证券营业部计算机网络安全分析与防范技术

摘要： 本文针对计算机网络在证券行业的应用特点，分析了目前存在的安全隐患，提出了具体的解决途径与设计方案。经实践证明是行之有效的。

关键词： 券商网络 安全问题 解决方案

孙 巨 （苏州大学 215021）

1 引言

本文在对证券营业部计算机网络现状及其管理方式调查了解的基础上，从三个方面就目前存在的安全隐患进行了分析，并给出了防范建议，以期促进和进一步提高券商计算机网络系统的安全性。

2 网络布线系统的安全策略

2.1 券商网络系统的现状

通常，券商的计算机网络应用系统主要是由行情服务系统和资金服务系统两大部分组成。前者主要负责与沪深两交易所通信，发送委托，接收回报，接收与揭示实时行情、资讯信息，以及提供行情的技术分析等。一般是基于 Netware 操作平台以及 DBF 数据库系统。后者主要负责股民的资金管理、证券管理、银证转帐和提供各种手段的委托交易等，并且由于受到交易规则变化、券商需求变化和开发商之间激烈竞争的影响，正变得越来越庞杂。现多数是基于 Windows NT 操作系统和 MS SQL SERVER 数据库系统。网络的信息传输也均是以“工作站 -- 桌面交换设备 -- 主干交换设备 -- 服务器”的模式进行数据的集中访问。使用千兆以太网或快速以太网架构营业部网络系统的主干：主干交换设备到服务器、主干交换设备之间、主干交换设备到桌面交换设备。使用快速以太网或以太网架构营业部网络系统的支干：桌面交换设备到工作站。营业部提给股民使用的工作站多为PC无盘站，利用远程启动映像文件启动、登网和用几乎公开的帐户与密码进入行情分析系统与委托交易系统。营业部内部人员则采用有盘站或无盘站进行相关的数据处理与业务操作，参见图 1。

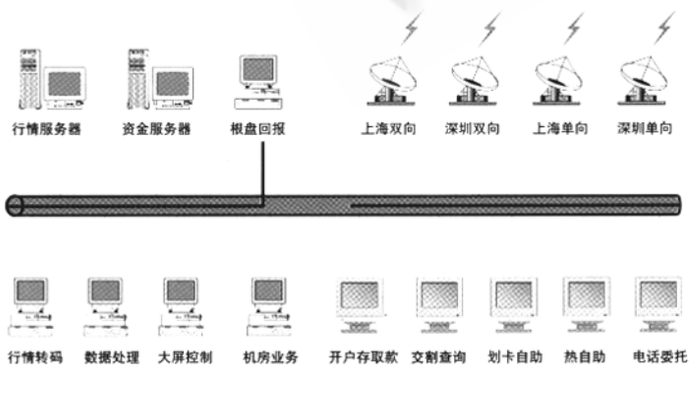

图 1 一般结构的网络拓朴示意图

2.2 三层网络结构

目前，营业部的客户工作站与资金服务器、卫星通讯机等关键设备均是处于同一物理网段，这就难以从根本上来保障券商网络的核心系统能够抵御来自外部黑客的侵袭。建议改造布线系统，实现内外网隔离，即将暴露于股民面前的行情、委托用机划分在外网环境运行，机房用机、重要柜面用机划分在内网环境运行。内外网分设两个Novell服务器处理，资金服务器置于内网，设行情转换机和数据处理机担任中间件实现内外网的通信连接。通过行情转换机从内网获得行情数据发向外网，通过数据处理机接收外网的委托请求传送给资金服务器，中间件的通信使用加密算法，从而实现三层分离的网络结构，这样

外部的入侵者因无法看到内网的资金服务器和行情报盘服务器而难以实施攻击，即使外网文件服务器被攻破，内网的核心服务器也是安全的，参见图2。

在完成布线系统改造之后，还应经常检查有否不再使用的信息点，通过跳线技术切断其与网络的连接，以防止外来电脑的非法接入。也可以在交换机的端口上设置工作站的网卡地址，实现用户接入的安全检查。

