- 网络协议分析软件使用不当，可能被黑客利用。
- 远程服务连接方式的脆弱性给计算机系统带来的风险。
- 通信设备、连接网络的传输介质的物理破坏。
- 网络安全管理及人为因素的影响。

鉴于铁路综合办公信息管理系统的复杂性，在设计与架构整个系统时，对整个系统的安全考虑，我们必须给予高度重视，并在成本与方便性、安全程度与复杂程度之间综合平衡，力求建立起一个安全、稳定、高效的计算机系统。图1示出了石长铁路总公司综合办公管理信息系统网络拓扑图。

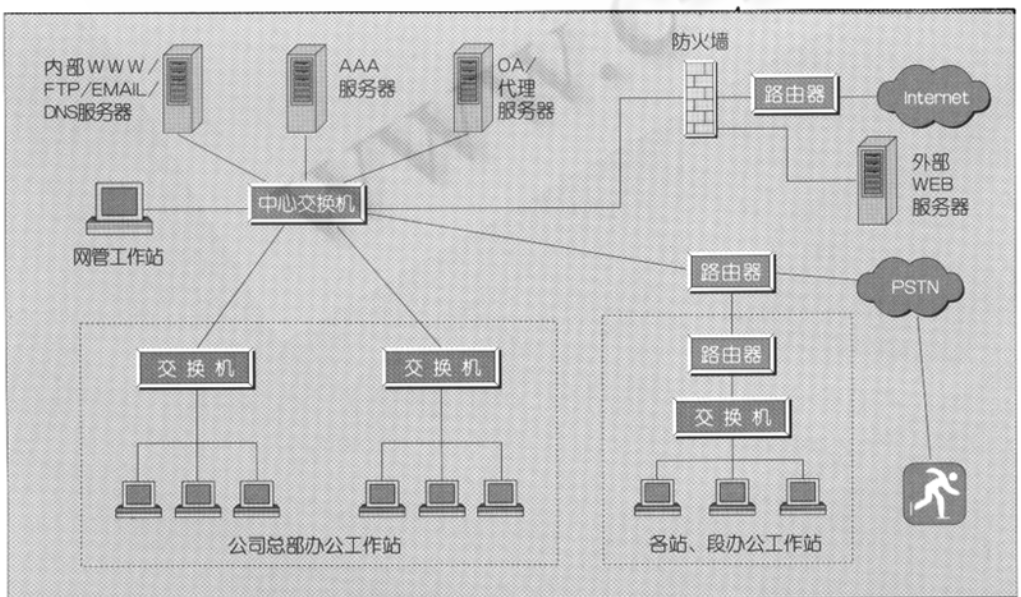


图1 石长铁路总公司综合办公管理信息系统网络拓扑图

3 网络安全解决方案

网络安全系统实际上是一组用于控制网络之间通信流的部件。安全是相对的，它是根据实际需要和自身条件所能达到的安全程度而定的。安全要求越高，系统所具备的安全功能就越多，其安全程度也越高，同时对网络的影响也越大。

3.1 网络信息安全模型

网络信息安全系统是涉及到方方面面的一项复杂的系统工程。一个完整的网络安全信息系统模型如图2所示：

- 社会的法律、法规以及企业

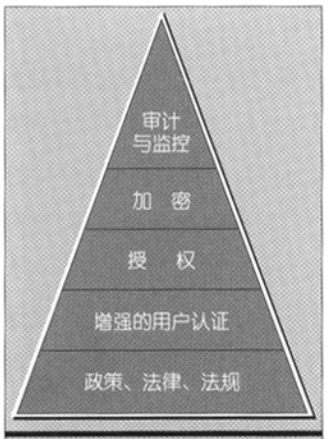


图2 网络信息安全模块

的规章制度和安全教育等外部软件环境。

• 技术方面，如网络防毒、信息加密、存储通信、授权、认证以及防火墙等。

• 审计和管理措施，如实时监控系统的安全状态，提供实时改变安全策略的能力等。

3.2 安全策略

设计网络安全系统时，首先要明确需要和目标，并制定相应的安全策略。制定安全策略首先要确定网络安全管理要保护什么，在这一问题上一般有两种不同的描述原则：一个是"没有明确表述为允许的都被认为是禁止的"，另一种是"一切没有表述为禁止的都被认为是允许的"。石长公司的安全策略就是将以上两个原则，根据系统及用户的不同情况制定目标和限制的。

