【摘 要】病毒、黑客攻击以及计算机威胁事件已成为我们日常生活的一部分。不仅是计算机的家庭用户会受到以上威胁，各种规模的企业也承受着各种各样的网络攻击风险。本文从内外两方面论述了威胁网络安全的因素。   
中国论文网 /8/view-1702018.htm  
　　【关键词】网络安全；威胁；因素   
　　 病毒、黑客攻击以及计算机威胁事件已成为我们日常生活的一部分。恶意程序通过互联网进行扩散、黑客窃取机密资料、垃圾邮件如洪水般灌入邮箱，这些就是我们在计算机带来方便的同时付出的代价。任何未受保护的计算机或网络都是脆弱的。   
　　家庭用户可能在无意中点击某个网站链接后，一些有价值的个人资料也随之流失；小朋友在交换游戏软件的同时也完成了病毒的传递；你接到一封需要升级信用卡的邮件通知，随后按着提示步骤完成升级，其实你是将银行账户资料拱手交给了背后的黑客；后门程序被安装在你的计算机中，你无意中已经成为传递垃圾邮件的帮凶。   
　　 １．威胁网络安全的主要因素   
　　计算机网络安全受到的威胁包括：   
　　1.1“黑客”的攻击   
　　1.1.1获取口令   
　　这种方式有三种方法：一是缺省的登录界面攻击法。二是通过网络监听，非法得到用户口令，这类方法有一定的局限性，但危害性极大。三是在知道用户的账号后利用一些专门软件强行破解用户口令，这种方法不受网段限制，但黑客要有足够的耐心和时间。   
　　1.1.2特洛伊木马攻击   
　　“特洛伊木马”技术是黑客常用的攻击手段。它通过在你的电脑系统中隐藏一个会在Windows 启动时运行的程序，采用服务器/客户机的运行方式，从而达到在上网时控制你电脑的目的，很多用户稍不注意就可能在不知不觉中遗失重要信息。   
　　1.1.3诱入法   
　　黑客编写一些看起来“合法”的程序，上传到一些FTP 站点或是提供给某些个人主页，诱导用户下载。当一个用户下载软件时，黑客的软件一起下载到用户的机器上。该软件会跟踪用户的电脑操作，它静静地记录着用户输入的每个口令，然后把它们发送给黑客指定的Internet 信箱。   
　　1.1.4寻找系统漏洞   
　　许多系统都有这样那样的安全漏洞，其中某些是操作系统或应用软件本身具有的，这些漏洞在补丁未被开发出来之前一般很难防御黑客的破坏。还有就是，有些程序员设计一些功能复杂的程序时，一般采用模块化的程序设计思想，将整个项目分割为多个功能模块，分别进行设计、调试，这时的后门就是一个模块的秘密入口。在程序开发阶段，后门便于测试、更改和增强模块功能。正常情况下，完成设计之后需要去掉各个模块的后门，不过有时由于疏忽或者其他原因（如将其留在程序中，便于日后访问、测试或维护）后门没有去掉，一些别有用心的人会利用专门的扫描工具发现并利用这些后门，然后进入系统并发动攻击。   
　　1.2计算机病毒   
　　计算机病毒是一个程序，一段可执行代码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。近年出现的红色代码、尼姆达、求职信、感染JPEG 图像文件的W32.Perrun等病毒，表明计算机病毒的传播是不断快速发展、变化的，其传播范围更加广泛，病毒编写技术越来越复杂，给单机及网络用户带来严重破坏，这也是网络病毒防御所面临的现状。病毒发展特征表现有：   
　　1.2.1计算机病毒涉及的领域越来越广泛   
　　网络的普及和网络技术的发展，将病毒制作者和黑客从传统意义上的两个独立的群体，合二为一，他们攻击系统漏洞，利用漏洞进行病毒传播，驻留后门及特洛伊木马程序，造成系统瘫痪、网络堵塞。   
　　1.2.2向混合型病毒方向发展   
