计算机信息技术与网络安全分析

李悌朝
苍南县旅游投资集团有限公司　浙江温州　325800

摘　要：计算机网络的出现改变了很多人们原有生活方式和习惯，它改变了货币流通的方式、改变了商品贸易的形式、改变了信息交互的模式，计算机已经成为人类生活、工作、学习的得力助手，同时在相关行业领域中发挥着不可或缺的作用。网络信息安全维护是确保互联网健康发展的前提，面对近年来频发的网络信息安全问题，需要创新网络信息安全技术管理的应用策略。

关键词：网络安全；计算机；信息管理；管理技术

Analysis of Computer Information Technology and Network Security

Tichao Li
Cangnan Tourism Investment Group Co., LTD., Wenzhou, Zhejiang 325800

Abstract: The appearance of computer networks has changed many people's original lifestyles and habits. It has changed the way money flows, the way goods are traded and the way information is exchanged. The computer has become the right hand in human life, work, and study, and plays an indispensable role in related industries. Network information security maintenance is the premise to ensure the healthy development of the Internet. Faced with frequent problems of network information security in recent years, it is necessary to innovate the application strategy of network information security technology management.

Key words: Network Security; Computer; Information Management; Management Technique

引言

在互联网和计算机技术的深入发展下，各个行业的进步发展也拥有了更多的技术形式，同时，面临复杂、多样的信息处理，计算机信息网络安全问题也开始凸显出来。计算机信息网络安全问题的出现制约了各个信息的有效使用，也限制了各个行业的发展，如何更好地发挥出计算机信息网络安全技术在各个领域中的应用作用成为相关人员需要思考和解决的问题。本文在分析计算机信息网络安全问题的基础上，就计算机信息网络安全技术的应用及安全防范进行分析。

一、网络安全与计算机信息管理技术概述

在现代计算机技术、网络技术快速发展和不断成熟，互联网逐渐普及的当下，网络安全逐渐成为与每个社会公民息息相关的事宜。在网络已然是国家不可或缺的一部分的情况下，网络安全自然而然地成为国家安全的一项基本内容。网络安全涉及的范围极广，既包括硬件安全，也包括软件安全，更包括信息安全。信息化时代背景下，网络信息安全的风险陡增，造成的威胁巨大。不管是个人隐私信息，还是企业机密信息，又或者是各种组织乃至国家机构的信息，都遭受着一定的网络信息安全威胁。无论是由于使用者本身的疏忽或问题导致的信息丢失、损毁和泄露，还是由于包括病毒、黑客攻击等在内的外在原因导致的信息安全问题，都是目前威胁网络信息安全的常见问题。如何有效保障网络安全尤其是网络信息安全，是信息化时代必须高度重视和要解决的问题。而计算机信息管理技术作为计算机应用与网络应用的关键技术，其本身内涵极为丰富，全面包含数据库技术、计算机网络技术、软件开发技术、程序设计技术等，在现代社会中有着广泛应用。在计算机信息管理技术的支持下，网络安全将进一步得到保障，实现对网络信息安全的有效检测与防护[1]。

二、计算机网络信息安全的风险

自然因素风险。计算机作为一个精密的软硬件结合机器，需要大量的基站、卫星建设。例如：手机通信的基站，从一代模拟移动通信系统到后来的 2G、3G、4G、5G，网络通信基站的建设密集程度、辐射强度直接决定了网络通信的流畅程度，随着基站的建设愈来愈频繁、数目越来越多，很大程度上增加了自然条件下设备受损的概率。自然因素风险主要包括各种自然灾害的发生，可能会造成基站受损、信息失联、数据丢失的情况。尽管自然灾害出现的概率相对较小，但一旦发生就很可能对信息网络造成不可逆转的坏结果。计算机很多时候由各种敏感材料组建，对于自然环境的要求有时是十分苛刻的，除了不可抗力的自然灾害外，环境的频繁改变

也会威胁到计算机网络安全，例如环境中的尘燥、湿度大以及温度过高等问题，都会影响计算机稳定运转[2]。

系统漏洞。计算机网络系统作为人为建设的系统，难免存在一定的漏洞。诸如计算机网络的不安全服务、配置以及初始化，均是较为常见的漏洞。如果计算机网络系统存在这些方面的漏洞，很容易导致整个系统瘫痪，进而给整个网络安全带来巨大威胁。一般来说，在对系统的各种操作和系统安全策略发生冲突时，就会产生安全漏洞，即系统本身不够完善，无法有效满足各种用户操作需求，而且很容易被病毒、木马以及黑客等入侵并攻击。

电脑病毒木马侵害风险。电脑病毒，这个新兴的名词已经是妇孺皆知，和人类生理病毒一样，电脑病毒也具有传播性、感染性极强的特征，计算机系统一旦感染这类病毒，各种垃圾文件就会像“外来物种”一样疯狂复制，充斥着计算机的硬盘，久而久之，计算机就被拖垮甚至被破坏。病毒对计算机系统的侵害一直都是难以解决问题，尽管市面上有很多不一样的杀毒防毒软件，但因其受众网民的专业化程度不高，对计算机系统的应用不够娴熟，很多时候会被伪装的病毒侵害，有些隐蔽性很强的木马软件也会植入到计算机软件程序中，实时监控计算机操作。因其广泛的传播范围、反反复复的衍生率而让大多数网民深受其害，让人防不胜防。所以，至今网络信息安全还是存在病毒侵扰这样的风险，也是网络信息安全技术人员重点关注的领域[3]。

