证券系统网络的安全性

【摘要】

我在一家证券公司信息技术部门工作，我公司在 1998 年建成了与各公司总部及营业网点的企业网络，并已先后在企业网络上建设了交易系统、办公系统，并开通了互联网应用。因将对安全要求不同、安全可信度不同的各种应用运行在同一网络上，给黑客的攻击、病毒的蔓延打开了方便之门，给我公司的网络安全造成了很大的威胁。

作为信息技术中心部门经理及项目负责人，我在资金投入不足的前提下，充分利用现有条件及成熟技术，对公司网络进行了全面细致的规划，使改造后的网络安全级别大大提高。

本文将介绍我在网络安全性和保密性方面采取的一些方法和策略，主要包括网络安全隔离、网络边界安全控制、交叉病毒防治、集中网络安全管理等，同时分析了因投入资金有限，我公司网络目前仍存在的一些问题或不足，并提出了一些改进办法。

【正文】

我在一家证券公司工作，公司在 1998 年就建成了与各公司总部及营业网点的企业网络，随着公司业务的不断拓展，公司先后建设了集中报盘系统、网上交易系统、OA、财务系统、总部监控系统等等，为了保证各业务正常开展，特别是为了确保证券交易业务的实时高效，公司已于 2002 年已经将中心至各营业部的通讯链路由初建时的主链路 64K 的 DDN 和备链路 33.3K PSTN，扩建成主链路为 2M 光缆作为主链路和 256K 的 DDN 作为备链路，实现了通讯线路及关键网络设备的冗余，较好地保证了公司业务的需要。并且随着网上交易系统的建设和网上办公的需要，公司企业网与互联网之间建起了桥梁。

改造前，应用系统在用户认证及加密传输方面采取了相应措施，如集中交易在进行身份确认后信息采用了 Blowfish 128 位加密技术，网上交易运用了对称加密和非对称加密相结合的方法进行身份认证和数据传输加密，但公司办公系统、交易系统、互联网应用之间没有进行安全隔离，只在互联网入口安装了软件放防火墙，给黑客的攻击、病毒的蔓延打开了方便

之门。

作为公司信息技术中心运保部经理，系统安全一直是困扰着我的话题，特别是随着公司集中报盘系统、网上交易系统的建设，以及网上办公需要，网络安全系统的建设更显得犹为迫切。但公司考虑到目前证券市场疲软，竞争十分激励，公司暂时不打算投入较大资金来建设安全系统。

作为部门经理及项目负责人，我在投入较少资金的前提下，在公司可以容忍的风险级别和可以接受的成本之间作出取舍，充分利用现有的条件及成熟的技术，对公司网络进行了全面细致的规划，并且最大限度地发挥管理功效，尽可能全方位地提高公司的网络安全水平。

在网络安全性和保密性方面，我采用了以下技术和策略：

（1）将企业网划分成交易网、办公网、互联网应用网，进行网络隔离。

（2）在网络边界采取防火墙、存取控制、并口隔离等技术进行安全控制。

（3）运用多版本的防病毒软件对系统交叉杀毒。

（4）制定公司网络安全管理办法，进行网络安全集中管理。

1、网络安全隔离

为了达到网络互相不受影响，最好的办法是将网络进行隔离，网络隔离分为物理隔离和逻辑隔离，我主要是从系统的重要程度即安全等级考虑划分合理的网络安全边界，使不同安全级别的网络或信息媒介不能相互访问或有控制的进行访问。

针对我公司的网络系统的应用特点把公司证券交易系统、业务办公系统之间进行逻辑分离，划分成交易子网和办公子网，将互联网应用与公司企业网之间进行物理隔离，形成独立的互联网应用子网。公司中心与各营业部之间建有两套网络，中心路由器是两台 CISCO7206，营业部是两台 CISCO2612，一条通讯链路是联通 2M 光缆，一条是电信 256K DDN，改造前两套链路一主一备，为了充分利用网络资源实现两条链路的均衡负载和线路故障的无缝切换，子网的划分采用 VLAN 技术，并将中心端和营业部端的路由器分别采用两组虚拟地址的 HSRP 技术，一组地址对应交易子网，一组地址对应办公网络，形成两个逻辑上独立的网络。改造后原来一机两用（需要同时访问两个网络信息）的工作站采用双硬盘网络隔离卡的方法，在确

