快速通道

文档分类
- 红盟公告
- 新手上路
- 漏洞分析
- 工具介绍
- **安全配置** <=
- 编程技术
- 安全技术
- 业界动态

本类热门
- WIN2000常用服务的列表
- 某大型企业局域网安全解决方案
- UNIX入侵检测方法
- IPSec打造FreeBSD下信息安全传输

某大型企业局域网安全解决方案

提交文章： 墨斗鱼
提交日期： 2003-07-28
文章属性： 原创
文档类别： 安全配置
浏览次数： 今7次/总13931次

原创作者：墨斗鱼
来源：红客联盟

前言：
这是我为某大型企业写一份局域网安全解决方案建议书。本来这是不应该公开的，但是由于种种原因未能被采纳，所以也没什么大碍，现在拿出来给大家当作是一份参考资料，写的不好多多指教。文章是让大家参考的，不是让大家翻录的
学会自己用自己的思路去写东西，做了一些修改，请大家见凉！

****

（列表省略）

****

第一章 总则

本方案为某大型局域网网络安全解决方案，包括原有网络系统分析、安全需求分析、安全目标的确立、安全体系结构的设计、等。本安全解决方案的目标是在不影响某大型企业局域网当前业务的前提下，实现对他们局域网全面的安全管理。

1.将安全策略、硬件及软件等方法结合起来，构成一个统一的防御系统，有效阻止非法用户进入网络，减少网络的安全风险。
2.定期进行漏洞扫描，审计跟踪，及时发现问题，解决问题。
3.通过入侵检测等方式实现实时安全监控，提供快速响应故障的手段，同时具备很好的安全取证措施。
4.使网络管理者能够很快重新组织被破坏了的文件或应用。使系统重新恢复到破坏前的状态，最大限度地减少损失。
5.在工作站、服务器上安装相应的防病毒软件，由中央控制台统一控制和管理，实现全网统一防病毒。

第二章 网络系统概况

2.1 网络概况

这个企业的局域网是一个信息点较为密集的千兆局域网络系统，它所联接的现有上千个信息点为在整个企业内办公的各部门提供了一个快速、方便的信息交流平台。不仅如此，通过专线与Internet的连接，打通了一扇通向外部世界的窗户，各个部门可以直接与互联网用户进行交流、查询资料等。通过公开服务器，企业可以直接对外发布信息或者发送电子邮件。高速交换技术的采用、灵活的网络互连方案设计为用户提供快速、方便、灵活通信平台的同时，也为网络的安全带来了更大的风险。因此，在原有网络上实施一套完整、可操作的安全解决方案不仅是可行的，而且是必需的。

2.1.1 网络概述

这个企业的局域网，物理跨度不大，通过千兆交换机在主干网络上提供1000M的独享带宽，通过下级交换机与各部门的工作站和服务器连结，并为之提供100M的独享带宽。利用与中心交换机连结的Cisco 路由器，所有用户可直接访问Internet。

2.1.2 网络结构

这个企业的局域网按访问区域可以划分为三个主要的区域：Internet区域、内部网络、公开服务器区域。内部网络又可按照所属的部门、职能、安全重要程度分为许多子网，包括：财务子网、领导子网、办公子网、市场部子网、中心服务器子网等。在安全方案设计中，我们基于安全的重要程度和要保护的对象，可以在Catalyst 型交换机上直接划分四个虚拟局域网（VLAN），即：中心服务器子网、财务子网、领导子网、其他子网。不同的局域网分属不同的广播域，由于财务子网、领导子网、中心服务器子网属于重要网段，因此在中心交换机上将这些网段各自划分为一个独立的广播域，而将其他的工作站划分在一个相同的网段。（图省略）

2.2 网络应用

这个企业的局域网可以为用户提供如下主要应用：
1．文件共享、办公自动化、WWW服务、电子邮件服务；
2．文件数据的统一存储；
3．针对特定的应用在数据库服务器上进行二次开发(比如财务系统)；
4．提供与Internet的访问；
5．通过公开服务器对外发布企业信息、发送电子邮件等；

