计算机通信网络安全隐患及其对策探讨

孙建伟
中国联合网络通信有限公司青岛市分公司，山东 青岛 266700

[摘要]随着信息化技术及网络应用的不断发展，计算机通信网络安全管理问题愈发引起重视。网络安全管理工作常采用运行状态监控、加密保护等方式展开，同时通过安全风险预测、安全防护策略等手段为通信网络的安全运营及网络应用的安全使用提供保障，为使用者营造健康的计算机通信环境。在数字经济背景下，高效的安全管理工作可以保护计算机通信网络用户的权益，进一步促进信息产业发展，加大安全管理工作力度对计算机通信网络建设至关重要。
[关键词]计算机通信网络；安全隐患；管理措施
DOI：10.33142/sca.v5i5.7361 中图分类号：TP393 文献标识码：A

Discussion on the Hidden Danger of Computer Communication Network Security and Its Countermeasures

SUN Jianwei
Qingdao Branch of China United Network Communications Co., Ltd., Qingdao, Shandong, 266700, China

Abstract: With the continuous development of information technology and network application, computer communication network security management has attracted more attention. Network security management is often carried out by means of operation status monitoring, encryption protection, etc. At the same time, security risk prediction, security protection strategies and other means are used to ensure the safe operation of the communication network and the safe use of network applications, so as to create a healthy computer communication environment for users. In the context of the digital economy, efficient security management can protect the rights and interests of computer communication network users, further promote the development of the information industry, and it is crucial to strengthen security management for the construction of computer communication networks.
Keywords: computer communication network; hidden danger; management measures

引言

计算机通信网络的发展经历了数据计算、文件处理到信息交互的变更，其技术及应用水平的快速发展在为广大使用者提供信息获取能力的同时，也给信息安全管理提出了更高的要求。计算机通信网络覆盖范围越广泛，用户在使用过程中所面临的安全隐患也就越多，这些隐患则可能给计算机通信网络及用户利益带来不可估量的损失。因此如何采用合理有效的方式完善计算机网络通信安全管理工作，以保护使用者的数据信息、创建安全的计算机通信网络环境，成为现代网络建设使用过程中十分严肃的问题。

1 计算机通信网络安全管理概述

信息的安全保护工作历来引起社会关注，也会采用不同的方式，如密码设定、暗号设定等，但并没有真正形成信息安全管理的概念。上世纪计算机技术诞生后，信息交流方式也在不断增多，信息交流、互换速度、处理效率不断加快，信息泄漏的风险也随之增加。因此，为了有效解决这一问题，信息安全管理的重要性成为重要话题，有关研究相继开展，信息安全管理理念也随之诞生。随着当代计算机技术突飞猛进的发展，信息安全管理工作领域也取得众多突破性的成绩。

计算机网络信息安全管理就是为信息交互工作提供安全保护，减少破坏、泄漏、篡改等问题，从而保证信息交互可以顺利进行。计算机通信网络安全管理不仅要控制信息泄漏问题，同时还需保证信息的真实性；同时做好信息安全保护加密工作，保证信息可以完整传递[1]。

2 计算机通信网络安全管理的重要性

计算机通信网络是连接各类网络的纽带，其两个重要标准便是连接过程满足相关标准协议和构建全球化网络。计算机通信网络是由众多路由器、交换设备、防火墙等网络设备构建而成的，同时还包括多种连接链路、种类较多的服务器以及众多的计算机终端。计算机通信网络安全是指在网络信息传递过程中，采用相应的硬件系统、软件系统有效的控制信息传输安全，从而减少网络安全隐患及问题，确保网络信息交互可以顺利进展。因此计算机通信网络安全管理工作具有非常重要的意义。

2.1 强化计算机通信网络安全管理可以为国家信息管理构建安全的环境

从现阶段整体发展形式来看，计算机通信网络与国家信息安全有着直接的关系，计算机通信网络中存在的安全隐患，可能会直接威胁到国家安全。因此，应落实网络强国战略，保证通信网络安全已经成为国家发展的重要工作内容，及时排查解决通信网络安全隐患问题，积极开展计