三、计算机网络安全问题的防范对策

3.1 强化计算机网络使用者的防护意识

计算机管理人员安全意识的疏忽是导致整个系统运行陷入瘫痪以及危险境地的一个关键，因此，为了能够保障计算机网络系统的运行安全，需要计算机使用人员能够树立一种网络安全防护意识，通过积极全面的学习来掌握更多的信息管理技术在维护网络安全应用中的方法，并在这个过程中及时发现计算机网络系统运作存在的安全隐患，针对隐患问题及时采取有方法予以解决。

3.2 法律法规的可靠支持

法制部门可以通过网络片宣传、线下讲座、海报宣传形式强化民众的知法守法意识，提高受众对于网络信息安全的认知程度，让群众在发现网络信息安全违法行为的第一时间，学会运用法律手段、借助信息渠道进行积极维权；当然，公安部门也理应加强网络信息安全的出警成功率，让群众看到国家法律是实实在在存在的，是对民众有所承诺的，人民有反映，国家有回应，也是促进“全民皆兵”的一大保障。通过法制保障，能够使社会各类群体乃至每个个体都能对法律法规进行严格地遵守，这样可使计算机网络的使用变得更加规范、安全、合理。只有用户群体和服务群体双方共同努力，才能真正展现法律的权威，真正营造安全的网络环境[4]。

3.3 做好操作系统的防护工作

当前，计算机网络技术在社会范围内的应用愈发的广泛，对各个领域的发展产生了深刻的影响。为了保证计算机信息技术网络系统的安全运行，还需要相关人员能够采取积极的措施做好计算机信息网络系统的运行防护工作，在整个系统运作的时候引入漏洞检测技术形式，确保整个计算机网络安全操作系统能够始终保持在安全的运作状态。一方面，通过模拟黑客攻击的方法来检测计算机网络系统的运作漏洞。另一个方面，可以通过端口扫描的方法来检测计算机网络系统的漏洞问题，根据获取的目标主机网络信息来为之提供与之匹配的漏洞库，由此来检测计算机网络系统是否处于一种安全的工作状态，在发现系统漏洞的时候要及时采取措施予以解决，提出对应的补救措施。

3.4 网络安全与计算机应用的应用

网络加密技术。随着网络犯罪数量的逐步增多，计算机技术现今也被广泛应用在网络安全等领域中。首先计算机技术在网络安全方面的应用便是网络加密技术的实现。网络加密技术是指通过利用加密算法，从而将用户所发送的原有数据进行重写编写，进而实现对数据信息安全性的保障。在应用网络加密技术的过程中，发送方所发出的明文首先会使用密钥进行加密处理，此时密钥也会通过数字信封的形式发送至接收方。当接收方受到密文后其便可以利用密钥进行解密，从而获取信息内容[5]。

网络评估系统。借助计算机信息管理技术建设网络评估系统，能够实现对网络安全全面、全过程的评估，进而发现其中存在的数据异常、信息安全问题等。通过构建事前评估、事中评估以及事后评估程序的方式，对用户行为进行全过程评估。在用户进行操作之前，对系统自身的安全性进行全面评估；在用户进行操作的过程中，实时检测异常信息；在用户操作结束之后，对相应的结果进行评估。通过事前、事中与事后的全过程综合化评估，能够及时发现网络安全风险与威胁，进而为相应的网络安全防护提供支持。

身份验证技术。通过利用计算机技术也进一步加强了身份验证技术的普及。最初的身份验证技术便是通过账号、密码所实现的，但由于无论是账号或密码均存在信息泄露、数据丢失等风险。因此，为了进一步加强身份认证的安全性，诸多互联网企业又逐步推出了指纹认证、面部识别认证以及虹膜认证等身份验证技术。此类身份认证技术的加强不仅有效保障了用户信息的安全性，同时更为网络环境的可靠性与安全性的提升起到了一定的促进作用。

网络病毒的控制。病毒的控制也是强化计算机技术网络安全管理的关键，从当前发展实际情况来看，市场范围内出现了比较多的计算机网络系统病毒防范软件，在这些病毒防范软件的作用下提升了整个计算机系统的防病毒成效，即在检测的过程中如果发现了计算机网络

系统病毒，相关人员会立刻使用杀毒软件来对这些病毒信息予以拦截处理，并在此基础上对整个计算机系统软件开展全面的清查，确保病毒能够被清理干净。在计算机系统中常用的杀毒软件是木马查杀，这类软件在使用的时候会显示出较强的病毒预防功能，比如隔离沙箱能够为网络用户创设安全的系统运作环境，且在程序运行优化管理上也会显示出强大的优势作用[6]。

四、结束语

综上所述，网络信息安全技术管理问题也是伴随互联网应用衍生的问题，只

要还在应用，就一定有这样的问题存在。重视网络信息安全工作的建设，保障用户的信息安全，营造良好的网络环境，更加高效地应用互联网信息为人类社会创造更大的价值，是每一位互联网工作者都要思考的问题。

参考文献：

[1] 王征 , 陈晶 , 王盛 . 基于网络信息安全技术管理的计算机应用思考 [J]. 网络安全技术与应用 ,2017(04):1+6.

[2] 孙素萍 . 基于网络信息安全技术管理的计算机应用 [J]. 电子技术与软件工程 ,2019(03):165-166.

[3] 白兰 . 基于网络信息安全技术管理的计算机应用 [J]. 信息系统工程 ,2012(03):83-84.

[4] 张强 . 计算机网络的信息安全防护对策分析 [J]. 电子技术 ,2021,50(08):26-28.

[5] 刘艳 . 浅议网络信息安全技术管理的计算机应用 [J]. 梧州学院学报 ,2016,26(06):27-30.

[6] 袁伟伟 . 基于网络信息安全技术管理的计算机应用 [J]. 无线互联科技 ,2017(15):123-124.