国际教育论坛
Journal of International Education Forum
第 6 卷◆第 9 期◆版本 1.0◆2024 年
文章类型：论文|刊号 ISSN: 2705-120X（O） EISSN: 2705-1196（P）

计算机网络信息安全及其防护策略的研究

开赛尔·吾斯曼
新疆职业大学 信息技术学院 830011

DOI:10.12238/jief.v6i9.10264

[摘 要] 信息化时代的快速发展，对人们的生产生活方式带来了巨大的影响，计算机网络逐渐成为人们日常生活不可分割的一部分。但是，在计算机网络为人们提供便利的同时，也潜在着一定的安全风险，由于使用计算机网络时会涉及到大量的用户个人信息，因此，如果出现网络信息安全问题，不但会导致用户的隐私被泄露，严重的还会造成巨大的财产损失。因此，无轮是工作中还是生活中，在应用计算机网络的过程中，要不断提升对网络信息安全问题的重视程度，进而做到有效防护。基于此，文章首先分析了保障计算机网络信息安全的重要性，然后针对常见的网络安全风险问题，提出了具体的信息安全防护措施，以供参考。

[关键词] 计算机；网络信息安全；防护

Research on Computer Network Information Security and its Protection Strategy

Kaiser Wusman
Xinjiang Vocational University，School of Information Technology 830011

[Abstract] The rapid development of the information age has brought a great impact on people's production and life style，and the computer network has gradually become an integral part of People's Daily life. However，in the computer network provides convenience for people at the same time，also potential security risks，because the use of computer network will involve a lot of user personal information，therefore，if the network information security problems，not only can lead to the user's privacy is leaked，serious also can cause huge property losses. Therefore，no wheel is in work or life，in the process of the application of computer network，we should constantly improve the attention to the network information security issues，so as to achieve effective protection. Based on this，the paper first analyzes the importance of ensuring computer network information security，and then puts forward specific information security protection measures for the common network security risk problems for reference.

[Key words] Computer；network information security and protection

1.计算机网络信息安全及其防护的重要性

1.1 维持用户信息安全

随着信息技术的快速发展，计算机网络得到了广泛的普及与应用，这为人们的生产生活提供了极大的便利，但是计算机网络还面临着巨大的信息安全威胁，诸如非法访问、黑客攻击、系统漏洞等问题时刻困扰着人们的信息安全，一旦信息遭到泄露、篡改，必将会给人们的生产生活带来极大的不便。如果网络平台无法保证用户的信息安全，必然会造成大量的用户流失，网络数据的流通与共享就无从谈起[1]。因此，互联网企业必须加强网络安全维护工作，确保用户的信息不会出现泄漏、篡改等问题，在提升网络服务质量的同时，为广大用户提供更好的网络使用体验，只有这样，互联网平台才能与用户建立信任，才能推动计算机网络的健康良性发展。

1.2 保障网络数据准确

做好网络信息安全维护工作，能够有效提升数据信息的准确性。互联网每时每刻都在传输大量的数据资料，如果数据传输过程中出现安全漏洞，可能导致整个数据系统出现错误，严重者使得整个网络出现瘫痪，给企业、用户造成巨大的损失。因此，网络从业者必须对网络信息安全给予高度重视，采用数据加密、防火墙、杀毒软件等，全面提升计算机网络的安全水

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

文章类型：论文|刊号 ISSN: 2705-120X（O） EISSN: 2705-1196（P）

平，降低信息被泄露、被盗窃、被篡改的可能，从根本上降低数据安全事故的发生概率。互联网具有较强的开放性特征，每个网络用户都可以在互联网上分享、查阅、下载网络信息，创造信息的数据财富，在此过程中，互联网平台应该建立强大的安全防御系统，来抵御网络病毒、网络黑客的攻击，保证网络数据的精准性、可靠性。

2.计算机网络信息存在的安全问题

2.1 安全制度不[1]够健全

安全管理体系的不足主要体现在企业或组织未能建立一套完整且系统的网络信息安全管理体系，由此造成网络安全防护策略的缺失，使得在面对不断演变的网络安全难题时显得力不从心。许多机构在构建安全政策时，往往侧重于技术方面的保护措施，而忽略了管理层面的制度完善，比如缺少严谨的访问权限管理、数据备份策略以及突发事件应对流程。某些企业在这方面的管理力度显得不够，缺乏定期审视与优化安全制度执行情况的机制，因此未能及时发现并修补安全上的疏漏。在某些企业内部，员工对于网络安全的认识存在不足，缺乏专门设计的教育与评估活动，导致既定规则成为摆设，无法有效抵御由人为错误或蓄意入侵所引发的安全威胁。鉴于网络安全规范与法律框架的持续演变，某些机构未能适时修订并强化其安全政策，从而使得现有规则陈旧，无力抵御新兴的安全难题。