保隔离的前提下实现双网数据的安全交换。

2、网络边界安全控制

网络安全的需求一方面要保护网络不受破坏，另一方面要确保网络服务的可用性。将网络进行隔离后，为了能够满足网络内的授权用户对相关子网资源的访问，保证各业务不受影响，在各子网之间采取了不同的存取策略。

（1）互联网与交易子网之间：为了保证网上交易业务的顺利进行，互联网与交易子网之间建有通讯链路，为了保证交易网不受互联网影响，在互联网与中心的专线之间安装了NETSCREEN 委托防火墙，并进行了以下控制：

- 只允许股民访问网上交易相应地址的相应端口。
- 只允许信息技术中心的维护机地址 PING、TELNET 委托机和路由器。
- 只允许行情发送机向行情主站上传行情的端口。
- 其他服务及端口全部禁止。并且在互联网和交易网之间还采用了 SSL 并口隔离，进一步保证了交易网的安全。

（2）交易网和办公网之间：对于办公网与交易网之间的互访，采用 CISCO2501 路由器进行双向控制或有限访问原则，使受控的子网或主机访问权限和信息流向能得到有效控制，主要采用的策略主要是对具体 IP 进行 IP 地址与 MAC 地址的绑定。

（3）办公子网与互联网之间：采用东大 NETEYE 硬件防火墙，并进行了以下控制：

- 允许中心上网的地址访问互联网的任何地址和任何端口。
- 允许股民访问网上交易备份地址的 8002 端口。
- 允许短消息访问公司邮件 110、25 端口，访问电信 SP 的 8001 端口。
- 其他的都禁止。

3、病毒防治

网络病毒往往令人防不胜防，尽管对网络进行网络隔离，但网络资源互防以及人为原因，病毒防治依然不可掉以轻心。因此，采用适当的措施防治病毒，是进一步提高网络安全的重要手段。我分别在不同子网上部署了能够统一分发、集中管理的熊猫卫士网络病毒软件，同

时购置单机版 KV3000 和瑞星防病毒软件进行交叉杀毒；限制共享目录及读写权限的使用；限制网上软件的下载和禁用盗版软件；软盘数据和邮件先查毒后使用等等。

4、集中网络安全管理

网络安全的保障不能仅仅依靠安全设备，更重要的是要制定一个全方位的安全策略，在全网范围内实现统一集中的安全管理。在网络安全改造完成后，我制订了公司网络安全管理办法，主要措施如下：

（1）多人负责原则，每一项与安全有关的活动，都必须有两人或多人在场，并且一人操作一人复核。

（2）任期有限原则，技术人员不定期地轮岗。

（3）职责分离原则，非本岗人员不得掌握用户、密码等关键信息。

（4）营业部进行网络改造的方案必须经过中心网络安全小组审批后方可实施。

（5）跨网互访须绑定 IP 及 MAC 地址，增加互访机器时须经过中心批准并进行存取控制设置后方可运行。

（6）及时升级系统软件补丁，关闭不用的服务和端口等等。

在进行网络改造后，我公司的网络安全级别大大提高。但我知道安全永远只是一个相对概念，随着计算机技术不断进步，有关网络安全的讨论也将是一个无休无止的话题。审视改造后的网络系统，我认为尽管我们在 Internet 的入口处部署了防火墙，有效阻挡了来自外部的攻击，并且将网络分成三个子网较减少了各系统之间的影响，但在公司内部的访问控制以及入侵检测等方面仍显不足，如果将来公司投资允许，我将在以下几方面加强：

（1）在中心与营业部之间建立防火墙，通过访问控制防止通过内网的非法入侵。

（2）中心与营业部之间的通讯，采用通过 IP 层加密构建证券公司虚拟专用网（VPN），保证证券公司总部与各营业部之间信息传输的机密性。

（3）建立由入侵监测系统、网络扫描系统、系统扫描系统、信息审计系统、集中身份识别系统等构成的安全控制中心，作为公司网络监控预警系统。

保障网络安全性与网络服务效率永远是一对矛盾，在计算机应用日益广泛的今天，要想网络系统安全可靠，势必会增加许多控制措施和安全设备，从而会或多或少的影响使用效率和使用方便性。如，我在互联网和交易网之间设置了放防火墙的前提下再进行了 SSL 并口隔离后，网上交易股民访问交易网的并发人数达到一定量时就会出现延时现象，为了保证股民交易及时快捷，我只好采用增加通讯机的办法来消除交易延时问题。