计算机网络安全的威胁因素与防范策略

白丽洁
辽源职业技术学院　吉林辽源　136200

摘　要：随着互联网时代的到来，计算机网络安全技术应用越来越广泛。在计算机体系运行过程中加强网络安全技术的影响因素分析，并结合实际对相关的风险及时防控，这样才能更好地保证计算机网络技术有效发挥其应有的功能。本文首先探究了计算机网络安全维护的重要性，并分析了计算机网络安全技术的一些威胁因素，最后针对如何加强计算机网络安全管理提出了具体的防范对策，以供参考。

关键词：计算机网络安全；影响因素；防范策略

引言：

当前，信息时代来临，计算机技术及网络技术已经在社会不同领域广泛应用，其不仅给人们的生活带来了极大的便利，为学习提供了便捷手段，还为企业安全及生产提供了支持。在应用计算机过程中，由于计算机网络利弊共存，所以网络工作人员必须加强信息加密技术及信息保护技术，以奠定网络信息安全的基础，对网络信息安全问题进行解决，本文就计算机网络信息安全的影响因素及防范措施进行论述分析。在“互联网+”的二十一世纪背景下，网络在生活、生产及学习中成为了不可或缺的重要工具，计算机网可被广泛应用于不同行业之中，科学技术的迅猛发展，导致网络环境的复杂程度不断提升，计算机网络安全问题已经成为其应用的最重大难题，为合理利用这一新时代发展的产物，就必须加强计算机网络安全建设，不断推进信息技术的发展，本文就网络信息安全现状出发，对计算机网络信息安全的影响因素进行重点分析，并提出了针对性的防范措施。

一、计算机网络安全维护的重要性

伴随着互联网和信息技术的高速发展，各行各业的人们传播信息的方式都已经离不开网络和计算机。计算机网络逐渐发展成为人们日常生活的必需品，人们对计算机网络的依赖性与日俱增。如高校的网络办公，学生宿舍的网络全覆盖，线上教学等对计算机网络要求越来越高。但是随着计算机网络的迅猛发展，网络安全问题日显突出。网络安全的重要性已成为一个大家都关心的社会问题。如果网络安全得不到保证，轻则会泄露、更改或破坏信息，重则会窃取资产或机密很有可能造成无可挽回的损失。所以保障计算机网络安全的重要性毋庸置疑[1]。

二、计算机网络信息安全威胁因素

1.计算机病毒攻击

计算机病毒其本质上属于计算机指令与计算机程序代码的组合，在程序编制或者插入代码及指令的过程中，计算机数据及计算机功能也会受到一定的影响，对计算机的正常应用产生不利影响。网络黑客，会以窃取计算机中重要信息资料为工作目标，或者以损坏重要信息为工作目的，依靠计算机病毒，对计算机进行目标性的攻击，由于病毒自身具有较强的隐蔽性、传感性、寄生性及触发性特征，其会极大程度对计算机网络信息安全产生不利影响，所以从计算机病毒出发，必须合理采取预防措施，减少计算机数据及程序受到病毒攻击的可能性，降低计算机数据被窃取或者程序丢失的可能性，维系计算机网络运行的正常化，降低网络瘫痪问题的发生概率[2]。

2.网络入侵

电脑网络被黑客利用各种非法获利就是网络入侵。网络入侵的方式也是各种各样：有监听法、特洛伊木马术、口令法、隐藏技术等。黑客主要是攻击信息网络，攻击政府网站、攻击金融机构、攻击国家重点高校（有国家比较重要的科研项目）网站等，黑客活动很频繁，采用非法拦截、破译、篡改、复制等形式进行盗取。因为黑客的存在，计算机网络信息安全会遭受严重威胁，国家安全利益也会受到威胁，给群众财产带来损失。

3.用户安全意识不足

计算机用户的安全防范意识极大程度对网络信息的安全性产生着影响，由于用户缺少对信息安全问题的重视程度，其不能正确认识杀毒软件及防火墙程序，大都认为这类软件会在极大程度上影响计算机运行的流程性能，所以大都选择不安装杀毒软件和防火墙，在此过程

中，若是用户于公共场合之中应用计算机，且用后并未清理个人资料，未对密码进行清理，将直接诱发重要信息资料泄露问题的发生。从总体角度分析，用户安全意识无法提升，属于计算机信息安全受到威胁的最主要因素。

4.运行管理制度不足

在计算机网络信息安全管理过程中，缺少相应的人力资源，因为在计算机网络下对于成本的投入并不多，而且用户的实际需求也各不相同。那么在用户提出更高要求的时候，相应的管理也会发生变化。在这一过程中，就需要相关管理人员能够对其进行管理，一旦缺少专业的管理人员和技术人员，就会影响计算机网络安全。

三、提升计算机网络安全防范的策略

1.运用防火墙技术

在构建网络安全系统的过程中，需要用到防火墙，通过对防火墙的利用，来有效地阻隔不良信息，避免计算机中毒。所以，在完善网络安全系统地过程中，就应该积极地利用防火墙技术，要能够将其和计算机系统有效结合，以此来提高防火墙的安全性能。在防火墙的组成中，网络级和应用级网关是中非常重要的内容，通过对应用级网关的有效应用，能够及时检查计算机传输和接收数据的安全性，并且能在网关的帮助下实施备份，通过这一技术更好地保证服务器与客户的有效联系。与此同时，通过对应用级网关的应用，还能及时地了解计算机的实际需求，并根据具体需求来进行访问[3]。网络防火墙是按照数据端口和具体需求来进行分析，检查信息的接收和传输。