2.3 网络结构的特点

在分析这个企业局域网的安全风险时，应考虑到网络的如下几个特点：

1.网络与Internet直接连结，因此在进行安全方案设计时要考虑与Internet连结的有关风险，包括可能通过Internet传播进来病毒，黑客攻击，来自Internet的非授权访问等。
。
2.网络中存在公开服务器，由于公开服务器对外必须开放部分业务，因此在进行安全方案设计时应该考虑采用安全服务器网络，避免公开服务器的安全风险扩散到内部。
3.内部网络中存在许多不同的子网，不同的子网有不同的安全性，因此在进行安全方案设计时，应考虑将不同功能和安全级别的网络分割开，这可以通过交换机划分VLAN来实现。
4.网络中有二台应用服务器，在应用程序开发时就应考虑加强用户登录验证，防止非授权的访问。
总而言之，在进行网络方案设计时，应综合考虑到这个企业局域网的特点，根据产品的性能、价格、潜在的安全风险进行综合考虑。

第三章 网络系统安全风险分析

随着Internet网络急剧扩大和上网用户迅速增加，风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统，引起大范围的瘫痪和损失；另外加上缺乏安全控制机制和对Internet安全政策的认识不足，这些风险正日益严重。

针对这个企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险我们必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。下述风险由多种因素引起，与这个企业局域网结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。下面列出部分这类风险因素：

网络安全可以从以下三个方面来理解：1 网络物理是否安全；2 网络平台是否安全；3 系统是否安全；4 应用是否安全；5 管理是否安全。针对每一类安全风险，结合这个企业局域网的实际情况，我们将具体的分析网络的安全风险。

3.1物理安全风险分析

网络的物理安全的风险是多种多样的。

网络的物理安全主要是指地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获。以及高可用性的硬件、双机多冗余的设计、机房环境及报警系统、安全意识等。它是整个网络系统安全的前提，在这个企业区局域网内，由于网络的物理跨度不大，，只要制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险是可以避免的。

3.2网络平台的安全风险分析

网络结构的安全涉及到网络拓扑结构、网络路由状况及网络的环境等。

公开服务器面临的威胁

这个企业局域网内公开服务器区（WWW、EMAIL等服务器）作为公司的信息发布平台，一旦不能运行后者受到攻击，对企业的声誉影响巨大。同时公开服务器本身要为外界服务，必须开放相应的服务；每天，黑客都在试图闯入Internet节点，这些节点如果不保持警惕，可能连黑客怎么闯入的都不知道，甚至会成为黑客入侵其他站点的跳板。因此，规模比较大网络的管理人员对Internet安全事故做出有效反应变得十分重要。我们有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

整个网络结构和路由状况

安全的应用往往是建立在网络系统之上的。网络系统的成熟与否直接影响安全系统成功的建设。在这个企业局域网络系统中，只使用了一台路由器，用作与Internet连结的边界路由器，网络结构相对简单，具体配置时可以考虑使用静态路由，这就大大减少了因网络结构和网络路由造成的安全风险。

3.3系统的安全风险分析

所谓系统的安全显而易见是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任。

网络操作系统、网络硬件平台的可靠性：对于中国来说，恐怕没有绝对安全的操作系统可以选择，无论是Microsoft的Windows NT或者其他任何商用UNIX操作系统，其开发厂商必然有其Back-Door。我们可以这样讲：没有完全安全的操作系统。但是，我们可以对现有的操作平台进行安全配置、对操作和访问权限进行严格控制，提高系统的安全性。因此，不但要选用尽可能可靠的操作系统和硬件平台。而且，必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

3.4应用的安全风险分析

应用系统的安全跟具体的应用有关，它涉及很多方面。应用系统的安全是动态的、不断变化的。应用的安全性也涉及到信息的安全性，它包括很多方面。
应用系统的安全动态的、不断变化的：应用的安全涉及面很广，以目前Internet上应用最为广泛的E-mail系统来说，其解决方案有几十种，但其系统内部的编码甚至编译器导致的BUG是很少有人能够发现的，因此一套详尽的测试软件是相当必须的。但是应用系统是不断发展且应用类型是不断增加的，其结果是安全漏洞也是不断增加且隐藏越来越深。因此，保证应用系统的安全也是一个随网络发展不断完善的过程。
应用的安全性涉及到信息、数据的安全性：信息的安全性涉及到：机密信息泄露、未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。由于这个企业局域网跨度不大，绝大部分重要信息都在内部传递，因此信息的机密性和完整性是可以保证的。对于有些特别重要的信息需要对内部进行保密的（比如领导子网、财务系统传递的重要信息）可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。
3.5管理的安全风险分析

