加强计算机网络工程安全的措施分析

刘忠伟

（中国广电山东网络有限公司潍坊市分公司，山东 潍坊 261061）

摘 要 当今社会已经步入信息技术高速发展阶段，网络的普及，计算机技术的广泛应用，二者的结合为人们的生活、生产带来了较大的便利性，同时关于计算机网络工程安全的问题也越来越得到人们的关注，但是由于随着网络技术以及计算机的不断更新换代，早期网络建设安全系数越来越低，难以满足人们对于安全的高要求，黑客攻击、数据非法窃取事件高发，所以加强计算机网络工程安全成了亟待解决的难题。本文在对计算机网络工程安全进行概述以后，探讨计算机网络工程面临的安全问题，进而提出行之有效的措施。

关键词 计算机 网络工程 安全措施

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1007-0745(2022)08-0019-03

信息技术是促进各行各业发展的动力，随着系统规模不断扩大，集成度也日益提高，在计算机网络技术安全方面同样也提出了较高要求，特别是伴随网络一起发展起来的黑客技术，导致用户数据及信息非法泄露，带来的经济损失难以估量。再加之计算机网络开发性、共享性特点明显，处于虚拟环境下，安全防护及管理成了难点，面临的挑战也越来越大。人工智能技术虽然也在很大程度上给予了计算机网络工程一定的安全保护，但依然需要站在多维角度考虑安全问题，进而确保计算机网络工程更好地运行。基于此，本文重点针对如何加强计算机网络工程安全进行了分析，通过给予的几点有效建议，旨在为计算机网络工程安全问题的解决提供新思路，打造安全可靠的运行环境。

1 计算机网络工程安全概述

1.1 计算机网络工程安全的内涵

计算机网络工程安全内涵的分析主要从以下两个层面着手：一是基于计算机使用程序，确保其安全性更高；二是基于计算机指令系统，体现其安全性问题。[1]在数据处理系统、计算机管理技术中，计算机网络工程更加安全才能确保二者更好地运行，避免软件、硬件、信息、数据免受损坏。计算机网络工程安全内容主要包含五个层面：一是网络安全，网络控制是网络安全保护的核心，分析各个环节的 IP 是不是合法合规，若未授权，不允许入站，以达到网络控制安全受到保护的目的；二是计算机系统安全，此环节主要是病毒、黑客带来的威胁，若要确保系统安全，需要对易受病毒侵害的端口给予防范，以免被黑客攻击，计算机系统安全运行；三是用户安全，是指用户在访问以及使用系统时是否有权限，基于类别设置权限，只允许用户身份认证以后，访问以及使用权限以内的数据及信息，确保用户安全；四是计算机应用程序安全，是指用户、数据安全，上一级能够对下级资源进行存取，下级及同级间数据获取会受取权限局限性；五是信息数据安全，是指信息数据机密性要得到保护，通过加密处理确保数据不被非法窃取。

1.2 计算机网络工程安全的特点

1. 脆弱性。互联网最大的特点就是共享性、开放性、无边界性，全球网络信息及数据均可共享及使用，计算机网络技术更新换代速度较快，早期网络建设难以满足人们在网络信息安全方面提出的高要求，系统极易被黑客非法攻击，数据泄露问题也时常发生。开放性与脆弱性是共存的，网络开放程度越来越高，表明安全性也会越来越脆弱，若网络安全管理不到位，极易被攻击，轻者文件损害，重者网络瘫痪。

2. 突发性。计算机病毒复制性较强，在网络中传播速度较快，对于计算机程序、数据破坏性较大，一些级别较高的病毒很难被发现，潜伏期较长，会突然间被触发，造成计算网络工程安全问题的发生，日常防范就显得极其重要了。

3. 全球性。网络环境是开放的，不会受到空间局限性，所以病毒会无国界传播，引发全球性计算机网络工程安全问题，若某一国网络安全问题较为严重，波及的是全球网络系统，国家间强化交流与合作，做

好计算机网络工程安全防范也是非常有必要的。

2 计算机网络工程面临的安全问题

2.1 系统操作方面的安全问题

虽然在网络信息技术快速发展进程中，我国计算机网络工程结构也在不断进行优化与改善，这在很大程度上推动了计算机网络工程在各行各业的广泛应用。[2] 但是关于操作过程中的安全问题也越来越突出，这与计算机网络工程具备较强开放性特点有着密切的关系，极易在外界环境影响下导致多种多样网络安全问题的发生。例如计算机网络工程操作人员系统操作时不规范，导致系统漏洞较多，为黑客非法攻击提供了机会，将病毒在不知情的情况下植入计算机系统内，不仅会对用户隐私造成较大危害，而且使人们的经济利益受损。