2.加强计算机网络访问权限控制工作

加强计算机网络访问权限控制工作是提高计算机网络信息使用安全性的有效途径。访问权限控制主要指的是通过对计算机网络用户进行严格的身份认证的权限控制达到防止非法用户入手的策略。通过区分不同的身份，为其分配唯一的账号作为统一电子身份标识，让其使用唯一的统一电子身份标识登录网络。加强计算机网络访问权限控制工作是一种最直接最有效的手段，极大地增大了计算机网络安全性。

3.持续加强计算机系统优化

计算机网络安全技术系统自身设计比较复杂，要全面加强计算机系统的优化升级，为此应当结合计算机网络现实发展需要，不断进行技术的共享交流，充分借鉴国内外在计算机网络系统升级管理维护等方面的经验，通过配置加密钥软件等方式实现对用户信息的全面核实；加强常规系统的优化配置，定期进行相关风险的排查，以此及时防范可能存在的问题。此外，还应当全面加强计算机硬件系统和软件系统的优化配置，及时更换不匹配的相关软件或者是老旧的器件，从而更好地营造良好的运行环境。

4.网络信息加密技术的应用

网络信息加密技术应用的效用可减少信息数据在传输中或者存储中产生的泄露现象，当前，信息时代来临，通过加密技术的应用，可有效保障用户信息数据的安全性。当前，密钥技术的应用，能够将硬件作为计算机信息安全防护的核心内容，对网络黑客进入计算机硬件系统产生防范作用，对其进入网络系统内部产生防范效果。这一技术在信息交互之中的应用，可以依靠密码配对方式，对网络攻击者进行识别，减少不法分子对网络安全漏洞及逆行应用以实现网络系统攻击情况的出现。密钥技术的应用，可在信息数据传输前，对信息技术进行加密处理，信息传输至对应目标之后，采取安全算法，依靠公钥或者私钥进行密码解开，不仅对信息传输的安全性进行了保障，还能够降低信息攻击和信息拦截问题的发生几率[4]。

5.学习先进技术

计算机网络安全的发展，需要有相应专业人员的帮助。所以，在计算机网络安全技术研究过程中，应该建设高素质安全管理团队，其不仅要能够加强对技术的研究，还应该在这其中不断学习先进技术，进而其更好地提高计算机网络技术水平。计算机安全管理人员可以采用设计问题的方法，在用户需要获取相应信息的时候，就可以通过这一方法来判断用户的身份，进而让用户及时地获取到自己想要的信息。还应该加强网络监控评估，要由专业管理团队来对网络设备进行进行评估，定期对网络设备检查，这也是保证网络安全的重要方法。

6.增强网络用户的安全意识

首先，对于各种威胁网络安全的现象，需要加强用户的网络安全意识，最主要的是用户的个人隐私信息的保护意识。相关单位加强对网络安全知识的普及，在单位内部能让员工，对网站上莫名弹出的“钓鱼”网站、网站链接保持警惕，可罗列典型的诈骗类、虚假类等网站模板，提升相关人员对虚假网站的认知。以此，避免员工误入来历不明的网站、软件的“圈套”。单位应定期宣传网络安全知识，让员工养成在下载软件时，先利用杀毒软件进行扫描的行为习惯，避免计算机网络被病毒感染。

7.完善管理机制

信息安全管理是通过科学的组织机制、规章制度以及管控手段等，对一些存在信息安全保障功能的软硬件设施、管理信息者、使用数据者等，进行全面整合，确保该组织可以实现预设的信息安全目标，对信息的安全、隐私确保可用。具体而言，信息安全管理包括两个内容：管理措施和安全方法。信息安全管理必须要在制度和手段等方面充分对技术进行思考其中的价值，只有通过制度、手段、技术等方面的结合，才能达到全面的融合，才可以达到最佳的安全管理作用。

四、结束语

综上所述，计算机网络逐渐发展成为人们日常生活的必需品，人们对计算机网络的依赖性与日俱增。随着计算机网络的深入发展，网络安全问题成为当前人们所关注的重要问题。从当前我国计算机网络安全现状来看，计算机网络安全存在着许多问题，这些问题的存在使得计算机网络安全面临着较大的隐患，可能会给人类社会造成无可挽回的损失。为最大程度地保障计算机网络安全，就必须针对其存在的问题采取有防范措施。

参考文献：

[1]张莉.基于物联网技术的计算机网络安全问题及应对策略研究[J].信息与电脑（理论版），2020，32（13）：203 ~ 204.

[2]周光前.大数据时代下计算机网络安全的防范措施[J].信息与电脑（理论版），2019，31（24）：189 ~ 190，193.

[3]郑莉凡，李刚.影响计算机网络安全技术的相关因素及防范策略[J].中国新通信，2019，21（9）：135.

[4]谢情.计算机网络安全技术的影响因素与防范策略[J].网络安全技术与应用，2021（2）：161-163.