计算机网络安全的主要隐患及管理策略

李叶欣

（广西科技大学　545006）

摘要：计算机网络主要是指在不同的位置以及通信线路实现相互连接外部性设备。其中，计算机系统能够充分地实现资源共享以及信息传输。随着我国计算机网络的发展和完善，已经为广大人民群众的日常生活以及工作带来了诸多的便利，但是，网络是一把双刃剑，也给人们的生活以及工作带来了安全风险。所以，这就需要对计算机网络安全问题引起重视，并同时采取管理措施，从而切实地保障计算机网络的可靠性以及安全性等。本文主要研究了计算机网络当中主要安全隐患以及提出管理措施，以供相关管理人员进行参考和借鉴。

关键词：计算机网络安全；主要隐患；管理策略

在当前的时代背景下，计算机网络日益发展和成熟起来，同时，计算机网络已被广泛应用于工作以及生活诸多领域。但是如今还是有部分人员会依照计算机网络当中的漏洞去攻击用户计算机，从而导致大量信息以及数据被泄露和篡改。这就会导致用户蒙受重大的经济财产损失，所以，需要针对计算机网络当中的安全隐患以及安全风险进行深入的研究，还需要采取管理措施降低计算机网络风险系数，从而切实地保障我国的计算机网络安全性以及可靠性增强。

一、计算机网络中存在的主要安全问题

随着我国社会经济以及科学技术的日益发展，计算机网络技术得到快速发展，但是，实际上，在计算机网络当中还是存在大量的安全隐患问题，值得引起高度重视，其中，主要的安全问题包括计算机漏洞、病毒、黑客以及网络欺诈现象等等[1]。

（一）网络漏洞

由于没有实现对计算机硬件以及软件的有效管理，导致计算机网络中可能出现漏洞，为不法网络分子通过网络来对计算机用户实施非法攻击或者入侵活动提供了机会。网络用户的安全意识是影响计算机网络安全性的一项重要因素，会影响其安全保护系统的使用效果，可能因网络长时间得不到修复而导致其被攻击或者是被病毒所感染[2]。

（二）网络病毒

网络病毒，实质上就是一个虚拟的计算机程序。在计算机网络中，不法网络分子为了达到自己的目的，经常使用网络病毒来攻击用户的计算机系统，在入侵成功之后，获取用户的隐私以及其他数据等[3]。这些网络病毒的主要特点有两个，隐藏性和依赖性。虽然目前市场上存在不少杀毒软件，但是仍然无法完全的消灭网络病毒。

（三）网络黑客

网络黑客是严重威胁计算机网络安全的因素之一，其采用的攻击方式就是借助技术手段来入侵用户的计算机系统，然后窃取用户的个人隐私信息以及重要文件等。比如，黑客可以借助相应的设备来破解计算机用户的个人账户，获取密码，然后进行一系列的非法操作，像删除用户的重要数据、转移用户的财产等。如果用户没有做好相关的安全工作，可能会导致计算机因黑客攻击而瘫痪，无法正常操作[4]。

（四）网络欺诈

计算机网络具备虚拟性、开放性以及自由性的特点，各种虚拟网络工具，比如微信、QQ、微博和其他的社交软件，以及网站等都可能成为犯罪分子实施欺诈行为的地方。这些罪犯通过建立虚假网络，并在其中发布虚假信息或者进行其他的欺诈活动，以此来诱骗计算机用户，获取不法收益。

二、加强计算机网络安全管理的主要措施

为了促使计算机网络安全得到科学以及合理的控制，这就需要相关管理人员能够采取必要的措施，其中，主要措施包括了有效的运用防火墙、安装更新杀毒软件、全面设置访问权限以及构建完善应急方案等等。

（一）有效的运用防火墙

防火墙作为安全屏障，可以将计算机系统的内外结构分离开来，其在计算机网路中的运用可以实现对计算机系统中所储存的各类数据信息以及资料等的全面保护。通过对防火墙的有效运用，可以对网络连接期间过滤和处理各类信息等，推动计算机程序相关防护工作的开展，能够及时的发现计算机运行中出现的问题，从而采取有效的处理措施，发出警告信息并进行拦截，确保计算机系统的安全。与此同时，计算机用户应当及时全面的更新防火墙，且在防火墙提出安全警告时，及时采取措施，对其进行合理处理，有效解决网络存在的问题。

（二）安装更新杀毒软件

在对计算机网络实行安全管理的过程中，用户或者管理员应当安装并及时更新相关的杀毒软件，确保计算机系统在运行过程中的安全性以及可靠性。由于网络病毒也是在不断更新变化的，使用杀毒软件并不能将其全部消除，因而需要用户依照有关规范以及要求等，合理有效的使用网络杀毒软件，及时对其进行更新优化，确保计算机网络的良好应用效果。

（三）全面设置访问权限

用户在实际使用计算机网络系统的过程中，应当针对访问权限实行全面的设置与管理，从而使计算机系统更加安全可靠。在此过程中，用户应当制定完善的访问机制，通过对访问权限的合理设置与管理来规避网络风险，实现对计算机的有效防护，提升其安全性能。因此，应当加强对计算机用户的相关教育工作，帮助其树立正确的安全意识与观念，设置计算机访问权限，从而尽可能地提高其计算机网络的安全性，促进配置效果的优化和提升，同时实现对计算机系统的全面监管[5]。

（四）构建完善应急方案

在管理计算机网络系统安全性的过程中，应当构建完善的应急方案，避免或减少其在运行期间因安全问题造成的经济损失，最大程度的实现计算机网络系统平稳运行。通过应急方案，能够实现对突发性计算机安全问题的应对和解决，同时也能在构建应急方案的过程中，贯彻落实各项安全管理制度，从而提升计算机网络的安全管理水平。

结语：

综上所述，计算机网络安全状况还是不乐观，存在大量安全风险，包括病毒传播、计算机漏洞以及网络诈骗等。所以，需要建立防火墙，应用杀毒软件以及全面设置访问权限等等。只有这样，才能切实保障计算机网络的安全性以及可靠性。

参考文献：

[1]林森.计算机网络与信息安全的主要隐患及其管理措施[J].科技与创新,2021(12):129-130.

[2]刘金霞.计算机网络与信息安全的主要隐患及其管理[J].电子技术与软件工程,2020(22):232-234.

[3]李昊林.计算机网络安全的主要隐患及管理措施分析[J].计算机产品与流通,2020(03):38.

[4]白萍.校园计算机网络安全的主要隐患及防范与控制[J].无线互联科技,2020,17(04):32-33.

[5]贾涛.计算机网络安全的主要隐患及管理措施分析[J].无线互联科技,2019,16(13):19-20.