网络维护方案

第一部分 网络安全概述

现代计算机系统功能日渐复杂，网络功能日渐强大，正在对社会的各行各业产生巨大深远的影响，但同时由于其开放性特点，使得安全问题越来越突出。 然而，随着人们对计算机网络依赖程度的日渐加深，网络安全也表现得越来越重要。由于网络的互联共享，来自企业内部和全世界各个地方不怀好意的计算机专业人士和黑客都有可能对其实施攻击。我们几乎每天都可以听到黑客对某某企业信息资源进行入侵、篡改和破坏的报道，所以分析和研究黑客入侵技术，研究安全漏洞并修补之，增强网络和信息的安全性能，抵抗黑客入侵破坏，构建一个安全的企业网络系统是非常重要的。

为了应对日益增长的信息安全事件及其相关的资金损失，在过去几年中已经出现了多种信息安全技术，其中包括防火墙、入侵系统检测 (IDS)、虚拟专用网 (VPN) 以及公钥基础结构 (PKI)。对信息安全解决方案的迫切需求已经促成了开发三类可满足一个安全计算环境基本需求的信息安全技术：防火墙（入侵阻止）；IDS（入侵检测），及 VPN（通过数据加密进行安全通讯）。在过去几年中，这些解决方案的全球市场平均年增长率约为 20%-30%， 且已构成信息安全的基本要素。

自网络问世以来，资源共享和信息安全一直作为一对矛盾体而存在着，计算机网络资源共享的进一步加强随之而来的信息安全问题也日益突出，各种计算机病毒和黑客（Hackers）对网络的攻击越来越激烈，许多企业遭受破坏的事例不胜枚举。

目前网络存在的漏洞：

l 现有网络系统具有内在安全的脆弱性。

l 对网络的管理思想麻痹，没有重视黑客攻击所造成的严重后果，没有投入必要的人力、财力、物力来加强网络安全性。

l 没有采取正确的安全策略和安全机制。

l 缺乏先进的网络安全技术、工具、手段和产品。

l 缺乏先进的系统恢复、备份技术和工具。

网络攻击

这个领域主要是对网络基础设施的攻击为主(例如，有线、无线、语音、远程接入等)。网络攻击的例子包括:

通过发动"拒绝服务"(DoS)攻击，破坏公司的网络，是网络的合法用户无法正常接入网络。

侵入使用宽带互联网连接的"永远在线"远程工作台位 (例如，通过"后门"入侵)，暴露公司的 IP，使其面临受到进一步攻击的风险。

在网络上插入一个未经授权的设备，并将其伪装成网络上的一个合法设备。

在公共 Web 服务器和电子商务服务器上发动入侵攻击。
精心策划并发动病毒攻击，破坏数据和应用。
数据攻击
攻击对在网络上传输的数据 (专用 IP、客户记录、员工信息等)、存储在数据服务器上的数据以及在网络上进行存取的各项应用 (电子邮件、Web、ERP、CRM 等)。数据攻击的例子包括:

有意破坏在网络上传输的信息，或者无意中窃取以有线或者无线的方式在网络上传输的口令以及其他保密信息。
窃取硬件并访问内嵌在设备上的(如设备 MAC 地址等)或者存储在设备的硬盘上的保密信息。
用户攻击 攻击对访问网络的用户(IT、终端用户、远程用户等)、用户设备(笔记本电脑、台式电脑等)。用户攻击的例子包括:

盗窃合法网络用户的身份，获取对网络上的保密信息和受保护的资源的访问权。
在用户的设备上发动 DoS 攻击，导致其中断和过载，使用户无法正常运行 。

第二部分 网络安全策略

明确安全防范的重点和对象：

I. 防外，防止外部的非法访问，防止黑客的入侵，保证整个企业内部网络的安全，保证企业的网络通信的畅通。

II. 防内，公司内部可能有一些员工对公司有不满情绪，对企业的网络直接发起攻击，因为他们的计算机直接在企业防火墙的内部，对企业网络内部发起攻击会比外部的黑客入侵有更大的危险性，防火墙无法了解和阻断这些攻击，因此内部网络安全的防范必须给予高度的重视。

III. 重点部门的防范，企业内部一些重点部门（如财务部）由于这些部门存放有公司的一些重要资料，因此必须重点保护。

病毒防治方案：

1. 安装防护工具

安装防毒软件来防范你的电脑被病毒入侵.建议全部机器采用我公司推荐病毒防火墙软件 MCAFEE，病毒库更新快速，覆盖面广。

2. 定期扫描电脑病毒

最少每星期进行一次电脑病毒扫描,而设定扫描时间最好在非繁忙工作时间,例如:放假时间,或午饭时间.

紧记要选择[扫描所有固定磁盘]（以 MCAFEE 为例）.不要只选择性地扫描应用文件,因为很多流行的电脑病毒和蠕虫会依附在.EML,.VBS.和.SHS 等文件上.

