计算机网络安全技术实践探讨

王鹤尧
中石油吉林化工工程有限公司，吉林 吉林 132000

[摘要]随着社会经济的迅速发展，科技水平的不断提高，计算机网络技术已经成为人们生产和生活中至关重要的组成部分，并且发挥了重要的作用。但是在实际的使用过程中，因为诸多因素的影响，极易产生网络安全问题，从而对计算机网络技术的正常使用产生不良的影响。而这也是人们关注的重点，并且一直在积极探索解决计算机网络安全技术问题的措施和方法。因此在本篇文章中我们主要对计算机网络安全技术实践进行了详细的分析与探讨，以供参考。
[关键词]计算机；网络安全；技术实践
DOI：10.33142/sca.v4i6.5050 中图分类号：TP393.08 文献标识码：A

Discussion on the Practice of Computer Network Security Technology

WANG Heyao
PetroChina Jilin Chemical Engineering Co., Ltd., Jilin, Jilin, 132000, China

Abstract: With the rapid development of social economy and the continuous improvement of scientific and technological level, computer network technology has become a vital part of people's production and life, and has played an important role. However, in the actual use process, due to the influence of many factors, it is very easy to produce network security problems, which has a negative impact on the normal use of computer network technology. This is also the focus of attention, and has been actively exploring measures and methods to solve the technical problems of computer network security. Therefore, in this article, we mainly analyze and discuss the practice of computer network security technology in detail for reference.
Keywords: computer; network security; technical practice

1 计算机网络信息安全的影响因素

1.1 网络平台对信息的筛选力度不够

当前，大数据信息在人们生产和生活中发挥着重要的作用，不管是计算机网络信息的传递，还是信息的存储，又或者是信息的共享，都与人们的生产和生活息息相关。但是因为没有能够对信息进行科学合理的筛选，因此使得一些错误信息传输到用户那里，这时如果用户无法对信息进行正确的判断时，就会对其价值观和世界观产生不良的影响，甚至做出错误的决定。

1.2 计算机配置的不合理性

因为一些计算机的内部存储空间非常有限，所以在长期的使用下，就会产生一些垃圾信息，而这些垃圾信息则非常有可能隐藏一些对计算机及其内部文件有很大危害的电脑病毒，一旦用户不小心点开，就会使其计算机内部存储的文件受到破坏，严重的话还可能会使用户的隐私产生泄漏。基于此，用户要想安全的使用计算机，就必须要定期对计算机内部的垃圾信息进行及时的清理，对一些有用的信息进行及时维护，还要对计算机是否出现故障问题进行定期的检查。所以要想安全的使用计算机网络，就必须要对其计算的硬件以及软件进行定期的维护和检查。

1.3 不法分子对计算机的入侵

当前，计算机网络安全除了要应对病毒侵入以外，就是要对黑客入侵进行有效的避免。黑客们通常具有很高的计算机操作水平，为了获得更多的个人利益，其往往会不顾法律限制，通过计算机技术来入侵其他账户或者系统，对他人计算机信息进行篡改或者破坏。再有还可能会将用户信息进行泄漏，专卖他人来获得一定的利益，从而给用户带来很大的不良影响。再有一些黑客还会入侵国家网站，从而使计算机网络安全防护能力出现丢失情况，危害社会稳定和人们的利益。

1.4 用户缺乏计算机网络安全防范意识

当前计算机在我国已经得到普及，很多计算机用户在操作方面也都比较熟悉，但是计算机还有很多相关的技术，用户并没有予以全面的了解和认识。尤其是在网络信息安全防护方面，很多用户的防护意识还比较薄弱，因此导致其在计算机使用过程中在对隐私的保护还有很多的不足和问题。因此基于此，用户就必须要不断提高计算机安全防护意识，对一些相对比较简单的计算机网络安全防护知识进行运用，比如，设置较为复杂的密码，防火墙以及安全杀毒软件等，这些措施都能在一定程度上起到保护作用。

2 计算机网络安全技术的具体应用

2.1 数据加密技术

数据加密技术主要四通过相应的算法来对计算机用户的数据进行转化，从而对数据进行二次加密，在加密以后，接收人员只有通过秘钥才能进行解锁。因此，通过密钥能够更好的提高数据的加密效果。而加密算法可以分为对称加密和非对称加密两种，其中对称加密算法加密以及解锁是利用了一个密码，非对称加密算法加密和解锁则使用的是不同的秘钥。因此在机密技术的实际选择中还是要依据实际情况来选择合适的加密技术，从而更好的实现提高数据安全程度的作用，避免数据在使用过程中出现被盗取的情况。

