计算机网络安全体系及其发展趋势综述

岑　莉
江西软件职业技术大学　江西南昌　330000

摘　要：随着互联网的普及应用，计算机网络安全已经成为各行各业网络信息化建设高度重视的问题，关乎到网络信息系统的安全运行。在网络安全建设中，要运用先进的网络安全防范技术构建起完善的计算机网络安全体系，消除计算机系统漏洞，防范非法入侵风险，全面维护网络运行安全。

关键词：计算机；网络安全；保护策略

Computer network security system and its development trend

Li Cen
Jiangxi University of Software Professional Technology, Nanchang 330000, China

Abstract: With the popularization of the Internet, computer network security has become a highly valued problem of network information construction in all walks of life, which is related to the safe operation of network information system. In the construction of network security, it is necessary to use advanced network security prevention technology to build a complete computer network security system, eliminate computer system loopholes, prevent illegal intrusion risks, and comprehensively maintain the security of network operation.

Keywords: Computer; Network security; Protection policy

引言

随着计算机信息技术的不断发展与完善，互联网使用的普及程度也越来越高。据 CNNIC 数据统计，2017 年年底，我国互联网的使用人数已经达到了 7.51 亿人次。在互联网信息技术的支持之下，我国各大企事业单位才能在疫情期间依然正常运转，各大教育部门才能正常开展教育工作，各级政府才能够将管理工作开展得井井有条。由此可见，互联网信息技术与我们的生产生活逐渐融为一体。然而，网络信息安全一直是使用者心中一块难以落下的石头，因此采取有效措施解决网络信息系统的安全问题刻不容缓。

一、计算机网络安全概述及意义

1. 计算机网络安全概述

计算机网络是由网络控制管理的软件、硬件以及网络服务等多个方面组成的集合。正因为计算机网络系统成分复杂，所以导致网络安全问题的原因也就多种多样。在对计算网络安全进行定义时，要综合多方面影响因素。如今，计算机网络信息系统已经发展到一个较为完善的程度，所以业界对其网络安全也已经形成了普遍的认识。在计算机网络信息系统正常运行过程中，因各种外界因素或自身因素导致的文件、数据以及软件等重要信息的损坏或泄露的现象就是广义上的计算机网络安全。

计算机网络信息安全的内涵可以从计算机所依托的硬件设备安全和依托计算机内部所储存用户信息数据的安全两个层面来理解。前者可以通过对硬件设备的保护以及更新换代来提升计算机网络信息的安全。后者则需要通过软件、系统程序来进行用户数据的保护。软硬件共同发展进步才能更好解决计算机网络信息安全问题。

2. 计算机网络安全意义

安全的计算机网络系统为职场人员创造了一个更加安全、放心的平台。目前，互联网技术已经渗透到各行各业的日常工作当中，重要信息数据的储存与处理都离不开计算机网络。因此，确保计算机网络的安全对于处在职场的工作人员而言至关重要。安全的计算机网络系统会推进互联网技术的普及。互联网技术发展至今，其优缺点已经充分暴露，剩下的一部分没有加入到互联网阵营当中的人大多数是因为计算机网络的安全性有待提升。所以，一旦计算机网络的安全问题得到解决，这一部分人会毫不犹豫使用互联网，计算机信息技术的普及程度将会再次大幅提升。计算机网络信息安全是计算机网络正常运转的一个重要前提。随着计算机技术的不断完善，越来越多的服务都可以线上办理。为了保障办理过程不出现失误，用户需要进行实名注册，提供个人相关信息。海量的用户信息一旦出现泄露就会导致大量的损失，对于计算机网络的发展也必然会产生一些消极影响。做好计算机网络信息安全维护工作，不仅可以使计算机网络系统平稳运转，同时还可以发挥计算机网络信息的价值。由此可见，维护计算机网络信息安全非常必

要。

二、当前国内计算机网络的安全现状

1. 计算机系统安全现状

系统安全是计算机网络安全中的常见问题，当前主流操作系统都存在着一些安全漏洞，不法分子经常利用系统自身漏洞对系统发起攻击，造成计算机瘫痪，大量数据信息出现永久性破坏。大部分计算机操作系统虽然配置了防火墙、入侵检测系统等，但是这些软件系统更新缓慢，很难主动处理网络安全漏洞，使得计算机系统易受到病毒入侵破坏。

2. 互联网新技术安全现状

随着大数据、云计算、物联网时代的到来，越来越多的先进技术需要借助计算机网络运行，对计算机网络安全提出了更高的要求 [2]。但是，由于计算机网络属于开放性的网络，安全管理难度大，所以导致互联网新技术应用面临一系列安全问题。如，在大数据技术应用中，该技术需要从计算机网络中搜集大量数据信息，提取有价值的数据，并利用特定算法得出数据分析结果，将分析结果传输到数据库中。如果在这一过程中出现网络安全漏洞，则会造成数据信息被恶意篡改或破坏，影响大数据挖掘分析的准确性。