2.2 设备及软件方面的安全问题

软硬件是计算机网络工程中极其关键的部分，如果软件、硬件存在问题，计算机网络工程安全运行便会受到较大影响，安全性难以得到保障。不管是软件的安装，还是设备的运行，通常情况下基于用户使用计算机的需求，由软件市场搜索一些与用户需求相匹配的软件或者硬件，然后将其下载至用户计算机中。下载的这些软件若自身安全隐患较大，那么必然会威胁到计算机的运行及使用。从目前的实际情况而言，计算机运行的网络环境存在较大的安全问题，而且市场中开发的应用软件质量参差不齐，种类繁多，在质量无法得到保证的情况下，安全隐患发生的概率自然也会较大，影响计算机的安全运行，用户在计算机体验方面也会越来越差，学习以及工作均会受到消极影响。

2.3 网络安全管理方面的问题

网络技术发展的速度非常快，计算机网络工程在各行各业生产中应用的范围也越来越广，由于涉及面较大，规模也逐渐拓展，网络安全管理的难度自然也会逐渐增大，很多不安全因素难以在第一时间被发现，进而影响到了计算机网络工程运行的安全性。[3] 再加之工作人员在网络安全技术方面有很大的提升空间，专业知识以及技术、技能的欠缺，同样也会导致问题发生以后难以做到及时处理，甚至严重时会造成问题扩大化，用户隐私、经济利益受到较大的损害。随着网络信息技术发展速度日益加快，黑客在入侵网络方面的技术也越来越高明，为计算机网络工程安全隐患的发生埋下了伏笔。除此之外，大多数用户在使用计算机网络时不重视安全问题，安全管理技术有很大的提升空间，技术人员未做到根据互联网具体情况将相应的技术进行优化与完善，难以满足复杂多变的网络环境提出的高要求。总之，网络安全管理水平普遍较低，安全性无法得到有效提高，不法分子便利用这些缺陷趁机攻击网络系统，引发网络信息泄露问题，对计算机网络工程造成不利影响。

2.4 网络硬件的配置不协调

文件服务器是计算机网络信息系统的核心部分，主要是为了保证计算机网络运行更加稳定。但当前大多数用户使用的计算机网络硬件在配置方面不达标，不协调、不完善问题较为严重，使整个网络系统运行质量较差，极易造成用户计算机网络硬件被非法损坏。与此同时有些部门以及工作人员未给予网络应用需求较高的重视度，不管是硬件型号的选择，还是网络设计环节缺少必要的关注度，阻碍了用户计算机更好的运行，影响了网络扩充性。

3 加强计算机网络工程安全的措施

3.1 提高计算机系统的安全性能

计算机网络工程运行更加有序顺利，就要根据具体情况给予计算机网络程序优化高度重视，推进安全防护性的提升，进而达到有效解决安全问题的目的。[4] 网络工程建设时，要根据不同因素以及条件对计算机网络程序进行精心设计，构建健全的安全防护系统，提高用户信息安全性。首先是防火墙技术的合理运用，实现不同类型危险源的有效防御，降低外界不明信息非法侵入计算机网络系统的概率。防火墙防御方面功能强大，可对外界及本地网络进行有效管控，危害信息被隔离在外，此过程中用户依然可以正常使用计算机，防火墙会统计计算机网络通信量，将安全信息导入，危险信息直接删除，同时还能够设置计算机浏览器，屏蔽或者拒访危险网站、链接，对用户隐私以及数据起到保护作用。

3.2 做好计算机病毒的防范

计算机也极易被病毒攻击，而此时用户要将自身防范意识提高，使用计算机时可安排杀毒软件，降低病毒及危险因素侵害的概率，同时还要将文件进行备份，以免计算机有病毒侵入以后，一些重要文件能够保存下来。选择杀毒软件时，用户一定要保证其是正规的，不安全网站、链接不浏览，用户更不要随意去点击奇怪链接，这也是对计算机病毒防范非常好的方法。工作人员也要在网络安全管理方面强化意识，定期对计算机网络运行情况检查，对安全漏洞及时排查，发现漏洞要在第一时间进行修补。

3.3 防止黑客入侵计算机系统

黑客对计算机网络系统进行攻击时要满足诸多条件，暴力破解以及利用其他非法手段获取用户身份认证信息是常用的入侵方法。[5] 最近几年，非法分子借助网络盗用用户资料，使得用户经济损失严重，隐私也被泄露，也有些黑客会通过计算机端口盗取用户密码、账号，使计算机用户系统被破坏。所以要想规避黑客入侵风险，用户可在计算机使用时做好自我防范，定期更改密码，运用防火墙技术做好病毒隔离，严控网络访问计算机的渠道及权限。

