信息工程建设中计算机网络安全问题及对策探究

翟　禹
哈尔滨惠众宜家网络科技有限公司　黑龙江　哈尔滨　150000

摘　要：信息工程建设中，计算机网络安全问题日益凸显，成为制约信息化发展的关键因素。本文深入探究信息工程建设中面临的计算机网络安全问题，包括技术漏洞、管理缺陷及外部威胁等，并针对性地提出加强网络协议安全性、完善操作系统与软件防护、建立健全安全管理制度、强化培训与教育、提升防护能力及加强监测与预警等对策。旨在为信息工程建设提供有效的网络安全保障策略，促进信息化事业的健康发展。

关键词：信息工程建设；计算机网络技术；安全问题；对策

引言：随着信息技术的飞速发展，信息工程建设已成为推动社会进步和经济发展的重要力量。计算机网络安全问题却如影随形，严重威胁着信息工程的稳定运行和数据安全。因此深入探究信息工程建设中的计算机网络安全问题及对策，对于保障信息化事业的健康发展具有重要意义。本文将从多个角度出发，全面分析并提出解决方案。

1 信息工程建设中计算机网络安全问题概述

1.1 计算机网络安全定义

计算机网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，数据的保密性、完整性及可使用性受到保护。它涵盖了物理安全和逻辑安全两个方面。物理安全指的是系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安全则是指计算机系统中的硬件、软件和数据资源不因偶然或恶意的原因遭到破坏、更改、泄露，从而保证网络系统连续可靠性地正常运行，网络服务正常有序。具体来说，计算机网络安全不仅包括组网的硬件、管理控制网络的软件，也包括共享的资源及快捷的网络服务。参照ISO给出的计算机安全定义，计算机网络安全旨在保护计算机网络系统中的硬件、软件和数据资源，确保它们不会因各种原因（包括偶然和恶意因素）而受到损害，从而保证系统能够持续、可靠地运行。

1.2 网络安全问题的类型

网络安全问题主要包括以下几类；（1）网络系统安全。主要涉及计算机和网络本身存在的安全问题，如物理安全、系统安全、数据库安全、网络设备安全及网络服务等。这些问题直接关乎电子商务平台的可用性和安全性。（2）网络信息安全。信息在网络的传递过程中可能面临被窃取、篡改、假冒或恶意破坏的风险。例如，电子交易信息在网络上传输时可能被非法修改、删除或重放，导致信息失去原有的真实性和完整性[1]。（3）网络交易安全。在电子商务虚拟市场交易过程中，存在交易主体真实性、资金被盗用、合同法律效应及交易行为被抵赖等问题。这些问题可能损害交易双方的声誉，甚至导致欺诈行为的发生。另外，网络安全问题还包括恶意软件的威胁，如计算机病毒、特洛伊木马程序等，它们可能破坏数据、运行破坏性程序或破坏受害者数据、应用程序或操作系统的机密性、完整性和可用性。

1.3 网络安全问题对信息工程建设的影响

网络安全问题对信息工程建设具有深远的影响，网络安全事件可能导致重要数据及大量个人信息的泄露，给企业和个人带来严重的经济损失和声誉损害。一旦关键信息基础设施发生网络安全问题，可能导致人民群众生产生活不可或缺的产品和服务提供中断，如通信、出行、电子交易等基础性服务的中断或短缺。能源、交通、水利等行业的关键信息基础设施发生网络安全问题后，可能对物理世界造成破坏，如交通事故、油气泄漏等。金融、公共服务、电子政务等领域关键信息基础设施的网络安全问题可能影响国家正常的金融秩序、服务提供和政令畅通等，从而损害国家的网络空间主权。

2 信息工程建设中计算机网络安全问题分析

2.1 技术因素

在信息工程建设中，技术因素是影响计算机网络安全的关键因素之一。首先，网络系统的设计和构建本身就存在潜在的安全风险。由于互联网的开放性和共享性，任何单位或个人都可以方便地传输和获取各种信息，这种特性使得网络系统极易受到来自外部的攻击。网络协议和数据传输方式也可能存在安全漏洞，如传输文件时使用的明码传输方式，使得文件在传输过程中容易被跟踪、拦截并复制，增加了信息泄露的风险。操作系统作为计算机系统的核心，其安全性直接关系到整个