2.2 防火墙技术

计算机网络安全维护主要体现在两个方面，一是防火墙技术，该技术主要作用就是对计算机服务器的安全进行有效的保护，为了能够保证对计算机服务器进行有效的保护，防火墙会对计算机进行全面的扫描，在扫描过程中，一旦发现有不正确的行为，防火墙就会自动切断服务器与网络之间的连接，从而有效的切断病毒的传输。通过防火墙技术，能够为计算机网络提供一个相对安全和优质的环境，对网络安全有着至关重要的作用。其次就是包过滤防火墙，该技术主要是通过路由器来对数据进行过滤，从而筛选出其中的不良数据。该技术的使用能够很好的对数据进行拦截，并且还能将拦截报告发送给用户，从而更好的提高用户的安全防护意识。

2.3 入侵检测技术

首先是数据的收集。计算机入侵技术在使用过程中首先接触的就是数据，其可以通过物理的方式来对入侵的数据安装 IDS 代理，并且依据不同的网络结构针对不同的数据而采用与之对应的连接方法。在连接方法中如果选择使用交换式集线器进行连接，那么就可以安装在计算机交换机的安装端口上，将 IDS 系统与端口进行有效的连接，鸡儿在交换机内部的关键入口以及出口等安装入侵检测系统。此外通过这一技术还能对入侵数据进行收集，由此针对不同来源的信息进行分析，找出其中存在的可疑问题，并且对其进行标注。其次就是对信息进行深入的分析。计算机安全员要提高对网络系统的认识和了解，并且在此基础之上提出有效的安全措施，然后通过模拟人为分析实现对计算机辨别的准确度，而且分析结果也会传输到控制管理中心。对于 TCP/IP 型的计算机，可以通过网络探测引擎就能够实现入侵检测工作的开展。在整个工作过程中通过旁路监听的方式来对数据进行检测，由此找出其中的不正确的行为和事件，及时汇报给控制中心，然后控制中心发出报警信息，对事件的方位进行确定。最后，就是信息响应。IDS 任务主要是针对入侵行为而发出的响应，在实际工作中先对数据进行分析，然后在对计算机的运行情况进行分析，从而找出其中存在的入侵信息，予以及时清理。但是信息响应的方法是不同的，比如网络引擎是通过发送邮件的方式来通知计算机管理人员。通过使用入侵检测技术，能够实现对现场进行有效的记录，从而对计算机安全予以科学完善的保护。

2.4 病毒查杀技术

通过计算机病毒查杀技术，能够及时帮助用户对计算机进行更新以及漏洞的修复工作。同时还能对用户自行下载的软件进行有效的监控和管理。而且在使用过程中，用户也要对自己的用网行为进行有效的规范，避免浏览不良网站，一旦下载了不文明的文件，就要及时对其进行查杀，而且下载的文件在确保没有病毒的情况下才能予以使用。

3 计算机网络安全技术对策

3.1 完善网络系统漏洞

对于计算机网络系统出现的漏洞，可以通过技术创新的方式来对网络系统自身的漏洞进行科学的防护，并且在使用过程中不断的进行加强和完善。而要实现这一目标，就需要专业的网络技术创新和防护人员，通过专业化的培训，不断提高其综合素质和专业技能，通过高超的技术来提高网络系统安全防护。此外为了更好的对技术人员进行激励。还要建立科学的激励措施，在教育层面为社会网络安全提供专业性的技术人才，从而在实现技术创新的同时，提高全民的安全意识。通过每次对计算机系统问题进行有效的处理，能够有效的减少网络不安全因素给用户带来的损失，从根本上提高网络安全防护。

3.2 建设功能完备的物理防护体系

对于计算机系统中的客观影响因素，在网络安全防护方面可以建立设备全备的计算机机房，由此增加系统的警务信息和硬件设备，在系统应用和普及的范围以内建立网络节点，并且在网络节点中设置全备的机器房，并在其中进行防火、防盗以及防水和防潮等处理措施，同时配置响应的安全设备保护人员，对人员的流动进行科学的控制，由此减少外在因素对计算机的不良影响，从而物理角度来加大网络安全防护力度。

3.3 加强网络安全防护理论知识传播

当前很多用户在网络安全意识方面还存在很大的不足，针对这一问题可以通过网络信息传播广泛性和快速性的特点对用户的安全意识进行普及，通过展开多方面的网络安全理论知识传播，帮助用户树立安全防护意识。或者也可以通过大 APP 的信息传播来对用户进行潜移默化的影响，增加网络安全信息泄漏的案例，缩短理论知识和生活之间的距离，通过实际案例来帮助用户提高安全防护意识的重视，通过全员参与的方式建立一个健康稳定和谐的网络环境。

3.4 安装应用杀毒软件，加密处理重要文件

在大数据背景下，用户进行网络安全防护时最为便捷和安全的方式就是安装杀毒软件。在计算机使用过程中，因

为用户对网络防护的认识度不高，所以经常会点开一些不知名的网址或者连接，由此导致病毒入侵，而通过安装杀毒软件，能够从根源上在应用端来对病毒进行拦截，从而消除病毒隐患，保证计算机的安全使用。因为病毒是不确定的，是不断变化的，所以杀毒软件也要对拦截方式进行更新，所以用户在使用杀毒软件时也要对其进行定期更换，保持杀毒软件时常开启，并且安装防火墙，从而提高对个人信息的保障。尤其是一些比较重要的文件，更是要对其进行加密处理，以及定期更换密码，由此更好的保护文件，避免给窃取的风险。

