浅析企事业单位网络安全防范策略

苏晓美[1]，方杰[2]，范利强[2]

（1.廊坊市畜牧水产局，河北省廊坊市 065000；

2.廊坊师范学院 信息与计算科学系，河北省廊坊市 065000）

摘　要：本文通过分析网络信息安全现状，结合廊坊市企事业单位网络设置，给出了针对企事业单位网络安全的几种合理有效的防范策略。

一、背景介绍

现代意义上的计算机网络是从 20 世纪 60 年代末美国国防部高级研究计划局（DARPA）建成的 ARPAnet 实验网开始的。20 世纪 90 年代，随着 Internet 学会的成立，计算机网络飞速发展，网络的信息流量每年都在成倍的增长，企事业单位基于网络的计算机应用也在迅速增加。网络信息系统给企事业单位的经营和管理带来了更大的经济效益，但随之而来的安全保障问题也在困扰着用户。

攻击者可以窃听网络上的信息，窃取用户的口令、数据库的信息，篡改数据库内容，伪造用户身份，否认自己的签名。更有甚者，攻击者可以删除数据库内容，摧毁网络节点，释放计算机病毒等等。在网络安全越来越受到人们重视和关注的今天，网络安全技术作为一个独特的领域越来越受到人们关注。

与发达国家相比，我国网络安全建设发展相对较晚，无论在网络安全意识还是网络安全防护技术等方面都存在一定差距。如何确保网络和信息安全，网络管理人员如何结合本单位实际情况，采取有效防护措施，已经成为当前网络安全的重要问题。

二、网络安全威胁和技术

网络安全其本质就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或恶意的原因而遭到破坏、更改和泄露，系统连续可靠运行，网络服务不中断[1]。网络安全要做到保密性、完整性、可用性和可审查性。

影响企事业单位的网络安全因素主要有物理安全、网络安全、系统安全、应用安全和管理安全等。

1、物理安全威胁

自然环境和社会环境对计算机网络会产生极大的影响。如恶劣的天气、自然灾害等都会

对网络造成损害和影响。

2、网络安全威胁

网络协议中使用最广泛的是 TCP/IP 协议，设计目标是互联、互通和互操作，而不是安全，同时由于它的安全公开性，使得协议中存在许多的安全隐患。

3、系统安全威胁

现在流行的操作系统都提供无口令入口，这为系统开发人员提供了便捷，但它也是黑客的通道。另外，操作系统的隐蔽通道，也给了黑客可乘之机。同时，很多操作系统都包含了各种常见的通用服务，如 telnet、ftp、www 等。而企事业单位所需要的服务通常具有一定的专属性，如果系统安装时没有关闭这些不相关的服务，它们就有可能成为入侵的途径。

4、应用安全威胁

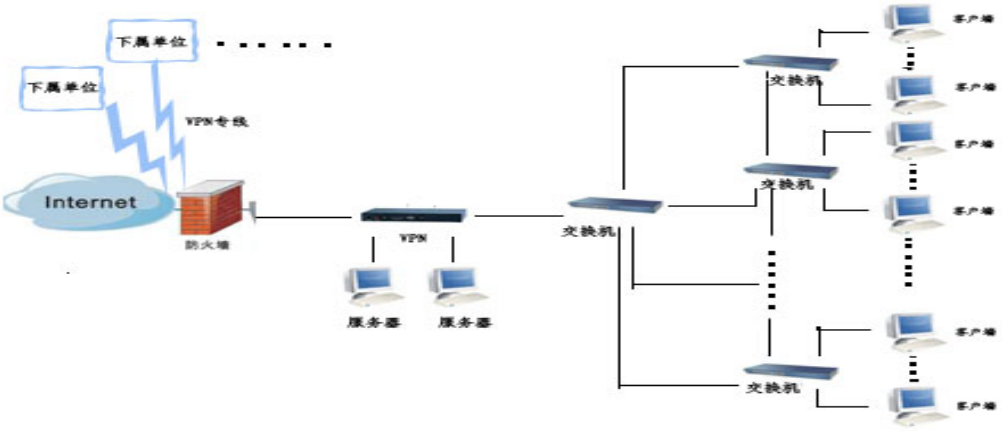
提供远程办公接入服务时，如果在接入服务器上对用户没有进行有效的认证、有效的控制访问范围、有效的督察用户，都会增加网络的安全威胁。企事业单位网络是一个庞大的系统，各个子系统对于安全的要求也不同，所以企事业单位各个子系统之间如果没有控制相互之间的访问，也可能导致内部信息泄露。

5、管理安全威胁

分工不明致使企事业单位网络使用权限与行政管理权限的不相匹配，从而增加了安全漏洞。网络管理人员如果缺乏保密意识，也容易造成安全威胁。多数企事业单位采用登陆密码作为管理员账号的认证方式，但是缺乏管理的管理员账号，以及口令本身也造成了安全隐患。例如口令的重复使用、采用明文传输、使用静态口令而不做定期修改、口令过于简单等，都会增大口令被破译的风险。