网络系统的安全。目前许多操作系统都存在着安全缺陷或漏洞，这些漏洞为黑客提供了可乘之机。黑客可以利用这些漏洞对系统进行攻击，从而获取系统控制权，窃取或篡改数据，甚至破坏整个网络系统。网络安全技术的更新换代也是影响网络安全的重要因素。随着网络技术的不断发展，新的网络安全威胁不断出现，如网络病毒、恶意软件等。这些新型威胁具有传播速度快、破坏性强等特点，给网络安全防护带来了极大的挑战。

2.2 管理因素

管理因素是影响计算机网络安全不可忽视的一环，网络安全意识的培养是保障网络安全的基础。在实际操作中，许多用户和管理员对网络安全的认识不足，缺乏必要的安全意识和技能。他们可能会轻易打开来路不明的邮件、浏览不良信息或未对敏感数据进行加密处理，从而给网络安全带来潜在威胁。网络安全管理制度的完善和执行也是保障网络安全的关键，一些企业或机构在网络安全管理方面存在制度不健全、执行不力等问题。例如，没有建立有效的网络安全防护体系、缺乏定期的网络安全检查和评估机制、未对重要数据进行备份和恢复等。这些问题可能导致网络系统在遭受攻击时无法及时响应和恢复，造成重大损失。网络安全人才的培养和引进也是提升网络安全管理水平的重要途径，目前网络安全人才短缺的问题依然突出。许多企业或机构缺乏专业的网络安全人才，导致网络安全防护能力不足。

2.3 外部因素

外部因素也是影响计算机网络安全的重要因素之一。首先，黑客攻击和网络病毒是网络安全的主要威胁之一，黑客可以利用各种技术手段对系统进行攻击，窃取数据、破坏系统或进行其他恶意行为[2]。而网络病毒则可以通过电子邮件、网络共享等方式快速传播，对计算机系统进行破坏和感染。其次，自然灾害和意外事件也可能对网络安全造成威胁，例如，地震、洪水等自然灾害可能导致网络设施受损或中断，影响网络的正常运行。而人为操作失误或恶意破坏也可能导致数据丢失或系统瘫痪等严重后果。

3 信息工程建设中计算机网络安全问题应对策略

3.1 加强网络协议的安全性

在信息工程建设中，网络协议的安全性是保障整个网络系统稳定运行的重要基础。针对网络协议存在的潜在漏洞，要深入了解并熟悉当前主流网络协议的工作原理及其存在的安全风险。这包括TCP/IP协议族、HTTP、HTTPS、FTP等常用协议。通过深入理解这些协议，可以更准确地识别并防范潜在的安全威胁。对关键网络协议进行加密处理，加密技术可以有效防止数据在传输过程中被窃取或篡改。通过使用SSL/TLS等加密协议，我们可以确保数据在网络中的安全传输，防止敏感信息泄露。还应加强网络协议的认证机制，通过引入数字签名、身份认证等技术手段，我们可以确保网络通信的双方身份的真实性，防止中间人攻击等安全风险。要定期对网络协议进行更新和升级，随着技术的不断发展，新的网络协议和加密技术不断涌现。应密切关注这些新技术的发展动态，及时将先进的协议和技术应用到网络系统中，以提高网络的整体安全性。

3.2 完善操作系统与软件的安全防护

操作系统和软件是计算机系统的核心组成部分，其安全性直接关系到整个网络系统的稳定与安全。为了完善操作系统与软件的安全防护，要定期更新操作系统和软件补丁，操作系统和软件在开发过程中难免存在漏洞，这些漏洞可能会被黑客利用进行攻击。应密切关注厂商发布的更新和补丁信息，及时安装这些更新和补丁以修复已知漏洞。加强操作系统和软件的访问控制，通过合理配置权限和角色，可以限制不同用户对系统和软件的访问权限，防止未经授权的访问和操作。还应加强操作系统和软件的日志审计功能，通过记录和分析系统日志，我们可以及时发现异常行为和安全事件，以便迅速采取措施进行应对。要定期进行系统和软件的漏洞扫描和风险评估，通过使用专业的漏洞扫描工具和安全评估软件，可以及时发现系统和软件中存在的潜在漏洞和安全风险，从而有针对性地采取措施进行防范和修复。

3.3 建立健全安全管理制度

安全管理制度是保障网络安全的重要基石。为了建立健全安全管理制度，可以从以下几个方面入手：首先，要明确安全管理的目标和原则，这包括确定网络安全防护的优先级、制定安全防护策略和标准等。通过明确目标和原则，可以为安全管理提供明确的指导和方向。其次，要制定详细的安全管理制度和流程，这包括制定网络访问控制制度、密码管理制度、数据备份与恢复制度等。通过制定这些制度和流程，可以规范网络系统的使用和管理行为，降低安全风险。另外，还应加强安全管理制度的执行和监督，通过定期检查、评估和审计等手段，可以确保安全管理制度得到有效执行，及时发现并纠正存在的问题[3]。最后，要不断完善和更新安全管理制度，随着技术的不断发展和网络环境的变化，应定期对安全管理制度进行审查和更新，以适应新的安全需求和挑战。