2.2 存在安全隐患

网络结构繁复且相互连接紧密，这显著增加了系统遭受内外部攻击的风险。在互联网架构中，若某个节点存在安全性缺陷，入侵者便能借此缺陷实施未经授权的访问、盗取信息，或策动后续的侵袭行动。举例而言，过时的软件、脆弱的密码以及未修补的系统均能构成可被利用的漏洞。伴随物联网装置与云端运算技术的普及，网络的界定日益暧昧不明，从而扩大了系统的可攻击范围，使得原有的安全防御手段难以实现全方位的保护。在网络空间内，充斥着众多未经严格验证的第三方应用程序与扩展组件，这些元素有可能暗藏有害程式或隐蔽通道，对整体网络安全构成不确定性威胁。社交工程攻击、欺诈性的电子邮件和其他方法正变得日益狡猾，轻易就能诱使用户暴露重要数据，从而显著扩展安全漏洞的范畴。

2.3 计算机病毒风险

计算机病毒是一种能够自我繁衍且具有恶意的程式，常透过网络、电子邮件等媒介侵入電腦系統。一旦遭受病毒感染，系统便可能执行多种破坏活动，如删除文件、篡改资料、盗取机密信息，乃至全面掌控被感染的设备。面对日益复杂的网络生态，病毒的传播速率与影响规模呈现显著增长态势，特别是在互联网接入设备数量持续攀升的背景下，病毒得以迅速蔓延，对广泛的计算平台构成威胁。当代病毒展现出高度的智能化与隐秘性，其不仅能够规避传统的反病毒软件及防火墙防护，还善于利用系统缺陷和用户操作的疏漏实施侵袭。病毒创造者持续研发新的病毒类型，如勒索软件、蠕虫病毒及特洛伊木马，这些病毒通过加密用户资料、遥控设备运作或盗取银行账号细节等方法，导致重大财务损失与个人机密外泄。计算机恶意软件不仅对个人构成威胁，也能够对企业的核心运营及政府的关键基础设施发起攻击，引发业务停摆、机密信息外泄，乃至危及国家的防御体系与战略利益。

3.计算机网络信息安全及其防护策略

3.1 完善管理体系

一个完善的管理架构不仅需要确立清晰的安全方针与规范，还需整合风险分析、危机处理预案、人员教育与周期性稽核等多重元素。企业应建立详尽的安全指南，明确界定数据存取权限、密码维护规则、设备操作规程以及网络活动的规范，旨在确保所有员工均能恪守一致的安全准则[2]。应当周期性地执行风险评价，辨识并评估可能的安全风险，并依据评价成果实施相应的防御策略，比如更新安全程序、修复系统缺陷等。还需构建敏捷的危机应对系统，以保证一旦出现安全问题便能即时作出对策，最小化损害。员工教育在组织管理架构内具有重要作用，借助周期性的安全培训与实操练习，旨在强化每位成员的安全认知及应急处理能力，以此减少因人为疏忽引发的安全隐患。管理框架理应内置周期性的安全性稽核与评价机制，旨在保证所有安全策略的实效性与不断优化。这些策略相辅相成，共同建立了一个周全且灵活的管理框架，旨在显著增强计算机网络信息的安全防护能力，抵御各种网络安全风险。

3.2 采用加密技术

加密机制涉及将原始信息，即明文，经过特定算法处理后转变为不可读的密文形式，以此确保在未授权的情况下，即便数据被截获，其内容也无法被解读，从而达到保护信息安全的目的，有效预防信息的泄露与篡改行为。这些方法借助加密通道确保数据的完整性和私密性，从而提升了数据传递的安全性。在数据储存领域，加密策略对部署于硬盘及云端等载体的机密资讯实施加密操作，以防范因硬件失窃或损坏引发的信息外泄事件。对数据库、加密文件系统及类似架构是确保静止数据安全的关键策略。在用户认证机制中，可以利用加密方法，结合加密后的密码及生物特征数据，以确保唯有经过授权的个体方能接入系统与获取资料，从而增强整体安全防护水平。加密机制亦能与多重身份验证、数字印鉴等安全策略协同运作，以强化全面的保护效能。借助恰当的加密策略，可以显著增强计算机网络中信息的安全防护能力，防止数据遭受各类恶意入侵与非法获取，确保信息的保密性、数据的完整性以及服务的可得性。

3.3 检测入侵行为

入侵检测机制一般被区分为网络基线与主机基线两种模

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

文章类型：论文|刊号 ISSN: 2705-120X（O） EISSN: 2705-1196（P）

式，网络基线 IDS 负责监视全网的信息流通，而主机基线 IDS 则聚焦于个别装置的运作动态。检测策略主要涵盖基于特征的检测与基于偏离常态的检测两大类。基于签名的方法凭借其能力快速对预定义的攻击特征进行匹配，从而有效辨识已知的威胁，然而，其在应对未知或创新攻击时显得力不从心[3]；相比之下，基于异常检测策略构建了一个正常操作的基准模型，旨在识别与常态显著偏离的异常行为，展现出更强的灵活性。不过，这一方法也可能导致较高的误报率。为了提升检测精准度，入侵检测系统常集成多样化的技术策略，如机器学习算法与行为模式识别，并与防火墙、加密机制等其他网络安全措施相辅相成，构建多维度的防御架构。迅速的事件应对与系统的持续优化是维持入侵检测系统高效运作的关键步骤。面对高误报频率与复杂性等难题，伴随技术的持续演进，入侵检测系统在强化网络安全防护、预防信息泄露及防止系统遭受攻击方面扮演着极为重要的作用。

