ISSN: 2661-3719(Print); 2661-3727(Online)

计算机信息网络安全技术及发展方向

柴亚杰
河南中烟责任有限公司许昌卷烟厂　河南省许昌市　461000

摘　要：信息化和数字化是现代社会发展的典型标志，计算机及网络技术给人们生产及生活带来的影响是十分巨大的，但其安全管理问题也值得引起重视。文章阐述了计算机信息网络安全技术的基本概念和重要性，分析了导致计算机信息网络安全产生风险的各类因素。分析了防火墙技术、数字加密技术、漏洞扫描技术、云安全技术的实际应用情况，对计算机信息网络安全技术的发展方向进行了展望，希望能为相关从业者提供参考。
关键词：计算机；信息网络；安全技术；发展方向

Computer information and network security technology and its development direction

Yajie Chai
Henan China Tobacco Co., LTD., Xuchang Cigarette Factory Xuchang, Henan 461000

Abstract: Informatization and digitization are typical signs of the development of modern society. The impact of computer and network technology on people's production and life is huge, but its safety management is also worthy of attention. The article expounds the basic concept and importance of computer information network security technology, and analyzes various factors that lead to computer information network security risks. The actual application of firewall technology, digital encryption technology, vulnerability scanning technology, and cloud security technology is analyzed, and the development direction of computer information network security technology is prospected, hoping to provide reference for relevant practitioners.
Keywords: computer; information network; security technology; development direction

引言：

如今社会经济快速发展，计算机软件技术及通信网络技术在人们生产及生活中扮演了越来越关键的角色，尤其是基于相关技术发展而来的大数据时代，让人们享受到了信息化带来的便利。但是，高度信息化随之而来的安全问题也给人们的信息安全产生了威胁，因此业界关于计算机信息网络安全技术的研究一直都很重视。尤其是在我国全面推动智慧城市及万物互联体系建设的背景下，更需要采用先进可靠的安全技术机制，为社会经济的稳定发展提供保障。

一、计算机信息网络安全技术概述

（一）技术概念

计算机信息网络安全技术主要是指针对计算机软件、数据库、信息处理系统的各类应用场景，为充分保证计算机硬件、软件及数据信息不会遭到恶意更改、损坏或窃取的情况，所采用的一系列软件技术、信息处理技术。关于计算机信息网络安全的概念，一般可以从逻辑和物理两个层面进行理解，前者是指当代社会大众比较熟知的信息安全，主要对信息完整性、私密性和可利用价值的保护，后者则是在逻辑安全的基础上，对互联网、移动通信网络乃至大数据体系下的信息完整性、保密性和可利用价值的保护[1]。自计算机软件技术及网络技术诞生以来，由于其涉及到的信息、数据价值被认可，一系列风险也随之产生。一方面，计算机硬件、软件可能本身在制造、设计或技术应用方面存在一定缺陷，导致数据在储存、传输或使用时面临安全风险；另一方面，在使用计算机、网络时，也可能因人为疏忽或恶意导致数据安全遭到侵害。因此，关于计算机信息网络安全技术

作者简介：柴亚杰，男，河南省许昌市，邮编：461000，河南中烟责任有限公司许昌卷烟厂，1979年11月，本科。

的研究一直都备受重视。

（二）重要性

自计算机及网络技术诞生以来，人们在信息化和数字化的道路上高歌猛进，发展至今，计算机软件、互联网已经深入到人们生产生活的方方面面，而人们在生产生活中的各类活动、要素都可以通过计算机软件处理为信息数据，进行储存、共享、传输和应用等。尤其在大数据背景下，关于数据信息价值的挖掘尤为重要，这也是未来社会发展的重要趋势。但是，在整个过程中，计算机信息网络安全问题一直都存在，并且在信息化社会深化发展的过程中产生越来越严重的威胁。首先，在网络时代中无论是个人还是企业单位都涉及到大量具有保密属性的信息，这类信息的保密性和安全性是人们所关注的。一旦其遭到破坏或窃取，可能导致个人或企业利益受损。其次，在现代社会的运转过程中，需要用到大量的信息数据，而这些信息数据的准确性、完整性如果受到损害，也可能给社会的稳定安全造成不良影响。所以，提升计算机信息网络安全技术应用水平，是信息化时代背景下保证数据信息安全的关键，也是大数据乃至智能技术发展应用的重要保障[2]。

