计算机信息安全技术及防护

岳滕飞 刘舰维

南阳农业职业学院，河南 南阳 473000

【摘 要】：随着社会的不断发展，科学技术也在不断创新，作为走在科技前沿的计算机技术一直处于飞速增长阶段，网络逐渐走进千家万户，成为人们日常生活中不可缺少的使用工具，给人们的工作和生活都提供了便利，网络的普及率也越来越高，并在近几年屡创新高。但是我们在享受着互联网给我们带来的便利的同时，也面临着巨大的信息安全隐患，计算机被黑客攻击、恶意软件威胁、信息泄露等事件层出不穷，网络信息安全防护是当前最严峻的挑战。本文将对计算机安全技术以及防护进行分析，以期维护计算机的信息安全。

【关键词】：计算机；信息安全技术；信息安全防护

随着计算机技术的快速发展，用户逐渐拥有大量的移动设备，这些移动设备成为用户储存信息的工具，这些信息往往都是个人隐私，对用户来说非常重要，同时也可能其它不法分子所觊觎的信息。由于网络信息具有开放性和复杂性等特点，于是很多不法分子为盗取他人信息，利用网络安全漏洞，通过泄露他人信息获取一定的利益，造成企业或个人的经济损失。因此必须不断创新网络信息安全防护技术，完善信息安全保护体系，在网络飞速发展的前提下，加强对网络的安全防护，保证用户的个人信息安全，减少不必要的经济损失，不再让不法分子有可乘之机。

1 计算机安全技术的重要性

计算机安全技术是集数据恢复技术、密码应用技术和信息等多种技术综合应用技术，此技术主要是根据网络病毒以及病毒攻击的基本原理，利用杀毒软件提高计算机的信息安全性，避免黑客攻击，从而实现计算机的安全防护。为保证计算机网络的正常运转，让用户能够顺利进行过网上支付或者数据传递，并减少其它的影响因素，当前比较基础的网络安全防范技术，就是设置支付密码，可有效保护用户信息安全，但是在遭到黑客攻击后，计算机防护系统就会崩溃，从而影响计算机的正常运行，这对计算机的损害相对较大。因此，想要在用户信息共享的前提下，保证信息的安全，需要不断更新信息安全技术，使信息安全技术能够紧跟计算机的发展步伐，不断与时俱进，成为计算机强有力的安全保障系统，实现信息的安全共享，减少黑客入侵的几率[1]。

2 计算机安全防护存在的问题

2.1 硬件和自然环境

随着计算机的快速发展，大型企业的信息越来越多，传统的信息存储方式已经无法支持强大的企业信息系统。于是很多企业会选择采用硬盘储存数据，但是硬盘本身没有任何防护措施，基本任何计算机都可访问，使得计算机信息安全无法得到保证。其次就是自然因素，计算机在运行的过程中是不能处于较高的环境下的，因为这样容易引发安全事故。一旦出现安全事故，数据必然会有所损害，无法实现信息的安全保护。

2.2 黑客的恶意攻击

黑客的恶意攻击是当前信息安全的主要威胁，根据攻击手段的不同，主要分为非破坏性攻击和破坏性攻击两种。非恶意对信息的破坏程度相对较小，不会泄露个人信息和资料，只是通过然乱系统正常的运行的方式，采取信息炸弹或者拒绝服务攻击手段，使网络服务器无法正常服务，即隔离用户使用的计算机，把宽带堵死，服务器会因此占据大量内存和 CPU，导致电脑延迟访问或者没有办法正常访问[2]。

恶意的黑客攻击指的是黑客通过非法手段在用户计算机系统内植入木马或者垃圾邮件。植入木马具体操作方式是利用植入在用户计算机内的木马，对用户信息进行非法控制，从而窃取计算用户的资料或者随意更改信息。植入垃圾邮件是另一种恶意攻击方式，主要通过向用户发送垃圾电子邮件的方式，如果用户不小心打开该邮件，黑客就会对该用户的计算机进行操控，进一步破坏或者窃取信息。

2.3 病毒入侵

病毒是当前对计算机安全造成最大影响的因素之一，其传播途径非常广，还无法实现有效预防。计算机病毒就像流感一样，把本身携带的病毒复制在用户计算机上，一旦用户编辑文档或文件，就会感染病毒，使计算机网络受到巨大伤害，直接或间接造成个人或企业的财产损失，严重者还可能导致国家安全受到威胁，成为社会动荡的因素。计算机病毒的传播途径主要有两种，其一是黑客给与计算机指令，让其自动产生可复制的代码，黑客即可获得电脑的操控权，从而破坏计算机储存的文件或者或者让计算的部分功能丧失，会严重威胁用户计算机的机卡和 CPU 的应用，从而给用户的利益带来严重损害。其二是黑客利用后门程序、木马程序等方式攻击用户计算机缓冲区溢出的程序，获得超级用户权限，实现对计算的绝对掌控，此病毒可能会使计算机的整个网络瘫痪、系统自动崩溃，严重影响计算机的网络安全，危害性极大[3]。