3.4 及时做好文件备份垃圾文件的清除

通常情况下，用户会将重要文件保存在计算机中，为确保安全，用户可将这些文件进行拷贝，放置在与网络不接触的存储设备中，避免病毒侵入时导致计算机格式化，文件受到损害。[6] 同时要将计算机中的文件进行区分，不随意点击可疑文件，这些文件也许被木马病毒感染，如果运行了文件极易造成计算机系统受损，严重时瘫痪。为此，用户要定期清理计算机中的垃圾文件，确保计算机运行效率更高。除此之外，用户还应该检测病毒入侵情况，恶意病毒攻击行为可采用防火墙拦截，确保计算机网络工程运行更加安全可靠。如果检测时发现存在网络攻击情况，就应该马上采取应对措施，例如将硬盘进行格式化，将网络断开等，尽可能降低损失。

3.5 做好网络工程管理人员的培训

网络工程管理人员是确保计算机网络工程运行安全的重要参与者，不断强化网络管理人员培训工作，能够帮助他们掌握最新的防范方法，进而做到科学合理地使用病毒防御手段，将病毒拒之门外。同时通过参加各种培训，网络工作管理人员工作能力得到不断提高，在计算机网络安全维护制度制定方面也能够提出更好的建议，在确保规范化管理，促进计算机网络系统安全性提高的同时，使其运行环境更加稳定。同时，为确保计算机网络工程使用安全及稳定，相关部门要在强化人员培训的过程中，给予相应监督管理，切实提高人员网络安全防范意识，能够做到有效维护网络工程安全性，推进计算机网络工程良性发展。

3.6 完善相应的法律法规

由于当前法律法规不完善，进而造成诸多恶意软件的存在，对计算机系统安全造成较大威胁。一些非法分子通过信息技术的运用窃取一些重要资源，以谋私利。黑客技术逐渐成熟，也为犯罪分子创造了范围的条件，增加了木马病毒侵害计算机网络工程的风险。为此，有关部门要根据实际情况，结合现状，在法律法规方面给予相应的制约，例如完善《计算机网络安全法》等条款，针对恶意传播木马、病毒的行为给予严厉打击及惩处，通过权威性的法律震慑不法分子，加大处罚的力度，增加黑客侵害计算机系统行为的成本，以此来减少非法入侵事件的发生，确保用户隐私权得到保护，经济利益得到保证。

3.7 增加访问控制的难度

计算机使用时，用户访问过程中要通过密码、账号的输入方可浏览，虽然在很多用户看来有些麻烦，但可以确保信息安全。用户有账号、密码设置时要尽可能复杂化，特别是密码要将大小写、符号、数字混合使用，将密码破解难度不断加大。需要注意的是，密码设置应避免使用生日、姓名全拼或者重复数字等。除此之外，在计算机使用过程中，用户可采用动态密码、账户设置的方法完成登录，这样也能够在很大程度上确保个人信息的安全性。

4 结语

总而言之，只有保证计算机网络工程更加安全地运行，才能维护用户隐私权，使用户计算机网络工程使用时安全性更高。为此，相关部门应该根据具体情况，对计算机网络安全系统进一步完善，将更多的目光放在计算机软件、硬件安全管理层面，确保计算机网络安全管理整体水平的提升，同时工作人员还要运用多种方法将计算机系统安全系统提高，尽可能避免病毒侵入。而作为计算机主要的使用人员——用户也要增强自身安全意识，不随便点击链接，合理使用安全管理技术，为计算机网络工程营造安全稳定的运行环境。

参考文献：

[1] 秦佳节 . 计算机网络工程的安全问题及其对策 [J]. 软件 ,2021,42(06):120-122.
[2] 范勇 . 计算机网络工程安全问题的分析与对策 [J]. 数字技术与应用 ,2020,38(10):195-196.
[3] 王晨 , 熊金 . 计算机网络工程安全问题与优化措施研究 [J]. 通讯世界 ,2020,27(04):44-45.
[4] 张曦月 . 计算机网络工程安全问题与解决策略 [J]. 计算机产品与流通 ,2020(03):25-26.
[5] 郭勇 . 计算机网络工程安全问题与优化措施研究 [J]. 计算机产品与流通 ,2019(10):34-35.
[6] 范德龙 . 计算机网络工程安全存在问题及其对策研究 [J]. 通讯世界 ,2019,26(08):181-182.