计算机网络信息管理安全防护问题与措施

蔡利峰
国网辽宁省电力有限公司朝阳供电公司　辽宁　朝阳　122000

摘　要：经济时代催生信息科学技术发展日新月异，国民的生活生产越来越离不开计算机的使用。本文从当前计算机网络信息管理的现存问题出发，寻找安全防护的可行性举措，通过增强全民的网络安全意识，加大防护技术的应用，不断提高相关人员的工作能力，多角度深层次保障网络信息使用安全，制定完备的安全管理制度，优化安全防护手段，逐步提高计算机网络信息管理效率。

关键词：计算机；网络信息管理；安全防护

引言：由于网络的广泛应用以及计算机技术的飞速发展，计算机网络已成为现代社会不可或缺的组成部分。然而，网络安全问题日益严重，给个人和企业带来了巨大的风险。因此，计算机网络信息管理安全防护问题与措施显得尤为重要。本文将探讨网络安全的重要性，并提出一些有效的防护措施。

1 计算机网络信息安全的重要性

随着互联网的广泛应用与完善，计算机网络早已成为人类日常生活、工作与学习所缺少的内容。然而，随着网络技术的不断进步，网络安全问题也日益凸显，给个人和企业带来了巨大的风险。因此，计算机网络信息安全的重要性不言而喻。在互联网时代，人们的生活越来越离不开网络，大量的个人信息、财产信息等都存储在网络上。一旦这些信息被不法分子窃取或滥用，将会给个人带来极大的损失。网络安全问题还可能导致个人隐私泄露，如身份证号、银行卡号等敏感信息被泄露，可能给个人的生活带来诸多不便。企业的商业机密、客户信息、财务数据等都存储在企业内部的网络系统中。一旦这些信息被黑客攻击或内部人员泄露，将会给企业带来巨大的经济损失和声誉损害。网络安全问题还可能导致企业的生产、销售等业务受到影响，甚至可能导致企业的破产。加强网络安全防护，确保国家信息安全是每个国家都必须面对的重要任务。网络犯罪、网络暴力、网络谣言等问题已经对社会秩序造成了很大的影响。加强网络信息安全管理，可以有效地减少这些问题的发生，维护社会稳定和谐。同时，良好的网络信息安全环境有利于创新和发展，推动经济社会的持续发展[1]。为了应对日益严峻的网络安全形势，企业和个人都应该采取积极措施，提高网络安全意识，加强网络安全防护。应该加大对网络安全的投入，加强对网络犯罪的打击力度；企业应该建立健全的网络安全防护体系，加强对员工的网络安全培训；个人应该提高自身的网络安全意识，谨慎使用网络服务，保护好自己的个人信息。计算机网络信息安全对于个人、企业、国家和社会都具有重要意义。只有大家共同努力，才能确保网络空间的安全和稳定，让互联网更好地造福于人类。

2 计算机网络信息管理安全防护问题

2.1 计算机网络的安全防护级别低

计算机网络信息管理安全防护问题是一个非常重要的问题。随着互联网的发展，网络安全问题也越来越严重。目前，计算机网络的安全防护级别普遍较低，这给网络安全带来了很大的隐患。计算机网络的安全防护级别低会导致数据泄露和数据丢失。在网络中，数据是非常重要的资源。如果网络安全防护级别低，那么黑客就可以轻易地窃取这些数据，从而造成重大损失。在网络中，系统是非常重要的组成部分。如果网络安全防护级别低，那么黑客就可以通过攻击系统来破坏整个网络。计算机网络的安全防护级别低还会影响企业的正常运营。在现代企业中，很多业务都是依赖于网络来完成的。如果网络安全防护级别低，那么企业就无法正常开展业务。

2.2 计算机网络的监管存在漏洞

随着互联网技术的飞速发展，计算机网络已经成为了人们生活、工作中不可或缺的一部分。然而，计算机网络的安全问题也日益凸显，给企业和个人带来了巨大的风险。在计算机网络信息管理安全防护方面，存在着许多问题亟待解决。许多企业和个人对网络安全的重视程度不够，缺乏基本的安全防护措施，如定期更新系统补丁、安装防病毒软件等。这导致了网络安全隐患的存在，容易受到黑客攻击和病毒感染。随着黑客技术的不断进步，传统的安全防护手段已经难以应对新型的网络攻击手段。企业和个人需要不断更新网络安全技术，提高自身的防护能

力。然而，目前市场上的网络安全产品和技术更新速度较慢，很难满足用户的需求。网络安全是一个高度专业化的领域，需要大量的专业人才来进行研究、开发和维护。然而，目前我国网络安全人才的培养和引进还存在一定的问题，导致网络安全人才的短缺。