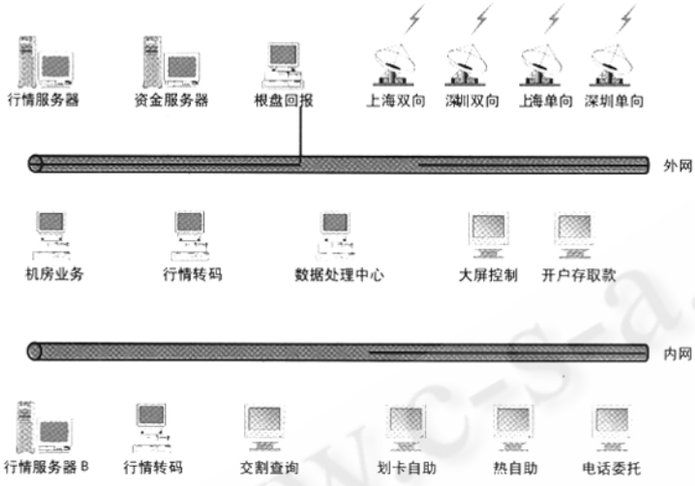

图 2 三层结构的网络拓朴示意图

3 网络操作系统的安全策略

3.1 Novell 无盘站批处理上网

无盘站的启动过程是从服务器上获取DOS环境启动DOS，再运行批处理程序上网及执行相应的应用程序。由于DOS系统的特性，批处理可以被键盘中断(如Ctrl-C 或Ctrl-Break)，造成网络数据裸现在用户面前。一旦用户权限设定不当，恶意入侵者就能轻易地修改和删除数据。对此，建议开发一个内存驻留程序，截取相应的组合按键，防止批处理被中断。同样，为限制用户用F5或F8键中断DOS的引导过程，还可以在config.sys中加入switchs=/N，使得DOS启动时不检查F5和F8键请求。

一般，营业部电脑人员为简便开机过程，提供给股民使用的电脑入网用户名与口令往往是公开或不设口令的，为彻底解决这种公开帐户的安全问题，避免网卡地址的信息泄露和被假冒，也可以在Novell的核心层上建立自动登录技术，实现不需要操作者干预情况下的无盘站自动带密码登录服务器及获取网络资源。当然这项技术需建立在与Novell公司深层次技术合作的基础上。

3.2 帐户与权限

任何的安全保护措施都不是绝对的，存在着有被攻破的可能。但是建立一个多重保护系统，各层保护相互补充，即使一层保护被攻破，其他层仍可以保护信息的安全。目前，券商与交易所的数据传送是以DBF文件形式进行的，严格管理这些关键数据显得极为重要。现不少营业部均存在着任一工作站均可登录超级用户和一些重要帐户的现象，一旦口令被泄露或非法截取，就会难以控制入侵者的冒名访问。因此，对于超级用户和访问权限较大的用户应通过某种指定关系，如绑定在某些网卡的MAC地址上，实现逻辑和物理的双重认证，甚至指定登录的时间段。同时，还应尽量少直接使用超级用户，而改用与它等效的帐户使用，对于NT的Administrator最好更名后使用。不仅如此，对于其他用户帐户的设定也应遵守最小权限原则，并经常检查，及时清理不再使用的帐户与guest帐户。

3.3 访问审计控制

任何情况下，访问审计都是安全管理必不可少的要素。由于审计的不可更改性和可以记录对于受保护资源的操作情况，一方面能给内部黑客产生心理威慑力，打消其不规行为的念头。另一方面，也是发现、跟踪、分析、侦破、证实各种黑客案件的犯罪物证。所以，对于关键用户、关键数据文件应进行审计核查。

Netware 4.11 审计功能缺省是不启用的，启用时，需在客户端运行auditcon应用程序，然后依据定义审计的对象和项目，进行审计功能的设置，将需审计的内容置为on。需注意的是必须合理地设定审计文件的大小，若当前审计文件的尺寸太大，可能会占满SYS卷，导致服务器死机。在设置Audit file maximum size的90%。对于NT审计功能的开启，只要运行开始->程序->管理工具->域用户管理器，点击某一用户，点击菜单中的规则->审核，选择审核下列事件，将所要事件全部选上，确认即可。

3.4 软件系统版本

网络系统软件有其各自的安全等级，许多黑客程序都是针对网络系统软件的漏洞进行攻击的，如针对Netware的Bindery系统的攻击程序，针对windows NT服务拒绝访问的攻击程序等。这些程序轻者会在不知不觉中侵入和破坏，重者则会造成网络系统的瘫痪。因此，对于网络系统软件应注意及时升级和增装补丁程序，关闭无需使用的端口与服务，删除带有隐患的工具程序，以全面提高整个系统的安全性。