企业网络系统安全策略可概括成如下几点：

• 职责划分
• 类型限制
• 授权管理
• 用户管理
• 跟踪审计
• 恢复策略

4 安全体系总结构

安全体系应该是一个多层次、多方面的结构。石长公司企业办公内部网络在安全体系总体结构上分为四个级别：

• 网络级安全
• 应用级安全
• 系统级安全
• 企业级安全

4.1 网络级安全

对于网络级安全，应充分考虑本单位的实际需要和网络现状，通过以下措施从网络的下三层（物理层、链路层、网络层）保证网络的安全。

4.1.1 可靠性安全措施

网络的可靠性主要是通过物理层的安全来加以保证，主要包括以下四个方面：

• 环境安全：严格按照国家标准建设计算机房。

• 设备安全：主要包括设备的防盗、防毁、防电磁辐射泄漏、防止线路截获，抗电磁干扰及电源保护等。

• 冗余备份：对重要的网络和计算机设备以及重要的通信线路采取冗余备份措施。

• 数据备份：对重要的数据采取备份措施。

4.1.2 站段网络接入安全

总公司与站段各区域网间的安全是通过在与广域网链路相联的路由器上设置过滤功能实现，即利用Cisco路由器本身具有的IOS安全特性来实现对区域网重要数据的防护。

4.1.3 与Internet的接入安全

尽管石长公司按照铁道部的统一部署，实行了企业内部网与Internet网的物理隔离，然而最终实现企业办公网与Internet互联是发展的必然趋势，为此主要采取了以下两项安全措施：(1)、在内部网络系统接入Internet的入口处设置了一台专用的防火墙设备。其作用是保护网络在阻止非授权用户访问敏感数据的同时允许合法用户无妨碍地访问网络资源，即防火墙可以减少外部侵袭的可能性，也能阻止用户发送危险的信息，是整个网络的第一道安全屏障。在安全策略上采取"没有明确表述为允许的都被认为是禁止的"的原则对内、外部用户进行严格控制，并通过设置一些安全策略来限制用户对国外一些色情站点或反动站点的访问。(2)、通过对防火墙的适当配置，在企业内部网络系统与Internet之间设立一个非军事化区（DMA），其中包含一台WEB服务器，用于向外界发布OA的公共信息。

石长公司防火墙采用的是天融信网络卫士NG FW2000防火墙，该防火墙采用软硬件一体化设计，具有以下功能：(1)抗IP假冒攻击、抗源路由攻击、抗极小碎片攻击;(2)防电子欺骗（防IP地址欺骗）；(3)可以检测到对网络或内部主机的所有TCP/UDP扫描以及多种拒绝服务攻击；(4)可以对来自外部网络的扫描和多种攻击进行实时响应；(5)抗DOS攻击：不但可以识别而且还可以对抗DOS攻击。

4.1.4 拨号网络安全

石长公司是通过总公司的一台Cisco路由器为远程用户提供PSTN电话拨号接入服务。在中心机房安装配置了一台CiscoSecure认证服务器，使用AAA技术为拨号入网的用户提供认证、授权、记帐服务，保证用户对公司内部网络系统的合法访问。即拨号用户首先向拨号访问服务器发出拨号请求，通过PPP链路确认，使用CHAP确保合法用户的身份确认。身份确认完毕后，拨号访问服务器把请求发到Cisco Secure认证服务器，由该认证服务器根据用户在里面的配置信息对用户进行授权、登记。

4.1.5 部门之间的安全：VLAN技术

公司办公大楼及各单位局域网分别采用虚拟局域网VLAN技术隔离广播域。核心交换机具有高性能的第三层功能，通过对交换机的设置，使整个机关及站段的局域网根据实际需要，以端口或MAC地址等多种方式灵活地划分VLAN，不同的部门隶属于不同的VLAN，其相互间的通信必须通过第三层交换技术来实现，以满足安全性和高性能的双重要求。

4.2 应用级安全

应用级安全主要从以下两个层次加以实现：利用企业内部网各系统自身专有的安全机制和数据库自身的安全机制。

4.2.1 应用系统安全机制

石长公司企业内部网应用系统安全机制主要是指在对石长公司内部网各大应用分系统进行开发时，与数据库安全机制和Domino/Notes安全机制的紧密、有机的结合。主要包括：

• 自定义的用户安全策略
• 应用系统用户身份认证
• 访问控制授权
• 数据加密传输。
• 审计监督

4.2.2 数据库安全机制

石长公司企业内部网系统充分利用 Lotus Domino/Notes 自身的安全机制保障办公管理信息系统应用级的安全。

Domino/Notes 的安全机制

• Domino/Notes为每个用户提供一个唯一的用户标识符作为判定用户访问服务器的权限。

• Domino/Notes的每个数据库都有一个存取控制表 (ACL)，用于控制用户、服务器和群组对数据库的访问。

• Domino/Notes支持多种加密功能：本地数据库加密、文档加密、域加密、传输加密。

• Domino WEB 服务器上可设置成不允许匿名用户连接，通过正确配置每个数据库的存取控制表，保证缺省用户的正确存取权限。可以通过安全通道安全协议(SSL)方式保证 Web 用户访问 Domino 服务器时数据传输安全。