2.3 计算机病毒

计算机病毒是计算机网络信息管理中的一大安全隐患。它通过复制自身并感染其他程序，破坏系统的稳定性和安全性，给企业和个人带来巨大的损失。计算机病毒的传播速度快，难以防范。病毒可以通过电子邮件、移动存储设备、网络下载等多种途径传播，一旦感染，病毒会在系统中迅速扩散，导致数据丢失、系统崩溃等问题。计算机病毒具有很强的隐蔽性。病毒往往会借助操作系统的缺陷进行入侵，使用户很难察觉到。而即使发现了异常，也常常无法及时定位病毒并加以消除。因此计算机病毒有高度的变异性。病毒制作者会不断对病毒进行升级和修改，使其更具破坏力和逃避检测的能力。这使得传统的杀毒软件很难完全应对新型病毒的威胁。计算机病毒还可能导致个人隐私泄露和企业机密泄露。病毒感染后，用户的个人信息可能被窃取，企业的商业机密也可能被竞争对手获取。

2.4 安全技术手段不够先进

随着互联网的普及和发展，计算机网络信息管理在各个领域都得到了广泛应用。然而，网络安全问题也日益凸显，尤其是安全技术手段不够先进，给企业和个人带来了诸多隐患。网络攻击手段不断升级，传统的防火墙、杀毒软件等防护措施已经难以应对新型的网络攻击。黑客利用漏洞、恶意软件等手段，可以轻易侵入企业的网络系统，窃取重要数据，甚至破坏整个网络环境。这种情况下，企业和个人的网络信息安全面临着巨大的威胁。随着云计算、大数据等技术的发展，企业对网络信息管理的需求越来越高。现有的安全防护手段往往无法满足这些需求，导致企业在数据传输、存储和使用过程中容易遭受攻击[2]。由于缺乏专业的网络安全人才，很多企业在面对网络安全隐患时束手无策，无法及时采取有效的防护措施。网络信息管理安全防护意识薄弱也是一个问题。许多企业和个人在使用网络时，缺乏基本的安全防护知识，容易成为网络攻击的目标。例如，使用简单的密码、点击不明链接等行为都可能导致网络安全问题。

3 计算机网络信息管理安全防护措施

3.1 建立计算机网络安全防护体系

由于计算机技术的飞速发展，计算机早已成为了现代社会中不可或缺的重要组成部分。但是，安全问题却接踵而来，给个人和企业带来了巨大的风险。因此，建立一套完善的计算机网络安全防护体系显得尤为重要。需要从技术层面入手，提高网络安全防护能力。这包括加强防火墙、入侵检测系统、安全审计等技术手段的应用，确保网络的安全稳定运行。加强对操作系统、数据库、应用软件等关键信息基础设施的保护，防止恶意攻击和病毒侵入。加强网络安全意识培训，提高全体员工的安全防范意识。通过定期举办网络安全知识讲座、培训班等形式，使员工充分认识到网络安全的重要性，掌握基本的网络安全知识和防护技能。还要建立健全网络安全管理制度，明确各部门和个人在网络安全工作中的职责和义务，确保网络安全工作的落实。加强与行业组织的合作，共同应对网络安全挑战。同时，加强与其他企业和行业组织的交流与合作，共享网络安全信息和资源，形成合力应对网络安全威胁。建立健全应急响应机制，确保网络安全事件的及时处置。制定详细的应急预案，明确应急响应流程和责任分工。一旦发生网络安全事件，要迅速启动应急预案，采取有效措施控制损失，及时报告相关部门，积极配合调查取证工作，防止事态扩大化。只有这样，才能确保计算机网络的安全稳定运行，为社会经济发展和人民生活提供有力保障。

3.2 完善计算机网络多模加密技术

随着互联网技术的发展，网络攻击手段日益翻新，企业面临的网络安全威胁也越来越大。因此，完善计算机网络多模加密技术显得尤为重要。企业应建立完善的网络安全管理制度，明确网络安全责任，加强网络安全培训，提高员工的网络安全意识。同时，企业应定期对网络安全进行检查，发现潜在的安全隐患，及时进行整改。采用多模加密技术，确保数据在传输过程中的安全。多模加密技术是一种结合了公钥加密和对称加密的加密方式，可以有效地防止数据被窃取或篡改。企业应根据实际需求选择合适的加密算法，如AES、DES、RSA等，确保数据的机密性、完整性和可用性。通过配置防火墙、入侵检测系统等安全设备，可以有效地阻止外部攻击，保障企业内部网络的安全。企业还应定期更新操作系统、应用软件等，修补已知的安全漏洞，降低被攻击的风险。在数据传输过程中，企业应使用安全的通信协议，如SSL/TLS等，确保数据在传输过程中不被泄露或篡改。同时，企业还可以采用虚拟专用网络（VPN）技术，实现远程办公时的数据安全传输。通过定期备份重要数据，确保数据丢失时能够快速恢复。企业还应制定应急预案，以便在发生网络安全事件时能够迅速应对，