3.4 加强网络安全培训与教育

提高员工的网络安全意识和技能是保障网络安全的重要手段。为了加强网络安全培训与教育，要定期组织网络安全培训课程，这些课程可以涵盖网络安全基础知识、安全操作规程、应急响应等方面的内容。通过参加这些课程，员工可以了解网络安全的重要性和基本防护技能。要利用多种渠道进行网络安全宣传教育，这包括通过公司内部网络、邮件、公告板等途径发布网络安全相关信息和提示。通过宣传教育，可以提高员工对网络安全问题的认识和警惕性。还可以组织网络安全知识竞赛、模拟演练等活动，这些活动可以激发员工的学习兴趣和参与度，帮助他们更好地掌握网络安全知识和技能。要鼓励员工积极参与网络安全培训和教育活动，通过设立奖励机制、提供学习资源等方式，我们可以激励员工不断提升自己的网络安全素养和能力。

3.5 提高网络安全防护能力

提高网络安全防护能力是确保网络安全不可或缺的一环。为了实现这一目标，加强网络安全设备的部署和配置显得尤为重要。防火墙、入侵检测系统以及安全审计系统等设备的合理应用，构成了网络安全防护的第一道防线。这些设备能够对网络流量进行实时监控和过滤，有效识别并阻断潜在的安全威胁，从而大大降低网络被攻击的风险。除了设备部署，采用先进的加密技术和安全协议也是保障数据安全的重要手段。SSL/TLS等加密协议和AES等高级加密算法的应用，确保了数据在网络传输和存储过程中的安全性，即使数据被窃取，也无法被轻易解密和篡改。身份认证和访问控制机制的加强也是提升网络安全防护能力的关键。通过引入数字证书、生物识别等先进技术，我们可以确保网络通信双方身份的真实性，有效防止未经授权的访问和操作，进一步巩固了网络安全的防线。然而仅有这些措施还远远不够。定期进行网络安全演练和测试，通过模拟真实的安全事件和攻击场景，可以检验网络安全防护体系的有效性和可靠性，及时发现并修复存在的问题，确保网络安全防护能力始终保持在较高水平。

3.6 加强网络安全监测与预警

网络安全监测与预警是及时发现并应对网络安全威胁的重要手段。建立完善的网络安全监测体系，这包括部署网络安全监测设备、建立安全事件日志库和数据分析系统等。通过这些手段，可以对网络流量、系统日志等数据进行实时监测和分析，及时发现异常行为和安全事件[4]。加强网络安全预警机制的建设，通过收集和分析网络安全态势信息、建立预警模型和指标体系等方式，可以提前发现潜在的安全威胁和风险，为应对网络安全事件提供有力的支持和保障。还应加强网络安全信息的共享和协作，通过与相关部门、企业和组织建立信息共享机制，我们可以及时获取最新的网络安全信息和威胁情报，共同应对网络安全挑战。要定期对网络安全监测与预警系统进行评估和更新，随着技术的不断发展和网络环境的变化，应定期对监测与预警系统进行审查和更新，以适应新的安全需求和挑战。同时还要加强系统的稳定性和可靠性测试，确保其在关键时刻能够发挥应有的作用。

结束语

在信息工程建设中，计算机网络安全问题及对策的探究是一个持续且复杂的过程。通过本文的探讨，不仅揭示了当前信息工程建设中面临的网络安全挑战，还提出了一系列切实可行的对策。网络安全工作永远在路上，我们需要不断适应新技术的发展，持续完善安全防护体系。未来，将继续深化研究，为信息工程建设提供更加坚实可靠的网络安全保障，共同推动信息化事业迈向新的高度。

参考文献

[1]李燕.计算机安全存储中云计算技术的应用研究[J].网络安全技术与应用,2022(1):66-67.

[2]刘永战,李苒,冯阳.面向云平台构建计算机网络安全和防范机制分析[J].通信电源技术,2022,39(2):127-129.

[3]罗振营.大数据时代下计算机网络信息安全问题分析[J].现代工业经济和信息化,2022,12(12):98-100.

[4]马越.大数据及人工智能技术的计算机网络安全防御系统设计[J].中国新通信,2022,24(24):132-134.