二、导致计算机信息网络安全受到威胁的各类因素

（一）硬件及软件缺陷

在计算机网络系统中，无论是硬件还是软件，都需要进行科学设计，采用可靠工艺进行制造，其中软件还需要利用科学技术进行优化调试。因此，如果在设计、制造或优化调试中出现问题，很容易导致计算机网络系统存在缺陷，这些缺陷将可能直接影响数据信息安全[3]。比如说，硬件质量不佳，引发各类故障，可能导致储存的数据信息被损坏。再比如软件系统存在漏洞，导致数据信息遗失或被窃取。虽然如今计算机软件设计制造技术越来越成熟，但是这种本身的缺陷风险依然存在。

（二）计算机病毒

计算机病毒一直是威胁计算机信息网络安全的重要因素，其作为一种具有破坏性的程序，具有较强的潜伏性、传染性和破坏性。从常见的木马病毒、蠕虫病毒，到各种类型的系统病毒，一旦绕过系统安全系统或程序进行入侵，很容易造成用户计算机中的信息数据被破坏或被窃取。在互联网背景下，计算机病毒时刻潜藏在各个领域中，稍有不慎就可能威胁人们的计算机信息网络安全。

（三）不法黑客因素

在信息化时代背景下，数据信息的价值不言而喻，因此也出现了为了利益而利用现代技术在计算机互联网中进行入侵、盗窃等不法活动的人员。黑客主要是通过设计程序或利用计算机网络漏洞，绕过破解计算机软件安全程序，做出侵害他人利益的行为。虽然我国目前已经完善了相关安全法规，但是在利益驱使下，计算机信息网络安全技术和黑客之间的斗争将会是长期性的。

（四）使用规范性和严谨性因素

如今计算机网络技术已经进入到人们生产生活的方方面面，在人们日常使用计算机及互联网时，可能因操作的规范性、合理性，导致数据信息安全受到威胁[4]。例如，由于加密信息保护不当，导致常规安全程序中最重要的密码被泄露；由于点击、访问不明来历的链接、网站，或是下载未经证实足够安全的文件，都可能导致计算机感染病毒，或被黑客入侵；计算机安全系统更新不及时、维护不到位，导致系统漏洞无法被及时修复，或是无法有效识别应对新型网络病毒的入侵；等等。

三、计算机信息网络安全技术的应用现状和发展趋势

（一）目前常见的技术类型

1.防火墙技术

防火墙技术是计算机网络诞生以来最为经典和常见的安全技术，其主要是由计算机硬件和软件构成，部署于内部网络的边界，对进出内部网络的各类数据进行监测，避免恶意代码、程序入侵内部网络，已达到保护内部网络数据安全的目的。防火墙安全技术在企业的计算机信息网络安全管理中扮演着关键角色，可以有效过滤、隔离风险因素。现代防火墙技术不仅对外部信息进行监测、过滤、防护，还会基于用户身份对其访问的网站类别进行限制，规避用户风险行为。另外，通过在内部网络中划分不同防护区域，可以避免因局部区域出现安全风险而引发全部内网安全问题的情况。值得一提的是，随着相关技术的不断发展，防火墙技术不再单单是一种防御性的计算机信息网络安全技术，而是可以主动对数据信息进行采集分析，以判断外部攻击风险，达到内部过滤、外部监控的防控效果[5]。

2.漏洞检测修复技术

前文提到，受到计算机网络硬、软件本身设计、工艺、运维或使用情况的影响，其可能存在一些漏洞，导致安全风险的出现。为此，针对漏洞进行扫描、检测和修复的安全技术应运而生。该技术主要是从硬件、软件两个层面，对计算机网络的安全性进行扫描，发现其中存在的漏洞，再进行修复。从更大技术范围角度来看，漏洞检测修复技术的应用，是和计算机硬、软件更新优化技术相辅相成的。即通过漏洞检测发现存在安全风险