4.3 系统级安全

石长公司办公管理信息系统对系统级安全的实现，主要通过Windows2000 Advance Server操作系统提供的安全机制，通过合理设置予以实现。

4.3.1 Windows2000 Server 系统中的安全设置

(1) Windows2000 Server 操作系统新的安全功能

① Windows2000 Serve活动目录为所有的域安全策略和帐户信息提供了存储。活动目录服务为多个域控制器提供了帐户信息的副本和有效性，并可以远程进行管理。

② Windows2000 Serve 活动目录为用户、组和机器帐户信息提供了一个分层的名字空间，可以按组织单元对帐户进行分组，优于以前版本中使用的单调域帐户名字空间。

③ 创建和管理用户或组帐户的管理员权限可以委派到组织单元级，可以对用户对象上的个别属性授予访问权限。

④ Windows2000 Serve安全包括了基于 Internet 标准安全协议的新的身份验证，这些协议中分布式安全协议包括Kerberos v5和传输层安全 (TLS)。此外，为了保证兼容性还支持 Windows2000 Serve LAN MANAGER 身份验证协议。

⑤ 安全通道安全协议 (SSL) 在实现中通过将公钥证书形式的用户信任证映射到现有Windows2000 Serve 帐户从而提供了强客户身份验证，通用管理工具被用来管理帐户信息和访问控制，可以使用共享秘密身份验证或者公钥安全。

⑥ 除了密码之外，Windows 2000 Serve 还支持在交互式登录时选择使用智能卡。智能卡支持密码技术和私钥与证书的安全存储，使得可以从桌面到 Windows2000 Serve 域进行强身份验证。

⑦ Windows2000 Serve为企业提供了微软证书服务器，企业可以用此证书服务器为他们的用户分配 X.509 版本 3 的证书。在 Windows2000 Serve 中包含了 CRYPTOAPI证书管理API和模块，可以使用它们来处理公钥证书，包括由商业证书机构(CA)第三方CA或者微软证书服务器发行的标准格式的证书。

(2) 在 Windows2000 Advance Server 系统采取的安全设置措施：

① 严格用户帐号管理，限定用户帐户的访问权限。在Windows-2000 Serve 的网络环境中 Active Directory 的最主要的功能就是实现用户身份验证。对于用户身份验证管理，Active Directory 提供了进一步的配置，它设置了一系列的安全模板，详细地设定了各方面的安全配置，包括用户帐户、用户操作的审核、各类事件的记录，对系统服务的配置，对注册表和文件系统的安全管理。对于非 Windows2000 的用户，也可以使用原来的 NTLM 的身份方式。同时 Windows2000 继承和扩展了NT中组策略的功能，管理员可以通过制定组策略来实现对用户和计算机的控制。

② 数据存储的安全性。用 NTFS 取代 FAT 并使用 ACL 来限制用户对 NTFS 卷上的磁盘、目录或文件的访问权限，保护计算机系统的配置参数和数据不被非法更改。Windows2000 系统中数据是存储在NTFS5.0格式的分区和卷中，NTFS5.0 的新的加密文件系统通过用一个随机产生的密钥对文件进行加密，使文件更加安全，克服了 NT4.0 文件本身没有加密，非授权用户可在硬盘上安装另一套 NT 就可以访问其没有访问权限文件的情况发生。同时采用备份、镜像技术、归档、转储、分级存储管理、制定灾难恢复计划等措施来保证重要数据的完整性。