管理是网络安全中最重要的部分
管理是网络中安全最最重要的部分。责权不明，管理混乱、安全管理制度不健全及缺乏可操作性等都可能引起管理安全的风险。责权不明，管理混乱，使得一些员工或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漏他们所知道的一些重要信息，而管理上却没有相应制度来约束。
当网络出现攻击行为或网络受到其它一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求我们必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。
建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

3.6黑客攻击

黑客们的攻击行动是无时无刻不在进行的，而且会利用系统和管理上的一切可能利用的漏洞。公开服务器存在漏洞的一个典型例证，是黑客可以轻易地骗过公开服务器软件，得到Unix的口令文件并将之送回。黑客侵入UNIX服务器后，有可能修改特权，从普通用户变为高级用户，一旦成功，黑客可以直接进入口令文件。黑客还能开发欺骗程序，将其装入UNIX服务器中，用以监听登录会话。当它发现有用户登录时，便开始存储一个文件，这样黑客就拥有了他人的帐户和口令。这时为了防止黑客，需要设置公开服务器，使得它不离开自己的空间而进入另外的目录。另外，还应设置组特权，不允许任何使用公开服务器的人访问WWW页面文件以外的东西。在这个企业的局域网内我们可以综合采用防火墙技术、Web页面保护技术、入侵检测技术、安全评估技术来保护网络内的信息资源，防止黑客攻击。

3.7通用网关接口（CGI）漏洞

有一类风险涉及通用网关接口（CGI）脚本。许多页面文件和指向其他页面或站点的超连接。然而有些站点用到这些超连接所指站点寻找特定信息。搜索引擎是通过CGI脚本执行的方式实现的。黑客可以修改这些CGI脚本以执行他们的非法任务。通常，这些CGI脚本只能在这些所指WWW服务器中寻找，但如果进行一些修改，他们就可以在WWW服务器之外进行寻找。要防止这类问题发生，应将这些CGI脚本设置为较低级用户特权。提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

3.8恶意代码

恶意代码不限于病毒，还包括蠕虫、特洛伊木马、逻辑炸弹、和其他未经同意的软件。应该加强对恶意代码的检测。

3.9病毒的攻击

计算机病毒一直是计算机安全的主要威胁。能在Internet上传播的新型病毒，例如通过E-Mail传播的病毒，增加了这种威胁的程度。病毒的种类和传染方式也在增加，国际空间的病毒总数已达上万甚至更多。当然，查看文档、浏览图像或在Web上填表都不用担心病毒感染，然而，下载可执行文件和接收来历不明的E-Mail文件需要特别警惕，否则很容易使系统导致严重的破坏。典型的“ CIH ”病毒就是一可怕的例子。

3.10不满的内部员工

不满的内部员工可能在WWW站点上开些小玩笑，甚至破坏。不论如何，他们最熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员工能造成更大的损失，例如他们可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据等等。

3.11网络的攻击手段

一般认为，目前对网络的攻击手段主要表现在：
非授权访问：没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。
信息泄漏或丢失：指敏感数据在有意或无意中被泄漏出去或丢失，它通常包括，信息在传输中丢失或泄漏（如"黑客"们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、帐号等重要信息。），信息在存储介质中丢失或泄漏，通过建立隐蔽隧道等窃取敏感信息等。
破坏数据完整性：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。
拒绝服务攻击：它不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。
利用网络传播病毒：通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

第四章 安全需求与安全目标

4.1安全需求分析

通过前面我们对这个企业局域网络结构、应用及安全威胁分析，可以看出其安全问题主要集中在对服务器的安全保护、防黑客和病毒、重要网段的保护以及管理安全上。因此，我们必须采取相应的安全措施杜绝安全隐患，其中应该做到：

