探讨计算机网络系统安全及管理策略框架构建

李凯
秦皇岛市第三医院

摘　要：在数字化时代，计算机网络的科技为我国公众的日常生活及工作环境提供了诸多便捷条件。但是，在网络运营的过程中，会遭遇诸如网络病毒、黑客的侵袭和各种软硬件设备的故障等众多风险。因此，有必要对计算机网络系统进行全面加强安全性建设，优化和强化网络安全管理战略，完善和强化计算机网络安全防护措施，以及周期性地进行计算机硬件和软件设备的检查和维修。本研究旨在探究计算机网络系统的安全性及其管理方法，期望这可以为未来的计算机网络系统安全管理策略提供参考与启示。

关键词：计算机网络系统；安全管理；策略
【DOI】10.12252/j.issn.2096-6261.2022.09.206

一、网络信息安全的特点

（一）网络信息安全的脆弱性

网络信息安全正常状态下处于脆弱性状态，主要因为网络技术的迅猛发展和开放性、匿名性以及身份鉴别的困难性等因素。此外，网络攻击技术也在快速发展，通过利用漏洞、社会工程学、恶意软件等攻击手段，黑客可以轻松入侵网络、获取和篡改数据、破坏网络服务。同时，网络安全也受到国家和政治利益的干扰，一些组织和政府可能会通过网络攻击来获取敌对国家或组织的机密信息[1]。因此，网络信息安全的脆弱性是一项需要时刻关注和解决的战略任务。

（二）网络信息安全的突发性

网络信息安全问题是指在网络上进行数据传输、存储、处理等活动的过程中出现的各种信息安全问题，包括黑客攻击、病毒攻击、木马攻击、僵尸网络等。网络信息安全问题的突发性主要表现在以下两个方面：首先，网络信息安全威胁具有突发性。由于网络的开放性和不可控性，黑客攻击、病毒攻击等网络安全威胁往往是突然发生的，并且由于攻击手段的不断创新以及网络环境的不断变化，网络安全威胁的类型和形式也在不断地更新和演化。这就需要网络安全从业人员时刻保持警惕，积极防范潜在的网络安全威胁。其次，网络信息安全问题的传播速度非常快。一旦网络信息安全问题发生，由于网络媒介的广泛和信息传播的快速，信息安全问题的影响面很快就会扩散，并且会对很多不同的领域造成影响，如商业、政治、社会等。例如，曾经的“勒索病毒”攻击发生后，很快就在全球范围内造成了极大的经济损失，甚至要求政府支付高额赎金来解决网络安全问题。

（三）网络信息安全的全球性

网络信息安全是一个全球性的问题，因为互联网已经成为人们生活中不可或缺的一部分，涵盖了方方面面的活动，包括社交网络、电子商务、在线银行业务、医疗保健、能源和公共设施等，这一普及程度使得网络攻击和数据泄漏等问题的发生更加频繁和严重。由于互联网的全球性和开放性质，任何人在任何地方都可以访问其内容，从而加剧了全球范围内的网络安全问题。随着互联网的不断发展，网络安全问题也不断涌现，尤其是在新兴技术领域如人工智能、物联网等领域，网络攻击方式也在不断创新和演变。网络安全问题已经成为一个重要的国际安全挑战，涉及人民生命财产安全、国家安全、经济安全和信息安全等多个方面。为了应对这个全球性的挑战，多个国际组织和政府机构已经开始加强合作，共同处理网络安全问题。例如，世界经济论坛、互联网工程任务组等各个机构已经开始就全球范围内的网络安全问题展开合作和探讨。此外，一些国际条约和公约也已经得到制定和签署，以确保国际社会在网络安全问题上形成共识和配合行动。

二、计算机网络安全防护技术的应用分析

（一）防火墙技术的应用

防火墙这项技术在现代计算机行业中已经成为一种普遍并且非常普遍的安全手段，能够为计算机网络系统的硬软件环境提供强有力的保护。在常规的情境中，防火墙技术在网络系统的边界位置起着关键作用，它结合了重点保护与普通保护的分层方法来确保网络系统的稳定运行和信息的安全性。利用防火墙技术可以精确地隔离计算机网络系统的外部侵害，借助信息与信号的连接，能够有效阻止外来攻击、入侵等不合法或异常迹象，确保网络内的信息数据传输始终安全和时效性。从防火墙技术的功能和作用角度考虑，它在基础上具有一定程度的阻隔和截获功能，确保计算机系统网络内外的顺畅隔离，并根据网络之间的距离或关键的网络边界层次来确保内部网络的结构和信息安全性[2]。考虑到这一情况，我们使用了过滤防火墙技术对网络系统中的数据

