浅谈计算机网络技术与安全管理维护

高敬瑜

（无锡商业职业技术学院，江苏　无锡　214151）

摘要：随着信息时代的到来，计算机网络技术已经得到广泛而具有普及性的应用。目前，我国已全面步入信息化时代，互联网技术的诞生给我国民众的生活、学习及工作带来了巨大的改变。但日益扩大的信息数据库规模，也给我国的信息安全带来了极大的考验。如何有效地对信息进行安全管理，成为现阶段我国信息化社会发展亟待解决的问题。基于此，本文将通过分析计算机网络技术与安全管理维护的特点及实施安全管理维护的必要性，探索影响网络安全的主要因素，并对计算机网络安全管理的优化提出一系列举措，以期能够提高网络环境的安全性，从而保障我国民众的根本利益。

关键词：计算机网络技术；安全管理维护；影响因素；优化措施

中图分类号：TP393　　**文献标识码：**A

DOI：10.12230/j.issn.2095-6657.2022.29.029

随着我国信息技术的不断发展，大众获得信息的方式也出现了变化。更方便的信息获取渠道，让民众能轻松地获取信息。然而，在计算机日益广泛的应用背景下，其安全隐患也逐渐暴露无遗，并且不能从根本上杜绝这些安全隐患。如何提高计算机网络安全技术，高效地开展网络安全管理维护，提高网络安全性能，是目前实现我国信息技术进一步发展中亟待解决的问题。因此，本文将结合相关概念内涵，重点探索影响网络安全的主要因素，并对计算机网路安全管理及维护提出一系列优化措施，旨在提高我国的计算机网络安全性，从而保障我国民众的根本利益。

1 计算机网络安全管理维护特点

1.1 完整性

信息储存是计算机网络数据库最基础的作用，也是计算机网络数据库存在最基本的价值。而计算机网络数据库安全管理是信息完整性的重要保障，若在计算机数据库中出现一些漏洞，会致使信息泄露或丢失，从而对信息的完整性造成一系列影响。因此，计算机网络安全管理最重要的一点就在于保证信息数据的完整性，对所有信息数据进行全面的记录。除此之外，还需要对储存的信息进行定期维护，这样才能保证信息数据的完整性不被损坏。

1.2 安全性

信息安全是计算机网络中尤为注重的一部分，因为缺乏安全特性的计算机网络数据库既不能向用户提供安全的信息，也不对能对数据库中的信息提供充足的安全保障。关于计算机网络数据库中的安全性问题，主要涉及以下两个层面：其一，是在信息储存过程中的安全性；其二，是要保障信息的完整度。为了提高信息安全性能，首先，需要建立起一套完善的安全系统，并对其进行管理和维护，避免信息从内部损坏；其次，为了保障信息在传输过程中的安全性，需要对传输的信息保密，并加大安全管理力度，使信息在传输过程中不会出现泄露或被拦截的情况。在保证这两点的前提下，才能使信息数据库正常运转。

1.3 实时性

实时性表现在数据库内的信息在不断地更新 . 若数据库出现运行故障，且故障的持续时间过长，则会致使用户在接收信息的过程中受到严重的干扰。因此，对网络数据库内的信息进行实时监管，能够有效地保障信息在运转过程中的有效性及可靠性。

2 计算机网络技术安全管理的必要性

2.1 保护数据库内信息安全

数据库内的信息丰富且多样，覆盖的领域也极其广泛。这些信息不仅对个人有非常重要的影响，也对整个社会具有重大影响。一旦发生信息泄露，则会对个人及整个社会带来巨大的损失。因此，对计算机网络技术实施安全管理，能够有效地保障数据库内的信息不被泄露，对整个社会具有重要意义。

2.2 保护操作系统安全

现今，信息技术迅速发展，有一部分计算机并没有对其操作系统起到一定的保护作用。对于黑客而言，这无疑是将操作权限拱手让人，他们能够在有限的信息中获取计算机的操控权，从而盗取其中的信息资源[1]。因此，计算机网络技术的安全管理对于操作系统的安全性而言，更加不容忽视。

3 影响计算机网络安全的因素

3.1 系统漏洞

网络技术是将所有的计算机串接在一起。计算机的软件及

硬件是计算机在网络运行中的安全保障，能够避免计算机系统被入侵[2]。目前，计算机系统都有着较为丰富的防入侵经验，在不断的发展过程中，对系统存在的漏洞也在进行不断的优化和完善。但在网络中，仍然会有威胁到计算机系统安全的因素存在，在众多未知网络中，安全性能较差的网络也有很多，其系统的漏洞也会逐渐显现，让黑客有机可乘。网络世界极为复杂，现阶段的所有计算机系统都不能做出绝对安全的保证，而系统的漏洞成为影响计算机网络安全的重要因素之一。