三、网络拓扑结构

考虑某事业单位有计算机 100 台，通过内部网相互连接，根据单位统一规划，通过防火墙与外网互联。在内部网络中，各计算机在同一网段，通过交换机连接。网络拓扑结构如图一所示：



图一 网络结构图

四、网络安全防范策略

任何形式的互联网服务都会导致安全方面的风险，网络安全方法的关键在于如何将风险降至最低。通过从事多年网络管理工作，总结出一些切实可行的网络安全防范策略。

1、设置防火墙，加固网络安全壁垒

从狭义上说防火墙是安装了防火墙软件的主机或路由器系统，从广义上讲它是包括整个网络的安全策略和安全行为[2]。所有的从外部到内部或从内部到外部的通信都经过它，只有有内部访问策略授权的通信才能被允许通过。目前的防火墙主要有包过滤防火墙、应用网关防火墙、代理服务防火墙、状态检测防火墙、自适应代理技术等几种。用防火墙实现网络安全的实质是：将主机按照安全等级和提供的服务划分成域，并在进出域的阻塞点上放置防火墙，允许或阻断信息的进出。现在多数企事业单位采用的拓扑结构都是“屏蔽子网结构”。它增加一层周边网络安全机制，用两部分分组过滤路由器将周边网络与内部网络和外部网络相隔开，即所谓的 “非军事区”，这样内部网和外部网没有直接连接，需通过非军事区进行中转，不存在危害网络的单一入口点。增加了攻击的难度，屏蔽的子网结构是一种比较完整的防火墙体系结构。通过以防火墙为中心的安全方案配置，能将所有安全软件(如口令、加密、身份认证)配置在防火墙上。其次利用防火墙对网络存取和访问进行监控审计。如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并做出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而降低了局部重点或敏感网络安全问题对全局网络造成的影响。

2、定期查杀病毒，增强系统免疫力

病毒是指一段可执行的代码，通过其他程序进行修改，可以感染这些程序使其含有该病

毒程序的一个副本，病毒类型有多种，寄生病毒、存储器驻留病毒、引导区病毒、隐形病毒、多型病毒等[3]。预防和查杀病毒必须从两方面入手，一方面是预防，一方面是检测和治疗。对于中小型企事业单位而言，最简单有效的方法就是安装最全面的杀毒软件，并时时更新，定期查杀病毒。杀毒软件从功能上可以分为网络防病毒软件和单机防病毒软件两大类。单机防病毒软件一般安装在单台 PC 上，对本地和本地工作站连接的远程资源采用分析扫描的方式检测、清除病毒。网络防病毒软件则主要注重网络防病毒，一旦病毒入侵网络或者从网络向其它资源传染，网络防病毒软件会立刻检测到并加以删除。

3、加密重要数据，进行身份认证管理

数据加密是通过对信息的重新组合，使得只有收发双方才能解码并还原信息的一种手段，对某些具有很强安全性的数据[4]，如用户密码，财务数据，重要文件等通过数据加密方法来保障数据的安全。常用的数据加密技术有 DES、 IDEA、 公钥加密算法和 RSA 算法，对于要获取主要数据的用户在客户端和服务器上进行验证，利用安全密码，信息卡等。密码口令可采用一次性口令，每次登陆后采用新密码。

身份认证是指计算机及网络系统确认操作者身份的过程[5]。基于 PKI 的身份认证方式是近几年发展起来的一种方便、安全的身份认证技术。它采用软硬件相结合、一次一密的强双因子认证模式，很好地解决了安全性与易用性之间的矛盾。USB Key 是一种 USB 接口的硬件设备，它内置单片机或智能卡芯片，可以存储用户的密钥或数字证书，利用 USB Key 内置的密码算法实现对用户身份的认证。

基于 PKI 的 USB Key 的解决方案不仅可以提供身份认证的功能，还可构建用户集中管理与认证系统、应用安全组件、客户端安全组件和证书管理系统通过一定的层次关系和逻辑联系构成的综合性安全技术体系，从而实现上述身份认证、授权与访问控制、安全审计、数据的机密性、完整性、抗抵赖性的总体要求。

4、定期备份数据，确保数据的万无一失

不论多么严格的防守，也不能保证网络百分之百的安全，为保证重要数据不丢失不破坏，一定要定期进行备份。数据备份包括对重要信息数据和软件系统的备份。备份的介质有硬盘、移动硬盘、光盘、网络硬盘、邮箱等。通常数据备份的方法有 windows 系统自带的数据备份程序、Ghost 数据备份、异地数据备份等。结合单位的具体情况和数据的特点，选择合适的方法对数据和系统进行定期的备份工作，以确保数据的万无一失。