公开服务器的安全保护

防止黑客从外部攻击
入侵检测与监控
信息审计与记录
病毒防护
数据安全保护
数据备份与恢复
网络的安全管理

针对这个企业局域网络系统的实际情况，在系统考虑如何解决上述安全问题的设计时应满足如下要求：

1.大幅度地提高系统的安全性（重点是可用性和可控性）；

2.保持网络原有的能特点，即对网络的协议和传输具有很好的透明性，能透明接入，无需更改网络设置；
3.易于操作、维护，并便于自动化管理，而不增加或少增加附加操作；
4.尽量不影响原网络拓扑结构，同时便于系统及系统功能的扩展；
5.安全保密系统具有较好的性能价格比，一次性投资，可以长期使用；
6.安全产品具有合法性，及经过国家有关管理部门的认可或认证；
7.分布实施。

4.2网络安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。该安全策略模型包括了建立安全环境的三个重要组成部分，即：
威严的法律：安全的基石是社会法律、法规、与手段，这部分用于建立一套安全管理标准和方法。即通过建立与信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。
先进的技术：先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。
严格的管理：各网络使用机构、企业和单位应建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

4.3系统安全目标

基于以上的分析，我们认为这个局域网网络系统安全应该实现以下目标：
建立一套完整可行的网络安全与网络管理策略
将内部网络、公开服务器网络和外网进行有效隔离，避免与外部网络的直接通信
建立网站各主机和服务器的安全保护措施，保证他们的系统安全
对网上服务请求内容进行控制，使非法访问在到达主机前被拒绝
加强合法用户的访问认证，同时将用户的访问权限控制在最低限度
全面监视对公开服务器的访问，及时发现和拒绝不安全的操作和黑客攻击行为
加强对各种访问的审计工作，详细记录对网络、公开服务器的访问行为，形成完 整的系统日志
备份与灾难恢复——强化系统备份，实现系统快速恢复
加强网络安全管理，提高系统全体人员的网络安全意识和防范技术

第五章 网络安全方案总体设计

5.1安全方案设计原则

在对这个企业局域网网络系统安全方案设计、规划时，应遵循以下原则：

综合性、整体性原则：应用系统工程的观点、方法，分析网络的安全及具体措施。安全措施主要包括：行政法律手段、各种管理制度（人员审查、工作流程、维护保障制度等）以及专业措施（识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等）。一个较好的安全措施往往是多种方法适当综合的应用结果。一个计算机网络，包括个人、设备、软件、数据等。这些环节在网络中的地位和影响作用，也只有从系统综合整体的角度去看待、分析，才能取得有效、可行的措施。即计算机网络安全应遵循整体安全性原则，根据规定的安全策略制定出合理的网络安全体系结构。

需求、风险、代价平衡的原则：对任一网络，绝对安全难以达到，也不一定是必要的。对一个网络进行实际额研究（包括任务、性能、结构、可靠性、可维护性等），并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定本系统的安全策略。

一致性原则：一致性原则主要是指网络安全问题应与整个网络的工作周期（或生命周期）同时存在，制定的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计（包括初步或详细设计）及实施计划、网络验证、验收、运行等，都要有安全的内容光焕发及

措施，实际上，在网络建设的开始就考虑网络安全对策，比在网络建设好后再考虑安全措施，不但容易，且花费也小得多。

易操作性原则：安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

分步实施原则：由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加。一劳永逸地解决网络安全问题是不现实的。同时由于实施信息安全措施需相当的费用支出。因此分步实施，即可满足网络系统及信息安全的基本需求，亦可节省费用开支。

多重保护原则：任何安全措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其它层保护仍可保护信息的安全。

可评价性原则：如何预先评价一个安全设计并验证其网络的安全性，这需要通过国家有关网络信息安全测评认证机构的评估来实现。

5.2安全服务、机制与技术

安全服务：安全服务主要有：控制服务、对象认证服务、可靠性服务等；

安全机制：访问控制机制、认证机制等；

安全技术：防火墙技术、鉴别技术、审计监控技术、病毒防治技术等；在安全的开放环境中，用户可以使用各种安全应用。安全应用由一些安全服务来实现；而安全服务又是由各种安全机制或安全技术来实现的。应当指出，同一安全机制有时也可以用于实现不同的安全服务。

