 DOI: https://doi.org/10.26549/bdai.v4i3.13862

Research on Computer Network Security Protection Strategy in the Information Age

Song Yue Tongjiang Gu Jiacheng Wang Bo Lu

Xinjiang Information Industry Co., Ltd., Urumqi, Xinjiang, 830000, China

Abstract

The rapid development of computer network technology has provided more convenience for people's production and life. However, while enjoying the convenience and assistance brought by computer network technology, people also need to recognize that the application of computer network technology also brings data security issues. If computer network security protection is not strengthened, it is easy to lead to corresponding problems such as information leakage or network system attacks. The paper also focuses on this, mainly discussing common factors that trigger computer network security issues, and elaborating on protective measures for computer network security in the information age, it is hoped that the discussion and analysis of the paper can provide more reference and assistance for people.

Keywords

information age; computer network; security protection; data security

信息化时代计算机网络安全防护策略研究

岳松 顾同江 王嘉程 鲁博

新疆信息产业有限责任公司，中国 · 新疆 乌鲁木齐 830000

摘 要

计算机网络技术的迅速发展为人们的生产生活提供了更多的便捷，但是人们在享受计算机网络技术带来的便捷和帮助同时也需要认识到计算机网络技术的应用也带来了数据安全问题，如果不加强计算机网络安全防护则很容易会导致信息泄露或网络系统受到攻击等相应的问题出现。论文也将目光集中于此，主要讨论了引发计算机网络安全问题的常见因素，阐述了信息化时代计算机网络安全的防护对策，希望通过论文的探讨和分析可以为人们提供更多的参考与帮助。

关键词

信息化时代；计算机网络；安全防护；数据安全

1 引言

在信息化时代下，数字信息的经济价值明显提升，人们可以利用数据信息来获取更多的资源，而计算机网络技术的飞速推广和普及无疑为人们的数据交换提供了更多的便捷与帮助，但同样也带来了信息泄露风险，在这样的背景下加强计算机网络安全防护则显得十分重要，在分析计算机网络安全防护对策之前首先则需要了解引发计算机网络安全问题的常见因素。

2 引发计算机网络安全问题的常见因素

就现阶段来看，引发计算机网络安全问题的因素是相对较多的，主要包含计算机操作系统漏洞、网络结构不安全、病毒攻击、安全防护技术不完善四个方面，如图 1 所示。

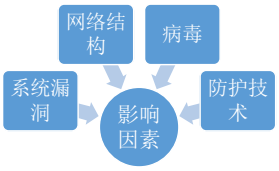

图 1 引发计算机网络安全问题的常见因素

2.1 操作系统漏洞

操作系统是保证计算机网络技术切实发挥其应有作用和影响的重要基础，人们可以通过操作系统来进行计算机操作，进而满足自己的生产生活需求，操作系统也是计算机运行启动的基本保障，是计算机网络技术的技术核心，而如果计算机内部缺乏完善的操作系统或操作系统存在漏洞，则代表着计算机抵御攻击的能力是相对偏弱的，因此很容易会受到病毒的影响，进而出现系统崩溃、信息丢失或信息被窃取等相应的问题。

2.2 病毒攻击

病毒问题是引发计算机安全问题的重要构件之一，也

【作者简介】岳松（1986–），男，中国新疆五家渠人，本科，助理工程师，从事网络安全研究。

是现阶段爆发频率相对较高的计算机网络安全问题，例如木马病毒就是现阶段较具有代表性的一种病毒类别，不法分子可以通过病毒植入的方式来盗取个人或企业的信息，并将这些信息作为牟利的手段，计算机一旦受到病毒入侵则会导致其系统无法正常运转，同时系统内部存有的数据也会受到破坏和影响，进而导致计算机瘫痪，做好病毒防控是计算机网络安全防护过程当中必须引起关注和重视的一大重点问题。除了病毒攻击以外，与之相类似的则是黑客攻击，一般情况下，黑客对于网络技术、计算机技术的了解程度相较于普通人要明显高得多，黑客善于利用计算机系统的漏洞或者是网络的漏洞来攻击计算机窃取信息数据，进而谋取利益，这也从很大程度上威胁了计算机网络技术的使用安全。