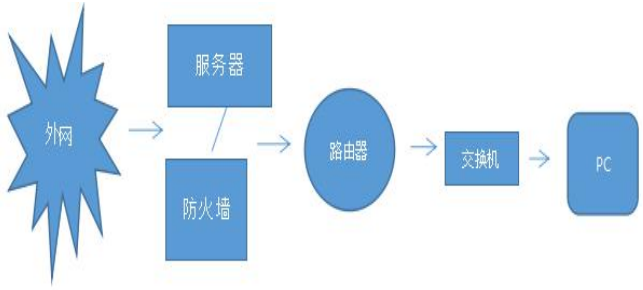
3 计算机的安全防护技术

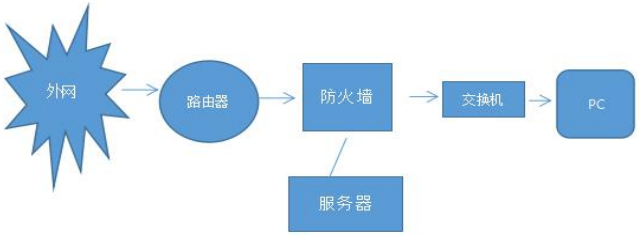
3.1 加强对计算机病毒的防范

计算机病毒种类繁多而且相对复杂，来源甚广，为实现病毒的有效控制，病毒防护软件开发公司建立了相对完整的典型病毒数据库，分析每个病毒文件的特征，并以此作为依据，安装相对专业的病毒防护软件，可以实现对病毒的防范。通过建立计算机网络防火墙等方式，对计算机系统进行权限设置，遵循白名单策略，将计算机系统设置成授权程度访问，减少不明访问的出现几率。同时也可以利用扫描和识别的方式对计算机系统文件进行安全检测，一旦发现病毒，及时删除。同时计算机安全维护人员应对流行计算机病毒有所了解，并制定相应的预防措施，建立健全计算机安全系统，加强对计算机的安全防护。

3.2 设置防火墙

防火墙技术能够保障用户的计算机安全运行，实现计算机网络的安全维护。防火墙优势是在用户的计算机设置一个网管，对信息进行筛选和过滤，从而实现对计算机软件和硬件的控制，保证信息的安全传递，让计算机能够安全运行，从而减少外部不明系统的入侵。此外，防火墙计算机还可以掌握多个通信行为，通过不断升级的黑客防范技术，全面了解整体网络的运行状况，更好的防范不法分子，从根本上保护计算机内部网络环境的安全。





例如：图中所示，只允许 192.168.1.103 访问所有外网的 IP 地址，禁止端口和外网 Ip 的通信，开启 IP 地址过滤功能，限制内网访问外网的 IP 地址，利用缺省过滤规则，过滤不符合的 IP 地址和数据包。

3.3 利用加密技术

数据加密技术的应用范围是保护用户存储的数据和传输的数据，主要方式是重新组织需要传输的数据，并对数据进行变化和置换，经由用户传输的数据会形成密文，只有合法授权者才能获取数据信息，其他人无法通过任何方式获知数据，即使侥幸被不法分子所获取，其数据信息也是密文，无法使用，从而提高信息的安全性。因此，相关企业必须要不断创新加密手段，钻研出最先进的加密技术，减少信息泄露的发生几率，如果发现病毒和黑客入侵，立即利用先进的加密手段进行安全防护，尽可能的减少用户损失。

结束语：

随着计算机的普及，计算机成为用户不可缺少的工具，成为人们储存数据和信息的主要渠道，但是随着计算机信息的开放和共享，很多不法分子，利用计算机的安全漏洞对用户计算机数据和信息进行窃取，给企业和个人造成了严重损失，因此相关企业必须不断更新信息安全防护技术，利用防火墙、数据加密等技术对计算机进行安全防护，让不法分子无法通过非法手段获取用户信息，或者对数据进行加密，即使黑客通过攻击用户电脑获取文件，信息也以被转换，从而真正实现信息的安全防护。

参考文献：

[1] 杨熹.计算机信息安全技术及防护[J].电子技术与软件工程，2019(17):194-195.

[2] 侯日森.计算机信息安全技术及防护分析[J].网络安全技术与应用，2019(05):3-5.

[3] 李艾国.计算机网络信息安全及防护技术[J].电子技术与软件工程，2019(09):211.