3.2 病毒入侵

病毒入侵是一种对计算机和互联网危害极大的入侵方式，其具有巨大的破坏力和传染性[3]。比如当时影响很大的“Sobig病毒”和“熊猫烧香病毒”等,给社会经济都带来了巨大的破坏。“Sobig病毒”的主要侵入手段是让用户下载带有病毒的电子邮件，并以此盗取客户的个人信息；而“熊猫烧香病毒”的侵入手段则主要是利用浏览器来破坏手机中的应用软件，其中就连杀毒软件也可能遭到破坏。

目前，病毒的类型、侵入手段、攻击方式等都越来越多样化，最常用的病毒类型包括脚本、木马等病毒。其中，木马病毒的入侵方式尤为突出，它藏匿在一段看似普通的程序中，但这个程序一旦被用户运行，便会与病毒的传播者建立联系，让其能够远程操控用户的计算机，从而盗取用户计算机中的信息及资料，甚至能够让计算机超负荷运行，从而破坏计算机的硬件系统，对用户造成严重的损失。随着电脑的广泛使用，其防病毒入侵系统也愈加健全，两者之间的斗争仍在继续；而加大对防病毒入侵软件的开发和完善，能够在最大程度上为用户的信息安全提供保障。

4 计算机网络安全技术

计算机网络安全技术是指对网络信息采取一系列保护措施，并将信息数据准确、迅速地传送至每一位用户的一项技术，用户也能在网络中对信息进行安全的接收和传输[4]。目前，最常用的计算机网络安全技术主要有以下几个方面：

4.1 防火墙技术

在现代的计算机网络安全体系中，防火墙技术具有很重要的地位，因为它们共同承担了对计算机软件与硬件之间的安全防护工作。在现代计算机系统中，在被防护网络和其他网络系统之间的边界部分，主要是为了对网络的实施管理、分析网络中的行为信息，而一旦出现和数据流相悖的错误消息之后，便建立起防火墙。

防火墙技术，除了可以遏制外界的危害影响之外，还具备维护国内有价数据不外传的功能，维护了互联网安全。基于其应用手段的不同，防火墙产品的应用大致分为两类：一类是网络防火墙，另一类是应用级网关。网络防火墙主要是针对网络信息的完整性进行筛选、处理，其检测重点主要是对数据流中的重要信息，并进行正确性判定分析且加以过滤，对不符合要求的信息进行废弃处理。应用级网关主要是根据专门的应用服务技术进行信息筛选处理的，一般适用于系统的复杂访问，在信息复制与传递中检验其安全性，以起到保护服务器和客户机的目的。

4.2 数据加密技术

信息加密技术，也是十分常见的基础性信息安全技术手段，是现代网络安全的重要基础之一[5]。由于其能力的提高，在最初的信息保存与传递的私密性方面上升到了密文保送的层次，即在传送过程中使旁人不能了解其传递讯息的具体内容。这种方法的使用安全性，关键于其所采用的密码方法和密码方式。而鉴于使用密码的不同特性，现代密码方法又主要分为对称性加密算法和非对称加密算法。对称性加密算法的方式具备一致性，密码的复杂性决定了安全性能的有效性，这种加密方法能够更为迅速地识别用户身份，进行加密和解密的操作；非对称加密算法的方式与之不同，其解密的操作更困难，需要用户告知解密方式才可进行。

4.3 网络入侵检验技术

计算机网络入侵检测技术也称为实时监测技术，主要作用就是对计算机软件和硬件中的流通信息进行检测，如果找到危险源或被入侵的部分，就可以做出断网、通知防火墙的反应，从而对重大危险源作出过滤处理[6]。该功能的使用，具备监测网络安全并发现实施攻击者的功能。但是，它仅仅以一种安全组件的方式而存在，并不能独立使用，而是要结合相应的技术才能使用。

5 计算机网络安全管理维护

5.1 网络故障管理

在网络管理中，计算机的网络故障管理对于网络的运行发挥着最为基本的作用。若网络在运转过程中出现故障，它就能迅速地找出故障发生的具体位置，并消除故障。通常而言，产生网络故障的原因有很多种，对故障进行分析的过程较为繁琐，因此，仅仅采取简易的隔断举措并不能消除故障，而是要采用网络修复技术。基于此，对网络运行中所产生的故障进行具体分析，当网络运行产生故障时，需要实施的管理步骤包括检测网络故障、隔断故障源、修复故障。在故障检测过程中，要依据网络运行的检测报告实施故障管理措施。如果故障简单，则不会影响网络系统的正常运转，则只记录故障；如果故障较为严重，已对网络系统造成威胁，就需要采用网络管理器运行技术处理措施。尤其是由于多种原因而导致的网络运转故障时，