2.3 计算机网络整体结构不健全

近几年来，计算机技术和信息技术以其独特的技术优势得到了迅速发展，其技术应用领域也在不断拓宽，但是不能否认的是，在计算机技术迅速发展的背景下计算机网络的整体结构却并没有随之做出革命性的发展，现阶段计算机网络仍旧以结构化设计为主，由通信处理器、通信线路、通信设备、网络协议等几个主要部分构成，配合集线器、交换器、路由器等相应的硬件设备来进行信息交互，而又因为计算机网络整体结构发展相对而言较为缓慢，并没有发生革命性的变化，导致了黑客或病毒会利用计算机网络整体结构的漏洞来窃取信息，进而威胁信息安全 [1]。

2.4 安全防护技术不完善

计算机防护技术的应用是有效解决计算机网络安全问题的重要手段，但是就现阶段来看，虽然计算机安全防护技术得到了大范围的应用，却并不能有效满足实际需要，因为相较于黑客攻击和病毒发展，计算机安全防护技术的发展速度是相对偏慢的，同时计算机操作能力并非每一个普通人都必须掌握的谋生技能，人们对于计算机技术认知较为匮乏也导致了安全防护技术应用的科学性、规范性和有效性受到了极大的影响，很多人甚至并不知道应当如何安装计算机安全防护软件也不明确如何应用安全防护技术，进而导致了计算机网络的抗攻击、抗入侵能力相对偏弱。

3 信息化时代计算机网络安全防护对策分析

想要更好地保障计算机网络安全则需要有效应用计算机网络安全防护技术，具体可以从计算机加密技术、计算机检测技术、病毒防护技术、防火墙技术四个角度来展开分析，如图 2 所示。

3.1 计算机加密技术

计算机加密技术可以更好地保障计算机系统内部数据的安全性，进而避免信息被窃取或信息丢失等相应的情况出现，就现阶段来看应用频率相对较高的计算机加密技术主要包含私钥加密算法和公钥私密算法两种，这两种计算机加密技术可以紧抓计算机网络在信息传播过程当中的传播节点来更好的保障信息安全，即便信息被窃取也会因为数据被加密而无法获悉信息的具体内容 [2]。

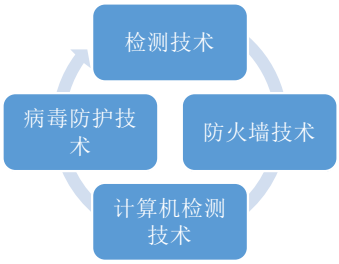

图 2 计算机网络安全防护技术

3.2 计算机检测技术

互联网是人们收集信息、浏览信息的重要渠道，但是人们在登录互联网浏览信息收集信息的过程当中很容易会受到病毒的攻击和黑客的攻击，进而导致计算机系统受到影响，出现信息被窃取或信息丢失等相应的情况，这种问题往往让人防不胜防。互联网作为信息互通的重要渠道，是人们信息交流的重要手段，但是如果在信息交流过程当中面临着病毒的威胁和黑客攻击的威胁，则很容易会影响互联网技术应有作用的发挥，为了更好地解决这一问题，则需要有效应用计算机检测技术。就现阶段来看，计算机检测技术的检测模式主要可以从异常检测模式和误用检测模式两个角度来展开分析和讨论。

异常检测模式可以通过计算机内部检测的方式来有效了解计算机内部数据是否出现相互矛盾的情况，分析计算机是否接收到了不可接收的文件，在保障计算机内部数据安全的同时确保系统的正常运行。而误用检测模式则是在信息接收到计算机时进行信息检测，判断信息数据是否会破坏计算机系统，及时的发现人们在互联网收集下载信息时是否同时接收了病毒，如果发现计算机接收的信息数据存在问题会及时的阻拦，这样则可以有效的实现信息识别，避免人们在信息浏览的过程当中让计算机系统遭到攻击。