5、利用网络监听，维护子网系统安全

一个小的企事业单位所有的计算机组成了一个局域网，攻击或异常既有来自外部的，

也有来自内部的，在服务器端应用流量监控软件，可随时发现问题，起到一定预警作用，网管人员通过情况分析，判断是哪里出了问题，及时进行制止，防患于未然。

6、实施物理隔离，轻松隔断内外网

中小企事业单位大都有涉密计算机，为保数据的安全可靠，可以采用物理隔离的形式，或者涉密计算机完全不具备上网功能，或者在每台电脑中通过主板插槽安装物理隔离卡，把一台普通计算机分成两台虚拟计算机，实现真正的物理隔离。目前的隔离卡分双硬盘物理隔离卡和单硬盘隔离卡。目前使用较好的是单硬盘物理隔离卡，它代表着国际上计算机物理隔离产品最先进的技术。它能在不增加其他硬件和软件成本、不对系统重新设置的情况下，实现单台计算机连接内外两个网络的物理隔离方案,完全杜绝了各种可能的内部及外部网络的攻击或泄密，且解决了物理隔离之后某些信息无法安全地进行交换的问题。

7、利用 VPN 技术，实现数据安全通信

对于一些经常和分支机构联系的企事业单位，由于地理位置的限制，要实现总部和分支的互联，考专线连接费用昂贵，而应用 VPN 技术实现即安全又廉价。虚拟专用网（VPN）是建立在公用网上的，由某一组织或某一群用户专用的通信网络，其虚拟性表现在任一对 VPN 用户之间没有专用的物理连接，而是通过 ISP 提供的公用网络来实现通信的。其专用性表现在 VPN 之外的用户无法访问 VPN 内部的网络资源，VPN 内部用户之间可以实现安全通信。实现 VPN 有许多关键技术，隧道技术、加解密技术、密钥管理技术和身份认证技术，这些技术保证信息在 intranet 内部安全的传输。企事业单位可以采取内联网 VPN 方案，实现总部和各分支单位 LAN 之间的连接，实现数据传输和视频会议。

8、加强物理安全，为网络运行创造环境

除了要保证要有电脑锁之外，更多的要注意消防安全,要将电线和网络放在比较隐蔽的地方。我们还要准 UPS，以确保网络能够以持续的电压运行。在电子学中，峰值电压是一个非常重要的概念，峰值电压高的时候可以烧坏电器,迫使网络瘫痪,峰值电压最小的时候,网络根本不能运行。使用 UPS 可以排除这些意外。

9、规范管理体制，保障网络安全的实施

单纯的从计算机和网络技术方面进行安全防范是远远不够的，必须从思想上深刻认识网络数据安全的重要性，这就要求企事业单位要严格管理制度，明确管理职责，配备专门人才，加强保密意思，建立完整有效的《网络信息安全管理规范》，并严格执行，这是保证网络安全的关键。

（1）机构建设

成立网络安全领导小组和工作小组，领导小组负责规划网络安全的目标、确定网络安全的内容、制定网络安全的规章、监督网络安全的实施，处理突发网络安全事件等；工作小组负责网络安全的日常管理和一般事件的处理，并设专人按照规章制度的要求实施安全维护工作，责任落实到具体的岗位和具体的人。

（2）制度建设

为保障网络安全有章可循，有据可依，可以制定一系列切实可行的规章制度，例如《网络信息安全管理规范》、《机房管理制度》、《网络突发事件应急管理预案》、《网络管理员守则》、《网络信息保密制度》等。只有严格按照管理制度实行，才能把网络安全做到实处。

（3）素质建设

网络的信息安全不仅仅是网管人员的责任，它涉及到企事业单位内的每位职工，只有职工的素质提高了，网络安全才有保障。可以采取集中培训和自学的形式，培养职工的安全意识，做好本职工作。

安全管理一直是网络系统的薄弱环节之一，而用户对网络安全的要求往往又相当高，因此安全管理就显得非常重要。企事业单位的网络管理者必须充分意识到潜在的安全性威胁，并采取一定的防范措施，尽可能减少这些威胁带来的恶果，将来自企事业单位网络内部和外部对数据和设备所引起的危险降到最低程度。

参考文献

[1] 雷震甲.《网络工程师教程》，清华大学出版社，2006.06
[2] 杨义先.《网络安全理论与技术》.人民邮电出版社，2003，10.
[3] 杨悦.企事业单位网络安全管理与防护策略.电脑知识与技术，2005.10
[4] 蒋天发.《网络信息安全》电子工业出版社.2009
[5] 范明钰，王光卫.《网络安全协议理论与技术》.清华大学出版社，2009
[6] 刘远生,辛一.《计算机网络安全》.清华大学出版社。2009

基金项目：河北省教育厅项目（2009138）