算机通信网络安全管理工作，提高安全防护等级，全面控制外界网络非法入侵。

2.2 强化计算机通信网络安全管理可以为信息产业发展提供动力

随着信息化进程在各社会产业中的深入，信息安全已引起各行业人员的重视，成为全社会所面临的重要问题。尤其是信息产业作为经济发展的重要组成部分，其蓬勃发展始终对计算机通信网络的承载能力有所依赖。计算机通信网络安全管理工作的有效开展，在保障通信网络健康发展、有序运营的同时，也为信息数据的传送提供有力保障，进而为信息产业的发展提供动力。

2.3 计算机通信网络安全管理可以为使用者创建安全的应用环境

互联网技术的不断发展，给人们的工作生活带来重大改变，人们利用互联网技术解决了购物、就医、教育、出行等方面的需求，但开放的网络环境也增加了使用者信息泄漏的风险。例如，若使用者在信息传输过程中网络存在安全风险，就可能出现外界盗取信息的问题，不法分子在得到用户个人信息后进而进行网络诈骗等违法行为，给使用者带来经济损失。因此，应从信息安全角度出发，进一步做好计算机通信网络安全管理及监督管理工作，同时对计算机通信网络平台进行规范化管理，减少网络安全隐患及问题[2]，营造安全的互联网应用环境。

3 计算机通信网络常见安全问题

3.1 操作系统及软件漏洞

操作系统及软件系统是计算机通信网络使用过程中的基础系统，当操作系统或软件存在漏洞时，计算机通信网络系统也会出现安全方面的问题，无法保证计算机通信网络运行安全。计算机操作系统及软件系统存在漏洞时，极易发生网页挂马、黑客入侵等安全事故。比如，在采用 Windows 操作系统时，常用 WinRAR 完成压缩文件管理，但是相关人员对 WinRARv5.70 试用版进行研究后发现，该系统在安全方面还存在漏洞，入侵者可以利用漏洞对使用者所发出的信息请求进行拦截与修改，进而远程修改计算机使用者的执行代码，实现远程入侵。

3.2 计算机信息网络安全管理措施不足

网络安全管理工作是计算机技术高速发展过程中的一项重要共组。从相关调查中不难看出，计算机信息网络安全防护措施虽然在不断完善，但是仍然存在一些不足。其一，计算机信息网络系统防火墙安全防护不到位，无法对外界入侵信息进行有效识别，导致安全问题的发生。其二，在未授权的情况下进行访问操作，此种情况并没有得到计算机系统的允许，采用相应的方式就可以得到计算机网络资源，并给网络系统带来破坏。

3.3 黑客入侵导致用户信息泄漏

黑客入侵是计算机通信网络使用过程中较为常见、后果严重的安全问题之一。随着数字经济的不断发展，黑客可以利用网络技术对使用者计算机系统进行恶意攻击，最终得到使用者信息或相关权限，给计算机信息网络使用者带来经济损失。更为严重的情况下，黑客的入侵行为会扩大影响范围，导致计算机通信网络系统出现崩溃等问题。

3.4 使用者操作不规范

导致计算机通信网络出现安全问题的原因，通常包括使用者操作不规范的情况。主要包括两种情况：其一，使用者在操作时没有建立起安全意识，未设置有保护功能的个人账号密码，给不法分子带来可乘之机，例如使用者在公共网络环境中登录个人银行账户，而导致账户密码被盗取；其二，使用者操作未按照规范进行操作，例如使用者在进行信息传输时，若没有做好加密工作，导致信息被不法分子窃取，造成信息泄漏，引发安全问题[3]。