包执行高效率的筛选，确保精确挑选出安全的数据包，并利用数据包协议地址这类关键因素确保数据包信息源的安全性和可信度。

此外，利用应用级网关对在具体的网络服务协议框架下的数据特性进行深入分析和筛选，可以生成完备的安全报告，以明确应用级网关的防护能力及其所带来的效果，从而更精确地管理网络系统并确保其有效运行。某家市场公司自行开发的防火墙产品主要聚焦于网络安全问题，具备阻止每日数以亿计的系统安全漏洞的能力，有效阻止数亿次来自外界的不熟悉的Bot请求，确保数万用户网络安全无虞。为了满足国家标准的合规性要求，这款产品采用了人工智能和语义算法等先进技术。通过构建一个多引擎和多层次的智能系统框架，该产品能够更好地加固网络安全防护体系，并对网络系统可能存在的运行缺陷、外部攻击及信息泄漏的问题进行准确检测，同时也具备持续监测、扫描和过滤功能，并能精确提供防护，以适应各种业务场景的需求。这也进一步说明，基于实时监控、准确判断和提供有效的防护措施，防火墙技术是其应用的关键支撑。

（二）入侵检测技术的应用

入侵检测技术主要负责识别和侦测网络内部的异常行为和入侵行为。系统通过监测网络流量、分析网络数据包及其行为，能及时检测出可能存在的安全风险，并实施必要的防护措施。在其应用实践中，入侵检测系统有能力实时监控网络流量和行为，通过运用特定规定和算法，它能够识别并应对突发的异常行为。这样，网络管理员便能迅速作出反应，制定相应的警报，确保网络安全得到充分的保障。入侵检测技术能够通过深入分析网络流量和用户行为特征来探测不正常的行为模式。通过建立描述正常网络行为的基本模型，该系统可以检测出与常规行为模式不一致的行为，并将其标记为潜在的安全风险。这使得入侵检测系统能够及时捕捉到新的攻击模式和不明安全风险。入侵检测系统有能力利用攻击签名检测技术，以鉴定已知的攻击模式和对应的攻击编码。与已知攻击签名进行比对后，该检测系统能迅速确定并实施有效的攻击行为防护，从而确保对各类常见攻击手段的准确性和效果都达到了相对较高的水准。入侵检测系统有能力进行行为的诊断和异常状况的识别，进而鉴别出不完全符合常规行为模式的活动行为。通过构建一个用户和网络行为模型，该系统能识别出不正常行为，并将其识别为可能的入侵活动。这对于检测内部的威胁以及进行无休止的攻击活动具有极其关键的作用。

（三）加密认证技术的应用

数据加密技术的发展至今已具备强大的安全保障能力，对于保护一些复杂网络系统的内部结构，起着至关重要的作用。为了加强网络系统中数据源和协议信息的安全防护，我们采用了高数据加密技术，确保在密文转换、储存和传输过程中，这些数据和协议信息能够免受外部攻击。为了确保信息源和数据流的安全，数据加密技术的安全防护级别起到了关键的作用，这个水平与在密文转换中加密的密码长度有着密切的关联[3]。换句话说，在不同的网络状态下，加密文本的转换效果以及加密密码的防护性都会有所不同和存在一定的差别。在当前的时代，基于数据加密技术主要集中在对称加密与非对称密码这两大算法技术方向。在此基础上，我们使用了对称加密和解密算法，采用一致的钥匙控制网络系统的运行安全性。当我们采用非对称密码算法，其核心是基于数据包加密和解密时密钥的差异性，而与密钥进行深入互动的过程则是增强数据信息安全的核心手段。

（四）防恶意代码技术的应用

恶意代码包括病毒、蠕虫、木马、间谍软件等，可以通过各种途径传播，比如电子邮件附件、可移动设备、恶意网站等，一旦感染计算机或网络系统，恶意代码可能导致数据丢失、系统崩溃、隐私泄漏等严重后果，所以防恶意代码技术的应用，对保护计算机网络安全具有重要意义。

首先，入侵检测和防护系统是常用的防恶意代码技术之一，通过实时监测网络流量和系统行为，识别并阻止恶意代码的传播和攻击行为，可以通过特征检测、行为分析和模式识别等技术手段，快速发现并应对恶意代码的威胁，有效保护计算机网络的安全。其次，恶意代码通常通过电子邮件附件和恶意链接进行传播，为了防止用户受到恶意代码的侵害，可以采用邮件过滤和恶意链接检测技术，邮件过滤技术可以通过对邮件内容的分析和规则匹配，自动拦截包含恶意代码的邮件，恶意链接检测技术可以对URL（uniformresourcelocator）进行实时扫描，识别并拦截包含恶意代码的链接[4]。最后，沙箱技术和行为分析是一种先进的防恶意代码技术，通过在隔离环境中运行可疑程序，观察其行为和影响，识别恶意代码的特征和行为模式，可以有效防止恶意代码对主机系统的感染和损害，行为分析可以及时发现和响应新型的恶意代码攻击。

