大数据时代计算机网络安全及防范措施

向　军
中共四川省巴中市恩阳区委保密机要局　四川巴中　636064

摘　要：伴随我国网络化信息技术的不断发展，计算机网络安全问题发生率也越来越高。一旦计算机出现网络安全问题将直接影响人们正常的生活和生产。因此计算机使用者需要具备较强的网络安全管理意识，采取有效的措施防范计算机网络安全问题，降低计算机网络安全问题发生率。

关键词：计算机；网络安全；问题；防范措施

Computer network security and precautions in the era of big Data

Jun Xiang
Security Bureau, Enyang District Committee, Bazhong Province, Sichuan Province, Bazhong 636064

Abstract: With the continuous development of network information technology in China, the incidence of computer network security problems is also getting higher and higher. Once the computer appears network security problems will directly affect people's normal life and production. Therefore, computer users need to have a strong awareness of network security management, take effective measures to prevent computer network security problems, and reduce the incidence of computer network security problems.

Keywords: computer; network security; problems; precautions

1　计算机网络安全的概述

（1）具有较强的保密性

网络大环境中用户的个人信息能得到有效的安全保证；

（2）数据信息传播速度更快

网络上的数据信息传播不受时间和地域的干扰，可以在最短时间内扩大信息传播范围。正是基于以上特点才更需要加强对计算机网络安全的有效管理，提高计算机网络系统的安全性和稳定性[1]。

2　计算机网络安全面临的问题

2.1 计算机病毒的侵袭

通常计算机病毒潜伏在计算机的程序内，不法分子可以通过编写病毒程序，对计算机和网络系统安全造成严重的影响和破坏。一旦病毒入侵，计算机系统中的信息和相关程序很容易遭到恶意的盗取、破坏和复制，严重时还会造成严重的系统崩溃。计算机病毒具有很强的隐蔽性、传染性和寄生性，通常会通过局域网共享以及网络媒介进行传播，很难对其进行彻底的清除。

2.2 计算机网络漏洞的威胁

微软软件是目前计算机用户使用最多的计算机系统。但是如今市面上盗版的微软软件层出不穷，使计算机网络面临诸多的漏洞，极大威胁了网络的安全性。在开放性的网络环境下，用户若存在不规范浏览网页的行为，容易促使病毒置入计算机内部，对内部系统进行攻击，产生较多的计算机漏洞，威胁整个网络系统的安全性[2]。

2.3 计算机用户的违规操作

计算机用户的违规操作也是引发计算机网络安全问题的重要原因。据调查我国多数的计算机用户数据安全意识较差，不具备专业的计算机操作知识，缺乏对计算机安全防护理论和防护技术的了解，导致计算机操作中存在随意浏览网页、评论、点赞、转发信息等行为。若用户一旦浏览含有病毒的网页，将为网络病毒的入侵打开大门，产生较大的计算机网络安全问题。

作者简介：向军，男，1982年，汉族，四川省巴中市人，大学本科，统计师，四川文理学院，档案专业馆员。

2.4 间谍软件和垃圾邮件的威胁

计算机网络具有较强的开放性，很多数据信息都是互通的，这为非法人员入侵创造了条件。一些非法人员会借助垃圾邮件传递网络病毒。计算机用户不经意就会授权使用，一旦打开这些垃圾邮件里面的病毒将入侵整个计算机网络，此时非法人员会窃取或者篡改重要数据，盗取用户个人隐私对计算机网络系统带来严重影响[3]。

2.5 网络黑客攻击

网络黑客是指攻击者通过网络对用户的网络进行非法访问、破坏，黑客可以偷窥别人的隐私，也可以对用户的信息进行篡改或者破坏等多方面的内容，因此黑客动机的不确定性对用户的利益安全有着重要的影响。若黑客只是好奇而窥探用户的隐私，不破坏用户的网络系统，虽对其危害较小，但也是对用户造成了一定的危害。若是黑客有不轨的目的对用户的网络系统进行破坏的话，后果不堪设想。比如有的黑客会对用户的目标网页和内容进行攻击，这样的操作能够导致网络的瘫痪，让用户无法正常使用，对自身利益也有很大威胁；有的黑客带有不良的情绪，比如恶意的攻击和破坏的心理，对用户的计算机中重要的数据信息进行篡改、毁坏，严重时可能会对国防、军事、经济、政治等国家机密情报造成威胁，让国家的安全处于众矢之的[4]。

2.6 计算机硬件设施故障

计算机硬件设置故障也会引起相应的网络安全问题。工作人员若不定期维护和保养计算机硬件设置，一旦部分硬件设施出现故障将干扰整个网络系统的正常运行，不仅降低计算机运行速度，也会使一些重要信息显示不全。

3 计算机网络安全的防范措施

3.1 增强计算机网络安全防范意识

计算机使用者在使用完计算机后，要及时清除计算机中的私密信息，对计算机中的信息进行加密处理，防止个人的信息在公用的计算机上遭到泄露。个人的身份证信息、照片、家庭地址等不能随意地在网络上暴露，以防止给自己带来不便。另个人在上网时，若遇到了可能存在问题的网站，则不要随意地点击，以防止给计算机系统带来病毒。在使用计算机时应安装防火墙，定期对系统中的漏洞和补丁等进行查杀，减少计算机病毒和漏洞等对计算机安全带来的影响[1]。

政府部门和企业在防范计算机网络安全问题时，应带来培养计算机网络安全方面的人才，并联合高校等建立人才培养机制，研发高效的网络安全防护方法，以减少黑客、病毒对等对计算机网络带来的威胁。特别是重点单位、企业的计算机中含有大量的重要信息和文件，在使用计算机时应增强网络安全防护意识，并采取有效地防护措施，减少病毒等对计算机系统构成的威胁。