3.4 使用防火墙技术

防火墙部署于网络的入口与出口，其关键功能在于监视并管理穿行网络的数据传输，以实现隔离与筛选，有效阻挡未获准的访问尝试及潜在的安全风险。防火墙技术主要有包过滤、状态检测以及应用层防火墙三类模式。包过滤防火墙根据事前设定的准则，评估每一个数据包的发源地标识、目的地标识、端点等细节，以此判断是否应准予其通行。状态检查防火墙不仅评估单一数据封包，还会监控整个会话流程以追踪状态，从而实现更为精进的安全管理措施。应用层防火墙渗透至应用层级，具备识别及遏制针对具体应用的侵袭的能力，例如 SQL 注入与跨站脚本攻击。该方法亦能借助代理伺服器隐匿内联网布局，提升安全性。

3.5 优化日常管理

网络安全的日常管理需要建立完善的安全管理制度，如制定详细的安全策略、访问控制规则和操作规范，这些制度应当明确每个岗位的安全责任和操作权限，确保网络资源的合理使用和敏感信息的有效保护。网络管理员必须对网络设备和系统进行定期检查和维护，及时发现和修复安全漏洞，更新防护措施，以抵御新的安全威胁。日志记录和监控也是日常管理的重要内容，通过实时监控网络流量、系统状态和用户行为，能够及时发现异常活动，并采取迅速的应对措施。优化日常管理还要求加强对网络用户的安全教育和培训，使其具备基本的安全意识和操作技能，避免因人为疏忽导致的安全事件。

3.6 提升人员水平

确保网络系统的安全并不仅仅是通过技术措施来实现，还需要有专门知识和安全意识的人员负责管理与维护工作。因此，定期为网络管理员、技术支持团队成员以及一般用户举办网络安全教育课程显得极为重要。培训课程需囊括当下最为尖端的安全难题、防御方法与安全软件的操作，旨在使参与者熟练掌握先进的安全技艺，同时培养其解决紧急状况的本领。增强人员能力时，务必强调培育其安全认知，教导其辨识网络钓鱼、社会工程学等普遍威胁策略，以防因操作失误引发安全隐患。企业能够通过实施认证机制，激励员工获取相应的网络安保证书，以增强其专业知识并保证团队的技术实力始终保持在业界的前沿位置。为了不断强化员工的专业技能，有必要定期组织内部模拟演练，通过仿真真实的安全事故场景，以评估并增强员工的危机应对能力。

3.7 提高监管力度

面对日益复杂的网络环境与多变的安全威胁，单纯依赖技术手段已不足以应对全部难题，亟需强化监管措施以提升网络防御能力。政府及其关联的监管机构需制定并执行严谨的信息安全法律条文，以保证网络服务遵从国家规范，并对触犯规则的活动施以重罚。这涵盖了实施数据保护法规、打击网络犯罪以及追究信息泄露责任等方面。监管机关需精心构建并实施全面的网络安全性评估体系，周期性地对核心网络设施与组织执行安全性检验，识别并处理隐匿的安全问题。还应提倡企业与机构构建内部的安全管理架构，并实施周期性的自我评估及第三方审核，旨在维持对网络安全的长效监督与优化。对于网络用户而言，提升自我防护意识极为重要，主动学习网络安全技巧，谨防点击未知链接与接收可疑文件。借助多方面协作与全面监督，能够显著增强网络总体安全性，降低安全事件的出现频率，保障用户隐私及数据安全。

4.小结

综上所述，在当今的大数据时代背景下，计算机网络已经成为人们工作和生活中不可或缺的重要工具，同时，伴随数据量的不断增加，对于网络信息安全的防护也成为社会各界广泛关注的重要课题。面对网络系统中的潜在安全风险，计算机使用者需要科学识别网络安全风险因素，并采取具有针对性的措施对网络信息进行有效防护，减少信息泄露或丢失的问题，进而保证用户信息的安全性。

[参考文献]

[1]李豪杰.计算机网络信息安全防护策略及评估算法分析[J].电脑编程技巧与维护，2023，（12）：168-170.

[2]王梓晗.大数据背景下的网络信息安全研究[J].中国新通信，2023，25（20）：104-106+136.

[3]陆叶.大数据时代计算机网络信息安全问题的解决路径[J].百科知识，2023，（33）：42-43.

[4]闫军.计算机网络中的信息安全技术应用[J].集成电路应用，2023，40（10）：174-175.

[5]赵圣隆，宋文彬.计算机网络信息安全及防护策略分析[J].电子技术，2023，52（10）：178-179.

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.