4 计算机信息网络安全管理措施

4.1 构建防火墙系统

防火墙系统的构建在实现计算机通信网络内部与外部通信交流的同时，可以实现安全信息识别功能，对计算机通信网络系统应用过程中的不安全信息进行有效控制。防火墙可以根据使用者使用情况实现拦截黑客攻击、阻止异常信息传入等功能，避免出现信息泄露等安全问题，同时可以减少安全隐患在网络中扩散。防火墙的建立不仅可以提高用户信息安全程度，还使计算机通信网络系统具有一定的隐蔽性，为使用者创建安全的保护网，确保使用者的网络安全。

4.2 做好信息加密处理

从目前计算机通信网络安全管理情况来看，安全保护工作并不全面。例如用 linux 系统对重要信息进行保存时，使用者信息与用户均要做好加密处理，当使用者应用软件或提取信息时，应先输入提前设置好的密码。做好软件与信息加密工作的同时，还应查询网络信息协议，确保网络传输协议可以满足相关法律法规要求。为了减少黑客给计算机硬件所带来的侵扰，可以对调节器、路由器间的权限进行协调，从而实现专业人员对以往的用户不规范行为的控制。

4.3 合理应用杀毒软件

目前，市场中的杀毒软件种类相对较多，杀毒软件的合理应用后可为计算机信息网络使用者构建安全的使用环境，提升计算机信息网络使用安全。杀毒软件可以将本地资源进行扫描，进而将有效的信息传递给计算机信息网络使用者。杀毒软件可以对计算机信息网络的病毒进行检测与清除，确保计算机信息网络使用安全。但是现阶段一些使用者并没有正确理解杀毒软件使用的意义，还有一些计算机通信网络使用者在使用杀毒软件时因杀毒软件中的弹窗或是报告发现木马病毒而有怨言，还有一部分使用者会删除文档等。但是在具体应用杀毒软件时可以上报系统所存在漏洞，可以将疑似木马病毒的文档进行删除，从而可以保证用户使用安全，因此可以采用杀毒软件对系统中的漏洞进行修补并有效控制病毒的侵入。

4.4 合理应用入侵检测技术

计算机信息网络在应用过程中，当有外部网络攻击时可以利用防火墙技术完成，此外，还应做好内部网络运行情况检测工作并及时发现运行过程中的问题，采用入侵检测技术后可以建设 IDS 入侵检测系统，从而可以对防火墙技术中的不足进行优化，以保证外部与内部供给错误检测工作的有效性，当发现异常后应提前进行处理并将非法入侵进行拦截，通过此类提升计算机信息网络安全并保证系统运行的稳定性。入侵检测技术在运用后可以将使用者的活动行为监管并可以及时审核系统结构与使用中的不足，通过系统完成运行检测工作并可以显现出系统运行情况，应根据需要构建科学的报警系统。对计算机信息网络系统中运行异常情况进行分析并判断系统信息是否完整，可以采用审核与跟踪方式控制系统运行情况，同时可以利用测算方式对安全管理中不规范的行为进行管理，再利用安全审计结果建立科学的防入侵方式，如事件记录、网络断链、预警处理等[4]。

4.5 合理应用身份认证技术

计算机信息网络系统使用者在进行网络访问时应采用身份认证技术，身份认证技术主要包括密码、用户名、人脸识别、指纹识别等，虽然认证方式较多但是使用者应从中选择出最适合的身份认证技术。利用身份认证技术可以保证使用者在应用相应的网站时可以实现一人一户登录，从而保证使用者信息的完整性、可控性、保密性等。假如采用口令身份认证使用者应先设置 ID 账号，确保该账户为使用者唯一账户，确保口令身份认证的安全性并确保口令身份认证 ID 账户中各使用人员均可知晓，在系统中应确保口令使用与信息存储均是安全的，整体认证过程中应保证口令传输的安全性，防止口令泄漏。在完成信息请求前应先认证使用者身份并避免口令误传给不相干人员。采用人脸识别认证技术时主要是以视网膜身份认证技术为主，采用视网膜认证技术具有终身差异性或是不变性特点，然后采用相关计算方式进行计算并提升视网膜认证技术应用的准确性。在应用视网膜认证技术时是将使用者视网膜信息传输到数据库中并完成人脸身份验证，目前此项技术被应用到不同的领域中可以提升操作的准确性。

