基于信息安全问题的计算机网络应用分析

吴　鹏

【摘　要】随着计算机技术的快速发展和普及，计算机网络应用已经成为人们生活和工作中不可或缺的一部分。然而，在计算机网络应用的过程中，信息安全问题也十分突出。网络中的各种攻击，如计算机病毒、黑客攻击、网络钓鱼等，给人们的生活和工作造成了很大的威胁和损失。因此，对于计算机网络应用中的信息安全问题进行深入研究和探讨，将有助于提高网络安全防护水平，保护个人和企业的信息安全，推动计算机网络应用的发展和进步。

【关键词】信息安全问题；计算机网络；应用

引言

网络信息技术迅速发展，已经成为时代发展的重大主题，在社会各个领域，计算机网络全面渗透，不断扩大自身信息的应用价值，同时也带来了信息泄漏、数据被窃取等众多网络安全问题。当前，计算机网络的应用开始强调保障信息安全这一基础要求，针对用户操作不当、病毒感染、信息泄密等现象，相关人员必须构建信息安全意识。除了依靠网络安全系统营造健康的应用环境，还需主动加强安全保障技术的优化，持续性提升计算机网络安全防护效果。

1.计算机网络应用中常见的信息安全问题

在互联网发达的今天，同时迎来了 5G、大数据、人工智能等新兴技术的繁荣发展，数据信息的互联互通促使网络信息安全风险持续升级，这不仅体现在个人计算机网络应用中的数据泄漏，同样在企业和国家网络系统平台运行中有更突出表现，如高危漏洞曝出使企业整个网络体系产生安全隐患，针对性的攻击频发影响系统的稳定性。以企业计算机网络应用来说，常见的信息安全问题有：网页内容篡改、网站入侵、数据泄漏、网络勒索、分布式拒绝服务攻击等。当产生网络恶意攻击事件，企业商业数据会遭受违规利用和大规模泄漏，使生产生活和经济行为深受影响，所以，计算机网络应用中需要特别强调信息安全问题，并采取有效措施加以应对。依据计算机网络应用中出现的种种信息安全隐患，比如病毒感染、网络系统漏洞、人为操作不当、黑客入侵等，可以从三个方面来归类常见的信息安全问题：

1.1.技术层面

技术层面的信息安全网络问题最为突出，这体现在网络通信线路和计算机设备的缺陷上，其中有终端接入、设备监听、网络攻击等，此外，还体现在软件的漏洞上，包括软件病毒入侵、漏洞软件被利用等。由于互联网迅猛发展，“网络黑客”、“病毒木马”、“信息垃圾”等越来越多的网络攻击和威胁源出现，而且一些计算机网络中的恶性病毒传播速度很快，会产生大范围的网络威胁，促使企业、政府在计算机网络应用上面临较大的信息安全管理挑战。在计算机应用系统中，信息基础设施是国家和行业至关重要的资产，如若数据泄漏、丧失应用功能，将会严重影响行业的平稳运行，造成财产损失。随着行业对信息网络的依赖性越来越强，由此需要不断升级关键信息基础设施的安全管理水平，更好应对技术层面的信息安全问题。

1.2.人员层面

人员是网络信息安全问题的关键控制者和影响要素，持有不同应用操作目标的人员，在这一领域有不同表现。如技术人员业务操作不当，会在无意中破坏计算机的保密系统；而系统操作人员在计算机网络应用中缺乏保密和防护意识，对重要信息不采取加密处理，共享文档和数据缺失必要的权限控制，由此会降低信息安全系数。另外在计算机网络应用中，专业人员和不法人员往往会对信息安全造成极大威胁，一些优秀的计算机专业人员会巧妙利用先进技术盗取信息，以非法手段访问系统；同时，不法人员也会采取破译、监听等方式窃取很多平台和行业的保密信息，由此会给用户带来较大损失。

2.基于信息安全问题的计算机网络应用管理措施

2.1.加强系统监测和管理

数据的安全性是计算机网络应用管理的重要问题之一。数据加密是保障数据安全性的重要措施之一。在存储和传输的过程中，对于重要数据，需要采用安全的加密措施，以保证数据不被篡改、泄露和非法获取。

对于存储的数据，可以采用加密算法进行加密，通过对敏感信息进行加密，可以防止数据被恶意窃取和篡改，保证数据的机密性和完整性。

对于传输的数据，可以采用传输层安全协议 TLS/SSL 等实现数据的安全传输，通过建立安全的通信信道，以保障数据传输过程中的机密性、完整性和可用性。

尤其是在云计算和物联网等领域，对于数据加密以及数据隐私保护更加关键。在对于云存储和云计算采用

数据加密的同时，可采用身份认证、访问控制等技术保护数据隐私。

并且，需要注意的是，数据加密仅仅是计算机网络应用管理的一个方面，还需考虑到数据备份、灾备以及接入人员的安全意识等因素综合保障数据安全。因此，数据的加密和保护必须全面考虑、多方面综合施策，以达到数据安全的最佳状态。

2.2.提高员工安全意识

提高员工安全意识是保障企业网络安全的基础。针对网络安全问题的普及教育和培训应该到位，确保员工掌握基本的安全知识、技能和习惯，并能有效地应对网络安全问题。

首先，企业应该开展网络安全知识的普及教育和培训，针对员工不同的岗位和层次进行量身定制，让员工了解常见的网络安全威胁和防范措施，如密码管理、安全访问、邮件安全等。

其次，企业可以通过模拟演练、考试等方式对员工掌握的安全知识进行测试和评估，发现存在的问题和漏洞，并加强训练和巩固。

另外，企业应该制定规范的安全管理制度和操作流程，规定员工在日常工作中的网络使用行为和限制，并进行监督和管理。

最后，企业需要持续提高员工的安全意识，形成全员参与的安全文化，提高员工自觉遵守安全规定的意识和能力。

3.结束语

为确保应用系统具备安全运行支持，通常要构建网络安全系统，确立网络信息安全处理模块和技术，满足计算机网络信息安全等级保护需求。面对愈加复杂的计算机应用环境，需要加强防火墙技术、加密技术等先进信息防护手段的应用，防范并抵御大规模和较强的恶意攻击，实时监测、跟踪、报警计算机网络中的入侵行为，对安全事件积极响应处置，使其能够在受到损害后快速恢复运行。

【参考文献】

[1]谢露莹，吴交树.计算机网络信息安全问题分析及解决策略探讨[J].无线互联科技，2022,19(12):26-28.

[2]赵丽辉.计算机网络信息安全及其防火墙技术应用分析[J].无线互联科技，2022,19(02):99-100.

[3]何代菊.大数据背景下计算机网络信息安全问题分析[J].南方农机，2021,52(23):126-128.

作者简介：吴鹏（1989 年 2 月），男，汉族，网络运维行业，本科学历，主要从事网络服务器运维和硬件维护 ，身份证号：6528271989****0078