# 计算机网络信息安全及防护策略研究

刘法坤　王　璐　于　琪
国网山东省电力公司昌乐县供电公司　山东　潍坊　262400

**摘　要：**随着信息技术的快速发展，计算机网络已经成为我们生活和工作中不可或缺的一部分。由于网络的普及，计算机网络信息安全问题也日益严重。如何保护计算机网络信息的安全，防止个人和组织的信息被窃取和利用，已经成为当前亟待解决的问题。本文将探讨计算机网络信息安全及防护策略的相关问题。

**关键词：**计算机网络；信息安全；防护策略

引言：本文研究了计算机网络信息安全及防护策略。我们分析了计算机网络信息安全的各种威胁，如黑客攻击、病毒和恶意软件、网络钓鱼和缺乏安全意识和知识等，并探讨了各种防护策略，如加强网络安全意识教育、加强网络安全管理和维护、使用防病毒软件和防火墙和善用网络防护技术等。我们也讨论了如何通过建立完善的安全管理制度和加强用户安全意识来进一步提高计算机网络信息安全的防护能力。

## 1 计算机网络信息安全保护的重要性

（1）综合性： 计算机网络信息安全保护需要从多个层面进行考虑和实施，包括硬件设备、操作系统、网络协议、应用程序和人员行为等。只有综合考虑各种因素，制定相应的安全策略和措施，才能有效防御各种安全威胁。（2）全面性： 信息安全保护需要覆盖计算机网络中的所有环节和组成部分，包括网络边界、内部网络、终端设备和用户终端等。全面性意味着不仅要保护整个网络系统的安全，还要保护其中存储、传输和处理的各类数据和信息的安全。（3）预防性： 信息安全保护注重预防，旨在提前识别和遏制安全威胁，减少安全事件和风险的发生。通过强化边界防御、访问控制、身份验证等手段，及时发现和阻止潜在的攻击行为，最大限度地提高系统的安全性[1]。（4）可持续性： 计算机网络信息安全保护是一个长期工作，需要持续地投入和关注。安全保护措施需要定期检查、评估和更新，以确保其有效性和适应性。同时，人员培训和意识教育也是保持安全性的重要环节。（5）合规性： 信息安全保护需要符合相关法律法规和标准要求，确保业务活动在合法合规的框架下进行。合规性包括对个人隐私保护、数据保护、知识产权保护等方面的合规要求。（6）灵活性： 信息安全保护需要根据不同的网络环境、业务需求和风险评估进行定制化设计。不同的组织和个体所面临的安全威胁和需求各不相同，因此安全保护策略和措施需要具备灵活性，以适应不同的情况和变化。

## 2 计算机网络信息安全存在的问题

计算机网络已成为现代社会高速发展的必需品和重要基础设施，但同时也存在着一些安全问题，这些问题对于个人和机构来说具有深远的影响。（1）黑客攻击。黑客攻击是计算机网络信息安全存在的主要问题之一。黑客通过各种手段入侵计算机网络，窃取或破坏计算机信息，获取敏感信息或商业机密，给企业和个人带来严重的损失。（2）病毒和恶意软件。病毒是一种自我复制的程序，可以破坏计算机系统或网络，导致计算机系统或网络瘫痪。恶意软件是一种非法的程序，它会在计算机系统中秘密安装，非法获取计算机信息或破坏计算机系统。（3）网络钓鱼。网络钓鱼是指通过伪造电子邮件、网站等手段，诱骗用户输入个人信息或敏感信息，从而获取用户的隐私。（4）缺乏安全意识和知识。缺乏安全意识和知识也是计算机网络信息安全存在的问题之一。如果用户对网络安全知识不了解，就可能在使用计算机过程中不注意保护个人信息，容易受到黑客攻击或感染病毒。

## 3 计算机网络信息安全防护策略

### 3.1 加强网络安全意识教育

（1）增强人们对潜在威胁的认知。很多人对网络安全的了解相对较少，缺乏对网络攻击、恶意软件和网络钓鱼等常见威胁的认识。通过网络安全意识教育，可以向人们普及各种网络安全威胁的类型、工作原理和防范方法。这样，人们就能更好地识别和预防潜在的网络安全风险，提高自己和组织的安全水平。（2）培养良好的网络行为习惯。良好的网络行为习惯对于保护个人和组织的安全至关重要。通过网络安全意识教育，可以教育人们遵循安全最佳实践，如定期更新操作系统和应用程序、使用强密码、不轻易点击可疑链接等。这样的良好习惯可以帮助人们建立起强大的网络防线，减少受到安