3. 用户网络安全现状

在计算机网络安全管理中，用户安全意识是影响网络安全运行的重要因素。但是，由于计算机网络用户素质参差不齐，对网络安全重要性认识程度不同，使得部分用户出现了大量的不安全操作行为。如，部分用户登录非法网站连接或在高风险网站上下载资源，为病毒入侵计算机网络提供了路径；部分用户的计算机系统操作技能不足，经常出现系统操作失误，引发数据信息损坏风险 [3]。

4. 软件安全现状

随着计算机网络功能的强大，各类型软件不断增多，部分软件在设计阶段存在安全漏洞，对计算机网络安全构成严重威胁。通过对近年来的计算机网络安全事件调查结果可知，软件漏洞是引发网络安全事件的主要原因。

5. 硬件安全现状

硬件设备是保障计算机网络安全运行的物质基础，当硬件设备存在安全问题时，极易引起计算网络安全事件，造成网络信息数据破坏。如，网络电缆是重要的硬件设备，主要由专线、光缆或电话线组成，每种电缆都会传递信息数据信号，当不法分子对网络电缆进行破坏后，能够直接窃取线缆传输的信号，获取机密信息。

三、网络信息安全的技术防范策略

1. 数字签名

针对在互联网上传播的电子文件，人们可以使用数字签名的方式来完成信息内容的确定。签字方式需要和相关的信息内容绑定在一起。以保证该信息内容正是经过签字方式所确定的对象，以克服假冒、抵赖、冒充和篡改内容等的信息安全问题。数字签名通常使用一种数据协定，要求接收数据的双方都能够符合两种要求：接受方可以识别发出方的身份；以及发出方无法否认与他传输过的数据相同这一事实。而数据签章则通常使用了不对称的密码技术，发出方经过对所有明文经过了密码转换后，得出一种数值结果，将之视为签章。而接受方则利用发送者的公共密钥对签章结论实行了解密计算，如其结论是明文，则签章为可靠，从而求证了对象的身份是真正性的。

2. 鉴别

鉴别的首要目的，是为了验明使用者或消息的真正身份。对实体所宣称的身份做出唯一鉴定，从而证实其来访要求，并确定消息源头以证实消息的完整性，从而有效地抵御非法访问、假冒、重演等危险。按照识别对象的差异，识别技术又应该分成消息辨别和通讯双方相互辨别；而按照鉴别内容的差异，识别技术又应该分成用户身份辨别和消息内容辨别。

3. 密码技术

是加密和解密的方法。密码是互联网与安全保密系统的主要基础。它是把原文内容用一种预定方法规律的重排、改写，使之成为他人读不懂的密文。而解密法则是把密文按照原来加密方式复原。目前，已形成的秘密方法有许多，如替换秘密、移位加密、一次性密码本增加、序列秘密等 [1]。

四、计算机网络安全防护措施

1. 加强网络信息安全管理人才的培养

网络信息安全管理离不开高质量技术人才。高等教育是一个培养人才的重要方式，但是目前的高等教育存在一定的滞后性。学生所接触到的知识不足以解决当前计算机信息管理面临的问题，所以人才培养的效率并不高。及时更新高等教育的内容使其与人才市场的需求相接轨是培养高质量人才的关键。另外，高等教育培养出的人才严重缺乏实战能力。学校大多数是进行理论知识的教育，忽略了实践能力的培养。因此，高等教育培养出的人才不能直接满足市场人才需求。这就需要高校进行教育改革，不仅要严抓学生理论知识的学习，同时还要加强实践能力的培养。“校企联合”可以为学生创造更多实战的机会，加快计算机信息安全管理人才的培养效率。

2. 做好杀毒工作

计算机网络用户若是能够打造一个优质的计算机防御系统，一般均能够有效地抵御不良信息的入侵，切实保证计算机网络使用方面的安全性。现阶段计算机防御系统一般主要由杀毒软件、防火墙还有入侵防御系统等部分组成。而对于杀毒软件来讲，属于其中最为关键的一个内容，用户必须要给予高度重视。目前来看，杀毒软件一般都会有：自动升级功能、病毒扫描功能、病毒

清除功能、数据恢复功能还有流量控制等诸多功能，所以能够出色防御入侵计算机网络的相应木马程序以及病毒，切实达到保护计算机网络安全的目的。因此，相关用户应在实际使用计算机网络的过程中，科学地选用相应的杀毒软件，以此不断提升自身网络运行的安全性。在实际操作中，用户选用杀毒软件时，应该尽可能地选用一些正规公司推出的正版杀毒软件，如果自身不懂或者是不了解，严禁盲目选用，应及时向专业人士进行请教和学习。在使用杀毒软件的过程中，对于软件提示的相关警告信息，必须要给予高度重视，然后结合杀毒软件的提示及时开展全面的杀毒工作。此外还应该定期升级杀毒软件，以此保证软件应用的有效性，从而切实保证计算机网络在实际使用时的安全性。