第六章 网络安全体系结构

通过对网络的全面了解，按照安全策略的要求、风险分析的结果及整个网络的安全目标，整个网络措施应按系统体系建立。具体的安全控制系统由以下几个方面组成：物理安全、网络安全、系统安全、信息安全、应用安全和安全管理

6.1物理安全

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提，物理安全是保护计算机网络设备、设施以及其它媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。 它主要包括三个方面：

环境安全：对系统所在环境的安全保护，如区域保护和灾难保护；（参见国家标准GB50173－93《电子计算机机房设计规范》、国标GB2887－89《计算站场地技术条件》、GB9361－88《计算站场地安全要求》
设备安全：主要包括设备的防盗、防毁、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等；
媒体安全：包括媒体数据的安全及媒体本身的安全。

在网络的安全方面，主要考虑两个大的层次，一是整个网络结构成熟化，主要是优化网络结构，二是整个网络系统的安全。

6.2.1网络结构

安全系统是建立在网络系统之上的，网络结构的安全是安全系统成功建立的基础。在整个网络结构的安全方面，主要考虑网络结构、系统和路由的优化。
网络结构的建立要考虑环境、设备配置与应用情况、远程联网方式、通信量的估算、网络维护管理、网络应用与业务定位等因素。成熟的网络结构应具有开放性、标准化、可靠性、先进性和实用性，并且应该有结构化的设计，充分利用现有资源，具有运营管理的简便性，完善的安全保障体系。网络结构采用分层的体系结构，利于维护管理，利于更高的安全控制和业务发展。
网络结构的优化，在网络拓扑上主要考虑到冗余链路；防火墙的设置和入侵检测的实时监控等。

6.2.2网络系统安全

6.2.2.1 访问控制及内外网的隔离

访问控制
访问控制可以通过如下几个方面来实现：
1.制订严格的管理制度:可制定的相应：《用户授权实施细则》、《口令字及帐户管理规范》、《权限管理制度》。

2.配备相应的安全设备：在内部网与外部网之间，设置防火墙实现内外网的隔离与访问控制是保护内部网安全的最主要、同时也是最有效、最经济的措施之一。防火墙设置在不同网络或网络安全域之间信息的唯一出入口。

防火墙主要的种类是包过滤型，包过滤防火墙一般利用IP和TCP包的头信息对进出被保护网络的IP包信息进行过滤，能根据企业的安全政策来控制（允许、拒绝、监测）出入网络的信息流。同时可实现网络地址转换（NAT）、审记与实时告警等功能。由于这种防火墙安装在被保护网络与路由器之间的通道上，因此也对被保护网络和外部网络起到隔离作用。

防火墙具有以下五大基本功能：过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止的业务；记录通过防火墙的信息内容和活动；对网络攻击的检测和告警。

6.2.2.2 内部网不同网络安全域的隔离及访问控制

在这里，主要利用VLAN技术来实现对内部子网的物理隔离。通过在交换机上划分VLAN可以将整个网络划分为几个不同的广播域，实现内部一个网段与另一个网段的物理隔离。这样，就能防止影响一个网段的问题穿过整个网络传播。针对某些网络，在某些情况下，它的一些局域网的某个网段比另一个网段更受信任，或者某个网段比另一个更敏感。通过将信任网段与不信任网段划分在不同的VLAN段内，就可以限制局部网络安全问题对全局网络造成的影响。

6.2.2.3 网络安全检测

网络系统的安全性取决于网络系统中最薄弱的环节。如何及时发现网络系统中最薄弱的环节？如何最大限度地保证网络系统的安全？最有效的方法是定期对网络系统进行安全性分析，及时发现并修正存在的弱点和漏洞。
网络安全检测工具通常是一个网络安全性评估分析软件，其功能是用实践性的方法扫描分析网络系统，检查报告系统存在的弱点和漏洞，建议补救措施和安全策略，达到增强网络安全性的目的。检测工具应具备以下功能：