全威胁的风险[2]。（3）提升组织的安全意识和整体安全水平。组织内部的员工是信息安全的重要环节，他们的行为直接影响着组织的安全性。通过向员工提供网络安全意识教育，使他们了解网络安全的重要性和自身在保护信息安全方面的责任。同时，也可以向员工介绍组织的安全政策和流程，并培养他们主动参与和支持组织安全工作的意识。（4）采取多种形式和渠道，以提高教育的效果和覆盖范围。可以通过组织网络安全培训课程、举办安全意识活动和演习，以及发布安全教育资讯等方式来进行教育。同时，借助互联网和社交媒体等新兴渠道，将网络安全知识传播给更广大的受众，提高公众对网络安全的认知和意识。

3.2 加强网络安全管理和维护

（1）建立健全的网络安全管理体系。这包括制定完善的网络安全管理制度、安全策略和安全标准等，以确保网络安全管理的有效性和规范化。同时，还需要建立完善的安全审计机制，对网络安全情况进行实时监控和审计，及时发现和解决网络安全问题。（2）加强安全流程管理。这包括对网络系统的访问控制、数据传输加密、防病毒、防黑客攻击等方面进行全面管理。需要制定完善的安全操作规程和安全流程，确保各项安全措施得到有效实施。（3）定期升级和更新软件补丁。软件是网络攻击的主要目标之一，软件的漏洞往往会被黑客利用，因此需要及时修复和更新软件，以避免漏洞被攻击者利用[3]。（4）定期备份数据。数据是计算机网络信息安全的重点保护对象，因此需要定期备份数据，以防止数据丢失或损坏。（5）建立完善的应急响应机制。在网络安全事件发生时，能够快速、有效地进行响应和处理，可以最大限度地减少损失和影响。

3.3 使用防病毒软件和防火墙

（1）使用防病毒软件非常重要。它可以在病毒和恶意软件入侵计算机系统之前进行检测和清除，避免计算机系统和网络受到危害。防病毒软件可以对计算机系统进行全面或自定义扫描，检测和清除计算机系统中的病毒、木马、广告程序等恶意程序。同时，防病毒软件还可以实时监控计算机系统的文件和应用程序，一旦发现异常行为，可以立即阻止病毒和恶意软件的入侵。（2）使用防火墙也是非常重要的。它可以监控网络数据流，阻止未经授权的访问和攻击，保护网络的安全和稳定运行。同时，防火墙还可以对网络流量进行过滤，阻止恶意软件通过网络传播，进一步保护计算机系统和网络的安全。（3）对于个人用户来说，使用防病毒软件和防火墙还可以提高自身的网络安全意识和行为。通过使用防病毒软件和防火墙，用户可以更好地了解网络安全威胁和防护措施，并采取相应的安全操作和行为。例如，不随意下载和安装未知来源的软件，不随意打开未知来源的链接等，避免遭受网络攻击和危害。

3.4 善用网络防护技术

（1）善用防火墙技术。防火墙是保护计算机系统和网络的重要屏障，它可以在计算机系统和网络之间建立一个安全通道，阻止未经授权的访问和攻击。防火墙可以根据不同的安全策略和安全规则对网络数据流进行过滤和监控，确保只有合法的数据流量可以通过防火墙。同时，防火墙还可以对网络流量进行统计和分析，帮助用户了解网络流量和安全状况。（2）善用加密技术。加密技术可以保护计算机系统和网络中的数据传输和存储的安全。在数据传输过程中，通过加密技术可以将数据转化为密文，防止数据被非法获取和篡改。在数据存储过程中，通过加密技术可以将数据转化为密文，防止数据被非法访问和泄露。同时，加密技术还可以提高数据的完整性和可信性，确保数据在传输和存储过程中的安全和可靠性。（3）善用入侵检测技术。入侵检测技术可以监测计算机系统和网络中的异常行为和攻击行为，并及时报警和响应。入侵检测技术可以通过分析网络流量、系统日志等方式获取计算机系统和网络的安全状态信息，并通过安全策略和规则进行判断和识别。如果发现异常行为或攻击行为，入侵检测系统可以及时发出警报，并采取相应的安全措施进行响应，防止攻击行为的进一步扩散和危害。