4.6 合理应用漏洞扫描技术

在应用漏洞扫描技术过程中应用者应先构建内部运行管理系统，通过扫描可以将网络运行中的问题进行了解并可以对黑客技术攻击情况进行检验，从而检查出网络中的漏洞以及网络运行过程中所存在的安全隐患，及时采用相应的措施进行处理。计算机信息网络系统具有一定的复杂性且当外部场景出现变化时若管理人员专业水平较低，就无法分析计算机信息网络系统运行过程中的安全隐患，因此，此种方式具有一定的不足。漏洞扫描技术在应用过程中应确保技术人员具有较强的操作能力，可以规范进行操作，同时可以对系统进行及时优化或是修补，从而减少计算机信息网络系统中的漏洞，保证系统运行安全。

4.7 提升计算机通信网络系统使用者安全意识

在进行计算机通信网络安全管理过程中，要想减少安全问题的发生，还应通过计算机信息网络安全宣传对信息安全管理思想进行普及，提升计算机通信网络系统使用者的安全使用意识和安全防范意识，保证计算机信息网络系统使用安全。计算机信息网络使用者应先确立安全意识，认识到计算机通信网络安全管理的重要性，从而减少在计算机通信网络使用过程中的安全事故。相关管理部门应强化计算机信息网络使用者安全教育，强化各使用者的安全防范意识。此外，在进行教育过程中还应让计算机信息网络使用者认识到信息泄漏后所带来的不利影响，例如信息丢失、信息泄露、经济损失等。近些年，计算机信息网络技术得到了迅猛的发展，因此应做好计算机信息网络系统的安全维护工作，减少病毒感染风险，满足时代发展的要求。用户应合理应用杀毒软件，做好软件系统及防火墙的维护和更新，及时清除电脑中的木马病毒，确保计算机通信终端的网络安全，进而保障计算机信息网络畅通运行。

4.8 提升计算机信息网络人才培养力度

现阶段，多数计算机信息网络使用者不仅没有构建网络安全意识，而且其操作过程隐藏了一定的安全隐患，但是此种现象并没有得到足够的重视。所以应强化计算机信息网络人才培养，通过专业人员让计算机信息网络使用者可以建立安全问题预防理念，提升网路安全使用意识，减少计算机信息网络运行安全问题。同时，计算机信息网络专业技术人员应定期对网络信息通道运行情况进行检查，当发现问题时应及时进行纠正与修补。另外，应由专门的网络管理人员进行计算机信息网络系统监管，加强监管力度，净化网络环境[5]。

5 结语

通过分析可知，在互联网背景下，对计算机信息网络进行安全管理具有非常重要的意义，应充分做好计算机通信网络安全管理工作，根据情况合理做好安全防护措施，确保使用者可以高效、安全的使用计算机通信网络。

[参考文献]

[1]刘玲.计算机通信网络安全隐患及其对策探讨[J].产业创新研究,2022(6):72-74.
[2]郭国智,梁岳赟.新形势下计算机通信网络安全隐患及其对策探讨[J].电脑知识与技术,2021,17(32):34-35.
[3]王增国,王昌伟.计算机通信网络安全防护措施[J].电子技术与软件工程,2021(17):239-240.
[4]徐景嵩.计算机通信网络安全维护措施研究[J].电脑知识与技术,2021,17(24):61-62.
[5]王懿嘉.新形势下计算机通信网络安全隐患及其对策探讨[J].科技创新导报,2020,17(17):132-133.

作者简介：孙建伟（1972.10-），男，汉族，中国联合网络通信有限公司青岛市分公司，网络维护主管，主要从事网络运行维护工作。