探究电子计算机的信息数据安全

孙忠民
内蒙古兴安盟大数据中心　内蒙古兴安盟乌兰浩特　137400

摘　要：在信息技术快速发展的背景条件下，计算机网络已经成为社会主流应用方案，走进了各行各业并得到充分应用。通过合理应用计算机网络，可以进一步拓展信息传播渠道，提高其整合效率，具有节约人力成本、提高工作质量的重要用途。但是，计算机网络信息应用普遍存在风险问题，若未采取可靠防护方案，便有可能导致负面问题产生，引发不必要的损失出现。本文探讨了电子计算机信息技术数据安全的重要性分析，分析了计算机网络信息安全面临的主要问题，研究了计算机网络防护信息安全对策，以供参考。

关键词：电子计算机；信息安全；大数据；网络信息

Exploring the information data security of electronic computers

Zhongmin Sun
Inner Mongolia Xing’an League Big Data Center Inner Mongolia Xing’an League Ulanhot 137400

Abstract: Under the background of the rapid development of information technology, computer network has become the mainstream application scheme of society and has entered all walks of life and been fully applied. The rational application of computer networks can further expand the information transmission channels, improve integration efficiency, has the important use of saving labor costs, and improve the quality of work. However, there are risk problems in the application of computer network information. If a reliable protection plan is not in place, it may lead to negative problems and lead unnecessary losses. This paper discusses the importance of computer information technology data security analysis, analyzes the computer network information security facing the main problems, and studies the computer network protection information security countermeasures for reference.

Key words: electronic computer; Information security; big data; network information

引言

信息安全处理技术是互联网时代最重要的网络技术，因为它可以降低网民遭受网络病毒和黑客侵犯的概率，确保网络信息安全，营造安全良好的网络环境。传统信息安全处理技术属于被动防护型技术，且随着互联网技术的不断发展，这些技术呈现出较大的局限性和落后性，使得传统信息安全处理技术在信息处理效率和质量上不尽如人意，不再适应当前信息爆炸的网络环境[1]。为了提高信息安全处理效率和质量，需要引入新的信息安全处理技术，这就是本文要研究的基于电子计算机的信息安全处理技术。

一、电子计算机信息技术数据安全的重要性分析

随着时代发展计算机信息技术数据安全的重要性不断提升，计算机信息技术数据安全漏洞已成为我国社会发展的重要隐患。计算机信息技术数据安全是指通过采取科学的加密技术和以及其它技术措施保证数据安全性，提高计算机信息技术的防护等级，降低计算机信息技术数据泄漏问题发生率，对保障群众的个人数据以及企业的数据具有重要作用。按国家统计局以及网络安全部门发布的相关资料看，近年来因计算机信息技术数据泄漏问题导致的经济损失每年超过 200 亿元，其中主要包括企业财产损失和个人财产损失；我国有超过 3/4 的企业都出现过计算机信息技术数据泄漏问题，对企业的发展和经济效益提升造成了极为恶劣的影响。现阶段，我国计算机用户中超过 80% 遇到过计算机信息技术数据泄漏问题，其中有超过 75% 的计算机用户受到木马、黑客入侵导致数据泄漏的问题超过 3 次[2]。计算机信息技术数据泄漏问题已对我国社会发展以及人民群众的日常生活造成很大的影响，一些不法分子通过入侵计算机网络信息系统非法获取用户的个人信息和数据，对用户造成了巨大的财产损失，严重影响社会的和谐和稳定。在群众对个人数据因素保护意识不断提高的背景下，关于计算机信息技术数据泄漏的问题也受到社会各界的广泛重视，国家网络安全部门相继出台多项措施，对内网和外网的安全防护等级进行全面提升，同时可用于计算机信息技术数据安全防护的加密技术也在不断创新，从而

使我国计算机信息技术数据泄漏问题得到较为有效的控制，但从整体情况看依然存在一些较为严重的问题，缺乏更为先进的加密技术和系统保护技术，计算机信息技术数据加密技术没有达到企业生产与群众日常生活的需要，相比于当前计算机信息技术发展较为落后，因此需针对不同的计算机信息技术数据泄漏问题，采用不同的计算机数据加密技术，加强计算机信息技术数据安全防护措施的创新，从而更好地保护我国社会群众的财产和数据安全。

二、计算机网络信息数据安全面临的主要问题

2.1 网络自身存在问题

计算机网络在应用过程中，往往面临较为复杂的主要风险问题。例如，网络本身会产生一定程度的安全风险，其破除了原有脱机体系下存在的信息传递时间与空间限制，使相关数据的共享途径得到显著拓展。但是，这一特性同时也加大了信息泄露风险，容易导致不必要的损失出现。在强开放性特征下，计算机网络传递途径可能会被黑客所利用，通过系统漏洞侵入本地环境，最终导致数据泄露或损坏。同时，一部分网络出于成本或兼容性考虑，未设置身份验证策略或设置不正确，导致不法分子利用简单脚本软件即可实现全自动扫描与入侵，大幅增加了计算机网络环境整体风险，不利于信息安全保护理念的落实[3]。因此，需要重视计算机网络在应用过程中存在的安全风险问题，并采取有效措施进行防范。