③ 认真设置并正确利用审计系统，对审计日志加强保护。

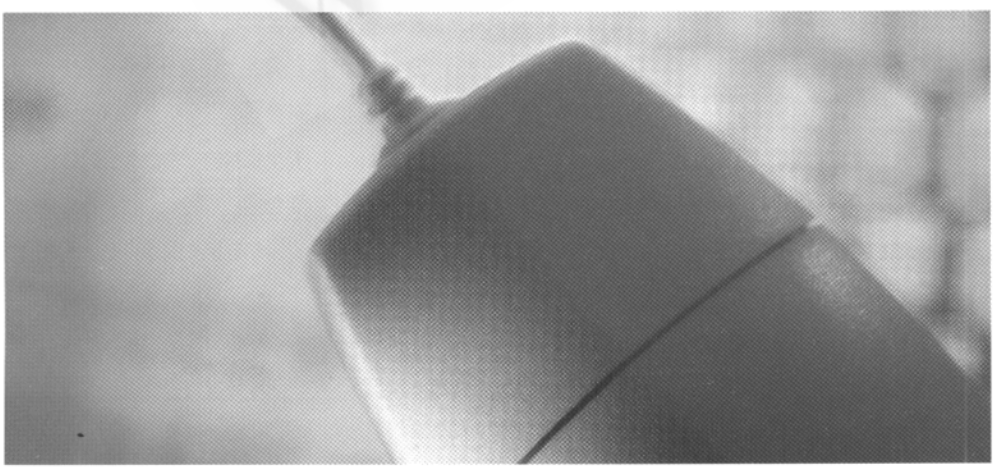
④ 认真利用 NT 域管理及域之间的委托关系。

⑤ 确保RED更新后对SAM数据库的防护。

⑥ 及时安装Service Pack更新软件包。

4.4 企业级安全

企业级安全管理主要可从“制定安全管理制度”和“计算机病毒防范”两个方面进行规划。



4.4.1 安全管理制度

仅仅依赖技术手段来保证系统尤其是一个企业内部网络的安全是远远不够的。只有加强内部人员的安全教育，在企业内部建立一套完善而严密的安全管理制度，并切实遵照执行，才能从根本上确保系统的安全。

内部的安全管理应坚持以下基本原则：分离与制约、有限授权、预防为主和可审计原则。内部安全管理的主要内容主要包括制定以下管理制度：

- 机构与人员安全管理制度
- 系统运行环境安全管理制度
- 软硬设施安全管理制度
- 网络安全管理制度
- 数据安全管理制度
- 技术文档安全管理制度
- 应用系统安全管理制度
- 操作安全管理制度
- 应急安全管理制度
- 加密算法与密钥安全管理制度。

4.4.2 计算机病毒防范

计算机病毒的防范应采取技术手段与管理手段相结合的办法进行综合防范。

(1) 技术上主要控制病毒传播的几个主要途径：

- 监视各节点病毒入侵情况，保护网络操作系统完整性与正确性不受病毒的破坏；
- 对来自节点入侵的病毒进行警告、杀灭，使网络系统对病毒的防御能力保持在同一水平；
- 重点保护企业内部网中的重要NT服务器，如FTP服务器、WEB服务器、邮件服务器、DNS服务器，防止因病毒破坏丢失重要数据。
- 配置系统整体的病毒检测、杀除时间表，实现对病毒检测和杀除的周期性、计划性；
- 加强桌面防毒，通过在NT主域服务器上配置企业级防病毒系统，给所有登录到NT域的客户机安装、更新防病毒软件和病毒代码库，并在用户随意卸载主机病毒系统后能够自动重新安装。
- 对病毒事件进行安全审计，向系统管理员提供证据，用来跟踪、追查各种可能的病毒事件；接受技术支持服务的升级操作，提高网络对病毒的防御能力。

(2) 管理方面主要在企业的各级部门开展安全教育，严格病毒防范管理：

- 对所有用户进行培训，使大家充分认识到病毒的危害，严格限制外来光盘的使用和“随意运行不明Internet下载程序”之类可能导致病毒入侵的源头。
- 定期对文件服务器进行病毒检查，若发现可疑情况及时查杀病毒。
- 重要文件要经常备份。

5 结束语

在今天的网络世界里，保障企业的信息、通信设施、计算机安全及知识产权已刻不容缓。我们只有充分认识计算机系统安全的重要性，并建立健全有效的计算机系统安全保障体制，才能确保计算机系统的安全、正常的运行。当然我们也应看到，计算机系统安全是一项系统工程，涉及面广，特别是随着计算机技术的飞速发展，对计算机系统的安全提出了更高的要求，我们只有紧跟时代的发展步伐，不断更新我们技术与观念，同时更寄希望于更多更好的国产计算机软硬件投入运行，这样我们才能做到未雨绸缪，防范于未然。

参 考 文 献

1 晶辰工作室，Windows 2000 Server企业组网实用教程，电子工业出版社，2001。

2 徐超汉，计算机网络安全与数据完整性技术，电子工业出版社，1999。

3 曙光信息产业有限公司，Lotus Notes使用与开发指南，电子工业出版社，1998。

4 汤庸等，群组系统Lotus Notes实用开发指南，人民邮电出版社，1997。

5 Scott Fuller和Kevin Pagan，Intranet防火墙，电子工业出版社，1997。