3. 提升反病毒的能力

反病毒能力对于计算机信息安全管理至关重要。软件和信息系统一般会设有防火墙来确保信息安全。然而，面对病毒的攻击大多数防火墙形同虚设。加强防火墙反病毒能力，设计人员首先需要对当前现存的各种病毒了如指掌。正所谓知己知彼百战不殆，只有清楚各种病毒的工作机理才能写出相应的程序抵挡病毒的侵犯。其次，病毒具有反复性和伪装性。所以，设计人员在进行反病毒防火墙程序的设计时，需要着重考虑实时监测、剥离伪装等功能的设计。最后，随着互联网技术的不断发展，病毒的种类也越来越多。每一次病毒的出现都会使计算机信息安全管理受到威胁。软件以及互联网信息管理系统的设计人员应时刻保持高度警惕，一旦有病毒攻击，就要立刻采取维护措施，避免用户信息数据丢失。

4. 注重持续提升网络安全意识

不断提升人们的计算机网络安全意识，属于高效防范计算机网络安全事件的一个重要举措，唯有计算机网络的使用者始终保持良好的防范意识以及清醒的头脑，方可有效抵制一系列网络诱惑，准确辨析各类数据信息的安全性，从而减少漏洞隐患，使得违法分子缺少可乘之机。而想要实现这一目标，应注重从以下几个方面着手：(1）计算机网络用户自身应该积极主动地开展有关网络安全知识方面的学习工作，在充分认识网络安全问题的前提下，逐步养成一个良好的计算机网络应用习惯，例如：不浏览一系列非法网页、不点击弹出来的页面以及不注册莫名账号等等。对于企业用户，还应该完善有关网络安全方面的监管制度，除了要包括上述内容之外，还应该严禁员工私自在企业内部计算机网络中接入私人移动设备、严格设置计算机网络的使用权限等。还应该健全相关责任制度，然后细化分解到个人，这样一旦出现相关违规操作使得网络安全遭受不利影响，能够及时追究个人责任，有助于全体树立良好网络安全意识，从而提高内部网络安全防范水平。(2）作为政府和相关网络安全管理部门等，应该积极发挥自身的引导作用，借助各类新旧媒体平台，广泛开展网络安全宣传教育工作，以此在潜移默化当中帮助社会公众逐步形成良好的网络安全意识，并能够在长期的影响下持续增强安全意识。具体操作过程中，有关部门可以借助微信公众号、微博以及抖音等平台进行宣传，也可以开展线下的宣传教育活动。在具体的内容上包括不限于：怎样辨别虚假信息、怎样正确使用计算机网络、出现网络安全事件后怎样进行处理等 [4]。(3）作为政府及相关部门还应该持续加大对计算机网络环境方面的管控力度，包括不限于：对一系列知名网络平台的审核、对各类不良信息给予严厉打击、迎合大数据时代的发展变化，积极完善有关网络安全方面的一系列法律法规、打造完善的信息安全防护体系等，尽可能地突出法律法规的权威性以及不断提升执行力。这样也能够在一定程度上促使人们的计算机网络安全意识不断提升，切实提高计算机网络的安全性。

五、结束语

综上所述，计算机网络安全管理是保障网络信息安全、净化网络运行环境以及促进信息化建设全面开展的一项重要工作。在计算机网络安全管理中，要以识别网络安全现状为前提，找到网络安全薄弱环节，再采用防火墙技术、入侵检测系统、身份认证技术、VPN 技术和防病毒技术等有效的安全防范技术措施，提高计算机网络安全等级，避免计算机网络受到非法入侵，从而保障网络信息安全。

参考文献：

[1] 汪源 . 计算机网络信息安全技术及其发展趋势 [J]. 信息记录材料，2021(02):208-209.

[2] 李富 . 计算机网络信息安全技术及其发展趋势研究 [J]. 信息通信，2020(03):179-181.

[3] 孙凯，石向炜 . 计算机网络信息安全技术及其发展趋势 [J]. 科技传播，2018(16):134-135.

[4] 张晓蓉 . 计算机网络信息安全技术及其发展趋势的探讨 [J]. 新课程（下），2015(09):163.

[5] 范清永 . 试论当下计算机网络安全现状及对策 [J]. 信息记录材料 ,2021(5):58-59.

[6] 刘超南 . 计算机网络安全现状及防御技术 [J]. 通讯世界 ,2019(1):123-124.

[7] 陈瑞 . 计算机网络安全现状分析与防御技术探讨 [J]. 科技资讯 ,2018(13):9-10.