则需要网络管理器对故障产生的原因进行测试，据此作出判断。

5.2 网络配置管理

电脑的网络配置管理所实现的主要功能就是分配网络上数据信息，在网络进入到初始化的工作状态以后，能够按照要求分配上网数据信息，保证各种网络服务的顺利进行。计算机网络要保持良好的工作态势，对计算机网络设置对象所起到的影响也是不容忽视的，主要设置的工作对象包括定义组、监视组、辨别组、控制组等。这种设置方式不仅能够保证在计算机网络工作中得到优质服务，同时能够确保计算机网络的各种特性保持态势。

6 计算机网络数据库安全管理技术的优化

6.1 安全管理模式

网络安全管理，也是计算机数据库安全的非常重要的一个方式，可以更合理地对计算机网络体系加以改造，修补系统漏洞，从而达到提升计算机安全水平的目的[7]。由于计算机网络体系较为繁杂，普通用户也很难更合理地对计算机进行保护，所以，安全网络模式就为个人用户提出了一种更加科学、合理的防护方式与对策。当用户开启安全模式之后，可以从多方面全面增强计算机的稳定性。集中式管理机制、分布式管理机制以及静态分层模式都是当前较为常见的一种安全模式，但是每个模式都有各自的优点与不足。因为分布式管理机制的安全性问题，在行业中的使用并不普遍，但是集中式管理机制已经普遍应用于各种环境。计算机的安全模式可以把数据资料分类存放到计算机系统中，同时可以对不同行者的信息进行分类管理，并设置不同等级的密码，进而实现管理目的的差异性，提高网络安全性能。除此之外，在电脑中要处理数量较多且较为复杂的信息时，可以利用安全管理模式，对这些信息进行识别检验，从而保障信息的安全，为网络系统创建安全的环境。

6.2 数据加密技术处理

数据加密技术是网络安全管理中一项十分重要的技术，也是使用率最高的一项技术，能够有效地起到防止病毒入侵的作用。数据加密技术主要是利用一些语言程序对数据进行保密管理。数据进行保密处理以后，所保存的数据被黑客或者病毒攻击的概率大大降低，所以就算数据被黑客或者病毒攻击之后，能破解出来的概率也是非常低的，甚至完全没有方法破解，因此，被暴力检测的成功率小于其他模式。虽然这种加密技术十分安全，不仅对系统信息起到良好的保护作用，也能在信息传输途中进行加密处理。不过，现阶段很难实现这一目的，由于现代的数据已过于丰富，在大数据时代对各种文件都进行加密处理是不能实现的。但是，可以针对部分比较大的数据进行保密处理，可采用划层次的方法，对相关信息进行加密处理，从而保证了数据的安全。在进行加密的过程中，也可以采用多种不同的方法，以提高黑客破解的难度，但过于单纯的密码设置方法会更容易被破解，而失去了信息本身的意义。

6.3 应用数据备份及恢复技术

在计算机的运行中，经常会由于硬件或是人为原因而造成各种问题，最严重的问题会导致信息的丢失与泄露，从而造成更大的经济损失。为了避免这些重大事故的出现，需要将数据备份和数据恢复技术全面运用，才能在根本上减少这类事故所造成的损失。目前，主要的备份和恢复方法是将信息拷贝至其他设备中，若信息所在的主机受到破坏而导致信息丢失，则可以在拥有备份的设备上将信息源进行有效找回，从根本上解决了信息丢失的问题，减少了因信息丢失而带来的损失。就现阶段而言，会出现以上问题的主要原因在于电脑系统出现故障、电力故障及人为造成的故障等。信息的备份和恢复技术，在解决这类故障方面都有良好的应用效果。

7 结语

综上所述，计算机的广泛使用标志着我国已经全面步入信息化时代，而计算机网络的安全性是每位网民基本利益的重要保障。为了有效地提高计算机网络技术与实现安全管理维护，需要充分考虑各种安全网络管理技术手段的使用能力与实用价值，为国家营造安全的计算机网络环境提供强大的科技保障。

参考文献：

[1]董景利.计算机网络技术与安全管理维护初探[J].数字通信世界，2020,(04)：1.

[2]王仕艳.探究计算机网络数据库安全管理技术的优化分析[J].信息通信，2020,(07)：158-159.

[3]赵越.基于计算机网络技术的计算机网络信息安全及其防护[J].电子世界，2020,(13)：2.

[4]王哲.探讨如何实现大数据时代的计算机网络信息安全[J].现代工业经济和信息化，2022，12(07)：125-126.

[5]杨光.计算机网络信息安全技术应用[J].无线互联科技，2022，19(09)：38-40.

[6]刘荣,吴万琼,陈鸿俊.计算机网络入侵与防御技术[J].电子技术与软件工程，2021,(11)：247-248.

[7]李健，李小虎，焦志勇.浅析计算机信息管理技术在维护网络安全中的应用[J].中国新通信，2020，22(20)：2.

作者简介：高敬瑜（1967-），男，河南禹州人，副教授，硕士研究生，主要从事计算机应用技术研究。