3. 限制员工的存取权限

尽量不要让其他人使用你的电脑系统,因为他们有可能引入有恶意的软件或病毒,感染你的电脑系统.如果必需和他人共用你的电脑系统,你也必须限制第三者对资料夹或硬盘的存取权限.

避免使用共享文件夹(shared folder),若真有此必要,则在共享文件夹设定使用者的名称和密码,这样可限制已被感染的电脑透过共享文件夹感染你的电脑系统.

4. 处理电子邮件的附加文档时要特别小心

不要随便打开来历不明的电子邮件附加文件，一些病毒或蠕虫会假装为节日的祝贺或庆祝语.求职信等等,除非你知道这个文件的内容,请不要执行任何附加文件.

不要散播恶作剧电子邮件,恶作剧的电子邮件通常散布虚假的信息,他们通常里连锁信形式散播病毒消息.

5. 检查外来文件,方可使用

软盘,光碟或从 Internet 下载(尤其在不知名的网站下载时)的外来文件，需先用防毒软件检查后才能打开或者使用.

6. 即时安装补丁程序

常用的软件,包括操作系统,浏览器和办公室应用程序.需经常安装补丁程序.

留意最新的补丁程序的资讯,关心微软最新推出的补丁程序.启动’’WINDOWS UPDATE”

7. 过滤一切传播病毒或蠕虫的渠道

电子邮件并非传播病毒的或者蠕虫的唯一渠道，其他传播途径,例如:浏览网站或着文件传送(FTP)亦要建立过滤机制阻截病毒或蠕虫.

8. 为系统及资料备份还原做好准备

预先准备一套或以上的还原光盘,并放置在不同而安全的地方,这套备份光盘能帮助你的电脑重新启动及可清除在硬盘上的病毒（先市面上大部分系统安装盘带有 DOS 杀毒工具）,此外,准备一套防毒软件的应急盘,可以用还原时做清除病毒.

将硬盘上的资料(重要数据)备份于另一个硬件,最好一个月替换一次最新的资料.例如:光盘或者服务器上,切勿存放在同一个系统上,就算电脑系统被完全破坏,也有办法恢复你的数据.

9. 其他保护方法

确定你的服务器和个人电脑不会从软驱或光驱启动(BOOT UP),更改 BIOS 或者 CMOS 的启动设置为从硬盘启动,这样可以有效的防范引导区类型的病毒.

安装防火墙(firewall),利用放火墙来防范病毒入侵.在没有硬件放火墙的前提下,设定防火墙的对外访问通信的限制,一般防火墙只限制了进入信息的设定.这样才能阻止木马程序的建立对外通信而导致数据丢失.

10．网络知识的培训

通过我们对员工进行基本的网络知识培训，让员工了解网络中常见的使用操作。

典型网络安全拓扑图：

采用这样的网络结构，有益于对服务器与客户机进行集中管理，接入 INTERNET，首先由防火墙过滤掉错误或数据包，在防火墙上进行正确的配置

日常维护须知：

不接入 INTERNET 下，所有机器的系统要 GHOST 备份；

升级最新病毒库；

设置 BIOS 登录密码，防止对系统配置有意无意的修改；

定期磁盘碎片整理；

更新系统补丁、各软件补丁，减少安全隐患；

时常备份重要数据（如有条件可用双硬盘＋RAID 1 做到万无一失）；

关闭不必要的服务，提高系统安全性与运行速度；

关闭默认共享；

不要随意共享整个盘符

如有条件可将重要资料刻录成光盘保存；

将“我的文档”指向除 C 盘外其他地方

尽可能少安装不必要软件，造成系统臃肿，运行缓慢；

使用 U 盘传递资料，需将其置于写保护状态，以防止它受到病毒感染；

对需使用的光盘或其他移动存储设备，先杀毒，后使用，做到安全预防；

接入 INTERNET 情况下，需使用代理服务器软件严格控制一切网络活动，网络防火墙与杀毒软件配合使用，切实更新至最新病毒库，以预防为主。各工作站不能随意打开不明邮件，更不能随意打开附件；下班后，关闭 INTERNET 连接。对重要文件进行备份。关闭默认共享，在系统登录帐号上，要尽量做到吝啬，只分配所需要之权限。不要在不可靠的渠道下载任何软件。如需使用 QQ，在朋友发来的信息有些奇怪时，应反覆确认。

最后，加强对员工的基础知识的培训，切实提高员工的个人安全意识非常重要，据以往经验

来看，往往一个员工看似合理的操作却带来很大的危害（例如，随意打开邮件附件、打开恶意病毒网页），人人多了解些日常安全知识，都能够给企业网络的正常运行添上重要的稳定性。

因此，我们的方案能更好的为贵公司的网络进行规划和管理，确保贵公司网络数据安全与更好的使用网络资源。