3.3 病毒防护技术

在上文中也有所提及，病毒问题是计算机网络安全防护过程中常见的问题，病毒带来的影响是相对较大的，一旦病毒入侵，计算机系统则会出现数据叠加、反复复制的问题，进而导致系统瘫痪，严重的情况下会破坏计算机的硬件系统，进而导致计算机无法正常使用，让人们蒙受财产损失，而为了更好地解决这一问题则需要有效应用病毒防护技术抵抗病毒入侵。在很多人的观念中，病毒防护技术的应用则是在计算机系统中安装病毒防护软件，如 360、安全卫士等等，但是病毒防护技术其实需要在计算机系统安装的过程当中就开始应用，因为很多病毒的作用方向都是计算机系统，因此在计算机系统安装的过程中需要及时察觉系统漏洞并作出有效处理，避免因为操作系统漏洞问题导致病毒抵抗能力偏弱。除此之外，在计算机应用的过程当中还需要定期

查杀病毒，就现阶段来看，计算机病毒演变速度是相对较快的，很多计算机病毒具有一定的潜伏期，而定期查杀病毒则可以较好地解决这一问题，及时发现系统中的病毒并有效解决，进而更好地保障计算机的使用安全和操作安全，避免因为病毒入侵导致计算机系统瘫痪或信息丢失等相应的情况出现 [3]。

3.4 防火墙技术

就现阶段来看，防火墙技术是计算机安全防护中较为常用的一种技术手段，防火墙技术的应用可以更好地提高计算机的病毒抵抗能力，将病毒隔绝在计算机之外，保障计算机的使用安全，一般情况下可以将防火墙技术分为网络防火墙、应用网关、电路级网关和防火墙检测四个主要方向。

网络防火墙技术主要的作用点是在系统端口，防火墙会自动识别计算机接收的各种信息是否存在病毒。除此之外，现阶段人们较为熟悉的路由器也是网络防火墙技术的应用形式之一，路由器能够通过数据检查的方式落实数据处理，进而更好地保障数据安全，但是路由器的防御能力是相对偏弱的，因为路由器无法有效地识别数据的来源和数据的流向，因此路由器在实践应用的过程当中只能做基础的数据筛选工作、传递工作。

应用网关可以实现对数据的有效检查，通过数据筛选的方式明确哪些数据属于受信数据，哪些数据属于不受信数据，在此基础之上做好数据的分类隔离，保障计算机的操作安全。电路级网关同样是一种防火墙技术的应用形式，且病毒防御能力相对较强，电路级网关可以更好地发挥其数据筛选功能做好数据识别，落实数据管理和数据分析，同时电路网关还可以有效监控数据，观察数据接收以后的变化，这样则可以及时发现计算机内部问题并有效地加以解决，进一步保障计算机操作安全。

防火墙检测则是防火墙技术迅速发展之后衍生的一种技术方式，它可以更好地整合应用网关、网络防火墙和电路级网关等相应技术的技术优势，通过数据算法的有效调整来更好地落实数据监督，有效地管理数据信息，并做好数据信息的分析工作。该项技术与电路及网关最为鲜明的区别则在于防火墙检测在应用的过程当中其判断准确性是相对较高的，且数据识别、管理、分析、筛选的效率也是相对较高的，这可以更好地满足人们日益增长的数据流通需求，快速完成数据管理工作，及时发现数据当中存在的问题并加以解决，提高数据流通效率的同时保证计算机操作安全 [4]。

4 结语

就现阶段来看导致计算机网络安全问题的因素是相对较多的，例如计算机操作系统存在漏洞、病毒攻击、网络结构不健全、安全技术应用不科学等相应的问题都会引发计算机网络安全问题，而为了更好地解决这些问题，则需要通过加密技术、检测技术、病毒防护技术、防火墙技术的有效应用来提高计算机网络的防护能力，避免信息丢失、数据被窃取或系统遭到攻击等相应的情况，以此为中心，更好地保障计算机的使用安全。

参考文献

[1] 张振华.信息化时代计算机网络安全防护技术探讨[J].网络安全和信息化,2022(11):34-35.

[2] 潘天昊.信息化背景下计算机网络信息安全防护策略分析[J].信息与电脑(理论版),2022,34(20):220-222.

[3] 吉红清.信息化时代计算机网络安全防护技术[J].数字技术与应用,2022,40(6):234-236

[4] 杜宁宁.信息化时代下计算机网络安全防护技术分析[J].数字通信世界,2022(1):73-75.