减少损失。

3.3 及时更新系统和软件

计算机网络信息管理安全防护措施是确保企业信息系统安全的关键。为了提高网络安全，我们需要采取一系列有效的防护措施，包括及时更新系统和软件、加强访问控制、定期进行安全检查等。随着技术的不断发展，黑客攻击手段也在不断升级，我们需要定期更新操作系统、浏览器、防病毒软件等，以修复已知的安全漏洞，防止黑客利用这些漏洞对系统进行攻击。及时更新软件也能确保我们能够使用最新的功能和特性，提高企业的工作效率。企业应该根据员工的职责分配不同的权限，确保敏感数据只能被授权人员访问。还需要加强对外部访问的控制，例如设置防火墙规则，限制外部设备对内部网络的访问[3]。通过实施严格的访问控制策略，我们可以有效地防止未经授权的访问和数据泄露。企业应该定期组织安全检查活动，对网络设备、服务器、数据库等进行全面检查，发现潜在的安全隐患并及时采取措施加以解决。还可以邀请专业的安全公司进行渗透测试，模拟黑客攻击，检验企业信息系统的安全性能。应该定期开展网络安全培训活动，教育员工如何识别网络钓鱼邮件、防范社交工程攻击等常见网络安全威胁。通过提高员工的安全意识，可以降低因人为疏忽导致的安全事故发生率。计算机网络信息管理安全防护措施是一个系统性的工作，需要我们从多个方面入手，才能确保企业信息系统的安全。只有做好这些防护措施，我们才能在信息化时代更好地应对各种网络安全挑战。

3.4 采用先进的安全技术手段

计算机网络信息管理安全防护措施是企业信息安全的重要组成部分。随着信息技术的不断发展，网络攻击手段日益翻新，企业面临着越来越严重的网络安全威胁。因此，采取有效的安全防护措施，确保企业网络信息安全至关重要。防火墙是网络安全的第一道防线，可以有效地阻止未经授权的访问和恶意攻击。企业应部署高性能的防火墙设备，对内部网络进行隔离，同时监控外部网络流量，防止潜在的网络攻击。IDS/IPS系统可以实时监控网络流量，检测并阻止潜在的入侵行为。企业应部署IDS/IPS系统，对网络流量进行实时监控，及时发现并阻止恶意攻击。数据加密技术可以保护企业的敏感数据，防止数据泄露和篡改。企业应采用先进的加密算法，对重要数据进行加密处理，确保数据在传输和存储过程中的安全。企业应实施严格的身份认证和访问控制策略，确保只有授权用户才能访问企业内部网络资源。通过使用多因素认证、数字证书等技术手段，提高身份认证的安全性[4]。建立完善的安全审计和日志管理系统，对网络活动进行实时监控和记录。通过对安全事件进行分析，及时发现并处置安全隐患，降低网络安全风险。加强员工的安全培训和意识教育，提高员工的安全防范意识和技能。通过定期开展安全培训和演练，使员工熟悉网络安全知识，掌握正确的安全操作方法。企业应综合运用上述先进的安全技术手段，构建完善的网络信息管理安全防护体系，确保企业网络信息安全。同时，企业还应关注网络安全技术的发展趋势，不断更新和完善安全防护措施，应对日益严峻的网络安全挑战。

结语

综上所述，提高计算机网络信息管理能力，落实安全防护举措是现代化信息技术发展的当务之急，通过对使用者普及信息安全管理理念，从而推动全社会的网络信息管理意识提高。对信息系统增强安全防护可以保证数据安全和生产生活稳定，构建绿色生态的网络环境，迎接互联网时代新的机遇和挑战。

参考文献

[1]张伟，王倩.计算机网络信息管理安全防护若干问题与措施[J].网络安全技术与应用，2020(7):10-12.

[2]李云.计算机网络信息管理安全防护的几个重要措施[J].信息安全研究，2021(4):45-47.

[3]马世明，王月.基于深度学习的计算机网络信息管理安全防护[J].网络安全技术与应用，2022(1):59-62.

[4]刘刚，杨新宇.基于攻击路径的网络信息管理安全防护[J].计算机与现代化，2020(11):69-72.