的漏洞，为计算机网络更新优化提供参考依据，经过研究处理之后形成该项漏洞的典型特征信息和修复补丁，交付给漏洞扫描程序进行对比扫描，发现漏洞，再进行修复。漏洞检测修复技术伴随着计算机网络技术的发展，是从计算机网络自身完善的角度出发，不断提高其抗安全风险的能力。

3.安全备份及加密技术

加密技术主要是在用户使用计算机及互联网时，通过对关键信息的加密，避免其遗失或被窃取的技术。安全备份一般是通过对重要信息、资料、文件的自动化备份，将其储存至安全数据库或云数据库中。加密技术则贯穿于用户使用管理信息数据的各种场景，静态加密一般用于数据资料的储存场所，在外部访问时检测其访问资格，以及判断是否存在安全风险。动态加密则一般是针对数据资料在内部网络乃至外部网络的共享期间，通过针对不同场景下的动态加密手段，保证其即使是被非法窃取，也难以被破译和利用。随着加密技术的进一步发展，业界也出现了一种更高等级的安全加密机制。即在加密程序判断该数据资料已经遭到窃取或处于外部破译的状态时，其会自动对数据资料进行销毁，而用户可以通过云端备份平台重新获取该数据资料。这种方式可以有效避免重要数据资料被非法利用，在当今企业单位及重要部门的工作管理中有重要应用。

（二）发展趋势

1.云安全技术

云安全技术是近年来基于云计算机、P2P技术发展起来的新型计算机信息网络安全技术，其主要是通过将用户计算机设备和信息网络平台连接起来，基于大数据分析和监测，形成更大规模的安全风险监测、病毒查杀网络平台。简单来讲，这是一种基于互联网领域的安全监测防护体系，可以有效利用大数据和现代软件信息技术，通过扩大网络病毒资源库、技术资源库的形式，形成大规模、系统化的安全防护矩阵。在未来，云安全技术将是计算机信息网络安全技术研究的重点领域，同时也将是计算机信息网络安全技术适应社会经济发展的关键要点。

2.智能安全技术

智能化是现代社会发展的重要趋势，智能化的实现主要依托于计算机软件及网络技术，因此在计算机信息网络安全方面，智能化也是大势所趋。目前，在智能工厂、智能家居乃至智慧城市的建设中，通过配置专家系统、智能分析软件等形式，初步形成了针对各类病毒、安全漏洞及外部入侵风险的智能化监测、防护、修复机制。智能安全技术具有典型的自动化、动态化成长属性，可以在有效减少人员介入的情况下，实现对各类安全风险的研究分析，以不断拓展其安全管控范围，同时提升风险识别、安全防护、安全问题紧急处理能力，进而推动计算机网络系统安全等级的持续提升。显然，未来的计算机信息网络安全技术将基于智能化技术，实现由静态向动态的方向发展[6]。

四、结束语

综上所述，现代社会经济快速发展，计算机网络在人们生产生活中发挥了重要的作用，但同时也产生了一定的安全风险。当前关于计算机信息网络安全的技术研究，初步形成了以防火墙、漏洞扫描及病毒查杀等为代表的技术体系，但在信息化时代进一步发展的背景下，需要通过积极的技术升级及创新，将现代化的云技术、智能技术应用到计算机信息网络安全管理之中，为社会经济的稳定健康发展打下可靠基础。

参考文献：

[1]韩腊萍.计算机信息网络安全技术及发展方向[J].科教导刊-电子版（下旬），2021（7）：275-276.

[2]王珊珊.高职院校计算机信息网络安全技术和安全防范策略[J].大众标准化，2021（8）：177-179.

[3]罗克佳.电力系统计算机信息网络安全技术及防范[J].数码设计（上），2020，9（10）：51.

[4]秦鸣昕.计算机信息网络安全技术及发展方向[J].网络安全技术与应用，2019（5）：5-6.

[5]王众魁.探索计算机信息网络安全技术及发展方向[J].电脑知识与技术，2021，17（8）：58-59.

[6]周垚.计算机信息网络安全技术和安全防范措施探讨[J].商品与质量，2020（19）：245.