　　病毒体可能是由一组或多个文件组成的，病毒感染系统后，在系统内有多种变形，增加了病毒清理的难度。   
　　1.2.3攻击反病毒软件的病毒有增无减   
　　近年攻击反病毒软件的病毒也越来越多，Win32.Yaha.C 是一个典型的攻击反病毒软件的病毒，KLEZ.H、中国黑客等病毒开始监控自己的进程，一发现自己的进程被杀，就立即杀掉对方或重新启动进程。   
　　1.2.4电子邮件病毒感染不断攀升   
　　现在的带毒邮件都有很吸引人的主题，或者带有色情图片，如求职信、送密码、MYLIFE 等病毒，很容易使人上当，用户一旦点击即受到感染。   
　　1.3拒绝服务攻击   
　　拒绝服务攻击即攻击者想办法让目标机器停止提供服务或资源访问，是黑客常用的攻击手段之一。这些资源包括磁盘空间、内存、进程甚至网络带宽，从而阻止正常用户的访问。其实对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。拒绝服务攻击问题也一直得不到合理的解决，究其原因是因为这是由于网络协议本身的安全缺陷造成的，从而拒绝服务攻击也成为了攻击者的终极手法。   
　　 2.威胁网络安全的其他因素   
　　此外，威胁网络安全的因素还包括以下几个方面：   
　　2.1操作系统的脆弱性   
　　(1)操作系统支持的程序动态连接与数据动态交换是现代系统集成和系统扩展的必备功能，而动态连接、I/O 程序与系统服务、打补丁升级可被黑客利用，滋生病毒。   
　　(2)操作系统可以创建进程，即使在网络的节点上同样也可以进行远程进程的创建与激活，且该进程有继续创建进程的权力，加上操作系统支持在网络上传输文件，在网络上能加载程序，二者结合起来就可以在远端服务器上安装“间谍”软件，常以打补丁的方式“打”人合法用户(尤其是齐特权用户)以躲避监测。   
　　(3)守护进程具有操作系统核心层软件同等权力，会被黑客利用。   
　　(4)网络操作系统提供的远程过程调用服务以及它所安排的无口令人口也是黑客的通道。   
　　2.2计算机系统的脆弱性   
　　(1)主要来自操作系统的不安全性，在网络环境下，还来源于通信协议的不安全性。   
　　(2)存在超级用户，如果入侵者得到了超级用户口令，整个系统将完全受控于入侵者。   
　　(3)计算机可能会因硬件或软件故障而停止运转，或被入侵者利用并造成损失。硬盘故障、电源故障和芯片主板故障都是人们应考虑的硬件故障问题，软件故障则可出现在操作系统中，也可能出现在应用软件当中。   
　　2.3协议安全的脆弱性   
　　TCP/IP 协议以及FTP、E-MAIL、NFS 等都包含着许多影响网络安全的因素，存在许多漏洞。   
　　2.4数据库管理系统安全的脆弱性   
　　由于数据管理系统(DBMS)对数据库的管理是建立在分级管理的概念上的，因此DBMS 的安全也可想而知。另外，DBMS 的安全必须与操作系统的安全配套，这无疑是一个先天的不足。   
　　2.5人为的因素   
　　不管是什么样的网络系统都离不开人的管理，但大多数网络系统缺少安全管理员，特别是高素质的网络管理员。此外，缺少网络安全管理的技术规范，缺少定期的安全测试与检查，更缺少安全监控。令人担忧的是许多网络系统已使用多年，但网络管理员与用户的注册、口令等还是处于默认状态。   
　　 3.结论   
　　不仅是计算机的家庭用户会受到以上威胁，各种规模的企业也承受着各种各样的网络攻击风险。关键数据被病毒破坏、财务资料被非法窃取、大量垃圾邮件极大地消耗了人力和技术资源等等，这些问题都昭示着，有效的风险管理体系对于企业的成功运作是至关重要的。 