三、计算机网络技术在网络系统安全管理维护方面的实际应用

（一）建构完善安全系统，加强网络安全管理

为了确保计算机网络系统的平稳与安全运作，必须

建立一个科学而可依赖的安全架构，而系统的安全性正是计算机网络安全管理的核心焦点。为了应对上述问题，我们运用防火墙、数据加密和访问控制等先进互联网技术，构筑了一个全面的网络安全体系。这个体系能确保网络数据存储、传递以及系统的内外网边界结构都能稳定安全地运作。同时，还加强了对数据信息的分析、控制以及备份存储与加密工作，从而有效地避免了网络数据流运行的混乱和异常[5]。此外，鉴于互联网的开放和交互性，我们特别加强了对计算机网络系统中的各种漏洞和薄弱环节的管理，以确保网络系统不会受到外界的攻击，预防对网络系统的稳定和安全造成伤害，并持续提升网络的安全防护水平。

（二）灵活应用网络技术，加强系统性能配置管理

在从计算机网络系统的构建、执行应用，到后续的管理维护环节，我们都可以充分利用网络技术来加强对网络系统的配置、效能和潜在故障的管理。特别是，网络系统配置直接影响到计算机网络的运行状态，可以通过初始化或重新配置相应的网络系统，以提供各种稳定和可靠的网络系统服务。网络配置系统的建设主要聚焦于网络的监听与监控、管理、定义和信息筛选等核心通讯内容，从而为提供特定和必要的功能创造了平台，实现优化网络性能或增强系统的某一特定优势。在管理网络系统的性能时，重视的焦点是对网络系统中的资源信息的分配、互动及其利用情况进行深入的统计和有效评价[6]。如果对网络系统的某处进行检测并重新配置网络，通过数据收集、分析以及处理，我们能够更好地提升网络系统的性能管理。此外，为优化计算机网络系统的故障管理，我们利用网络科技对网络系统内部某些组件出现的故障进行了深入的跟踪和分析，以确保系统能够迅速并准确地识别故障来源，并解决故障。实际上，网络系统的故障可能是由众多组件的起源共同造成的。除了确切识别这些故障，我们也应该首先对其进行修复和完善，根据具体的故障原因来采纳相应的解决方法，以防相似的问题再次出现。当进行网络故障的管理时，我们需要全面地基于故障的分析检查、隔离问题和处理故障的细节方法进行操作。

（三）注重网络系统日常管理维护

在计算机网络管理中，专业团队应该拥有出色的网络防护觉悟，能够预先灵活地制定针对常出现的网络攻击事件的管理策略，并进行必要的预防性管理。面对网络攻击和其他行为，计算机网络系统的管理人员应依据具体攻击模式和实际状况进行预警和判断，以此为依据，决定并采纳适当的管理方案。在新的环境背景下，对数据信息的提前筛查和预防是全方位防御攻击的基本步骤。只有结合当前的具体情境，我们才会采取切实可行的应对策略，确保分布式的攻击预防行动得以无缝地执行，并提升各种网络安全技巧的实施效益。日常运营中，计算机管理专家们对网络系统进行常规的安全检测和系统的更新更新更新，他们还会定时进行恶意软件的检测，以加大系统缺陷的修复力度，并努力提升网络系统的安全性能作为基础。计算机网络管理与技术人员在各种类型的安全网络防护技术支持下，依赖先进的算法和智能化手段进行程序设计和模型构建。通过多种灵活的操作方式，他们能最大限度地满足各种用户需求，提供具有针对性的技术支持，从而确保计算机网络的安全和稳定性得到最大化。

结束语

在科技日益进步和日新月异的当代，计算机网络技术迅猛发展，对人类的日常生活和工作产生了深远的影响。同时，由于计算机网络安全问题持续不断地出现，网络安全面临了巨大的潜在危险。所以，在构建计算机网络的过程中，务必要加强网络的安全措施，以确保整个计算机网络能够稳定地运行。本文深入研究了计算机网络建设的准则和安全防护的核心要点，旨在为大家提供一系列计算机网络安全的防护建议，期望为大家构建一个更为安全的网络平台。

参考文献

[1]戴冬生.计算机网络数据库的安全管理研究[J].信息与电脑（理论版），2021，33（19）：226-228.

[2]黄明源.计算机网络系统安全维护策略研究[J].网络安全技术与应用，2021，（07）：167-168.

[3]杨光，蒋庆文.计算机网络安全的主要隐患及管理[J].网络安全技术与应用，2021，（05）：161-162.

[4]田华锋.计算机网络系统管理中信息安全及防护策略研究[J].中国管理信息化，2021，24（10）：203-204.

[5]范文峰，王龙飞.计算机网络数据库的安全管理工作研究[J].信息与电脑（理论版），2021，33（09）：200-202.

[6]张映勇.计算机网络信息安全管理系统面临的问题探讨[J].江苏通信，2021，37（02）：110-111.

[7]吴亚楠.计算机网络安全与防护策略探讨[J].济南职业学院学报，2021，（01）：115-118.

作者简介：李凯，1985年2月17日，男，汉，河北，秦皇岛市，初级职称，专业是电子工程-计算机及应用。