4 网络应用系统的安全策略

4.1 柜面交易软件安全体系设计

在券商的各个应用软件系统中，柜面交易软件的安全性最为重要。一个好的柜面软件设计可以修改/屏蔽/克服其他底层的安全威胁，从应用系统的最高层保证系统的整体安全。如，应用程序拥有自己的帐户管理、数据加密、身份验证和数据维护。通常，应用软件是利用其所依赖的软件平台来帮助实现安全管理的。如早几年的XBASE和Btrive数据库，正是因为存在着较大的安全漏洞，现已基本上不被柜面系统所采用，而改用基于SQL语言的数据库。这种数据库有着自己的用户管理机制，加上Client/Server结构使得客户机只能通过数据通信协议与数据库打交道，因而在一定程度上保证了应用数据的安全。目前，柜面交易软件的结构基本上是由前台应用程序和后台数据库所组成，其安全性是通过前台操作系统和后台数据库系统的身份校验和访问控制机制来保证的。前台操作系统根据系统用户的不同控制其对系统资源（文件、磁盘等）的访问，后台数据库系统根据数据库用户的不同控制其对数据库资源（数据库、表和存储过程等）的访问。由于这种结构不能从逻辑与物理上隔离前台业务与后台数据库，存在着客户机可以直接访问数据库的不利因素。因此，应当引入新一代三层结构的柜面交易软件，即在原来两层体系结构的基础上增加一中间层----应用网关，使得所有的前台操作请求需通过应用网关转发间接地访问数据库。网关与前台应用之间采用IPX/SPX或TCP/IP协议包方式通讯，并进行良好的数据加密。同时，网关中记录下所有的重要操作日志与客户资料的修改日志，如日期、时间、操作员、工作站、操作内容。并提供对某个操作员可登录系统的站点地址限制，这样整个数据库的安全性便能在网关中得到单点集中控制。

4.2 防火墙

防火墙是近期发展起来的一种保护计算机网络安全的软硬技术措施，可以理解为处在广域网与局域网之间的一道安全屏障。其目的是阻止外部网络的未授权访问，防火墙实现手段有包过滤技术和代理技术。现许多证券营业部都陆续开通了银证转帐和网上交易，一般是采用双网卡方式进行隔离，有的也增设了防火墙。通用的防火墙除价格较高之外，安全配置也较复杂，不少入侵事件都是因配置不当而使黑客有机可趁。所以，对于证券营业部来说，也可以采用对特定通讯端口（如串口或并口）的屏蔽来实现对局域网的安全保障。端口的通讯程序根据具体的应用专门开发，不支持任何网络通讯协议如TCP/IP和IPX，这样来自外部的未经授权的任何数据都会被阻断在串/并口处而无法进入券商的局域网。

4.3 病毒防范

计算机病毒是计算机系统安全的另一天敌。处在当今网络时代，计算机病毒不再只是来自共享的软盘，也可以通过E-mail，Web下载和网络服务器更为直接地进入客户端，其危害程度小到引起使用者的厌烦，影响系统性能，大到破坏数据，使系统瘫痪。因此，必须安装一个易于管理的从服务器端到客户端的多层次的病毒防御系统，并注意不断升级。

5 内部员工管理

在将注意力集中于外部攻击的同时，不能忽视内部攻击和授权滥用的可能。美国的FBI统计资料表明，因黑客攻击所造成的损失，有80%是由内部人员攻击和系统管理员失误所造成的。内部人员拥有合法的帐户和较高的权限，对网络及系统结构有足够的了解，既可以假装成黑客，以此作掩饰实施难以发现的侵入。又可以利用设备条件之便运行监听程序，截获未授权的信息，侵范股民利益或越权操作数据。还可以泄露机密给他人，实施内外勾结侵入。更可以直接利用其合法身份有意或无意地破坏系统。对于内部攻击的防范，从措施上讲已超出了经典技术的范畴，更多地需要和营业部的管理制度结合起来。只有不断加强员工的思想道德教育、法律知识教育、操作规范教育，强调三权分开，即操作系统管理员、应用系统管理员、审计监督员三者之间职责划分明确，权利各不相同，彼此相互协调、相互制约，再配合技术上的安全措施，才有可能将恶意的入侵者拒之于门外。■