2.2 不法分子对计算机网络的攻击

根据当前的网络使用情况来看，计算机网络信息安全面临的最大威胁是不法分子的恶意攻击。例如不法分子会将自己编写的各种木马程序投放到计算机网络中，若用户在使用计算机的时候操作不当，计算机就容易被木马程序入侵，而这些木马程序在编写的时候本身就具有一定的针对性，比如针对性地窃取用户网络数据信息和行业机密等。现在，随着电商行业的发展，网络购物已经成为人们的日常所需，人们在进行网络购物的时候不仅要填写自身信息，还需要填写银行卡信息，有些针对性木马程序就会盗取相关的信息，直接威胁用户的财产安全。还有些木马程序针对性篡改和破坏信息，造成重要用户数据丢失，继而造成巨大的经济损失。最具代表性的就是最近全球范围内爆发的 “ 比特币病毒（WannaCry ）”，它是一种 “ 蠕虫式 ” 的勒索病毒软件，一旦感染，用户计算机中的所有图片、视频、文档等文件都会被锁住，用户要想使用，就必须要支付一定的比特币才行，大量计算机用户的工作和生活受到严重影响，全球计算机网络安全也受到了极大的破坏[4]。

2.3 防火墙安全漏洞问题

防火墙是保护用户计算机信息系统的重 要 安全组件，但受到技术水平的限制，当前许多用户采用的防火墙系统存在较多漏洞，木马病毒、非法入侵等能通过防火墙系统的安全漏洞轻而易举进入用户的个人数据库中，在用户没有察觉的情况下搜集用户的大量数据，且防护难度较大，即使用户查看防火墙日志等也难以及时察觉，当前防火墙系统中还存在着较多的漏洞，是威胁计算机用户数据安全的重要因素，所以需加强对防火墙安全漏洞的管理。

三、确保电子计算机数据信息安全的处理策略

3.1 利用大数据加密技术实现信息安全处理

为了更好地保证计算机大数据的信息安全处理，就要相应提高相关操作人员的安全操作意识。因为在实际的情况中，大数据处理和人们的工作和生活有着密切的关系，在使用中为了保证大数据的安全和数据传输的安全，相关人员就要在进行操作的时候重视操作安全，实现大数据的加密处理。因为实际操作中的安全隐患是无处不在，应该引起操作人员重视，不要随意点击未知连接，防止造成病毒侵入。在正常使用的过程中，为了保证操作的可靠性，尽量不要随意对非法网页进行登录，从而保证大数据处理稳定性和安全性。同时在使用过程中，要注意对数据及时储存，科学实现对大数据处理信息进行储存和加密，保证数据的安全性。因为计算机大数据信息具有其自身的价值，所以在实际的处理储存过程中，还是需要进行特别管理，在信息存储安全要求较高的情况下，当然也可以单独对大数据进行储存和处理，从而进一步保证大数据的信息安全。

3.2 应用病毒防护与防火墙

计算机平台软硬件属于网络信息技术应用的基础架构，为尽可能提高安全级别，应当重视软硬件平台的防护对策部署，以确保相关体系具有健全特征，降低出现不良问题的概率。针对软件平台进行防护，可以通过安装病毒防护软件与防火墙软件等途径，强化计算机本地对于信息的保障力度。当前，病毒防护方案能够集成入侵检测、应用程序控制、启发式分析等多种先进技术。这些技术可以有效提高软件平台应用安全性，使网络信息传递能够在理想条件下执行，最大限度降低风险级别。除此之外，防火墙还可以部署硬件防护类型。硬件防火墙相对于软件能够承受较大的流量攻击，如 DDOS 等，有利于保障计算机网络应用可靠性，避免由于违规操作引发的瘫痪问题。因此，需要重视软硬件防护对策的应用，确保相关负面因素能够得到排除，实现理想控制目标。(2) 及时修补系统漏洞。漏洞属于计算机系统与网络系统不可避免的缺陷，其本质上与底层逻辑以及程序编写方式存在关联，无法预先解决。因此，为降低漏洞对计算机网络信息产生的负面影响，应当采取漏洞同步修护策略，确保相关系统能够及时获取更新补丁，解决程序中存在的漏洞，避免受到针对性网络攻击。大部分网络信息攻击风险均需要利用潜在漏洞，使自身能够获得系统最高权限，进而执行破坏指令。通过设立相关条例规范漏洞更新，或定期检查漏洞情况，可以避免漏洞被

不法分子所利用，损害计算机网络信息传递体系。因此，需要重视漏洞更新工作，确保系统能够在理想条件下运行，提高网络信息技术应用安全性。

3.3 运用软件加密技术

软件安全漏洞是威胁计算机用户数据安全的主要因素之一，所以需用科学的软件加密技术，当前应用作为广泛的为计算机杀毒软件，通过在计算机中配置相应的杀毒软件，该杀毒软件能定期对计算机中的数据进行扫描，当扫描到异常数据时会对该数据进行清理，在防范木马病毒方面具有重要的作用，能有效修复计算机信息系统存在的数据漏洞问题。当前市场中存在多种不同类型的杀毒软件，对常规的诱导性网页链接和木马病毒都能起到良好的保护作用，主要是因杀毒软件中采用较为先进的加密技术，通过安装软件则能提高计算机信息系统的数据安全防护能力，是应用最广泛的一种加密技术形式。

四、结束语

随着科技的不断发展，计算机的使用已经渗透到人们工作生活的方方面面，计算机网络的安全问题也开始日渐增多，我们不仅要提升用户计算机网络安全的防护意识，还需定期扫描系统，及时发现并修复系统漏洞，以保障计算机网络信息的安全性。

参考文献：

[1] 罗键新 , 陈嘉升 . 高校计算机网络信息存在的安全问题及防范对策分析 [J]. 信息记录材料 ,2021,22(10):38-39.

[2] 徐大海 . 数据加密技术应用在计算机网络信息安全中的应用 [J]. 中国新通信 ,2020,22(10):88-89.

[3] 杨佳 . 计算机网络信息管理及其安全防护策略 [J]. 贵州农机化 ,2021(4):47-48+51.

[4] 陈富斌 . 关于计算机网络安全防范措施的思考 [J]. 电脑与电信 ,2021(12):84-85.