3.5 增加身份验证和访问控制功能

（1）确认用户的身份和权限，只有经过身份验证的用户才能访问和操作计算机系统和网络。身份验证可以通过多种方式实现，例如用户名和密码、数字证书、指纹识别等。这些身份验证方式可以确保只有经过授权的用户才能访问和操作计算机系统和网络，避免未经授权的用户访问和操作计算机系统和网络。（2）可以限制用户的访问权限，只有经过授权的用户才能访问和操作计算机系统和网络。访问控制可以通过多种方式实现，例如基于角色的访问控制、基于属性的访问控制等。这些访问控制方式可以根据用户的角色和属性等条件限制用户的访问权限，确保只有经过授权的用户才能访问和操作计算机系统和网络，避免未经授权的用户访问和操作计算机系统和网络。

3.6 定期组织网络安全演练

通过定期组织网络攻防演练，可以模拟实际网络攻击场景，让网络安全管理人员及时发现和处理安全威

胁，提高网络安全管理的应对能力和反应速度。（1）增强网络安全管理人员的安全意识。通过模拟实际网络攻击场景，可以让网络安全管理人员更加直观地了解网络攻击的手段和方式，从而提高对网络安全的认识和了解。同时，通过演练中的攻防对抗，可以让网络安全管理人员更加熟悉和了解网络安全防护措施的有效性，提高安全防范的水平[4]。（2）可以锻炼网络安全管理人员的应对能力和反应速度。在演练中，可以模拟各种网络攻击场景，包括不同类型的病毒攻击、黑客攻击、网络钓鱼等，让网络安全管理人员在第一时间发现和处理这些安全威胁，提高应对能力和反应速度。同时，通过演练中的攻防对抗，可以让网络安全管理人员更加熟悉和了解网络攻击的手段和方式，提高对网络攻击的识别和应对能力。（3）还可以加强网络安全管理团队的协作和交流。在演练中，可以组织不同部门和不同岗位的网络安全管理人员共同参与，提高团队协作和交流能力。通过演练中的攻防对抗，可以让不同部门的网络安全管理人员更加了解彼此的工作和职责，增强团队协作和交流能力，提高网络安全管理的整体水平。

3.7 实施网络流量监控和审计

通过监控和审计网络流量，可以及时发现异常活动和潜在的安全威胁，从而采取相应的安全措施进行防范和应对。（1）实施网络流量监控和审计可以监测网络流量中的异常行为和活动。通过网络流量监控，可以实时监测网络中的数据流和数据包，分析其行为和活动是否正常。如果发现异常行为或活动，可以及时报警并采取相应的安全措施进行应对，防止安全事件的发生和扩大。（2）可以记录网络活动和事件，提供证据用于调查和追踪安全事件。在网络流量监控和审计的过程中，可以记录网络中的所有活动和事件，包括用户访问、数据传输、网络流量等。这些记录可以作为证据用于调查和追踪安全事件，了解安全事件的产生原因、过程和影响，从而采取相应的措施进行应对和防范。（3）还可以提高网络安全管理的透明度和可控性。通过网络流量监控和审计，可以了解网络中的所有活动和事件，包括正常的和异常的，从而更加透明地了解网络状况。同时，通过网络流量监控和审计，可以掌握网络中的潜在安全威胁和安全事件，从而更加有效地进行安全管理。

结语：综上所述，本文提出了加强网络安全管理和维护的重要性，并探讨了几个关键策略，包括黑客攻击、病毒和恶意软件、网络钓鱼和缺乏安全意识和知识等，并探讨了各种防护策略，如加强网络安全意识教育、加强网络安全管理和维护、使用防病毒软件和防火墙和善用网络防护技术等。这些策略有助于组织提高对网络安全威胁的防范能力，保障计算机网络信息的安全性和可靠性。然而，网络安全领域仍然面临着不断发展和变化的挑战，因此，持续关注最新的安全威胁和技术发展，并及时调整和改进防护策略，才能有效应对网络安全风险，确保网络环境的安全与稳定。

**参考文献**

[1]蔡彬彬，孙忠辉.计算机网络信息安全问题及防护策略研究[J].长春理工大学学报（自然科学版），2019，42（3）：128-132；137.

[2]史伟民. 计算机网络信息安全及防护策略研究[J]. 通信电源技术,2021,38(5):186-188.

[3]孟东雪. 计算机网络信息安全及防护策略研究[J]. 数码世界,2019(4):229.

[4]辛培成. 大数据时代计算机网络信息安全及防护策略研究[J]. 中国新通信,2021,23(3):131-132.