3.5 积极应用防火墙

在计算机网络安全防护中，防火墙是一种非常有效的防护保障，通过防火墙能够在很大程度上提高计算机网络的安全系数，确保计算机能够正常顺利的运行；其次防火墙在使用过程中需要与互联网安全系统进行结合，通过对内外网双向重视实现互联互通，科学掌控计算机网络，消除一些不良影响，提高计算机运行的质量和效率。针对计算机软件出现的漏洞，则需要对网络病毒的工作模式进行明确，由此才能对数据信息被盗取以及利用的情况进行避免和防范。在木马传播时，通过切断其传播模式以及加强漏洞的修复都能够帮助用户对计算机软件中存在的问题和不足进行有效的认识，从而帮助其积极的使用系统补丁来对相关缺陷和漏洞进行处理，由此来避免一些安全问题的出现。计算机用户在使用过程中也要对计算机的状态进行随时监测，确保计算机的运行状态时良好的，从而更好的对病毒入侵进行预防，提高计算机使用的安全性。

3.6 重视安全认识的提升

在云时代发展背景下，计算机网络安全已经充分得到了广大计算机用户的重视，不管是个人还是公司通过计算机查询信息或者交易的概率都非常高，所以更加需要不断提高自身的计算机网络安全知识，强化计算机使用的安全性。在云技术应用的过程中，用户要不断提高自身认识，对网络安全性问题也要予以高度关注，一旦发现威胁计算机安全的因素都要及时进行切断和清除。公司在计算机使用过程中更是要制定严格的计算使用管理制度，提高互联网平台的安全性。公司的监管部门也要对计算机的使用进行正确引导，社区和公司还要加大计算机网络安全的宣传力度，积极预防网络安全风险，保证人身财产安全。

3.7 提高安全管理技术能力

很多计算网络安全都是因为用户的安全防护意识不到位导致的，不管是公司还是个体用户都需要加强计算机的日常维护工作，积极学习相关的知识，掌握网络安全防护技术。一旦在使用过程中发现计算机漏洞存在，就要及时对其进行处理，通过科学方法对计算机漏洞进行修复，主动加强计算机的安全防护力度，对加密技术进行加强处理，提高网络安全技术的应用范围，提高用户的实际需要，由此更好的推动计算机行业顺利健康的发展。

3.8 安装相关杀毒软件进行保护

面对当前的大数据时代，很多不法分子会利用病毒来对计算机进行攻击，而这时就需要通过反病毒软件来对这些病毒进行有效的处理。通过使用杀毒软件，不仅能够充分保证计算机的安全使用，而且还能够对一些长规定的病毒进行有效的抵挡，一旦计算机受到黑客的供给，杀毒软件还能够及时发出报警，提醒相关人员及时发现并予以有效的处理，从而维护计算机数据的安全。当前我国市场上流行很多杀毒软件，通过云计算就能够实现对病毒库进行更新，确保计算机网络安全。

3.9 强化信息储存传输安全

对于计算机安全来说，其一个重要目标就是为了对用户的网络数据信息的准确性进行有效的保证。大数据时代的到来，互联网为人们提供了非常便利的服务，以及高效安全的传递了数据信息。但是同时也出现了一些不足，尤其是数据信息的安全方面，更是要不断加大安全防护力度，通过将信息数据进行加密处理，避免信息被恶意截获和破解，提高数据信息的安全性。

4 结束语

随着我国科学技术水平的飞速发展，我国计算机逐渐的得到了普及，让我国很快的进入了大数据时代，但是与此同时计算机网络安全问题也随之出现，要想在大数据时代保证计算机网络的安全性，就必须要对威胁计算机安全的相关因素进行有效的把握，一旦出现风险，就要对其进行有效的处理，从而充分保证用户在计算机网络平台中实现数据安全稳定的传输，为人们的生产和生活提供更大的便利。

[参考文献]

[1]孙一方,焦晓凯.基于云计算环境的计算机网络安全研究[J].网络安全技术与应用,2020(9):34.
[2]王宏宇.基于云计算环境的计算机网络安全研究[J].电子技术与软件工程,2020(13):58.
[3]杨欢.高职数学课堂计算机网络信息化技术及运用研究[J].无线互联科技,2020(23):45.
[4]贺海成,郑莉.大数据时代计算机网络信息安全及防护措施研究[J].电脑知识与技术,2021(24):89.

作者简介：王鹤尧（1989.8-）男，英国 Teesside 大学，计算机专业，中石油吉林化工工程有限公司，技术工程师，中级职称。