具备网络监控、分析和自动响应功能

找出经常发生问题的根源所在；
建立必要的循环过程确保隐患时刻被纠正；控制各种网络安全危险。
漏洞分析和响应
配置分析和响应
漏洞形势分析和响应
认证和趋势分析

具体体现在以下方面：

防火墙得到合理配置
内外WEB站点的安全漏洞减为最低
网络体系达到强壮的耐攻击性
各种服务器操作系统，如E_MIAL服务器、WEB服务器、应用服务器、，将受黑客攻击的可能降为最低
对网络访问做出有效响应，保护重要应用系统（如财务系统）数据安全不受黑客攻击和内部人员误操作的侵害

6.2.2.4 审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，它是提高安全性的重要工具。它不仅能够识别谁访问了系统，还能看出系统正被怎样地使用。对于确定是否有网络攻击的情况，审计信息对于去定问题和攻击源很重要。同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。

因此，除使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

6.2.2.5 网络防病毒

由于在网络环境下，计算机病毒有不可估量的威胁性和破坏力，一次计算机病毒的防范是网络安全性建设中重要的一环。
网络反病毒技术包括预防病毒、检测病毒和消毒三种技术：
1.预防病毒技术：它通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有，

加密可执行程序、引导区保护、系统监控与读写控制（如防病毒软件等）。
2.检测病毒技术：它是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。
3.清除病毒技术：它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。

网络反病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和监测；在工作站上用防病毒芯片和对网络目录及文件设置访问权限等。

所选的防毒软件应该构造全网统一的防病毒体系。主要面向MAIL 、Web服务器，以及办公网段的PC服务器和PC机等。支持对网络、服务器、和工作站的实时病毒监控；能够在中心控制台向多个目标分发新版杀毒软件，并监视多个目标的病毒防治情况；支持多种平台的病毒防范；能够识别广泛的已知和未知病毒，包括宏病毒；支持对Internet/ Intranet服务器的病毒防治，能够阻止恶意的Java或ActiveX小程序的破坏；支持对电子邮件附件的病毒防治，包括WORD、EXCEL中的宏病毒；支持对压缩文件的病毒检测；支持广泛的病毒处理选项，如对染毒文件进行实时杀毒，移出，重新命名等；支持病毒隔离，当客户机试图上载一个染毒文件时，服务器可自动关闭对该工作站的连接；提供对病毒特征信息和检测引擎的定期在线更新服务；支持日志记录功能；支持多种方式的告警功能（声音、图像、电子邮件等）等。

6.2.2.6 网络备份系统

备份系统为一个目的而存在：尽可能快地全盘恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有：场点内高速度、大容量自动的数据存储、备份与恢复；场点外的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时亦是系统灾难恢复的前提之一。

在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份，有“冷备份”和“热备份”两种。热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到令一个非工作的分区或是另一个非实时处理的业务系统中存放。“冷备份”是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。热备份的优点是投资大，但调用快，使用方便，在系统恢复中需要反复调试时更显优势。热备份的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；另一种方法是，将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。冷备份弥补了热备份的一些不足，二者优势互补，相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。

6.3系统安全

系统的安全主要是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。对于操作系统的安全防范可以采取如下策略：

对操作系统进行安全配置，提高系统的安全性；系统内部调用不对Internet公开；关键性信息不直接公开，尽可能采用安全性高的操作系统。
应用系统在开发时，采用规范化的开发过程，尽可能的减少应用系统的漏洞；
网络上的服务器和网络设备尽可能不采取同一家的产品；
通过专业的安全工具（安全检测系统）定期对网络进行安全评估。

6.4信息安全

在这个企业的局域网内，信息主要在内部传递，因此信息被窃听、篡改的可能性很小，是比较安全的。

6.5应用安全

在应用安全上，主要考虑通信的授权，传输的加密和审计记录。这必须加强登录过程的认证（特别使在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。另外，在加强主机的管理上，除了上面谈的访问控制和系统漏洞检测外，还可以采用访问存取控制，对权限进行分割和管理。应用安全平台要加强资源目录管理和授权管理、传输加密、审计记录和安全管理。对应用安全，主要考虑确定不同服务的应用软件并紧密注视其Bug ；对扫描软件不断升级。