3.2 安装计算机安全防护软件

安装安全防护软件是确保计算机网络安全的有效措施，可极大提高计算机网络系统的安全性。安全防护软件可以有效防止病毒对计算机网络系统的如前。一旦网络病毒入侵计算机系统，安全防护软件的功能会快速启动，过滤并拦截网络病毒，实现对整个计算机网络环境的实时性健康和保护。安全防护软件可以监管并把控计算机网络系统中的病毒信息，一旦网络病毒恶意更改计算机系统内数据资料时，安全防护软件会在第一时间弹出，提醒用户注意查杀计算机网络病毒，以此确保计算机网络数据信息的安全性[2]。

3.3 及时安装漏洞补丁

伴随我国现代化科学技术的不断发展，计算机硬件设置也越发完善。

软件类型和功能也越发齐全，计算机会时常出现安装补丁和系统更新的提示。若计算机用户忽视这些更新提示，难以及时安装补丁和更新系统，容易促使计算机网络出现相应的漏洞。针对此种问题，计算机用户可以在官网上下载相应的病毒查杀软件和安全防护软件，其中瑞星杀毒和360安全卫士就是最常见的病毒查杀软件和安全防护软件，此种类型的软件可最大程度确保计算机系统的安全性。

3.4 定期备份电脑重要文件

计算机用户要养成定期备份电脑文件的习惯，尤其是重要的文件资料计算机用户要定期内粉存储。黑客和计算机病毒攻击带有较强的随机性，它们的攻击方式、攻击时间等都具有不确定性，对计算机网络系统来说是最大的安全威胁。计算机用户养成定期备份计算机重要文件的习惯，最大程度避免重要信息不被泄露出去，对于维护计算机网络系统的安全与稳定意义重大[3]。计算机用户将重要的文件备份到其他硬盘装置中保存下来，这样即便计算机网络受到了恶意攻击也不会出现重要数据丢失的问题，能有效确保用户数据信息的安全性。

3.5 使用数据加密技术

该技术可以对计算机网络中存在的数据信息进行加密处理，最大程度避免计算机网络数据信息被窃取、篡改的问题，确保了计算机网络数据信息传输过程中的安全性。数据加密技术包括多种类型，比如明文数据加密技术、密文数据加密技术、密钥数据加密技术、加密算

法技术等。其中数据加密技术最重要最关键的技术就是密钥加密技术，该技术可确保计算机网络数据信息的安全性和私密性，有效杜绝了非法人员和恶意软件对数据信息的篡改和窃取，极大保护第三方使用者的合法利益。数据签名技术作为数据加密技术之一，可确保互联网信息传输的安全性。数据签名技术可有效避免外部力量窃取网络数据信息。数据传输的各个阶段都可以应用数字签名技术，用户使用安全密码可以保护重要计算机网络数据信息，确保数据信息在整个计算机网络传输过程中的安全性，维护用户合法权益[4]。

3.6 加强网络系统监控

在网络系统运作的过程中，各种非法入侵的现象时有发生，若不及时发现，则会对网络系统的安全埋下隐患，并造成难以估量的损失。

为对计算机网络在的一些安全风险进行有效方法，网络系统的监控必不可少。入侵检测属于综合防护技术，通过对网络通信的分析监控系统运行状况的实时监控，及时发现网络系统在发生的非法入侵现象。在网络系统的监管过程中，会通过对签名和统计进行分析，通过对网络系统的漏洞的监管以及对网络系统运行状态进行统计分析，以更加有效的处理潜在的安全问题，为网络安全提供保障。

3.7 加强对计算机硬件设施的维护

工作人员要定期加强对计算机硬件设置的维护和保养，以免线路故障和部件损坏阻碍主机的正常运行，提高计算机网络的安全性和稳定性。计算机用户要避免外界环境对网络的干扰，避免计算机处在潮湿环境和静电环境下，以免外界因素干扰计算机网络的安全运行[1]。

3.8 网络防火墙的设置

对网络防火墙进行有效应用，可以对来自外界的恶意攻击进行有效的防护，也可以对企业内部用户的访问存在安全隐患的网站进行约束。若企业内部的计算机系统与互联网进行连接，网络安全问题不仅需要对病毒进行有效的抵御，也应对系统漏洞进行预防。此外，要重视对黑客的防范工作，凭借网络防火墙能够对外部网络的恶意入侵采取严密的防范措施。在此基础之上，需要对企业内部的网络进行合理的划分，最大程度的消除安全问题对于企业内部网络所造成的影响。防火墙的设置可以对网络信息传输和读取的过程进行严密的监测与审核，并对所有的访问记录进行详细的记录，在此基础之上生成相应的访问日志，从而可以为后续的网络安全维护工作提供有力的参考。一旦出现网络安全问题，防火墙能够在第一时间发出警报，同时也可以提供问题的类型以及相关的处理意见[2]。

4 结语

目前，计算机网络系统中主要存在系统漏洞、电脑病毒和信息泄露等问题，这些对于系统的稳定性和数据信息的安全性造成了威胁。因此，为进一步提高计算机网络的安全性，需要增强用户的安全防范意识，并引入安全防护技术，加强对网络系统的监控，从而有效保障网络系统的安全性和稳定性。

参考文献：

[1]王薇.计算机网络安全问题及其防范措施分析[J].无线互联科技，2021，18（3）：37-38.

[2]张鹰.计算机网络安全问题及其防范措施[J].精品，2021（4）：246.

[3]阎培儒.计算机网络安全问题和防范措施初探[J].中国宽带，2021（2）：17.

[4]李尊.计算机网络安全问题及其防范措施分析[J].无线互联科技，2021，18（6）：28-29.