6.6安全管理

为了保护网络的安全性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，安全管理规范也是网络安全所必须的。安全管理策略一方面从纯粹的管理上即安全管理规范来实现，另一方面从技术上建立高效的管理平台（包括网络管理和安全管理）。安

全管理策略主要有：定义完善的安全管理模型；建立长远的并且可实施的安全策略；彻底贯彻规范的安全防范措施；建立恰当的安全评估尺度，并且进行经常性的规则审核。当然，还需要建立高效的管理平台。

6.6.1安全管理规范

面对网络安全的脆弱性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，还必须花大力气加强网络安全管理规范的建立，因为诸多的不安全因素恰恰反映在组织管理和人员录用等方面，而这又是计算机网络安全所必须考虑的基本问题，所以应引起各计算机网络应用部门领导的重视。

1.安全管理原则

网络信息系统的安全管理主要基于三个原则。
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。这些人应是系统主管领导指派的，他们忠诚可靠，能胜任此项工作；他们应该签署工作情况记录以证明安全工作已得到保障。具体的活动有：
访问控制使用证件的发放与回收；
信息处理系统使用的媒介发放与回收；
处理保密信息；
硬件和软件的维护；
系统软件的设计、实现和修改；
重要程序和数据的删除和销毁等；
任期有限原则：一般地讲，任何人最好不要长期担任与安全有关的职务，以免使他认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。
职责分离原则：在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。出于对安全的考虑，下面每组内的两项信息处理工作应当分开。

计算机操作与计算机编程；
机密资料的接收和传送；
安全管理和系统管理；
应用程序和系统程序的编制；
访问证件的管理与其它工作；
计算机操作与信息处理系统使用媒介的保管等。

2.安全管理的实现
信息系统的安全管理部门应根据管理原则和该系统处理数据的保密性，制定相应的管理制度或采用相应的规范。具体工作是：
根据工作的重要程度，确定该系统的安全等级
根据确定的安全等级，确定安全管理的范围
制订相应的机房出入管理制度对于安全等级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。出入管理可采用证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段，对人员进行识别、登记管理。
制订严格的操作规程
操作规程要根据职责分离和多人负责的原则，各负其责，不能超越自己的管辖范围。
制订完备的系统维护制度
对系统进行维护时，应采取数据保护措施，如数据备份等。维护时要首先经主管部门批准，并有安全管理人员在场，故障的原因、维护内容和维护前后的情况要详细记录。
制订应急措施
要制定系统在紧急情况下，如何尽快恢复的应急措施，使损失减至最小。建立人员雇用和解聘制度，对工作调动和离职人员要及时调整响应的授权。

6.6.2网络管理

管理员可以在管理机器上对整个内部网络上的网络设备、安全设备、网络上的防病毒软件、入侵检测探测器进行综合管理，同时利用安全分析软件可以从不同角度对所有的设备、服务器、工作站进行安全扫描，分析他们的安全漏洞，并采取相应的措施。

6.6.3安全管理

安全管理的主要功能指对安全设备的管理；监视网络危险情况，对危险进行隔离，并把危险控制在最小范围内；身份认证，权限设置；对资源的存取权限的管理；对资源或用户动态的或静态的审计；对违规事件，自动生成报警或生成事件消息；口令管理（如操作员的口令鉴权），对无权操作人员进行控制；密钥管理：对于与密钥相关的服务器，应对其设置密钥生命期、密钥备份等管理功能；冗余备份：为增加网络的安全系数，对于关键的服务器应冗余备份。安全管理应该从管理制度和管理平台技术实现两个方面来实现。安全管理产品尽可能的支持统一的中心控制平台。

第七章 安全解决配置方案
以下省略主要涉及到一些东西，这篇文章的目的教你怎样去设计一个安全解决方案，所以具体的安全解决配置，我就不在叙述了，具体的思路已经写出来了，剩下的配置就要根据实际情况去做了。 如果有什么不对的地方，请多指教，谢谢！（有一些图我省略了，思路出来了图也就出来了）

****

文章版权归cnhonker和作者本人所有，如要转载请注明出处

****

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.
中国红客网络技术联盟 www.cnhonker.com
webmaster@cnhonker.net